CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Tecnologie satellitari e sicurezza
Lo spazio come nuova frontiera cyber

Cybersecurity e spazio

L’innovazione come chiave di sviluppo

Matteo Lucchetti

Direttore Operativo

Cyber 4.0 – National Cybersecurity Competence Center

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cybersecurity e spazio

- Cybersecurity **per lo** spazio
  - Sicurezza delle applicazioni spaziali
  - Sicurezza delle tecnologie satellitari

- Cybersecurity **dallo** spazio
  - Utilizzo delle tecnologie spaziali per rafforzare la cybersecurity a terra, QKD

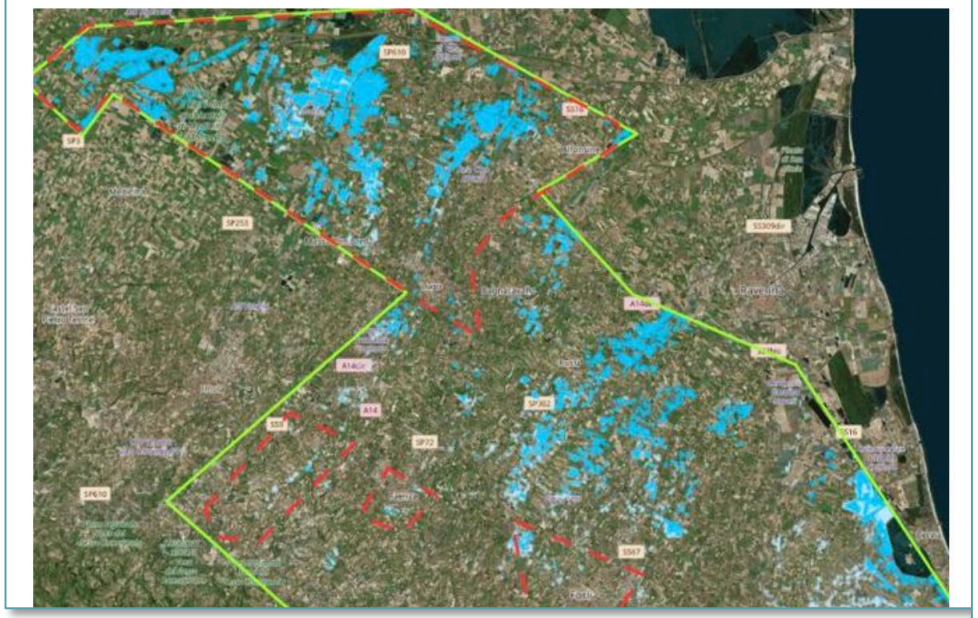
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Tecnologie satellitari all'opera

Emilia-Romagna, l'alluvione vista dal satellite: «L'area sommersa si è allargata negli ultimi due giorni»

di Paolo Virtuani

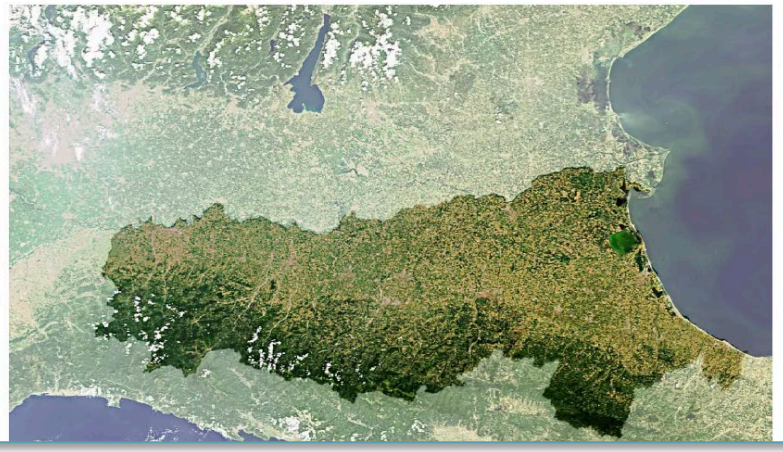
Grazie dal radar a bordo di Cosmo-SkyMed. Eccezione dettaglio delle aree invase dall'acqua visibili campo per campo, via per via



Alluvione Emilia Romagna: l'Ue attiva Copernicus per la mappatura satellitare di emergenza

Alluvione Emilia Romagna: attivato il servizio Copernicus in modalità di mappatura rapida per aiutare le autorità italiane

