ITS HELLAS
Intelligent Transport Systems

6ο ITS Hellas Ψηφιακό Συνέδριο 2020

«Ευφυή Συστήματα Μεταφορών και Εξελίξεις στην Ελλάδα»

Multimodality ecosystems and Cyber-security challenges

Konstantinos Maliatsos

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

UNIVERSITY OF THE AEGEAN
GREECE

Με την υποστήριξη:

Ευρωπαϊκή Επιτροπή
Αντιπροσωπεία στην Ελλάδα

Υπο τις αιγίδες:

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΠΟΔΟΜΩΝ ΚΑΙ ΜΕΤΑΦΟΡΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

Σύλλογος Ελλήνων Συγκοινωνιολόγων

ΕΣΕΕ
ΕΛΛΗΝΙΚΗ ΣΥΝΟΜΟΣΠΟΝΔΙΑ ΕΜΠΟΡΙΟΥ & ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑΣ

ΣΕΚΕΕ

ILME
ΙΝΣΤΙΤΟΥΤΟ LOGISTICS MANAGEMENT ΕΛΛΑΔΟΣ

GREEK COLD STORAGE & LOGISTICS ASSOCIATION

ΟΔΑΕ
ΟΜΟΣΠΟΝΔΙΑ ΦΟΡΤΗΓΩΝ ΑΥΤΟΚΙΝΗΤΩΝ ΕΛΛΑΔΟΣ

Multimodality

- **Multimodality** is the application of multiple literacies (or modes or media) within one system, eco-system or platform.
- **Multimodal systems** provide the user with multiple modes of interaction with the system.
- They provide several distinct tools for using or utilizing the offered services.

- The term "multimodal" is generally used to describe means of communications, e.g. "communication practices in terms of the textual, aural, linguistic, spatial, and visual resources"
- used in: math (multimodal distribution), physics (multimodal propagation), social sciences (multimodal anthropology, multimodal interaction), IT (multimodal learning, fusion) and more.
- Also used to describe heterogeneity in the modern use and utilization of Essential Services
  - **Multimodal Transport**

Operators of Essential Services

- Energy
- **Transport**
- Finance / Banking
- Health
- Water Supply
- Digital Infrastructure

Operators of Essential Services

Essential Services

- High value for the people
- High impact for the societal structure

but

- Popular target for terrorists, cyber-attackers, hackers, etc.

Determination of incident severity

Criteria for incident assessment

- Affected population - geographical distribution
- Impact on the country/EU economy
- Public functions, public safety / order
- Threat to human life
- Impact on public opinion
- International relations / influence in other countries
- Interdependence with other sectors
- Impact on the environment
- Recovery time after the incident

Areas of Essential Services system protection

Physical and environmental security
Security of supplies
Contractual relationships' management
Outsourcing Management
Access control to premises
Physical and logical separation of essential systems
Essential system access controls
Essential systems activity log
Processed-stored-transmitted information
Development and maintenance of essential systems
Hardware management
Software change management
Project Management

Multimodal transport

- The transportation of goods
  - under a single contract,
  - but performed with at least two different modes of transport;
  - One carrier is liable for the entire trip,
- Multimodal transport extends in urban mobility. The way people travel by various:
  - Public/mass transport systems (usually managed by the city).
  - Means of transport, including bikes, cars, buses, subways, and micromobility devices such as electric scooters.

