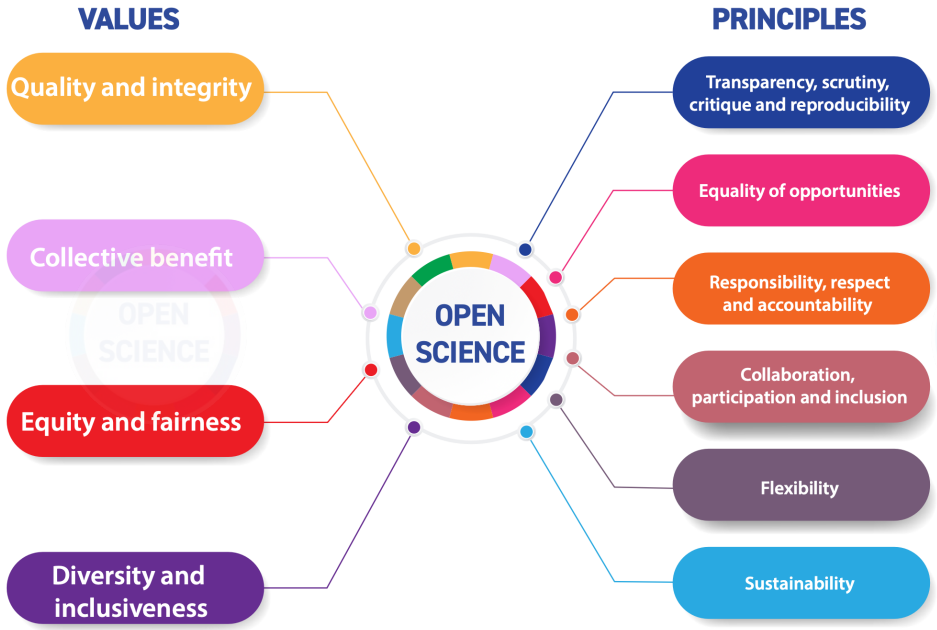
Incontro sulla **sicurezza della ricerca** e sull'equilibrio tra **libertà** e **responsabilità** dei ricercatori, alla luce delle sfide tecnologiche attuali (AI, quantum, superconduttività e altre attività dual use) e delle complesse relazioni internazionali.

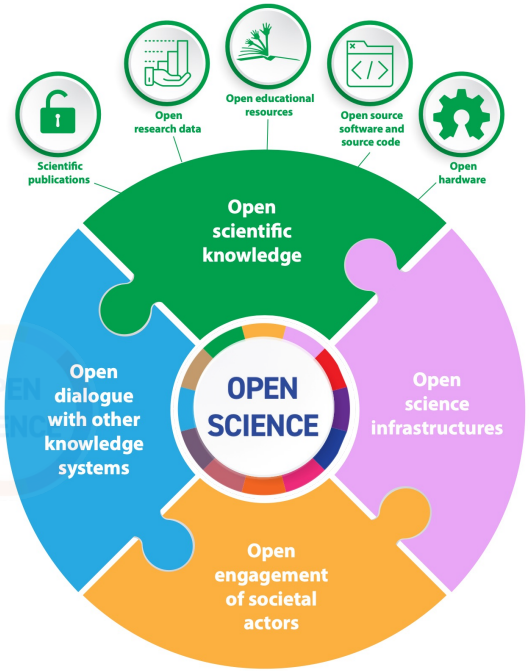
Un difficile equilibrio

Scienza aperta

Valori e **principi** volti ad aprire la scienza – e i suoi **benefici** – a tutta la **società**

Raccomandazione
UNESCO sull'Open Science





Valori e principi che sono ampiamente condivisi **nelle comunità scientifiche** e promossi **dalle istituzioni**, politiche e accademiche, in particolare quello della **massima condivisione conoscenza** e dei suoi strumenti, fisici e virtuali.

Ma che succede quando **soggetti malevoli** utilizzano la conoscenza condivisa **CONTRO tali valori**, non a beneficio della società, ma a **danno** dei **diritti** dei cittadini o contro gli **interessi** economici e strategici dei Paesi e dei soggetti che hanno prodotto tale conoscenza?

