Horizon 2020 Sécurité

Les appels à propositions de 2020

Sécurité

PCN - Horizon2020

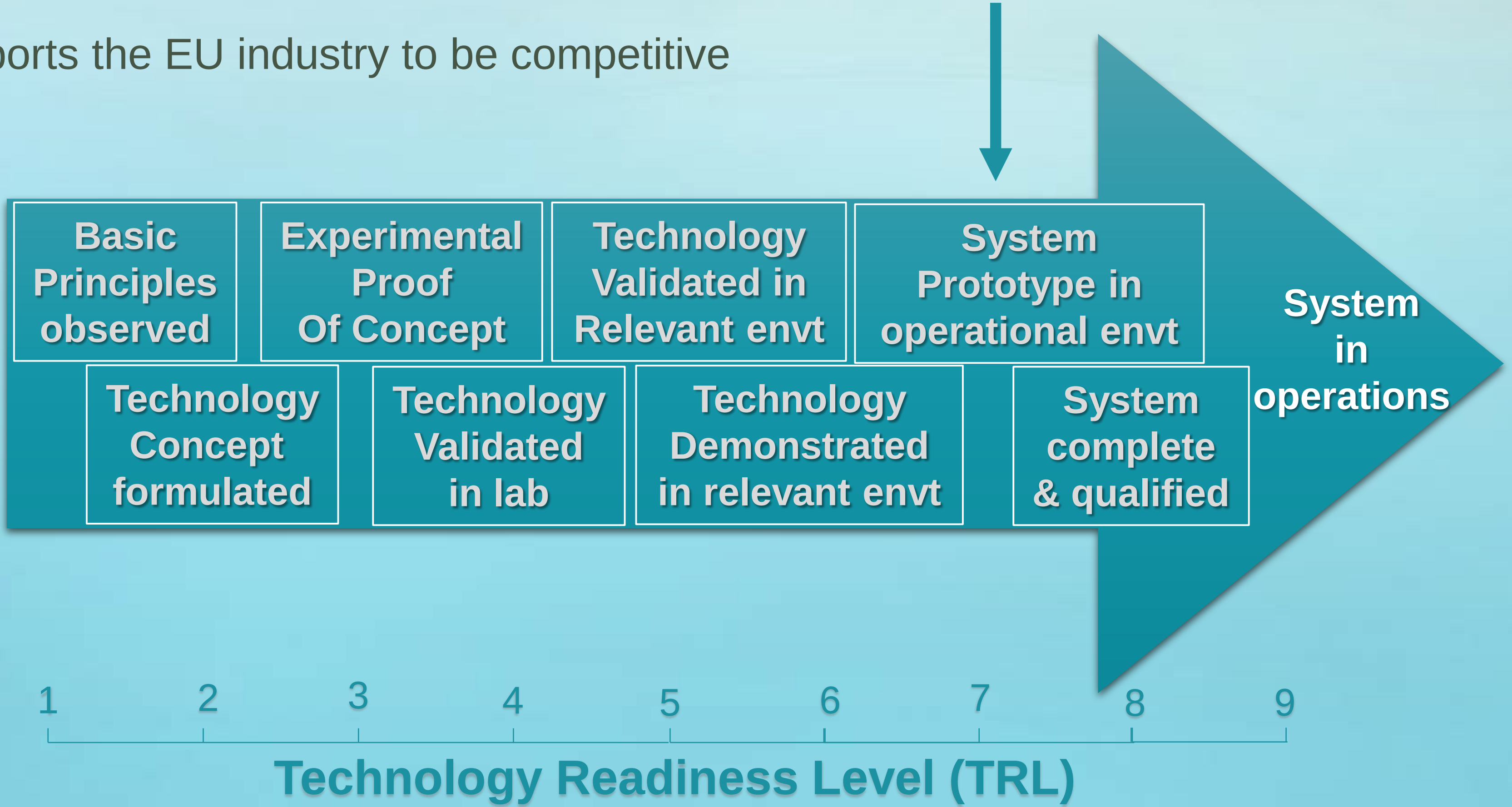
Armand Nachef – CEA
armand.nachef@cea.fr – 06 73 73 71 98

Security Research

Horizon 2020 - Secure Societies

Supports EU internal and external security policies

1. Follows a mission-oriented approach
2. Strengthens the involvement of the end-users / practitioners
3. Takes more into account the Societal Dimension
4. Supports the EU industry to be competitive