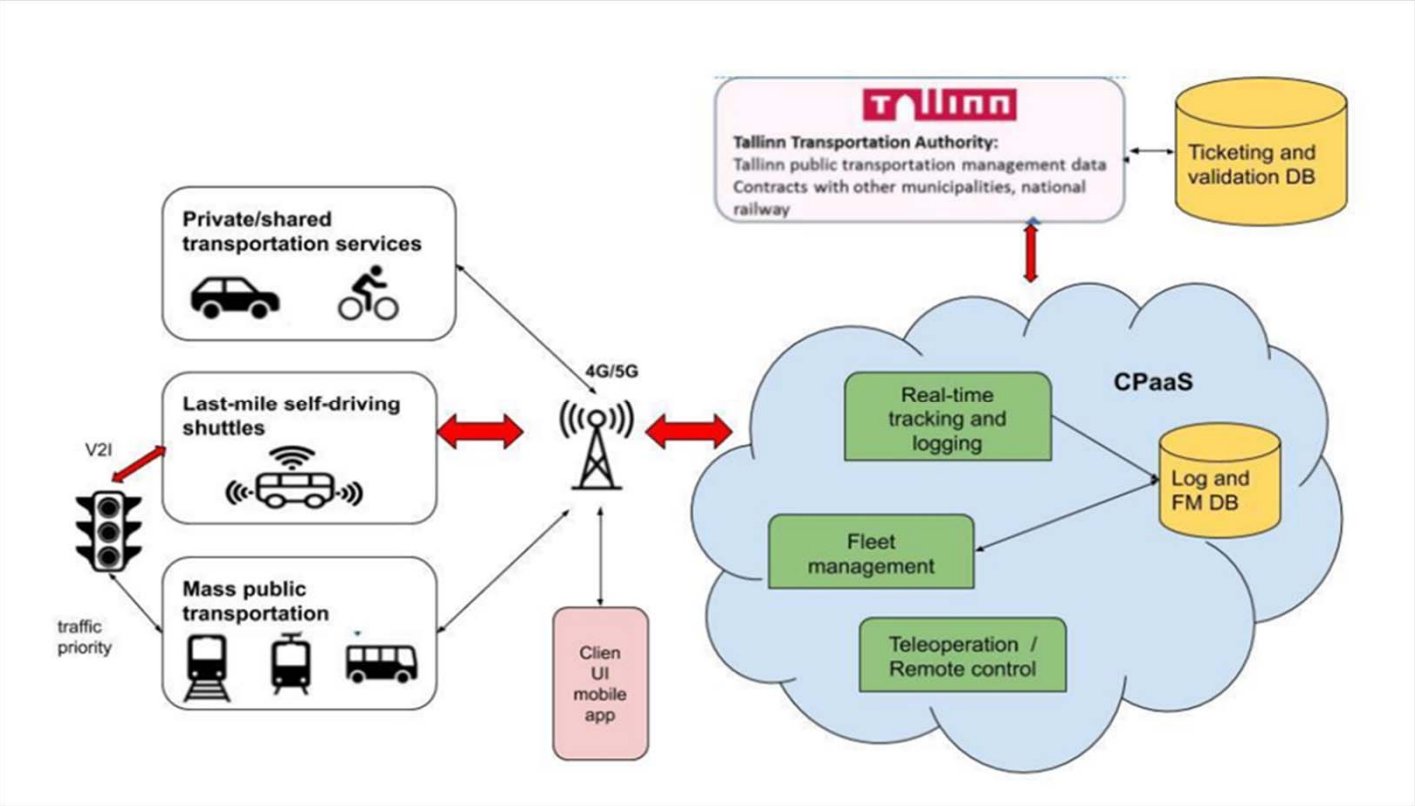
Multimodal transport

only functional through ICT

- People quest for alternative transportation modes with roads and highways congested
- Requires coordination of public and non-public transport operators
- **Multi-modal transport requires data exchange and interconnection**
  - High quality of service – Quick commute
  - Shared mobility
  - On-demand ride services
- The last-mile problem

