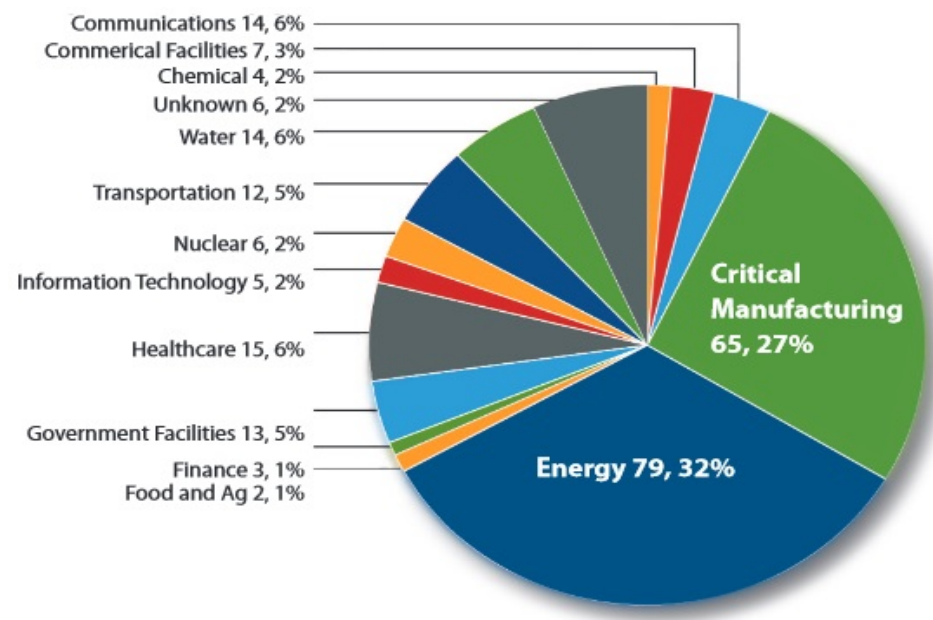
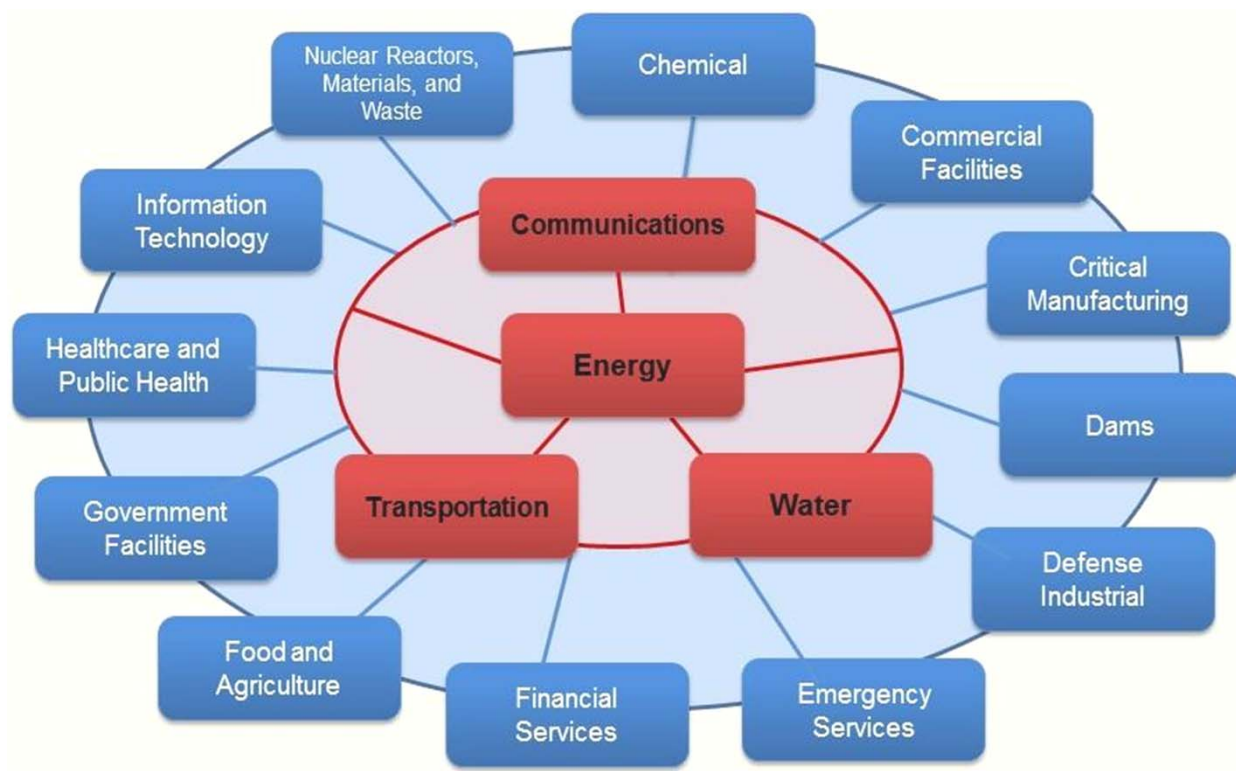


