PREVISION Project

Key Project Information

Kostas Demestichas

Institute of Communication and Computer Systems (ICCS)

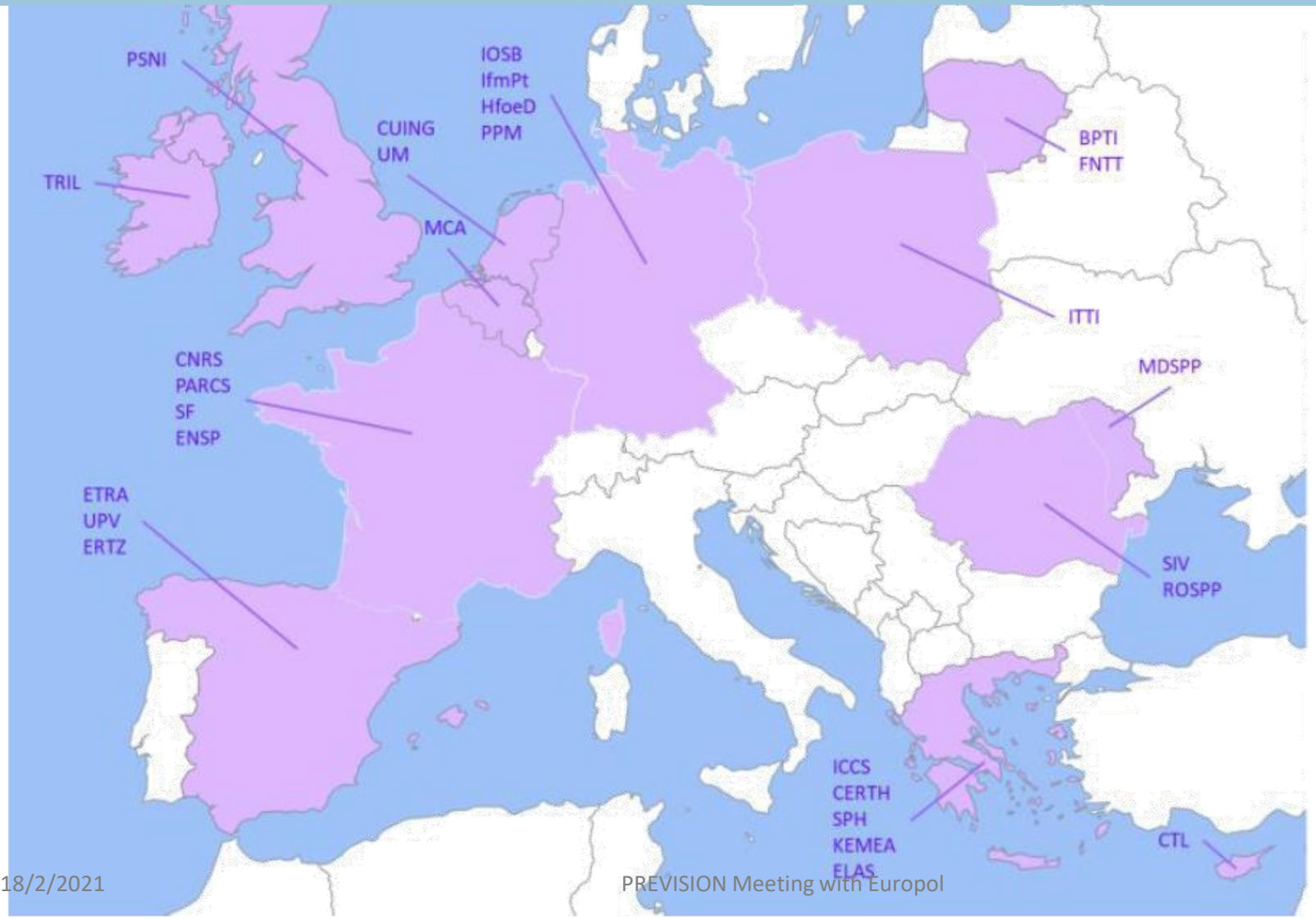
Agenda 17.02.21

1. Overview of the PREVISION Architecture
2. PREVISION Tools: Extreme-scale heterogeneous data streams processing
3. PREVISION Tools: Machine Learning and Automated Cognitive Capabilities
4. PREVISION Demo: Illicit Trafficking of Cultural Goods
5. Q&A – Future steps

