Poste Italiane S.p.A. – Spedizione in abbonamento postale – 70% DCB Roma Aut. N. 1

ISSN 2039-8271

GARR NEWS

le notizie
sulla rete dell'Università e della Ricerca

numero **31** 2024

garrnews.it

GARR NEWS - Numero 31
2024 - Semestrale
Registrazione al Tribunale di Roma n. 243/2009 del 21 luglio 2009

Direttore editoriale: Claudia Battista

Direttore responsabile: Gabriella Paolini

Caporedattore: Carlo Volpe

Redazione: Elis Bertazzon, Sara Di Giorgio, Marta Mieli, Erika Trotto

Consulenti alla redazione: Claudio Allocchio, Mauro Campanella, Massimo Carboni, Sabrina Tomassini, Davide Vaghetti, Simona Venuti

Hanno collaborato a questo numero: Edoardo Angelucci, Claudio Barchesi, Luca Carbone, Marco Cirilli, Marco Falzetti, Emanuele Guerrini, Alessandro Inzerilli, Leonardo Lanzi, Mario Maiorino, Laura Moretti, Carmine Piccolo, Roberto Puccinelli, Andrea Ranaldi, Fabio Romani, Gianluigi Spinaci, Sandro Torlontano, Enrico Venuto, Luisa Verdoliva

Progetto grafico: Carlo Volpe **Impaginazione:** Carlo Volpe, Marta Mieli

Editore: Consortium GARR, Via dei Tizii, 6 - 00185 Roma

---

tel 06 49622000 info@garr.it www.garr.it
ReteGARR

Stampa: Tipografia Graffietti Stampati snc, S.S. Umbro Casentinese Km 4.500, 00127 Montefiascone (VT)
Tiratura: 8.000 copie **Chiuso in redazione:** 18 dicembre 2024

Il filo

Claudia Battista

Direttrice
Consortium GARR

Cari lettori e lettrici,

Il tema centrale di questo numero è la **sicurezza**, declinata in molteplici ambiti: dal ruolo delle nuove normative europee, alla protezione di dati e infrastrutture con monitoraggio continuo e rilevamento proattivo delle minacce, passando per l'attenzione alla catena degli approvvigionamenti (o supply chain) e alla ricerca su tecniche di intelligenza artificiale per identificare falsi contenuti video o immagini (deepfake).

L'attenzione alla **supply chain** è diventata cruciale: la vulnerabilità di un singolo fornitore, infatti, può compromettere intere infrastrutture, come dimostrato da episodi globali come il caso SolarWinds e il recente attacco a Ivanti. La **normativa europea**, con la direttiva NIS2 e il Cybersecurity Act, punta a rafforzare la protezione lungo tutta la catena, introducendo standard più rigorosi e misure proattive per mitigare i rischi. In questo contesto, la crescente diffusione di **immagini sintetiche e contenuti manipolati** creati con l'AI generativa rappresenta una nuova sfida che aumenta il rischio di disinformazione e frodi. In tutto ciò il fattore umano resta cruciale, sia come punto debole della sicurezza sia come opportunità per rafforzare la resilienza e per questo è fondamentale accrescere la consapevolezza e le competenze.

Riguardo le infrastrutture, il **Piano Triennale di GARR** pone l'accento su un **ecosistema digitale indipendente e sostenibile**, capace di supportare la ricerca italiana ed europea. La visione include interventi su scala nazionale e internazionale, come lo sviluppo di reti sottomarine nel Mediterraneo e connessioni ad altissime prestazioni per centri di supercalcolo. Queste infrastrutture non solo migliorano la capacità di elaborazione dei dati, ma abilitano applicazioni scientifiche avanzate, dal sensing su fibra ottica alla distribuzione di chiavi quantistiche.

Grazie a tecnologie come **LoLa**, poi, dimostriamo ancora una volta come sia possibile abbattere le barriere geografiche, creando un ponte tra istituzioni culturali e accademiche come quello tra il Conservatorio Tartini di Trieste e la Academy of Arts di Novi Sad in Serbia.

Un ponte per le competenze, invece, è quello costruito dal progetto **Skills4EOSC**, coordinato da GARR, che sta creando una rete europea di competence centre per sviluppare **competenze nell'Open Science e nella gestione FAIR dei dati**. Questi centri agiscono come nodi chiave per la formazione e la condivisione di buone pratiche, sostenendo una visione unitaria e inclusiva per la scienza aperta in Europa.

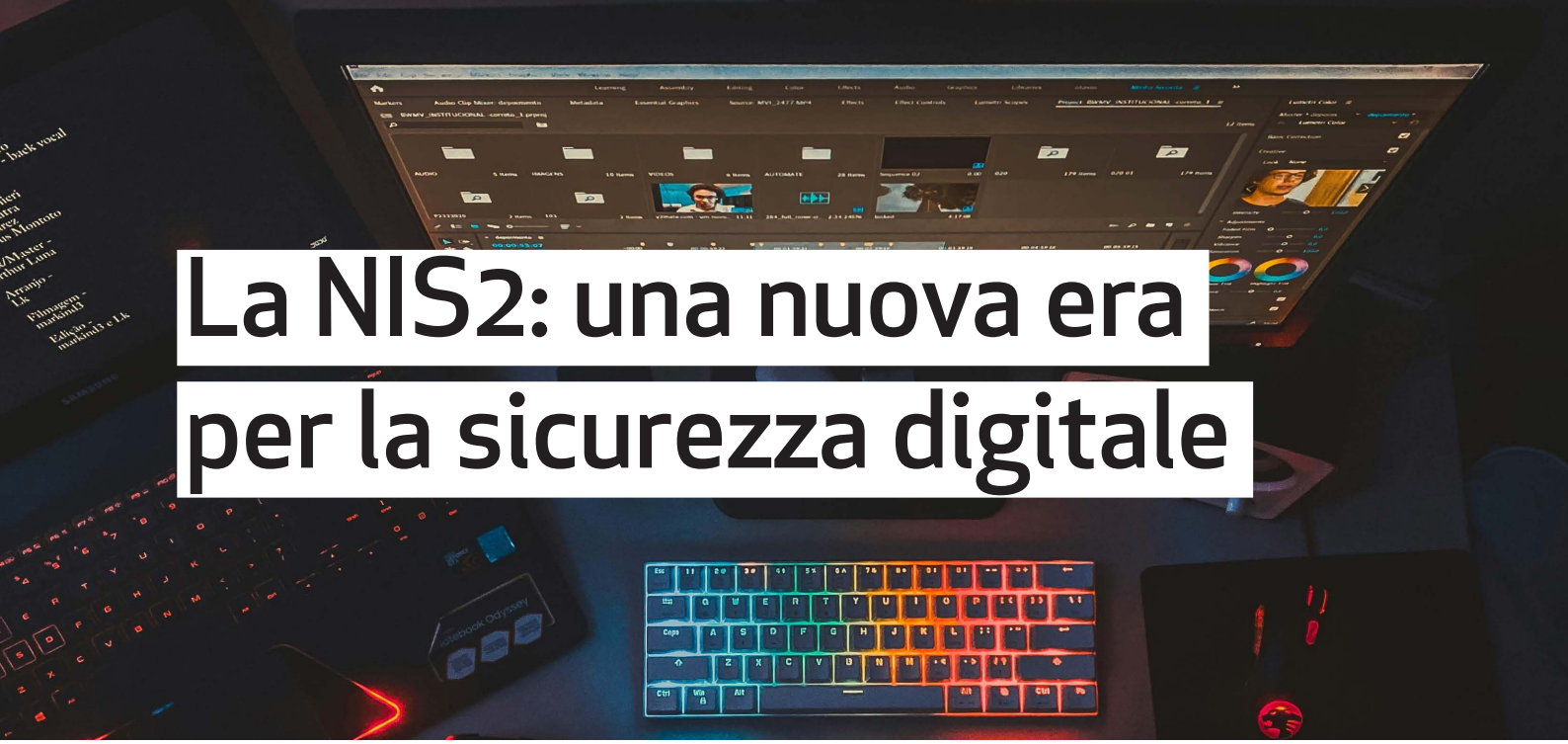
Sul tema dell'autonomia digitale e la **capacità della comunità della ricerca di produrre innovazione**, Massimo Carboni, CTO di GARR, sottolinea l'importanza di essere protagonisti dello sviluppo delle nuove tecnologie dell'Intelligenza Artificiale, in modo da sfruttarne il valore senza però delegare il potere decisionale ai giganti tecnologici che dominano il mercato.

E sempre riguardo la **sovranità tecnologica**, il dibattito sul prossimo Programma Quadro europeo FP10 ci invita a riflettere sull'importanza della ricerca e innovazione come motori della competitività europea.

Questo e molto altro dalla rete nazionale della ricerca e dell'istruzione.

Buona lettura!

In questo numero



La NIS2: una nuova era per la sicurezza digitale

Regole più chiare, obiettivi ambiziosi e opportunità strategiche per proteggere dati e infrastrutture

di Erika Trotto

Al Workshop GARR 2024, la sessione "Sicurezza: nuove regole e opportunità", moderata da Leonardo Lanzi, ha fatto luce sulle novità normative in arrivo in ambito cybersecurity. Al centro dell'attenzione, la direttiva europea NIS2, destinata a trasformare la protezione delle infrastrutture critiche e dei dati sensibili, anche in ambito accademico e di ricerca.

La direttiva NIS2 rappresenta un punto di svolta per il rafforzamento della cybersicurezza in Europa. Con il Decreto Legislativo 138/2024, il campo di applicazione è stato esteso a 18 settori strategici, tra cui energia, trasporti, sanità, infrastrutture digitali e pubblica amministrazione. Gli enti coinvolti saranno classificati in due categorie: essenziali e importanti, in base a criteri oggettivi. Le nuove normative introducono obblighi proporzionati al livello di rischio, supportati da misure flessibili e adattabili, fondate su un'attenta analisi delle minacce. Tra gli obiettivi principali figurano una gestione avanzata del rischio informatico, che include la protezione della catena di approvvigionamento e l'adozione di misure di sicurezza calibrate sui profili di rischio. A partire dal 2026, la direttiva prevede la notifica obbligatoria degli incidenti significativi entro 24 ore, seguita da un rapporto dettagliato entro 72 ore. L'Agenzia per la Cybersicurezza Nazionale (ACN) sarà incaricata di definire le misure di sicurezza, elaborando specifiche linee guida per la protezione della supply chain e garantendo un approccio flessibile e su misura per le diverse organizzazioni.

Basta un solo anello debole per rendere insicura tutta la catena. Un singolo punto di attacco può propagare l'infezione a tutti gli altri anelli, mettendo a rischio intere infrastrutture. La sicurezza della supply chain diventa quindi centrale: contratti specifici con i fornitori, valutazioni periodiche e processi di risposta agli incidenti condivisi sono strumenti essenziali per mitigare i rischi.

Questo ampio aggiornamento normativo sta generando un impatto diretto anche sul modo in cui le organizzazioni affrontano la sicurezza informatica. **Luca Carbone**, dirigente tecnologo dell'Istituto Nazionale di Fisica Nucleare (INFN), durante il workshop ha evidenziato la crescente **"bulimia normativa"** che caratterizza il settore. "La sicurezza informatica non è mai stata così complessa", ha dichiarato Carbone, sottolineando come la NIS2 e la Legge 90/2024 stiano aumentando la difficoltà di gestione della protezione digitale. In particolare, il ruolo del management è un fattore molto importante nella definizione delle misure di sicurezza. L'INFN ha avviato da tempo un processo strutturato istituendo, già qualche anno fa, il Nucleo di Cybersecurity (NuCS), che coordina attività tra le sue 25 strutture e comprende gruppi di lavoro su protezione, monitoraggio, risposta agli incidenti e un Security Operation Center (SOC) centrale. Un audit interno indipendente garantisce la compliance normativa, mentre procedure dettagliate permettono la gestione delle notifiche di incidenti significativi, coinvolgendo lo CSIRT-INFN come punto di contatto con le autorità e con GARR-CERT. Carbone ha inoltre sottolineato l'importanza della formazione, del dialogo con gli uffici legali e della partecipazione a tavoli

> La direttiva NIS2 rappresenta un punto di svolta per il rafforzamento della cybersicurezza in Europa

settoriali per sviluppare soluzioni condivise.

Riguardo alla necessità di avere un approccio graduale nell'adozione della NIS2, **Andrea Ranaldi**, sistemista e sviluppatore presso ISPRA, che ha descritto il percorso intrapreso da ISPRA per approcciarsi alla direttiva NIS2 (adottata con il DL 138/2024) e alle leggi correlate, come la Legge 90/2024. Ha parlato della necessità di un approccio graduale nell'adozione della NIS2, evidenziando come gli approcci top-down non considerino le specificità delle organizzazioni. "La sicurezza informatica non è una soluzione preconfezionata, ma un processo continuo", ha dichiarato, suggerendo che le organizzazioni si evolvano passo dopo passo per adattarsi alla nuova normativa. ISPRA, infatti, ha adottato un approccio incrementale, simile al sistema Kanban, che suddivide le attività in obiettivi progressivi, per garantire che ogni fase della conformità venga gestita in modo efficiente. Ranaldi ha inoltre sottolineato l'importanza della creazione di una mappa delle risorse per identificare rischi e responsabilità, uno strumento fondamentale per la gestione delle minacce.

Enrico Venuto, coordinatore della sicurezza informatica del Politecnico di Torino, ha partecipato alla discussione introducendo il concetto di **distributed accountability**. "La sicurezza informatica non è solo una questione che riguarda il nucleo di sicurezza IT di ateneo, ma una responsabilità di tutti i centri ed i dipartimenti", ha dichiarato Venuto, spiegando come il Politecnico abbia creato una rete di referenti IT nei dipartimenti cui affidare la gestione della sicurezza dei propri asset e dei propri servizi, anche attraverso l'accesso con credenziali dedicate ad un sistema di gestione della vulnerabilità. Questo approccio responsabilizza, diminuisce i tempi di risposta e riduce il carico sul team centrale di cybersecurity, che può concentrarsi su attività di coordinamento e monitoraggio. Venuto ha anche evidenziato l'importanza della formazione continua per gli operatori di sicurezza, poiché solo un aggiornamento costante può garantire una risposta efficace alle sfide moderne.

L'importanza di un approccio proattivo nell'implementazione delle normative è stata evidenziata dall'amministratore delegato di IPS S.p.A., **Fabio Romani**, che ha presentato il **primo Laboratorio accreditato di prova (LAP) per la cybersicurezza nazionale**, realizzato da IPS, fornitore globale di soluzioni di Cyber Intelligence con oltre 30 anni di esperienza nel mercato high-tech. "La cybersecurity è un investimento, non un costo", ha affermato Romani, ribadendo che il LAP rappresenta una risorsa essenziale per garantire la sicurezza delle infrastrutture critiche. Il laboratorio, che opera sotto la direzione del Centro di Valutazione e Certificazione Nazionale (CVCN), svolge attività fondamentali di test di intrusione e analisi di vulnerabilità, con l'obiettivo di verificare la robustezza dei sistemi. Romani ha anche parlato delle necessità economiche extra che derivano dall'adeguamento alle normative, un processo che impone importanti investimenti che dovrebbero essere condivisi tra governo, enti pubblici, fornitori di tecnologia e cittadini. Ha concluso ribadendo l'importanza di un approccio proattivo nell'implementazione delle normative, invitando tutti a contribuire con piccoli ma determinanti passi individuali per conseguire obiettivi strategici comuni, come l'autonomia tecnologica e la resilienza nazionale.

È importante la formazione continua per gli operatori di sicurezza, poiché solo un aggiornamento costante può garantire una risposta efficace alle sfide moderne

NIS2 e GDPR: un'alleanza per proteggere i dati personali

La NIS2 e il GDPR si integrano nella protezione dei dati. Sebbene abbiano obiettivi distinti, **Roberto Puccinelli**, DPO del CNR ha messo in luce come le due normative condividano un approccio basato sul rischio. "Una solida cybersecurity è la base per garantire la protezione dei dati personali", ha affermato Puccinelli. L'approccio integrato tra il responsabile della sicurezza informatica (CISO) e il responsabile della protezione dati (RPD) è fondamentale per evitare sovrapposizioni di competenze e per promuovere un sistema sicuro. La collaborazione tra queste due figure è essenziale per ottimizzare la gestione delle risorse e migliorare la resilienza complessiva dell'organizzazione.

La sessione ha messo in evidenza l'importanza della collaborazione e della formazione per affrontare le sfide della NIS2. Questa direttiva rappresenta un cambiamento cruciale nel panorama della sicurezza informatica, con regole ambiziose e strumenti avanzati per proteggere dati e infrastrutture critiche. Tuttavia, il successo dipenderà dalla capacità di ogni attore di impegnarsi collettivamente, trasformando la sicurezza da obbligo tecnico a priorità strategica. Solo un approccio condiviso e strutturato potrà garantire la resilienza digitale necessaria per affrontare le minacce di un mondo sempre più connesso.

I protagonisti della sessione:
Andrea Ranaldi, Enrico Venuto, Fabio Romani, Luca Carbone, Roberto Puccinelli insieme al moderatore Leonardo Lanzi (GARR)

Guarda la sessione "Sicurezza: nuove regole e opportunità" del Workshop GARR 2024

Vero o falso? Come l'AI smaschera le immagini sintetiche

di Luisa Verdoliva
Università degli studi di Napoli Federico II

Distinguere tra ciò che è reale e ciò che è sintetico sta diventando una sfida cruciale per la sicurezza digitale, con l'avanzare delle tecnologie di intelligenza artificiale generativa. Ma quali sono i progressi, i limiti e le prospettive delle tecniche per riconoscere e attribuire le immagini sintetiche?

L'ascesa delle tecnologie di intelligenza artificiale generativa ha trasformato radicalmente la creazione di immagini e video digitali, portando il realismo a livelli mai raggiunti prima. Se da un lato tali innovazioni aprono nuove prospettive per settori come il cinema, la pubblicità e l'arte, dall'altro pongono rischi significativi legati all'uso improprio di contenuti manipolati. La crescente facilità con cui è possibile creare immagini e video falsi rende indispensabile sviluppare strumenti e tecniche per il loro riconoscimento.

L'AI generativa comprende una serie di tecniche che consentono la creazione automatica di contenuti digitali, come immagini, video, audio e testo, utilizzando modelli matematici. Tra le tecnologie principali in questo ambito ci sono **le reti generative avversarie (GAN) e i modelli di diffusione (DM)**. Le GAN funzionano grazie a due reti neurali che si sfidano tra loro: una genera immagini sintetiche, mentre l'altra cerca di distinguere quelle reali da quelle create artificialmente. Questo processo di "competizione" consente un miglioramento continuo della qualità delle immagini generate. I modelli di diffusione (DM), invece, agiscono come una forma di "rumore controllato", trasformando gradualmente un'immagine di rumore puro in un'immagine finale di alta qualità. Questi progressi hanno reso possibile la generazione di immagini ad alta risoluzione a partire da semplici descrizioni testuali, amplificando le possibilità creative e la flessibilità nella produzione di contenuti digitali.

Tuttavia, questa capacità di creare immagini così realistiche comporta anche rischi significativi. Con l'accesso a software gratuiti e facili da usare, chiunque, anche un utente privo di competenze specifiche, può generare contenuti visivi falsificati. Queste immagini possono essere impiegate per scopi illeciti, come manipolare l'opinione pubblica, commettere frodi o diffondere disinformazione, con gravi conseguenze politiche, sociali ed economiche.

La sfida della ricerca: analisi dell'autenticità e identificazione della provenienza

Studi recenti hanno dimostrato che gli esseri umani non sono in grado di distinguere in modo affidabile tra le immagini reali e quelle generate artificialmente: l'accuratezza media è solo del 50% per osservatori non addestrati e del 60% per quelli addestrati. La ricerca si concentra sulla creazione di strumenti automatici per il riconoscimento dei deepfake, perseguendo due obiettivi leggermente diversi: **l'analisi dell'autenticità** e **l'identificazione della provenienza**. Il primo obiettivo si concentra sul determinare la probabilità che un'immagine sia sintetica, fornendo un "punteggio di integrità": più è alto, più è verosimile che l'immagine sia stata generata

Gli studi dimostrano che le persone non sono in grado di riconoscere immagini reali da quelle false. L'accuratezza media è solo del 50%

Guarda il webinar "Synthetic Media Verification in the Era of Generative AI" a cura di Luisa Verdoliva in occasione del Cyber Security Month 2024

Luisa Verdoliva è professoressa ordinaria presso l'Università Federico II di Napoli, dove insegna "Elaborazione di Segnali Multimediali" e "Image and Video Processing for Autonomous Driving". La sua attività di ricerca riguarda l'elaborazione di segnali, e in particolare la rivelazione e localizzazione di contraffazioni in immagini e video.

artificialmente. L'identificazione della provenienza, invece, si concentra sul riconoscimento dello specifico modello di intelligenza artificiale impiegato per generare l'immagine.