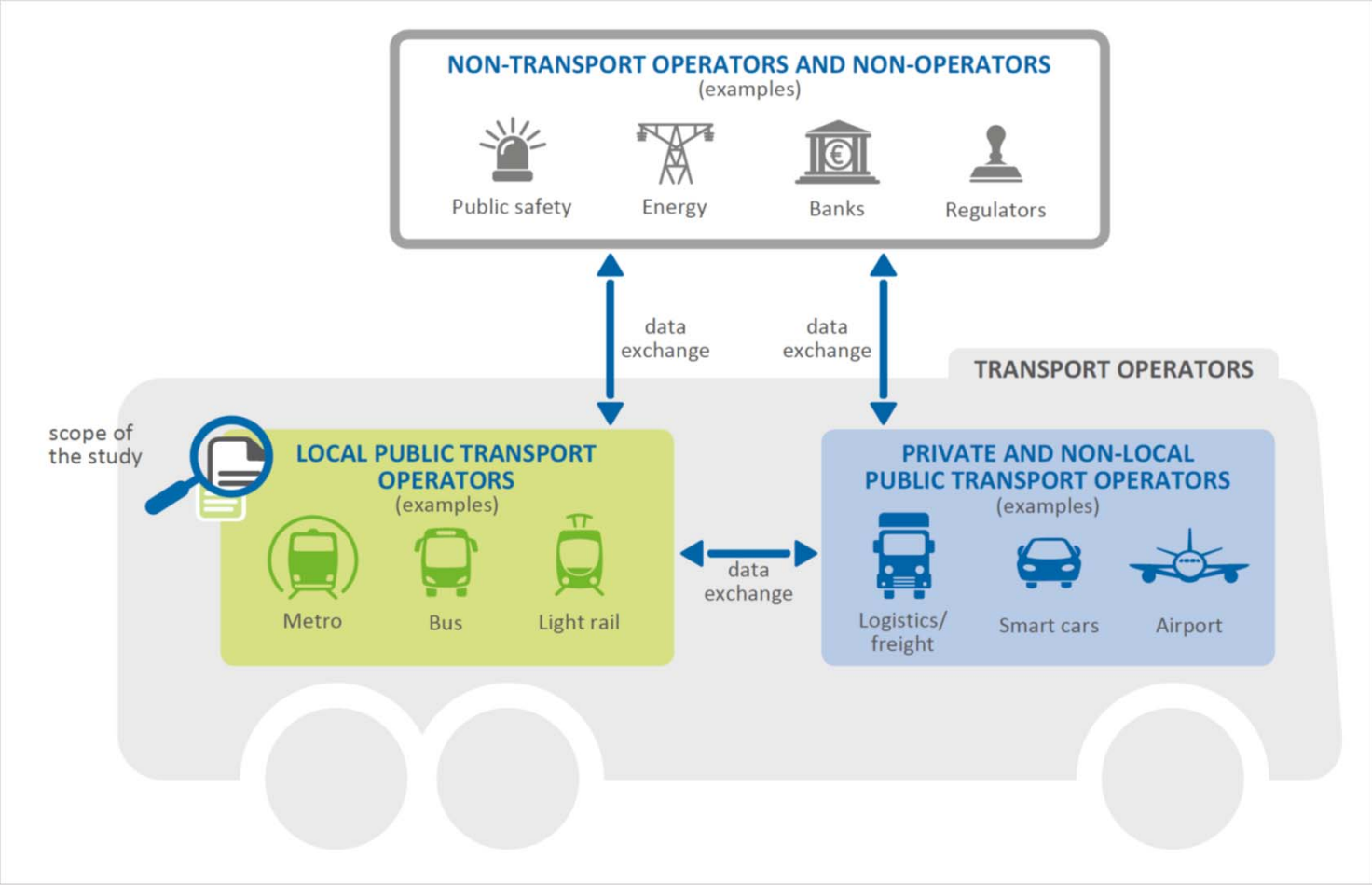
Multimodal transport

in the urban environment



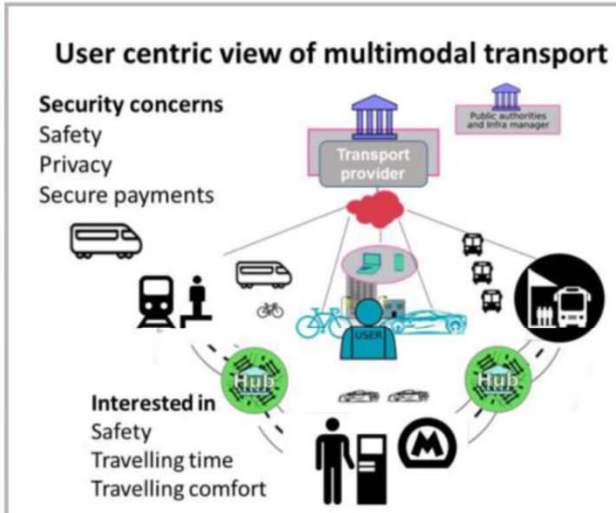
- Intelligent city example (CitySCAPE: Tallin city use case)