Project Info

- **Call:** SU-FCT03-2018
  - Information and data stream management to fight against (cyber)crime and terrorism
- **Grant Agreement Number:** 833115
- **Coordinator:** ICCS (Greece)
- **Partners:** 28 Partners from 13 different European countries
- **Duration:** 24 Months
- **Funding type:** Innovation Action
- **Effort:** 1170 Person-months

Consortium



Research Centers & Universities
ICCS
IOSB
BPTI
CERTH
UPV
CNRS
UM

Non-Profit Organizations
CUING
MCA
SF

Industries & SMEs
ETRA
ITTI
IfmPt
SIV
SPH
PARCS
TRIL
CTL

LEAs/Practitioners
ENSP
ERTZ
FNTT
ELAS
HfoeD
KEMEA
MDSPP
PPM
PSNI
ROSPP

Vision

A series of novel and enhanced capabilities

Analyzing	multiple massive data streams, coming from different sources (open web, Darknet, online social networks, CCTV and video surveillance systems, traffic and financial data sources)
Integrating	information into dynamic knowledge graphs that capture the structure, interrelations and trends of terrorist groups and individuals, cybercriminal organisations and OCGs
Predicting	abnormal or deviant behaviour and radicalisation risks, based on sound predictive policing methods, underpinned by valid psychological, sociological and linguistic models
Performing	dependable soft target risk assessment and cybercrime trend prediction at different timescales
Becoming	continuously more knowledgeable of the operations and activities of criminal organisations, by coupling the semantic technologies with deep and ensemble learning techniques
Maintaining	high situation awareness at all times by means of user-centred visual analytics and human-machine interaction techniques

Main Technologies

- Visual Intelligence
- Data Mining for Crime Prevention and Investigation
- Semantic Technologies and Semantic Integration
- Predictive Policing, Trends Detection and Risk Prediction
- Detection of Cyber-criminal Activities
- Human-Machine interfaces and Situation Awareness

Objectives

SO-1

Open, scalable and customizable toolset that provides support for extreme-scale data streams analytics

SO-2

Semantic fusion powerful knowledge graphs combined with advanced reasoning and machine learning engines

SO-3

Situation awareness enabling applications tailored to specific operational needs of LEAs

SO-4

Common platform architecture available to end-users for thorough validation (TRL-7)

SO-5

Demonstration and evaluation in realistic cases

Training activities

Transferability framework

SO-6

Compliance with the legal, ethical, privacy, societal and court-acceptance guidelines and EU best practices

