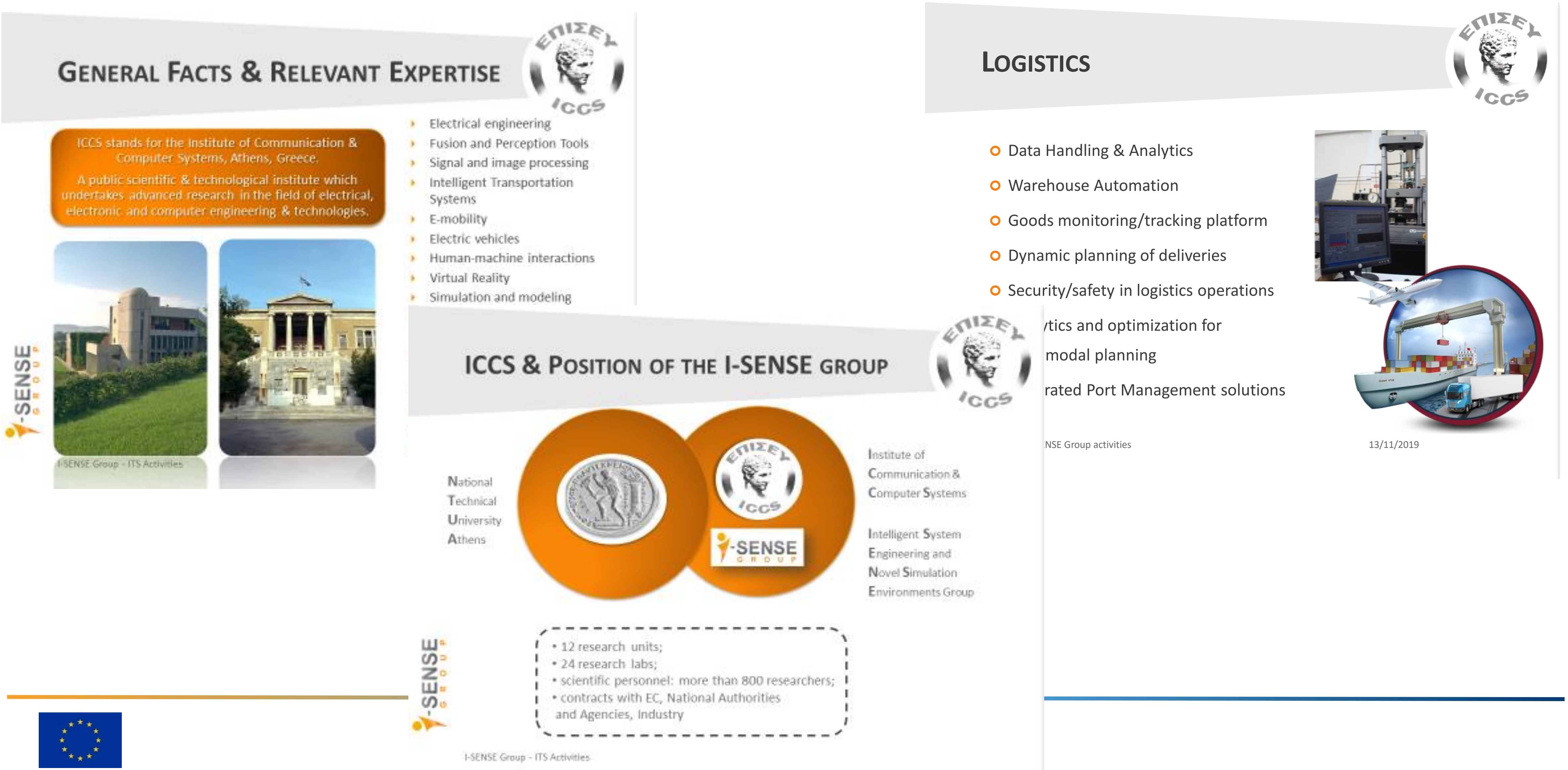
Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain (Cyber-MAR)

Giannis Karaseitanidis, I-SENSE/ICCS

Who we are?



General Facts & Relevant Expertise

ICCS stands for the Institute of Communication & Computer Systems, Athens, Greece.

A public scientific & technological institute which undertakes advanced research in the field of electrical, electronic and computer engineering & technologies.