Cyber and Physical Security management

1st ECSCI Workshop on Critical Infrastructure Protection
Virtual workshop
24-25 June 2020

Prof. Theodore Zahariadis
University of Athens
Technical Manager of H2020 DEFENDER

Critical Infrastructures (CI)



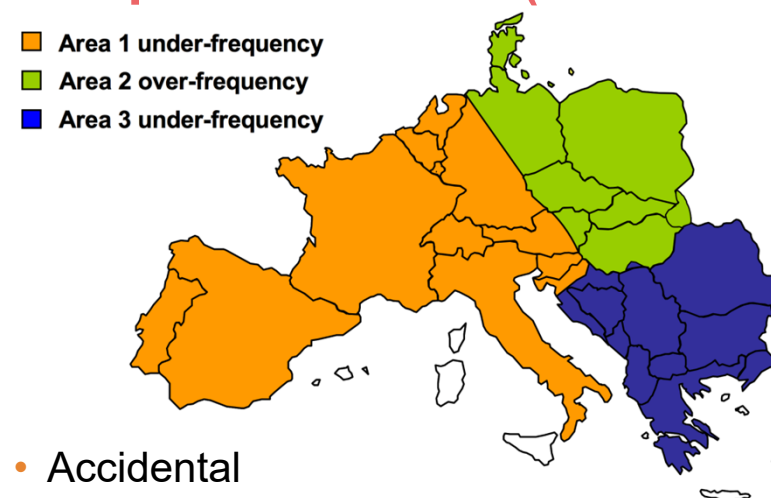
Examples of incidents on CEI

Ukrainian grid cyber attack (Dec. 2015)

1. Compromise of corporate networks via emails infected with phishing malware (**at least 6 months!**)
2. Took **SCADA control**, then remotely switching off 43 substations
3. Disabled **IT infrastructure components**
4. Destructed of files stored on servers and workstations with the **KillDisk** malware
5. Denial-of-service **attack on call centres** to deny consumers updating on the blackout.

Orchestrated ICT threats can lead to more complex and sophisticated threats targeting at core CEI operations

European blackout (Nov. 2006)



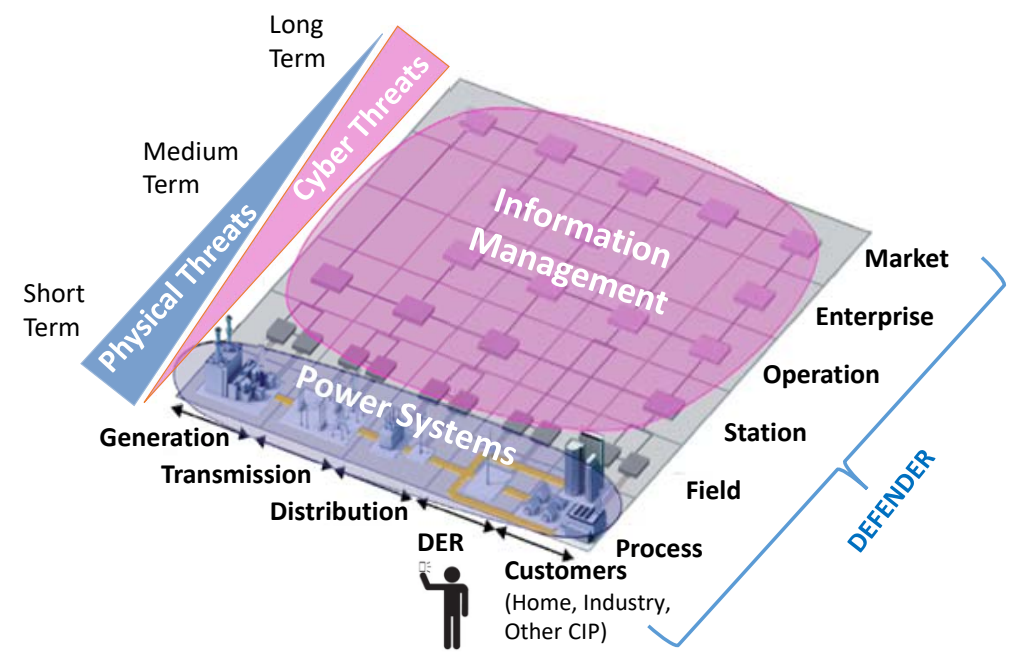
- Accidental
- Non fulfilment the N-1 criterion
- Insufficient inter-TSO co-ordination