Integrità e sicurezza

I valori e i principi della ricerca costituiscono un **mosaico** fatto di tessere **diverse**, ma tutte ugualmente **importanti**: apertura, autonomia, valutazione, trasparenza, **ma anche** integrità, sicurezza, privacy, …

e – soprattutto – non in contraddizione tra di loro

"**G7 Common Values and Principles on Research Security and Research Integrity**" [June 2022]

Research integrity is the **adherence** to the professional **values**, **principles**, and **best practices** that underpin our research communities. It forms the base on which to **collaborate** in a **fair, innovative, open, and trusted** research environment.

Integrity is a **pre-condition for Open Science** deeply connected with **research assessment** [Honk Kong Principles, San Francisco Declaration (DORA), etc.]

Valori e principi

alla base dell'integrità della ricerca

Research security involves the actions that **protect our research communities from actors and behaviours posing economic, strategic, and/or national and international security risks**.

Particularly relevant are:

- the risks of **undue influence**, interference, or **misappropriation of research**;
- the outright **theft** of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity;
- other activities and behaviours having adverse economic, strategic, and/or **national security** implications.

Minacce

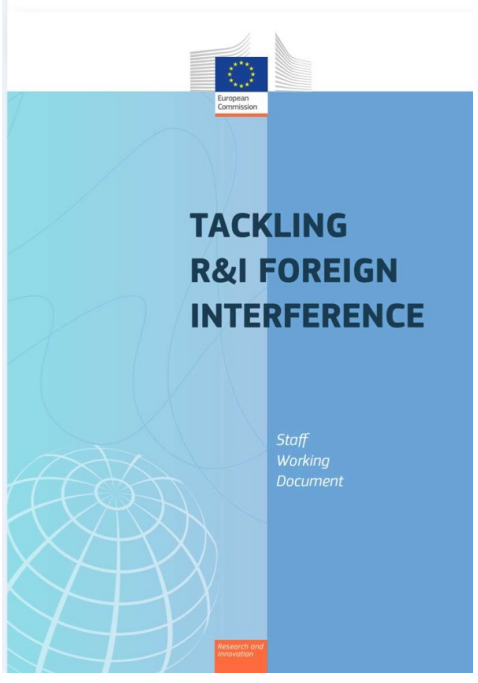
a tali valori e principi

*Una **minaccia** dal punto di vista della **sicurezza** della ricerca si traduce nella compromissione delle condizioni che permettono di rispettare i principi di **integrità della ricerca** [fiducia, onestà, eguali opportunità, ecc.] e di conseguenza è di ostacolo alla realizzazione dei principi della scienza aperta*

Minacce

Attenzione crescente da parte delle istituzioni in Europa [EU, OCSE] e oltre [G7]

- Accento iniziale su «**foreign interference**» sui ricercatori
  - Minacce alla **libertà accademica**, sia sui nostri partner sia nelle nostre istituzioni
  - **Pressione** sui decision makers e **disinformazione**
- Focus successivamente sulla perdita di **competitività tecnologica** ed **economica**
  - **Sicurezza dei dati** e **proprietà intellettuale**
  - **Appropriazione illecita di conoscenze** e tecnologie
- Più di recente, crescente attenzione all'**uso distorto** dei risultati della ricerca **anche per fini militari**
- E sull'**alterazione dei dati** e possibili **manipolazioni dell'output** delle attività di ricerca



Sicurezza della ricerca *[in pratica]*

- **Acquisire illecitamente** risultati scientifici e tecnologici,
- **Influenzare o utilizzare in modo distorto** [difforme dall'intento dichiarato] processi, dati o risultati della ricerca

Anche attraverso **minacce ibride** e:

- Sfruttando **informazioni condivise** in buona fede
- Tramite personale di ricerca, attraverso l'**accesso a informazioni o materiali proprietari**
  - Sia di iniziativa propria sia eventualmente sotto pressione esterna
- Tramite l'**utilizzo improprio di infrastrutture fisiche** o **digitali**
- Attraverso la leva dei **finanziamenti** per **acquisire** o **distorcere/influenzare** conoscenze

A livello di **sistema**:

- Uso di scienza e tecnologia per **scopi non pacifici** o **contrari ai principi fondamentali** [per es. **diritti civili e umani**] o che **minacciano la sicurezza** del Paese, dell'UE e alleati
- Oppure minando la **sicurezza economica** [**concorrenza sleale**]

A livello **individuale**:

- **Violazioni dei principi etici**
- **Conflitti di interessi**
- **Conflitti di commitment**

*Un tema che riceve crescente attenzione in un **quadro geopolitico** in rapido mutamento, non solo in relazione alle **tecnologie critiche**, ma che interessa anche la ricerca «di base» o a basso TRL*

Raccomandazione Consiglio EU 23/5/2024

La **Raccomandazione del Consiglio EU del 23 maggio 2024** chiede agli Stati Membri di **sviluppare** e **implementare** un insieme coerente di "**policy actions**" per migliorare la sicurezza della ricerca.