Uno degli approcci più usati per rilevare contenuti manipolati o generati artificialmente si basa sull'analisi degli artefatti forensi, ossia delle tracce lasciate dal processo di generazione, che possono essere utilizzate per identificare la natura sintetica di un'immagine. Questi artefatti possono essere di alto livello, come asimmetrie nei volti, incongruenze nelle ombre o nella prospettiva, o di basso livello, come anomalie nel rumore digitale o nei pattern di compressione. In passato, gli artefatti visibili erano sufficienti per rilevare contenuti falsificati, ma con l'evoluzione delle tecniche di AI, molte di queste anomalie sono state eliminate, rendendo più difficile il riconoscimento visivo.

Un'altra tecnica si basa sull'uso del PRNU, una sorta di impronta digitale che ogni fotocamera lascia nelle immagini che scatta. Questa firma è causata da piccole imperfezioni nel sensore di acquisizione ed è unica per ogni singola fotocamera, per cui può essere utilizzata per capire se un'immagine proviene da una fotocamera specifica. Quando un'immagine viene modificata, questa "impronta" cambia, e quindi è possibile rilevare una possibile manipolazione.

Nonostante i notevoli progressi nel riconoscimento delle immagini sintetiche, i metodi attuali presentano ancora diversi limiti. In primo luogo, la robustezza dei classificatori rappresenta un punto fondamentale. Gli strumenti devono essere infatti in grado di resistere a manipolazioni, come la compressione delle immagini, che potrebbero ridurre le tracce di falsificazione. Inoltre, l**a generalizzazione dei metodi è un altro problema critico**. I classificatori addestrati su un particolare tipo di generatore di immagini spesso non funzionano altrettanto bene con nuovi generatori che utilizzano tecniche diverse, riducendone così l'efficacia.

Con l'accesso a software gratuiti e facili da usare, chiunque, anche un utente privo di competenze specifiche, può generare contenuti visivi falsificati

Per risolvere questi limiti, è importante che nella fase di addestramento si includano esempi di immagini provenienti da generatori molto diversi e che il classificatore si possa facilmente adattare a contesti vari in modo da aumentarne la robustezza. Un approccio promettente è l'utilizzo di metodi multimodali, che combinano analisi di immagini, video e audio per aumentare la precisione dei classificatori. Ad esempio, l'uso simultaneo di immagini e audio può essere utile per identificare i deepfake video, che sono diventati una minaccia crescente grazie alla loro capacità di ingannare gli spettatori.

Le implicazioni di sicurezza e le direzioni future

I progressi nell'AI generativa pongono sfide significative per la sicurezza informatica. Le minacce derivanti dall'uso illecito dei contenuti sintetici richiedono strumenti sempre più sofisticati per proteggere l'integrità delle informazioni. **Un'area di ricerca promettente è l'identificazione della provenienza delle immagini sintetiche**, che consente di risalire al modello di AI utilizzato. Infatti, ogni modello lascia un'impronta digitale, un pattern unico che può essere usato per tracciare la provenienza dell'immagine. Tuttavia, questi metodi devono affrontare diverse sfide, come il fatto che nuovi modelli generativi vengono proposti ogni giorno oppure la presenza di possibili attacchi avversari, come **l'inserimento di rumore artificiale nell'immagine allo scopo di ingannare il classificatore**.

Un approccio promettente è l'utilizzo di metodi multimodali che combinano analisi di immagini, video e audio per aumentare la precisione dei classificatori

È bene osservare che l'integrazione di tecniche come l'analisi biometrica e i modelli linguistici pre-addestrati può contribuire a distinguere meglio i contenuti reali da quelli falsificati, ma richiede aggiornamenti continui per rimanere efficaci.
La ricerca in corso nel campo dell'analisi dell'autenticità delle immagini sintetiche è cruciale per garantire una protezione adeguata contro l'uso improprio di questi contenuti e per promuovere un utilizzo consapevole delle tecnologie AI.

La **collaborazione tra ricercatori, istituzioni e aziende sarà fondamentale** per affrontare le sfide future e garantire che queste tecnologie vengano utilizzate in modo sicuro e responsabile.

La comunità GARR protagonista della campagna europea per la sicurezza di GÉANT

di Elis Bertazzon

Ottobre è stato un mese all'insegna della sicurezza informatica grazie alla campagna Cybersecurity Month 2024 (CSM24) organizzata da GÉANT, la rete europea per la ricerca e l'istruzione. Focalizzata sul tema del social engineering, la campagna ha invitato utenti e organizzazioni a riflettere sull'importanza di difendersi dai rischi informatici secondo il mantra: "È il tuo cervello la prima linea di difesa". GARR insieme alla comunità italiana della ricerca, ha partecipato attivamente alla campagna, contribuendo sia alla sua ideazione che alla condivisione di contenuti e iniziative, in sinergia con le altre reti europee.

La minaccia del social engineering

Tra i temi principali della campagna il primo posto è occupato dall social engineering, o ingegneria sociale, che si riferisce alle tecniche psicologiche usate dai criminali per manipolare le persone e indurle a compiere azioni dannose, come rivelare informazioni sensibili. La campagna ha posto l'attenzione su truffe comuni come il CEO fraud (truffa dell'amministratore delegato), le romance scams (truffe su base sentimentale), il phishing (email e messaggi malevoli scritti appositamente con lo scopo di spingere le vittime a cadere nella trappola) e il tailgating (accesso non autorizzato attraverso l'inganno), spiegando come queste tecniche sfruttino fattori quali l'autorità, la reciprocità o la distrazione.

I contributi di GARR e della comunità

GARR ed esponenti della comunità hanno partecipato alla creazione di materiali didattici e informativi, contribuendo al successo della campagna. Tra le iniziative, sono stati apprezzati:

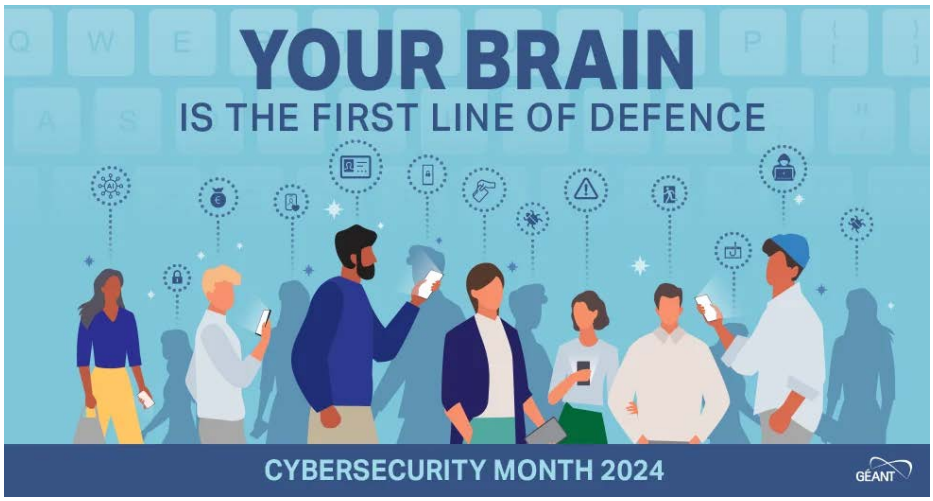
Video divulgativi: una serie di brevi video educativi ha coperto temi come l'uso sicuro degli smartphone, i rischi del Wi-Fi pubblico e l'importanza di gestori di password.

Articoli: numerosi i contributi per la campagna. Anche qui GARR e la comunità italiana della ricerca e dell'istruzione hanno partecipato attivamente. GARR ha condiviso l'articolo "*Errare humanum est. But what about everything else*?" di Simona Venuti (GARR-CERT) che si domanda cosa accada quando le macchine, ritenute sicure, hanno un abbaglio compromettendo la sicurezza. Inoltre con l'articolo "*Cybersecurity: where do universities and research stand*?" Carlo Volpe (GARR) presenta una panoramica delle azioni di cybersecurity intraprese da alcuni atenei italiani, così come sono state raccontate durante la Conferenza GARR dello scorso giugno.

> GARR ed esponenti della comunità hanno partecipato alla creazione di materiali didattici e informativi, contribuendo al successo della campagna

Dall'Università di Messina, inoltre, Salvatore Todaro ha scritto l'articolo "*The Importance of Cybersecurity: a cost for everyone*", che si concentra sull'impatto di una scarsa cybersicurezza, sottolineando come gli effetti di un attacco informatico finiscono con avere un impatto che dall'individuo si estende su tutta la società. Dal Politecnico di Torino, invece, Enrico Venuto ha contribuito con un articolo che mette in discussione la visione dell'utente come "l'anello debole" della catena di sicurezza, ricordando che è proprio attraverso la consapevolezza che l'utente può reagire ed intervenire di fronte a delle minacce che, a volte, di tecnologico hanno ben poco.

Webinar: seminari online tenuti da esperti, tra cui rappresentanti della comunità GARR, hanno affrontato questioni cruciali, come il ruolo dell'AI nella sicurezza e l'analisi del social engineering. Tra questi, spicca il contributo della professoressa Verdoliva dell'Università degli



L'immagine grafica e il titolo ideati da GÉANT per l'edizione 2024 del Cybersecurity Month

Studi di Napoli Federico II "*La verifica dei media sintetici nell'era dell'intelligenza artificiale generativa: cosa funziona e cosa ancora non esiste*".

Materiali condivisi: la vera novità di quest'anno è la creazione di un repository aperto a tutti e contenente i materiali messi a disposizione da GÉANT e dalle altre reti della ricerca europee. Blog, interviste, linee guida, video, giochi, materiale di promozione...le risorse disponibili sul Security Awareness Resources Hub sono davvero molte e sono destinate a crescere nel tempo in quanto ogni organizzazione può autonomamente mettere a disposizione di tutti i suoi materiali.

sia al lavoro che nella sfera privata" dice **Simona Venuti**, GARR CERT e membro del cybersecurity awareness group di GÉANT, "è per questo che iniziative come il mese europeo della cybersecurity sono così importanti. Vedere la comunità italiana dell'istruzione e della ricerca partecipare con entusiasmo a questa edizione è la prova di quanto sia sentita la necessità di diffondere questa consapevolezza. Sono certa che l'impegno crescerà sempre di più e spero che gli esperti di sicurezza italiani nel mondo della ricerca continuino a dare il loro prezioso contributo."

→ connect.geant.org/csm24

→ security.geant.org/security-awareness-resources-hub

La vera novità è la creazione di un repository aperto a tutti e contenente i materiali messi a disposizione da GÉANT e dalle altre reti della ricerca europee

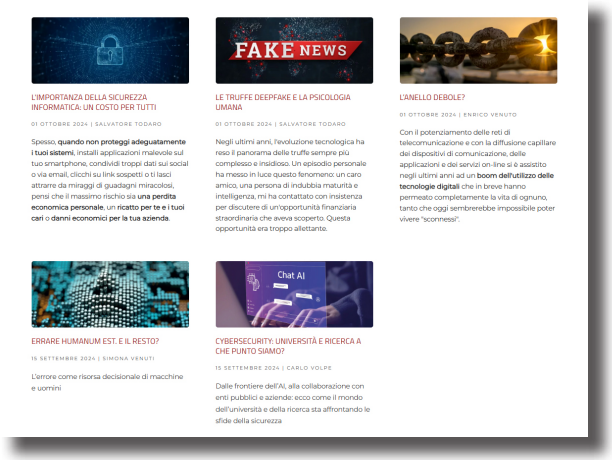
Una narrazione innovativa: Jake Doubt

Tra i contenuti di punta, la serie animata Jake Doubt ha reso il tema della sicurezza informatica accessibile e coinvolgente. Il protagonista, responsabile della sicurezza in una università fittizia, ha affrontato casi di social engineering in episodi narrati in stile true crime, combinando humor e sensibilizzazione. La serie, sottotitolata in italiano, è disponibile su **https://connect.geant.org/csm24**.

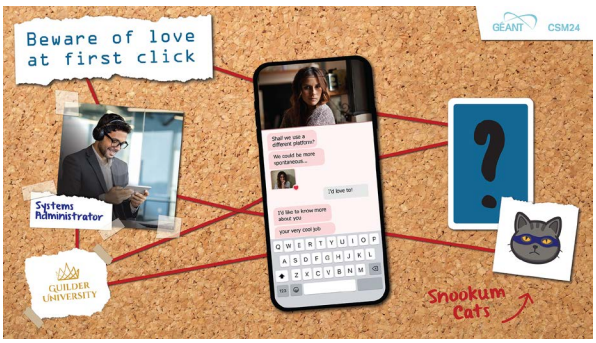
Uno sguardo al futuro

CSM24 si è conclusa, ma la consapevolezza della sicurezza informatica resta al centro delle attività di GÉANT e GARR. A livello europeo, il prossimo appuntamento sono i Security Days previsti a Praga dall'8 al 10 aprile 2025. Per quanto riguarda GARR, le attività sono pubblicate sul portale Learning GARR e, oltre alle attività online, sono previsti corsi interattivi sulla cyberdefence nei giorni precedenti alla conferenza e ai workshop annuali.

"La cyber-consapevolezza dovrebbe raggiungere tutti, perché il digitale ormai fa parte della nostra vita,



Guarda i video della miniserie e leggi gli articoli della comunità GARR sulla pagina dedicata al Cybersecurity Month su garrnews.it



A Trieste l'alta formazione musicale si fa internazionale

Al Conservatorio Tartini il primo diplomato al Joint Master Degree in Guitar/Performing Arts

di Marta Mieli

Trieste si distingue come centro di eccellenza europeo nell'Alta Formazione musicale grazie al Conservatorio Tartini, promotoare di iniziative innovative come il Joint Master Degree in Guitar/Performing Arts, un diploma accademico di II livello in chitarra. Questo programma biennale, realizzato in collaborazione con l'Academy of Arts di Novi Sad (Serbia), ha celebrato un **importante traguardo con il primo diplomato, Mihajlo Dordevic,** che il 25 ottobre scorso ha ottenuto il titolo congiunto con il massimo dei voti e la lode. A presiedere la Commissione d'esame, il direttore del Conservatorio Tartini, Sandro Torlontano con tre docenti del Conservatorio di Trieste, Stefano Bonetti, Matteo Rigotti e Andrea Vettoretti, insieme a tre docenti dell'Accademia di Novi Sad: Zoran Krajisnik, Petar Popovic e Srdan Tosic.

Ad oggi, si tratta del primo corso internazionale di Alta Formazione Musicale (AFAM) con titolo congiunto, tuttora l'unico in Italia autorizzato dal MUR (Ministero italiano dell'Università e della Ricerca).

"Pur essendo prassi diffusa per le Università" spiega il direttore del Conservatorio Tartini, **Sandro Torlontano** "i Conservatori italiani ancora non potevano contare su un titolo di studio congiunto internazionale rilasciato dal Ministero della Ricerca".

Questo traguardo è frutto di una collaborazione intercorsa negli anni fra il Conservatorio Tartini e la Academy of Arts di Novi Sad (Serbia), ci spiega il direttore, "una collaborazione portata avanti con reciproca soddisfazione, attraverso decine di mobilità docenti e studenti scambiate all'interno dei programmi Erasmus, oltre che per gli eventi congiuntamente organizzati nell'ambito del Protocollo di Cooperazione culturale tra Italia e Serbia (legge 212/2012), che ha dato vita ad un'articolata sequenza di iniziative per la formazione e fruizione musicale".

Questo progetto è stato reso possibile anche grazie all'uso della tecnologia **LoLa**, sviluppata dal Conservatorio Tartini insieme a GARR, per garantire una trasmissione audio-video a bassa latenza e alta qualità. Questo sistema ha permesso di **gestire esami finali in modo del tutto nuovo** e di consolidare una collaborazione tecnologica che rafforza ulteriormente il prestigio di questa iniziativa internazionale.

Approfondiremo ora gli elementi più significativi di questo progetto attraverso alcune domande al Direttore del Conservatorio.

> Questo progetto è stato reso possibile grazie all'uso della tecnologia LoLa, sviluppata dal Conservatorio Tartini insieme a GARR, per garantire una trasmissione audio-video a bassa latenza e alta qualità

Come la tecnologia può facilitare la collaborazione tra istituzioni musicali geograficamente distanti?

Con l'ausilio di LoLa, l'innovativo sistema di trasmissione audio/video a bassa latenza e alta qualità per l'esecuzione e l'interazione musicale in rete si possono abbattere le distanze spazio-temporali tra le istituzioni musicali. Il sistema consente infatti di trasmettere e ricevere il suono ed il video senza ritardo percepibile e gli esecutori possono quindi interagire come fossero nello stesso luogo, cioè in tempo reale. Questo è fondamentale sia in caso di una lezione che di una prova a distanza con

esecutori che si trovano in diverse istituzioni musicali anche a migliaia di chilometri di distanza.

In che modo le tecnologie digitali stanno trasformando l'insegnamento e l'apprendimento della musica?

Oltre ai sistemi di rete per la trasmissione in tempo reale dei dati audiovisivi, le tecnologie digitali hanno oggi un ruolo importante in altri ambiti dell'insegnamento della musica. Per esempio la **videoscrittura musicale**, ovvero la possibilità di scrivere musica nonché di farla eseguire dal computer mediante software dedicati, fornisce un ausilio innovativo di enorme rilevanza per chi studia composizione. Mediante le tecnologie digitali si possono inoltre realizzare ambienti software di apprendimento della musica, che permettono allo studente di esercitare l'orecchio musicale in forma interattiva e autonoma.

LoLa è un software concesso in licenza gratuita a tutte le istituzioni musicali che ne vogliano fare un uso accademico o didattico senza scopo di lucro

Come vengono gestite le differenze infrastrutturali tra paesi diversi in progetti internazionali?

LoLa è un software concesso in licenza gratuita a tutte le istituzioni musicali che ne vogliano fare un uso accademico o didattico senza scopo di lucro. In tutti gli altri casi, può essere rilasciata una licenza shareware per supportare degli specifici progetti. Il Conservatorio Tartini detiene i diritti di proprietà intellettuale e il GARR funge da suo agente e rappresentante. Dal punto di vista hardware è sufficiente che ogni istituzione si doti delle attrezzature suggerite sul sito di LoLa; è anche necesario che l'istituzione sia connessa alla propria reta nazionale per l'educazione e la ricerca (NREN).

Un'immagine del giorno dell'esame finale del primo diplomato Mihajlo Dordevic. Nella foto oltre al giovane laureato: Sandro Torlontano, Direttore del Conservatorio Tartini, i docenti di chitarra del Conservatorio di Trieste Matteo Rigotti e Andrea Vettoretti e online i tre docenti dell'Accademia di Novi Sad: Zoran Krajisnik, Petar Popovic e Srdan Tosic.

Qual è il ruolo delle reti di ricerca come GARR nello sviluppo di soluzioni tecnologiche avanzate?

Il GARR, come tutte le altre reti di ricerca nazionali degli altri stati, hanno il ruolo fondamentale di garantire e gestire di volta in volta l'infrastruttura di rete per la trasmissione con latenza minima dei dati di LoLa.

Con questo importante progetto, riconosciuto dal MUR nell'estate 2021 e successivamente dal Ministero serbo nel 2022, Trieste si conferma quindi capitale dell'Alta Formazione musicale, anche a livello europeo. Attraverso il Joint Master Degree, infatti, ogni biennio quattro studenti selezionati dalle due istituzioni hanno la possibilità di completare il ciclo formativo attraverso una annualità svolta a Trieste e una a Novi Sad, con il coinvolgimento formativo di una ventina di docenti tra le due istituzioni, sapendo di poter contare sul pieno riconoscimento del titolo acquisito sia in Italia che in Serbia. La tecnologia LoLa diviene a questo punto una componente essenziale del percorso di formazione, permettendo agli studenti di "essere contemporaneamente in due istituzioni nello stesso istante".

→garr.it/lola

Cos'è LoLa

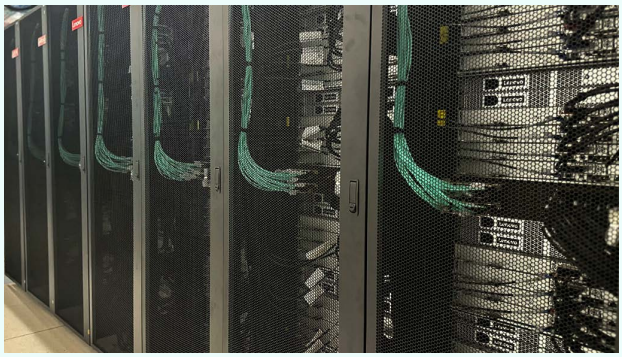
LoLa (Low Latency AV streaming system) è un sistema audio/video ultra HD sviluppato da **GARR** e dal **Conservatorio Tartini di Trieste**. Questa tecnologia permette performance musicali in tempo reale tra artisti situati in luoghi diversi, connessi attraverso reti della ricerca come GÉANT. Il sistema converte i segnali audio-video mantenendone l'alta qualità e li trasmette attraverso la rete in fibra ottica, consentendo **esibizioni tra luoghi distanti fino a 3.000 km** con una **latenza inferiore ai 30-35 ms**.