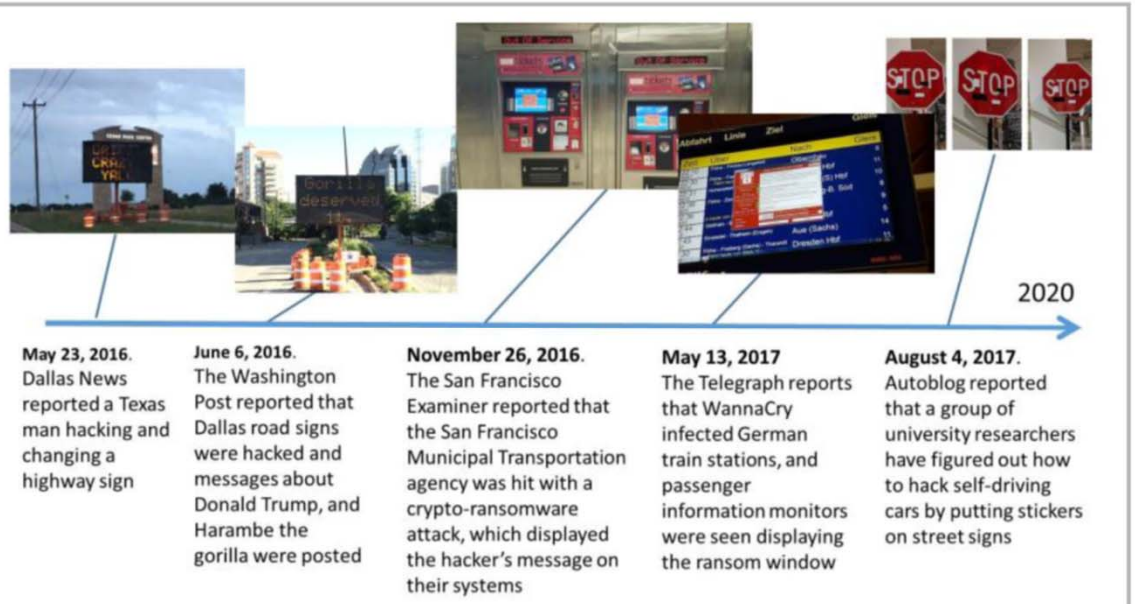
Data Exchange between modes and domains



Attacks on Transport Systems

- A huge attack surface





Types of Threats

- Denial of Service
- Manipulation of software
- Malware
- Modifications of hardware
- Software vulnerabilities
- Network vulnerabilities
- System failure
- Failures of devices
- Physical destruction of device
- Natural disaster
- Data alteration
- Data leakage
- Personal Data Sharing and Identity theft
- Incorrect or Outdated Personal Data
- Injection of false/malicious data on the network
- Man-in-the-middle / Insecure channels
- Wiretapping/Eavesdropping
- Insider threats
- Operator and/or user errors

Vulnerabilities

- Common to other IT systems
- Wireless communications and networks
- Vulnerabilities introduced with the integration of physical and virtual layers
- Problems due to increased automation
- Cohabitation between legacy and new systems
- Scale and complexity of transportation networks
- Applying networked technology across large transport systems
- Multiple interdependent systems
- Access to real-time data
- Higher volumes of passengers and freight
- Online passenger services

Impact and risks

Business

- Impact on operations:
- Loss of revenue
- Impact on reputation / loss of trust
- Non-compliance with the regulation on data protection
- Risks on hardware and software
- Reliance on invalid information
- Lack of security of dependencies
- Unavailability of a dependency

Societal

- Unavailability of the Transport service
- Disruption to the society
- Passengers' health and safety
- Environmental impact
- Confidentiality and privacy