Basic Principles observed

Technology Concept formulated

Experimental Proof Of Concept

Technology Validated in lab

Technology Validated in Relevant envt

Technology Demonstrated in relevant envt

System Prototype in operational envt

System complete & qualified

System in operations

1 2 3 4 5 6 7 8 9

Technology Readiness Level (TRL)

2020 SC7 Call for proposals

SU-INFRA

Physical and cyber threats to critical infrastructure
INFRA01 **(IA)**

including for novel installation designs

SU-AI

R&D roadmap of Artificial intelligence for LEAs
AI01-2020 **(CSA)**

AI technologies, tools and solutions in support of LEAs
AI02-2020 **(IA)**

Human factors, and ethical, societal, legal and organisational aspects of using AI in support LEAs
AI03-2020 **(CSA)**

SU-FCT

FCT Human factors

- fight human beings trafficking and child sexual exploitation
- counter violent radicalisation
- **NO** open subtopic

FCT01 **(RIA)**

FCT Technologies

- Money flows tracking
- Identify terrorist content online
- Open subtopic

FCT02 **(RIA)**

Information and data stream mgt to secure *soft targets*
FCT03 **(IA)**

Chemicals: intelligence, detection, forensics
explosives, neurotoxins, new drugs, etc.
FCT04 **(IA)**

SU-DRS

DRS Human factors
DRS01**(RIA)**

Technologies for first responders:

- Methods and guidelines for pre-hospital life support and triage
- Open subtopic

DRS02 **(RIA)**

Pre-normative R&Demo for DRS

- First aids vehicles deployment, maintenance, and remote centralized coordination means

DRS03 **(IA)**

CBRN cluster
DRS04 **(RIA)**

SU-BES

BES Human factors

- indicators of threats at the EU external borders
- **NO** open subtopic

BES01 **(RIA)**

Technologies for BES

- Disruptive technologies for non-intrusive identification of hidden goods
- Open subtopic

BES02 **(RIA)**

Demo of applied solutions

- Improved systems for the vessel tracking
- Open subtopic

BES03 **(IA)**

SU-GM

Networks of practitioners:

- intelligence
- fighting cybercrime

GM01 **(CSA)**

PCP of advanced Systems
GM02 **(PCP)**

SU-DS

Intelligent security & privacy mgt

- Dynamic governance, risk mgt & compliance
- Cyber-threat information sharing and analytics
- solutions for users or soft developers
- Distributed trust mgt and digital identity solutions

DS02 **(IA)**

Cyber security & privacy for Micro-SMEs and citizens
DS03 **(IA)**

Cybersecurity in the Electrical Power and Energy System (EPES)
DS04 **(IA)**

SU-ICT

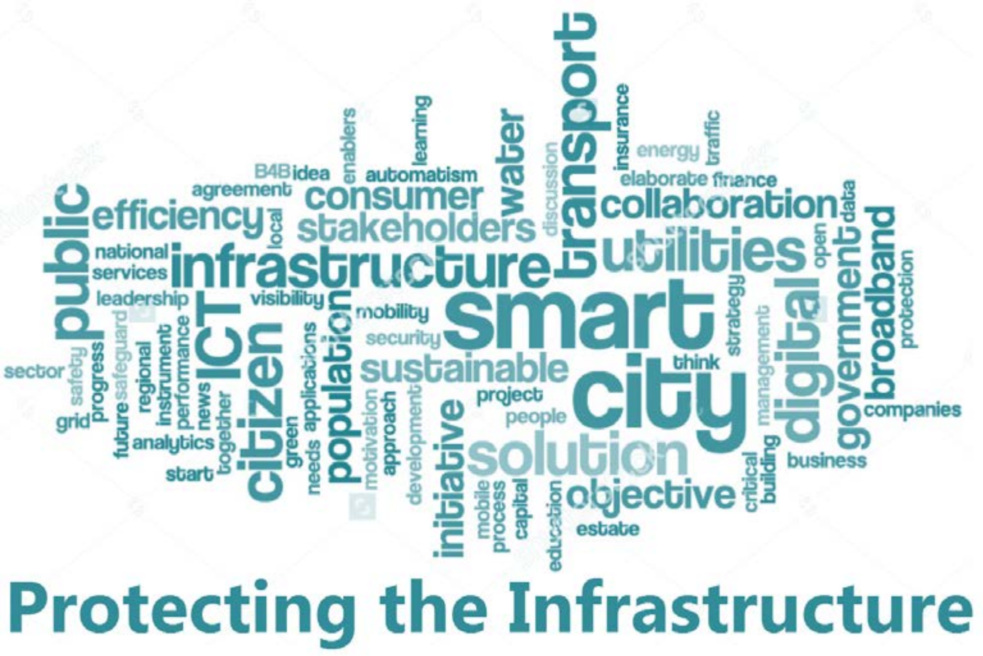
Building blocks for resilience SU- ICT-02-2020 (RIA)