Il sistema LoLa permette, ad esempio, di tenere masterclass e lezioni di musica a distanza, realizzare performance con artisti e pubblico distribuiti geograficamente e aumentare le possibilità di prove prima dei concerti in presenza. Il sistema elimina le distanze negli eventi dal vivo, rendendo le arti performative in tempo reale più sostenibili e aprendo nuove opportunità nel campo delle network performing arts, dove l'arte si fonde con la tecnologia di rete avanzata. Il progetto di realizzazione di LoLa è iniziato nel 2005, dopo una masterclass di viola tra Pisa e Miami, e ha debuttato pubblicamente nel 2010 con un concerto tra Trieste e Parigi.

Oggi il sistema è utilizzato da numerose istituzioni collegate alle reti della ricerca in tutto il mondo.

La ricerca comunica

a cura degli uffici stampa degli enti di ricerca



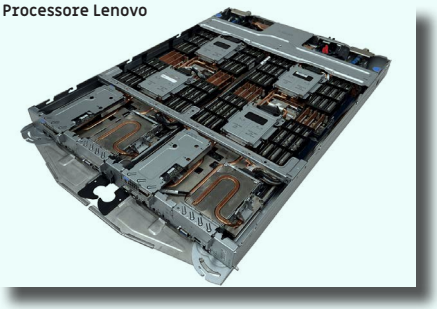
ENEA

Nuovo supercomputer per la ricerca sull'energia da fusione nucleare

ENEA, Cineca ed EUROfusion hanno scelto il supercomputer Lenovo per accelerare in Italia la ricerca sulla fusione nucleare. Il nuovo sistema si chiamerà Pitagora ed entrerà a far parte del Tecnopolo di Bologna, diventando uno tra i primi 50 supercalcolatori al mondo. Dedicato alla simulazione numerica della fisica del plasma e all'analisi strutturale di materiali avanzati per la fusione nucleare, sarà in grado di effettuare circa 55 milioni di miliardi di operazioni al secondo riducendo del 15% il consumo di elettricità grazie al sistema di raffreddamento Lenovo Neptune™ Direct Water-Cooling.

"I ricercatori avranno a disposizione un'infrastruttura di calcolo innovativa, dotata delle più recenti librerie software e ambienti di sviluppo", spiega Giovanni Ponti, responsabile della Divisione Sviluppo dei Sistemi per l'Informatica e l'ICT dell'ENEA, "confermando il nostro posizionamento nella progettazione e configurazione di infrastrutture di calcolo avanzato per la comunità scientifica".

→ www.enea.it



Processore Lenovo

INGV

Una storia lunga 25 anni alla scoperta delle Scienze della Terra

L'Istituto Nazionale di Geofisica e Vulcanologia (INGV), istituito il 29 settembre del 1999, dalla fusione di cinque enti di ricerca, ha festeggiato i primi venticinque anni d'attività.

L'INGV è un istituto di rilievo internazionale, svolge attività di sorveglianza sismica e vulcanica sul territorio nazionale, progetta e coordina programmi internazionali sulle geoscienze a 360 gradi, sempre in prima linea per la divulgazione, la formazione ed una corretta informazione.

L'anno giubilare si è aperto con la celebrazione nella Sala Koch del Senato della Repubblica, a cui hanno partecipato alcune tra le più alte personalità del panorama scientifico e politico del Paese.

In occasione del venticinquennale, l'Istituto ha promosso varie attività su tutto il territorio nazionale che andranno avanti anche nel 2025. Seminari, incontri nelle scuole, visite guidate all'interno delle proprie strutture ed eventi volti a valorizzare il contatto continuo e diretto con i cittadini, a testimonianza del costante impegno dell'INGV nella diffusione presso il pubblico delle Scienze della Terra.

→ https://25anni.ingv.it

Un momento dell'incontro nella Sala Koch del Senato della Repubblica avvenuto lo scorso 7 ottobre 2024

CNR

Fabio Martinelli è il nuovo direttore dell'Istituto di calcolo e reti ad alte prestazioni

Ricercatore di primo piano nel campo della cybersecurity, e dal 2010 dirigente di ricerca del CNR, il nuovo direttore del CNR-ICAR ha dedicato la sua carriera allo sviluppo di soluzioni per la sicurezza, la fiducia e la privacy nei sistemi distribuiti.

Significativi e numerosi i successi a livello nazionale e internazionale e numerosi gli incarichi internazionali, tra questi quello di vicepresidente del consiglio dell'ECSO, partnership europea per la sicurezza informatica che comprende oltre 300 organizzazioni.

Con la nomina di Fabio Martinelli, il CNR-ICAR si prepara a una fase di crescita e innovazione, puntando a consolidare la sua eccellenza in un ampio ventaglio di campi di ricerca, che spazia dall'Intelligenza Artificiale ai Cyber Physical Systems, dalla Data Science fino al Quantum Computing.

→ www.cnr.it

Indipendente e sostenibile. Quale visione per la rete GARR?

Presentato il Piano Triennale della rete GARR con i principali obiettivi e azioni per rispondere alle sfide tecnologiche della comunità scientifica e accademica

di Carlo Volpe

Una maggiore capillarità per offrire un accesso equo alle risorse, l'indipendenza e l'ottimizzazione della rete per assicurarne la sostenibilità sono alcuni dei pilastri su cui si fonda la strategia GARR per i prossimi anni. Nel Piano Triennale 2025-27, approvato a dicembre, questi aspetti emergono, infatti, come elementi imprescindibili affinché GARR continui a far evolvere la rete in una piattaforma tecnologica all'avanguardia, capace di sostenere l'ecosistema scientifico e accademico italiano.
Abbiamo intervistato la **direttrice GARR**, **Claudia Battista**, per conoscere da vicino cosa ci aspetta nell'immediato futuro.

Come fare per raggiungere questi obiettivi così ambiziosi?

I nostri obiettivi sono certamente sfidanti, ma in linea con le nostre potenzialità e con i valori che ci caratterizzano profondamente. Le azioni che metteremo in campo sono incentrate sul potenziamento della capillarità della rete fisica, sulla gestione flessibile e programmabile delle risorse di rete, sul mantenimento di un ambiente aperto e non vincolato a specifici fornitori.

Mantenere e rafforzare queste caratteristiche, che ci contraddistinguono da sempre, sarà fondamentale per assicurare che la rete GARR rimanga una risorsa di centrale importanza per la comunità dei suoi utilizzatori e un catalizzatore di innovazione.

I nostri obiettivi sono certamente sfidanti, ma in linea con le nostre potenzialità e con i valori che ci caratterizzano

Una visione che non si limita all'Italia ma che è molto attenta agli scenari internazionali.

Per essere un punto di riferimento tecnologico è necessario essere parte integrante del sistema mondiale delle reti della ricerca e dell'istruzione (le cosiddette NREN). Non esistono confini nella ricerca e tutti i settori sono molto dinamici e interconnessi. In questo contesto, **GARR intende rafforzare la collaborazione per l'ampliamento della dorsale europea GÉANT e dei collegamenti intercontinentali**, quali elementi essenziali per le attività di ricerca della propria comunità.
Per noi e per i nostri utenti questo è un tratto distintivo e unico, rispetto a quanto sia possibile con altri operatori. Solo in questo sistema di reti della ricerca si può fare sperimentazione di frontiera, disponendo di fibra a livello nazionale e transfrontaliero, sia terrestre che sottomarina. Alcuni esempi sono l'utilizzo dei cavi come sensori distribuiti che permettono la rilevazione di terremoti, il monitoraggio ambientale e delle infrastrutture, nonché lo sviluppo di altre applicazioni scientifiche e tecnologie come quelle quantistiche.

Allo stesso modo, è molto importante essere in prima linea nelle iniziative italiane ed europee a supporto della evoluzione digitale come quella della **EuroHPC Joint Undertaking** per offrire un sistema avanzato di interconnessione ad altissime prestazioni (fino al Terabit al secondo) dei centri di supercalcolo di livello pre/exascale. Ma non solo, GARR continuerà ad essere coinvolto nelle operazioni che

hanno l'obiettivo di rafforzare la cooperazione tra infrastrutture di ricerca e infrastrutture di calcolo e dati e migliorarne la sostenibilità, l'accessibilità e la resilienza all'interno della European Research Area.

In che modo sarà rafforzata l'infrastruttura GARR?

La strategia prevede interventi su più fronti: sia sul territorio italiano che internazionale, con lo **sviluppo di Cross Border Fibers e di infrastrutture sottomarine**. In Italia, potenzieremo la rete GARR-T aumentandone la capillarità, la capacità e l'efficienza.

Allargando i confini, invece, lavoriamo per realizzare infrastrutture transfrontaliere con le vicine reti nazionali della ricerca, migliorando la resilienza delle reti e aprendo la strada all'utilizzo di tali infrastrutture anche per i servizi che vanno oltre il trasporto dei dati, i cosiddetti **non data service** come il trasporto di tempo/frequenza, la Distribuzione di Chiavi Quantistiche (QKD) e il supporto al Quantum Computing anche a livello internazionale.

Una particolare attenzione è riservata alle reti sottomarine, che sono sempre più strategiche, soprattutto nel Mediterraneo. Come già fatto per la connessione della Sardegna, collaboriamo con partner industriali e NREN per sfruttare i cavi sottomarini equipaggiati con tecnologie di nuova generazione anche per attività di ricerca molto promettenti come ad esempio il sensing su fibra ottica.

A livello nazionale, quale sarà l'impatto degli interventi finanziati nell'ambito del PNRR?

Le attività previste nei due progetti in cui GARR è coinvolto, TeRABIT e il Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing (ICSC), sono state condotte con un ritmo serrato in questi ultimi anni e ormai manca poco per il totale completamento che porterà interconnessioni ad alte prestazioni tra i data storage e i data centre per supportare applicazioni di High Throughput Computing (HTC) oltre che High Performance Computing (HPC).

Il 2025 vedrà la **piena realizzazione di due interventi rilevanti e strategici attesi da molto tempo in Sardegna e in Abruzzo**. Nel primo caso, avremo la messa in produzione della dorsale ottica sottomarina di 1.500 km, dell'anello regionale di 2.000 km di fibra terrestre accesa e di nuovi PoP ottici. Sarà incrementata drasticamente la connettività tra Cagliari, Sassari, Roma e Milano con servizi a 400 Gbps e l'interconnessione sia con la dorsale nazionale che con la rete europea GÉANT. In Abruzzo, invece, sarà operativa una tratta di 350 km di fibra ottica terrestre accesa tra L'Aquila e Pescara, per migliorare l'affidabilità dei collegamenti di importanti siti a carattere scientifico come i Laboratori Nazionali del Gran Sasso dell'INFN.

Ovviamente, oltre al raggiungimento del traguardo, una grande attenzione è rivolta al tema della **sostenibilità a lungo termine dell'infrastruttura** attraverso una scrupolosa attività di scouting tecnologico e un'ottimizzazione delle risorse.

Per gestire al meglio l'infrastruttura, è sempre più importante l'automazione. Quali azioni sono previste in questa direzione?

Si tratta di un aspetto cruciale per migliorare il controllo e l'efficienza della rete. Stiamo lavorando per introdurre progressivamente tecnologie e strumenti innovativi di automazione e programmazione che consentano una gestione dinamica in funzione del traffico. Sono previsti interventi mirati, come la realizzazione di sistemi di monitoraggio in tempo reale per rilevare anomalie, di diagnostica predittiva per prevenire guasti e di tecnologie per ottimizzare l'efficienza energetica. Saranno adottate piattaforme di gestione centralizzata, strumenti avanzati di visualizzazione e provisioning automatico per una risposta rapida alle esigenze degli utenti.

> Lavoriamo per introdurre tecnologie e strumenti innovativi di automazione e programmazione per gestire la rete in modo dinamico e dare risposte rapide alle esigenze degli utenti

Inoltre, si completerà lo sviluppo del sistema GAMON per il monitoraggio delle infrastrutture cloud e avvieremo una transizione verso piattaforme di virtualizzazione alternative, incluse quelle open source, per consentire prestazioni elevate, continuità operativa ed evitare costose dinamiche di vendor lock-in.

La neutralità e l'indipendenza sono due valori importanti per GARR. In che modo orientano le attività dell'organizzazione?

Per noi è assolutamente fondamentale non essere condizionati dalle scelte commerciali dei fornitori. L'autonomia digitale è un tema importante che, in maniera crescente, ci interroga sulla responsabilità del

Claudia Battista, direttrice GARR dal novembre del 2022

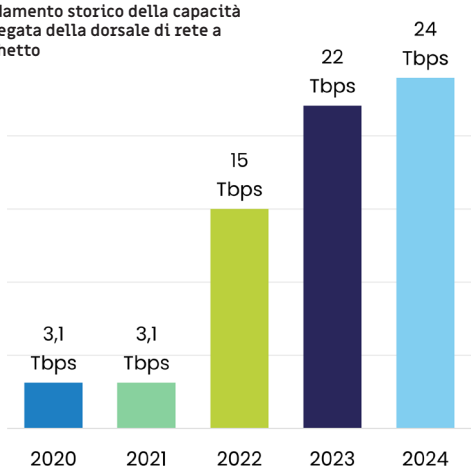
mondo della ricerca e dell'università nell'evoluzione del settore ICT.

Per la rete ottica, ad esempio, adottiamo una piattaforma di linea aperta, che sia indipendente dai vendor, con uso flessibile dello spettro ottico e dei trasponder dalle funzionalità all'avanguardia. Sul piano dell'innovazione e sviluppo di nuovi servizi, **stiamo collaborando con il Politecnico di Torino per creare un gemello digitale della rete GARR-T** per sperimentare l'utilizzo di tool aperti e per attività di pianificazione e design di reti ottiche open.

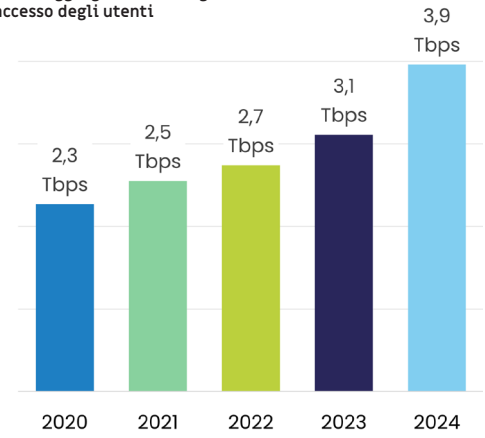
L'autonomia digitale è un tema importante che, in maniera crescente, ci interroga sulla responsabilità del mondo della ricerca e dell'università nell'evoluzione del settore ICT

Allo stesso tempo, siamo convinti che una crescita collettiva, indispensabile per sfruttare a pieno le funzionalità avanzate della rete, ma anche per mantenere o attrarre i talenti, passi attraverso un'adeguata formazione. Ed è per questo che continueremo a puntare molto sull'offerta di un ricco e qualificato programma per il potenziamento delle competenze.

L'andamento storico della capacità aggregata della dorsale di rete a pacchetto



Rete a pacchetto: evoluzione della capacità aggregata dei collegamenti di accesso degli utenti

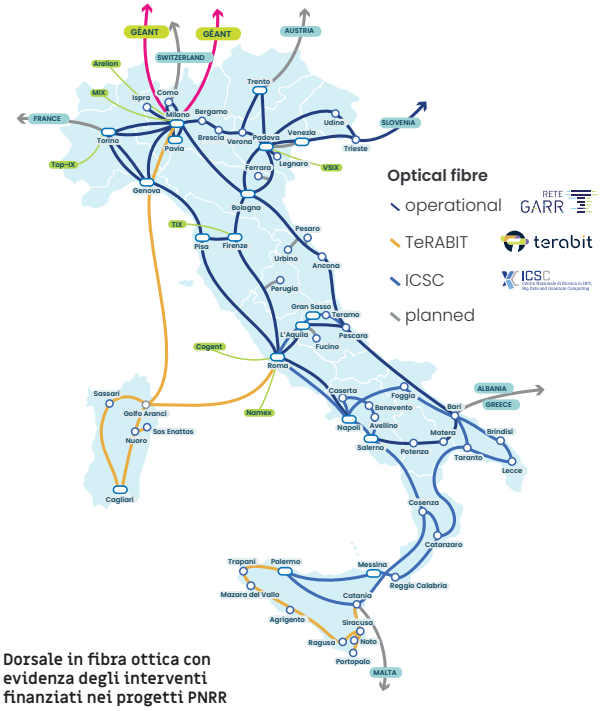


Un'altra priorità strategica è quella della sicurezza informatica. Quali passi state intraprendendo per garantirla?

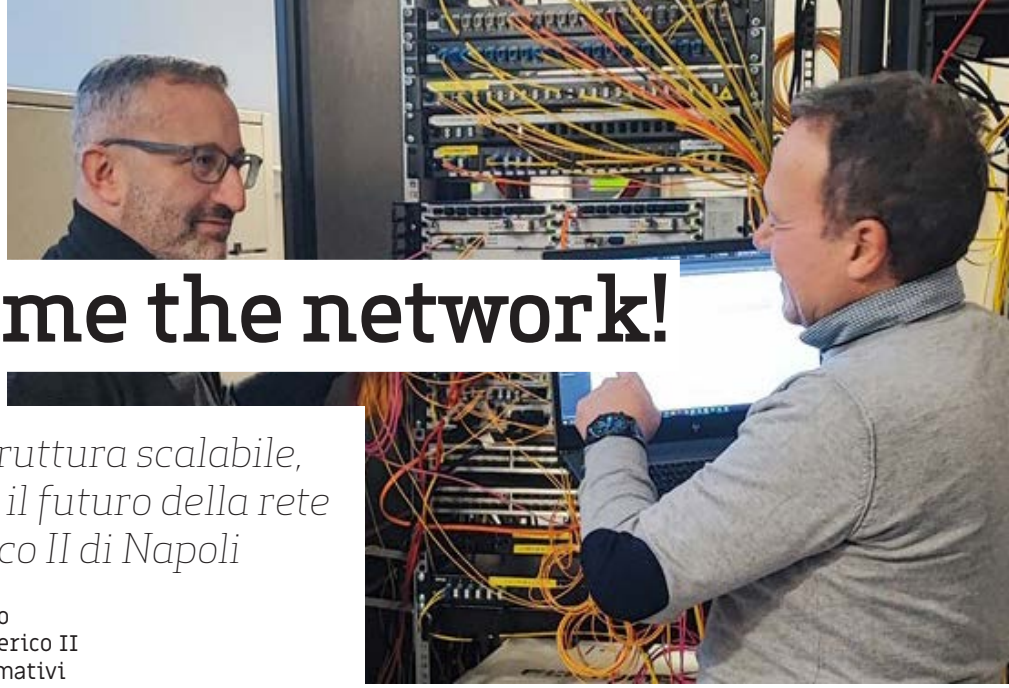
Per affrontare la sfida della sicurezza **stiamo adottando un approccio integrato affinché l'infrastruttura e i dati siano protetti**. Le misure principali includono il monitoraggio continuo e il rilevamento proattivo delle minacce, la segmentazione dei dati sensibili, la crittografia e la protezione dei dispositivi connessi, unitamente a una forte capacità di rispondere prontamente agli incidenti. Promuoviamo, inoltre, una **cultura della sicurezza** attraverso la formazione continua e la collaborazione con le autorità, la comunità di utenti e le altre reti della ricerca internazionali. Ovviamente, il massimo impegno è rivolto anche a garantire la conformità con le norme e i regolamenti sulla sicurezza cibernetica e a mantenere la certificazione ISO27001 per l'infrastruttura di calcolo e storage destinata ai servizi cloud per gli utenti.

Per la rete ottica adottiamo una piattaforma di linea aperta, che sia indipendente dai vendor

Affine al tema della sicurezza è, inoltre, l'attività sulla gestione delle **identità digitali**. L'obiettivo è migliorare l'affidabilità e l'interoperabilità delle identità federate, supportando, nella protezione avanzata dei dati, la comunità scientifica che richiede standard di autenticazione equiparabili a quelli governativi. In campo internazionale, GARR svolge un ruolo significativo nel servizio eduGAIN, e nei prossimi anni l'intento è quello di potenziarlo facendolo evolvere in una vera e propria federazione aggiungendo, a quello attuale in Polonia, altri due siti indipendenti di erogazione in Italia e Svezia.



