WP2018-2020 SC7

Call SU-INFRA

Workshop with the ICT National Contact Points
18 July 2019

CNECT.H1 Cybersecurity Technology & Capacity Building

Call - Protecting the infrastructure of Europe and the people in the European smart cities

H2020-SU-INFRA-2018-2019-2020

SU-INFRA01-2018-2019-2020:

PREVENTION, DETECTION, RESPONSE AND MITIGATION OF COMBINED PHYSICAL AND CYBER THREATS TO CRITICAL INFRASTRUCTURE IN EUROPE

SU-INFRA01-2018-2019-2020

1. What are you looking for? (1 of 4)
   - State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure.
   - Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure.
   - In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.

SU-INFRA01-2018-2019-2020

1. What are you looking for? (2 of 4)
   - Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure.
   - Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the critical infrastructure.
   - Security risk management plans integrating systemic and both physical and cyber aspects.

SU-INFRA01-2018-2019-2020

European Commission

1. What are you looking for? (3 of 4)
   - Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure.
   - Where relevant, test beds for industrial automation and control system for critical infrastructure in Europe, to measure the performance of critical infrastructure systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines.
   - Test results and validation of models for the protection of a specific critical infrastructure against physical and cyber threats.
   - Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats..

SU-INFRA01-2018-2019-2020

1. What are you looking for? (4 of 4)
   - Convergence of safety and security standards, and the pre-establishment of certification mechanisms.
   - Secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
   - Contributions to relevant sectorial frameworks or regulatory initiatives.

SU-INFRA01-2018-2019-2020 : Specific Challenge

- Disruptions in the operation of our countries' critical infrastructure may result from many kinds of hazards and physical and/or cyber-attacks on installations and their interconnected systems.
- 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.
- Budgetary constraints on both the public and private sectors mean that new security solutions must be more accurate, efficient and cost-effective, and possibly more automated than the ones currently available.

SU-INFRA01-2018-2019-2020: Scope (1 of 6)

- Proposals should cover 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, over the life span of the infrastructure,
- with a view to achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

SU-INFRA01-2018-2019-2020: Scope (2 of 6)

- Proposals should:

(a) assess in detail all aspects of interdependent physical (e.g. bombing, sabotage and attacks with a variety of weapons against installations, buildings and ships; plane or drone overflights and crashes; spreading of fires, floods, landslides, disastrous consequences of global warming, seismic activity, space weather, combined threats, etc.) and cyber threats and incidents (e.g. malfunction of SCADA system, non-authorised access of server, electronic interference, distributed attacks), and the cascading risks resulting from such complex threats,

SU-INFRA01-2018-2019-2020: Scope (3 of 6)

(b) demonstrate the accuracy of their risk assessment approach using specific examples and scenarios of real life and by comparing the results with other risk assessment methodologies,

(c) develop improved real-time, evidence-based security management of physical and cyber threats, taking account of the ageing of existing infrastructure,

and (d) provide scenarios and recommendations for policy planning, engagement of the civil society, and investment measures encompassing all aspects of prevention-detection-response-mitigation

SU-INFRA01-2018-2019-2020: Scope (4 of 6)

Innovative methods should be proposed for sharing information with the public in the vicinity of the installations - including through social media and with the involvement of civil society organisations -, for the protection of first responders such as rescue teams, security teams and monitoring teams, and for ensuring service continuity

In 2020, while keeping the coverage of the assessment of risks, prevention, detection, response and mitigation of consequences, proposals should also address the interrelations between different types of critical infrastructure with the objective of developing tools and methods to minimise cascading effects and allow rapid recovery of service performance levels after incidents.

SU-INFRA01-2018-2019-2020: Scope (5 of 6)

When selecting for funding the proposals submitted in 2018 or 2019 or 2020, the Commission will take due account of similar projects financed in the previous years since 2016, with a view to cover the largest possible spectrum of installations. Each year, a list of infrastructures excluded from the Call will be published on the Funding and Tenders Portal.

Consortia should involve the largest variety of relevant beneficiaries, including infrastructure owners and operators, first responders, industry, technologists and social scientists, etc. The participation of SMEs is strongly encouraged.

SU-INFRA01-2018-2019-2020: Scope (6 of 6)

In line with the EU's strategy for international cooperation in research and innovation international cooperation is encouraged, and in particular with international research partners in the context of the International Forum to Advance First Responder Innovation in which the Commission has decided to participate.

SU-INFRA Call in SC7

Type of Action: IA **SU-INFRA01-2018-2019-2020**

Budget: 20.7 MEUR

Expected EU contribution/project: 7-8 MEUR

Duration: maximum 24 months

Expected final TRL: 7

- **At least 2 operators in at least 2 EU of Associated countries.**
- **Participation of industry able to provide security solutions is required.**

GA 30.3 option to object transfer to third countries

Opening: 12/03/2020

Deadline: 27/08/2020

SU-INFRA01-2018-2019-2020

3. Is this new or has it been called before?

This topic was called in 2018 and in 2019.