Accidents may be as catastrophic as attacks

CEI Protection Scope

CEI covers the complete value chain

- From Generation to Consumption
- From Process to Market



Physical Security



National Disasters



Aging Infrastructure



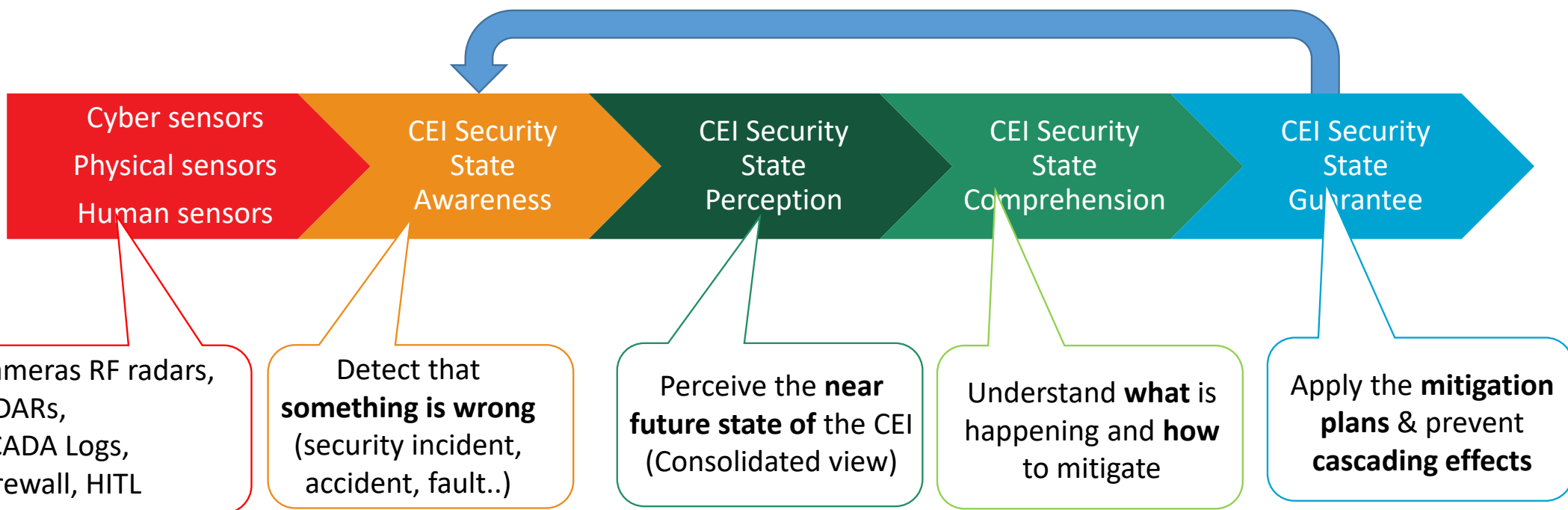
Cyber Security



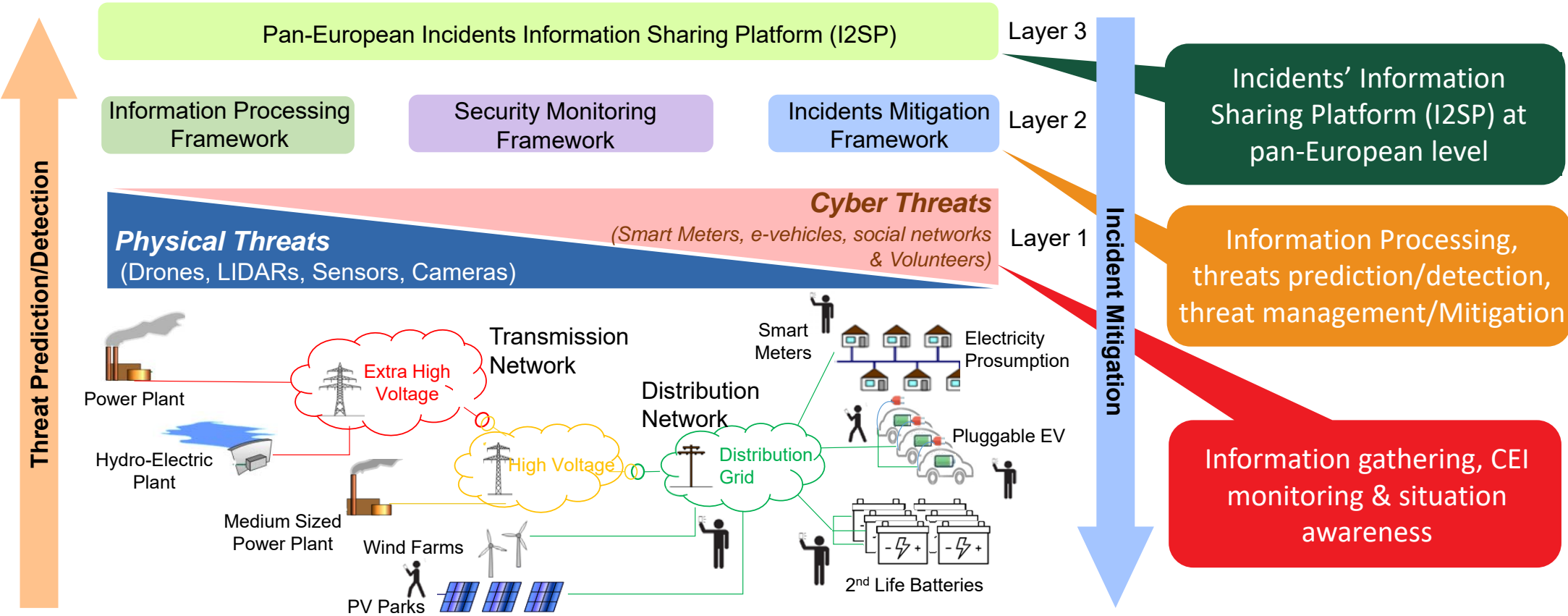
Aging Workforce

From Monitoring to CEI Security Guarantee

Feedback & Full Lifecycle Governance



CEI Security Protection System



CEI Security Monitoring “Musts”

Builds on real-time multi-aspect monitoring to ensure that:

- ✓ CEI security state is known at every given moment
- ✓ The future CEI security state is predictable
