LABORATORIO VIRTUALE CYBER SECURITY (LV-CS)

TOWARDS A TRUSTWORTHY DIGITAL TRANSITION

FABIO MARTINELLI

Consiglio Nazionale delle Ricerche

Sommario

- La cybersecurity come area di interesse primario in Europa ed in Italia
- Il LV Cyber del CNR
- Le attivita' progettuali del LV Cyber

Notizie

EDIZIONI LOCALI | CORRIERE TV | ARCHIVIO | TROVOCASA | TROVOLAVORO | SERVIZI

DDOS

Il cyber attacco contro Internet negli Usa partito dalle case «intelligen

L'attacco è arrivato da oggetti «smart»: videoregistratori, frigoriferi, telecam sicurezza, router e sistemi per il controllo dei neonati. Wikileaks rivendica

https://edition.cnn.com/2021/05/13/business/gas-shortage-colonial-pipeline/index.html

CNN BUSINESS Markets Tech Media Success Perspectives Videos Edition

MARKETS			see all →
DOW	33.751,10	+189,59	+0,56%
S&P 500	4.092,59	+32,37	+0,80%
NASDAQ	13.178,41	+146,34	+1,12%

FEATURED

Crypto 101
Everything you need to know about bitcoin, blockchain, NFTs and more.

LATEST

Alibaba's sales surge but cloud growth slows
Colonial Pipeline is restarting but the gas crisis isn't o
What's happening at US gas stations

Colonial Pipeline is restarting but the gas crisis isn't over

By Matt Egan, CNN Business
Updated 1246 GMT (2046 HKT) May 13, 2021

2020: The Year the COVID-19 C

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-br

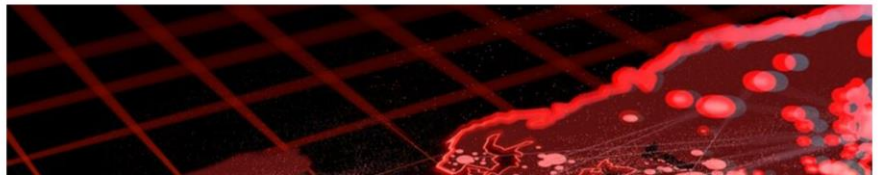
Analytics

LOHRMANN ON CYBERSECURITY & INFRASTRUCTURE

2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic

2020 will be remembered as a uniquely disruptive year — but not just for a global health crisis. Online life was digitally transformed, as exponential change accelerated at home and work via cyberspace.

BY DAN LOHRMANN / DECEMBER 12, 2020



ANSA.it › Motori › Attualità

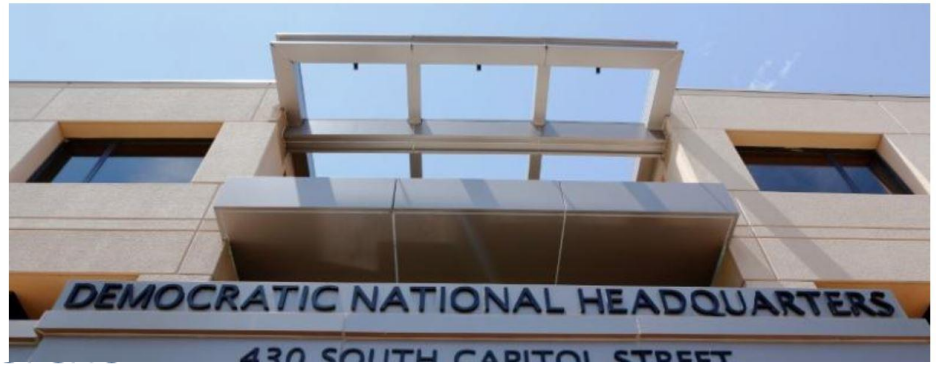
Ad General Motors, 'cyber auto minaccia crescente'

Problema per tutti, serve collaborazione tra case'

Redazione ANSA 25 LUGLIO 2016 14:03

POLITICS | Sat Oct 8, 2016 | 6:48am EDT

U.S. formally accuses Russian hackers of political cyber attacks



FINANCIAL TIME

COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Warfare + Add to myFT

inese hackers targeted US aircraft carrier

r security group says attack launched against visitors to vessel uth China Sea

Rilevanza scientifica / politica

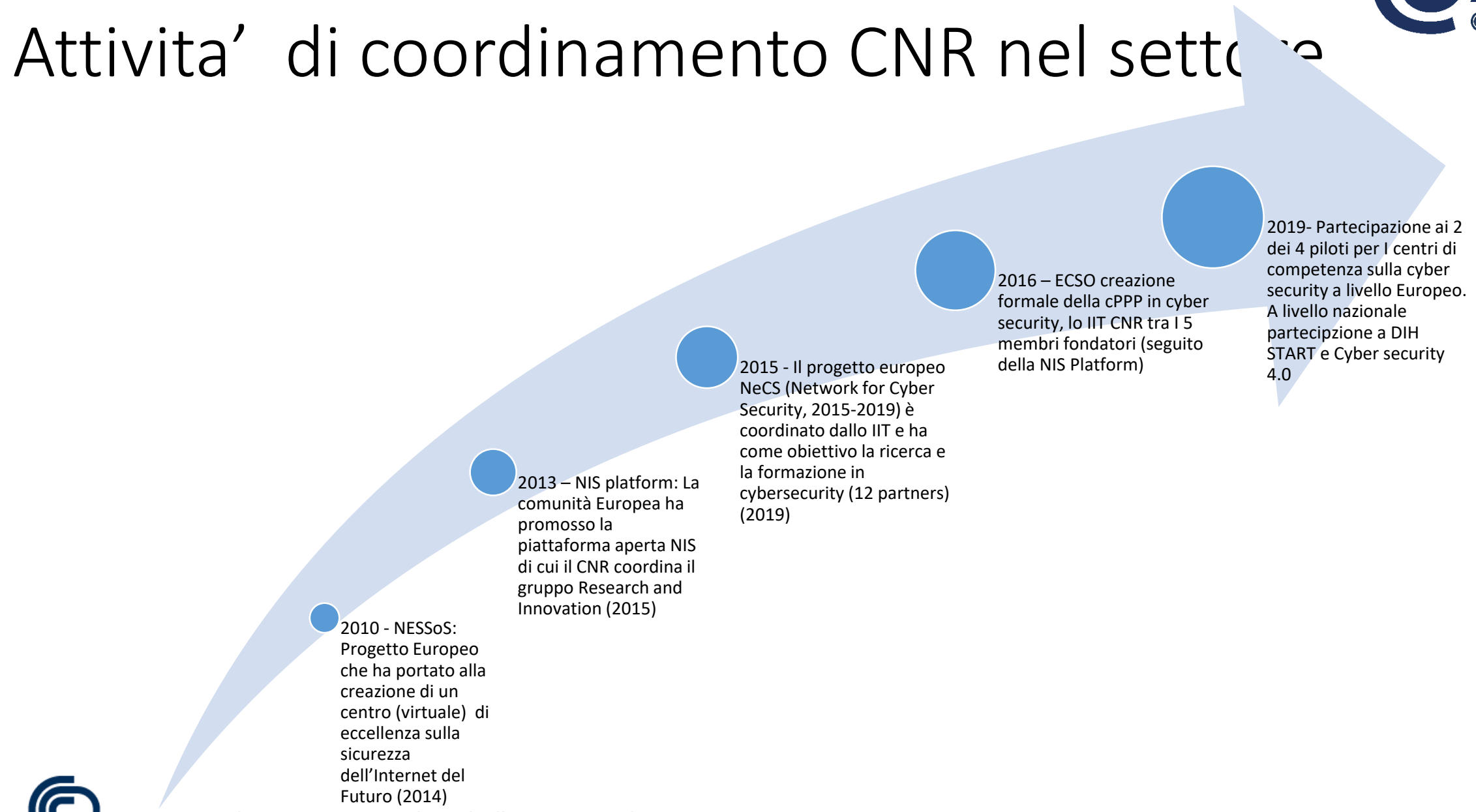
Lo Scientific Advise Mechanism (SAM) della Commissione Europea ha identificato la cyber security tra i primi due argomenti di azione.