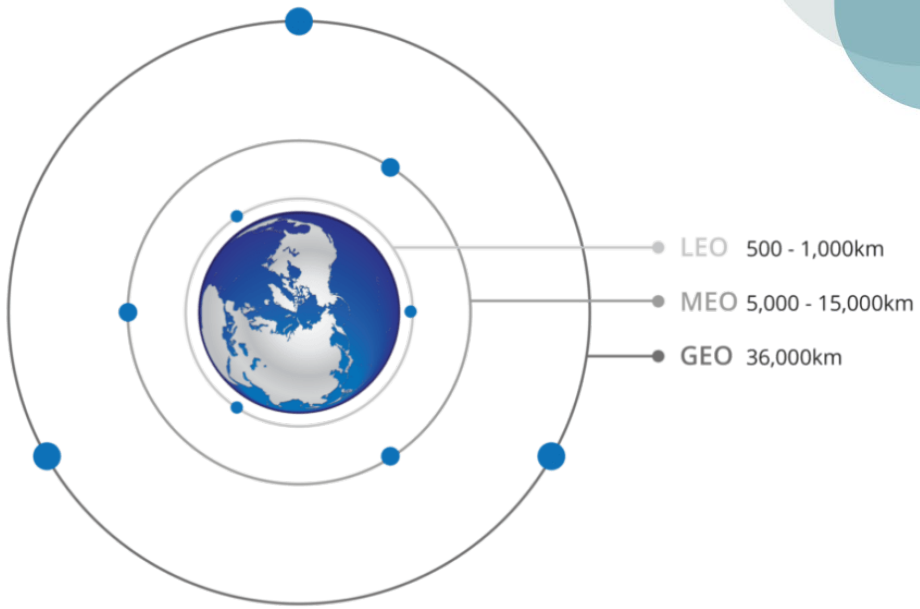
di Beatrice Raso 18 Mag 2023 | 14:27



CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Lo scenario

- **7.702 satelliti attivi in orbita**
- LEO (84% del totale), più facili da raggiungere, comunicazioni radio più rapide → ideali per comunicazioni Internet e per Industrial IoT
- Rapido incremento del numero dei satelliti piccoli (94% del totale dei lanci ad oggi, contro il 34% degli anni 1990)
- Costi di lancio diminuiti → Incremento soggetti privati (SpaceX, Orgin, etc.)
- Nascita di nuove start-up, contesto con fortissimo tasso di innovazione tecnologica



- Parallelo, consistente **aumento della superficie di attacco cyber**
  - **Motivazioni economiche**
  - **Motivazioni geopolitiche**

L’attacco alla rete satellitare KA-SAT

- **24 Febbraio 2022**, giorno dell’invasione russa in Ucraina
- Cyber attacco a modem e router che comunicano con la rete satellitare KA-SAT, che fornisce **accesso Internet a decine di migliaia di cittadini in Ucraina ed Europa**
- **Wiper malware «AcidRain»**, con l’intenzione di rendere indisponibile il servizio, non di accedere a dati o sistemi
- Attribuzione → Forze armate russe, per rendere inservibile il centro di comando delle forze armate Ucraine durante l’invasione
- L’azione ha avuto effetti in tutta Europa
  - Una compagnia energetica tedesca ha perso il controllo su 5.800 turbine eoliche

*Ultimately, **tens of thousands of modems that were previously online and active dropped off the network, and these modems were not observed attempting to re-enter the network**. The attack impacted a majority of the previously active modems within Ukraine, and a substantial number of additional modems in other parts of Europe. Subsequent investigation and forensic analysis identified a **ground-based network intrus**ion by an attacker exploiting a misconfiguration in a VPN appliance **to gain remote access to the trusted management segment of the KA-SAT network**. The attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this network access to **execute legitimate, targeted management commands on a large number of residential modems simultaneously**. Specifically, these **destructive commands overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable**.*

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Jamming, hijacking

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING &

OFFENSIVE CAPABILITIES —

China building cyberweapons to hijack enemy satellites, says US leak

Document assesses Beijing's ambitions to disrupt communications during wartime.

MEHUL SRIVASTAVA, FELICIA SCHWARTZ, AND DEMETRI SEVASTOPULO, FT - 4/21/2023, 3:28 PM

[…] These attacks, first developed in the 1980s, attempt to drown out signals between low-orbit SpaceX satellites and their on-ground terminals by broadcasting on similar frequencies from truck-borne jamming systems such as the Tirada-2.

China's more ambitious cyber attacks aim to mimic the signals that enemy satellites receive from their operators, tricking them into either being taken over completely or malfunctioning during crucial moments in combat. […]