*according to ENISA

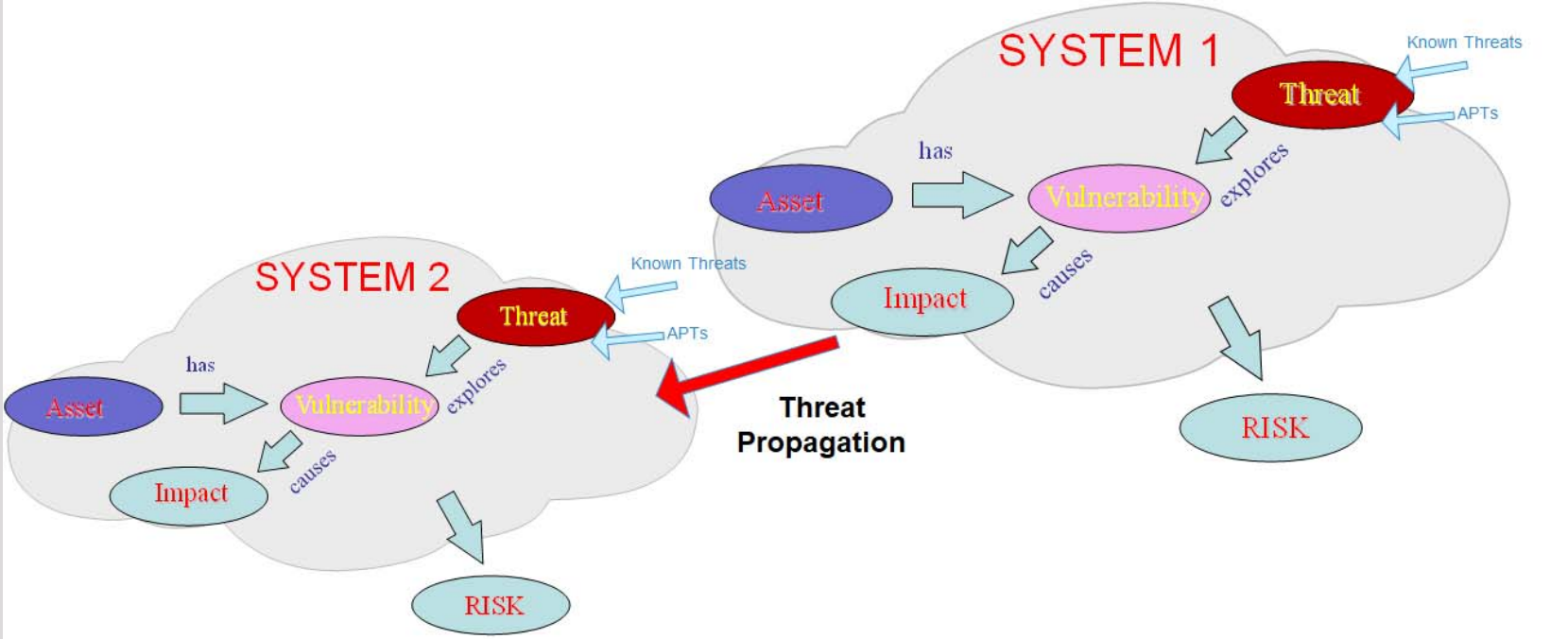
Challenges

- Integration of security for safety
- Collaboration and exchange information on cyber security
- Situational awareness of cyber threats
- Phasing out of legacy systems
- Data exchange between Transport and Smart Cities operators
- The importance and spending being afforded to cyber security
- Checking for sufficient countermeasures
- Resistance to security adoption

Is there a Fix? The CitySCAPE vision

- ACT PROACTIVELY!!
- Perform risk analysis and risk assessment
- Apply security assurance practices
- Investigate propagation of threats and identify common threats
- Employ alarms/surveillance for protecting physical and digital assets
  - capture the propagation of threats
  - estimate the risk level/criticality
  - assess the financial impact terms for tangible and 'non-tangible' assets
- Use communication, experience and learning for timely detection/prevention
  - collaborative investigation of severe incidents by CERT/CSIRTs authorities and OES including real-time notifications to their network
  - predict upcoming malicious acts
  - propose/use updated countermeasures
- Apply security countermeasures
  - secure digital access controls to networks and data and encryption
  - Develop secure and private communication networks
  - identity management and authentication systems:
- Employ intrusion detection/protection systems
- Failover – failback to a minimum
- Automatically and/or remotely deactivate compromised assets to isolate risk