“Cybersecurity is no longer a technological ‘option’, but a societal need”

Il ruolo rilevante del CNR in Europa negli ultimi 10 anni

- Il CNR ha coordinato due reti di eccellenza per quasi una decade (2010-2019)
- Il CNR ha coordinato il gruppo di lavoro 3 della piattaforma tecnologica NIS nel 2013 co-editando la prima strategic research agenda nel settore
  - La piattaforma ha contribuito per la parte tecnica alla prima direttiva europea nel settore (NIS directive)
- Il CNR ha contribuito alla creazione (tra i 5 fondatori, unico RTO/academia) della cPPP ECSO in cyber security nel 2016 che ha raddoppiato il budget disponibile per la cyber in H2020
  - ECSO ha anche un ruolo nella nuova strategia Europea del 16 dic. 2020.
- Il CNR attualmente ha il ruolo di vice-chairman di ECSO in rappresentanza di tutti gli RTO/Accademia (ECSO ha 260 organizzazioni ora al suo interno)
- Il CNR e' in due dei quattro progetti Pilota Europei per centri di competenza (SPARTA e CS4EU)
- Il CNR partecipa al Comitato Nazionale per la ricerca in Cyber security con CINI e CNIT (firmato in sede CNR nel 2017) e promuove la Cybersecurity Made in EU label
- Nel centro di competenza nazionale Cyber 4.0 e START 4.0 (a guida CNR)

Attivita’ di coordinamento CNR nel settore



Direttiva e piattaforma NIS (Network and Information Security)

La direttiva sulla Network and Information Security (NIS) e' stata approvata il 6 luglio 2016 e richiede che gli stati membri la mettano in opera entro il 2018. L'iniziativa legislativa e' nata nel 2013

- Anche per supportare lo sviluppo della normative, una piattaforma tecnologica (NIS platform) e' stata creata per:
  - Comprendere meglio le sfide inerenti la NIS
  - Mettere insieme esperti tecnici e legali per definire le sfide presenti e future ed in particolare per influenzare le attivita; di ricerca ed innovazione su NIS To influence future R&D in NIS issues

- Tre gruppi di lavoro sono stati creati, due per definire le regole operative uno per le sfide della ricerca.
  - **Come CNR abbiamo coordinato il grupp di lavoro (WG3) su R&D che ha prodotto la prima Strategic Research Agenda nel settore**


CYBERSECURITY STRATEGIC RESEARCH AGENDA – SRA

Produced by the
European Network and Information Security (NIS) Platform

Final version v0.96
Last modified: August 2015

Editors:

Pascal Bisson (Thales), Fabio Martinelli (CNR) and Raúl Riesco Granadino (INCIBE)

Contractual Public/Private/Partnership (cPPP in cyber security) ECSO ed il contributo del CNR

Scopo

1. Stimolare la cooperazione tra gli attori pubblici e privati
2. Stimolare l'industria Europea per la cyber security

BUDGET

La comunita' Europea ha investito €450ME in questa partnership, sotto il programma di ricerca e sviluppo Horizon 2020 tra il 2017-2020 (rispetto ai 200ME precedenti). Gli attori privati devono mostrare investimenti per € 1350 mln per un totale €1800 mln.

MEMBRI

Circa 260 tra le industrie, gli enti di ricerca, le universita' e le pubbliche amministrazioni in Europa. Tutti I maggiori attori sono presenti.

Il CNR e' stato tra I 5 cofondatori nel 2016 di questa iniziativa e attualmente rappresenta nel Board tutti i 70 RTO e universita' (quindi un ruolo riconosciuto di leadership)

Centro di competenza Europeo in cyber security (ECCC)

- Cyber security act (2017)
- Centro di competenza europeo sulla Cyber Security, con una serie di centri di coordinamento nazionale ed una comunita' di organizzazioni
- CNR e' in 2 dei 4piloti (SPARTA e Cybersec4EU) 16ME / 44 partners
  - Questa azione e' stata coordinate dalla AP/Cyber Lab
- Il Centro di competenza Europeo sara' a Bucarest
- Ogni nazione deve creare il centro di competenza nazionale

Motivazioni ed obiettivi del Lab

- **Facilitare la partecipazione a progetti nazionali ed internazionali**

- Contribuire alla sicurezza del sistema paese collaborando con tutti gli attori
  - Favorire rapporti con Istituzioni, enti governativi, industrie, PMI, accademia

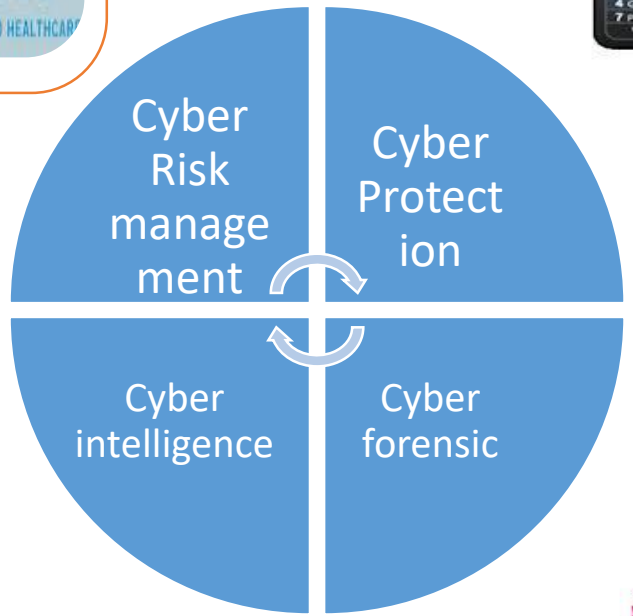
- Consolidare ed estendere negli anni futuri il ruolo del CNR nel settore continuando ad investire su cooperazioni strategiche

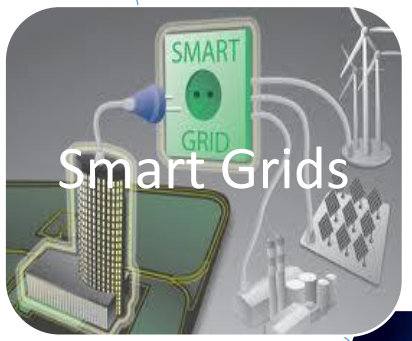
- Promuovere la crescita e la formazione di personale

- Cooperazione internazionale
  - ECSO; ERCIM; IFIP; EDA
- Attivita di disseminazione e formazione
  - Inclusi eventi, corsi specialistici….

LV-CS Cyber Security

- Ricercatori di vari Istituti/sedi coinvolti:
  - IAC – Napoli
  - IAC – Roma
  - ICAR – Cosenza
  - ICAR - Napoli
  - IEIIT – Torino
  - IEIIT – Genova
  - IIT
  - IMATI – Genova
  - IMATI – Milano
  - INO - Firenze
  - IRCRES – Torino
  - ISTC – Roma
  - ISTI
  - ITAE - Messina
  - …

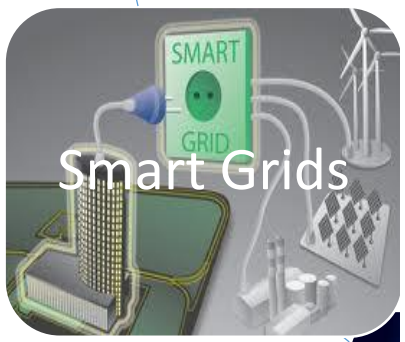




Aree tematiche del Lab of CNR

3 progetti Europei coordinati dal CNR (in rosso) dal 2020.

Quantum is coming!!!



Meetings

- Come core AP cyber abbiamo avuto eventi regolari negli ultimi anni (e ci siamo strutturati come centro di “competenza” gia’ nel 2017)
- Come LV cyber abbiamo tenuto un meeting in Febbraio
- **Questo pomeriggio di oggi avremo altro incontro con stakeholders esterni e con ricercatori di altri Istituti che si sono uniti piu’ recentemente al Lab**
- Abbiamo pianificato un meeting per il 14/15 Giugno favorire la cooperazione scientifica e progettuale (invito seguira’ a breve)

Meeting del Laboratorio Virtuale (LV) di CyberSecurity

Data: 14 Maggio 2021
Virtual: Microsoft Teams meeting
Click here to join the meeting

14.00-15.30 Tavola rotonda sugli aspetti di cyber security nelle aree ICT, Ingegneria e Energia e Trasporti, il punto di vista di alcuni stakeholders.