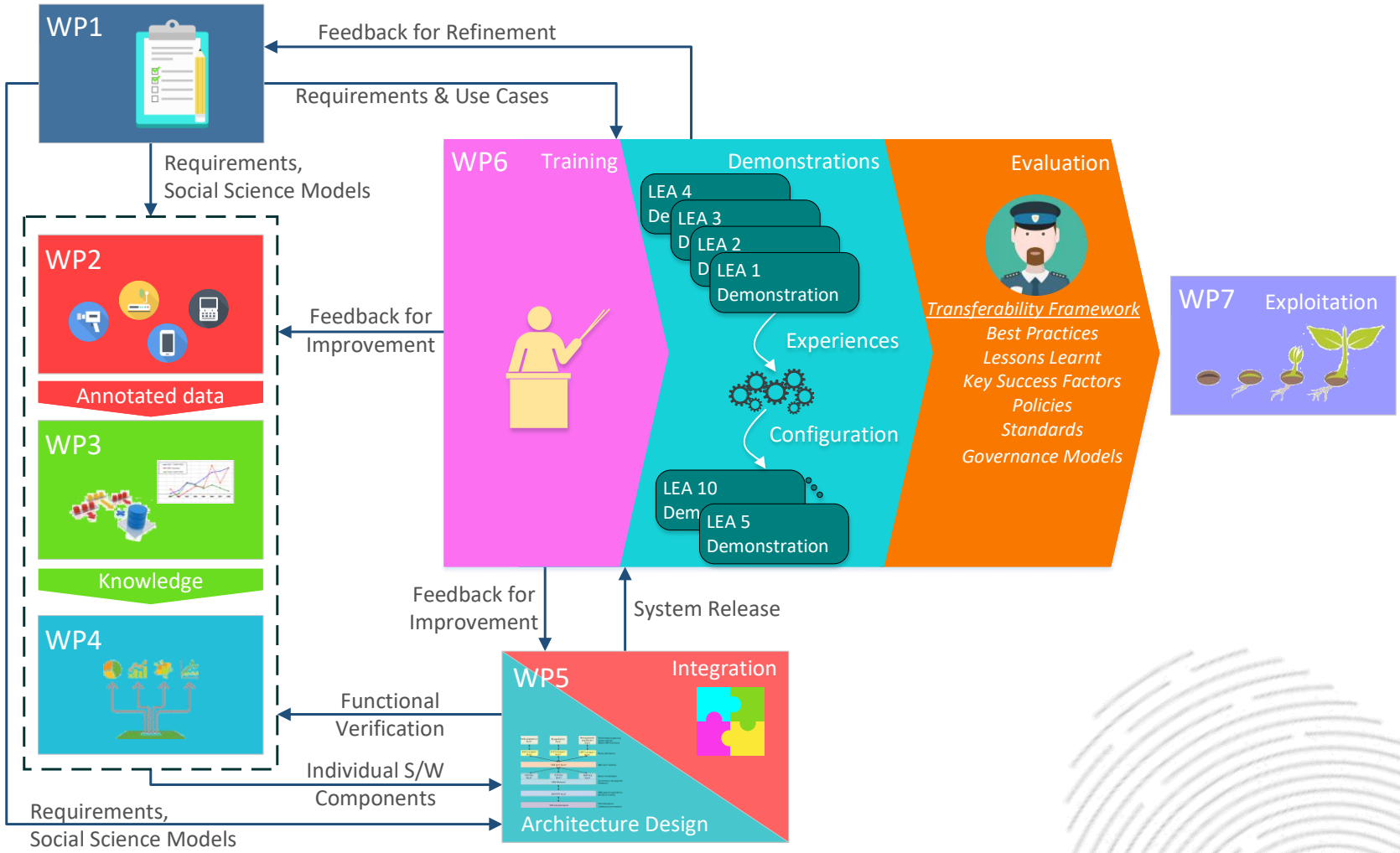
SO-7

High multi-dimensional impact, continuity and business perspective of project results

Objectives linked to tangible results

SO-1	SO-2	SO-3	SO-4	SO-5	SO-6	SO-7
R1 – AEDAS: Advanced Extreme-scale Data-stream Analytics tool-Set	R2 – CIMARA-DB: Models for Adaptive Risk Assessment of Deviant Behaviour	R5 – EC-VAT: Extensible and Customizable Visual Analytics Toolkit	R7 – IPPA: Integrated PREVISION Platform Architecture	R8 – PTF: PREVISION Transferability Framework	R10 – PLESCA: Privacy, Legal, Ethical, Societal and Court-Acceptance framework	R11 – PBESP: PREVISION Business, Exploitation and Sustainability Plan
	R3 – ICONU: Intelligent Criminal Organisation Networks Unveiled	R6 – CPI-SApps: Crime Prevention and Investigation, Situation Awareness supporting applications		R9 – TC-P3: Training Curriculum in PREVISION-enabled Predictive Policing		
	R4 – LLM4CONets: Lifelong Learning Machines for Criminal Organisation Networks					