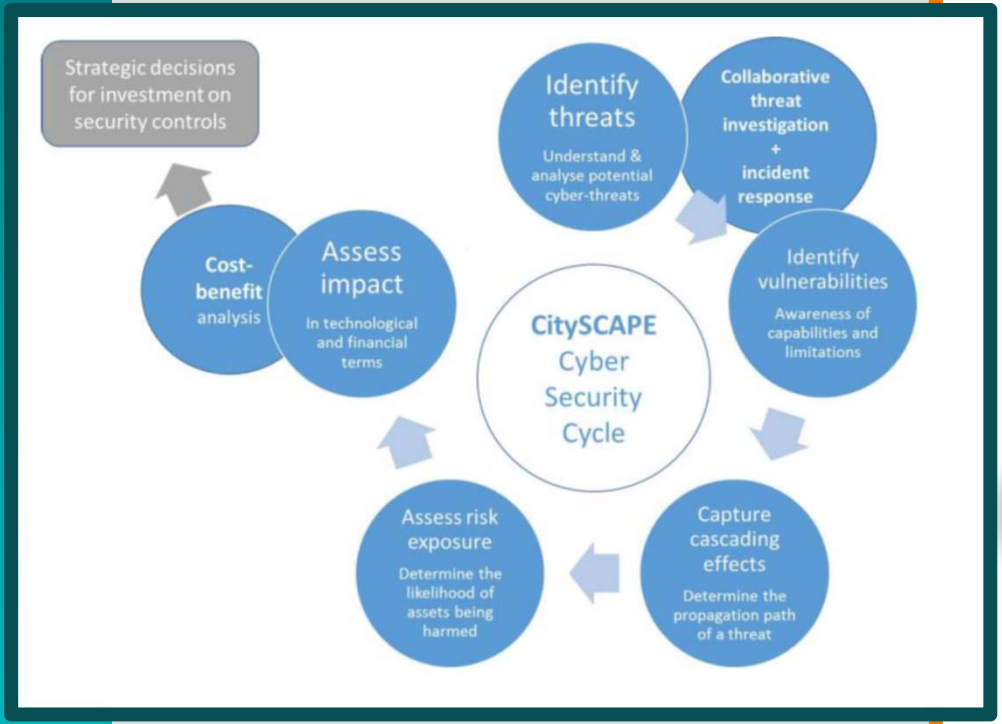
Risk Modeling and Cascading Effects



To proceed (in terms of modelling) we need:

The list of Assets
The vulnerabilities of each asset (asset – vulnerability association)
All potential Threats
The vulnerabilities that each Threat can explore (Threat – Vulnerability association)
At this point we have the indirect association "Which Threats (Attacks) can affect each Asset"

CitySCAPE


Strategic decisions for investment on security controls
Identify threats
Understand & analyse potential cyber-threats
Collaborative threat investigation + incident response
Identify vulnerabilities
Awareness of capabilities and limitations
Capture cascading effects
Determine the propagation path of a threat
Assess risk exposure
Determine the likelihood of assets being harmed
Assess impact
In technological and financial terms
Cost-benefit analysis
CitySCAPE Cyber Security Cycle


Risk analysis and impact assessment engine
Financial impact assessment engine
Collaborative threat investigation platform
CitySCAPE
IPS
IDS/IPS engines
SIEM as a Correlation engine with backlog of markers
Collaborative security incident response platform
Training

ITS HELLAS
Intelligent Transport Systems

6ο ITS Hellas Ψηφιακό Συνέδριο 2020

«Ευφυή Συστήματα Μεταφορών και Εξελίξεις στην Ελλάδα»

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

UNIVERSITY OF THE AEGEAN
GREECE

Ευχαριστώ πολύ!

Έχετε ερωτήσεις;

This work is a part of the CitySCAPE project.
This project has received funding from
the European Union's Horizon 2020 research and innovation
programme under grant agreement No 883321.
Content reflects only the authors' view and European Commission is not
responsible for any use that may be made of the information it contains.

Κωνσταντίνος Μαλιάτσος