- Moderatore: Fabio Martinelli - IIT
- Speakers:
  - Sandro Mari (MISE)
  - Guido Ancarani (Distretto Tecnologico Ferroviario – DITECFER)
  - Matteo Lucchetti (Centro di Competenza Cyber 4.0)
  - Paolo Roccetti (ENGINEERING)
  - Domenico Sacca (Unical e Relatech)
  - Giovanni Tusa (BaxEnergy)

15.30-16.45 Alcune aree di ricerca in cyber security presentate da esperti del LV Cyber:

- Moderatore: Eda Marchetti – ISTI
- Speakers:
  - Gianpiero Costantino – IIT (Cybersecurity per il settore **Automotive**)
  - Ugo Finardi – IRCRES (Persone, denaro e regole: uno sguardo **socioeconomico** sulla cybersecurity)
  - Andrea Orlandini – ISTC (**Robotica** e resilienza)
  - Giovanni Schmid – ICAR (**Blockchain:** sfide ed opportunità)
  - Francesco Sergi – ITAE (Aspetti di cyber security e sistema **energetico**)
  - Andrea Zavatta – INO (Secure **quantum** communication)

16.45 Chiusura dei lavori

Attivita’ flagship del LV Cyber

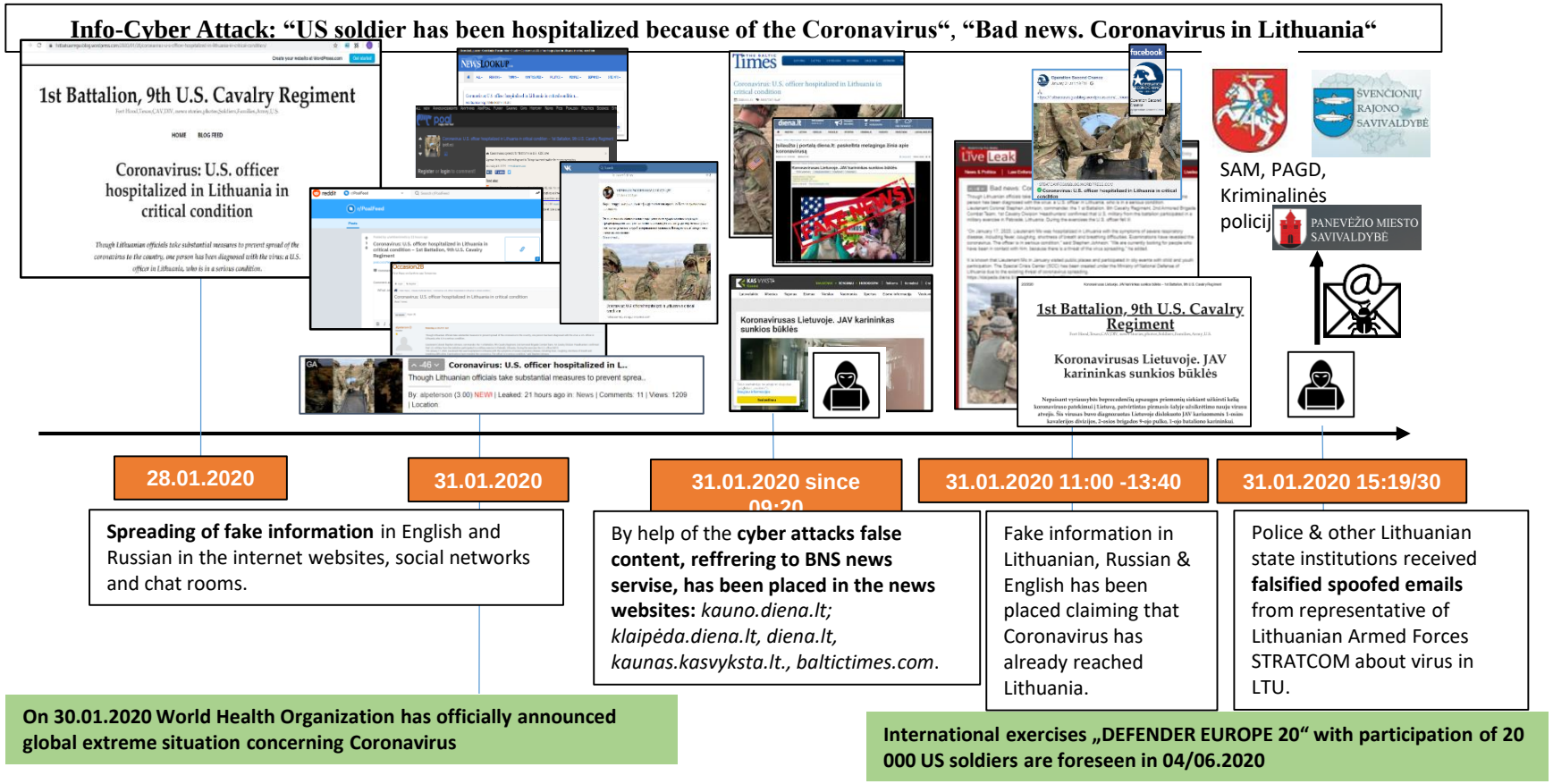
- Full Spectrum Cyber Security Observatory
- Social impact of Distributed Ledger Technologies
- Secure Critical National Infrastructures

Activity:
CyberSecurity osservatorio
full spectrum situation awareness

Main concept

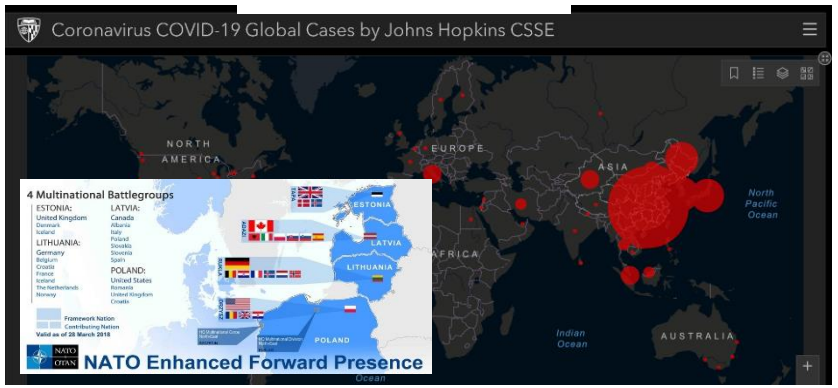
- Use the experience and competence of the Cyber Lab of CNR to :
  - Monitor cyber and physical treats in a unique HUB:
    - Network
    - Systems
    - Social media
    - IoT
    - Critical infrastructures (Cloud, Energy, Transport, …)
    - ….
  - Link virtual world and physical one
    - **Cyber attacks + Information attacks = full spectrum**
  - Offering actual services to the wider community, improving collaborative situation awareness
    - With special emphasis to cyber security in transport section

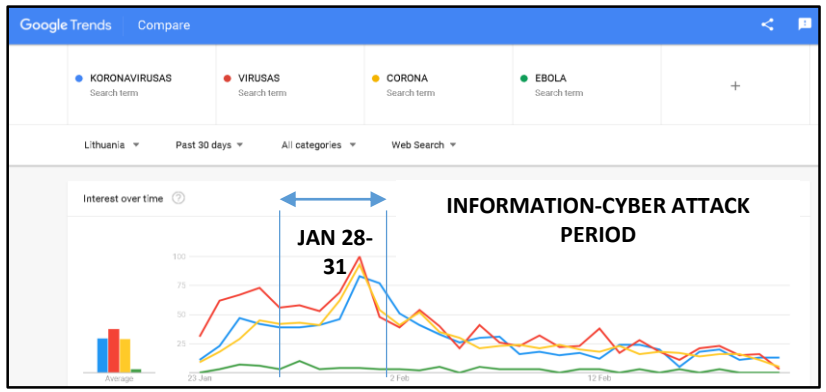
Example – cyber – physical virus interaction