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

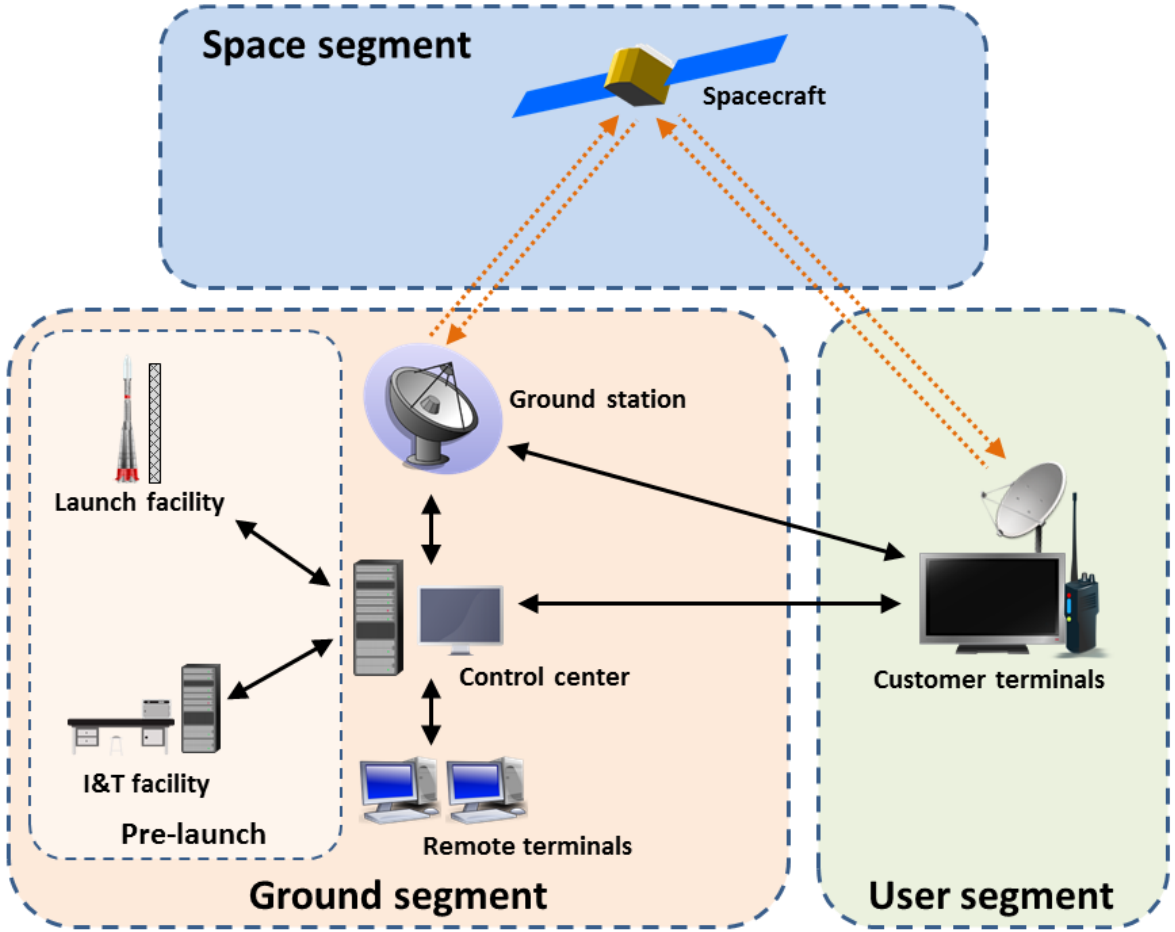
La prima esercitazione di ethical hacking su un satellite

THALES SEIZES CONTROL OF ESA DEMONSTRATION SATELLITE IN FIRST CYBERSECURITY EXERCISE OF ITS KIND

| 25 APR 2023 |

- For the third edition of CYSAT, the European event entirely dedicated to cybersecurity for the space industry, taking place on 26-27 April 2023 at Station F in Paris, the European Space Agency (ESA) set up a satellite test bench to simulate attempts to seize control of OPS-SAT, a nanosatellite operated by the agency for demonstration purposes.
- Thales's offensive cybersecurity team stepped up to the challenge, identifying vulnerabilities that could enable malicious actors to disrupt operation of the ESA satellite.
- The results of the ethical satellite hacking exercise, the first of its kind in the world, will be used to tighten security for the satellite and its onboard applications, helping to improve the cyber resilience of space systems, protect sensitive data and support the long-term success of space programmes.

Vulnerabilità dei sistemi e fattore umano



- **Infrastruttura legacy** spesso datata e aggiornamento software spesso non semplice, con necessità di test molto accurati per assicurare che non ci siano interferenze con altre funzioni critiche
- Anche se tecnicamente possibile, le risorse per attaccare direttamente le vulnerabilità dell'infrastruttura di telemetry, tracking and control del **ground segment** di una rete satellitare sono ingenti → attacco più probabile per attori statuali
- Molto più semplice, diffuso e probabile, un attacco di **social engineering** per avere accesso alle infrastrutture di controllo tramite credenziali legittime o tramite malware.
- Le tecnologie IT alla base delle applicazioni satellitari sono complesse, ma sono sempre più connesse a **sistemi commerciali che presentano vulnerabilità** che possono essere sfruttate facilmente attraverso tipologie di attacco ben note (e.g. ransomware)

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Quali misure

- **Security by design** per le nuove applicazioni satellitari
- Sistemi IAM evoluti (e.g. basati su identificazione intelligente tramite Machine Learning)
- Aggiornamento e hardening dei dispositivi IoT a bordo
- Sistemi IDS/ IPS/ logging per il monitoraggio continuo delle sequenze di comando – sia a bordo che a terra (cross-check), telemetria, stato dei ricevitori, configurazioni, in modo da prevenire comportamenti inattesi, sospetti o malevoli, e in grado di tornare sempre a uno stato cyber-safe
- **Supply chain** risk management
- **Software sviluppato con processi certificati e sicuri**
- Protezione contro **attacchi alle comunicazioni** (jamming, spoofing), e.g. monitoraggio della forza del segnale, securizzazione dei trasmettitori e dei ricevitori, etc.
- …