*The predecessor topic **CIP-01-2016-2017** was called in 2016 and 2017.*

It is linked to other topics in the current WP:

Cybersecurity Call in the LEIT programme

Digital Security Call in SC7

SU-INFRA01-2018-2019-2020

5. Current project portfolio

RESISTO, FINSEC, STOP-IT,

DEFENDER, SAURON, SAFECARE

InfraStress, SecureGas, SATIE

SU-INFRA01-2018-2019-2020

7. Are there any additional / background documents?

- **European Agenda on Security - Communication "The European Agenda on Security" of 28.4.2015 – COM (2015) 185 final**
- Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" - JOIN(2017) 450 final, Brussels, 13.9.2017
- Digital Single Market Strategy - Communication "A Digital Single Market Strategy for Europe" of 6.5.2015 - COM(2015) 192 final
- NIS Directive - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Cybersecurity cPPP

Proposal for a European Cybersecurity Competence Network and Centre (COM 2018) 630 final.

Upcoming events / information days

9. Please list upcoming information days and other events of relevance to this area

ICT Proposers' Day 2019 at Helsinki scheduled 19-20 September 2019.

Security Research Event at Helsinki scheduled 6-7 November 2019 (organized by DG HOME and DG CONNECT).

WP2018-2020 SC7 Call AI and Security H2020-SU-AI-2020

Workshop with the ICT National Contact Points
18 July 2019

CNECT.H1 Cybersecurity Technology & Capacity Building

Call - Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe

H2020-SU-AI-2020

Interconnected aspects to be addressed to provide support to LEAs:

1. How can AI help LEAs in preventing, detecting and investigating criminal activities and terrorism and in monitoring borders?
2. At the same time, in order to support LEAs in their work, how can the malicious use of AI tools for criminal activities and terrorism be prevented, including malicious use of the AI tools developed in point 1?
3. Then, how can the AI tools used by LEAs, including the ones in point 1, be protected against cyber threats and attacks?
4. Finally, how can AI help in protecting LEA infrastructures from cyber threats and attacks?

SU-AI01-2020:

DEVELOPING A RESEARCH ROADMAP REGARDING ARTIFICIAL INTELLIGENCE IN SUPPORT OF LAW ENFORCEMENT

SU-AI01-2020

1. What are you looking for?
   - Identification of key areas in which AI would beneficial for LEAs, meeting their operational and collaborative needs, and of key areas in which it could pose a threat to security.
   - A carefully planned roadmap in order for Law Enforcement to benefit as much as possible from the AI based technologies, systems, solutions, including their protection.
   - Increased awareness regarding the state of the art and trends in AI-based criminal activities.

SU-AI01-2020: Specific Challenge

- There is a need to better understand:
  - how AI-based systems, services and products could enhance the objectives of the security sector;
  - how AI technologies can be protected from attacks;
  - how to address any potential abuse of AI for malicious purposes;
  - how to establish cybersecurity requirements for AI.

- From the Law Enforcement point of view, these dimensions have to be analysed in a longer term, taking into account that the potential AI benefits for Law Enforcement Agencies (LEAs) are threefold, i.e., through:
  - 1) proactive policing (from reactive to anticipative policing);
  - 2) data analysis (e.g., connecting the dots, discovering criminal patterns and defragmenting LEA actions), and
  - 3) identity checks (improving detection, targeting and interdiction).

SU-AI01-2020: Scope (1 of 2)

- provide an EU AI roadmap for LEAs, meeting their specific operational and cooperation needs,
- provide recommendations for further work to be done under Horizon Europe, Digital Europe, or the Internal Security Fund as well as for policy and market uptake.
- which AI based technologies, systems and solutions could support/enhance the work of LEAs and how, what the corresponding restraints (including ethical and legal) are, as well as related risks, security challenges and protection measures.

SU-AI01-2020: Scope (2 of 2)

- provide specific real-life LEAs scenarios, examples and evidence supporting their recommendations.

- The proposing consortium is expected to incorporate relevant security practitioners, researchers, civil society organisations and LEAs.

- proposals should foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices

AI and Security Call in SC7

SU-AI01-2020

Type of Action: CSA
Budget: 1.5 MEUR
Expected EU contribution/project: 1.5 MEUR
Duration: maximum 60 months
At least 3 LEAs from at least 3 EU of Associated countries

Complementary grants GA options for SU-AI0x, x=1,2 and 3
GA 30.3 option to object transfer to third countries

Opening: 12/03/2020
Deadline: 27/08/2020

SU-AI01-2020

3. Is this new or has it been called before?

This topic is rather new.

It is linked to other topics in the current WP:

Robotics, Big Data, IoT topics and Cybersecurity Call in the LEIT programme

Digital Security Call in SC7

SU-AI02-2020:

SECURE AND RESILIENT ARTIFICIAL INTELLIGENCE TECHNOLOGIES, TOOLS AND SOLUTIONS IN SUPPORT OF LAW ENFORCEMENT AND CITIZEN PROTECTION, CYBERSECURITY OPERATIONS AND PREVENTION AND PROTECTION AGAINST ADVERSARIAL ARTIFICIAL INTELLIGENCE

SU-AI02-2020

1. What are you looking for? (1 of 4)
   - Development of a European representative and large enough high-quality multilingual and multimodal training and testing dataset available to the scientific community that is developing AI tools in support of Law Enforcement;
   - EU common approach to AI in support of LEAs, centralized efforts as well as solutions on, e.g., the issue of huge amount of data needed for AI.

SU-AI02-2020

1. What are you looking for? (2 of 4)

- Improved capabilities for LEAs to conduct investigations and analysis using AI, such as a specific environment/platform where relevant AI tools would be tailored to specific needs of the security sector including the requirements of LEAs;
- Ameliorated protection and robustness of AI based technologies against cyber threats and attacks;
- Raised awareness and understanding of all relevant issues at the European as well as national level, related to the cooperation of the scientific community and Law Enforcement in the domain of cybersecurity and the fight against crime, including cybercrime and terrorism regarding the availability of the representative data needed to develop accurate AI tools;
- Raised awareness of the EU political stakeholders in order to help them to shape a proper legal environment for such activities at EU level and to demonstrate the added value of common practices and standards;
- Increased resilience to adversarial AI.