Full spectrum situation awareness

STRATEGIC EVENTS

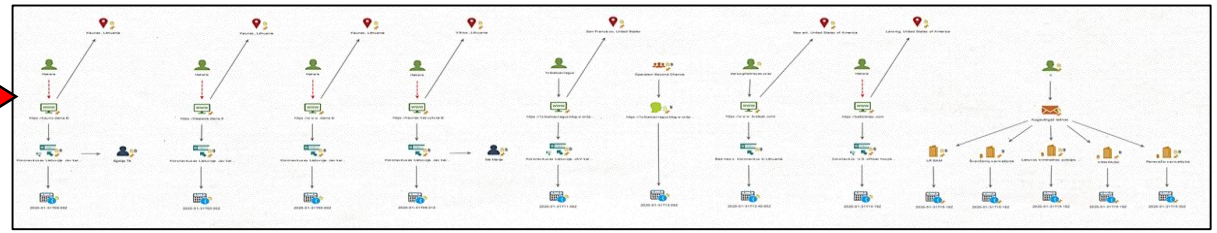




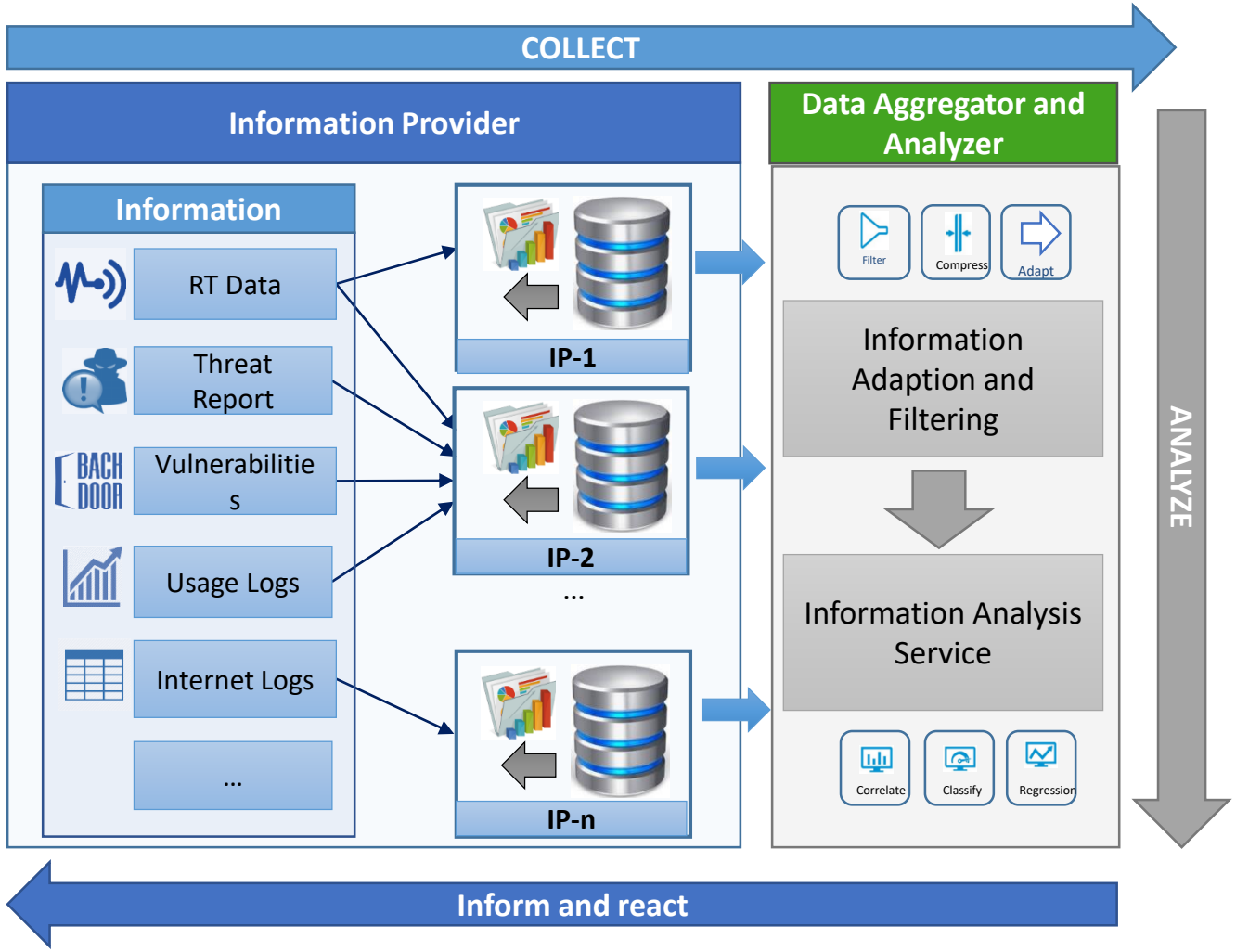
FAKE NEWS SAMPLE

INFORMATION-CYBER ATTACK VECTOR

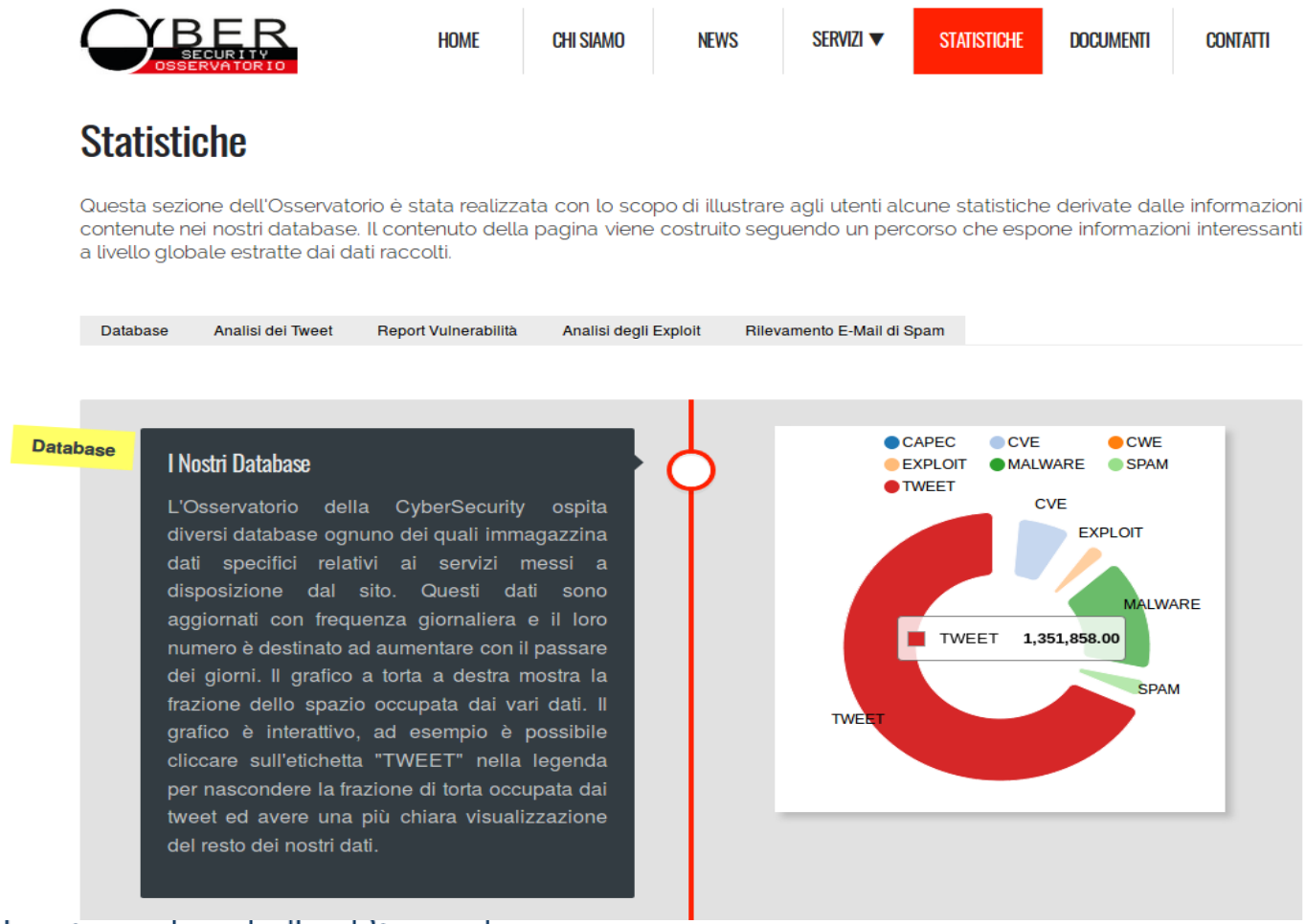
CYBER ATTACKS (DEFACEMENT WITH FAKE CONTENT OF MEDIA WEBSITES)
FAKE CONTENT DISSEMINATED/SHARED OVER SOCIAL NETWORKS AND WEBSITES
FAKE CONTENT DISSEMINATED WITH SPOOFED EMAILS TO GOV ORGANISATIONS



Collection of multiple sources



Cybersecurityosservatorio.it



Consiglio Nazionale delle Ricerche

Current services

1. Thesaurus e ontologia per la cyber security
2. Strumenti per il self assessment
3. Scansione di vulnerabilità
4. Strumenti per il GDPR
5. Analisi Social Bot
6. Analisi di vulnerabilità (CVE & Exploit)
7. Analisi email
8. Rilevamento di Domain Generation Algorithm (DGA)
9. Antimalware
10. Rilevamento Ransomware
11. Rilevamento e analisi di Mirai botnet
12. Visualizzazione 3D Attacchi
13. Analitiche generiche (distribuzione spazio/temporale)
14. Fake news
15. Fake accounts
16. Analysis of access policies
17. …