- ✓ The CEI security guaranteed at all times

Physical

- Thermal/PMZ cameras, RF radars, LIDARs
- Fibre optics, Taut wires, Buried geophones

Cyber

- Logs, Firewall status, SCADA systems
- CPSS and Machine Learning at local and pan-European level

Human

- Acting as first-responders on possibly CEI incidents



(a) Surveillance Camera



(b) Laser Fence Sensor (LFS)



(c) 360° Perimeter Laser Sensor



(d) Efficient Doppler detector



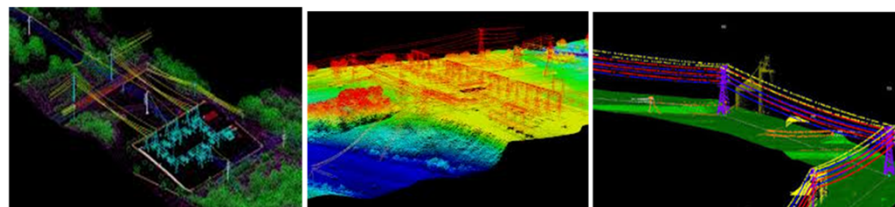
(e) Wireless seismic & IR sensor



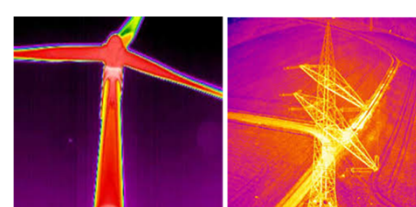
(f) Laser Radar Sensor (LRS)



(a) Thermal Camera



(b) LIDAR images of Critical Energy generation, transmission and distribution networks