I fattori abilitanti

COMPETENZE E INNOVAZIONE

Cyber 4.0

Centro di competenza nazionale sulla cybersecurity

Centro di competenza nazionale ad alta specializzazione sulla cybersecurity, promosso e finanziato dal MIMIT, inizialmente nel piano Industria 4.0 e ora soggetto attuatore PNRR

- Avviato nel 2020, **Operativo da Aprile 2021, HQ al Tecnopolo Tiburtino – Roma**
- **8 Organismi di ricerca, 1 Istituzione pubblica, 35 Partner privati**
- **Target delle attività – Imprese e PA**
- **Mandato istituzionale**
  - Linea A: Infrastruttura del Centro per erogazione servizi – 3.5 M€
  - Linea B1: finanziamento progetti R&I – 6 M€
  - Linea B2: servizi di innovazione – 4M€
- Possibilità di erogare **servizi commerciali**
- **Partecipazione a iniziative finanziate**

Cyber 4.0

Compagine associativa

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Università di Roma Tor Vergata
ROMA TRE UNIVERSITÀ DEGLI STUDI
UNIVERSITÀ DEGLI STUDI DELL'AQUILA
SAPIENZA UNIVERSITÀ DI ROMA
UNIVERSITÀ DEGLI STUDI DELLA TUSCIA
UNIVERSITÀ DEGLI STUDI DI CASSINO E DEL LAZIO MERIDIONALE
LUISS
UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA
sogei
Posteitaliane
FORMIT
INAIL ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO
Clusit Associazione Italiana per la Sicurezza Informatica
TIM
Consiglio Nazionale delle Ricerche
AlmavivA
YOROI
LEONARDO
BV TECH Securing the Future.
CY4GATE ELETTRONICA GROUP
aizoon TECHNOLOGY CONSULTING
NETGROUP
ENGINEERING THE DIGITAL TRANSFORMATION COMPANY
SISTEMI FORMATIVI CONFINDUSTRIA
FONDAZIONE E. AMALDI
POLO DI INNOVAZIONE AUTOMOTIVE
LAND
TECHNO CENTER
TELESPAZIO a LEONARDO and THALES company
ThalesAlenia Space a Thales / Leonardo company
DP
DI.GI. Academy
HMS IT
LAZIO CONNECT
INNOVERY INNOVATION DISCOVERY
RADIO6ENSE
S&A SISTEMI & AUTOMAZIONE
ARPEX Environment Trentino
PRISMA improve your business
mediavoice
TECNORAD PERSONAL DOSIMETRY SERVICE

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cyber 4.0 come soggetto attuatore PNRR
Servizi di innovazione

Attività istituzionali | Servizi di mercato | Progetti finanziati | Networking

Azioni co-finanziabili con intensità di sconto correlata alla dimensione aziendale:

- Audit tecnico, valutazione maturità tecnologica – **Assessment**
- Prova prima dell'investimento – **Test-before-invest**
- **Formazione**
- Consulenza su proprietà intellettuale
- Consulenza su **accesso ai finanziamenti**
- Consulenza su **innovazione tecnologica di processo e di prodotto, sensibilizzazione e networking**
- **Progettazione dell'intervento di innovazione**

Co-finanziamento

- Micro – 70-100%
- Piccole – 70-100%
- Medie – 60-90%
- Grandi – 40-50%

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività istituzionali

Orientamento PMI e PA

Orientamento PMI

Vademecum PMI

- **12 azioni** per un business sicuro
- Basato su 12 Step ENISA

Ministero delle Imprese e del Made in Italy

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

Postura cyber security PMI

- Basato su **Framework Nazionale Cybersecurity e Data Protection**
- **Analisi** aree di intervento prioritario, remediation roadmap, impatto economico e benefici
- **Estensione nazionale** – DIH, PID, Case Tecnologie Emergenti