Self assessment tools

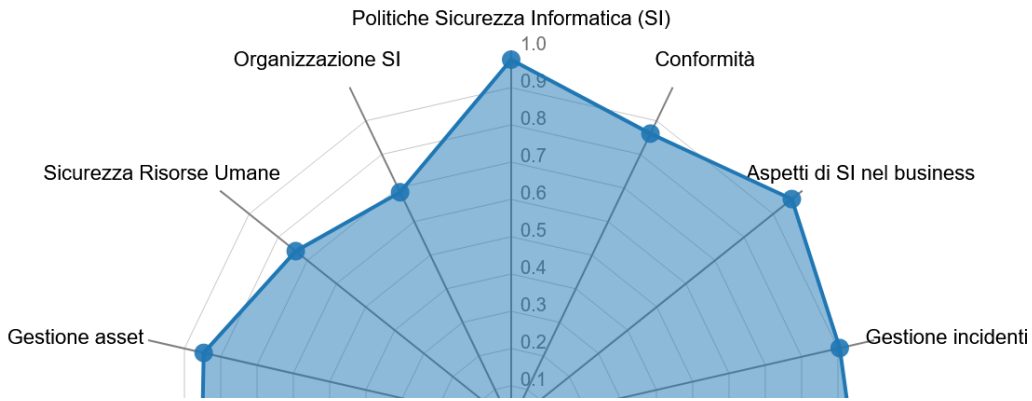
CYBER SECURITY OSSERVATORIO

HOME | CHI SIAMO | NEWS | SERVIZI ▼ | STATISTICHE | DOCUMENTI | CONTATTI

Calcolo Rischio

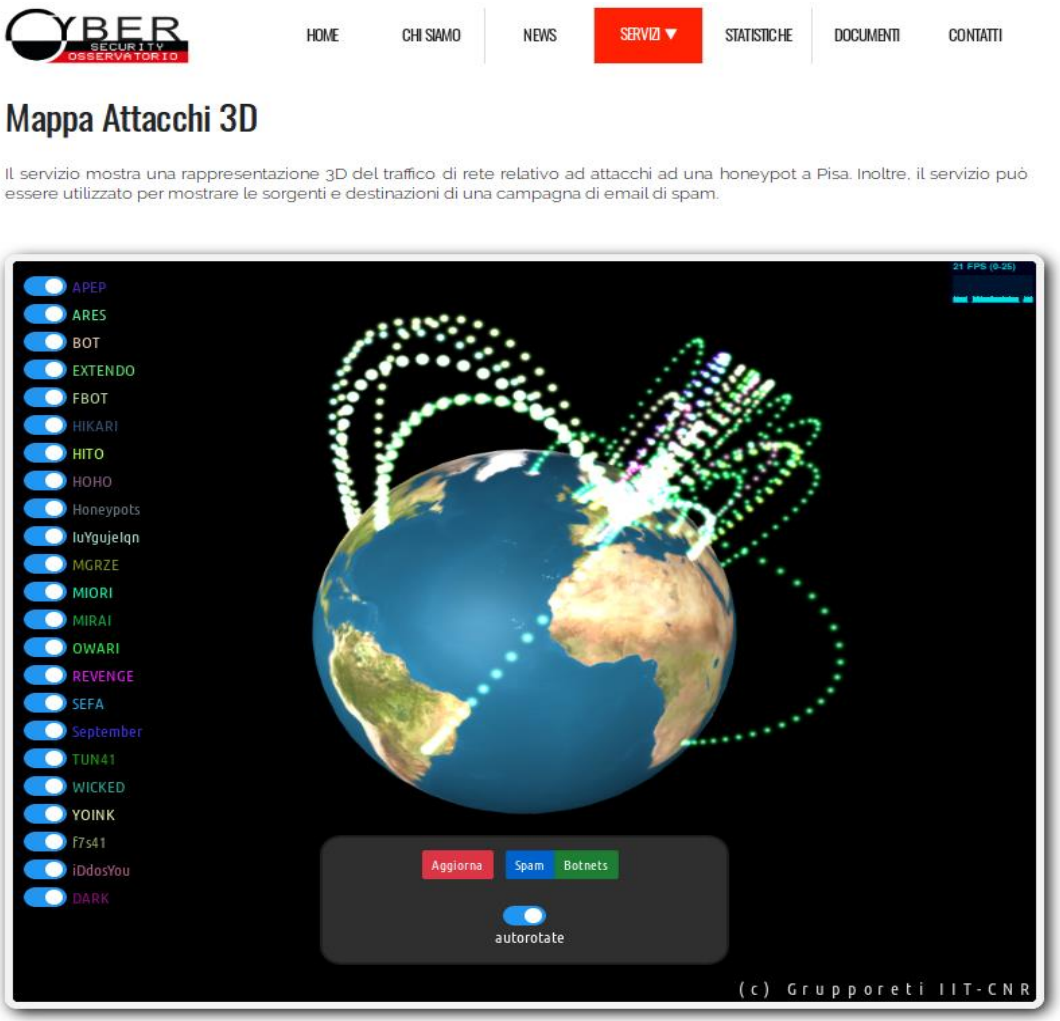
Il radar chart mostra quanto la tua organizzazione conforme rispetto alcune categorie di rischio della cybersecurity. La tabella mostra l'analisi del rischio della cybersecurity.

Calcolo Rischio



Consiglio Nazionale delle Ricerche

3D visualization



Supporting projects of this activity

SPARTA

C3T Centro di Competenza in Cybersecurity Toscano

C3ISP
Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

CYBERSANE

E-CORRIDOR
Edge Enabled Privacy & Security Platform For Multi Modal Transport

Flagship activity:

Social Impact of Distributed Ledger Technologies

Ettore Ritacco

Distributed Ledger Technology (DLT)

- **Distributed Ledgers** (DLs) are databases that exist across several locations or among multiple participants

- **Properties**:
  - Decentralization – no need of authorities or intermediaries
  - Replication – any participant owns a synchronized copy of the ledger
  - Consensus – all participants agree on data updates

- **DLs guarantee**:
  - Immutability and incorruptibility
  - Integrity and non-repudiation
  - Transparency

- **Relevant Applications:**
  - Supply chain
  - Digital Rights

Decentralised Ledger

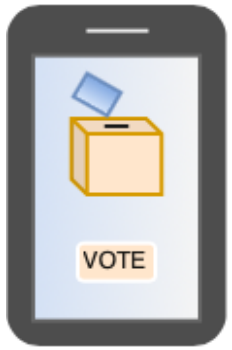
2020 and DLT

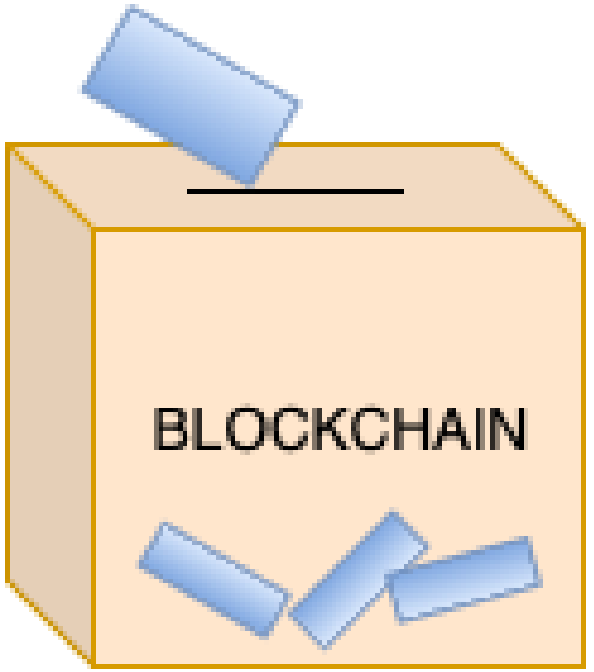
- The emergency arisen in 2020 made the projects deeply change

- Two brand new research themes:
  - E-voting
  - Smart working

E-voting and DLT

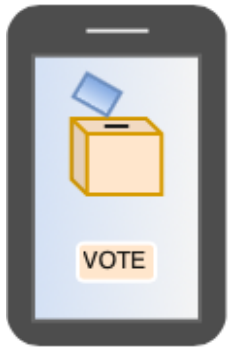
- **Research theme**:
  - Consensus and opinion protection and certification
- **Goals**:
  - Define methodologies, technologies and platform for enabling remote voting “anytime – anywhere”
- **Challenges**:
  - Easy-to-use and robust system
  - Vote confidentiality
  - Citizen anonymity
  - Vote uniqueness
  - Vote immutability
  - Vote coercion
  - Cost

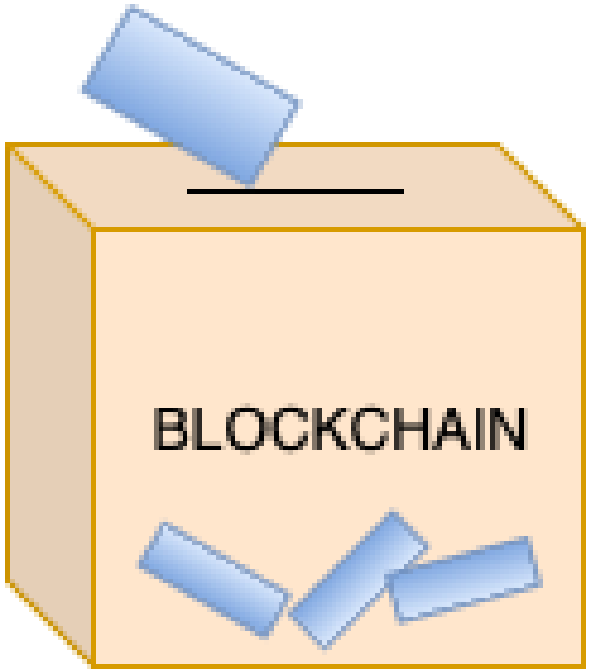




E-voting and DLT

- **Strengths**:
  - Immutable records
  - Transparency with privacy
  - Low cost in the long term
  - Instant results
  - Election adaptability (variable durations, conditions and target groups)
- **Weaknesses**:
  - Implementation
  - Scalability issues
  - Lack of platforms and tools
  - High initial cost
- **Opportunities**:
  - Secure storage and records
  - Once learned, easy for elderly and disabled people
  - Liquid democracy
  - Less bureaucracy