SU-AI02-2020

1. What are you looking for? (3 of 4)

- Improved capabilities for trans-border LEA data exchange and collaboration;
- Modernisation of work of LEAs in Europe and improvement of their cooperation with other modern LEAs worldwide;
- A European, common tactical and human-centric approach to AI tools, techniques and systems for fighting crime and improving cybersecurity in support of Law Enforcement, in full compliance with applicable legislation and ethical considerations;
- Fostering of the possible future establishment of a European AI hub in support of Law Enforcement, taking into account the activities of the AI-on-demand platform;

SU-AI02-2020

1. What are you looking for? (4 of 4)

- Making a significant contribution to the establishment of a strong supply industry in this sector in Europe and thus enhancing the EU's strategic autonomy in the field of AI applications for Law Enforcement;

- Creation of a unified European legal and ethical environment for the sustainability of the up-to-date, representative and high-quality training and testing datasets needed for AI in support of Law Enforcement; as well as for the availability of these datasets to the scientific community working on these tools;

- Development of EU standards in this domain.

SU-AI02-2020: Specific Challenge (1 of 2)

- Research is needed to assess 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 (LEAs) at national and at EU level to identify and successfully counter those threats.

- data quality, integrity, quantity, availability, origin, storage and other related challenges are critical, especially in the EU-wide context.

SU-AI02-2020: Specific Challenge (2 of 2)

- For AI made in Europe, three key principles are: "interoperability", “security by design” and “ethics by design”.

- Potential ethical and legal implications have to be adequately addressed so that developed AI systems are trustworthy, accountable, responsible and transparent, in accordance with existing ethical frameworks and guidelines that are compatible with the EU principles and regulations

SU-AI02-2020: Scope (1 of 6)

- exploring use of AI in the security dimension at and beyond the state-of-the-art, and exploiting its potential to support LEAs in their effective operational cooperation and in the investigation of traditional forms of crime where digital content plays a key role, as well as of cyber-dependent and cyber-enabled crimes

- 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, in support of LEAs to better prevent, detect and investigate criminal activities and terrorism and monitor borders, i.e., opportunities and benefits of AI tools and solutions in support of the work of Law Enforcement and to strengthen their operational cooperation.

SU-AI02-2020: Scope (2 of 6)

- establish a platform of easy-to-integrate and interoperable AI tools and an associated process with short research and testing cycles, which will serve in the short term perspective as a basis for identifying specific gaps that would require further reflection and development

- develop cybersecurity tools and solutions for the protection of AI based technologies in use or to be used by LEAs, including those developed under this project against manipulation, cyber threats and attacks,

SU-AI02-2020: Scope (3 of 6)

- exploit AI technologies for cybersecurity operation purposes of Law Enforcement infrastructures, including the prevention, detection and response of cybersecurity incidents through advanced threat intelligence and predictive analytics technologies and tools targeting Cybercrime units of LEAs, Computer Security Incident Response Teams (CSIRTs) of LEAs, Police and Customs Cooperation Centers (PCCCs), Joint Investigation Teams.

- tackle the fundamental dual nature of AI tools, techniques and systems, i.e.: resilience against adversarial AI, and prevention and protection against malicious use of AI (including malicious use of the LEA AI tools developed under this project) for criminal activities or terrorism.

SU-AI02-2020: Scope (4 of 6)

- address the problem of securing European up-to-date high-quality training and testing data sets in the domain of AI in support of Law Enforcement, proposals under this topic should, from a multidisciplinary point of view, identify, assess and articulate the whole set of actions that should be carried out in a coherent framework *(refer to the call for details)*

- Taking into account the European dimension of the topic, the role of EU agencies supporting Law Enforcement should be exploited

SU-AI02-2020: Scope (5 of 6)

- Proposals should analyse the societal implications of AI and its impacts on democracy. Therefore, the values guiding AI and responsible design practices that encode these values into AI systems should also be critically assessed.

- In addition, AI tools should be unbiased (gender, racial, etc.) and designed in such a way that the transparency and explainability of the corresponding decision processes are ensured, which would, amongst other, reinforce the admissibility of any resulting evidence in court.

SU-AI02-2020: Scope (6 of 6)

- Proposals' consortia should comprehend, besides industrial and research participants, relevant security practitioners, civil society organisations, experts on criminal procedure from a variety of European Member States and Associated Countries as well as LEAs. Proposals should ensure a multidisciplinary approach and have the appropriate balance of IT specialists as well as Social Sciences and Humanities experts

- proposals should foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices.

AI and Security Call in SC7

Type of Action: IA **SU-AI02-2020**

Budget: 17 MEUR

Expected EU contribution/project: 17 MEUR

Duration: maximum 60 months

Expected final TRL: 7-8

At least 5 LEAs from at least 5 EU of Associated countries

GA Article 31.5 on access rights for EU and Member States

Complementary grants GA options for SU-AI0x, x=1,2 and 3

GA 30.3 option to object transfer to third countries

Opening: 12/03/2020

Deadline: 27/08/2020

SU-AI02-2020

3. Is this new or has it been called before?

This topic is rather new.

