CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Banche & Sicurezza 2021

Roma, 26 Maggio 2021

Transizione digitale e l'azione del competence center nazionale CYBER 4.0

Matteo Lucchetti

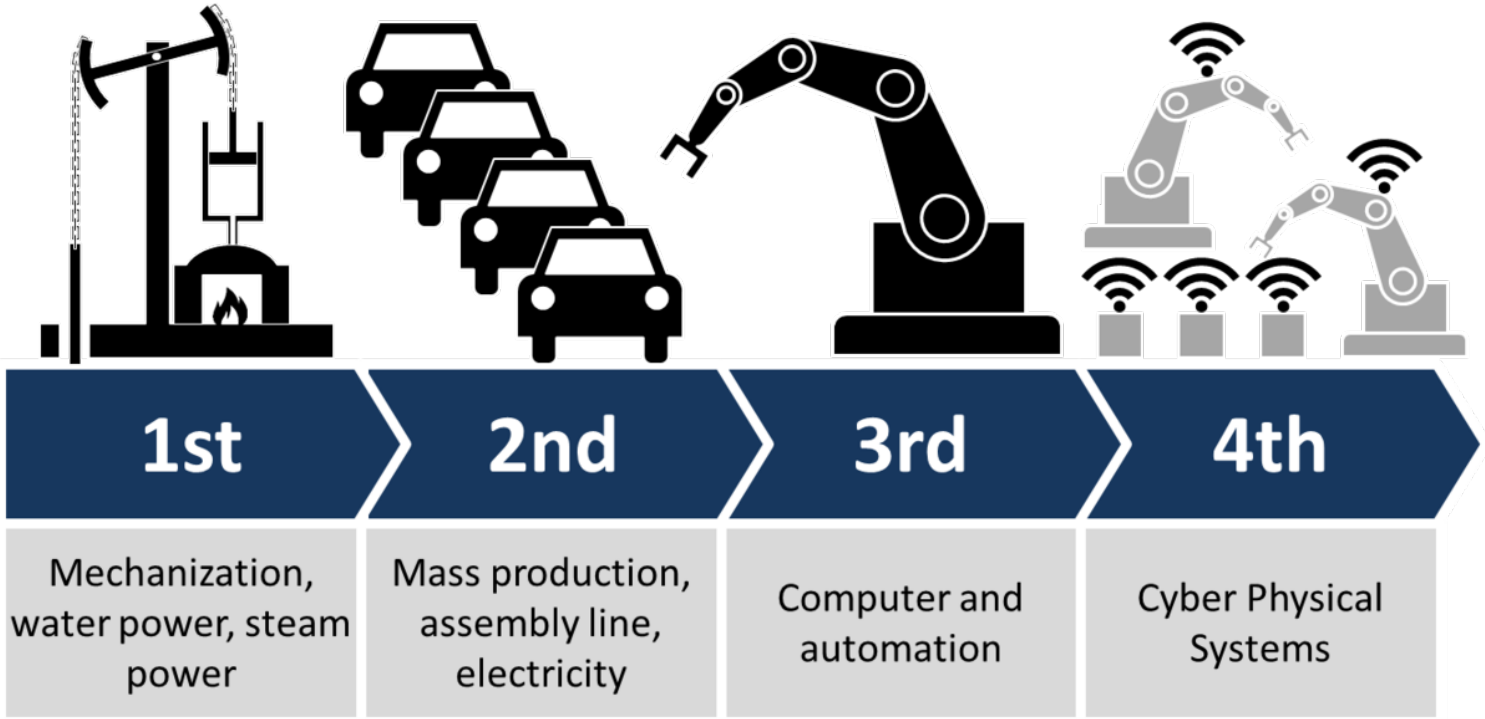
Direttore Operativo, CYBER 4.0

Matteo.Lucchetti@cyber40.it