Le **azioni** elencate sono:

- Predisporre un **processo trasparente** che porti a stilare delle **linee-guida nazionali**, con il supporto e la guida della Commissione
- Creare delle **strutture di supporto e di analisi**
- Facilitare lo **scambio di informazioni** tra **istituzioni** accademiche, **agenzie finanziatrici** e **intelligence**
- Migliorare la **sinergia tra le varie agenzie e decisori** nei vari settori coinvolti (industria, affari internazionali, istruzione, ricerca, intelligence, cybersicurezza, ecc.)
- Rafforzare l'applicazione delle norme in materia di **exports control e dual use**
- **Coinvolgere** il **settore privato**
- Incoraggiare la **condivisione di strumenti**

Con **particolare attenzione** alle principali tipologie di rischio:

- **Mobilità dei ricercatori**
- **Collaborazioni internazionali**
- **Cybersicurezza**

Raccomanda inoltre di costituire una **one-stop-shop platform** europea che fornisca **servizi e strumenti** per affrontare le influenze straniere su ricerca e tecnologia

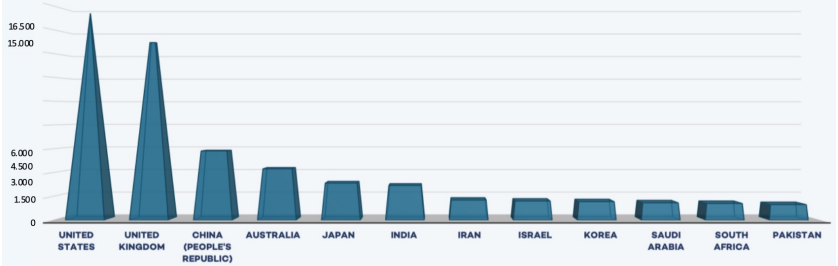
In generale, raccomanda che il **risk assessment & mitigation** sulla sicurezza entri nella valutazione **al livello di singolo progetto di ricerca**

Francesco Priolo
Coordinatore Tavolo CoPER-CRUI Etica della Ricerca

- Oltre **5.500 ricercatori** (tutti i ruoli) **stranieri** in Italia nel 2023
- Quasi **2.800** accessi (nuove iscrizioni) di **dottorandi stranieri (39° ciclo)** (di cui oltre 1500 da Paesi asiatici)
- Circa **6.500 stranieri** iscritti a **Corsi di Dottorato** nell'AA 2022/2023 (di cui oltre 3000 da Paesi asiatici)

Su **158.000** prodotti (anno 2022) **81.000** sono in collaborazione con ricercatori di paesi dell'Unione Europea (> 50%)

Fonte OECD da Scopus Custom Data, Elsevier, Version 1.2024



Integrazione con la recente normativa **NIS-2** [Direttiva EU e D.lgs. 138/2024 https://direttivanis2.eu

Cosa fare

In generale, applicare il **principio** generale di:

"as open as possible, as closed as necessary"