It is linked to other topics in the current WP:

Robotics, Big Data, IoT topics and Cybersecurity Call in the LEIT programme

Digital Security Call in SC7

SU-AI02-2020

4. Current project portfolio

Proposals should take into account the existing EU and national projects in this field, as well as build on existing research and articulate a legal, ethical and practical framework to take the best out of the AI based technologies, systems and solutions in the security dimension.

Whenever appropriate, the work should complement, build on available resources and contribute to common efforts such as (but not limited to) ASGARD, SIRIUS, EPE, networks of practitioners, AI4EU, or activities carried out in the LEIT programme, namely in Robotics, Big Data, and IoT.

SU-AI03-2020:

2020: HUMAN FACTORS, AND ETHICAL, SOCIETAL, LEGAL AND ORGANISATIONAL ASPECTS OF USING ARTIFICIAL INTELLIGENCE IN SUPPORT OF LAW ENFORCEMENT

SU-AI03-2020

1. What are you looking for? (1 of 2)
   - Improved and consolidated knowledge among EU Law Enforcement Agency (LEA) officers on the issues addressed in this topic;
   - Exchange of experiences among EU LEAs about human, social and organisational aspects of the use of AI in their work;
   - Raised awareness of civil society about benefits of AI technologies in the security domain and opportunities it brings.

SU-AI03-2020

1. What are you looking for? (2 of 2)

- European common approach for assessing risks/threats involved by using AI in the security domain, and identifying and deploying relevant security measures that take into account legal and ethical rules of operation, fundamental rights such as the rights to privacy, to protection of personal data and free movement of persons;

- Advances towards the implementation of the AI tools and technologies in support of Law Enforcement, in the areas of cybersecurity and fight against crime, including cybercrime, and terrorism, by strengthening the civil society perception of the EU as an area of freedom, justice and security.

SU-AI03-2020: Specific Challenge (1 of 2)

- There is 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, but a broader engagement of civil society on the values to be embedded in AI and the directions for future development is crucial.
- This fact becomes extremely important in the security domain.
- There is a need to find ways to build a human-centred and socially driven AI, by, amongst other, fostering the engagement of citizens and improving their perception of security

SU-AI03-2020: Specific Challenge (2 of 2)

- Possible side effects of AI technological solutions in the domain of security need to be considered carefully, both from the point of view of citizens and from the point of view of Law Enforcement: e.g., their concerns regarding a strong dependence on machines, risks involved, how AI will affect their jobs and their organisation, or how AI will affect their decisions.

- Many open aspects exist that can be a source both of concern and of opportunity and should be addressed in a comprehensive and thorough manner.

- Finally, the legal dimension should be tackled as well – e.g., how the use of data to train algorithms is dealt with, what is allowed and under which circumstances, what is forbidden and when.

SU-AI03-2020: Scope (1 of 2)

- Provide 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 in the fight against crime, including cybercrime, and terrorism.

- suggest approaches that are needed to overcome these concerns and that stimulate the acceptance of AI tools by civil society and by Law Enforcement.

- 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.

SU-AI03-2020: Scope (2 of 2)

- The societal dimension should be at the core of the proposed activities.
- Proposals should be submitted by consortia involving relevant security practitioners, civil society organisations as well as Social Sciences and Humanities experts.
- should foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices.

AI and Security Call in SC7

SU-AI03-2020

Type of Action: CSA
Budget: 1.5 MEUR
Expected EU contribution/project: 1.5 MEUR
Duration: maximum 24 months
At least 3 LEAs from at least 3 EU of Associated countries

Complementary grants GA options for SU-AI0x, x=1,2 and 3
GA 30.3 option to object transfer to third countries

Opening: 12/03/2020
Deadline: 27/08/2020

SU-AI03-2020

3. Is this new or has it been called before?

This topic is rather new.

It is linked to other topics in the current WP:

Robotics, Big Data, IoT topics and Cybersecurity Call in the LEIT programme

Digital Security Call in SC7

For all cybersecurity calls/topics in WP2018-20

7. Are there any additional / background documents? (1 of 3)

- **Digital Single Market Strategy - Communication "A Digital Single Market Strategy for Europe" of 6.5.2015 - COM(2015) 192 final**
- European Agenda on Security - Communication "The European Agenda on Security" of 28.4.2015 – COM (2015) 185 final
- **Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" - JOIN(2017) 450 final, Brussels, 13.9.2017**
- **NIS Directive - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)**
- Data protection Directive for Police and Criminal Justice Authorities - Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

For all cybersecurity calls/topics in WP2018-20

7. Are there any additional / background documents? (2 of 3)

- eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- **GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**
- e-Privacy regulation - Proposal for a Regulation of the European Parliament and of the Council - COM(2017) 10 final of 10.1.2017
- Communication on "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" - COM(2016) 410 final, Brussels, 5.7.2016
- Cybersecurity Act - Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') - COM/2017/0477 final
- Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres to support the development of the technological and industrial capabilities necessary to autonomously secure its digital economy and increase Europe's competitiveness with regard to cybersecurity and privacy - COM(2018) 630

For the call AI and Security in SC7

7. Are there any additional / background documents? (3 of 3)

- **Artificial Intelligence – A European Perspective**, EUR 29425 EN, 2018.
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS **Artificial Intelligence for Europe, COM(2018) 237**.
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS **Coordinated Plan on Artificial Intelligence, COM(2018) 795 final.**
- **Guidelines of the European Group on Ethics in Science and New Technologies** (regulatory framework expected to be ready in March 2019)

Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Artificial Intelligence and Cybersecurity pillars in Digital Europe Programme.