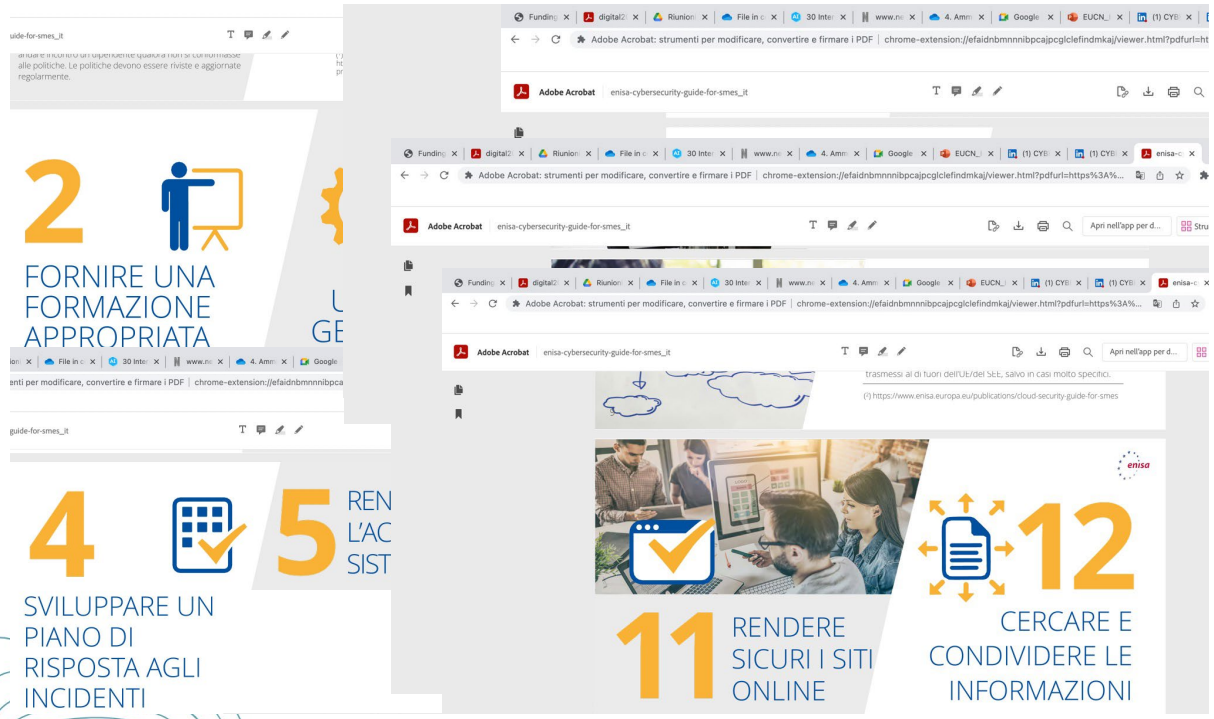
Roadshow Cyber 4.0

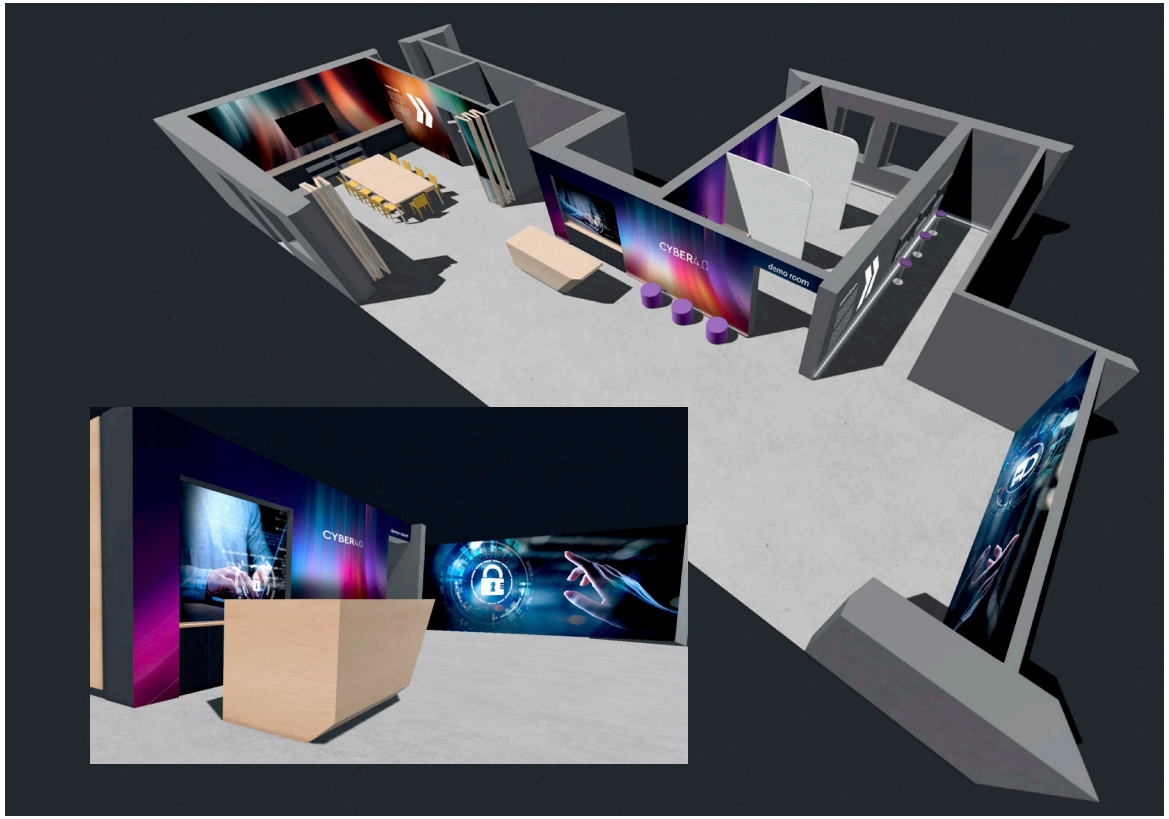
- Coinvolgimento DIH e altre realtà attive in regione (Polizia Postale, CTE, etc.)
- Sessioni di info/ formazione e incontri con esperti, case studies e buone pratiche, quick Cyber Checkup
- Aggregazione di comunità locali per **information sharing**

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività istituzionali
Orientamento PMI e PA

Demo Lab e Test Before Invest – T4





CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Attività istituzionali
Ricerca e Innovazione