- Electrical engineering
- Fusion and Perception Tools
- Signal and image processing
- Intelligent Transportation Systems
- E-mobility
- Electric vehicles
- Human-machine interactions
- Virtual Reality
- Simulation and modeling

I-SENSE Group - ITS Activities

ICCS & Position of the I-SENSE group

National Technical University Athens

Institute of Communication & Computer Systems

Intelligent System Engineering and Novel Simulation Environments Group

- 12 research units;
- 24 research labs;
- scientific personnel: more than 800 researchers;
- contracts with EC, National Authorities and Agencies, Industry

I-SENSE Group - ITS Activities

Logistics

- Data Handling & Analytics
- Warehouse Automation
- Goods monitoring/tracking platform
- Dynamic planning of deliveries
- Security/safety in logistics operations
- ytics and optimization for modal planning
- rated Port Management solutions

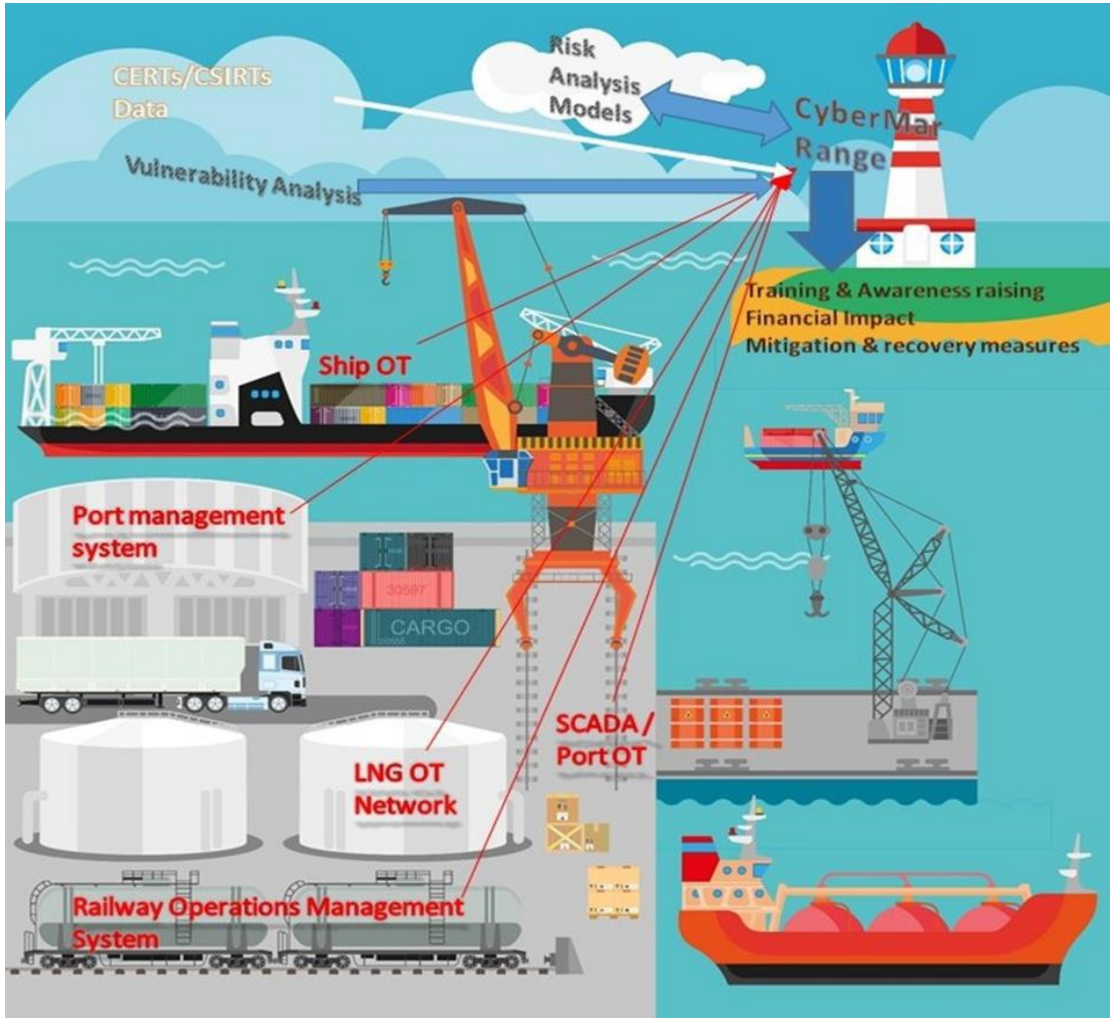
NSE Group activities 13/11/2019

#Maritime industry is easy meat for #cyber criminals

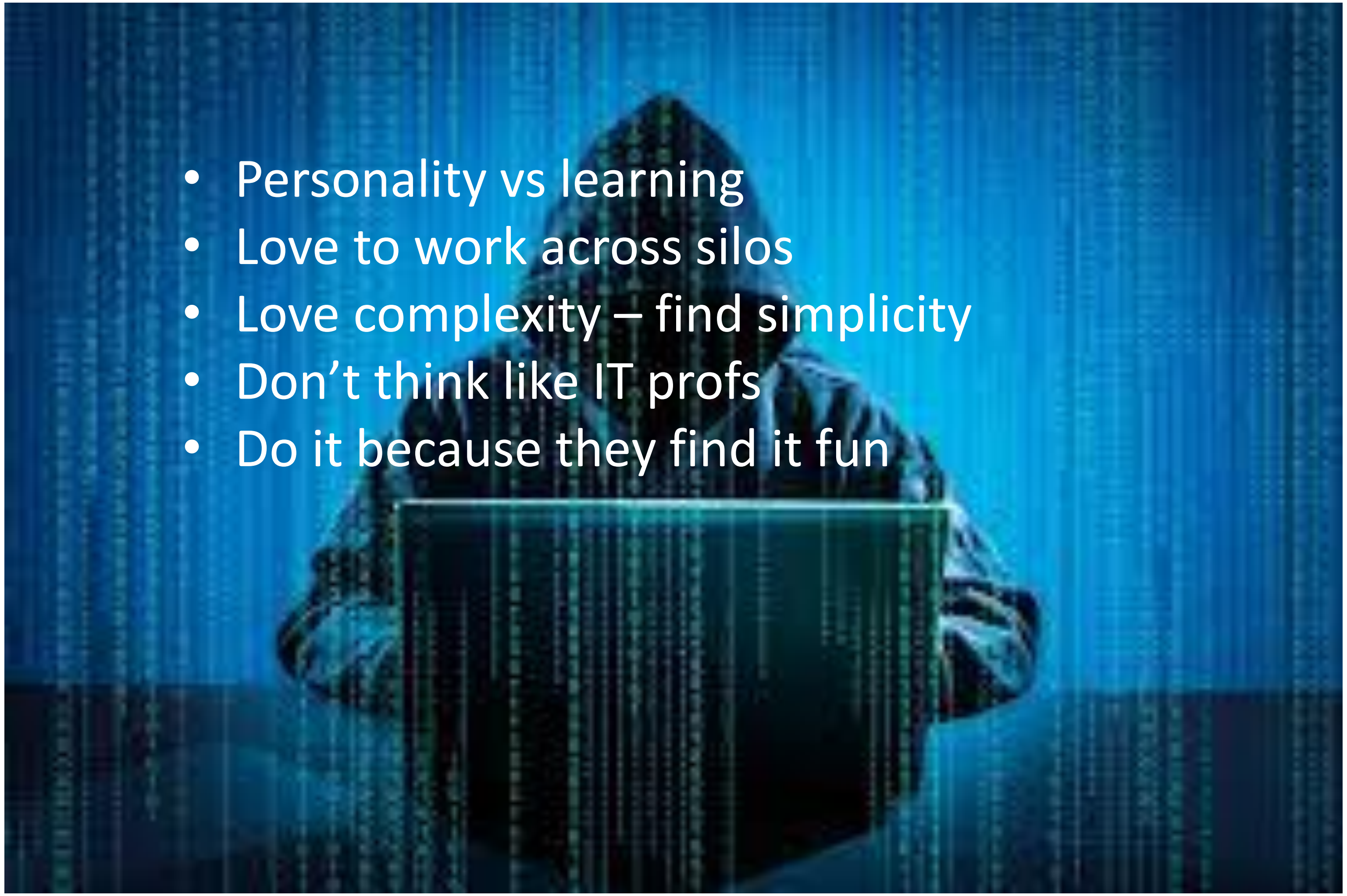
Cyber-MAR at a glance

Cyber-MAR takes advantage of cyber range environment and adopts a three-tiered approach targeting at:

- **People:** Continuous training through involvement in pilots, training sessions and familiarised with Cyber-MAR platform
- **Technologies:** Test technologies and identify complex vulnerabilities
- **Procedures:** Uncover areas for improvement and deficiencies in current procedures followed



Responding to new kind of threats



- Personality vs learning
- Love to work across silos
- Love complexity – find simplicity
- Don’t think like IT profs
- Do it because they find it fun

Cyber-MAR Impacts

Short Term

1. Response time metrics, including mean time to incident discovery and mean time to patch improved by at least 5%.
2. Cyber-MAR platform is security-vendor agnostic
3. Increased interconnection and interoperability
4. Standardisation and dissemination to the CSIRTs network
5. Use of available historical data (evidence-based) of cyber-security attacks and data privacy breaches
6. Econometric model for quantifying the impact from cyber-attack of ports.
7. Flexible hybrid solution for mixing virtual and physical (real) IT components of an organisation and assessing their joint/integrated response and resilience to cyber-attacks and privacy breaches