Proposal for a European Cybersecurity Competence Network and Centre (COM 2018) 630 final.

Upcoming events / information days

9. Please list upcoming information days and other events of relevance to this area

ICT Proposers' Day 2019 at Helsinki scheduled 19-20 September 2019.

Security Research Event at Helsinki scheduled 6-7 November 2019 (organized by DG HOME and DG CONNECT).

with a specific panel on AI and Security

WP2018-2020 SC7 Call Digital Security (DS)

Workshop with the ICT National Contact Points
18 July 2019

CNECT.H1 Cybersecurity Technology & Capacity Building

SC7 – Digital Security Call - Overview

Topics 2020:

SU-DS02-2020: Intelligent security and privacy management

SU-DS03-2019-2020: Digital security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises (IA, Budget: 18 MEUR)

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

Opening: 12/03/2020; Deadline: 27/08/2020

SU-DS02-2020
Intelligent security and privacy management

Subtopics:

(a) Dynamic governance, risk management and compliance (IA; TRL 7; indicative EU grant : 2-5 MEUR)

(b) Cyber-threat information sharing and analytics (IA; TRL 7; indicative EU grant: 2-5 MEUR)

(c) Advanced security and privacy solutions for end users or software developers (RIA; TRL 6; indicative EU grant: 2-5 MEUR)

(d) Distributed trust management and digital identity solutions (RIA; TRL 5-6; indicative EU grant: 3-6 MEUR)

Budget: IA: 18.00 MEUR; RIA: 20.00 MEUR
Opening: 12/03/2020; Deadline: 27/08/2020

SU-DS02-2020

1. What are you looking for? (1/4)
   - Actions addressing security threats, minimizing security risks, by integrating in ICT systems state-of-the-art approaches for security & privacy management in a holistic & dynamic way.
   - Tools to automatically monitor & mitigate security risks.
   - Actions foreseeing collaboration & sharing information, with similar ongoing H2020 projects, EU pilots on a cybersecurity competence network, with different actors in the area of security and privacy management.
   - Actions that consider the relevant human factor and social aspects when developing innovative solutions.

SU-DS02-2020

1. What are you looking for? (2/4)
   - Advanced security & privacy management approaches which include designing, developing and testing:

     (i) security/privacy management systems based on AI;

     (ii) AI-based static, dynamic and behaviour-based attack detection, information-hiding, deceptive and self-healing techniques;

     (iii) immersive, highly realistic, pattern-driven modelling & simulation tools;

     (iv) real-time, dynamic, accountable and secure trust, identity and access management;

SU-DS02-2020

1. What are you looking for? (3/4) - **Impact**
   - Reduced number and impact of cybersecurity incidents;
   - Efficient, low-cost implementation of NIS Directive, GDPR;
   - Effective, timely co-operation & information sharing between and within organisations, as well as self-recovery;
   - Availability of comprehensive, resource-efficient, flexible security analytics and threat intelligence;
   - Availability of advanced tools and services to CERTs/CSIRTs;
   - EU industry better prepared for threats to IoT, ICS, AI and other systems;
   - Self–recovering, interoperable, scalable, dynamic privacy-respecting identity management schemes.

SU-DS02-2020

1. What are you looking for? (4/4) - **Impact**
   - Availability of better standardisation and automated assessment frameworks for secure networks and systems;
   - Availability, widespread adoption of distributed, enhanced trust management schemes (incl. people, smart objects);
   - Availability of user-friendly, trustworthy on-line products, services and business;
   - Better preparedness against attacks on AI-based products and systems;
   - Stronger, more innovative and competitive EU cybersecurity industry, reducing dependence on technology imports;
   - More competitive offer of secure products & services by European providers in DSM.

SU-DS02-2020: Specific Challenge

- Security threats – multi-tier, interconnected, computing architectures, with multi-faced, cascading effects;
- Increasing prevalence and sophistication of IoT, AI, broadening attack surface and risk of propagation.
- Need for tools to automatically monitor and mitigate security risks, including those related to data and algorithms.
- Storage, processing of data in different interconnected places may increase dependency on trusted third parties to coordinate transactions.
- Advanced security and privacy management approaches include designing, developing and testing:
  - security/privacy management systems based on AI;
  - AI-based static, dynamic and behaviour-based attack detection, information-hiding, deceptive and self-healing techniques;
  - immersive and highly realistic, pattern-driven modelling and simulation tools;
  - real-time, dynamic, accountable and secure trust, identity and access management.

SU-DS02-2020: Scope (b) Cyber-threat information sharing and analytics

- Develop and test threat detection frameworks, which should include: (i) collaborative, open, and dynamic repositories of information on threats and vulnerabilities; (ii) build on and update existing ontologies, taxonomies and models; (iii) dynamic tools for automated detection with advanced analytic capabilities, and where possible response and recovery; (iv) accountability and audit techniques; and (v) synchronised real time self- encryption/decryption schemes with recovery capabilities.
- Propose technologies enabling collaboration in cyber threat intelligence and alerting, taking into consideration technical, but also human aspects such as behavioural patterns, gender differences, privacy, ethics, sovereignty, psychology, linguistic and cultural boundaries.
- Tools and services developed should support the operations of CERTs/CSIRTs and their networks.
- Develop incident response tools and test processes for coordinated response to large-scale cross-border cybersecurity incidents and crises.