Progetti di ricerca e innovazione finanziati dal Centro

- Alto TRL, breve-media durata
- **Cofinanziamento 2.2 M€**, budget totale progetti ca. 7 M€
- **15 progetti finanziati** (2021-2023), 29 aziende coinvolte – 80% PMI innovative e start-up
- **Rifinanziamenti per 5.5 M€** (2023-2025)

CORE CYBER SECURITY

- **ConTI** – Contextual Threat Inteligence
- **BRIE** – Blockchain register for Import Export
- **KEEPCALM** – Kernel Engines Enable (to) Prevent Cyber Attacks (with) Learning Machines
- **CybersecH** - Cybersecurity hardening for A.I. solutions
- **BINTRAWINE** - Blockchain, Tracking and Tracing solutions for Wine

AUTOMOTIVE

- **M-A-C-S** – Multibrand Automotive Cybersecurity Software
- **SHINE-ON** - Secured HIgh accuracy localizatioN Equipment for automotive applicatioNs

HEALTHCARE

- **MAPS-EH** - Policy di sicurezza in campo eHealth
- **ISHealth** - Improved Security e-Health
- **SI-PAC** - Sistema Informativo per la Sicurezza della Gestione dei Pacchetti Ambulatori Complessi
- **PEHSA** - Pleyo E-Health: Secure APP
- **SEPLES** - SEcure PLatform of E-health Services
- **CY-CAD** - Cyber-security framework for medical data dissemination

AEROSPACE

- **QCS-TB** - Quantum Communication and Synchronization Testbed
- **QKD SVS** - QKD System Volume Simulator

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cybersecurity **dallo** spazio
Quantum Key Distribution

- Crittografia classica basata su algoritmi ad alta complessità computazionale
- Cambio di paradigma imposto dall'avvento delle tecnologie quantistiche – non più complessità computazionale, ma leggi della fisica
- Se un attaccante intercetta una comunicazione cifrata con chiavi quantistiche ne altera irreversibilmente lo stato quantistico dei fotoni e viene rilevato
- Il segnale quantistico però non può essere amplificato o rigenerato lungo il canale di comunicazione, che introduce un'attenuazione
- Massima distanza raggiungibile in fibra ottica – ca. 100km
- Nello spazio libero l'attenuazione è molto minore → utilizzo delle **tecnologie satellitari per la distribuzione delle chiavi crittografiche** – QKD

QKD – System Volume Simulator

Realizzazione di una **piattaforma software per la simulazione end-to-end di un servizio di distribuzione di chiavi quantistiche**.

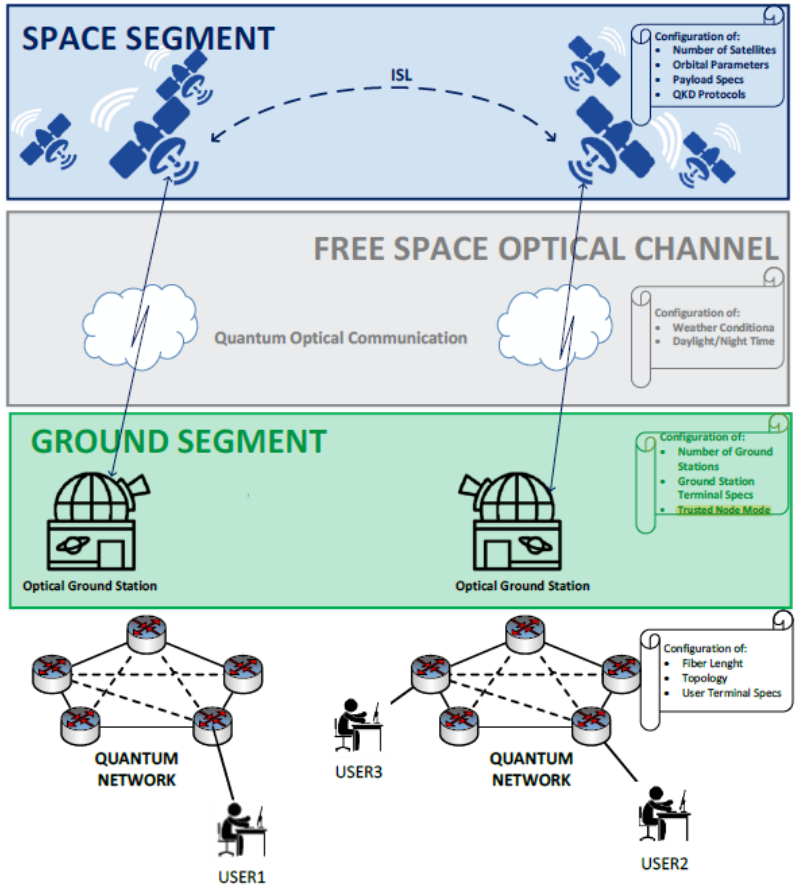
Il tool permetterà di valutare per mezzo di scenari dinamici (comprendenti aspetti funzionali ed ambientali) le soluzioni architetturali, operative e le relative problematiche di sicurezza in termini di disponibilità e prestazioni del servizio stesso

QKD SVS will enable:

- **HW resources** optimization (number of satellites, size of ground and space optical terminals, …);
- **Costs** optimization;
- **Performance** evaluation of different scenarios;
- **Risk** analysis;
- Realization of a **digital twin** of the system.

