„AN EXAMPLE FOR THE NATIONAL UPTAKE OF SECURITY RESEARCH OUTPUTS: THE LITHUANIAN MODEL OF CENTRE OF COMPETENCE"

Egidija Veršinskienė, Lithuanian Cybercrime Centre of Excellence for Training, Research and Education

19th-20th of February 2020, Brussels

driver+

Driving Innovation in Crisis Management for European Resilience

L3CE – LITHUANIAN CYBERCRIME CENTER OF EXCELLENCE

- Non-profit public organization, funded by two national universities – Mykolas Romeris university and Kaunas University of Technology
- Clients: EU defense and security agencies
- L3CE invests in the development of new defense, security and intelligence approaches by integrating social and technical innovations, traditional methods with new technologies:
  - Artificial Intelligence
  - Natural language processing
  - Analysis process automation
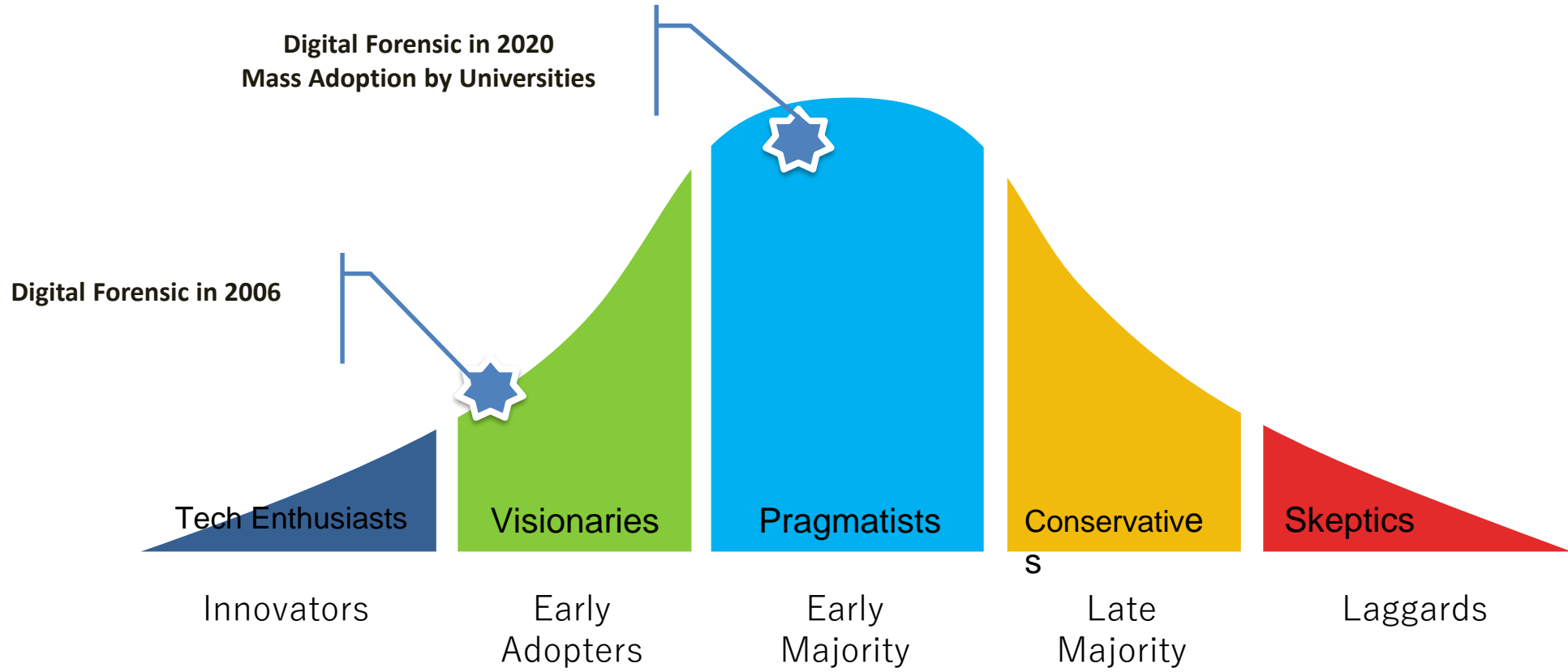 - Visual analytics for more efficient cyber related operations and decision making

NATIONAL SECURITY CAPABILITIES – WHAT IS NEXT BIG STEP?