SU-DS02-2020: Scope (c) Advanced security and privacy solutions for end users or software developers

- Develop automated tools for checking the security & privacy of data, systems, online services and applications, in view to support end users or software developers (poss. Incl. developers of AI solutions) in their efforts to select, use and create trustworthy digital services.
- Address real application cases and at least one of the following services:
  - automatic code generation,
  - code and data auditing,
  - trustworthy data boxes,
  - forensics,
  - certification and assurance,
  - cyber insurance,
  - cyber and AI ethics,
  - penetration testing.

SU-DS02-2020: Scope (d) Distributed trust management and digital identity solutions

- With particular consideration to IoT contexts, propose and test/pilot innovative approaches addressing both of the following points:

  (i) distributed, dynamic, automated trust management & recovery solutions;

  (ii) developing novel approaches to managing the identity of persons and/or objects, including self-encryption/decryption schemes with recovery ability.
- Address real application cases.

SU-DS02-2020

2. What do you NOT want?

- Proposals which do not address all requirements for each subtopic;
- Poorly prepared proposal, without enough innovative elements;
- Replications of already funded similar projects;
- Proposals missing key elements;

SU-DS02-2020 – topic evolution

3. Is this new or has it been called before?

The topic is new, addressing new, actual challenges in the specific area.

But still there are links with:

- topics in previous WPs;
- other topics in the current WP.

SU-DS03-2019-2020

Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises

Subtopics:

(a): Protecting citizens' security, privacy and personal data (IA; TRL 7; indicative EU grant: 4-5 MEUR)

(b): Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection (IA; TRL 7; indicative EU grant: 3-4 MEUR)

Budget 2020: 10.80 MEUR
Opening: 12/03/2020;

Deadline: 27/08/2020;

SU-DS03-2019-2020

1. What are you looking for? (1/2)
   - Actions providing affordable solutions for security & privacy in favour of the more vulnerable members of the digital society: citizens and SMEs&MEs.
   - Actions foreseeing collaboration & sharing information with relevant H2020 projects, EU pilots on a cybersecurity competence network, with different actors, and envisaging resources for clustering.
   - Actions that consider the relevant human factor and social aspects when developing innovative solutions.
   - Proposals addressing subtopic (a) as well as proposals addressing subtopic (b).

SU-DS02-2020

1. What are you looking for? (2/2) – **Impact**
   - Citizens and SMEs&MEs better protected and more active players in the Digital Single Market, including in implementation of the NIS directive and the application of the General Data Protection Regulation.
   - Security, privacy and personal data protection strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs&MEs.
   - Reduced economic damage caused by harmful cyber-attacks, privacy incidents and data protection breaches.
   - Paving the way for a trustworthy EU digital environment benefitting all economic and social actors.

SU-DS03-2019-2020: Specific Challenge

- Significantly increased scale, value, sensitivity of personal data in cyberspace; citizens uncertain about who monitors, accesses and modifies their personal data.
- Personal data breach facilitating abuse by third parties, including cyber-threats such as coercion, extortion and corruption.
- Citizens should assess the risk involved in their digital activities and configure their own security, privacy and personal data protection settings and controls across these services; be fully aware of their informed consent and capable in providing permission/consent to allow accessing their data/devices/terminals.
- Need for increased capacity of citizens to modulate the level and accuracy of the monitoring tools used by services.
- SMEs&MEs lack sufficient awareness, being an easier target, as they can allocate limited technical and human resources to counter cyber risks.
- Security professionals working in SMEs&MEs should be in a constant learning process.

SU-DS03-2019-2020: Scope (a) Protecting citizens' security, privacy and personal data

- Provide innovative solutions, including innovative approaches, techniques and user-friendly tools;
- Develop new applications & technologies, enabling citizens to better monitor and audit their security, privacy, personal data protection, to become more engaged and active in the fight against cyber risks;
- Engage end-users by involving them in design and implementation, ensuring usability and acceptability;
- Assurance, transparency - easily accessed, identified, monitored by citizens, independently of their physical condition or ICT skills;
- Build bridges/synergies with data protection authorities and CERTs/CSIRTs.

SU-DS03-2019-2020: Scope (b) SMEs&MEs: defenders of security, privacy and personal data protection (1/2)

- Deliver innovative solutions to increase the knowledge sharing in digital security across SMEs&MEs and with larger providers.
- Support SMEs&MEs by democratizing access to tools and solutions of varied sophistication level, to allow them benefitting from innovative targeted solutions addressing their specific needs and available resources (currently reserved to larger organisations, due to their cost and availability of internal expertise).
- Propose tools and processes to facilitate the participation of user SMEs&MEs in cyber ranges for cybersecurity.

SU-DS03-2019-2020: Scope (b) SMEs&MEs: defenders of security, privacy and personal data protection (2/2)

- Develop targeted, user-friendly, cost-effective solutions enabling SMEs&MEs to:

  (1) dynamically monitor, forecast and assess their security, privacy and personal data protection risks;

  (2) become more aware of vulnerabilities, attacks and risks influencing their business;

  (3) manage and forecast their security, privacy, personal data protection risks in an easy and affordable way;

  (4) build on-line collaboration between SMEs&MEs associations and CERTs/CSIRTs, enabling individual SMEs&MEs to report any incident.

SU-DS03-2019-2020

2. What do you NOT want?

- Proposals which do not strive to address all bullet points described in each subtopic;
- Poorly prepared proposal, without enough innovative elements;
- Proposals missing key elements;

SU-DS03-2019-2020 – topic evolution

3. Is this new or has it been called before?

Topic opened in 2019 (deadline: 22/08/2019).