Agenda

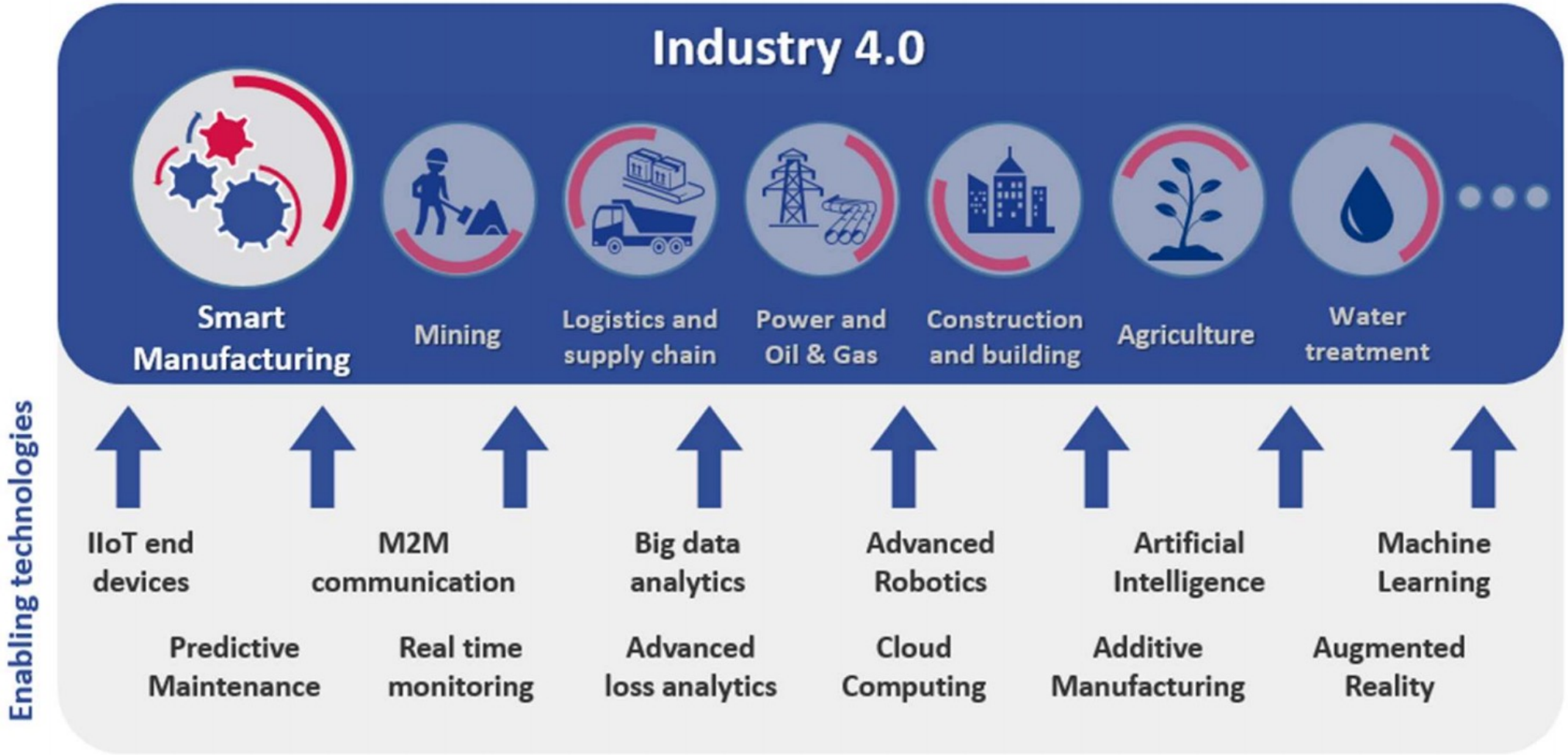
- **Transizione digitale e tecnologie abilitanti**
- **Banche e Industria 4.0**
- **CYBER 4.0**

La quarta (ri)evoluzione



ENISA: "**a paradigm shift towards digitalised, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies**".