Deadline: novembre 2019

http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf

SU-INFRA

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



SU-INFRA01-2018-2019-2020 * (1/3)

Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

• **Type of Action**	Innovation Action
• **Output TRL**	7
• **Project duration**	maximum **24 months**
• **Budget per project**	between 7 and 8 M€
• **Total budget**	20,7 M€ in 2020
• **Eligibility conditions**	At least 2 operators as beneficiaries (not necessary coordinators) *Participation of industry to provide security solutions* *Consortia should involve, infrastructure owners and operators,* *first responders, industry, technologists, social scientists, and SMEs*
• **Deadline**	27 Aug 2020

- **Challenge**
  - ❑ Increased combined physical and cyber-attacks due to their interdependencies.
  - ❑ Need of a complete approach to secure existing or future connected and interdependent installations, plants and systems.
  - ❑ New security solutions need to be more cost-effective and automated.

SU-INFRA01-2018-2019-2020 - Scope (2/3)

Forecast, assess **physical and cyber risks**, prevent, detect, response, mitigate consequences, and achieve fast recovery **(including novel installation designs)**

Achieve the security and resilience of all functions performed by the installations, and of **neighbouring populations and the environment.**

Share information with the public in the vicinity of the installations, for ensuring service continuity, and for the protection of first responders.

Proposals should:

a) address all aspects of interdependent physical and cyber threats and incidents, and cascading risks
b) demonstrate the accuracy of the risk assessment approach using specific examples of real life
c) develop improved real-time, evidence-based security management
d) provide scenarios and recommendations for policy planning, and investment measures encompassing all aspects of prevention-detection-response-mitigation

In 2020, proposals should:

- Address the interrelations between different types of critical infrastructure
- Develop tools and methods to
  - minimise cascading effects
  - allow rapid recovery of service performance levels after incidents.

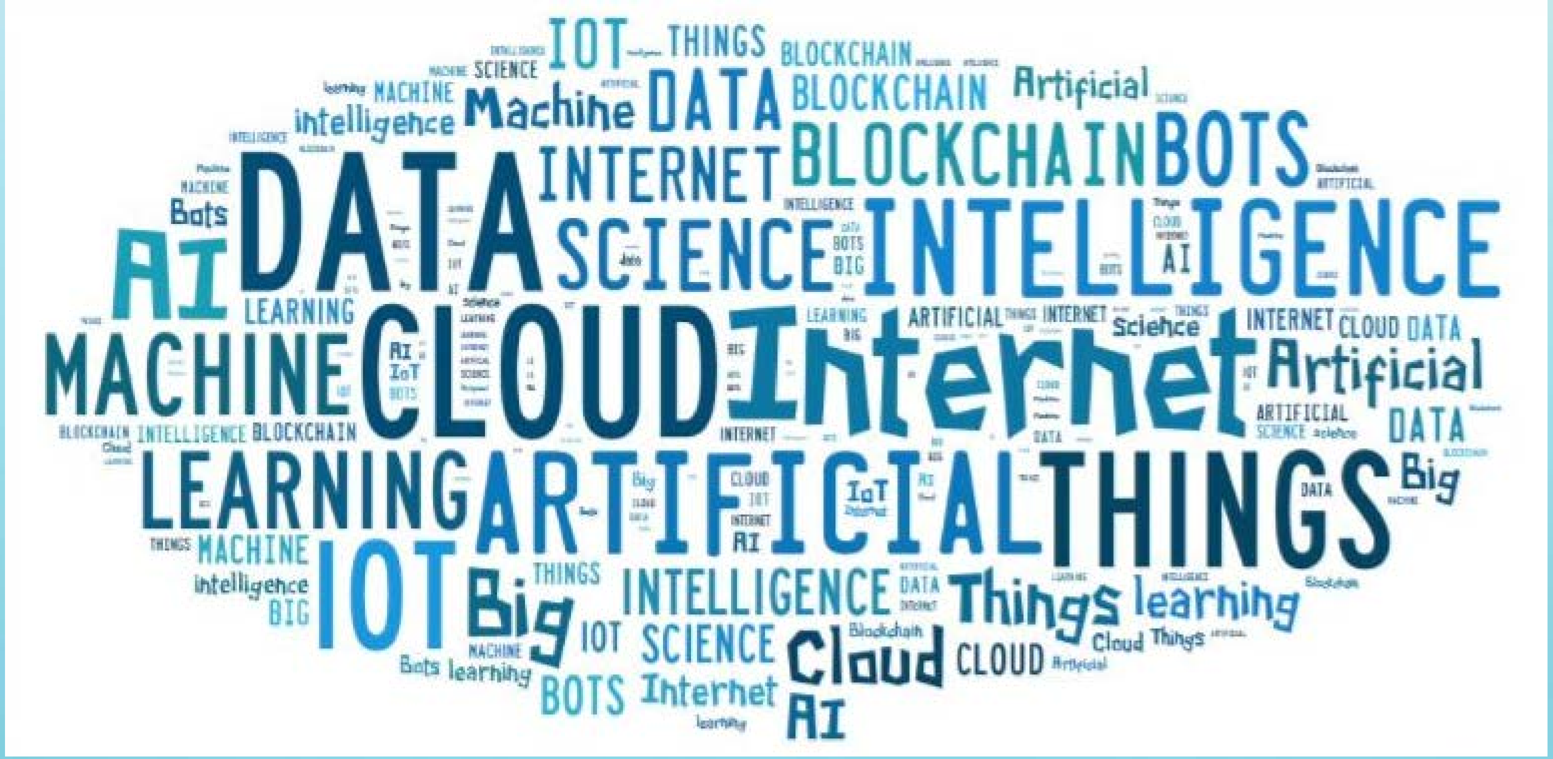
SU-INFRA01-2018-2019-2020 - Scope (3/3)