- Impact of security research results is still not sufficient enough to make a marked difference in preventing cyber incidents, crimes, threats.
- Key challenges of security and defense agencies:
  - Lack of resources human/financial
  - Competences in digital intelligence and investigation
  - Political and societal pressures
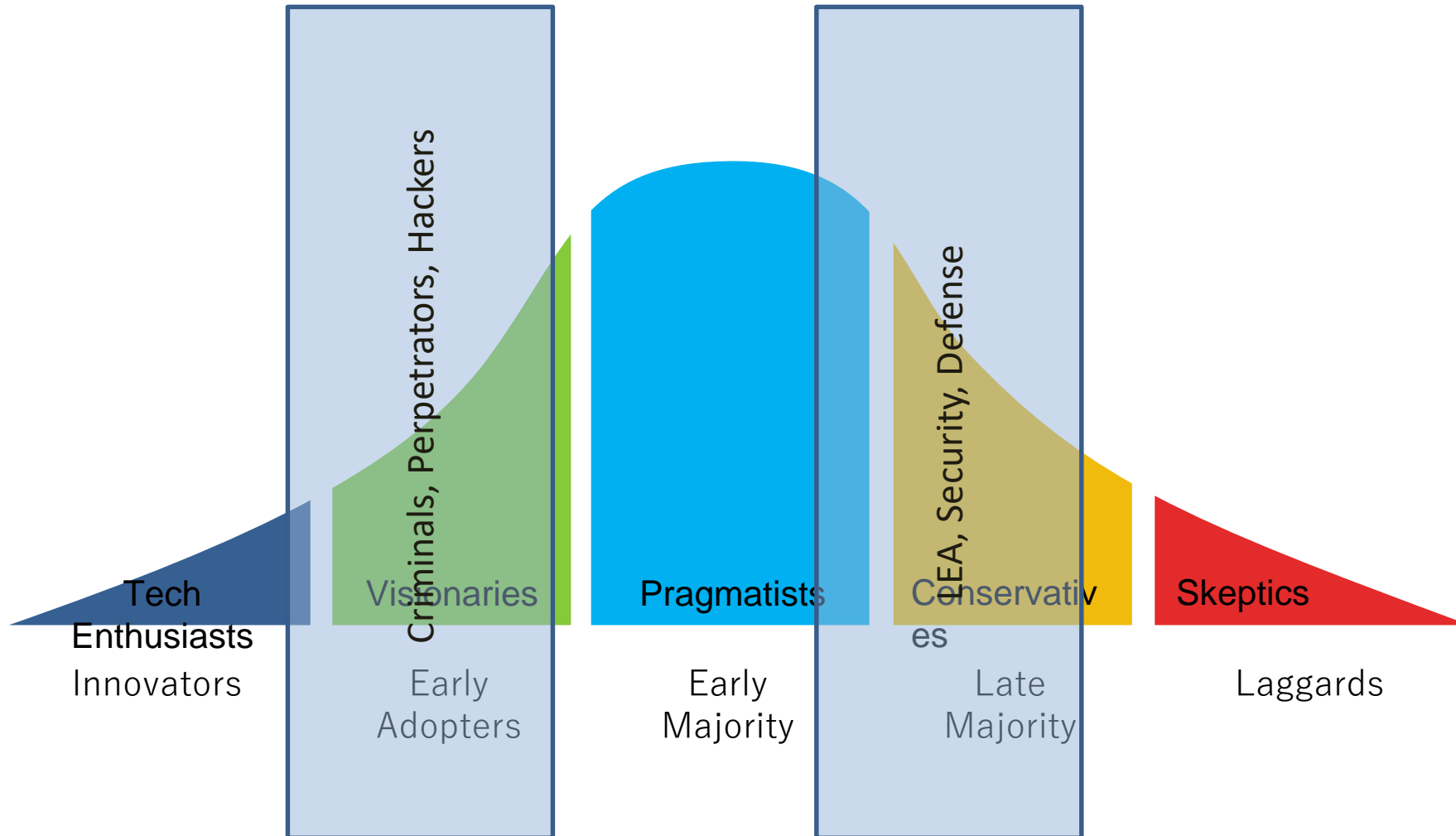 - Relevant tools and technologies

PRESENTATION OF NAAS
(Information Security and Information Threats' Detection, Analysis, Research and Education Ecosystem)