Le tecnologie abilitanti dell'Industria 4.0



Banche e Industria 4.0

- Mutate esigenze dei clienti di nuova generazione
- Aumento di produttività ed efficientamento dei costi tramite l’uso di tecnologie 4.0
- Maturità delle tecnologie abilitanti
- Banche maggiori investitori in tecnologia dopo il comparto ICT
- Effetti della pandemia spingono operatività online in modo pervasivo

Banche e Industria 4.0

- **Artificial Intelligence, Big Data Analytics, Cloud Computing**
  - Disegno di nuovi prodotti finanziari, Marketing, Risk management, Servizi al cliente
  - Esempio MyBank, Ant Group
    - 2 Trillion yuan loans to 16 Million SMEs, Real-time data + 3000-variables risk models
    - Loan applications are processed in 3 minutes
- **5G**
  - Il GSMA stima che le connessioni 5G cresceranno dai 10 milioni di fine 2019 a 1.8 miliardi entro il 2025
  - Accesso ad applicazioni cloud molto più veloce → processi più complessi in minor tempo
  - Migliore customer experience sul canale mobile, ATM e chioschi, pagamenti più efficienti
  - Prevenzione frodi proattiva con dati in real time
  - 3G e 4G diventeranno più accessibili e la base clienti su mobile si allargherà
- **Blockchain**
- **Robotic Process Automation**
  - AI workforce per supportare l'esecuzione di compiti ripetitivi (es. apertura conto, KYC e AML, etc.)
  - Entro il 2022 macchine e bots eseguiranno tra il 10% e il 25% dei compiti in banca (McKinsey, 2019)
- **IoT**
  - Acquisizione real-time dati del cliente per marketing, ma anche fraud detection, IoT Trading, Gestione asset

Industria 4.0 e IoT
Problematiche di sicurezza

- **Complessità gestionale** e vulnerabilità di processo
  - Numerosità ed eterogeneità delle sorgenti di dati
- **Aspetti legali** di gestione dei dati
- **Integrazione/ interoperabilità con sistemi legacy**
  - Hardware potenzialmente obsoleti/ non aggiornati, vulnerabilità presenti da anni
- **Vulnerabilità software e dispositivi**
  - In banca e fuori
- **Sicurezza della rete**
  - Connessioni non sicure
  - Nuove sfide per forze dell’ordine
- **Fattore umano**
  - Nuovi tipi di dati, sistemi, reti

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

L'ecosistema dei Competence Center per l'Industria 4.0

I centri di competenza sono partenariati pubblico-privati il cui compito è quello di svolgere attività di **orientamento e formazione** alle imprese su tematiche Industria 4.0 nonché di **supporto nell'attuazione di progetti di innovazione, ricerca industriale e sviluppo sperimentale** finalizzati alla realizzazione, da parte delle imprese fruitrici, in particolare delle Pmi, di nuovi prodotti, processi o servizi (o al loro miglioramento) tramite tecnologie avanzate in ambito Industria 4.0.

Gli otto centri che sono stati selezionati sono:

- CIM 4.0 - Competence Industry Manufacturing 4.0
- Made - Competence Center Industria 4.0
- BI-REX - Big data Innovation-Research EXcellence
- ARTES 4.0 – Industry 4.0 Competence Center on Advanced Robotics and enabling digital TEchnologies & Systems 4.0
- SMACT Competence Center
- MedITech Competence Center I 4.0
- START 4.0– Sicurezza e ottimizzazione delle Infrastrutture Strategiche Industria 4.0
- **CYBER 4.0 – Cybersecurity Competence Center**

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER 4.0

Centro di competenza nazionale sulla cyber security, promosso dal MiSE.