One of the following critical infrastructures

- Energy infrastructure
- Transport infrastructure
- Communication infrastructure
- Water systems
- Ground segments of space systems
- Health services
- E-Commerce and postal infrastructure
- Sensitive industrial sites and plants
- Financial services

SU-AI

Artificial Intelligence

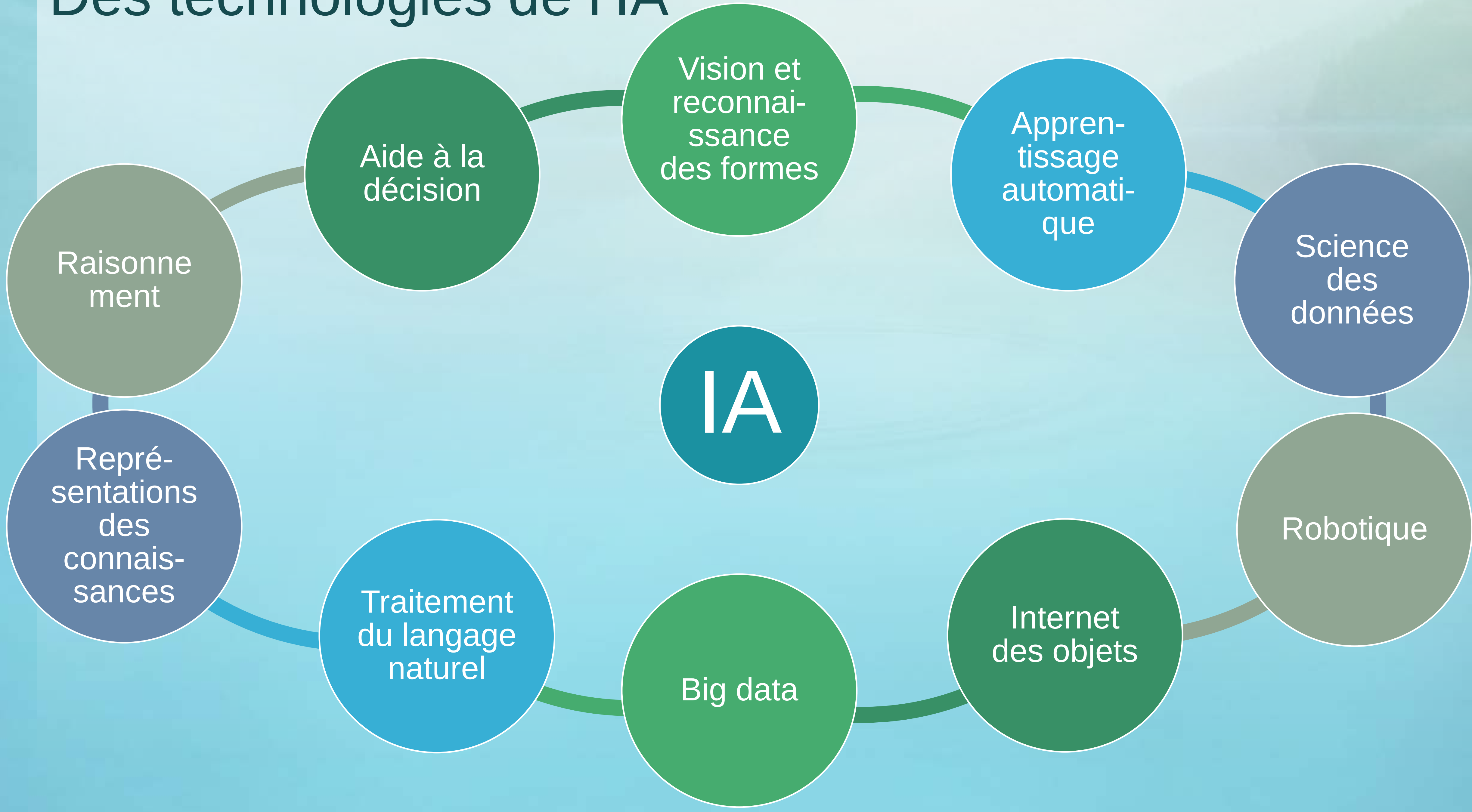


Appel **H2020-SU-AI-2020**

- L'intelligence artificielle (IA) fait référence à toute machine ou algorithme capable

1. d'observer son environnement,
2. d'apprendre,
3. et peut prendre des mesures intelligentes ou proposer des décisions (en se basant sur les connaissances et l'expérience acquises