QKD SVS will be **highly configurable:**

- Number of satellites and their orbits;
- Number of ground stations and users and its geolocation;
- Type of ground and space optical terminals;
- Network topology;
- Channel parameters (transmittance, wavelength, turbulence …)
- Scenario parameters (bit rate, priority, security, …)



QKD – System Volume Simulator

- Durata progetto: 18 mesi
- Data di avvio: 01/04/2022
- **Budget totale: EUR 439.634,64**
- **Co-finanziamento: EUR 199.817,00**

- **5 Work Packages**
  1. Requirements and use case definition
  2. Modelling the QKD simulator
  3. Development of the software platform
  4. Validation & Verification campain
  5. Results evaluation and use case validation

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Quantum Communication and Synchronization Testbed

Realizzazione di una infrastruttura prototipale di comunicazione e sincronizzazione sicura basata su distribuzione quantistica delle chiavi crittografiche

Nel segmento di terra, il segnale di sincronizzazione distribuito su fibra ottica sarà cifrato e la chiave distribuita con tecnologie quantistiche di Quantum Key Distribution. Nel segmento in aria (free-space) sarà sviluppata la tecnologia per eseguire la stessa operazione su distanza di una decina di chilometri in atmosfera.

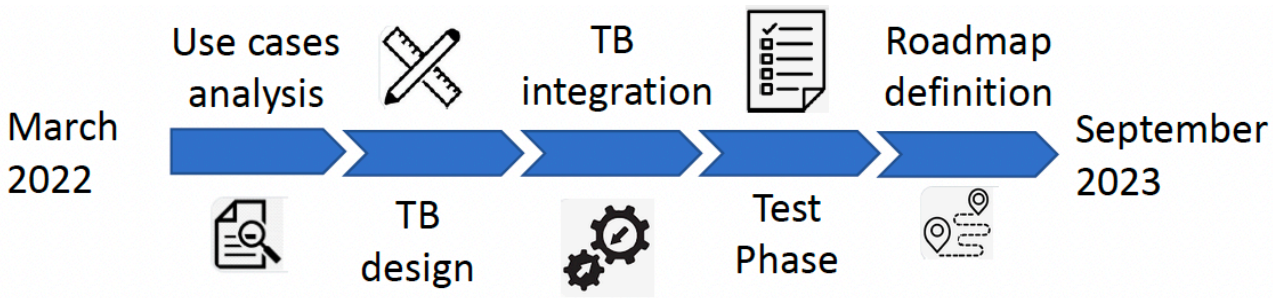
I collegamenti saranno realizzati sfruttando ed estendendo infrastrutture ottiche e quantistiche di rilevanza per il territorio, in particolare la dorsale quantistica in fibra ottica che collega Torino e Roma.

Obiettivi

- Establish a **QKD secured Communication and Time dissemination link over optical fiber**
- Establish a **QKD secured link over FSO channel**
- **Experiment an E2E communication and synchronization scenario involving both optical fiber and FSO links**
- Experiment and assess the role and criticalities (security and operation wise) of a Trusted node

QCS Testbed

- Durata progetto: 18 mesi
- Data di avvio: 01/03/2022
- **Budget totale: EUR 405.846€**
- **Co-finanziamento: EUR 151.000,00**



CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Servizi di mercato
Catalogo servizi

Servizi a catalogo che il Centro eroga attraverso i propri soci

Identificazione e gestione dei rischi	• Cyber risk assessment and management • Risk monitoring • Vulnerability assessment e Penetration Testing • Threat Intelligence • Monitoraggio della supply chain
Protezione dei Dati	• Data Protection Office as as service • Data protection assessment • Privacy governance • Data protection impact assessment
Protezione dei Sistemi	• Identity and access management, Identity governance and administration • Network security • End Point security • Defence in depth • Patch management
Consulenza	• Consulenza tecnica, organizzativa, strategica in merito a: ICS, SCADA, IoT, CLOUD • Ricerca on demand, in collaborazione con il mondo accademico • Innovation Ecosystem

Monitoraggio e rilevamento minacce cyber	• Cyber threat intelligence e cyber threat modelling, SIEM, Threat detection, Proactive monitoring • Sistemi di early warning e rilevamento attacchi • Ransomware readiness
Risposta e gestione degli incidenti	• Orientamento e consulenza in merito a: SOC, CSIRT / CERT as a services • Supporto alla definizione di un modello (tecnico ed organizzativo) per la gestione degli incidenti informatici • Supporto alla gestione operativa di incidenti cyber
Certificazione	• Supporto per l'ottenimento di certificazioni in ambito information security e cybersecurity • Laboratorio di Valutazione di Sicurezza accreditato dall'organismo di certificazione OCSI
Formazione	• A catalogo • Custom • Piani di awareness

European Digital Innovation Hub

Digital Europe – EDIH NEST

The Network for European Security and Trust is a one-stop shop for **cybersecurity solutions and capacity building initiatives**, targeting **SMEs and Public Administration of Central Italy**.