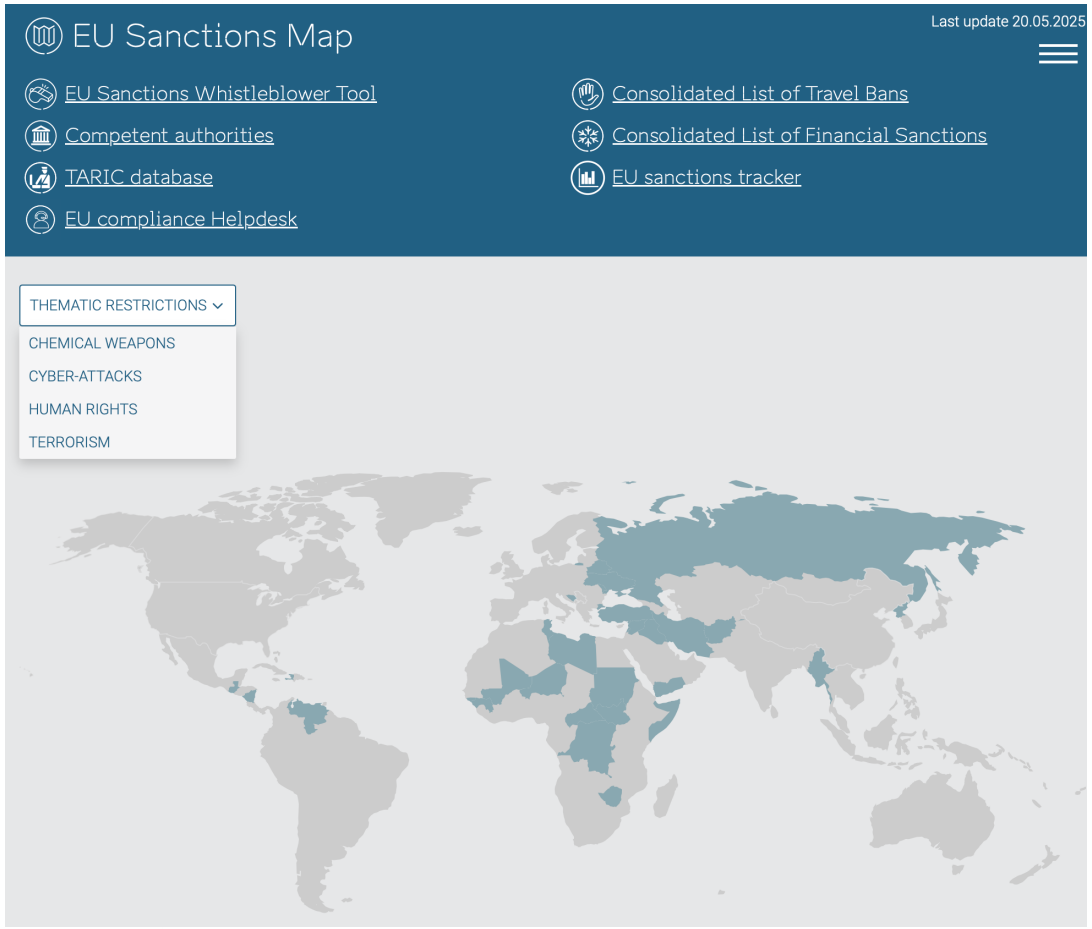
da applicare tenendo conto sia della **natura** della conoscenza, sia della **proprietà** dell'informazione

tuttavia

ci sono segnali che il principio applicato in Horizon Europe possa cambiare in FP10

- Ribaltando dall'apertura massima possibile, alla chiusura di default
- Dibattito su dual use
- Possibile inclusione della ricerca militare

- Nessuna **discriminazione**, diretta o indiretta
- Inoltre: **evitare di scoraggiare** collaborazioni e scambi di personale sulla base di **auto-censura** o **preoccupazioni** legate alla sicurezza.



tuttavia

Esistono diverse liste di **Paesi sanzionati**, e di **tecnologie «sensibili»** sulle quali limitare l'accesso

Tecnologie critiche

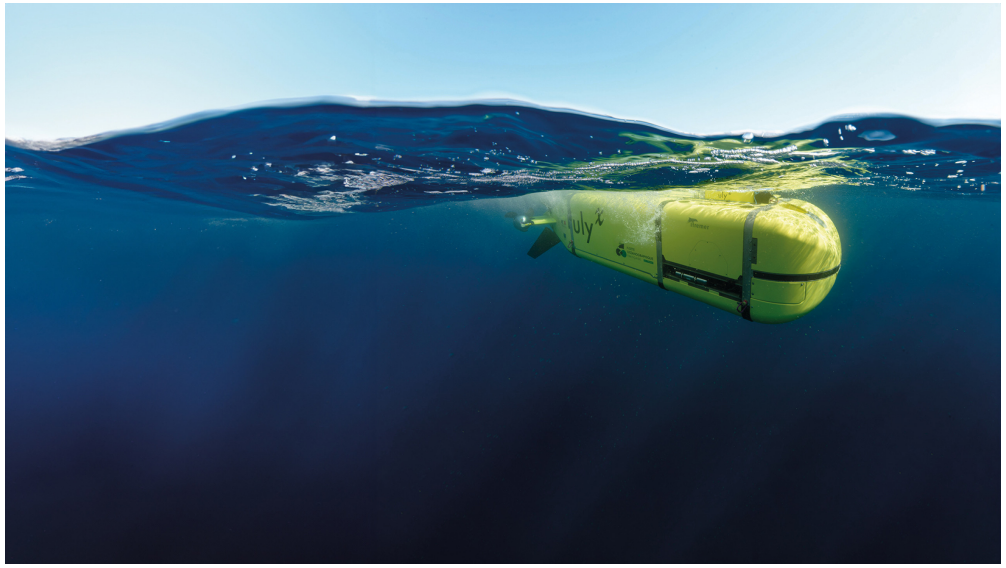
In ottobre 2023, Direttiva EU sulle **aree tecnologiche critiche** innanzitutto per la **sicurezza economica**:

- Advanced semiconductors
- Artificial intelligence
- Quantum technologies
- Biotechnologies

Prevede una **valutazione del rischio a livello europeo** [non sufficiente solo una valutazione a livello nazionale]

Più le aree con aspetti più evidenti di applicazioni a **uso duale**, ad esempio: **aerospazio, subacquea…**

Le incertezze maggiori nascono però dalle situazioni lontane da [entrambi] gli estremi dello spettro: è abbastanza ovvio che epigrafia latina sia non critica, mentre lo sviluppo di droni lo è, ma come considerare la radioprotezione?



Cosa fare

Implementare un **modello** di **gestione e mitigazione del rischio** senza aggiungere un **carico burocratico non necessario**

Osservazione: sarebbe interessante **integrare** questa tipologia di rischio con la gestione della sicurezza convenzionale, il crisis management, l'aderenza ai principi etici, il gender balance, ecc.

Includere le valutazioni relative ai rischi legati alle **collaborazioni internazionali** **ogni volta** che si predispongono accordi, partendo dai principi di **integrità**, **protezione della proprietà intellettuale** e **reciprocità**

Osservazione: esiste una **buona base di partenza** nelle nostre istituzioni scientifiche e accademiche, con buone pratiche orientate alla **protezione della IP**; occorre una maggiore attenzione ai temi della **reciprocità** e dei potenziali **misuse**

Effettuare una **valutazione del rischio** per i **programmi di scambio con paesi terzi**:

- dotandosi di di **competenze** specifiche **in house** tramite dei **responsabili della sicurezza della ricerca** **a livello di singola istituzione**
- allo scopo di coadiuvare **governance** e **ricercatori** nelle azioni di valutazione e **mitigazione** del rischio

Sviluppare un **programma di formazione**

- **sia** per **tutto il personale di ricerca**
- **sia** mirato a **degli specialisti**

Osservazione: si tratta di **specialisti** che sono presenti in **minima o nessuna parte** nelle nostre istituzioni scientifiche e accademiche; occorre individuare come implementare la **formazione specifica**

Assicurare **trasparenza** rispetto a **fonti di finanziamento** e **affiliazioni** dei ricercatori **evitando conflitti di interessi** o **conflitti di commitment** e dipendenza da paesi terzi

Compartimentare adeguatamente l'**accesso** a **laboratori**, **infrastrutture di ricerca** e **dati**

Valutare il rischio di acquisizioni di **strumenti** o di **finanziamenti** da parte di **paesi terzi**

Osservazione: queste misure sono probabilmente quelle che necessitano maggiore **cambiamento** nelle **pratiche** delle nostre istituzioni scientifiche e accademiche;

Occorre soprattutto:

- dare ampia **informazione** sulle **motivazioni** che sono alla base di queste richieste
- e assicurare un **supporto** adeguato ai ricercatori per implementare **correttamente** e **in modo semplice** la policy richiesta