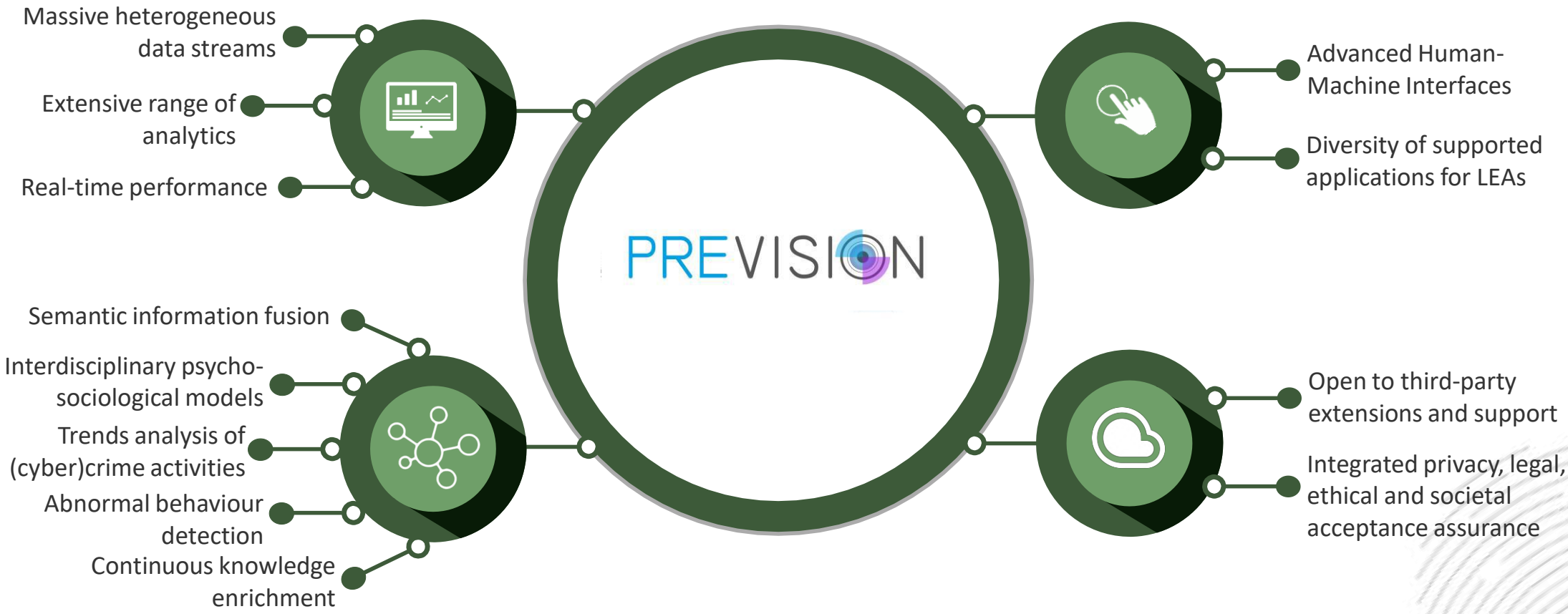
Methodology



Use Case Categories

1. Soft Targets protection
2. Radicalisation & terrorist threat prevention
3. Financial Crime Investigation
4. Cyber-enabled crime
5. Illicit markets investigation