Dorsale in fibra ottica con evidenza degli interventi finanziati nei progetti PNRR



Go on, blame the network!

Sviluppo di un'infrastruttura scalabile, sicura e resiliente per il futuro della rete dell'Università Federico II di Napoli

di Carmine Piccolo e Mario Maiorino
Università degli studi di Napoli Federico II
Centro di Ateneo per i Servizi Informativi

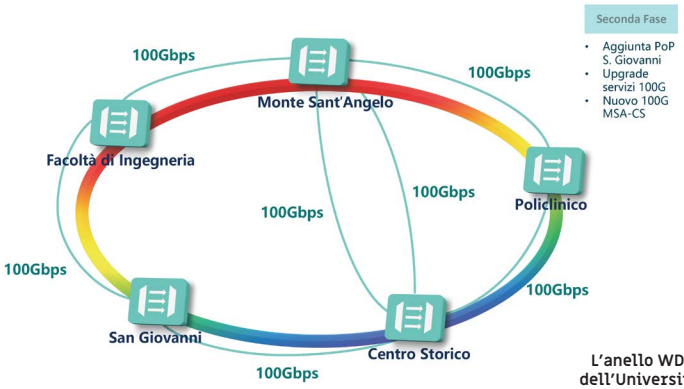
"Go on, blame the network!". Comunque vada, è sempre colpa della rete! Negli ultimi anni, è divenuto un mantra che accompagna i direttori tecnici delle aree reti del CSI (Centro di Ateneo per i Servizi Informativi) dell'Università degli Studi di Napoli Federico II. In accordo con la richiesta del management dell'Ateneo di avere, nell'anno dell'ottocentesimo anniversario della prima università laica in Europa, una rete che, confrontandosi con gli attuali e futuri bisogni, potesse ritenersi stabile, robusta e scalabile, ci siamo interrogati su quali interventi infrastrutturali e logici potessero migliorare e far evolvere la rete dell'università.

Il **progetto evolutivo ha avuto una durata di tre anni**. La prima fase prevedeva la migrazione dell'anello metropolitano di ateneo (con collegamenti P2P su dark fibre e una banda massima di 10 Gbps) verso un'infrastruttura incentrata su tecnologia DWDM. La nuova infrastruttura doveva essere scalabile in modo da permettere di ampliarne la capacità con successivi interventi, rendendo così il progetto economicamente più sostenibile nel tempo.

La rete della Federico II, definita durante il workshop GARR come "rete universitaria regionale" copre, al netto della provincia sannita, punti in tutta la regione campana collezionando numeri da medio service provider come i 75.000 punti rete, i 25.000 utenti giornalieri o una media di 2 milioni di sessioni al secondo negli orari d'ufficio.

L'impronta della nuova infrastruttura DWDM è basata su 5 PoP (Point of Presence) situati nell'area metropolitana a cui afferiscono, collegate in dark fibre, tutte le sedi dell'ateneo. Negli step successivi, si è puntato ad ampliare la banda arrivando ad una capacità di 200 Gbps complessivi di cui 100 dedicati all'infrastruttura dell'anello metropolitano e i rimanenti 100 dedicati ai collegamenti client dell'utenza "tributaria".

La nuova infrastruttura, definita in un case study su contesto europeo come "The biggest Campus Lan and DWDM of the EU", oltre ad assicurare la realizzazione su via protetta dei link primari garantendo la **completa trasparenza per l'utenza finale, anche in caso di possibili tagli fibra**, permette inoltre un'immediata gestione dei guasti mediante gli strumenti di misura integrati nel sistema delle tratte in dark fibre, capaci di inviare segnalazioni in tempo reale.



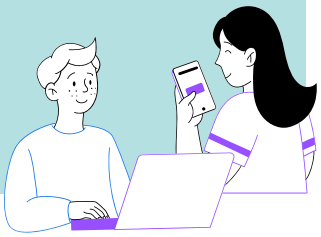
L'anello WDM dell'Università Federico II di Napoli

Ulteriori peculiarità sono la **possibilità di realizzare circuiti on demand** da dedicare alle nuove utenze, riprogrammando i circuiti, come successo in occasione dello spostamento della sede napoletana del CINECA e non ultima la possibilità che la soluzione scali ulteriormente fino ad una banda di 400 Gbps per singolo ramo in vista di evoluzioni future.

In ultima analisi, la struttura originaria ad anello è stata "sporcata" attraverso l'introduzione di un link diretto nord-sud tra i due PoP principali di Monte Sant'Angelo e della sede storica al fine di aumentare l'efficienza e la ridondanza nell'utilizzo della rete da parte dell'utenza dell'ateneo.

La rete di ateneo in numeri

:: 25.000 utenti al giorno
:: 2 milioni sessioni al secondo
:: 5 PoP
:: 2500 apparati wired
:: 2100 access point
:: 8 firewall
:: 10 router di PoP
:: 75.000 punti di rete



Accanto ad una infrastruttura di rete che evolve in capacità e prestazioni, non poteva non essere rivista l'intera concezione di **cybersecurity** a supporto della rete e dei sistemi di ateneo. Le sfide a cui si intendeva rispondere erano sostanzialmente tre: aumento della visibilità, della capacità di controllo e della segregazione del traffico di rete da e verso Internet ma soprattutto, vista la vastità della rete, anche quello interno all'ateneo stesso.

Dopo una prima fase di analisi e pianificazione, in cui sono stati evidenziati i principali punti di debolezza e sofferenza dell'architettura legacy, **si è deciso di passare da un modello routed a un modello spine-leaf** che prevede la presenza di una coppia di firewall in ogni PoP, adatti a gestire il traffico generato dallo specifico nodo, su cui terminare tutto il traffico di rete e gestire l'inter-vlan routing. Il funzionamento nativo del firewall in questa configurazione, per definizione, limita fortemente gli attacchi laterali oltre a protegge da quelli esterni.

Il passaggio da una topologia routed legacy a una spine-leaf elimina un livello di rete e permette di aumentare la velocità della rete di circa un 30%

Come completamento logico del progetto, l'intera rete si aggrega, per accedere ad Internet, su uno stretched cluster geografico, i cui nodi sono situati presso MSA e Centro storico, sede rispettivamente del PoP GARR di Monte S. Angelo (NA1) e PoP GARR di Monte di Dio (NA2). Entrambi i nodi del cluster gestiscono due VDOM (Virtual Domain), uno attivo e relativo all'area di competenza e l'altro dormiente per l'atra zona. I due nodi sono sincronizzati tra loro attraverso un link DWDM metropolitano layer2 in via protetta.

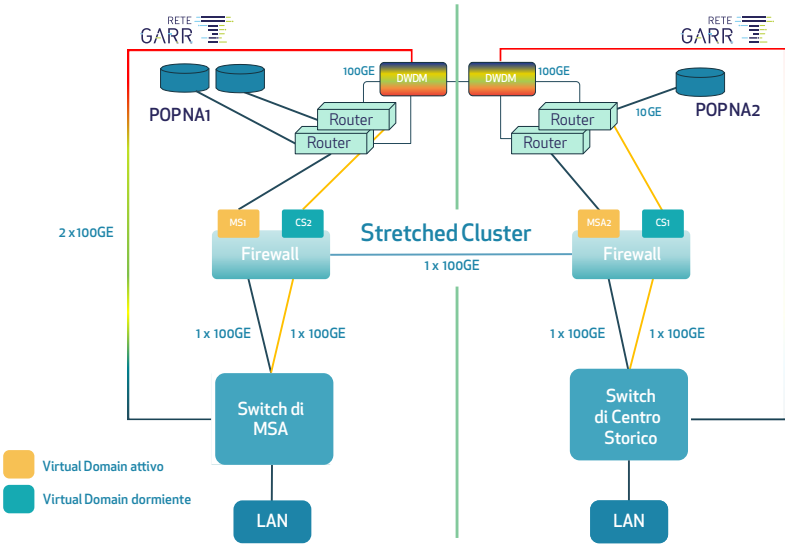
Questa configurazione offre un **effettivo sistema di disaster recovey** caratterizzato da un automatismo indirizzato a garantire la business continuity delle attività dell'ateneo anche sfruttando il doppio link di uscita (primario e backup) verso il PoP GARR di Monte S. Angelo e quello verso il PoP GARR di Monte di Dio. In caso di fault di un uno dei due nodi, il sistema convoglia automaticamente il funzionamento della rete, spostando il layer2 sul nodo che resta attivo, con un tempo di convergenza che è annoverabile nell'ordine di qualche decina di secondi (tempo legato al refresh delle ARP table) quasi impercettibile per l'utenza.

Il passaggio da una topologia routed legacy a una spine-leaf elimina un livello di rete e permette di aumentare la velocità della rete di circa un 30%. L'utilizzo di **Next Generation Firewall** su tutti i PoP, oltre ad aggiungere la capacità di operare analisi sul traffico da e verso la rete metropolitana, fino al livello 7 dello stack protocollare, ha permesso di implementare un secondo livello di sicurezza all'interno della rete di ateneo. La possibilità di gestire, controllare e ispezionare, su ogni PoP sia la connettività verso l'anello metropolitano che quella intra-nodo, permette una maggior profondità e precisione nell'isolare le minacce informatiche direttamente sul nascere e nel punto più prossimo alla generazione del traffico.

In termini di controllo, **l'uso di analizzatori del traffico di rete dedicati ed una infrastruttura SIEM, ha offerto la possibilità di analizzare, e filtrare, l'enorme quantità di traffico internet/intranet generato** e ottenere visibilità sulla postura di sicurezza dell'intera rete di Ateneo e dei suoi utenti.

Il completamento del progetto triennale ha certamente restituito all'ateneo federiciano una rete con una **banda disponibile aumentata di un ordine di grandezza, stabile e ridondata in ogni sua componente e con una elevata capacità di gestione dei guasti**. Da un punto di vista della cyber security la rete presenta due livelli di sicurezza (front-end e back-end) ed una gestione dell'accesso alla rete GARR attraverso un cluster geografico di firewall che permette di applicare meccanismi di business continuity all'intera infrastruttura di rete. Questo tipo di infrastruttura, per quanto detto, consente di applicare i controlli di sicurezza, di filtraggio e di protezione nel punto più vicino all'utenza e, allo stesso tempo ottimizza il carico, distribuendo in più punti il lavoro necessario ad ispezionare il traffico generato dalle decine di migliaia di utenti che quotidianamente frequentano i vari campus e sedi dell'ateneo.

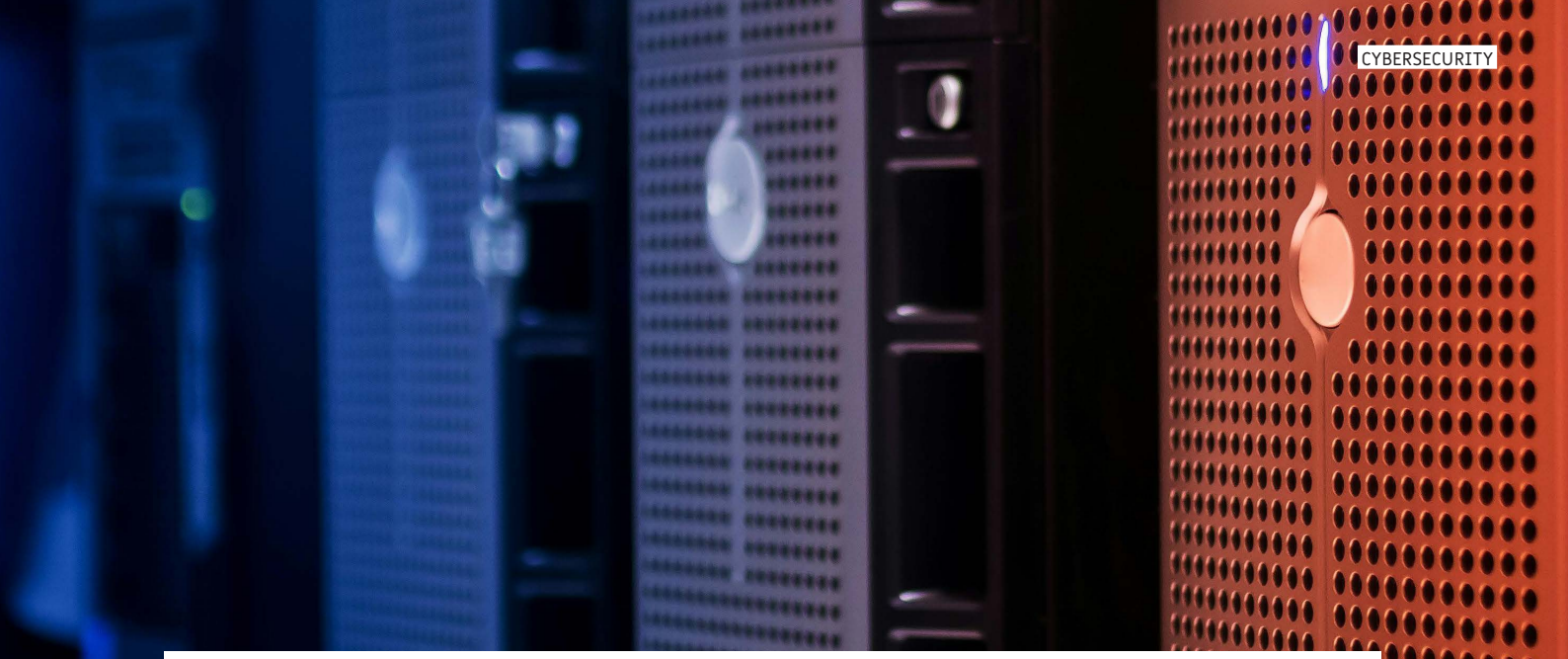
→ unina.it



Il modello "spine-leaf" della rete dell'Università Federico II di Napoli

Carmine Piccolo e Mario Maiorino durante la loro presentazione al Workshop GARR 2024

Guarda l'intervento su GARR.tv



Il supplizio della supply chain

Quando la nostra sicurezza dipende anche da ciò che compriamo

di Simona Venuti

Come è stato detto più volte, la misura della sicurezza di una organizzazione è data dalla sicurezza dell'anello più debole della catena. Negli anni gli enti hanno investito e studiato soluzioni per poter migliorare la propria postura di sicurezza e cercare di tenere fuori i criminali dai propri dati e servizi. I criminali però continuano ad ingegnarsi con sistemi sempre più complessi e sofisticati per trovare brecce, vulnerabilità e raggiungere i propri scopi, per esempio andando a cercare gli anelli più deboli, che sempre più spesso non sono all'interno dell'organizzazione da attaccare, ma nella rosa dei propri fornitori di hardware, di software e di servizi. Mi riferisco ad una tematica di sicurezza ancora poco esplorata, ma che sta diventando sempre più importante: la sicurezza nella supply chain o catena di approvvigionamento.

L'impatto di una compromissione o vulnerabilità di un fornitore nella sicurezza di una organizzazione sta diventando sempre maggiore. Il rapporto Verizon sui data breach nel 2023 ci racconta che il 15% della perdita di dati è dovuto a problemi sul software e hardware acquisito da terzi. Anche se la percentuale non è (ancora) altissima, c'è da notare che nello stesso rapporto per il 2022 la supply chain non compariva proprio, il che significa che l'aumento (oppure "la comparsa di quella voce" oppure "quel 15%") è molto significativo. In questi ultimi tempi ce ne siamo anche accorti, dato che ci sono stati episodi di impatto notevole che hanno coinvolto brecce di sicurezza nella supply chain.

Il 15% della perdita di dati
è dovuto a problemi sul software
e hardware acquisito da terzi

La vicenda SolarWind alza sull'intero globo l'asticella della minaccia

Il primo esempio eclatante che tutti ricorderanno è avvenuto nel 2020, in cui criminali sono entrati nell'azienda **SolarWind**, un fornitore di software per la gestione IT e sono riusciti ad **iniettare codice malevolo in un aggiornamento dei loro programmi**, utilizzati da molte aziende e pubbliche amministrazioni. Queste organizzazioni, pensando di installare un aggiornamento legittimo del software SolarWind, hanno in realtà inconsapevolmente installato anche il malware, che da marzo a novembre è rimasto silente a raccogliere dati su ciascuna struttura, per poi sferrare l'attacco ed esfiltrazione dei dati in dicembre.

L'impatto enorme di questo incidente di sicurezza ha portato per primi i legislatori USA ad emanare l'**Executive Order on America's Supply Chains** (24 febbraio 2021) e i legislatori europei ad emanare una nuova direttiva NIS, la **NIS2**, in cui uno degli aspetti preponderanti è proprio l'attenzione alla catena dei fornitori.

Impatto su enti governativi in tempi incerti

Fra la stesura della NIS2, la sua emanazione e il recepimento, è accaduto un altro incidente grave, che ha coinvolto istituzioni governative danesi ed europee: quello di **Ivanti**. Anche Ivanti è un software di gestione IT, in particolare il loro modulo per la distribuzione delle patch aveva un bug RCE (esecuzione di codice arbitrario da remoto), che permetteva di ottenere privilegi elevati sul server di patch. In questo caso, dal momento che il software vulnerabile si occupa di distribuire le patch a tutti i sistemi del parco IT, avrebbero potuto inserire codice malevolo in tutti i sistemi dell'organizzazione. Il governo danese ha fatto sapere che di essere stato

compromesso dal bug di Ivanti, e che dati sensibili di alcuni membri del governo e parlamento erano stati esfiltrati. Non sono stati rivelati ulteriori dettagli, ma **la preoccupazione, dovuta anche all'incertezza geopolitica e a possibili attacchi "state-sponsored", è elevata**.

Impatto sui cittadini

Il problema di attacchi alla supply chain ci coinvolge non solo come enti che forniscono un servizio ai propri utenti, ma anche come cittadini. Ne abbiamo avuto esperienza durante lo scorso 19 luglio, quando **CrowdStrike** ha rilasciato un update del proprio software di EndPoint Detection and Response (EDR) che ha provocato un'epidemia di schermate blu e disservizi in tutto il mondo. In questo caso non era stato compromesso niente, semplicemente **l'azienda aveva distribuito un aggiornamento non funzionante che bloccava le macchine**. Questo blocco si è propagato in pochissimo tempo in numerosi servizi essenziali, fra cui trasporti, aeroporti, banche e ospedali, che sono stati indisponibili per lungo tempo.

Fattori di rischio legati alla supply chain sono nell'utilizzo di sistemi cloud per macchine e/o servizi, forniti da terze parti

Supply Chain nel "piccolo"

Nel nostro piccolo altri fattori di rischio legati alla supply chain sono nell'utilizzo di sistemi cloud per macchine e/o servizi, forniti da terze parti, oppure semplicemente un software di gestione delle fatture in cui, grazie ad alcune vulnerabilità, vengono cambiate al volo le coordinate bancarie del beneficiario in modo che venga pagato qualcun altro al posto del fornitore, oppure l'utilizzo di piattaforme come WordPress per pubblicare contenuti web, che sono controllate, ma che possono utilizzare plugin di terze parti vulnerabili, mai aggiornati, o addirittura malevoli di per sé.
Ma questo è solo l'ingresso della tana del Bianconiglio.

Il mondo open source

Uno dei più grossi problemi dovuti alla supply chain è occorso a dicembre 2021, con la vulnerabilità nel **software open source log4j**, una libreria Apache per i log applicativi. Anche in questo caso la vulnerabilità (CVE-2021-44228) era riconducibile ad un RCE. L'impatto è stato devastante nel numero di dispositivi affetti. Il software open source è generalmente utilizzato non solo da migliaia di utenti che non vogliono utilizzare strumenti commerciali o a codice chiuso, ma è largamente utilizzato anche da quelle stesse aziende commerciali che prendono software aperto di ottimo livello e lo riutilizzano per i propri prodotti, rivendendolo. In questo caso, le strutture che utilizzavano log4j vulnerabile erano i maggiori fornitori di cloud (Microsoft, AWS, Google Cloud), software finanziario di applicazioni bancarie, applicazioni e dispositivi medici, i server Minecraft e la gran parte di sistemi e applicativi web, sia open che a pagamento. Come risultato **si stima che il bug log4j abbia impattato su miliardi di dispositivi, milioni di aziende e utenti**.