Modello e linee guida italiane

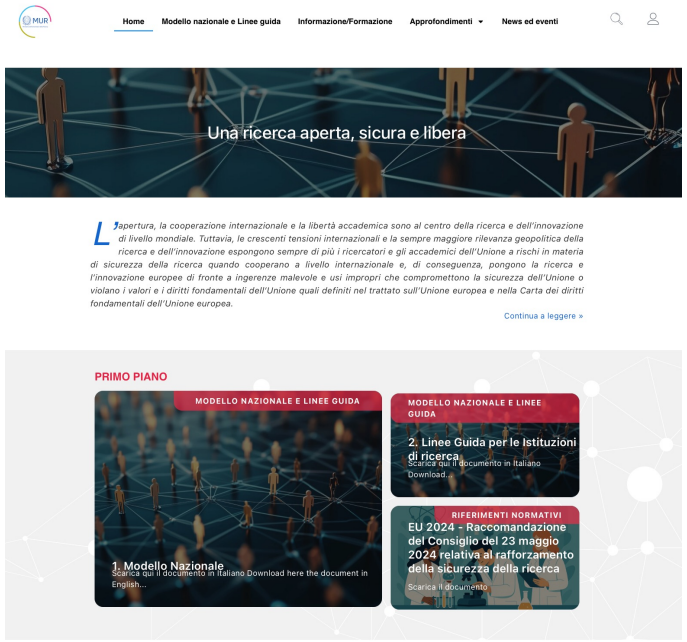
Gruppo di lavoro del MUR con rappresentanti CRUI, CoPER e della comunità scientifica [coord. prof. F. Cupertino]

Con l'obiettivo di **sviluppare** un **modello nazionale** e delle **linee guida** che rafforzi l'ecosistema della ricerca e **impedisca interferenze esterne**, seguendo la **Raccomandazione** del Consiglio EU:

- **Coinvolgendo** la comunità scientifica e accademica
- **In armonia** anche con gli orientamenti degli altri Paesi like-minded, in particolare del **G7**
- Traendo ispirazione e esempio da esempi di **best practice** dei Paesi con maggiore esperienza

Risultati **presentati** al Workshop nazionale di Bari [4 dicembre 2024] e **approvati** da un largo tavolo inter-istituzionale

https://www.sicurezzaricerca.mur.gov.it/area-tematica/modello-nazionale-e-linee-guida/



https://www.sicurezzaricerca.mur.gov.it/news/conferenza-bari-4-12-2024/

Programma

Presentazioni:

- Etica della Ricerca: risultati del gruppo CRUI-CoPER
- Sicurezza e Integrità della Ricerca: le riflessioni G7 e OCSE
- Come altri Paesi UE ed extra-UE stanno affrontando il tema della Sicurezza e Integrità della Ricerca
- Quadro Normativo Europeo e Nazionale
- Il gruppo di lavoro MUR sulla sicurezza della ricerca. Linee guida, architettura sito, consultazione pubblica e road map
- Griglia di valutazione: istruzioni per l'uso
- Linee di mitigazione: esempi
- Moduli formativi

Modello e linee guida italiane

Input:

- Normativa europea, in particolare Raccomandazione 23.5.2024 sulla Research Security e Direttiva sui **settori tecnologici critici**
- Direttiva e normativa nazionale su **NIS-2**
- ACN, per la parte di cybersicurezza
- Materiali **SIGRE** [G7 group on Security and Integrity of the Global Research Ecosystem] e dalla Virtual Academy [rappresentante italiano prof. F. Esposito]
- Materiali di diversi **like-minded countries**
- **CRUI**: tavolo CRUI–Enti di ricerca su «Etica nella Ricerca» [coord. prof. F. Priolo]
- Consulta dei Presidenti degli enti di ricerca [**CoPER**]

Output:

- Modello nazionale per la sicurezza della ricerca
- **Raccomandazioni** e linee guida per la mitigazione del rischio
- Bozza di **strumento di autovalutazione**
- Materiale informativo e **formativo**
- **Sito web** come riferimento e punto di raccolta di case studies e best practise

Modello e linee guida italiane

Tre elementi fondamentali:

1. **Formazione** specifica **per aumentare la consapevolezza** sui **vari aspetti** legati alla sicurezza della ricerca:
   - Destinata a tutti gli attori, ma con **moduli specifici** per i **responsabili di attività** e per le **governance**
   - **Protocollo visitatori**
   - **Protocollo** per i viaggi
   - **Cybersicurezza** e sicurezza dei dati

2. **Autovalutazione** da parte del responsabile dell'attività di ricerca basata su tre fattori di rischio fondamentali:
   - **Aree** scientifiche e tecnologiche **critiche**
   - **Collaborazioni** internazionali, in particolare extra-EU
   - Fonti di **finanziamento**, in particolare extra-EU o non pubbliche/profit