Maintenance acceleration

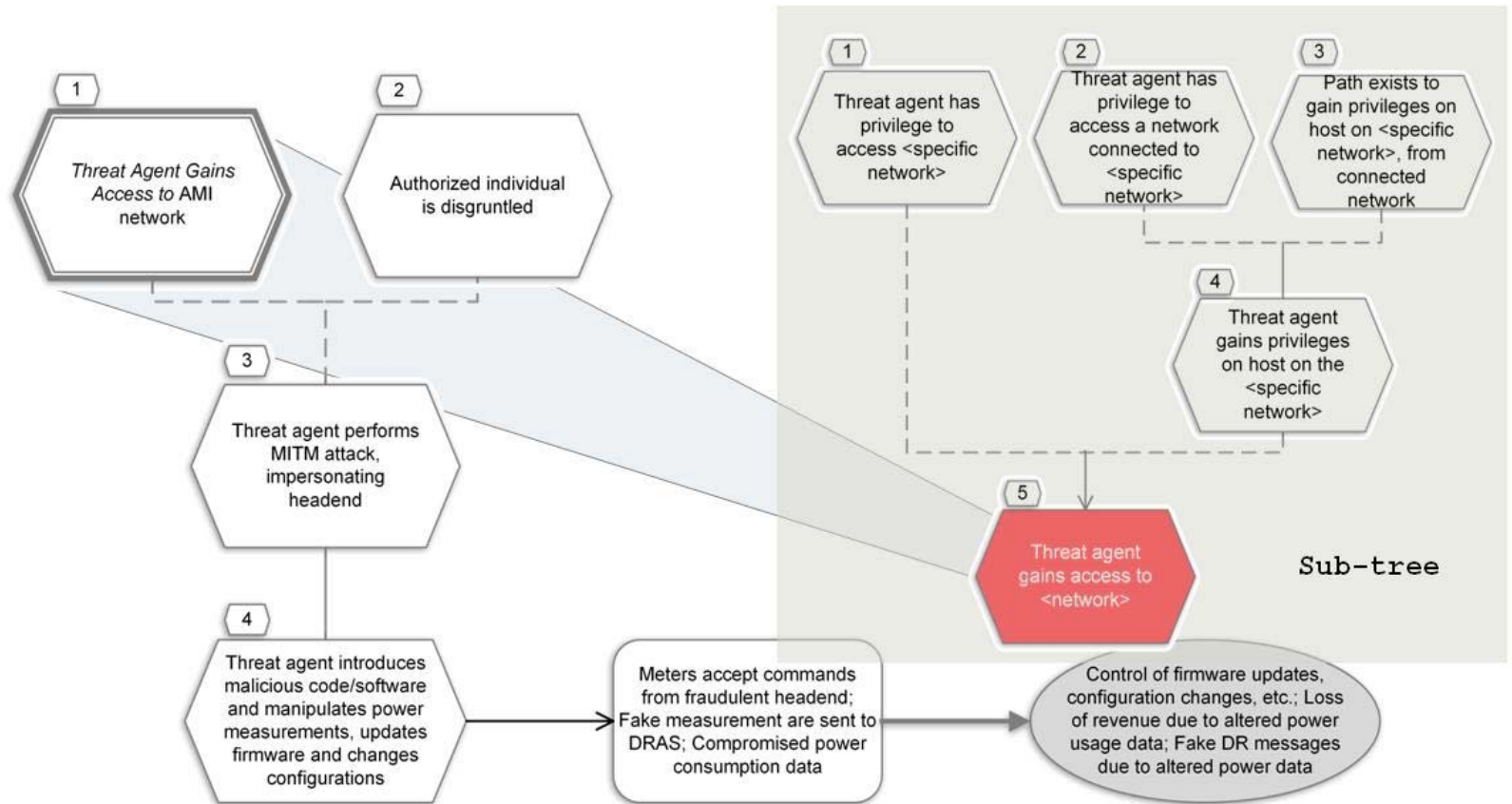


Drone Visual Detection

CEI Security Monitoring “Musts”

From CEI security state Awareness to Comprehension

- Threats and attack vectors are **semantically enriched**
- Extensive use and integration of:
 - Near real time monitoring
 - **Data mining** on logs
 - **Machine learning**
 - Full-stack Apache Spark, Apache Zeppelin
- Security comprehensive

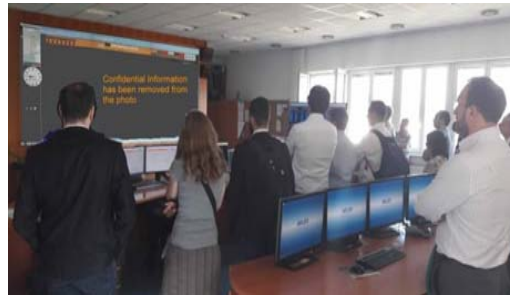


CEI Security Monitoring “Musts”