Des technologies de l’IA



IA

Vision et reconnaissance des formes

Apprentissage automatique

Science des données

Robotique

Internet des objets

Big data

Traitement du langage naturel

Représentations des connaissances

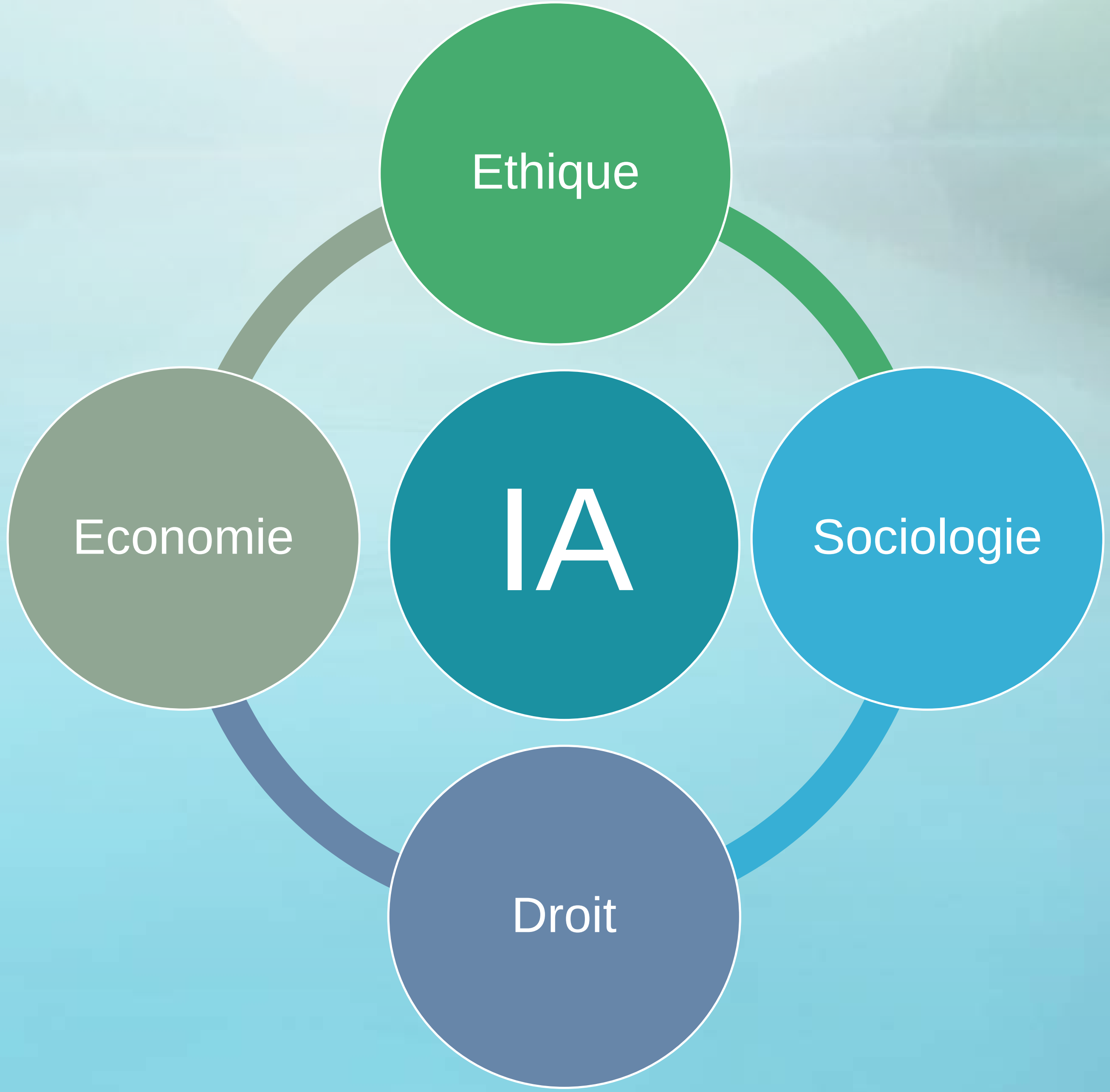
Raisonnement

Aide à la décision

IA et SHS

Approche plaçant les personnes au centre du développement de l’IA

« IA centré sur l’être humain »



SU-AI02-2020:

Technologies, outils et solutions d‘IA sécurisés et résilients pour
le maintien de l’ordre et la protection des citoyens,
les opérations de cybersécurité
et pour la prévention et la protection contre l‘IA antagoniste (1)

- Au moins 5 organisations de forces de l’ordre
- Durée du projet 5 ans Budget 17 M€ Action d’Innovation

- Tirer le meilleur parti des technologies basées sur l'IA pour le soutien des forces de l’ordre.
  - améliorer la cybersécurité des infrastructures de sécurité
  - prévenir, détecter et répondre à des incidents de cybersécurité , ciblant entre autres
    - les unités de lutte contre la cybercriminalité,
    - les équipes de réponse aux incidents de sécurité informatique (CSIRT) des forces de l’ordre,
    - Le centres de coopération policière et douanière,
    - Les équipes communes d'enquête
- Les systèmes d'IA sont de plus en plus utilisés par les cybercriminels
  - analyser leurs capacités et faiblesses pour lutter contre leurs usages malveillants

SU-AI02-2020:
Technologies, outils et solutions d‘IA (2)

- Créer une plate-forme d'outils d‘IA faciles à intégrer et interopérables,
  ainsi qu'un processus associé comportant de courts cycles de recherche et de test (voir projet ASGARD)
  pour identifier les lacunes spécifiques qui nécessiteraient une réflexion et un développement plus poussés.
- Créer une communauté autour de la plateforme IA pour les forces de l’ordre pour définir, développer et évaluer des outils avec des utilisateurs finaux, en utilisant une approche itérative