Il problema più difficile da risolvere, nel caso di librerie open source vulnerabili, è il fatto che è difficile capire quale sia la versione utilizzata e da chi all'interno di una struttura

Inoltre, quest'anno per la prima volta è successa una cosa mai vista prima: uno degli sviluppatori della **libreria XZ**, libreria open source di compressione, dopo oltre un anno che lavorava come sviluppatore, ha inserito del codice malevolo nel github della libreria, facendolo passare come fix di un bug. Questa persona godeva di piena fiducia da parte del manutentore della libreria XZ e la sua richiesta di pubblicare il fix è stata accettata. **Ma il fix era malware**, in una libreria utilizzata su scala globale da moltissimi software, tanto che non si è neanche riusciti a capire l'impatto sul numero di device affetti o compromessi.

Il problema più difficile da risolvere, nel caso di librerie open source vulnerabili, è il fatto che molto spesso è difficile capire quale sia la versione utilizzata e da chi all'interno di una struttura, perché molto spesso sono utilizzate da software commerciali, che sono chiusi, o vengono chiamate all'interno del codice di software autoprodotto, e non si sa quale versione abbiano usato né se siano vulnerabili.

Tutto questo ha portato alla ribalta il rischio sull'utilizzo non solo di software e programmi vulnerabili, ma anche solo di librerie utilizzate poi da numerosi programmi, in cui diventa impossibile risalire alla catena di approvvigionamento, sapere se ce l'abbiamo, se possiamo censirla, se siamo vulnerabili.

Ci siamo resi conto che **avere vulnerabilità in librerie piuttosto che nel software è un salto di qualità** e cambio di paradigma a cui dobbiamo essere preparati.

E l'hardware?

Pensiamo a tutto l'hardware che acquistiamo. Più volte è stato dimostrato che oggetti collegati ad internet, ad esempio televisori, telecamere di videosorveglianza, giocattoli, apparati IoT o di domotica, comunicano costantemente con indirizzi sconosciuti (perlopiù cinesi), inviando loro tutti i dati che riescono a raccogliere. Come possiamo essere sicuri che un oggetto che compriamo per un servizio erogato dalla nostra struttura, non contenga delle backdoor "di fabbrica" che al momento opportuno consentano lo sfruttamento di quell'hardware da parte di altri?

Ci aiuta il CyberSecurity Act

La questione, sia per quanto riguarda il software che

hardware, è talmente importante che i legislatori europei hanno emanato un regolamento apposito, il **Cybersecurity Act**, che si occupa proprio di creare, a livello di ciascuna nazione, agenzie che stabiliscano degli standard di sicurezza per l'hardware e software, e che si occupino di controllare che tali standard siano rispettati mediante audit e laboratori di test. Una sorta di marchio CE di sicurezza cyber per hardware e software.

Prima della sua emanazione comprendeva una sezione che obbligava anche gli sviluppatori di software open source ad intraprendere le procedure per ottenere la certificazione del proprio software, ma questo avrebbe portato alla morte del software libero, dal momento che molti sviluppatori non hanno le risorse umane e finanziarie per poter testare e certificare i loro programmi. Per fortuna è passato un **emendamento che obbliga soltanto le aziende commerciali che utilizzano software libero ad ottenere la certificazione di sicurezza**, non gravando sui singoli sviluppatori e contribuenti all'open source. Ritengo che lo sviluppo del software libero sia di fondamentale importanza, e che sia meglio utilizzare un software libero con le sue vulnerabilità nella supply chain che piano piano vengono scoperte, piuttosto che un software chiuso che non possiamo sapere se abbia vulnerabilità non divulgate (e di solito ce l'ha). Avremmo potuto fare di meglio, per esempio spingendo le nazioni a supportare attivamente, mediante contributi, lo sviluppo del software libero, magari anche contribuendo economicamente alla sua certificazione, cosa che avrebbe portato ad avere software libero più sicuro.

Ma noi, alla fine, cosa possiamo fare per difenderci?

Dal punto di vista normativo abbiamo la **NIS2**, che per sistemi nel Perimetro di sicurezza cibernetica nazionale obbliga alla fornitura di materiale certificato. Abbiamo il **Cybersecurity Act** che stabilisce le procedure per la certificazione. Per alcune pubbliche amministrazioni abbiamo anche la **legge 90 del 2024**, che per acquisti informatici obbliga gli enti ad indicare nel capitolato misure precise di sicurezza che il fornitore deve mettere in opera per vincere la gara e in ogni caso nelle gare non si può guardare al prezzo più basso ma anche alla garanzia dei requisiti minimi di sicurezza del fornitore.

La situazione purtroppo è complicata, e in un ambiente libero come quello di università e ricerca è veramente difficile capire quali siano tutte le catene di approvvigionamento per ciascun ufficio, servizio, dipartimento, docente o ricercatore. Il nostro più grande sforzo dovrebbe essere inizialmente **censire le varie tipologie di supply chain**: fornitori hardware, fornitori software, ma anche settore DevOps e programmatori per capire quali librerie di terze parti vengano utilizzate nel software autoprodotto.

Una volta censita tutta la catena sarà necessario, come sempre, approcciarsi a districare la matassa effettuando un'**analisi del rischio**, poi **stabilire delle priorità** e successivamente affidarsi agli strumenti che possiamo utilizzare facilmente, per esempio utilizzando **prodotti certificati**, effettuando **scansioni di vulnerabilità e/o pen-test**, monitorando i sistemi.

Per quanto riguarda la catena "open source, DevOps e librerie" sarà necessario cambiare paradigma: non possiamo più aspettare che lo sviluppatore pubblichi una patch, ma dobbiamo intervenire prima, attraverso analisi del software autoprodotto, e lavorando sulla singola vulnerabilità: sapere quanto è grave, sapere se esiste un exploit, sapere se è facilmente sfruttabile, sapere se ce l'abbiamo.

Ma non solo, nell'ambiente di sviluppo è molto importante il contesto: abbiamo bisogno di sapere se la vulnerabilità è nell'ambiente di produzione o test, se il servizio è esposto, che tipo di dati processa e come si relaziona agli altri sistemi, sapere il raggio di azione. Il contesto è multidimensionale e importante per capire la priorità di intervento. Dobbiamo anche tenere in conto il fatto che con l'AI il cosiddetto **time to exploit**, cioè il tempo che serve ad un attaccante a scrivere codice per l'exploit una volta individuata una vulnerabilità, sta diventando pericolosamente basso, è stato appena stabilito il record di 22 minuti, rispetto ai mesi che ci volevano per scriverlo a mano. Quindi è fondamentale trovare soluzioni che facilitino l'identificazione e la correzione del problema in tempi concorrenziali con l'attaccante.

Questo ultimo punto è cruciale, dato che i software di scansione vulnerabilità attualmente sul mercato non riescono a capire quali librerie sono utilizzate da un programma e la loro versione. D'altra parte non possiamo richiedere ai nostri programmatori né ai fornitori di software di fare una lista delle librerie utilizzate con la relativa versione. Ci sono al momento tentativi di approcciarsi a questo problema, ma è un mondo ancora tutto da inventare.

Conclusioni

Fare la sicurezza è sempre stato un "inseguire i nuovi modi di attacco", ma con i rischi sulla supply chain in qualche modo dovremmo iniziare ad essere più veloci e sistemare le vulnerabilità prima che esca l'exploit.

Per approfondire

Rapporto Verizon 2024
https://u.garr.it/verizon2024

Executive Order on America's Supply Chains:
https://u.garr.it/americassupplychain

SolarWind
https://u.garr.it/solarwind

Ivanti
https://u.garr.it/ivantisecurity

Log4j
https://u.garr.it/log4j

Librerie XZ
https://en.wikipedia.org/wiki/XZ_Utils_backdoor

Nuovo record "time to exploit"
https://u.garr.it/bleepingcomputer

Skills4EOSC: la rete europea dei Competence Centre per l'Open Science

di Sara Di Giorgio
GARR, coordinatrice del progetto Skills4EOSC

Il progetto Skills4EOSC, coordinato dal GARR, sta creando una rete paneuropea di Competence Centre per sviluppare competenze essenziali nell'ambito dell'Open Science e del FAIR data management. Questa iniziativa mira a colmare le lacune di competenze esistenti e a standardizzare la formazione in tutta Europa, supportando la visione dell'European Open Science Cloud (EOSC) e trasformando l'Open Science nella nuova normalità della ricerca scientifica.

L'Open Science rappresenta un insieme di principi e pratiche volti a rendere la ricerca scientifica accessibile a tutti

Nell'era della digitalizzazione, l'Open Science sta emergendo come un paradigma fondamentale per accelerare la ricerca scientifica e l'innovazione. L'European Open Science Cloud (EOSC) ha l'ambizioso obiettivo di creare un "**Web di dati e servizi FAIR**" per la scienza in Europa. Tuttavia, per realizzare questo scenario, è essenziale colmare il divario di competenze esistente tra i ricercatori e gli stakeholder coinvolti. È in questo contesto che si inserisce il progetto Skills4EOSC, che attraverso **una rete di Competence Centre**, si propone di armonizzare l'attuale panorama formativo per lo sviluppo di materiali didattici, curricula e percorsi di apprendimento per ricercatori, curatori e gestori di dati, in grado di trasformare il modo in cui svolgono la ricerca, elevando la qualità dei risultati e favorendo la collaborazione e la partecipazione a EOSC.

L'Open Science: un nuovo paradigma per la ricerca

Secondo la Raccomandazione UNESCO, l'Open Science rappresenta un insieme di principi e pratiche volti a rendere la ricerca scientifica accessibile a tutti, a beneficio sia della comunità scientifica che dell'intera società. Questo approccio mira non solo a rendere accessibile la conoscenza scientifica, ma anche a garantire che la sua produzione sia inclusiva, equa e sostenibile.
L'Open Science è anche fortemente sostenuta dalla Commissione europea, attraverso l'European Open Science Cloud (EOSC), una vasta iniziativa lanciata nel 2018, per creare un'infrastruttura federata e aperta che permetta a ricercatori e professionisti di tutta Europa di condividere e riutilizzare i dati scientifici in modo facile e sicuro. L'obiettivo principale è la creazione di un ecosistema digitale FAIR di dati e servizi per favorire la collaborazione e l'avanzamento scientifico. Per realizzarlo pienamente, è essenziale sviluppare competenze mirate tra ricercatori, professionisti e decisori politici.

Il progetto Skills4EOSC: colmare il divario di competenze

Il progetto Skills4EOSC, avviato nel settembre 2022 e con termine previsto nell'agosto 2025, si propone, grazie a un consorzio di 46 partner provenienti da 18 paesi, di **unificare l'attuale panorama formativo in un ecosistema pan-europeo comune e affidabile.**
Il progetto mira a colmare tre lacune principali identificate nell'Agenda Strategica di Ricerca e Innovazione dell'EOSC (Strategic Research and Innovatoin Agenda, SRIA):
1. La mancanza di competenze in Open Science e gestione dei dati
2. L'assenza di una chiara definizione dei profili professionali legati ai dati e dei relativi percorsi di carriera
3. La frammentazione delle risorse formative

I Competence Centre: il cuore pulsante di Skills4EOSC

Al centro della strategia di Skills4EOSC c'è la creazione di una **rete di Competence Centre per la Scienza Aperta.** Questi centri fungono da punti di

riferimento chiave all'interno di un paese, una regione o un'area tematica, offrendo competenze nelle pratiche di Open Science e gestione FAIR dei dati.

I Competence Centre si impegnano ad adottare i risultati del progetto e a partecipare al programma di formazione dei formatori (Training the Trainers). Questa rete, grazie ad un meccanismo di governance leggero, permette di condividere le migliori pratiche e di costruire una visione unificata per lo sviluppo dell'Open Science in Europa.

Il Minimum Viable Skillset: definire le competenze chiave

Un elemento innovativo del progetto Skills4EOSC è il concetto di **Competenze Minime Essenziali** (Minimum Viable Skillset ,MVS). Questo approccio delinea le competenze essenziali per vari ruoli che operano a diversi livelli per attuare la Scienza Aperta, tra cui ricercatori, data steward, policy maker, esperti di questioni legali ed etiche e molti altri.

L'MVS non solo guida la creazione di programmi di formazione su misura, ma fornisce anche una base comune per lo sviluppo di curricula in tutta Europa. Questo approccio standardizzato, pur rimanendo flessibile e adattabile a vari contesti e domini, garantisce una coerenza nella formazione a livello continentale, essenziale per l'adozione diffusa delle pratiche di Open Science.I profili MVS infatti servono come base per sviluppare programmi e corsi di formazione per le figure professioni e i ruoli individuati, in modo che le competenze acquisite siano direttamente applicabili e rilevanti per ciascun ruolo specifico nell'ecosistema dell'Open Science.

La metodologia FAIR-by-design: garantire un ampio riuso dei materiali didattici

Skills4EOSC ha sviluppato una metodologia FAIR-by-design per la creazione di materiali didattici.Questo approccio in sei fasi assicura che tutte le risorse formative siano progettate e reallizzate per essere reperibili (Findable), accessibili (Accessible), interoperabili (Interoperable) e riutilizzabili (Reusable).

La metodologia propone un **percorso operativo per la realizzazione dei corsi e dei moduli di formazione**, aiutando il docente e il ricercatore ad affrontare questioni cruciali come la proprietà intellettuale, le licenze e l'attribuzione, mettendo in risalto la necessità di utilizzare l'uso di schemi di metadati, vocabolari controllati e identificatori persistenti per la corretta descrizione e referenziazione dei materiali.

Il programma di formazione dei formatori: effetto a cascata per diffondere la conoscenza

Un elemento chiave del progetto è il programma Training the Trainers (TtT). Ogni Competence Centre che fa parte della rete di Skills4EOSC, seleziona dei Master Trainer che partecipano a corsi intensivi su vari aspetti dell'Open Science e del FAIR data management, che Skills4EOSC terrà nel corso di quest'ultimo anno.Una volta formati, questi Master Trainer tornano nei loro centri per condividere le migliori pratiche e le lezioni apprese con i formatori locali. Questo approccio a cascata assicura una diffusione capillare delle competenze in tutta la rete, creando un effetto moltiplicatore che amplifica l'impatto del progetto e accelera l'adozione dell'Open Science in tutta Europa.

Riconoscimento e certificazione delle competenze: valorizzare le competenze

Skills4EOSC non si limita alla formazione, ma si occupa anche del riconoscimento delle competenze acquisite. Il progetto sta sviluppando un framework di riconoscimento che si integrerà con l'European Digital Credential for Learning (EDC). Ogni corso offre un badge di certificazione specifico al completamento, e completando tutti i moduli di un corso, i partecipanti ottengono la **Certificazione di Master Trainer**, dimostrando la loro esperienza e padronanza nel campo.

Questo sistema di riconoscimento non solo motiva i partecipanti, ma crea anche un standard riconosciuto di competenze nell'ambito dell'Open Science e del FAIR data management a livello europeo.

L'espansione della rete dei Competence Centre

Attualmente, la rete di Skills4EOSC conta 8 Competence Centre, con l'obiettivo di raggiungere almeno 10 centri. Il progetto è in contatto con altri 11 potenziali Competence Centre, a testimonianza del crescente interesse e l'importanza di questa iniziativa.

L'espansione della rete non è solo una questione di numeri, ma di creare una comunità diversificata e inclusiva che possa affrontare le sfide dell'Open Science da molteplici prospettive. Infatti la rete pan-europea facilita la collaborazione e lo scambio di best practice tra paesi e discipline, creando un ecosistema di conoscenza veramente aperto e interconnesso.

Ogni Competence Centre seleziona dei Master Trainer che partecipano a corsi intensivi su vari aspetti dell'Open Science

ICDI: il Competence Centre italiano per l'Open Science

All'interno della rete europea dei Competence Centre, l'Italia partecipa attivamente attraverso ICDI (Italian Computing and Data Infrastructure). ICDI, in qualità di Competence Centre nazionale, erogherà i corsi Skills4EOSC alla comunità italiana di ricercatori e professionisti. Il centro adatterà i materiali formativi al contesto italiano, fungendo da ponte tra le iniziative europee e le esigenze locali.

Tra i primi corsi in programma, ci sarà "Science4Policy", un corso innovativo che mira a colmare il divario tra l'open science e la pratica decisionale basata su evidenze. Questo corso esplorerà il ruolo delle politiche per la Scienza Aperta, l'integrazione delle

evidenze nei processi decisionali e metodologie di coinvolgimento degli stakeholder. I partecipanti apprenderanno come utilizzare gli strumenti dell'open science per supportare il processo decisionale e come interpretare i dati della ricerca.

Allineamento dei Competence Centre con gli EOSC Nodes

I Competence Centre di Skills4EOSC lavoreranno in stretta integrazione con gli EOSC Nodes, che rappresentano il nucleo operativo della EOSC Federation. Il 22 novembre 2024, durante l'EOSC Symposium, è stato ufficialmente lanciato l'EOSC EU Node, una piattaforma centrale che promuove la collaborazione interdisciplinare e multinazionale attraverso l'uso di dati FAIR e servizi interoperabili. Questo nodo europeo fungerà da punto di riferimento principale, mentre i nodi nazionali e tematici, attualmente in fase di selezione, si collegheranno a esso per formare un ecosistema federato. I Competence Centre, con il loro ruolo di coordinamento delle competenze e di formazione, saranno integrati nei nodi nazionali per rafforzare la coerenza delle pratiche di Open Science e supportare le comunità di ricerca a livello locale e tematico. Questo approccio combinato assicura una rete interconnessa che favorisce la condivisione di risorse, conoscenze e migliori pratiche in tutta Europa, rendendo l'Open Science un pilastro centrale del panorama scientifico europeo.

Conclusioni e prospettive future

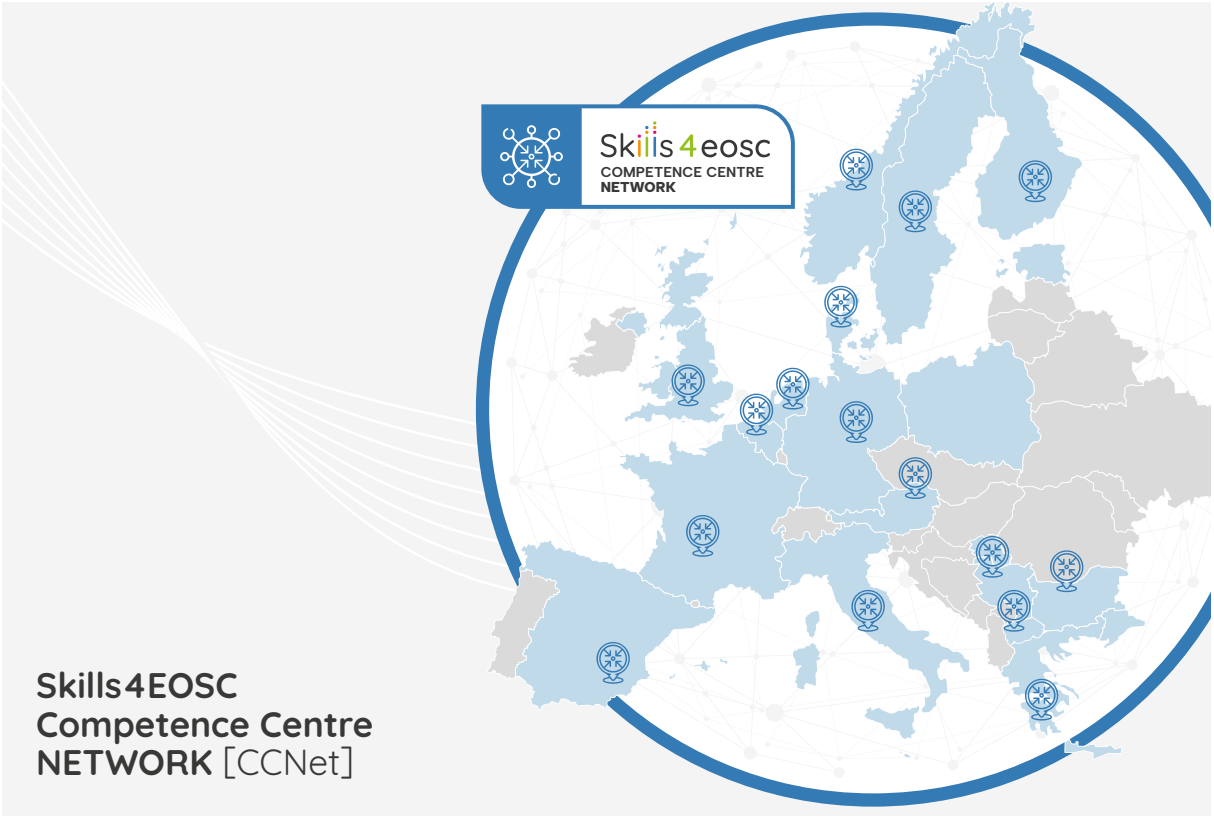
Skills4EOSC rappresenta un passo fondamentale verso la realizzazione della visione dell'European Open Science Cloud. Creando una rete paneuropea di Competence Centre, il progetto sta gettando le basi per un futuro in cui l'Open Science non è solo un ideale, ma una pratica quotidiana per ricercatori, professionisti e decisori politici in tutta Europa. Mentre il progetto entra nel suo terzo e ultimo anno di attività, l'attenzione si sposterà sulla formazione dei Master Trainer e la definizione di raccomandazioni per sostenere ed espandere la rete dei Competence Centre oltre la durata del progetto. Questo garantirà che l'impulso verso l'Open Science continui a crescere e a evolversi, adattandosi alle nuove sfide e opportunità del panorama scientifico in rapida evoluzione.