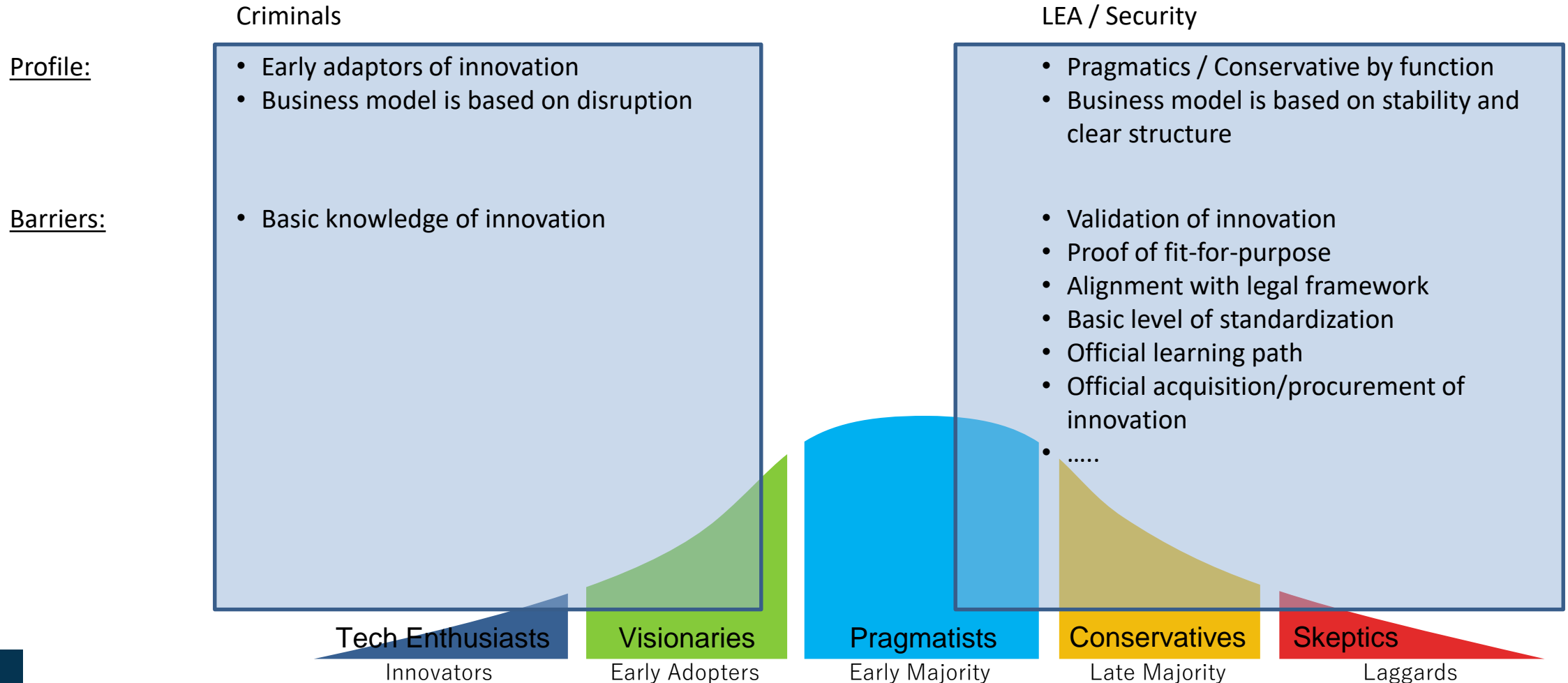# PRODUCT ADOPTION CURVE AND NEW CRIMES/THREATS

Digital Forensic in 2020
Mass Adoption by Universities

Digital Forensic in 2006

Tech Enthusiasts

Visionaries

Pragmatists

Conservatives

Skeptics

Innovators

Early Adopters

Early Majority

Late Majority

Laggards

PRODUCT ADOPTION CURVE AND NEW CRIMES/THREATS

DISRUPTIVE INNOVATION ADOPTION BY SECURITY ACTORS

Criminals

LEA / Security

Profile:

- Early adaptors of innovation
- Business model is based on disruption

- Pragmatics / Conservative by function
- Business model is based on stability and clear structure

Barriers:

- Basic knowledge of innovation

- Validation of innovation
- Proof of fit-for-purpose
- Alignment with legal framework
- Basic level of standardization
- Official learning path
- Official acquisition/procurement of innovation
- …..

Tech Enthusiasts	Visionaries	Pragmatists	Conservatives	Skeptics
Innovators	Early Adopters	Early Majority	Late Majority	Laggards