- La plate-forme devrait permettre un accès direct des forces de l’ordre à un ensemble initial d'outils

- Accorder une attention particulière aux
  - données : leur qualité, structure, étiquetage, intégrité, quantité, disponibilité, origine, stockage, accès et pertinence pour le problème à traiter
  - 3 principes clés : "interopérabilité", "sécurité par conception" & "éthique par conception"
  - différentes préoccupations législatives, technologiques, sécuritaires, éthiques et juridiques
  - à la sensibilité des données qui complique l'accès
  - à une coopération étroite des différents systèmes nationaux de sécurité et judiciaires
  - à la capacité de produire de preuves devant les tribunaux
  - à la formation

SU-AI02-2020:
Technloogies, outils et solutions d‘IA - Impact attendu

Court terme :

- Mise au point d'un ensemble de données européennes représentatives et suffisamment vastes, multilingues et multimodales, pour la communauté scientifique qui développe des outils d'IA en soutien des forces de l’ordre

Moyen terme :

- Amélioration de la capacité des forces de l’ordre à mener des enquêtes et des analyses à l'aide de l'IA
- Résilience accrue à l'IA antagoniste

A plus long terme :

- Modernisation du travail des forces de l’ordre en Europe et amélioration de leur coopération
- Création éventuelle à l'avenir d'un centre européen d’IA à l'échelle de l'Union européenne

SU-DRS

Disaster-Resilient Societies

SU-DRS01-2018-2019-2020

Human factors, and social, societal, and organisational aspects for disaster-resilient societies

Type of Action	Research & Innovation Action
Output TRL	not specified
Project duration	not specified
Budget per project	5 M€
Total budget	5 M€ in 2020
Eligibility conditions	At least 3 first responders from 3 different EU or associated countries
Deadline	27 Aug 2020