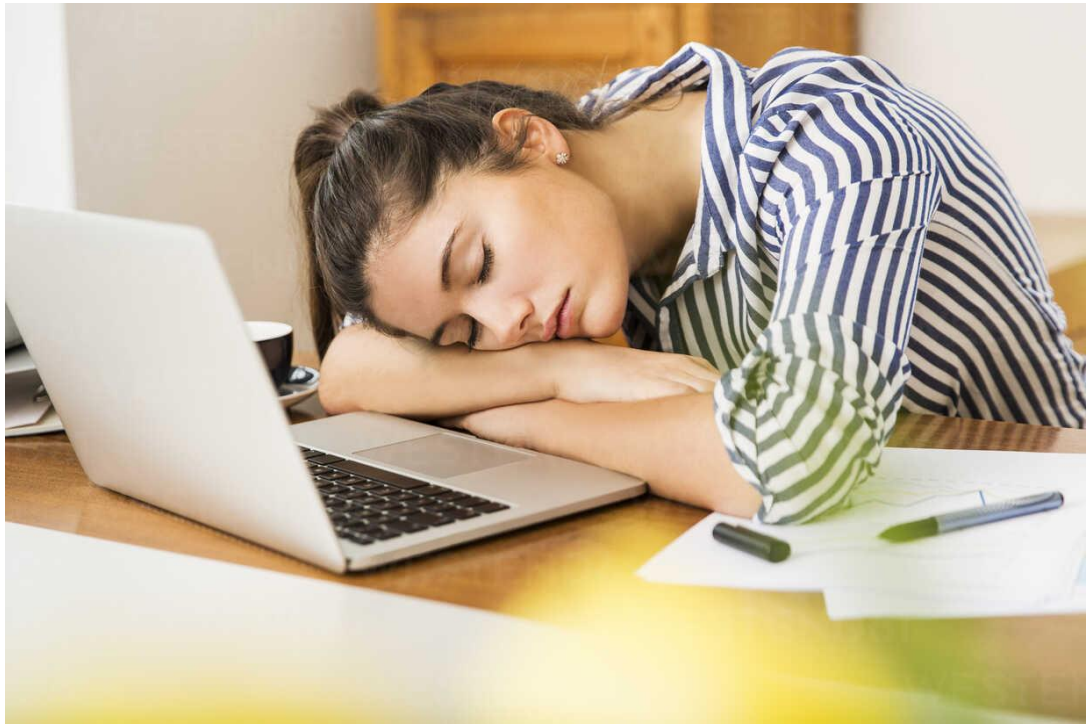


Smart working and DLT

- **Research theme**:
  - Enabling auditing process in smart working scenario

- **Goals**:
  - Certify worker activities
  - Effective control of work activities
  - Keeping social interactions
  - Maintain/Improving productivity

- **Challenges**:
  - Privacy
  - Flexibility
  - Adaptability



cnr DIITET

CYBER LAB SECURITY
Consiglio Nazionale delle Ricerche

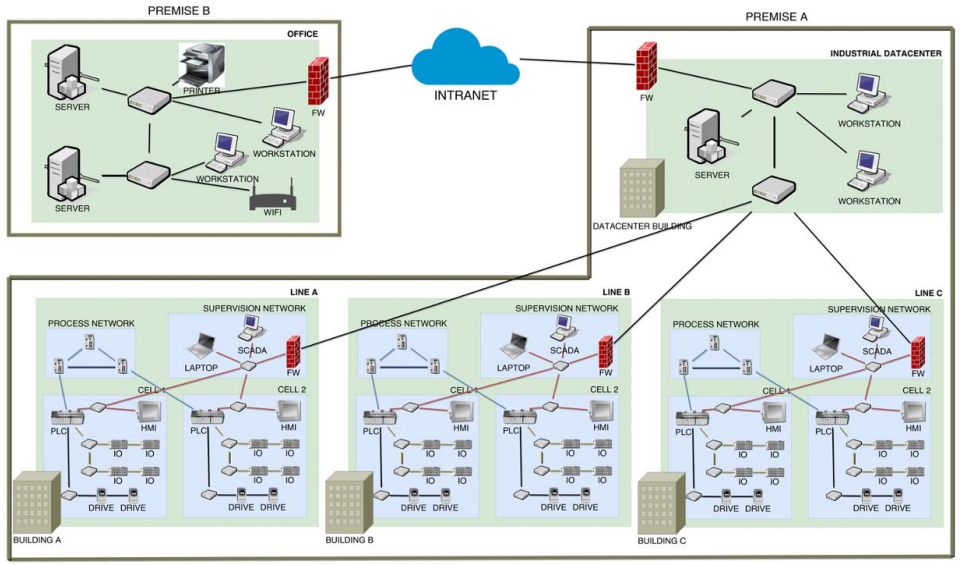
Flagship activity:

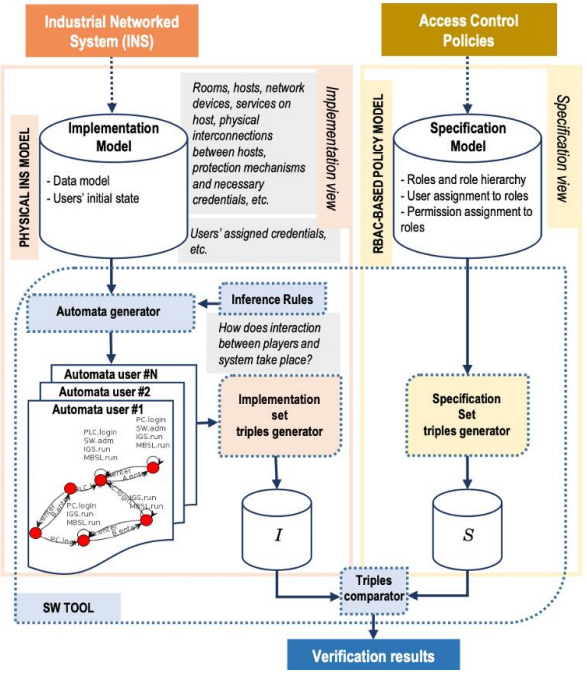
Secure Critical National Infrastructures