TACKLING DISRUPTIVE CHALLENGES

Tackling new challenges …

"wicked"

disruptive

continuous innovation

novel ideas

business as usual

supply
ideas for potential solutions

known ideas

known problems

unknown problems

demand
problems that need solutions

© Ulf Ehlert

http://www.understandinginnovation.wordpress.com
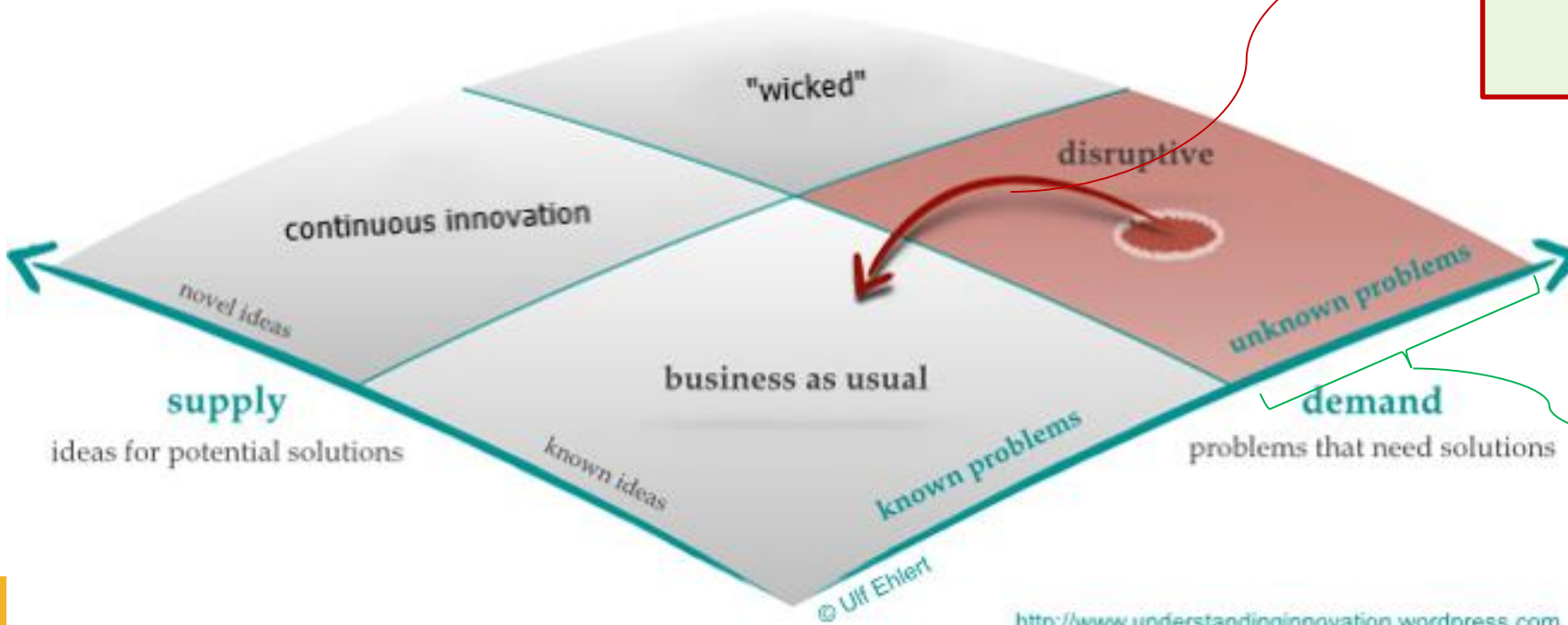
We need to establish ecosystem that **facilitate and speed-up** LEA innovation uptake for disruptive challenges

Criminals are Early Adaptors of technological and social innovations and acts as disruptive challenge for LEA/Security