FORMAZIONE

ORIENTAMENTO

RICERCA E INNOVAZIONE

Operativo da Aprile 2021:

- 8 Organismi di ricerca – Università (Sapienza, Luiss, Tor Vergata, Roma Tre, etc.), CNR
- 1 Istituzione pubblica
- 35 entità private, inclusi i maggiori player nazionali (Leonardo, TIM, Thales, Telespazio, Poste Italiane, BV Tech, Cy4Gate, etc.), PMI, Servizi Formativi Confindustria e alcune Fondazioni

Coordinatore: Sapienza Università di Roma

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

VISION

Agire con fiducia nello spazio cyber

CYBER 4.0

CYBERSECURITY COMPETENCE CENTER

MISSION

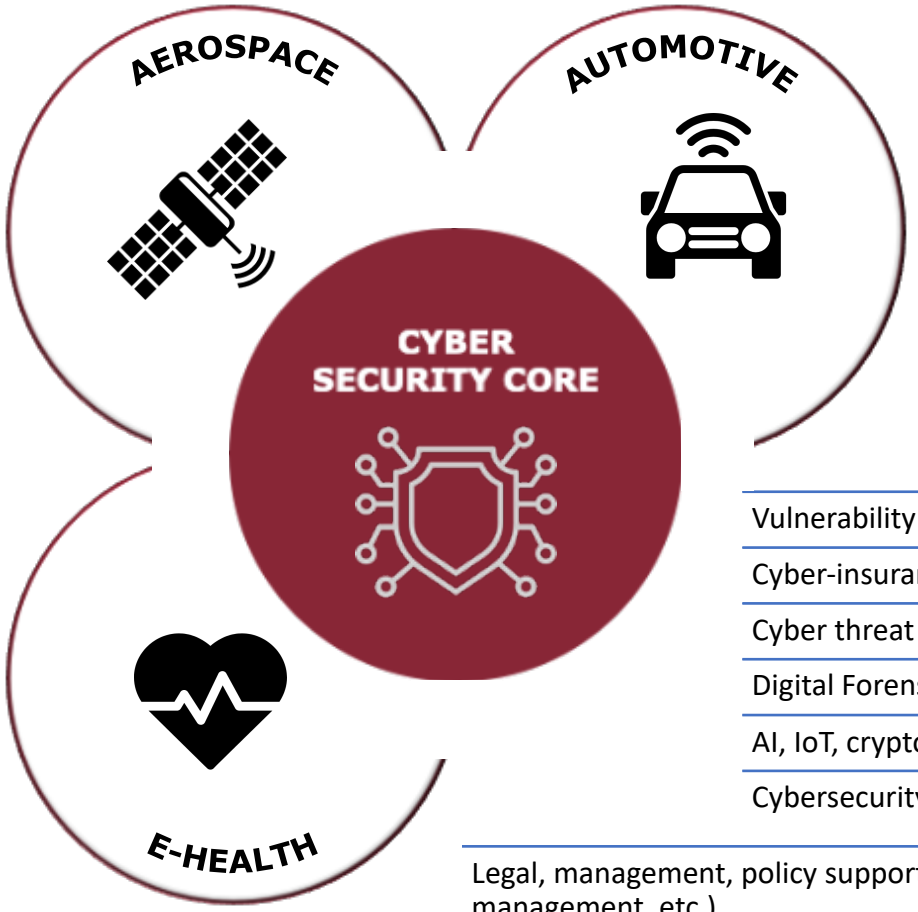
Accompagnare policy makers, imprese e PA in un percorso di crescita verso una digitalizzazione sicura, grazie a soluzioni concrete, strategiche e sostenibili basate su conoscenze, tecnologie innovative e servizi abilitanti sviluppati con le competenze del nostro network, che valorizzino le eccellenze del Paese nel contesto europeo e internazionale

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Aree di competenza

- Artificial Intelligence
- Cybersecurity of Aerospace HW development
- Use of COTS HW in aerospace projects
- Secure use of satellite data
- Design and manufacturing of aerospace components

- Resilience vs cyber threats
- Cryptography and authentication
- Interconnected Embedded Sensor
- Machine learning applications
- Privacy of passengers and vehicles
- Data analytics tools for Cloud-IoT/Fog computing architectures



- Security infrastructure, encrypted communication for telemedicine
- Remote collection, measurement and analysis of biometric data
- Meta analysis and integration of social, genetic and epigenetic data
- Risk Analysis and personalized medical assistance
- Security of online connected medical devices, and privacy
- Certification and security assessment of saensors and devices