L'armonizzazione tra i Competence Centre e gli EOSC Nodes sarà essenziale per creare un ecosistema veramente integrato, in cui la condivisione di risorse e conoscenze favorisca l'innovazione e l'accesso equo alla conoscenza scientifica in tutta Europa.

Il successo di Skills4EOSC dimostra che investire nello sviluppo delle competenze è fondamentale per realizzare il pieno potenziale dell'EOSC. Con la continua collaborazione e l'impegno di tutte le parti interessate, possiamo aspettarci un futuro in cui l'Open Science non è solo una possibilità, ma una realtà quotidiana che accelera l'innovazione e democratizza l'accesso alla conoscenza scientifica in tutta Europa.

→ skills4eosc.eu

Skills 4 eosc



Tra passato, presente e futuro

di Marco Falzetti, Direttore APRE
Agenzia per la Promozione della Ricerca Europea

Il rientro dalla pausa estiva ha segnato un momento particolarmente effervescente nel contesto del dibattito sul futuro Programma quadro di Ricerca e Innovazione dell'Unione europea, al momento ancora individuato come **FP10**. Ci eravamo lasciati a luglio con un insieme di documenti di posizionamento espressi dai principali paesi e/o organizzazioni dove venivano espressi molti suggerimenti e richieste, talvolta anche diverse e contrastanti, ma tutte in una visione del futuro FP10 sostanzialmente conservativa, ovvero, dando per scontato che la struttura, ma anche l'idea stessa di Programma quadro restasse in linea di massima la stessa. Già a quel tempo, ci lasciammo con l'idea che al rientro la discussione si sarebbe rapidamente riaccesa a valle di una serie di importanti documenti attesi nella finestra settembre-ottobre: il rapporto Draghi, il rapporto Heitor, la lettera di missione per la nuova Commissaria alle "Startup, ricerca e innovazione". Tutto questo è effettivamente avvenuto, ma con non poche sorprese. Diciamo che settembre ed ottobre sono stati un momento di grande confusione dove, per quanto non scritto ma trapelato, per quanto detto male e poi corretto, per quanto interpretato e poi consolidato, si è avuta l'impressione che forse non ci sarebbe neanche stato un futuro Programma FP10, o almeno non nella forma e immagine di quello che sin qui eravamo abituati a pensare.

È auspicabile che la prima bozza di proposta per FP10 venga presentata nella seconda metà del prossimo anno

Pur riconoscendo l'importanza di un solido Programma quadro di ricerca e innovazione per il futuro, il **rapporto Draghi**, con la sua forte enfasi sulla competitività del sistema europeo, ha lasciato intravedere la possibilità di una destrutturazione dell'attuale Horizon Europe. Si ipotizza così una sua riorganizzazione, in cui attività legate al rafforzamento della competitività potrebbero essere collocate altrove, anche al di fuori del Programma stesso. Questo approccio segna una rottura rispetto alla linea adottata dalla Commissione negli ultimi due Programmi quadro (H2020 e HE), che avevano puntato sull'integrazione tra ricerca e innovazione proprio per sottolineare come la competitività europea dovesse necessariamente fondarsi su una sinergia tra i due elementi, essenziale per alimentare la competizione tecnologica.

Al momento attuale, la nuova Commissione ha appena cominciato a fare i primi passi, ed è difficile immaginare come il dibattito sul nuovo FP10 prenderà davvero forma. Di certo si può affermare che quel momento di incertezza e confusione che ha caratterizzato i mesi autunnali sia stato superato e, pur non potendo dare al momento nulla di scontato, alcune delle paure connesse con un potenziale dissolvimento dell'integrità del futuro FP10, sono in buona parte rientrate.

La prima proposta del futuro Programma sarà messa sul tavolo dalla Commissione solo a valle della prima definizione dell'**MFF, il Multiannual Financial Framework**, che stabilirà la struttura e i volumi del bilancio del prossimo periodo di programmazione 2028- 2034. Tale documento prenderà forma nei primi sei mesi del 2025, ed è quindi auspicabile che la prima bozza di proposta per FP10 venga presentata nella seconda metà del prossimo anno.

Nel frattempo, proseguiranno le discussioni nei tavoli nazionali ed europei su come ciascuno immagina il prossimo Programma, alimentando un processo informale ma intenso e partecipato. Questo confronto fornirà, si auspica, indicazioni e suggerimenti utili alla Commissione per elaborare una prima proposta di qualità. L'obiettivo condiviso è di arrivare a una proposta capace di superare le principali limitazioni e debolezze dell'attuale Programma, interpretando al meglio l'esigenza di scommettere sul futuro. Una scommessa che, per l'Europa, rappresenta non solo una sfida per promuovere una società più attenta all'ambiente e al sociale, ma anche un **passo decisivo verso l'autonomia tecnologica**. Tale autonomia sarà fondamentale per affrontare con maggiore resilienza sfide cruciali come il fabbisogno energetico, la disponibilità di materiali strategici e una più indipendente capacità di difesa.

APRE ha recentemente pubblicato un documento, primo italiano, che delinea la sua posizione sui temi essenziali del prossimo Programma quadro FP10. Questo documento, basato sul rapporto esteso **"Verso FP10"** e

arricchito dai contributi di esperti e dal dibattito delle parti interessate, pone l'accento sul ruolo cruciale della Ricerca e Innovazione per la competitività europea.

Nel documento si è voluto sottolineare **l'importanza della R&I come motore della competitività europea**, un tema enfatizzato anche dai recenti studi (Draghi e Heitor) e nelle linee e visioni della Commissione europea. Per raggiungere questo obiettivo, è fondamentale che il prossimo Programma quadro abbia una dotazione finanziaria significativamente aumentata, con un bilancio di almeno 200 miliardi di euro. Questo incremento non solo aumenterebbe la dotazione del futuro Programma contribuendo anche ad innalzare il tasso di successo della partecipazione, ma contribuirebbe anche ad aumentare l'incidenza della componente europea sulla spesa di ricerca e sviluppo, attualmente poco superiore al 10%.

L'obiettivo di migliorare la competitività non deve limitarsi al recupero della produttività industriale, ma deve puntare ad aumentare la qualità e le prestazioni dell'intero sistema socio-economico. Questo approccio deve **affrontare le grandi sfide sociali con una visione sistemica, transdisciplinare e partecipativa**. Inoltre, le priorità della cooperazione internazionale devono essere chiaramente definite per contribuire agli obiettivi strategici dell'Unione e alla sua sovranità tecnologica.

Il documento evidenzia la necessità di adottare un approccio sistemico nella definizione del quadro di governance della R&I, evitando una distribuzione dispersiva delle responsabilità. È essenziale valorizzare le sinergie mediante approcci collaborativi, per evitare il "rischio silos" che potrebbe derivare dalla moltiplicazione delle agenzie. Inoltre, è importante **armonizzare ulteriormente le regole e le procedure per facilitare l'approccio collaborativo**.

Innovazione di frontiera

Per recuperare competitività, l'Europa deve poter contare su un sistema di R&I capace di produrre innovazione di frontiera e valorizzarla sui mercati globali. A tal fine, oltre ad aumentare la dotazione finanziaria dell'EIC (European Innovation Council), è necessario introdurre un meccanismo per il finanziamento di azioni "ad alto impatto potenziale", ispirato all'esperienza ARPA. Questo meccanismo dovrebbe concentrare una quota rilevante dei fondi su azioni mirate alla ricerca e sviluppo di soluzioni a sfide sociali prioritarie.

Per recuperare competitività, l'Europa deve poter contare su un sistema di R&I capace di produrre innovazione di frontiera e valorizzarla sui mercati globali

Ricerca collaborativa

La R&I collaborativa ha svolto un ruolo determinante nella costruzione dell'Europa della ricerca e innovazione, promuovendo la collaborazione tra pubblico e privato, tra accademia e industria, e tra Stati membri. È quindi fondamentale continuare a **finanziare progetti di R&I collaborativa**, poiché garantiscono opportunità di accesso per tutti gli attori della R&I e rappresentano un fattore di connessione insostituibile tra ricerca e innovazione.

Coinvolgimento di Stati membri e Regioni

I finanziamenti europei rappresentano una quota minoritaria delle spese totali di R&I della UE. Per rafforzare il ruolo di leverage del PQ, è necessario incoraggiare gli Stati membri a finanziare progetti che hanno ricevuto il Seal of Excellence e promuovere azioni di capacity building a livello regionale. Questo approccio permetterà di cogliere più efficacemente le specificità subnazionali in termini di sviluppo e bisogni.

Partecipazione delle PMI

Nonostante la partecipazione delle PMI ai PQ sia cresciuta negli ultimi decenni, il livello attuale non rispecchia il loro peso reale nell'economia europea. È quindi necessario **introdurre misure specifiche e strumenti dedicati alle PMI innovative** per facilitarne l'accesso ai finanziamenti di R&I. Inoltre, è importante sostenere la trasformazione delle PMI tradizionali in PMI tecnologicamente avanzate mediante un fondo ad hoc.

Attrazione e valorizzazione dei talenti

La competizione mondiale per attrarre e trattenere i talenti di chi fa ricerca e innovazione si è intensificata, penalizzando l'Europa. Per contenere il fenomeno della "fuga dei cervelli", è necessario intervenire con investimenti consistenti e coordinati in infrastrutture di ricerca e con riforme strutturali che valorizzino il merito e migliorino le condizioni di carriera dei ricercatori.

Quadro organizzativo e operativo

Per raggiungere efficacemente gli obiettivi del PQ, sono necessari interventi e riforme organizzative. Tra le priorità, vi è la rivisitazione del ruolo e delle competenze delle Agenzie esecutive, la semplificazione del processo di valutazione dei progetti e la verifica delle competenze dei programme managers. Inoltre, potrebbe essere utile riformare il sistema di application per favorire una maggiore armonizzazione delle regole tra programmi e strumenti.

In conclusione, il documento dell'APRE offre una visione chiara e articolata delle sfide e delle opportunità per il prossimo Programma quadro FP10. Le proposte avanzate mirano a rafforzare il ruolo della R&I come motore della competitività europea, promuovendo un approccio sistemico, collaborativo e orientato all'innovazione di frontiera.

→ apre.it

Ricerca e AI: autonomia digitale per l'innovazione

di Massimo Carboni
Chief Technical Officer GARR

L'avvento dell'Intelligenza Artificiale e, in particolare dell'AI Generativa, ha avuto un impatto travolgente nell'era digitale, promettendo immense opportunità ma sollevando anche cruciali interrogativi etici e pratici. Questa trasformazione epocale richiede una profonda riflessione su come **bilanciare i potenziali benefici dell'AI con i rischi di una delega eccessiva della capacità decisionale** umana a pochi soggetti tecnologici dominanti. È importante dunque comprendere quale sia un giusto approccio per mantenere il ruolo guida dell'essere umano in questa nuova era tecnologica, assicurando che l'AI rimanga uno **strumento al servizio dell'umanità e non un fine in sé.** E in questo contesto, la comunità dell'università e della ricerca può e dovrebbe dare un contributo determinante.

L'avvento dell'AI Generativa, ha avuto un impatto travolgente nell'era digitale, promettendo immense opportunità ma sollevando anche cruciali interrogativi etici e pratici

La conoscenza come motore dell'evoluzione umana

Il progresso dell'umanità è stato guidato dallo sviluppo cognitivo, dalla curiosità e dalla creatività che ci contraddistinguono come specie. Questi tratti ci hanno spinto a sviluppare strumenti e tecnologie per soddisfare i nostri bisogni e migliorare le nostre condizioni di vita. Tuttavia, il vero motore propulsivo dell'evoluzione umana risiede nell'apprendimento sociale, nella comunicazione e nella collaborazione. È stata la capacità di condividere la conoscenza, di tramandarla e di costruire collettivamente che ha permesso all'umanità di compiere progressi senza precedenti. Un esempio emblematico è la scoperta del fuoco, un'innovazione che ha rivoluzionato la vita dell'uomo primitivo e che, nel corso dei millenni, è stata compresa, trasformata e perfezionata fino a condurre alle più moderne tecnologie energetiche.

La tecnologia digitale e in particola l'intelligenza artificiale rappresenta il tentativo più recente e finora dirompente di utilizzare tutta la conoscenza collettiva dell'uomo per dare una risposta a problemi che sono sempre più collettivi e di respiro globale, dai problemi di sicurezza (cyber e non), alle catene di approvvigionamento delle risorse a minacce per la stessa esistenza della specie, come il cambiamento climatico o l'antibiotico resistenza.

Affinché si possa continuare ad evolvere ed affrontare i grandi temi che riguardano l'umanità è necessario che questo motore alla base dell'evoluzione umana rimanga ben vivo anche e soprattutto nell'era dell'AI, in modo che l**a tecnologia continui ad essere una risposta ai bisogni dell'uomo e non diventi uno strumento per creare nuovi bisogni**.

La tempesta perfetta: complessità e semplificazione

Nell'attuale panorama digitale, stiamo affrontando quella che potremmo definire una "tempesta perfetta". Da un lato, il mondo si fa sempre più complesso: per affrontare problemi su scala globale il processo di digitalizzazione sta procedendo in modo disordinato e non strutturato, con una moltitudine di attori che perseguono simultaneamente obiettivi individuali, aumentando esponenzialmente la complessità del sistema. Dall'altro lato, vi è la tendenza a semplificare il sistema attraverso la tecnologia, confidando in particolare nell'AI generativa come mezzo per semplificare questa complessità, **alla stregua di un oracolo**. Ma proprio come un oracolo, i meccanismi e le basi dati su cui poggia questa tecnologia non sono trasparenti o accessibili agli utilizzatori, che così si trovano a delegare l'onere della decisione a soggetti terzi.

Di fronte a questo scenario appare evidente che l'utopia iniziale che portò alla nascita di Internet come sistema neutrale, aperto e paritario che rimuove gli intermediari dall'accesso al sapere, si sta rapidamente trasformando in una realtà in cui **pochi giganti tecnologici detengono un potere sempre maggiore**, di fatto diventando nuovi intermediari del sapere.

Questa situazione rischia di scivolare verso un contesto distopico in cui la capacità decisionale viene delegata a una manciata di soggetti che controllano l'AI. Rimanendo in ambito di metafora, ciò che si prefigura è un futuro in cui il **golem**, l'automa privo di vera intelligenza ma dotato di una forza sovrumana creato per aiutare l'essere umano, diventa autonomo e sfugge al controllo del suo creatore.

Investimenti globali, vantaggi, rischi ed effetti collaterali dell'AI

Gli investimenti globali nell'AI hanno raggiunto cifre record, con gli Stati Uniti e la Cina in testa e l'Europa che insegue a distanza. Questi investimenti massicci stanno alimentando un'accelerazione senza precedenti nello sviluppo dell'AI.

Nonostante i potenziali benefici, l'adozione diffusa dell'AI comporta anche rischi significativi e effetti collaterali che non possono essere ignorati. Innanzitutto è importante sottolineare che l'AI generativa sia una tecnologia estremamente energivora a causa del gran numero di data centre necessari al suo funzionamento. Da un punto di vista ambientale, **la sostenibilità dei grossi sistemi di deep learning (LLM) è in discussione** al punto che, a causa dell'aumento delle emissioni di CO_2 prodotta, grossi player come Google hanno dichiarato che difficilmente potranno raggiungere gli obiettivi climatici di carbon neutrality del 2030. Inoltre, uno dei rischi più pressanti è sicuramente la polarizzazione delle risorse e del potere decisionale nelle mani di pochi attori tecnologici dominanti. Questa concentrazione di potere è accentuata dalle enormi barriere all'ingresso rappresentate dagli investimenti necessari per sviluppare e addestrare modelli AI avanzati.

Mantenere il controllo: il ruolo dell'università e della ricerca

L'AI generativa può portare tanti benefici ma i rischi vanno presi in considerazione. Per scongiurare il rischio di omologazione e continuare ad essere rilevanti nella creazione di nuovo sapere e di innovazione, è necessario che la comunità accademica e della ricerca, e GARR con essa, partecipino allo sviluppo di questa tecnologia, investendo tempo e risorse per poter utilizzare l'AI in modo consapevole ma anche economicamente sostenibile. È necessario partecipare allo sviluppo tecnologico nonostante l'attuale asimmetria di risorse in gioco con i big player. Per fare ciò è necessario dotarsi degli strumenti che permettendo di mantenere l'autonomia, ossia la capacità di porsi nuove domande per immaginare nuove risposte e nuove soluzioni, oltre alle richieste del mercato e con la lungimiranza che solo chi pensa al futuro può avere.

Un modo per mantenere il controllo della tecnologia, sfruttando al contempo le capacità dell'AI generativa può essere quello di sviluppare SLM (Small Language Model) con dati interni per sviluppare la knowledge base, una soluzione che è più facilmente controllabile rispetto ad un LLM, sebbene richieda dati di maggiore qualità per l'addestramento e un lavoro maggiore da parte dei data scientist. Nel caso di GARR, una soluzione di questo tipo permetterebbe di sfruttare i molti dati a disposizione sulla rete per ottimizzarla, coltivando e mantenendo le competenze necessarie per il suo funzionamento.

A livello di **comunità della ricerca**, però, è necessario il coinvolgimento di tutti gli attori in gioco, dallo stato alle università al sistema paese e alle collaborazioni con le industrie. A livello europeo è importante collaborare per avere strumenti che aiutino la ricerca europea e non la frenino.

Un modo per mantenere il controllo della tecnologia è quello di sviluppare Small Language Model con dati interni per sviluppare la knowledge base

Comprendere per innovare

Affinché la comunità a della ricerca continui a contribuire alla conoscenza e a fare innovazione è fondamentale cogliere l'opportunità di far parte di questa tecnologia da protagonisti, fungendo da argine all'oligopolio delle grandi aziende al suo sviluppo.

L'idea è quella di **continuare a creare innovazione e tecnologia**, investendo sulle competenze e sviluppando soluzioni che riescano a sfruttare il valore aggiunto dell'AI senza delegare l'onere della decisione. Ritornando alla metafora del golem: è importante mantenere la conoscenza (emet) per poter controllare la tecnologia.

Guarda la presentazione di Massimo Carboni in occasione della Conferenza GARR 2024

Gli utenti della rete GARR

RETE GARR

La rete GARR è realizzata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Istruzione, dell'Università e della Ricerca. La rete GARR è diffusa in modo capillare e offre connettività a circa 1000 sedi.