NAAS* COLLABORATIVE MODEL FACILITATED BY CENTER OF EXCELLENCE

SPARTA NETWORK

ENLETS NETWORK

ASGARD COMMUNITY

DRIVER+ COMMUNITY

NATO STRATCOM R&D units

EUROPOL EC3

INTERPOL

INTERNATIONAL COLLABORATION

NATIONAL LEVEL
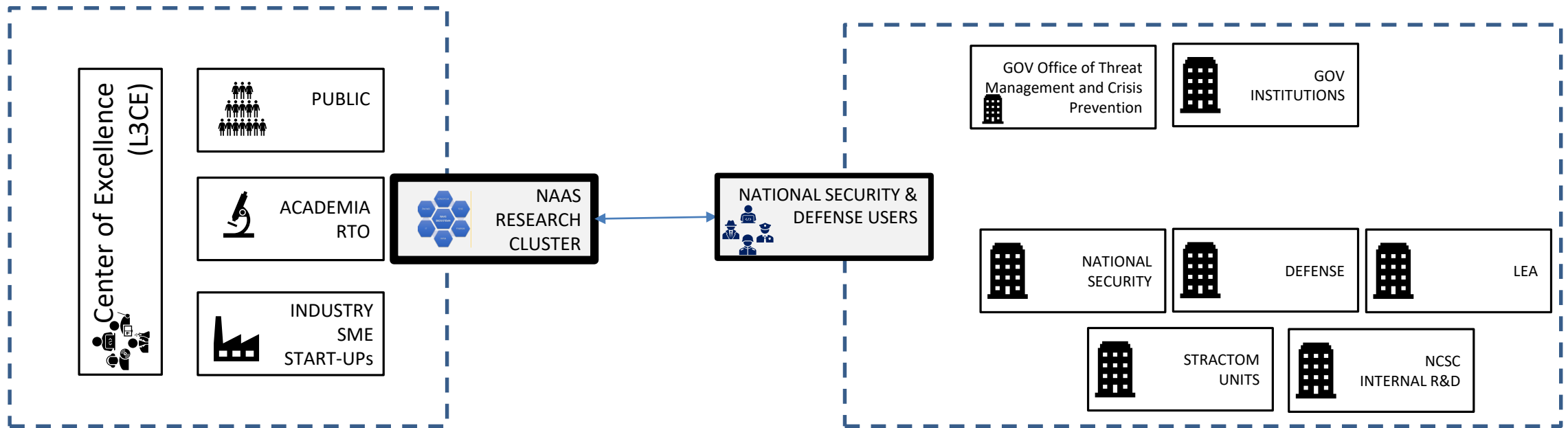
Center of Excellence (L3CE)

PUBLIC

ACADEMIA RTO

INDUSTRY SME START-UPs

NAAS RESEARCH CLUSTER

NATIONAL SECURITY & DEFENSE USERS

GOV Office of Threat Management and Crisis Prevention

GOV INSTITUTIONS

NATIONAL SECURITY

DEFENSE

LEA

STRACTOM UNITS

NCSC INTERNAL R&D

* NAAS – "Information Security and Information Threats' Detection, Analysis, Research and Education Ecosystem"

CRITICAL SUCCESS FACTORS

- **Trusted Environment**
- **Co-Creation**
- **Fit For Purpose**
- **Function or Goal Oriented**
- **Open Innovation**