- Vulnerability assessment , Cyber risk mitigation, incident response
- Cyber-insurance
- Cyber threat intelligence
- Digital Forensics
- AI, IoT, cryptography security aspects
- Cybersecurity by design

- Legal, management, policy support (GDPR, contracting, cybercrime, IPR, IT governence, Data management, etc.)
- Cybersecurity awareness

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività CYBER 4.0

Bandi progetti di ricerca

- Bando 1/2021 – scadenza 21 Maggio
- Bando 2/2021 – lancio il 10 Giugno

Strategic Design

- Metodologia di Design Thinking
- Vision, mission milestone plan

Costituzione roster di esperti

Formazione e orientamento

- Corso PA
- Assessment PMI

Iniziativa esterna

Aree di ricerca

1. Cyber security core
2. Aerospace
3. Automotive
4. eHealth

Dotazione 2.2Mln €

Progetti 12-18 mesi

TRL 5 → TRL 7

https://cyber40.it/bandi

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività CYBER 4.0

Bandi progetti di ricerca

- Bando 1/2021 – scadenza 21 Maggio
- Bando 2/2021 – lancio il 10 Giugno

Strategic Design

- Metodologia di Design Thinking
- Vision, mission milestone plan

Costituzione roster di esperti

Formazione e orientamento

- Corso PA
- Assessment PMI

Iniziativa interna

Percorso in 6 fasi

1. Stakeholder ed esigenze
2. Vision & Mission
3. Servizi e soluzioni
4. Business Plan
5. Comunicazione e web
6. Milestone plan

Follow up

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività CYBER 4.0

Bandi progetti di ricerca

- Bando 1/2021 – scadenza 21 Maggio
- Bando 2/2021 – lancio il 10 Giugno

Strategic Design

- Metodologia di Design Thinking
- Vision, mission milestone plan

Costituzione roster di esperti

Formazione e orientamento

- Corso PA
- Assessment PMI

Iniziativa interna

Lotti di competenze

1. Legale
2. Policy/ processi cyber security
3. Tecnologie di cyber security
4. Formazione PA
5. Formazione PMI
6. Orientamento PA
7. Orientamento PMI
8. Collaborazione internazionale

Validità biennale, rinnovabile

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Piano previsto di attività del CC

- **Formazione** PA, PMI
  - Dirigenti
  - Operativi
- **Progetti di ricerca** e innovazione in ambito cyber security
  - Consulenza su accesso a programmi di finanziamento
- **Censimento catalogo servizi di cyber security**
  - Monitoraggio eventi cyber
  - Prevenzione, controlli di sicurezza
  - Servizi ad-hoc
- **Assessment** PMI, PA → orientamento su azioni conseguenti
- **Osservatorio** cyber security PA, PMI
- **Demo lab/ Showroom**, Test before invest
  - Virtuale/ Fisica

Network

STAKEHOLDER GROUP

- Stakeholder nazionali e internazionali
- Meeting semestrale con Comitato Scientifico e di Indirizzo
- Vivaio per idee di attività da erogare da parte di CYBER 4.0
- Comunicazione mirata

RETE DEI CC NAZIONALI

- Coordinamento con MISE
- Accordo con ENEA Tech, ITS
- Accordo quadro di collaborazione inter-CC per proposte EDIH

COLLABORAZIONI INTERNAZIONALI

- EDIH, call (27/5?)
- Altri centri di innovazione
- Progetti EU

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

NEST Proposal for EDIH

Network for European Security and Trust

- **Test before invest**
  - Proof of concept/ demos, Security Assessment and evaluation, Online channels monitoring, Early warning, Information Sharing
- **Training**
  - Security awareness, Standard courses for non specialist, Standard courses for specialist, Custom training for Public Administration, Custom training for SOC operators
- **Access to funds**
  - Grant scouting, Partnering, Proposal drafting support, contracting, budget and finance
- **Innovation ecosystems**
  - Assessment, business matching, business planning, funding and ventures

Grazie

Matteo Lucchetti
Direttore Operativo CYBER 4.0

Matteo.Lucchetti@cyber40.it