Innovation Potential



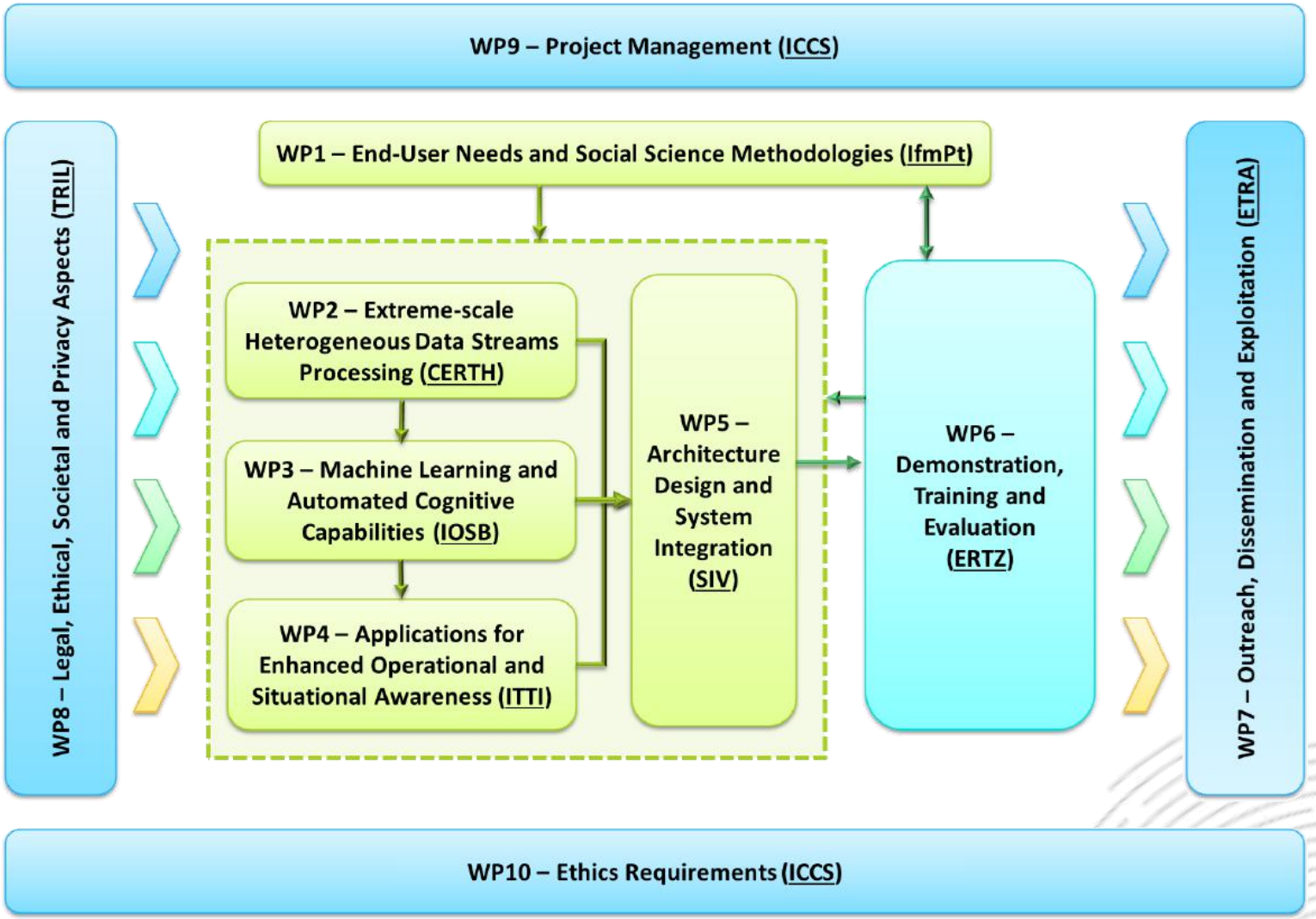
Impact – Work Programme

- Improved support for the work of LEAs in managing Big Data
- Increased awareness regarding the state of the art and trends in cybercriminal activities
- In-depth knowledge of means of preventing and countering emerging and future cybercriminal activities
- Improved capabilities to combine and analyse in near-real-time large volumes of heterogeneous data to anticipate criminal events
- Shorter delays between the emergence of new cybercrime activities and the deployment of countermeasures
- Provide a European, common strategic approach for preventing and countering an emerging cybercrime activity in its early stage of development
- Provide a European, common strategic approach for processing and combining huge amounts of data in the context of crowd protection in full compliance with applicable legislation on protection of personal data

Impact – Security Union

- ***Denying terrorists the means*** – accelerate cybercrime detection and speed up illegal trafficking investigation in illicit markets (e.g. Darknet).
- ***Protecting Europeans online*** – provide insights on cybercrime groups' activities and address terrorist radicalisation online in a preventive manner.
- ***Sharing information*** – provide knowledge graphs and interfaces with open specifications, encourage interoperability, support team collaboration within and across LEAs.
- ***Soft targets protection*** – produce new data-driven and data-intensive methods of proactive law enforcement.
- ***Facing the challenges of cyber threats*** –enable adaptive risk assessment of cybercrime threats.
- ***Protecting personal data while supporting efficient criminal investigations*** – tightly integrate ethical, legal and societal impact assessment and organise training activities.

Work Packages



Platform & Tools

- Why a Platform?
  - Ability to chain tools together, create service bundles and entire workflows
  - Ability to plug new tools that are compatible with existing ones
  - Reduce the effort of jointly exploiting disjoint tools and facilities
  - Utilize core underlying infrastructure services, like authentication and authorization, logging, encryption, messaging, visualization, etc.
- Why Tools?
  - Ability to quickly test and deploy small S/W components

Thank you

Kostas Demestichas (cdemest@cn.ntua.gr)