NAAS: VALUE EXCHANGE MODEL
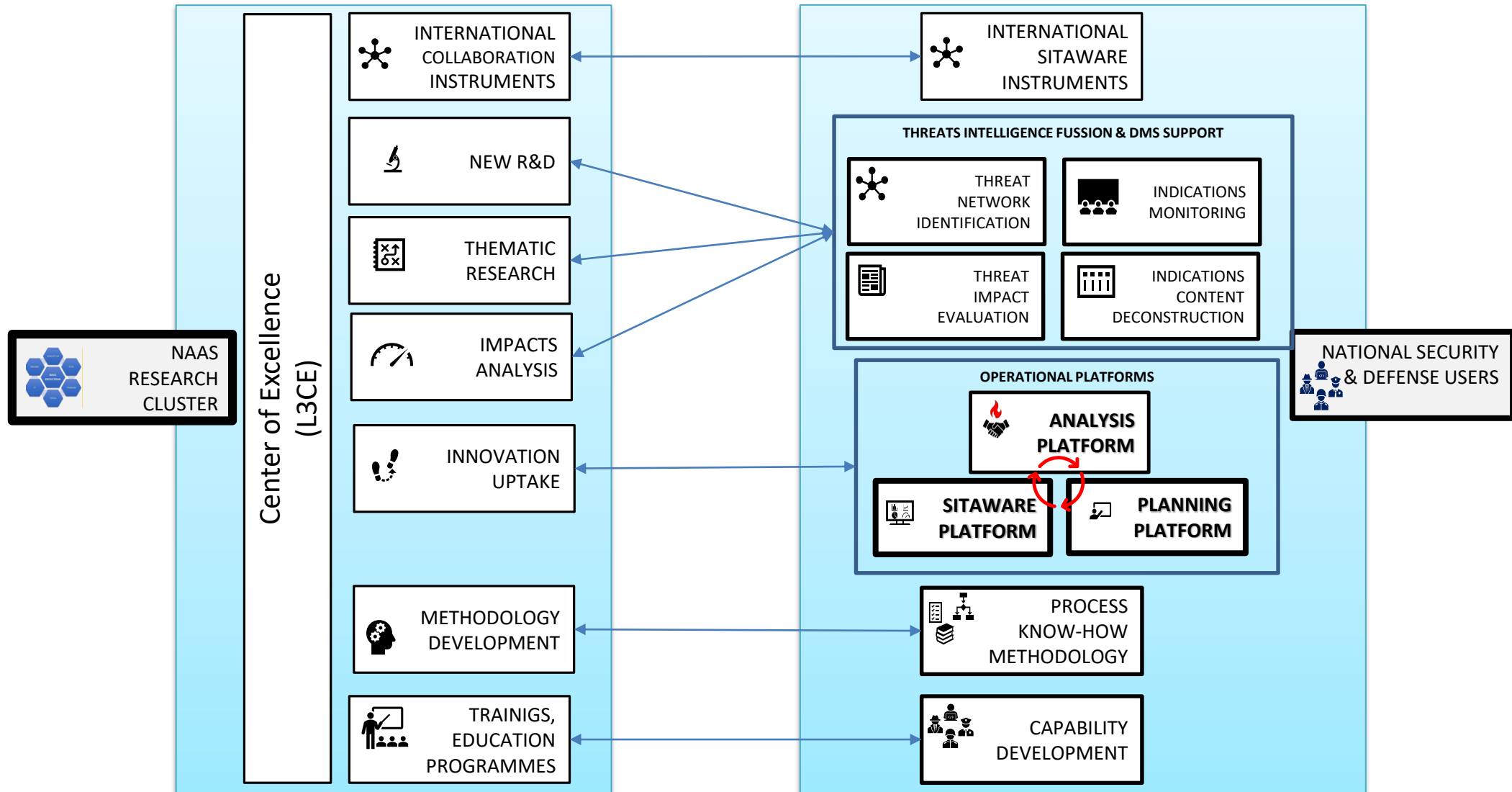
EXPECTATION ALIGNMENT

EFFECTS
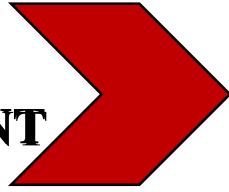
ON TIME INFORMED NATIONAL INSTITUTIONS MANAGEMENT ON THREATS
PROTECTED, SUPPORTED DEFENCE & SECURITY DECISION MAKING PROCESSES
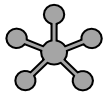NATIONAL RESOURCES ARE **EFFECIVELY PLANNED**

EVOLVING ENVIRONMENT
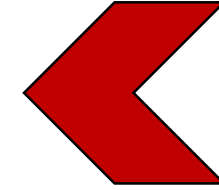
EVOLVING THREATS

NEW ACTIVITIES
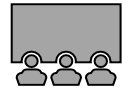
Training of professionals

Scientific research

Scientific collaboration

New concepts, methods development

Funding instruments

VALUE ADD
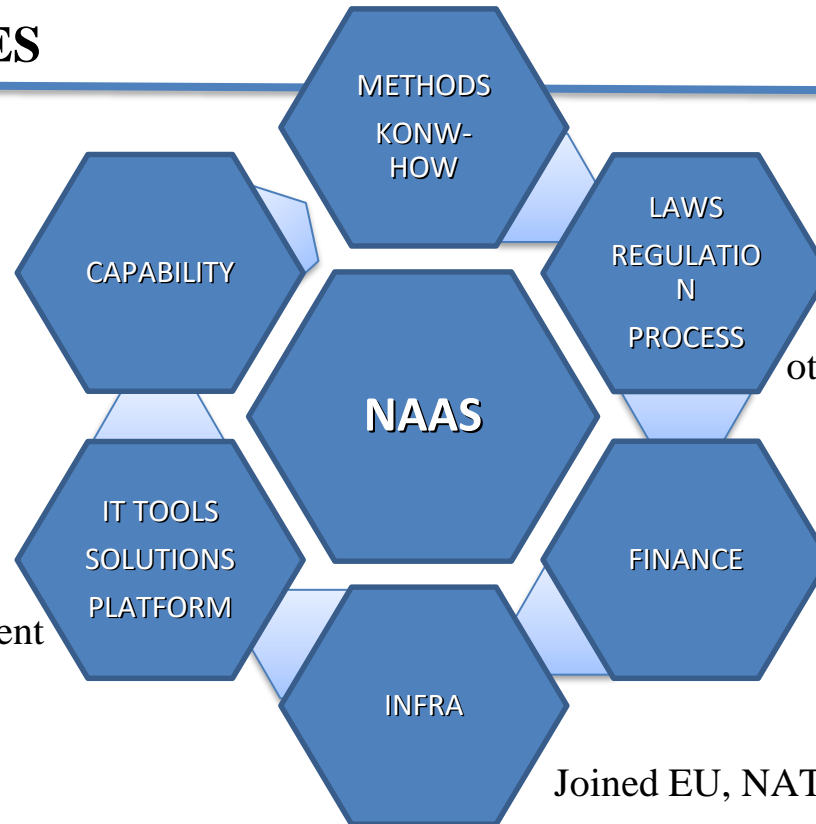
Public Resilience,
Hybrid Threats Analysis Specialists