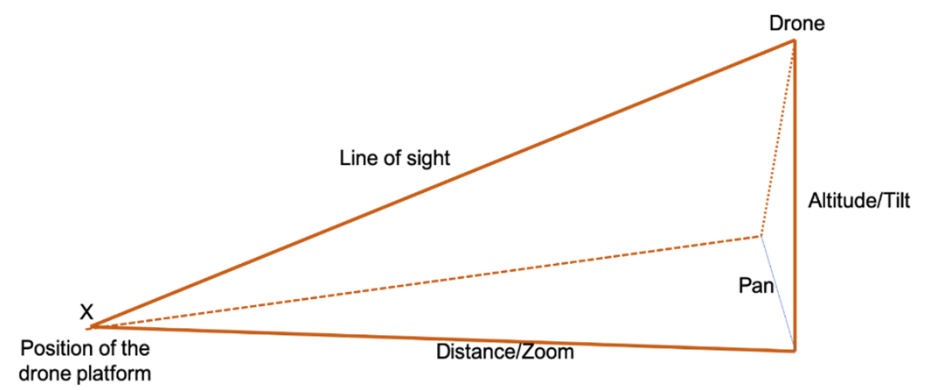
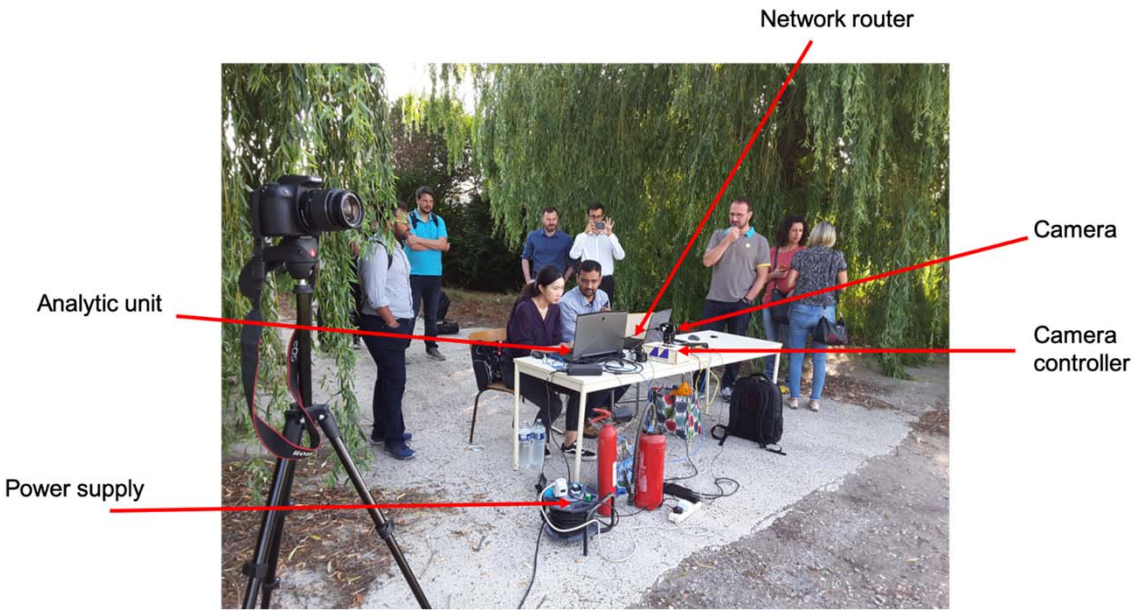
CEI Security Guarantee



- **CEI Security “by-design”**
 - Resilience (e.g. Double virtualization)
 - Self-healing (e.g. fault-location /restoration)
 - Data Protection (e.g. Cryptography/Blockchains)
- **CEI Security “by innovation”**
 - Countermeasures toolbox for incident mitigation
 - Decision support systems to assist CEI security authorities when automated mitigation is not possible
 - Avoidance of cascading attacks by notification & “Human Sensors”



Drones locking



CEI Security Monitoring “Musts”

HITL acting as cyber security sensors

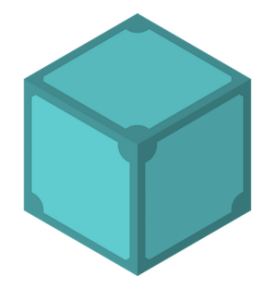
- Volunteers or LEAs acting as first responders (report via specialized applications possibly accidents or suspicious incidents)