E. Cambiaso, M. Cheminod, E. Marchetti

Consiglio Nazionale delle Ricerche

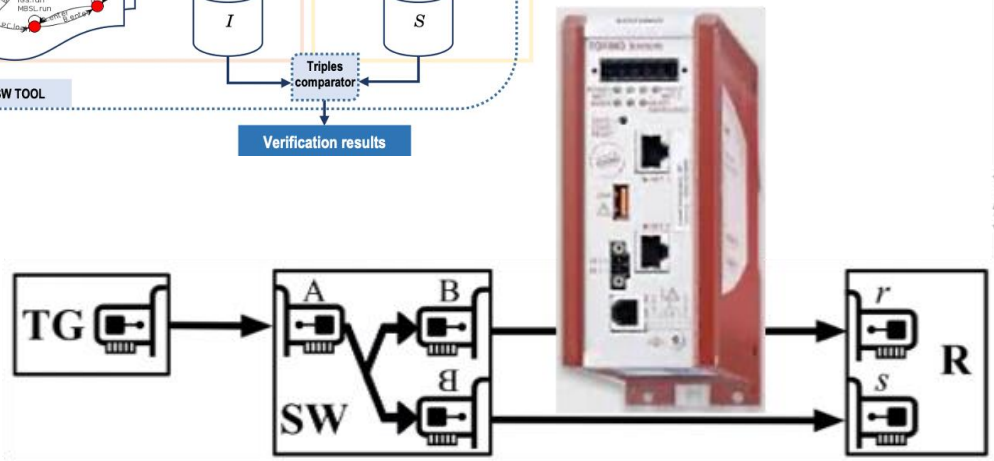
Access Control Policies Verification

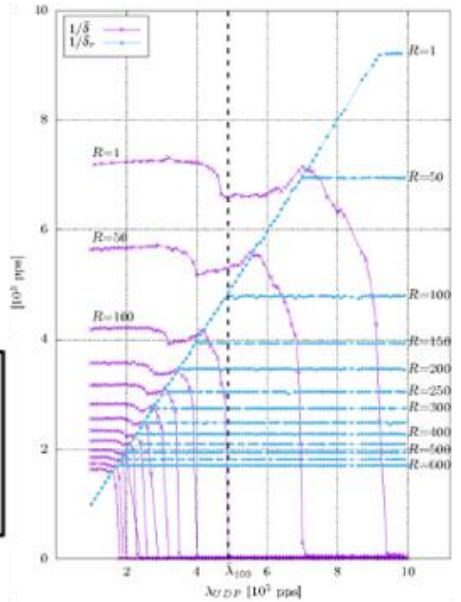




Cyber Security for Europe

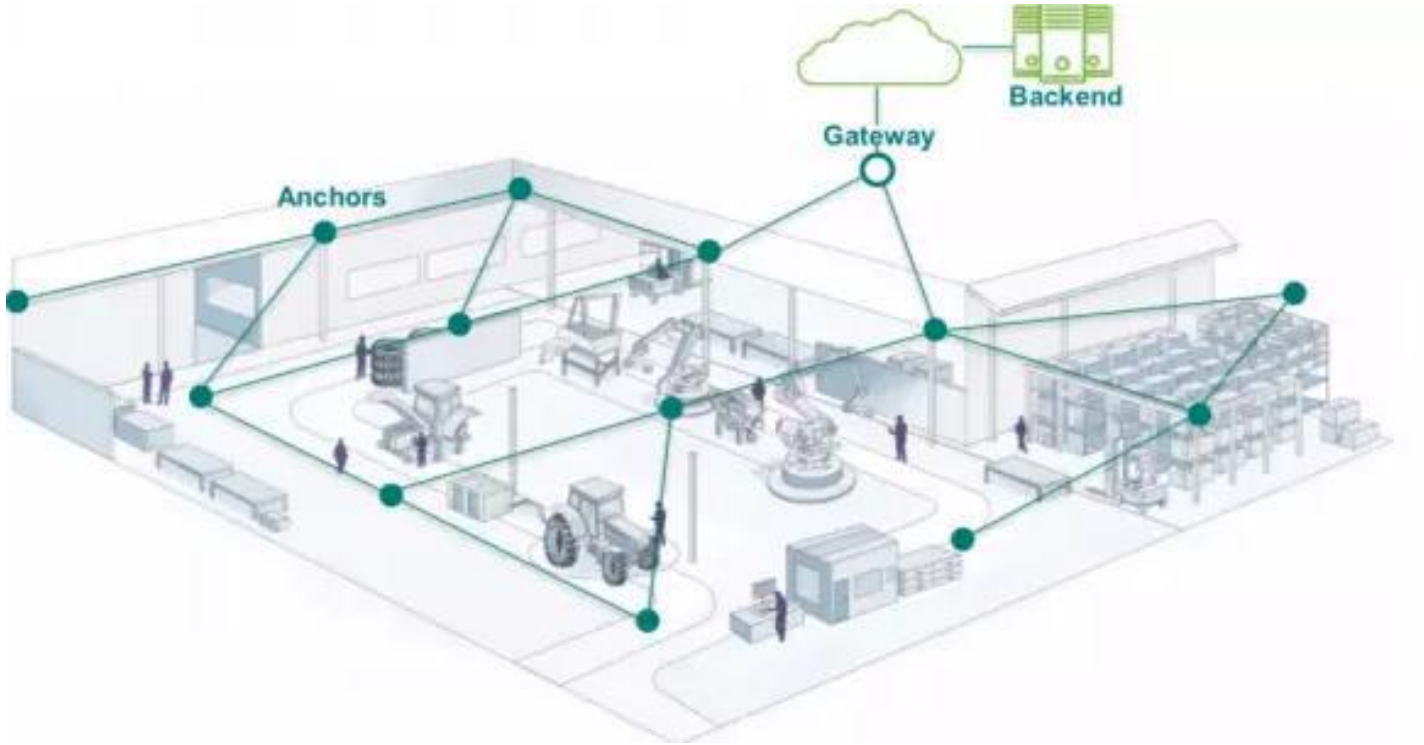
Performance of security mechanisms

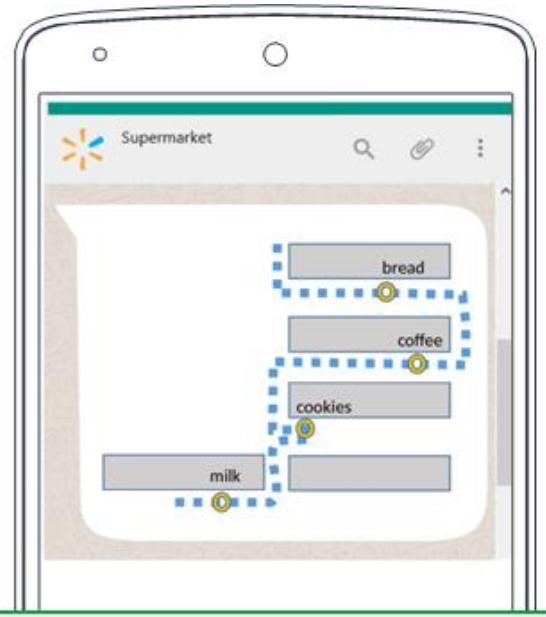




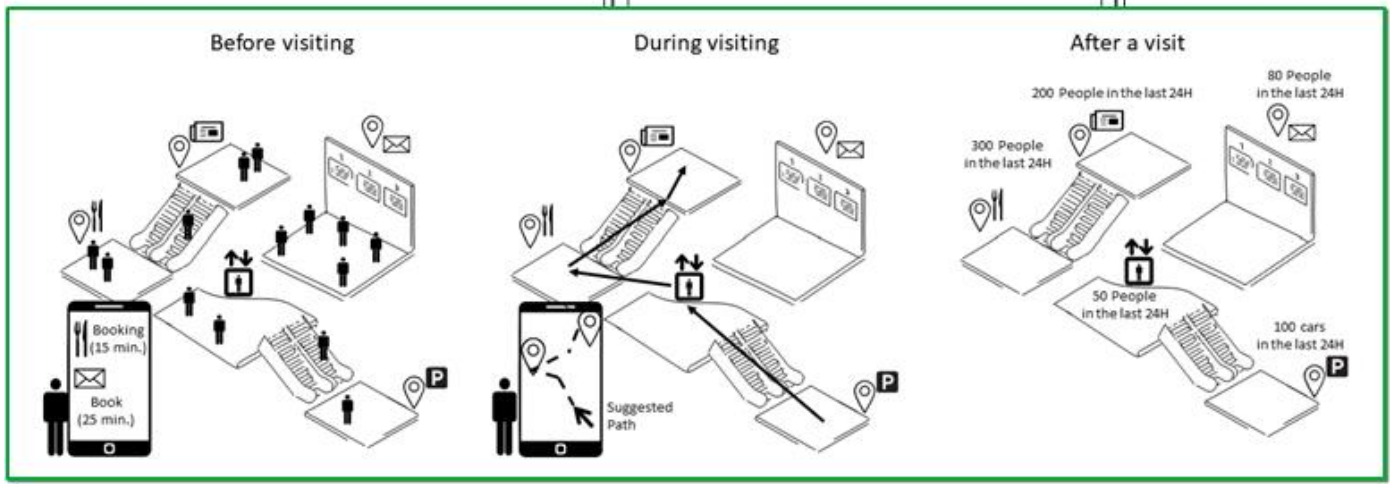
Consiglio Nazionale delle Ricerche

GDPR-Based Indoor Localization Systems





GDPR-Based ILS for social distancing and improving user experience with Covid-19 safety restrictions



Consiglio Nazionale delle Ricerche

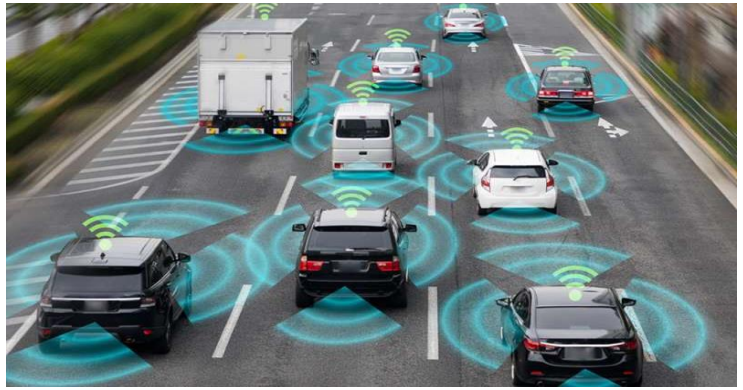
Joining Data Privacy and Data security

Methods and tools for specification, testing and monitoring data protection and compliance applicable in different application domains