Info Threats impact analysis and
other phenomena based research & analysis

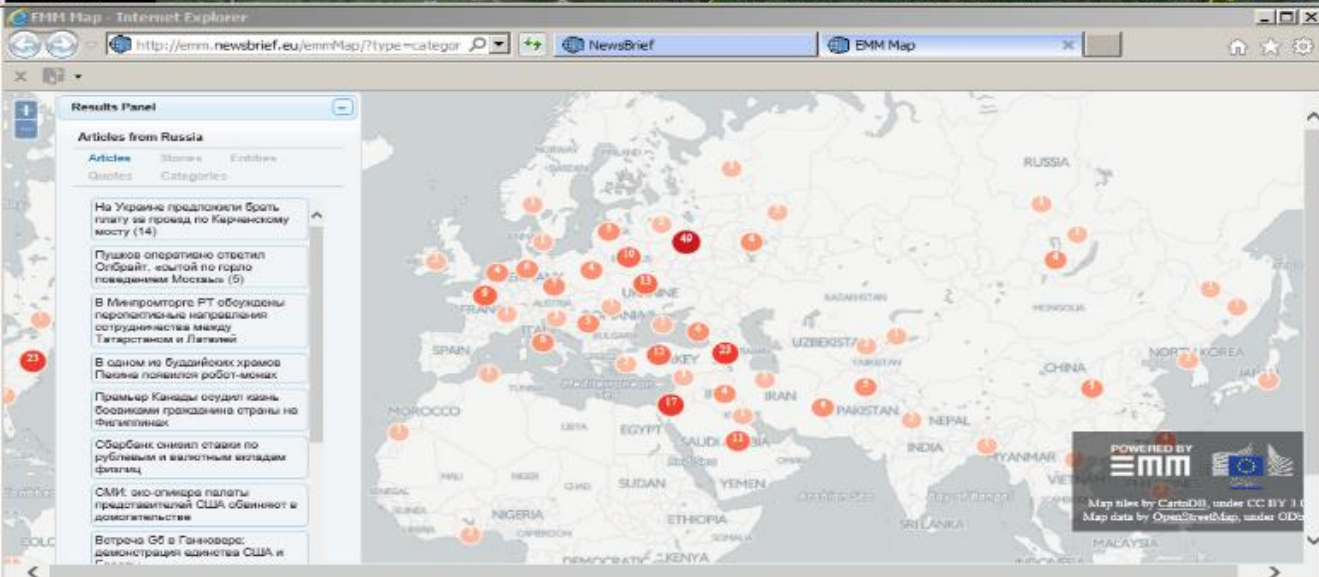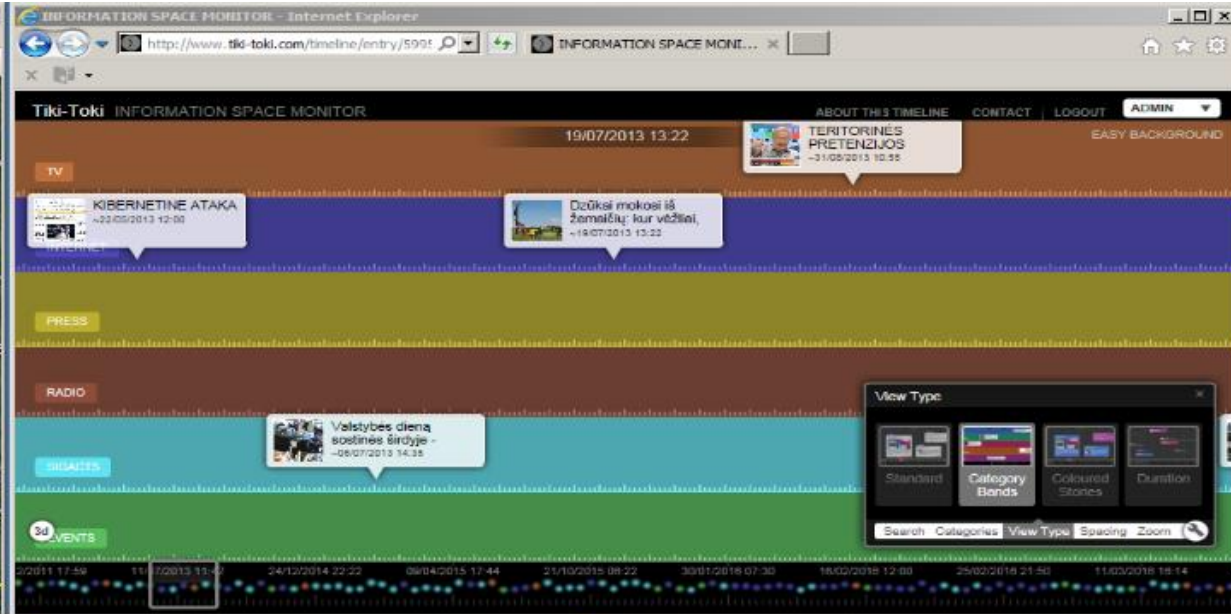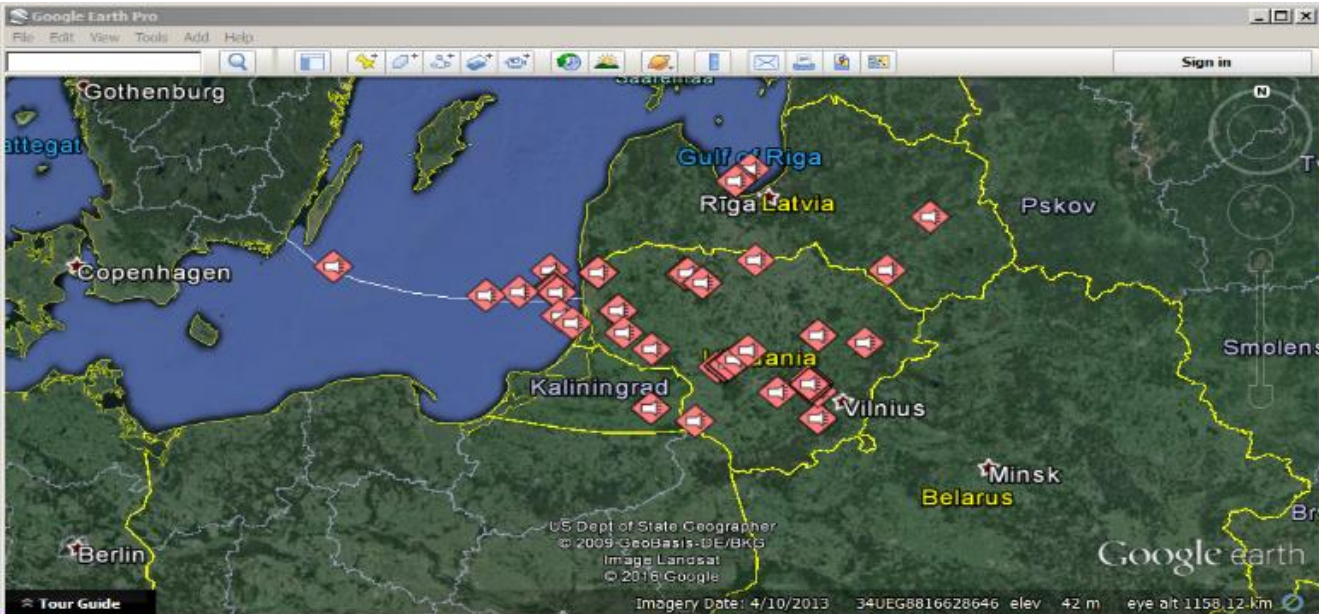National and international
collaboration