- **Challenge**
  - ❑ The resilience of societies heavily rely on how their citizens behave individually or collectively
  - ❑ The spread of new technologies and media are inducing dramatic changes in how individuals and communities behave
  - ❑ Building the resilience requires a better understanding and implementation of these new technologies to raise disaster risk awareness, to improve citizen understanding of risks, and to enhance governance

SU-DRS01-2018-2019-2020 - Scope

Human factors … for DRS

- Diversity in risk perception and in understanding responses to crises requires research addressesing the issues of geographical diversity
- Take into account cultural changes
- Consider social media and crowd-sourced data, and the involvement of the citizens in the process validation
- Analyse both the positive and negative roles of social media and crowd-sourced data in crisis situations. Assess such practices for different disaster scenarios (natural hazards, industrial disasters, terrorist threats).
- Look into how to implement the concept of ‘Building Back Better’ of the Sendai Framework, taking account of tangible and intangible cultural heritage, and traditional know-how.
- Learn from countries are constantly under natural threat where risk is perceived differently (e.g. Japan)

SU-DRS02-2018-2019-2020

Technologies for first responders

Type of Action	Research & Innovation Action
Output TRL	4 to 6
Project duration	not specified
Budget per project	~7 M€
Total budget	21 M€ in 2020
Eligibility conditions	At least 3 first responders from 3 different EU or AC (or at least 5 first responders for the open sub-topic)
Deadline	27 Aug 2020

- **Challenge**
  - □ Resilience is critical to allow authorities to take measures in response to severe disasters.
  - □ Innovation for disaster-resilient societies may draw from novel technologies.

SU-DRS02-2018-2019-2020 - Scope
Technologies for first responders

❑ Sub-topic 3: [2020] Methods and guidelines for pre-hospital life support and triage

- Development of innovative tools, methodologies and pre-hospital guidelines for first responders of medical services, fire services and police and hospital trauma teams in order to ensure faster and more effective evaluation and control of numerous seriously injured casualties in disaster and/or emergency situations.
- This should take account of lessons learned from military mass-casualty techniques such as damage-control surgery. The aim is to ensure more effective pre-hospital triage of victims with appropriate digital traceability of actions and data transfer from the event to the hospital(s), including across administrative and political boundaries..

❑ Sub-topic: [2020] Open - Technologies for use by first responders, including:

- communicating and smart wearables for first responders and canine units including light-weight energy sources;
- situational awareness and risk mitigation systems for first responders using UAV and robots, connected and swarms of drones; systems based on the internet of things;
- solutions based on augmented or virtual reality;
- systems communication solutions between first responders and victims;
- risk anticipation and early warning technologies;
- mitigation, physical response or counteracting technologies; etc.

SU-DRS03-2018-2019-2020
Pre-normative research and demonstration for disaster resilient societies

- **Type of Action** Innovation Action
- **Output TRL** 6 to 7
- **Project duration** not specified

- **Budget per project** 6M€
- **Total budget** 6 M€ in 2020

- **Eligibility conditions** At least 3 first responders from 3 different EU or associated countries
- **Deadline** 27 Aug 2020
- **Challenge**
  - A reason for the difficult interaction among practitioners, lies in the insufficient harmonisation and standardisation, which pre-normative research and demonstrations may address effectively.

SU-DRS03-2018-2019-2020 - Scope

Pre-normative research and demonstration for disaster resilient societies

Pave the way to improved standards, including voluntary Standard Operating Procedures (SOPs) and/or ISO or EN standards

❑ Sub-topic 3: [2020] First aids vehicles deployment, training, maintenance, logistic and remote centralized coordination means

- Improved standards and common communication data exchange mechanisms

  for an effective deployment of resources during the run-up

  to related to any kind of disaster either natural (including resulting from climate-related extremes) or man-made

  immediately after the event, for example in case of a mass evacuation from an urban area

SU-FCT

Fight Against Crime and Terrorism

Fight against Crime

Fight against Terrorism

SU-FCT03-2018-2019-2020

Information and data stream management to fight against (cyber)crime and terrorism

Type of Action	Innovation Action
Output TRL	5 to 7
Project duration	maximum **24 months**
Budget per project	8M€
Total budget	8 M€ in 2020
Eligibility conditions	At least 3 LEAs from 3 different EU or associated countries
Deadline	27 Aug 2020

- **Challenge**
  - ❑ A Large amounts of data and information from a variety of origins have become available to practitioners involved in fighting crime and terrorism.
  - ❑ Full advantage is not currently taken of the most advanced techniques for Big Data analysis, and artificial intelligence

SU-FCT03-2018-2019-2020 - Scope

Information and data stream management to FCT

❑ Sub-topic b: [2020] enhance citizens' security against terrorist attacks in places considered as soft targets, including crowded areas (transport stations, shopping malls, entertainment venues, etc.)