- Short messages
- Photographs
- Videos



We need to ensure

**Trusted, Traceable, Private,
Bi-directional Communications**

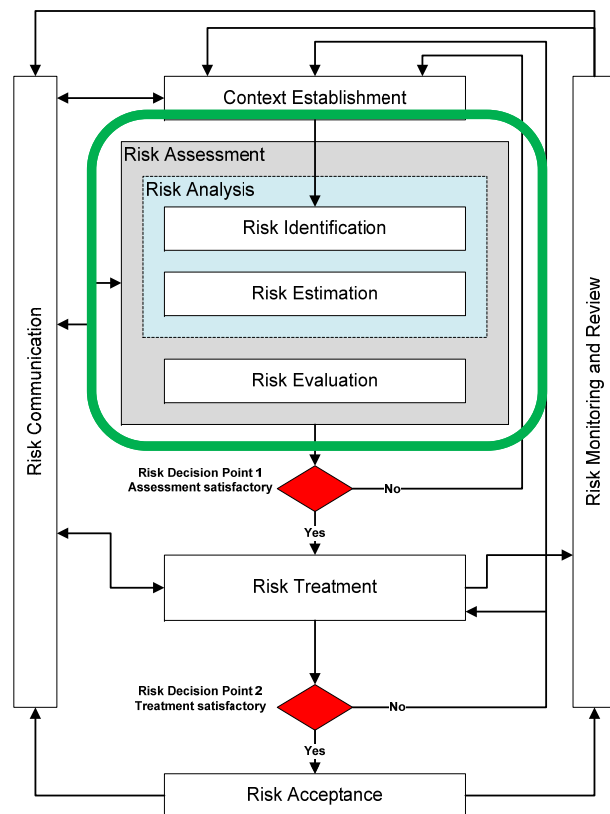


Ethereum as Consortium **blockchain**

IPFS distributed, encrypted file system

End-to-end encryption

CEI Secure Tiers Classification



Risk Management Process - ISO/IEC 27005

Risk Assessment consists of

- Risk Analysis partitioned into
 - Risk Identification
 - Risk Estimation
- Risk Evaluation

The outcome of the Risk Assessment Process is a set of prioritized risks. The next step is to suggest a Risk Treatment set of measures to the Operator.


CEI Secure Tiers Classification

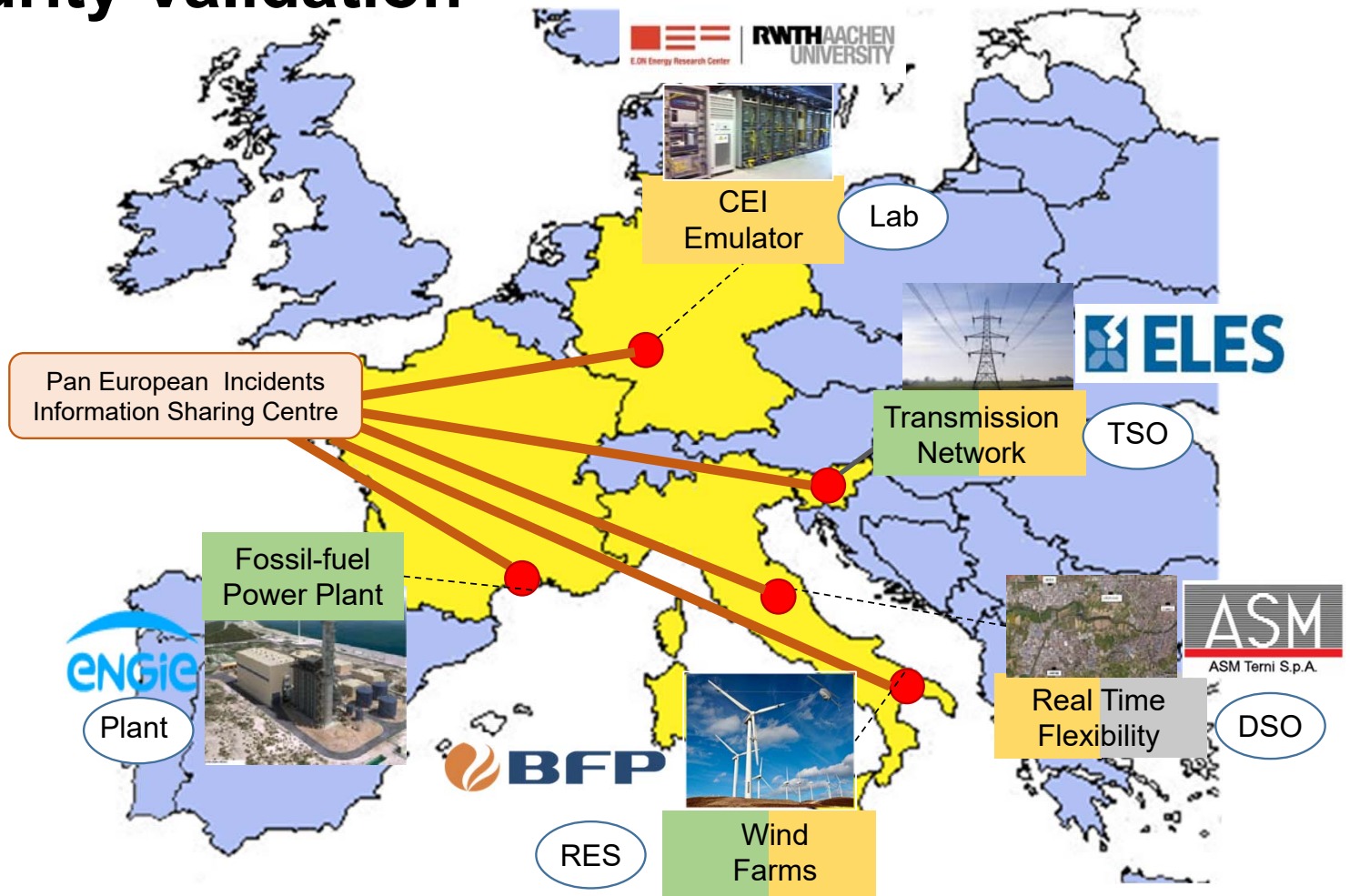
4 Security tiers are created for Risk Evaluation