Has links with:

- topics in previous WPs;
- other topics in the current WP.

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

Type of Action: IA (TRL 7)
Budget 2020: 20.00 MEUR
Indicative EU grant: 6-8 MEUR
Opening: 12/03/2020;
Deadline: 27/08/2020;

SU-DS04-2018-2020

1. What are you looking for? (1/3)

- Solutions to make the sector more cyber secure, more resilient to growing, more sophisticated cyber and privacy attacks;
- Support for the transformation of the energy system, for the transition to a decentralized system, with improved performance and cost savings;
- Designing a cyber-secure system architecture;
- Making legacy assets (SCADA, ICS) resilient;

SU-DS04-2018-2020

1. What are you looking for? (2/3) - **Impact**

- Built/increased resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector.
- Ensured continuity of the critical business energy operations and resilience against cyberattacks, including large scale, demonstrating effective solutions to:

  a) the real-time constraints of an electric system,

  b) barriers to the cascading effect,

  c) the adaptation of legacy equipment or their coexistence with state of the art technology.

SU-DS04-2018-2020

1. What are you looking for? (3/3) - **Impact**

- Energy sector better enabled to easily implement NIS directive.
- Availability of a set of standards and rules for certification of cybersecurity components, systems and processes in the energy sector.
- Cyber protection policy design and uptake at all levels from management to operational personnel, in the energy sector.
- Manufacturers providing more accountability and transparency, enabling third parties monitoring and auditing the privacy, data protection and security of their energy devices and systems.

SU-DS04-2018-2020: Specific Challenge

- Digital technologies playing a more important role in the energy system, which is facing higher risks and vulnerabilities, exposed to an increasing range of cyber threats;
- With increased digitalisation, EPES faces an increasing range of threats requiring an attentive evaluation of the cyber security risk, allowing taking proper countermeasures;
- Older technologies in legacy systems designed when cybersecurity was not part of the technical specifications for the system design;
- Control system in EPES under attack might not be easily disconnected from the network (safety issues, brownouts or even blackouts);
- Micro grid operations and/or islanding could be further exploited against cyber-attacks and cascading effects in EPES;
- Need for new security approaches in detecting and preventing threats, building protection against cyber and privacy attacks;

SU-DS04-2018-2020: Scope (1/2)

- Develop solutions making the energy sector more resilient to growing and more sophisticated cyber & privacy attacks, more cyber secure;
- Demonstrate resilience of EPES through design and implementation of adequate measures able to make assets and systems less vulnerable, reducing exposition to cyber-attacks;
- Develop scenarios for possible attacks, with appropriate counteracting measures, designed, described, tested on a demonstrator, to verify effectiveness;
- Apply measures to new assets or to existing equipment where data flows were not designed to be cyber protected;
- Develop security information and event management system collecting security-related documentation;

SU-DS04-2018-2020: Scope (2/2)

- Implement activities to make the electric system cyber secure:
  - assess vulnerabilities and threats in a collaborative manner;
  - design adequate security measures to ensure a cyber-secure system;
  - implement both organisational and technical measures in representative demonstrator to test the cyber resilience of the system with different types of attacks/severity;
  - demonstrate the effectiveness of the measures with a cost-benefit analysis;
- Define cybersecurity design principles with a set of common requirements to inherently secure EPES;
- Formulate recommendations for standardisation & certification in cybersecurity at component, system and process level;
- Propose policy recommendations on EU exchange of information;

SU-DS04-2018-2020: Specific conditions

- Dimension of a pilot/demonstrator: at large scale level (e.g. neighbourhood, city, regional), involving generators, one primary substation, secondary substations and end users;
- Include types of entities such as: TSO, DSO, electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers;
- Proposals may refer to Industry 4.0 and other proposals and/or projects dealing with cybersecurity in energy;
- Foresee activities and envisage resources for clustering with other projects funded under this topic and other H2020 relevant projects in the field, in particular under the BRIDGE initiative (http://www.h2020-bridge.eu/);

SU-DS04-2018-2020: Energy Policy context

- **Clean Energy for all Europeans Package**
  - Risk Preparedness Regulation (EU) 2019/941: mandates Member States to develop national risk preparedness plans and coordinate their preparation at regional level, including measures to cope with cyber-attacks
  - Recast of the Electricity Regulation (EU) 2019/943: gives a mandate to the Commission to develop a network code on cyber security for the electricity sector in order to increase its resilience and protect the grid
- **Regulation of Security of Gas supply (EU) 2017/1938: includes provisions to consider cybersecurity as part of Member States' national risk assessments**
- **Sector-specific guidance for the energy sector - Recommendation C(2019)240 final and Staff Working Document SWD(2019)1240 final**

SU-DS04-2018-2020

2. What do you NOT want?

- Proposals missing key elements either in energy or in cyber area;
- Proposals not adequately addressing topic's requirements;
- Poorly prepared proposal, without enough innovative elements;
- Replications of already funded similar projects;

SU-DS04-2018-2020 – topic evolution

3. Is this new or has it been called before?

The topic was open in 2018 and projects were funded (to be found on Participant Portal);

The topic has also links to other topics in:

- previous WPs (SC7 – CIP/INFRA, DS calls);
- current WP (SC7 – INFRA, DS calls);