- Partners: **Cyber 4.0** (Coordinator), **DIH Lazio, DIH Umbria, DIH Abruzzo, Innova**
- Budget: **4.7 M€**
- Duration: **36 months** (2023-2025)
- Endorsements and collaborations: **National Cybersecurity Agency**, **Regione Lazio**, **Enterprise Europe Network, Italian Banking Association**

Cybersecurity tools and services	**Facilities for test-before-invest**	**Capacity building initiatives**
Assistance for access to finance and funding	**Innovation ecosystems**	**EU regulatory framework, policies and strategies**


SEAL OF EXCELLENCE

European Commission

European Commission

Digital Europe Programme

The project proposal

101120871 — NEST

"NEST - Network for European Security and Trust"

submitted under the Digital Europe Programme call

DIGITAL-2022-EDIH-03-INITIAL — Initial Network of European Digital Innovation Hubs

by

Associazione Cyber 4.0 and other participants

following evaluation by an international panel of independent experts

was recognised as a high-quality project proposal in a highly competitive evaluation process

Case delle Tecnologie Emergenti

MIMIT – Case delle Tecnologie Emergenti

CAGLIARI DIGITAL LAB

Valore totale progetto: € 12.550.000 – **Durata**: 24 mesi – **Decorrenza**: 02/02/2023

Allestimento:

- ***piattaforma di quantum computing*** per sperimentazione di soluzioni per le smart cities;
- ***infrastruttura 5G indoor***
- ***infrastruttura 5G outdoor e mobile edge computing***;
- ***piattaforma in cloud con nodi adatti allo sviluppo di applicazioni di Intelligenza Artificiale e Deep Learning***;
- ***piattaforma di open APIs*** per l'integrazione dei servizio.

Attività Cyber 4.0: soluzioni di cybersecurity per tutti i sistemi e applicativi sviluppati, animazione, gestione comunicazione/divulgazione

PESARO CTE SQUARE

Valore totale progetto: € 10.977.000 – **Durata**: 24 mesi – **Decorrenza**: 02/02/2023

Allestimento:

- **Laboratorio Attivo** per ricerca, sviluppo, e sperimentazione in ambiente reale, trasferimento tecnologico di tecnologie innovative in ambiente urbano
- **Innovation Accelerator:** Startup building, Hackathon, Open Call, incubazione e accelerazione.
- **ICT Skill Transfer**: Coinvolgimento attivo end user

Attività Cyber 4.0: soluzioni di cybersecurity per tutti i sistemi e applicativi sviluppati, animazione, gestione comunicazione/divulgazione

La rete di collaborazioni istituzionali

- **Collaborazione con ACN**
- **MIMIT**
  - **Strategia industria cyber nazionale**
  - Network dei **Competence Center**
  - Network delle **CTE**
- **EDIH Network**
  - **EEN**
  - **ECSO - EDIH Cybersecurity**
  - **Regione Lazio**
  - **Associazione Bancaria Italiana**

- **Accordi e partnership a livello nazionale**
  - Partnership con rete dei DIH di Confindustria
  - Collaborazione con **rete dei PID delle Camere di Commercio**
  - MoU con **Lazio Innova**
  - Protocollo d'Intesa con **Società Italiana di Intelligence (SOCINT)**
  - **MoU Quantum for Space**
  - Protocollo d'Intesa con **Fondazione Amaldi**

- **Networking internazionale**
  - Ad Hoc Working Group su ECSF di **ENISA**
  - Membri di **ECSO**
  - Protocollo di intesa con **Agenzia Catalana di Cybersecurity**
  - Membri di **Global Cyber Alliance**
  - Advisory Board **GFCE**
  - Membri dello Stakeholder Group di **EU CyberNet**


FORUM
CYBER 4.0
SAVE THE DATE
AULA MAGNA LA SAPIENZA
ROMA | 6-7 GIUGNO 2023
PER INFO: forumcyber40@cyber40.it
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Forum Cyber 4.0
Agenda

6 Giugno	7 Giugno
Sessione istituzionale alto livello • Presentazione di Cyber 4.0 • Testimonianze partner/ stakeholder	**Progetti di innovazione** • Digital Europe/ ECCC • Core Cybersecurity • Aerospace
Sessione internazionale • Commissione Europea • ENISA	• Automotive • Healthcare
Strategia industria cyber • Priorità nazionali, ACN, MIMIT • Contesto industria cyber nazionale • Priorità aziende	**Formazione e Orientamento** • Panel competenze, ACN/ ENISA • Scrutinio tecnologico • T4 Demo Lab
Sessione speciale dedicate a PMI, co-organizzata con Unindustria • ENISA • Presentazione Vademecum PMI • Iniziative Unindustria	**Ecostistemi** • Infosharing/ ISAC • EDIH • CTE • Conclusioni

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Tecnologie satellitari e sicurezza
Lo spazio come nuova frontiera cyber

Grazie

Cyber 4.0 – National Cybersecurity Competence Center

cyber@cyber40.it

Roma, 24/5/2023