Public Resilience, Information Security
and Defense Methodology

Joined EU, NATO RIA actions and projects,
Innovations' uptake

NAAS

METHODS KONW-HOW

LAWS REGULATION PROCESS

CAPABILITY

IT TOOLS SOLUTIONS PLATFORM

FINANCE

INFRA

CASE STUDY: UPTAKE OF ECOPOL PROJECT
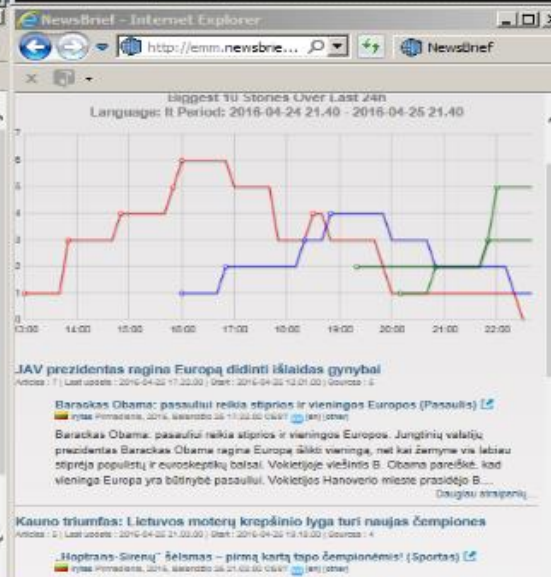
CONTACT
REACH US

@driver_project

Groups:
Driver Project

Driver Project

More information about the project - coordination@projectdriver.eu
Interested in collaborating with us? - cooperation@projectdriver.eu
Communication and media contact communication@projectdriver.eu

driver-project.eu