- Minimal importance, green, 1 to 3, leave out
- Small importance, yellow, 4 to 6, monitor and re-evaluate
- Medium importance, orange, 8 to 12, schedule a mitigation plan
- High importance, red, 15 to 25, immediate attention and mitigation plan

Risk Rating Matrix		Risk Impact				
		Minimal	Small	Medium	High	Severe
Risk Likelihood	Almost certain	5	10	15	20	25
	Likely	4	8	12	16	20
	Possible	3	6	9	12	15
	Unlikely	2	4	6	8	10
	Rare	1	2	3	4	5

CEI Security Validation

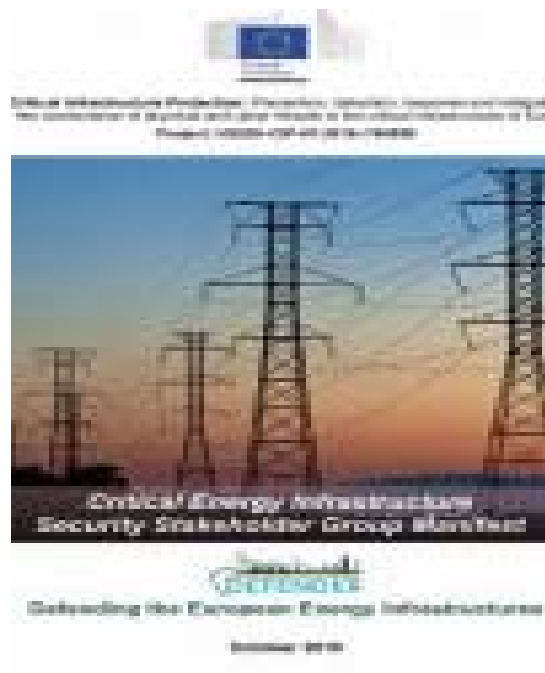
- Physical Protection
- Cyber Protection
- Human in the Loop
-  Smart Meters



Publicity & Stakeholders are critical



CEI Security Stakeholders Group (CEIS-SG)



<https://defender-project.eu/ceis-sg/>

Conclusions

- Critical Energy Infrastructure (CEI) threats include:
 - Cyber-Physical Security
 - Natural Disasters
 - Aging Infrastructure – Aging Workforce
- From Monitoring to CEI Security Guarantee, state awareness and comprehension play a significant role.
 - Sharing data is quite problematic
- Risk Rate may be evaluated as Risk Impact X Risk Likelihood
- CEI Security Roadmap should
 - Identify the major threats
 - Rate them
 - Define countermeasures

Thank you!