With a focus on private operators, as public spaces are often owned and operated by private entities

❑ Convert voluminous and heterogeneous data sets (images, videos, geospatial intelligence, communication data, traffic data, financial transactions related date, etc.) into intelligence

- Predictive analytics from open source intelligence gathering, social network and darknet data analysis
- Behavioural/anomaly detection systems (using a large variety of sensors) by the analysis and processing of enormous quantities of data to allow for the identification of suspicious events

SU-BES

Border and External Security

SU-BES03-EBCGA-2018-2019-2020

Demonstration of applied solutions to enhance border and external security

Type of Action	Innovation Action
Output TRL	6 to 8
Project duration	maximum **18 months**
Budget per project	5M€
Total budget	10 M€ in 2020
Exceptional funding rates	Cost of fuel is excluded from the costs eligible
Eligibility conditions	At least 3 border/coast guards from 3 different EU or AC (or at least 5 for the open sub-topic) Consortia must be coordinated by a practitioner under civilian authority
Deadline	27 Aug 2020

- **Challenge**
  - ❑ BES solutions at high TRL exist but they need to be demonstrated in the context of actual operations

SU-BES03-EBCGA-2018-2019-2020 - Scope

Demonstration of applied solutions to enhance BES

❑ Sub-topic 3: [2020]
Improved systems for the vessel tracking, behaviour analysis and automatic anomaly detection.

- The aim is to provide more precise, more robust and earlier anomaly detection.
- Current maritime reporting systems produce huge quantities of data which cannot be directly exploited by the human operators in the various maritime control centres.
- The solutions should be based on implementation agnostic, innovative algorithms for artificial intelligence and machine learning, applied to existing ship reporting systems and maritime databases and information sources.
- Should clearly demonstrate how they complement and do not overlap with actions undertaken in the Preparatory Action on Defence Research under topic PADR-US-01-2017: Technological demonstrator for enhanced situational awareness in a naval environment.

SU-DS

Digital Security
Cybersecurity and Digital Privacy

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

*Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks **

Type of Action	Innovation Action
Output TRL	7
Budget per project	6 to 8 M€
Total budget	20 M€ in 2020 (Half of the budget is originated from Societal Challenge 3)
Deadline	27 Aug 2020

- **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,
  - ❑ EPES will face an increasing range of threats requiring an attentive evaluation of the cyber security risk
  - ❑ Without appropriate cyber-defence measures, systems access could be violated and may cause power outages, damages and cascading effects to interconnected systems
  - ❑ To pursue the integration of the renewables within the existing EPES and to ensure that it benefits from the advantages brought by a modern digitalised electricity grid, there is a need for new security approaches.

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

*Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks **

Demonstrate how the actual EPES can be made resilient to new cyber and privacy attacks taking into account the developments of the grid towards a decentralised architecture and involving all stakeholders.

Different scenarios of attacks should be envisaged and the relative counteracting measures should be designed, described, tested (sandboxing, simulations) on a representative energy demonstrator to verify effectiveness

The proposals shall implement the following series of activities:

i. assess vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy provision supply chain)

ii. design a cyber-secure system architecture describing the advantages of the solution adopted compared to others

iii. implement both organisational and technical measures in representative demonstrator to test the cyber resilience of the system with different types of attacks/severity

iv. demonstrate the effectiveness of the measures with a cost-benefit analysis.

v. develop security information and event management system collecting logs and other security-related documentation for analysis that can also be used for information sharing across operators of essential infrastructures and CERT

vi. define cybersecurity design principles with a set of common requirements to inherently secure EPES

vii. formulate recommendations for standardisation and certification in cybersecurity at component, system and process level;

viii. propose policy recommendations on EU exchange of information.

- Pilot/demonstrator shall be at city level, involving generators, one primary substation, secondary substations and end users.
- Shall include the following types of entities: Transmission system operator (TSO), Distribution system operator (DSO), electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers.

SU-ICT & ICT

Cybersecurity in ICT

SU-ICT-02-2020
Building blocks for resilience in evolving ICT systems

- Scope:

  At least one of the following:

  - *Cybersecurity/privacy audit, certification and standardisation*
  - *Trusted supply chains of ICT systems*
  - *Designing and developing privacy-friendly and secure software and hardware*

Deadline: novembre 2019

Type	Output TRL	Budget/proj. (M€)	Total Budget total (2020)
RIA	5	4-5	47 M€