Soci:
CNR, ENEA, Fondazione CRUI, INAF, INFN, INGV, le università statali italiane, gli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e gli Istituti Zooprofilattici Sperimentali (IZS)

CNR

- Area della Ricerca di Bari
- Area della Ricerca di Bologna
- Area della Ricerca di Catania
- Area della Ricerca di Cosenza
- Area della Ricerca di Firenze
- Area della Ricerca di Genova
- Area della Ricerca di Lecce
- Area della Ricerca di Milano 1
- Area della Ricerca di Milano 3
- Area della Ricerca di Milano 4
- Area della Ricerca di Napoli
- Area della Ricerca di Padova
- Area della Ricerca di Palermo
- Area della Ricerca di Pisa
- Area della Ricerca di Portici (NA)
- Area della Ricerca di Potenza
- Area della Ricerca di Pozzuoli (NA)
- Area della Ricerca di Roma1
- Area della Ricerca di Roma 2
- Area della Ricerca di Sassari
- Area della Ricerca di Torino
- Base radar, Mesagne (BR), Torchiarolo (BR)
- Biblioteca Area della Ricerca, Bologna
- Biomics Bioinformatica per le Scienze Omiche, Bari
- Complesso di Anacapri, ex Osservatorio Solare Svedese, Anacapri (NA)
- IAC Ist. per le Applicazioni del Calcolo M. Picone, Napoli
- IAS - Ist. per lo studio degli impatti Antropici e Sostenibilità in ambiente marino, Capo Granitola (TP), Castellammare del Golfo (TP), Oristano, Genova
- IBB Ist. di Biostrutture e Bioimmagini, Napoli
- IBBA Ist. di Biologia e Biotecnologia Agraria, Milano, Pisa
- IBBE Ist. di Biomembrane e Bioenergetica, Bari
- IBBR Ist. Bioscienze e BioRisorse, Palermo, Portici (NA)
- IBCN Ist. di Biologia Cellulare e Neurobiologia, Monterotondo Scalo (RM)
- IBE Ist. per la BioEconomia, Bologna, Firenze, Follonica (GR), San Michele Adige (TN), Sassari, Livorno, Sesto Fiorentino (FI)
- IBF Ist. di Biofisica, Genova, Pisa
- IBFM Ist. di Bioimmagini e Fisiologia Molecolare, Milano
- IBP Ist. di Biochimica delle Proteine, Napoli
- ICAR Ist. di Calcolo e Reti ad Alte Prestazioni- Palermo, Napoli, Arcavacata di Rende (CS)
- ICB Ist. di Chimica Biomolecolare, Catania, Pozzuoli (NA), Sassari
- ICCOM Ist. di Chimica dei Composti Organo Metallici, Bari, Pisa
- ICMATE Ist. di Chimica della Materia Condensata e di Tecnologie per l'Energia, Lecco
- ICVBC Ist. per la Conservazione e la Valorizzazione dei Beni Culturali, Milano
- IEIIT Ist. di Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni, Genova
- IENI Ist. per l'Energetica e le Interfasi, Genova, Milano, Padova
- IEOS Ist. per l'Endocrinologia e l'Oncologia "Gaetano Salvatore", Napoli
- IFC Ist. di Fisiologia Clinica, Lecce, Massa Carrara, Milano, Pisa, Reggio Calabria
- IFT Ist. Farmacologia Traslazionale, L'Aquila
- IGAG Ist. di Geologia Ambientale e Geoingegneria, Milano
- IGB Ist. di Genetica e Biofisica "Adriano Buzzati Traverso", Napoli
- IGG Ist. di Geoscienze e Georisorse, Pavia, Pisa, Torino
- IGM Ist. di Genetica Molecolare, Chieti, Pavia
- IIT Ist. di Informatica e Telematica, Pisa, Arcavacata di Rende (CS)
- ILC Ist. di Linguistica Computazionale, Pisa, Genova
- IMAA Ist. di Metodologie per l'Analisi Ambientale, Tito Scalo (PZ), Marsico Nuovo (PZ)
- IMATI Ist. di Matematica Applicata e Tecnologie Informatiche "E. Magenes", Genova, Milano, Pavia
- IMEM Ist. dei Materiali per l' Elettronica ed il Magnetismo, Parma
- IMM Ist. per la Microelettronica e i Microsistemi, Agrate Brianza (MB), Bologna, Catania, Lecce, Roma
- IN Ist. di Neuroscienze, Milano, Pisa
- INM Ist. di Ingegneria del Mare (INM), Roma
- INO Ist. Nazionale di Ottica, Firenze, Pisa, Pozzuoli (NA)
- IOM Ist. Officina dei Materiali, Trieste
- IPCB Ist. per i Polimeri, Compositi e Biomateriali, Catania, Napoli, Portici (NA), Pozzuoli (NA)
- IPCF Ist. di Tecnologie Biomediche, Bari, Pisa, Messina
- IPSP Ist. per la Protezione Sostenibile delle Piante, Bari, Portici (NA), Torino
- IRBIM Ist. per le Risorse Biologiche e le Biotecnologie Marine, Ancona, Mazara del Vallo (TP), Messina
- IRCrES Ist. di Ricerca sulla Crescita Economica Sostenibile, Milano, Moncalieri (TO), Torino
- IREA Ist. per il Rilevamento Elettromagnetico dell'Ambiente, Milano, Napoli
- IRET Ist. di Ricerca sugli Ecosistemi Terrestri, Napoli, Porano (TR), Sassari
- IRGB Ist. di Ricerca Genetica e Biomedica, Lanusei (OG), Monserrato (CA), Sassari
- IRIB Ist. per la Ricerca e l'Innovazione Biomedica, Catanzaro, Messina
- IRISS Ist. di Ricerca su Innovazione e Servizi per lo Sviluppo, Napoli
- IRPI Ist. di Ricerca per la Protezione Idrogeologica, Padova, Perugia, Torino
- IRPPS Ist. di Ricerche sulla Popolazione e le Politiche Sociali, Penta di Fisciano (SA), Roma
- IRSA Ist. di Ricerca sulle Acque, Bari, Brugherio (MB), Taranto, Verbania Pallanza (VB)
- ISA Ist. di Scienze dell'Alimentazione, Avellino
- ISAC Ist. di Scienze dell'Atmosfera e del Clima, Bologna, Lamezia Terme (CZ), Lecce, Padova, Torino
- ISAFoM Ist. per i Sistemi Agricoli e Forestali del Mediterraneo, Ercolano (NA)
- ISASI Ist. di Scienze Applicate e Sistemi Intelligenti "Eduardo Caianiello", Napoli, Pozzuoli (NA)
- ISE Ist. per lo Studio degli Ecosistemi, Pisa
- ISEM Ist. di Storia dell'Europa Mediterranea, Cagliari, Roma
- ISIB Ist. di Ingegneria Biomedica, Padova
- ISM Ist. di Struttura della Materia, Tito Scalo (PZ), Trieste
- ISMAC Ist. per lo Studio delle Macromolecole, Milano
- ISMAR Ist. di Scienze Marine, Bologna, Genova, Lesina (FG), Napoli, Pozzuolo di Lerici (SP), Trieste, Venezia
- ISMed Ist. di Studi sul Mediterraneo, Napoli
- ISMN Ist. per lo Studio dei Materiali Nanostrutturati, Bologna
- ISN Ist. di Scienze Neurologiche, Catania, Mangone (CS)
- ISOF Ist. per la Sintesi Organica e la Fotoreattività, Bologna
- ISP Ist. di Scienze Polari, Padova
- ISPA Ist. di Scienze delle Produzioni Alimentari, Foggia, Lecce, Oristano, Sassari
- ISPAAM Ist. per il Sistema Produzione Animale in Ambiente Mediterraneo, Napoli, Sassari
- ISPC Ist. di Scienze del Patrimonio Culturale, Lecce, Tito Scalo (PZ)
- ISPF Ist. per la Storia del Pensiero Filosofico e Scientifico Moderno, Milano
- ISSIA Ist. di Studi sui Sistemi Intelligenti per l'Automazione, Genova
- ISSMC, Ist. di Scienza, Tecnologia e Sostenibilità per lo Sviluppo dei Materiali Ceramici, Faenza (RA)
- ISTC Ist. di Scienze e Tecnologie della Cognizione, Padova, Roma
- ISTEC Ist. di Scienza e Tecnologia dei Materiali Ceramici, Torino
- ISTI Ist. di Scienza e Tecnologie dell'Informazione, Pisa
- ISTM Ist. di Scienze e Tecnologie Molecolari, Milano
- ISTP Ist. per la Scienza e Tecnologia dei Plasmi, Milano, Padova

- ITAE Ist. di Tecnologie Avanzate per l'Energia, Messina
- ITB Ist. di Tecnologie Biomediche, Pisa, Segrate (MI)
- ITC Ist. per le tecnologie della costruzione, Bari, L'Aquila, Milano, Padova, San Giuliano Milanese (MI)
- ITD Ist. per le Tecnologie Didattiche, Genova
- ITM Ist. per la Tecnologia delle Membrane, Arcavacata di Rende (CS)
- ITTIG Ist. di Teoria e Tecniche dell'Informazione Giuridica, Firenze
- NANOTEC Ist. di Nanotecnologia, Lecce, Bari
- OVI Ist. del Vocabolario Italiano, Firenze
- SCITEC Ist. di Scienze e Tecnologie Chimiche "Giulio Natta", Genova, Milano, Roma
- Sede Centrale, Roma
- SPIN Ist. per i Superconduttori, Materiali Innovativi e Dispositivi, Genova
- SPR RSI Struttura di Particolare Rilievo Reti e Sistemi Informativi, Roges di Rende (CS)
- STEMS - Ist. di Scienze e Tecnologie per l'Energia e la Mobilità Sostenibili, Candiolo (TO), Cassana (FE), Napoli, Torino
- STIIMA Ist. di Sistemi e Tecnologie Industriali Intelligenti per il Manifatturiero Avanzato, Biella, Milano
- UARIE - Ufficio Attività e Relazioni con Istituzioni Europee, Napoli

ENEA

- Centro ricerche Ambiente Marino S. Teresa, Pozzuolo di Lerici (SP)
- Centro ricerche Bologna
- Centro ricerche Brasimone, Camugnano (BO)
- Centro ricerche Brindisi
- Centro ricerche Casaccia, S.Maria di Galeria (RM)
- Centro ricerche Frascati (RM)
- Centro ricerche Portici (NA)
- Centro ricerche Saluggia (VC)
- Centro ricerche Trisaia, Rotondella (MT)
- Laboratori di ricerca Faenza (RA)
- Laboratori di ricerca Foggia
- Laboratori di ricerca Ispra (VA)
- Laboratori di ricerca Lampedusa (AG)
- Laboratori di ricerca Montecuccolino, Bologna
- Sede centrale, Roma
- Ufficio territoriale della Puglia, Bari
- Ufficio territoriale della Sicilia, Palermo
- Ufficio territoriale della Toscana, Pisa

INAF

- CTA Cherenkov Telescope Array, Roma
- IASF Istituto di Astrofisica Spaziale e Fisica Cosmica, Bologna, Milano, Palermo
- OAC SRT Sardinia Radio Telescope, S. Basilio (CA)
- IRA Istituto di Radioastronomia, Bologna, Staz. Radioastronomica di Noto (SR), Staz. Radioastronomica di Medicina (BO)
- Laboratorio di Astrofisica di Palermo
- Osservatorio Astrofisico di Arcetri (FI)
- Osservatorio Astrofisico di Catania
- Osservatorio Astronomico di Abruzzo, Teramo
- Osservatorio Astronomico di Bologna
- Osservatorio Astronomico di Brera, Merate (LC), Milano
- Osservatorio Astronomico di Cagliari, Selargius (CA)
- Osservatorio Astronomico di Capodimonte, Napoli
- Osservatorio Astronomico di Padova
- Osservatorio Astronomico di Palermo
- Osservatorio Astronomico di Roma, Monte Porzio Catone (RM)
- Osservatorio Astronomico di Torino, Pino Torinese (TO)
- Osservatorio Astronomico di Trieste
- Presidenza, Roma

INFN

- Amministrazione centrale, Frascati (RM)
- CNAF Centro Nazionale per la ricerca e lo sviluppo nelle tecnologie informatiche e telematiche, Bologna
- Gruppo collegato dell'Aquila
- Gruppo collegato di Alessandria
- Gruppo collegato di Brescia
- Gruppo collegato di Cosenza
- Gruppo collegato di Messina
- Gruppo collegato di Parma
- Gruppo collegato di Salerno
- Gruppo collegato di Siena
- Gruppo collegato di Udine Laboratori Nazionali del Gran Sasso, Assergi (AQ)
- Laboratori Nazionali del Sud, Catania
- Laboratori Nazionali di Frascati (RM)
- Laboratori Nazionali di Legnaro (PD)
- Laboratorio Portopalo di Capo Passero (SR)
- Sezione di Bari
- Sezione di Bologna
- Sezione di Cagliari
- Sezione di Catania
- Sezione di Ferrara
- Sezione di Firenze
- Sezione di Genova
- Sezione di Lecce
- Sezione di Milano
- Sezione di Milano-Bicocca
- Sezione di Napoli
- Sezione di Padova
- Sezione di Pavia
- Sezione di Perugia
- Sezione di Pisa
- Sezione di Roma
- Sezione di Roma-Tor Vergata
- Sezione di Roma Tre
- Sezione di Torino
- Sezione di Trieste
- TIFPA Trento Institute for Fundamental Phisycs and Application, Povo (TN)
- Uffici di Presidenza, Roma

INGV

- Amministrazione Centrale, Roma
- Sede distaccata di Grottaminarda (AV), Sede Irpinia
- Sede distaccata di Lipari (ME), Osservatorio Geofisico
- Sede distaccata di Nicolosi (CT)
- Sede distaccata di Stromboli (ME), Centro Operativo
- Sezione di Bologna
- Sezione di Catania, CUAD Sistema Poseidon
- Sezione di Catania, Osservatorio Etneo
- Sezione di Catania, Sede di Messina
- Sezione di Cosenza
- Sede Storica, Ercolano (NA)
- Sezione di Napoli, Osservatorio Vesuviano
- Sezione di Milano
- Sezione di Messina
- Sezione di Palermo
- Sezione di Pisa
- Sezione di Portopalo di Capo Passero (SR)

IRCCS Istituti di Ricovero e Cura a Carattere Scientifico

- Azienda Ospedaliero Universitaria, Bologna
- Azienda Ospedaliera Universitaria Meyer, Firenze
- Centro Cardiologico S.P.A. Fondazione Monzino, Milano
- Centro Neurolesi Bonino Pulejo, Messina
- Centro San Giovanni di Dio Fatebenefratelli, Brescia
- CROB Centro di riferimento oncologico della Basilicata, Rionero in Vulture (PZ)
- CRO Centro di Riferimento Oncologico, Aviano (PN)
- Ente Ospedaliero specializzato in gastroenterologia Saverio De Bellis, Castellana Grotte (BA)
- Fondazione Ca'Granda – Ospedale Maggiore Policlinico, Milano
- Fondazione del Piemonte per l'Oncologia, Candiolo (TO)
- Fondazione Don Carlo Gnocchi, Milano
- Fondazione G.B. Bietti per lo studio e la ricerca in oftalmologia, Roma
- Fondazione IRCCS Ist. Nazionale dei tumori, Milano
- Fondazione Ist. Neurologico Carlo Besta, Milano
- Fondazione Ist. Neurologico Casimiro Mondino, Pavia
- Fondazione Policlinico San Matteo, Pavia
- Fondazione Policlinico Universitario Gemelli, Roma
- Fondazione San Gerardo dei Tintori, Monza (MB)
- Fondazione Santa Lucia, Roma
- Fondazione Stella Maris, Calambrone (PI)
- IDI Ist. Dermopatico dell'Immacolata, Roma
- IEO Ist. Europeo di Oncologia, Milano
- IFO Ist. Fisioterapici Ospitalieri, Ist. Dermatologico Santa Maria e San Gallicano, Roma
- ISMETT Ist. Mediterraneo per i Trapianti e Terapie ad Alta Specializzazione, Palermo
- Ist. Auxologico Italiano, Milano
- Ist. Clinici Scientifici Maugeri, Pavia
- Ist. Clinico Humanitas, Rozzano (Milano)
- Ist. delle Scienze Neurologiche, Bologna
- Ist. Eugenio Medea, Bosisio Parini (LC)
- Ist. Giannina Gaslini, Genova
- Ist. Nazionale di Riposo e Cura per Anziani, Ancona
- Ist. Nazionale Tumori Fondazione Giovanni Pascale, Napoli
- Ist. Neurologico Mediterraneo Neuromed, Pozzilli (IS)
- Ist. Oncologico Veneto, Padova
- Ist. Ortopedico Galeazzi, Milano
- Ist. Ortopedico Rizzoli, Bologna
- Ist. per le Malattie Infettive L. Spallanzani, Roma
- Ist. scientifico romagnolo per lo studio e la cura dei tumori, Meldola (FC)
- Ist. Tumori Giovanni Paolo II, Bari
- Multimedica, Milano
- Oasi di Maria Santissima, Troina (EN)
- Ospedale Casa Sollievo della Sofferenza, San Giovanni Rotondo (FG)
- Ospedale infantile Burlo Garofolo, Trieste
- Ospedale pediatrico Bambino Gesù, Roma
- Ospedale Policlinico San Martino, Genova
- Ospedale San Raffaele, Milano
- Policlinico San Donato, S. Donato Milanese
- San Camillo IRCCS S.r.l., Venezia
- San Raffaele Pisana, Roma
- SYNLAB SDN, Napoli

IZS Istituti Zooprofilattici Sperimentali

- IZS del Lazio e della Toscana, Roma
- IZS del Mezzogiorno, Portici (NA)
- IZS del Piemonte, Liguria e Valle d'Aosta, Torino
- IZS dell'Abruzzo e del Molise G. Caporale, Teramo
- IZS dell'Umbria e delle Marche, Perugia
- IZS della Lombardia e dell'Emilia Romagna, Brescia
- IZS della Puglia e della Basilicata, Foggia
- IZS della Sardegna, Sassari
- IZS della Sicilia M. Mirri, Palermo
- IZS delle Venezie, Legnaro (PD)

Università

Università statali

- CRUI Conferenza dei Rettori delle Università Italiane, Roma
- GSSI Gran Sasso Science Institute, L'Aquila
- IMT Institutions, Markets, Technologies Institute for Advanced Studies, Lucca
- IUSS Istituto Universitario di Studi Superiori, Pavia
- Politecnico di Bari
- Politecnico di Milano
- Politecnico di Torino
- Scuola Normale Superiore, Pisa
- Scuola Superiore S.Anna, Pisa
- Scuola Superiore Meridionale
- Seconda Università degli Studi di Napoli
- SISSA Scuola Internazionale Superiore di Studi Avanzati, Trieste
- Università Ca' Foscari Venezia
- Università della Basilicata
- Università della Calabria
- Università della Tuscia
- Università dell'Aquila
- Università dell'Insubria
- Università del Molise
- Università del Piemonte Orientale Amedeo Avogadro
- Università del Salento
- Università del Sannio
- Università di Bari Aldo Moro
- Università di Bergamo
- Università di Bologna
- Università di Brescia
- Università di Cagliari
- Università di Camerino
- Università di Cassino e del Lazio Meridionale
- Università di Catania
- Università di Chieti-Pescara G. D'Annunzio
- Università di Ferrara
- Università di Firenze
- Università di Foggia
- Università di Genova
- Università di Macerata
- Università di Messina
- Università di Milano
- Università di Milano-Bicocca
- Università di Modena e Reggio Emilia
- Università di Napoli Federico II
- Università di Napoli L'Orientale
- Università di Napoli Parthenope
- Università di Padova
- Università di Palermo
- Università di Parma
- Università di Pavia
- Università di Perugia
- Università di Pisa
- Università di Roma Foro Italico
- Università di Roma La Sapienza
- Università di Roma Tor Vergata
- Università di Roma Tre
- Università di Salerno
- Università di Sassari
- Università di Siena
- Università di Teramo
- Università di Torino
- Università di Trento
- Università di Trieste
- Università di Udine
- Università di Urbino Carlo Bo
- Università di Verona
- Università IUAV di Venezia
- Università Magna Græcia di Catanzaro
- Università Mediterranea di Reggio Calabria
- Università per Stranieri di Perugia
- Università per Stranieri di Siena
- Università Politecnica delle Marche

Università non statali

- Humanitas University, Pieve Emanuele (MI)
- IULM Libera Università di Lingue e Comunicazione, Milano
- Libera Università di Bolzano
- Libera Università di Enna Kore
- LUISS Libera Università Internazionale degli Studi Sociali Guido Carli, Roma
- LUM Libera Università Mediterranea J. Monnet, Casamassima (BA)
- LUMSA Libera Università Maria SS. Assunta, Roma, Palermo
- SDA Bocconi School of Management, Roma
- UNINT Università degli Studi Internazionali di Roma
- UniTelma Sapienza, Roma
- Università Campus Bio-Medico di Roma
- Università Cattolica del Sacro Cuore, Milano
- Università Commerciale Luigi Bocconi, Milano
- Università della Valle d'Aosta, Aosta
- Università Suor Orsola Benincasa, Napoli
- Università Telematica Internazionale Uninettuno, Roma
- Università Vita-Salute San Raffaele, Milano

Università Internazionali

- Cornell University, Roma
- European University Institute, Firenze
- Johns Hopkins University, Bologna
- New York University, Firenze
- The American University of Rome, Roma
- Venice International University, Venezia

Consorzi interuniversitari, collegi, enti per il diritto allo studio

- CINECA, Napoli, Roma, Bologna
- CISIA Consorzio Interuniversitario Sistemi Integrati per l'Accesso, Pisa
- Collegio Ghislieri, Pavia
- Collegio Nuovo - Fondaz. Sandra e Enea Mattei, Pavia
- Collegio Universitario Alessandro Volta, Pavia
- Collegio Universitario Santa Caterina da Siena, Pavia