Cyber-MAR Target Markets/Stakeholders

1. Decision Makers / Public Authorities
2. Port Authorities / Shipping operators / Freight transport / Logistics actors
3. CERT/CSIRTs network
4. European and international organizations for cyber security
5. Insurance companies
6. Academic and scientific actors
7. EU Cyber security Projects

Cyber-security in the new era

CYMOTIVE TECHNOLOGIES

Assets	Data	People & Environment
Threats	Availability Confidentiality Integrity	Resilience Privacy Safety
Goal	Liability	Growth
Orientation	Compliance	Trust
Approach	Reactive (preventive)	Proactive (event driven)
Players	Local	Across lines of Business
Change	Technology	Process/Culture Change

Cyber-MAR Objectives

O1. Enhance capabilities of cybersecurity professionals and raise awareness on cyber-risks

O2. Assess cyber-risks for operational technologies (OT)

O3. Quantify the economic impact of cyber-attacks across different industries with a focus on port disruption

O4. Promote cyber-insurance market maturity in the maritime logistics sector (adaptable to other transport sectors as well)

O5. Establish and extend CERTs/CSIRTs, competent authorities and relevant actors collaboration and engagement

Cyber-MAR Facts & Figures

Name: **Cyber** preparedness actions for a holistic approach and awareness raising in the **MAR**itime logistics supply

Project ID: 833389

Funded under: H2020

Funding scheme: IA - Innovation action

Duration: From 2019-09-01 to 2022-08-31,

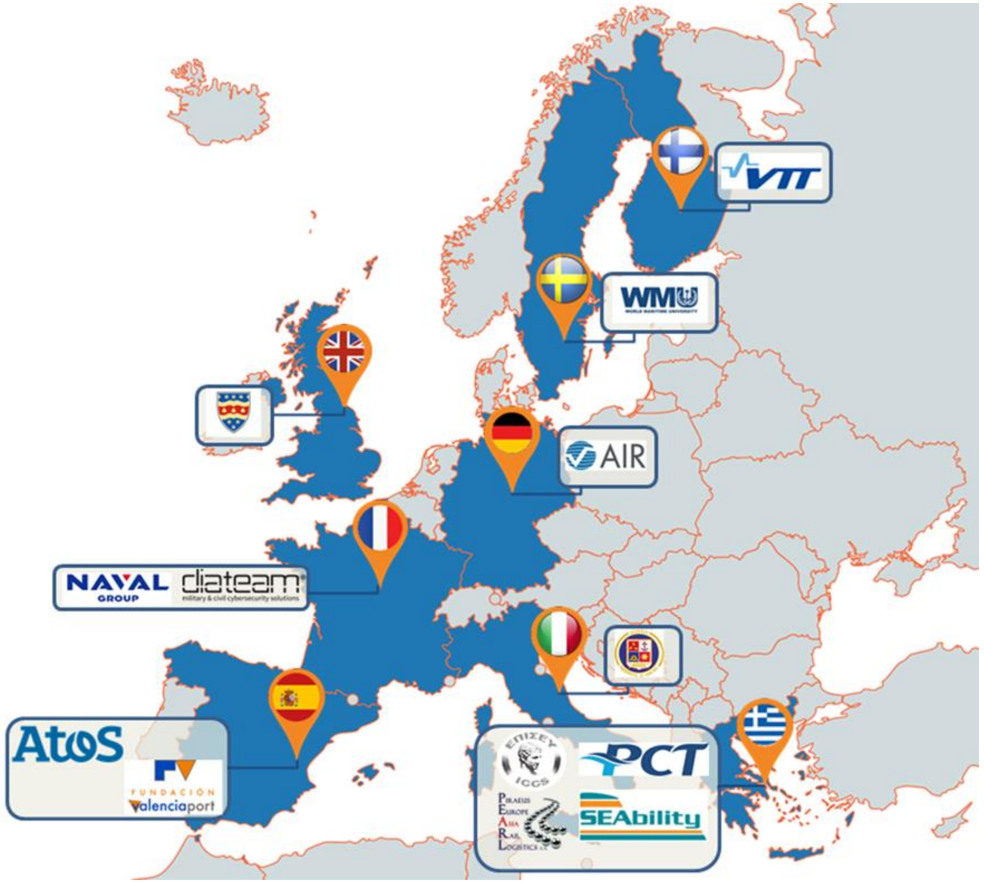
Total cost: EUR 7 154 505.00

EU contribution: EUR 6 018 367.507

Call for proposal: H2020-SU-DS-2018

Topic: SU-DS01-2018 – Cybersecurity preparedness-cyber range, simulation and economics

Coordinated by: Institute of Communication and Computer Systems (ICCS), Greece



Cyber MAR

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

i-SENSE GROUP

ΕΠΙΣΕΥ ICCS

Giannis Karaseitanidis

✉ gkara@iccs.gr

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389