General information for all 3 topics

4. Current portfolio
5. Leading players
6. Key group of actors (eg. cPPP or other)
7. Additional / background documents
8. Information about future trends, emerging initiatives, roadmaps, key players in this area
9. Upcoming information days and other events of relevance to this area

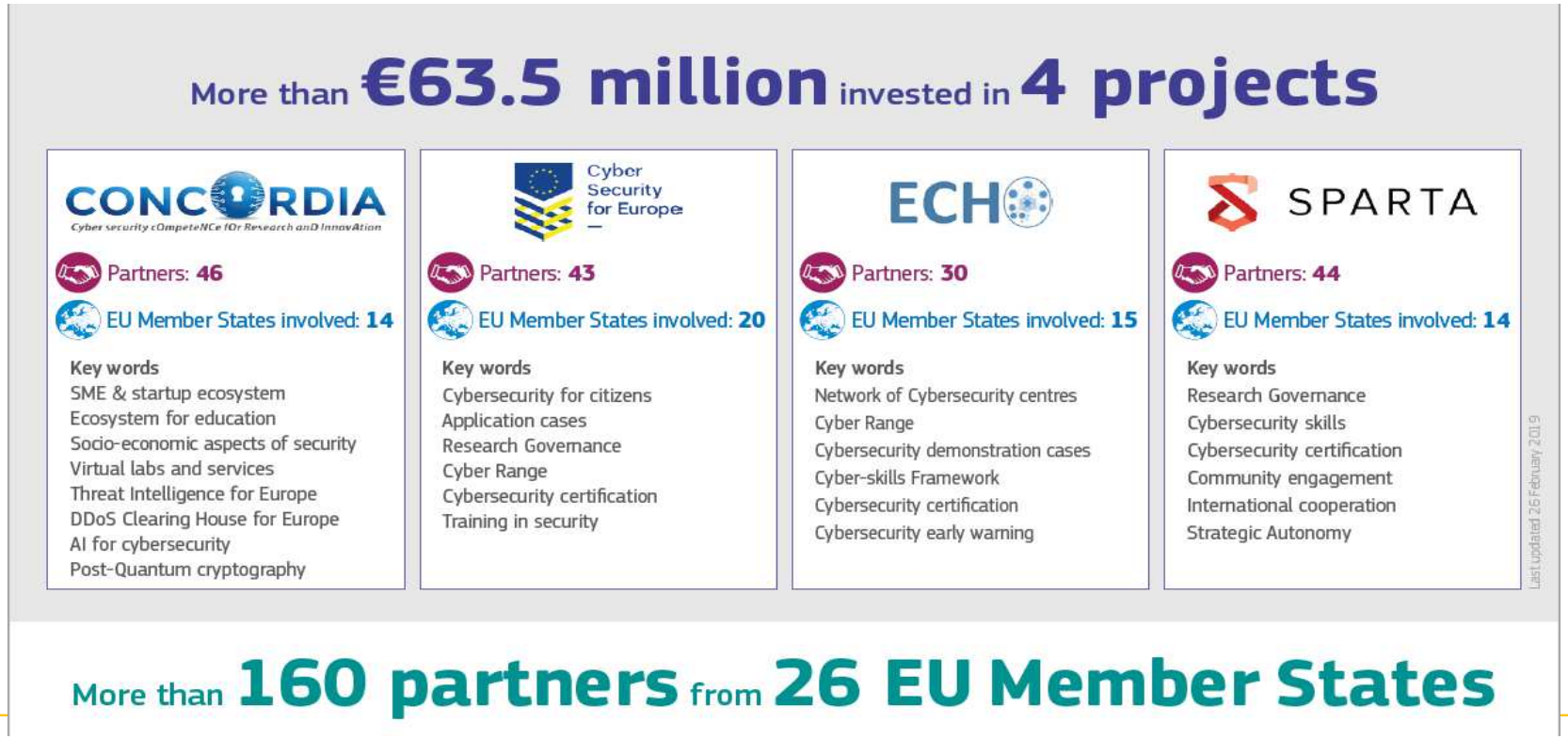
DS02, DS03, DS04 – topic evolution

4. Current project portfolio

- Similar ongoing projects in SC7 – DS and CIP/INFRA calls;
- 4 EU pilots financed under SU-ICT-03-2018
- Cybersecurity projects in LEIT-ICT

DS02, DS03, DS04 – topic evolution

4. Current project portfolio – EU pilots



DS topics (DS02, DS03, DS04) – Key actors

5. Who are the leading players?

DG CNECT

DG ENER (SU-DS04-2018-2020)

6. Is there a key group of actors (eg. cPPP or other) driving this?

cPPP on Cybersecurity - ECSO

DS topics (DS02, DS03, DS04)

7. Are there any additional / background documents?

- Background documents mentioned in WP
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act).
- Horizon Europe – Cluster 3 on security.
- Cybersecurity pillar in Digital Europe Programme.
- The 4 EU Pilots aforementioned.

Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

- Proposal for a European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres (COM 2018) 630 final
- Cybersecurity pillar in Digital Europe Programme
- The 4 EU Pilots aforementioned

Upcoming events / information days

9. Please list upcoming information days and other events of relevance to this area

- Community of Users – Brussels, 16-18 September 2019
- Digital Excellence Forum @ ICT Proposers' Day 2019 – Helsinki, 19-20 September 2019
- R&I Days – Brussels, 24-26 September 2019
- Security Research Event – Helsinki, 6-7 November 2019 (organized by DG HOME and DG CONNECT)