Consent and Access Management

Indoor Localization Systems

Smart Cities

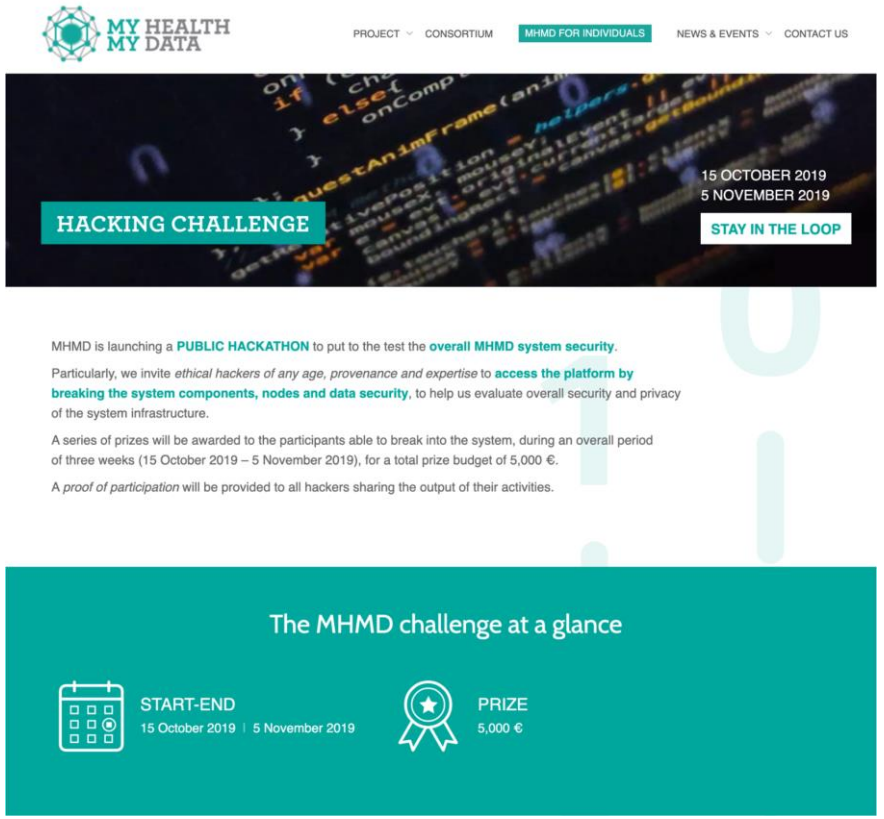


Cyber Physical Systems

Consiglio Nazionale delle Ricerche

Participation to CIP-related projects

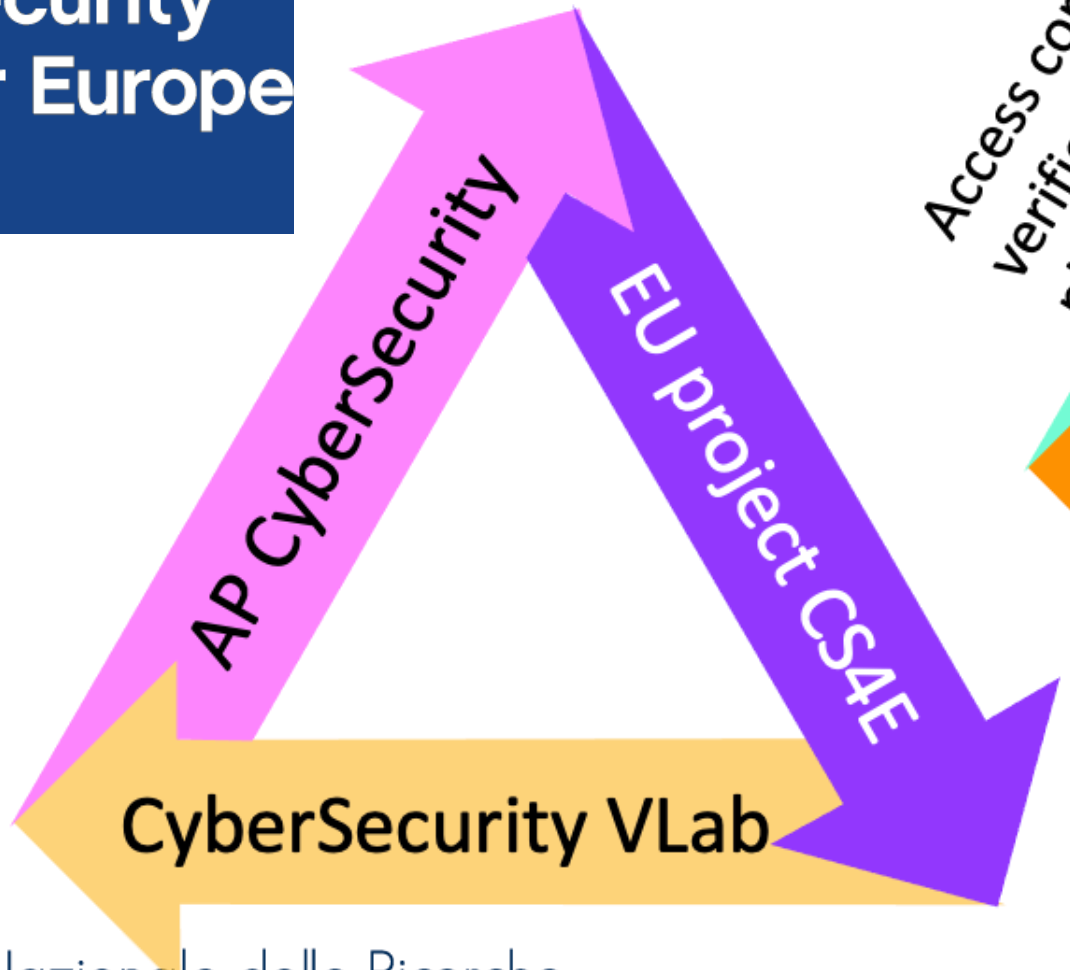
- Multiple contexts
  - Healthcare
  - Cyber-physical
  - Finance
- Multiple activities
  - Development of security components
  - Protocol attacks
  - Penetration testing
  - Hacking challenge organization

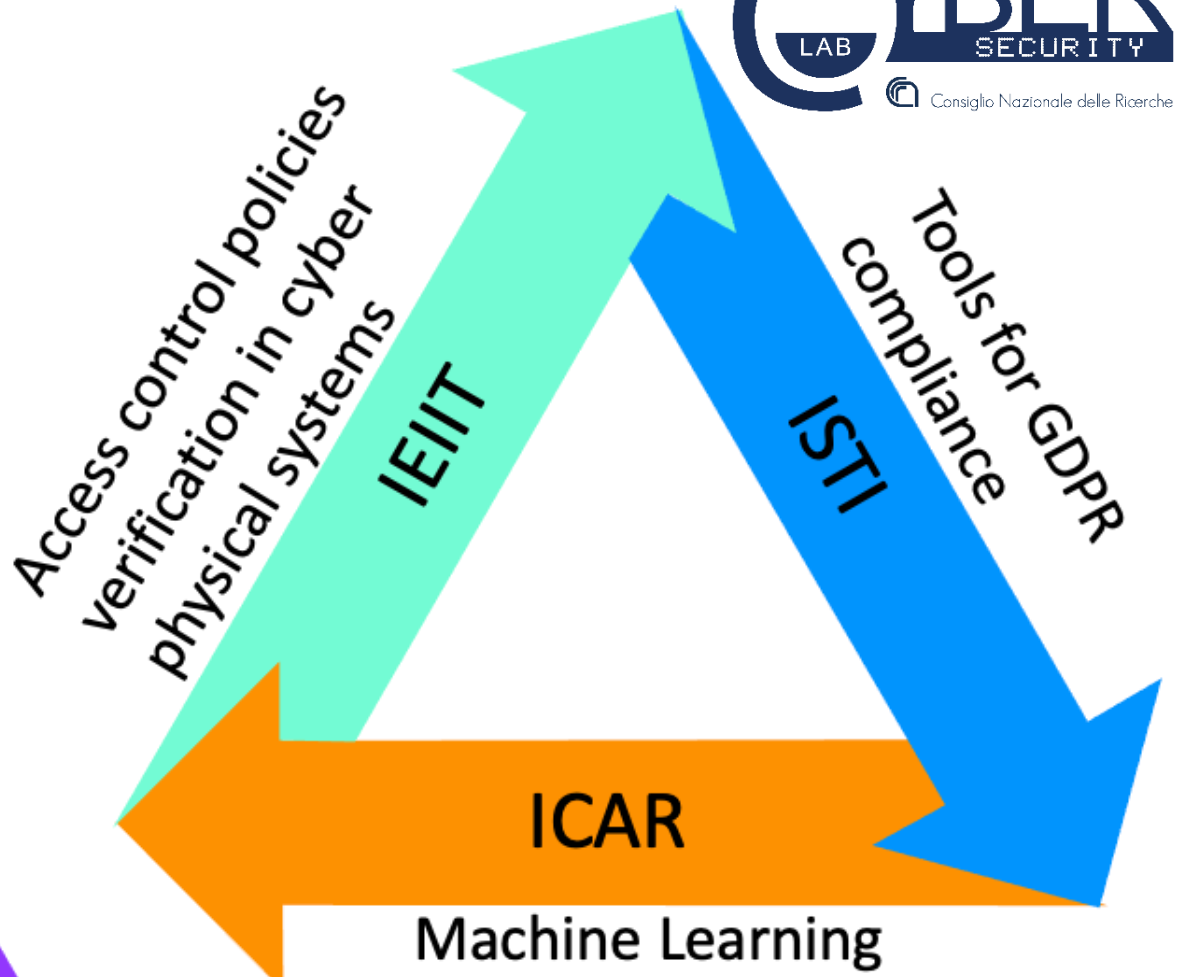


Consiglio Nazionale delle Ricerche

Focus on Pilot Project

Cyber Security for Europe





Consiglio Nazionale delle Ricerche