Enti di ricerca scientifica e tecnologica

- AREA Science Park, Trieste
- ARPAS Agenzia Regionale per la Protezione dell'Ambiente della Sardegna, Cagliari, Sassari
- ASI Agenzia Spaziale Italiana
  - ALTEC Advanced Logistic Technology
  - Engineering Center, Torino
  - Centro di Geodesia Spaziale, Matera
  - Centro Spaziale del Fucino, Avezzano (AQ)
  - Scientific Data Center, Roma
  - Sede Centrale, Roma
  - Sardinia Deep Space Antenna, San Basilio (CA)
- Centro Fermi - Museo Storico della Fisica e Centro Studi e Ricerche Enrico Fermi, Roma
- CERIC - ERIC Central European Research Infrastructure Consortium, Basovizza (TS)
- CIRA Centro Italiano Ricerche Aerospaziali, Capua (CE)
- CMCC Centro Euro-Mediterraneo per i Cambiamenti Climatici, Bologna, Lecce
- CNIT Laboratorio Nazionale di Comunicazioni Multimediali, Napoli
- Consorzio CETMA Centro di Progettazione, Design e Tecnologie dei Materiali, Brindisi
- Consorzio TeRN Tecnologie per le Osservazioni della Terra e i Rischi Naturali, Tito Scalo (PZ)
- CORILA Consorzio Gestione del Centro di Coordinamento delle Attività di Ricerca Inerenti al Sistema Lagunare di Venezia
- COSBI The Microsoft Research – University of Trento Centre for Computational and Systems Biology, Rovereto (TN)
- CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria, Bari, Bologna, Pontecagnano (SA)
- CRS4 Centro Ricerca, Sviluppo e Studi Superiori in Sardegna, Pula (CA)
- CSP Innovazione nelle ICT, Torino
- CTAO - Cherenkov Telescope Array Observatory, Bologna
- ECMWF European Centre for Medium-Range Weather Forecasts, Bologna
- EGO European Gravitational Observatory, Cascina (PI)
- EUMETSAT European Organisation for the Exploitation of Meteorological Satellites, Avezzano (AQ)
- FBK Fondazione B. Kessler, Trento
- FIT Fondazione Internazionale Trieste
- Fondazione E. Amaldi, Roma
- G. Galilei Institute for Theoretical Physics, Firenze
- Global Campus of Human Rights, Venezia
- Hypatia - Consorzio di Ricerca sulle Tecnologie per lo Sviluppo sostenibile, Roma
- ICRA International Centre for Relativistic Astrophysics, Roma
- ICTP Centro Internaz. di Fisica Teorica, Trieste
- IIT Istituto Italiano di Tecnologia, Aosta, Bari, Genova, Lecce, Milano, Napoli, Roma, Torino
- INRIM Ist. Nazionale di Ricerca Metrologica, Torino
- ISPRA Istituto Superiore per la Protezione e la Ricerca Ambientale, Livorno, Roma, Ozzano dell'Emilia (BO), Palermo, Venezia
- ISTAT Istituto Nazionale di Statistica, Roma
- LaMMA Laboratorio di Monitoraggio e Modellistica Ambientale per lo sviluppo sostenibile, Livorno, Sesto Fiorentino (FI)
- JRC Joint Research Centre, Ispra (VA)
- LENS Laboratorio Europeo di Spettroscopie Non Lineari, Firenze
- NATO CMRE, Centre for Maritime Research and Experimentation, La Spezia
- OGS Istituto Nazionale di Oceanografia e di Geofisica Sperimentale, Sgonico (TS), Udine
- Registro.it, Pisa, Milano, Roma
- Sincrotrone Trieste
- Stazione Zoologica A. Dohrn, Ischia, Messina, Napoli, Portici (NA)

Istituti di ricerca biomedica

- Azienda Ospedaliera Monaldi, Napoli
- Azienda Ospedaliero-Universitaria, Cagliari
- CBIM Consorzio di Bioingegneria e Informatica Medica, Pavia
- EMBL European Molecular Biology Laboratory, Monterotondo (RM)
- Fondazione CNAO - Centro Nazionale di Adroterapia Oncologica, Pavia
- Fondazione Human Technopole, Milano
- Fondazione Toscana Gabriele Monasterio per la Ricerca Medica e di Sanità Pubblica, Pisa
- ICGEB International Centre for Genetic Engineering and Biotechnology, Trieste
- IIGM Foundation - Italian Institute for Genomic Medicine, Torino
- ISS Istituto Superiore di Sanità, Roma
- TIGEM Telethon Institute of Genetics and Medicine, Napoli, Pozzuoli (NA)

Istituti di cultura, ricerca e promozione scientifica

- Accademia della Crusca, Firenze
- Accademia Nazionale dei Lincei, Roma
- Centro Congressi Ex Casinò e Palazzo del Cinema, Venezia
- Chancellerie des Universités de Paris, Villa Finaly, Firenze
- Comando per la Formazione e Scuola di Applicazione dell'Esercito di Torino
- Ecole Française de Rome
- ESCP École Supérieure de Commerce de Paris - Business School, Torino
- EURAC Accademia Europea di Bolzano
- FEEM Fondazione ENI E. Mattei, Milano, Venezia
- Fondazione Collegio Carlo Alberto - Centro di Ricerca e Alta Formazione, Torino
- Fondazione E. Majorana e Centro di Cultura Scientifica, Erice (TP)
- Fondazione Eucentre Centro Europeo di Formazione e Ricerca in Ingegneria Sismica, Pavia
- Fondazione IDIS - Città della Scienza, Napoli
- Fondazione LINKS Leading Innovation & Knowledge for Society, Torino
- Fondazione per la Scuola della Compagnia di San Paolo, Torino
- Fondazione U. Bordoni, Milano, Roma
- Fondazione Ufficio Pio della Compagnia di San Paolo, Torino
- Fondazione 1563 per l'Arte e la Cultura della Compagnia di San Paolo, Torino
- GSoM Graduate School of Management, Milano
- INSR Ist. Nazionale di Studi sul Rinascimento, Firenze
- Istituto di Norvegia in Roma
- IVSLA Istituto Veneto, Accademia di Scienze, Lettere ed Arti, Venezia
- Kunsthistorisches Institut in Florenz - M.Planck Institut, Firenze
- LIS Laboratorio dell'Immaginario Scientifico, Grignano (TS)
- MIB - School of Management, Trieste
- MUSE Museo delle Scienze, Trento
- Museo Galileo - Istituto e Museo di Storia della Scienza, Firenze
- San Servolo Servizi Metropolitani di Venezia

Archivi, biblioteche, musei

- Archivio di Stato di Bologna
- Archivio di Stato Centrale, Roma
- Archivio di Stato di Milano
- Archivio di Stato di Napoli
- Archivio di Stato di Palermo
- Archivio di Stato di Roma
- Archivio di Stato di Torino
- Archivio di Stato di Torino - Sezioni Riunite
- Archivio di Stato di Venezia
- Biblioteca Angelica, Roma
- Biblioteca Casanatense, Roma
- Biblioteca di Storia Moderna e Contemporanea, Roma
- Biblioteca Estense e Universitaria, Modena
- Biblioteca Europea di Informazione e Cultura, Milano
- Biblioteca Marucelliana, Firenze
- Biblioteca Medica Statale, Roma
- Biblioteca Medicea Laurenziana, Firenze
- Biblioteca Nazionale Braidense, Milano
- Biblioteca Nazionale Centrale di Firenze
- Biblioteca Nazionale Centrale V. Emanuele II di Roma
- Biblioteca Nazionale Marciana, Venezia
- Biblioteca Nazionale Universitaria di Torino
- Biblioteca Palatina, Parma
- Biblioteca Riccardiana, Firenze
- Biblioteca Statale Antonio Baldini, Roma
- Biblioteca Statale di Trieste
- Biblioteca Universitaria Alessandrina, Roma
- Biblioteca Universitaria di Bologna
- Biblioteca Universitaria di Genova
- Biblioteca Universitaria di Napoli
- Biblioteca Universitaria di Padova
- Biblioteca Universitaria di Pavia
- Biblioteca Universitaria di Pisa
- Bibliotheca Hertziana Ist. M. Planck per la Storia dell'Arte, Roma
- Fondazione Palazzo Strozzi, Firenze
- Galleria dell'Accademia di Firenze
- Gallerie degli Uffizi, Firenze
- ICCU Ist. Centrale per il Catalogo Unico delle Biblioteche Italiane e per le Informazioni bibliografiche, Roma
- Ist. Centrale per gli Archivi, Roma
- Ist. Centrale per i Beni Sonori ed Audiovisivi. Roma
- Ministero della Cultura - Direzione Generale Educazione, ricerca e istituti culturali, Roma
- Museo Nazionale Romano - Crypta Balbi, Palazzo Altemps, Palazzo Massimo, Terme di Diocleziano
- Parco Archeologico del Colosseo, Roma - Colosseo e Palatino, via in Miranda
- Parco Archeologico di Pompei
- Procuratoria di San Marco, Venezia

Accademie, conservatori, istituti d'arte

- Accademia di Belle Arti di Bologna
- Accademia di Belle Arti di Brera, Milano
- Accademia di Belle Arti di Firenze
- Accademia di Belle Arti de L'Aquila
- Accademia di Belle Arti di Macerata
- Accademia di Belle Arti di Palermo
- Accademia di Belle Arti di Perugia
- Accademia di Belle Arti di Urbino
- Accademia di Belle Arti di Venezia
- Conservatorio di Musica N. Piccinni, Bari
- Conservatorio di Musica C. Monteverdi, Bolzano
- Conservatorio di Musica G. Verdi, Como
- Conservatorio di Musica S. Giacomantonio, Cosenza
- Conservatorio di Musica C. Monteverdi, Cremona
- Conservatorio di Musica G.F. Ghedini, Cuneo
- Conservatorio di Musica G. Frescobaldi, Ferrara
- Conservatorio di Musica L. Cherubini, Firenze
- Conservatorio di Musica L. Refice, Frosinone
- Conservatorio di Musica N. Paganini, Genova
- Conservatorio di Musica Egidio R. Duni, Matera
- Conservatorio di Musica G. Puccini, La Spezia
- Conservatorio di Musica P. Mascagni, Livorno
- Conservatorio di Musica G. Verdi, Milano
- Conservatorio di Musica G. Cantelli, Novara
- Conservatorio di Musica C. Pollini, Padova
- Conservatorio di Musica A. Boito, Parma
- Conservatorio di Musica A.Casella, L'Aquila
- Conservatorio di Musica F. Vittadini, Pavia
- Conservatorio di Musica G. Rossini, Pesaro
- Conservatorio di Musica G. Lettimi, Rimini
- Conservatorio di Musica Santa Cecilia, Roma
- Conservatorio di Musica G. Martucci, Salerno
- Conservatorio di Musica R. Franci, Siena
- Conservatorio di Musica G. Tartini, Trieste
- Conservatorio di Musica J. Tomadini, Udine
- Ist. Superiore per le Industrie Artistiche, Faenza (RA)
- Ist. Superiore per le Industrie Artistiche, Urbino

Scuole

Piemonte

- Convitto Nazionale Umberto I, Torino
- Liceo Statale Regina Margherita, Collegno (TO)
- Liceo Scientifico Ferraris, Torino
- ITI Majorana, Grugliasco (TO)
- IIS M. Curie - C. Levi, Collegno (TO)
- IIS Avogadro, Torino
- IIS Santorre di Santarosa, Torino
- ITIS Pininfarina, Moncalieri (TO)
- Scuole connesse nell'ambito della collaborazione tra GARR e CSP Innovazione nelle ICT
- Scuole connesse nell'ambito del progetto Riconnessioni finanziato dalla Fondazione per la Scuola della Compagnia di San Paolo e che vede la collaborazione di GARR e TOP-IX www.riconnessioni.it

Lombardia

- ISIS Carcano, Como
- IPS Pessina, Como
- ITE Caio Plinio II, Como
- Liceo Scientifico e Classico Majorana, Desio (MB)
- Scuola Europea di Varese

Veneto

- ITC Einaudi-Gramsci, Padova
- ITIS Severi, Padova
- Liceo delle Scienze Umane Amedeo di Savoia Duca d'Aosta, Padova
- Liceo Artistico Modigliani, Padova

Friuli Venezia-Giulia

- IT Zanon, Udine
- Liceo Marinelli, Udine
- Liceo Scientifico Galilei, Trieste
- Liceo Scientifico Oberdan, Trieste

Emilia-Romagna

- Scuole connesse nell'ambito della collaborazione con la rete dell'Emilia-Romagna Lepida

Liguria

- Convitto Nazionale Colombo, Genova
- IIS Ferraris-Pancaldo, Savona
- IIS Vittorio Emanuele II - Ruffini, Genova

Toscana

- IIS Cellini, Firenze
- IIS Enriques Agnoletti, Sesto Fiorentino (FI)
- IIS Salvemini-D'Aosta, Firenze
- IIS Vespucci-Colombo, Livorno
- IPSIA Fascetti, Pisa
- IPSSAR Matteotti, Pisa

- ISIS Leonardo da Vinci, Firenze
- IT Cappellini, Livorno
- ITC Pacinotti, Pisa
- ITIS Galileo Galilei, Livorno
- ITIS Leonardo da Vinci, Pisa
- Liceo Artistico Russoli, Pisa
- Liceo Classico Galileo Galilei, Pisa
- Liceo Scientifico Buonarroti, Pisa
- Liceo Scientifico Dini, Pisa
- Liceo Statale Carducci, Pisa
- Liceo Statale Federigo Enriques, Livorno
- Polo Liceale Francesco Cecioni, Livorno

Marche

- IIS Volterra Elia, Ancona
- ITIS Mattei, Urbino
- Liceo Scientifico Galilei, Ancona
- Liceo Scientifico e delle Scienze Umane Laurana-Baldi, Urbino

Lazio

- Convitto Nazionale Vittorio Emanuele II, Roma
- IIS Einaudi-Baronio, Sora (FR)
- IIS Caffè, Roma
- IIS Medaglia D'Oro, Cassino (FR)
- Istituto Magistrale Statale Gelasio Caetani, Roma
- ITCG Ceccherelli, Roma
- ITI Ferraris, Roma
- ITIS Volta, Roma
- IT Nautico Colonna, Roma
- ITS Pascal, Roma
- ITST Istituto Tecnico Fermi, Frascati (RM)
- Liceo Scientifico Malpighi, Roma
- Liceo Scientifico Plinio Seniore, Roma
- Liceo Statale Ginnasio Virgilio, Roma

Campania

- Convitto Nazionale Vittorio Emanuele II, Napoli
- IIS Casanova, Napoli
- IIS Don Lorenzo Milani, Gragnano (NA)
- IIS Livatino, Napoli
- IIS Nitti, Napoli
- IPIA Marconi, Giugliano in Campania (NA)
- IPSSAR Rossi Doria, Avellino
- ISIS Pagano-Bernini, Napoli
- ISIS Vittorio Emanuele II, Napoli
- Ist. Polispecialistico San Paolo, Sorrento (NA)
- ITIS Focaccia, Salerno
- ITIS Giordani, Caserta
- ITIS Giordani-Striano, Napoli
- ITIS Luigi Galvani, Giugliano in Campania (NA)
- Liceo Classico Carducci, Nola (CE)
- Liceo Classico Tasso, Salerno
- Liceo Classico Vittorio Emanuele II, Napoli
- Liceo Scientifico De Carlo, Giugliano in Campania (NA)
- Liceo Scientifico Genoino, Cava dè Tirreni (SA)
- Liceo Scientifico Segrè, Marano di Napoli (NA)
- Liceo Scientifico Tito Lucrezio Caro, Napoli
- Liceo Scientifico Vittorini, Napoli

Puglia

- IC Mazzini-Modugno, Bari
- IC Perotti-Ruffo, Cassano delle Murge (BA)
- IIS Carafa, Andria
- IIS Carelli-Forlani, Conversano (BA)
- IIS Colasanto, Andria
- IIS Copertino, Copertino (LE)
- IIS Marzolla-Simone-Durano, Brindisi
- IIS Medi, Galatone (LE)
- IIS Pacinotti-Fermi, Taranto
- IIS Perrone, Castellaneta (TA)
- IIS Righi, Cerignola (FG)
- IISS Da Vinci, Fasano (BR)
- IISS De Pace, Lecce
- IISS Euclide, Bari
- IISS Majorana, Brindisi
- IISS Majorana, Martina Franca (TA)
- IISS Trinchese, Martano (LE)
- IPSSAR Pertini, Brindisi
- ISIS Fermi, Lecce
- ISIS Righi, Taranto
- ITE Carlo Levi, Andria
- ITE e LL Marco Polo, Bari
- ITE Giordano, Bitonto (BA)
- ITE Lenoci, Bari
- ITELL Giulio Cesare, Bari
- ITE Pascal, Foggia
- ITIS Fermi, Francavilla Fontana (BR)
- ITIS Giorgi, Brindisi
- ITIS Jannuzzi, Andria
- ITIS Modesto Panetti, Bari
- IT Pitagora, Bari
- ITS Elena di Savoia, Bari
- ITT Altamura-Da Vinci, Foggia
- Liceo Carolina Poerio, Foggia
- Liceo Classico e Musicale Palmieri, Lecce
- Liceo Don Milani, Acquaviva delle Fonti (BA)
- Liceo Scientifico e Linguistico Vallone, Galatina (LE)
- Liceo Scientifico Fermi-Monticelli, Brindisi
- Liceo Scientifico Galilei, Bitonto (BA)
- Liceo Scientifico Salvemini, Bari
- Liceo Scientifico Scacchi, Bari
- Liceo Tito Livio, Martina Franca (TA)
- Scuola Sec. I Grado Michelangelo, Bari
- Secondo IC, Francavilla Fontana (BR)

Calabria

- IIS Fermi, Catanzaro Lido
- IPSSEOA Soverato (CZ)
- IT Calabretta, Soverato (CZ)
- ITE De Fazio, Lamezia Terme (CZ)
- ITI Scalfaro, Catanzaro
- ITIS Monaco, Cosenza
- Liceo Scientifico Guarasci, Soverato (CZ)
- Liceo Scientifico Pitagora, Rende (CS)

Sicilia

- IC Battisti, Catania
- IIS Ferrara, Mazara del Vallo (TP)
- IIS Majorana, Palermo
- IIS Medi, Palermo
- IIS Minutoli, Messina
- Ist. Salesiano Don Bosco-Villa Ranchibile, Palermo
- Istituto Magistrale Regina Margherita, Palermo
- IT Archimede, Catania
- ITE Russo, Paternò (CT)
- ITES A. M. Jaci, Messina
- ITI Marconi, Catania
- ITIS Cannizzaro, Catania
- ITI Vittorio Emanuele III, Palermo
- ITN Caio Duilio, Messina
- Liceo Classico Internazionale Meli, Palermo
- Liceo Classico Umberto I, Palermo
- Liceo De Cosmi, Palermo
- Liceo Scientifico Basile, Palermo
- Liceo Scientifico e Linguistico Umberto di Savoia, Catania
- Liceo Scientifico Fermi, Ragusa
- Liceo Scientifico Galilei, Catania
- Liceo Scientifico Santi Savarino, Partinico (PA)
- Liceo Scientifico Seguenza, Messina
- Liceo Scienze Umane e Linguistico Dolci, Palermo

Credits immagini:

Immagine di copertina: iStockphoto

Edoardo Angelucci (pag. 3, 4, 6, 15, 18, 28)
Cnr (pag. 13)
Enea (pag.13)
Ingv (pag. 13)
Pexels (pag. 4, 5, 9, 19, 21, 22, 25, 27,)
Canva (pag. 7)
Adobe Express (pag. 11)

I servizi GARR

Rete e accesso

GARR NOC
Gestione della rete

GARR NIC
Nomi a dominio

GARR LIR
Indirizzi IP

Sicurezza informatica

GARR CERT
Gestione e prevenzione

GARR SCARR
Scansioni di vulnerabilità

Identità e mobilità

idem garr aai
Identità digitali

IdP in the cloud
Identity as a Service

GARR Certification Service
Certificati digitali

eduroam
Wi-Fi in mobilità

Cloud

GARR cloud
IaaS e object storage

Videoconferenza e streaming

BlueMeet GARR

eduMEET
Soluzioni open per la videoconferenza

GARR TV
Streaming e video

Applicazioni

GARRbox
Storage personale

FILESENDER
Trasferimento file

GARR Mirror
Software Mirror

url GARR
URL brevi

GARR speedtest
Test di connessione

GARR NEWS

garrnews@garr.it
www.garrnews.it
retegarr

RETE GARR

GARR è la rete nazionale ad altissima velocità dedicata alla comunità dell'istruzione e della ricerca. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale.

La rete GARR è ideata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Università e della Ricerca.
Gli enti soci sono CNR, ENEA, Fondazione CRUI, INAF, INFN, INGV, le università statali italiane, gli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e gli Istituti Zooprofilattici Sperimentali (IZS).

Alla rete GARR sono connesse oltre 1.000 sedi tra enti di ricerca, università, ospedali di ricerca, istituti culturali e di formazione, biblioteche, musei, scuole.