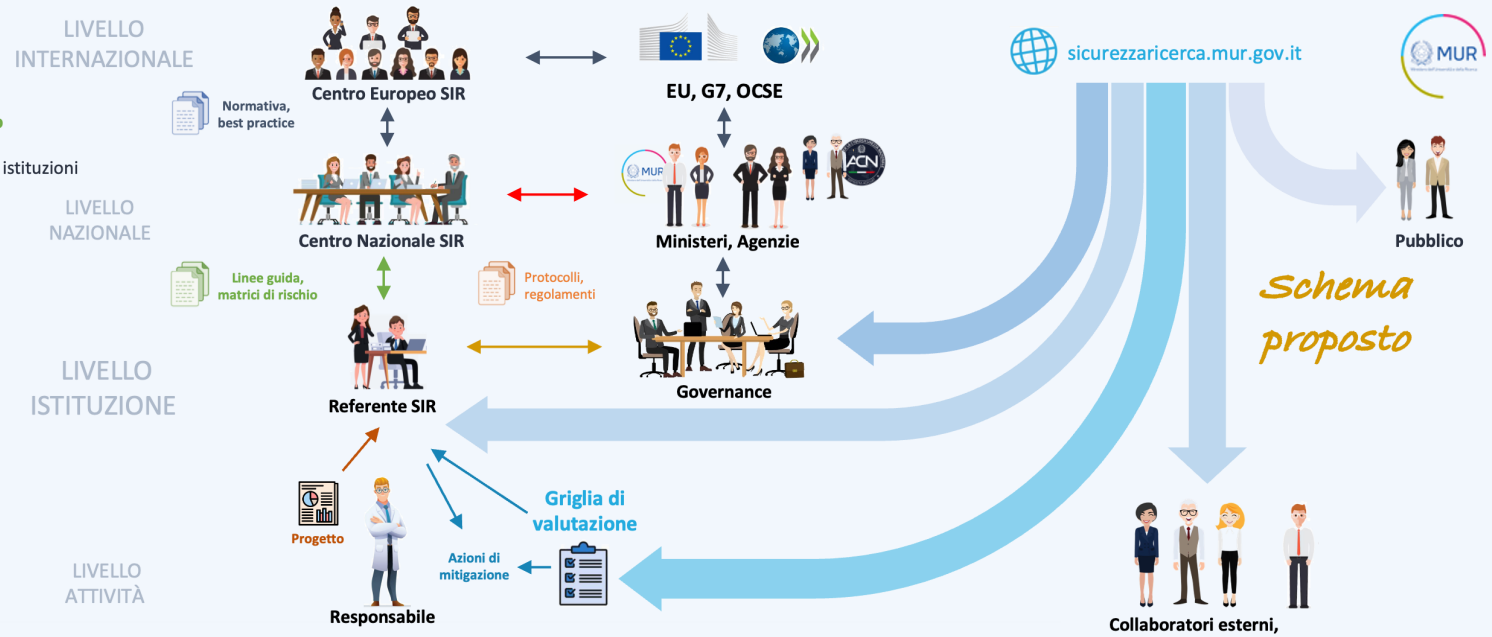
3. **Struttura di supporto** per valutare **rischi**, azioni di **mitigazione** e **best practise**, su **3 livelli**:
   - Un **referente** in ciascuna istituzione di ricerca [o aggregazione di Enti/Università]
   - Un **livello nazionale**, coordinato/supportato dal Ministero dell'università e ricerca
   - Un **centro europeo**, probabilmente con un **modello a rete** di centri nazionali

Linee guida italiane

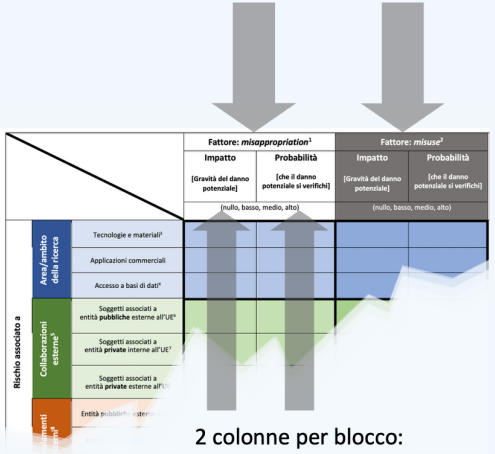
Centro Nazionale per la Sicurezza e Integrità della Ricerca
- Agisce da **raccordo con ministeri e agenzie rilevanti**
- Predispone e aggiorna: **raccomandazioni e linee guida, matrici di rischio**
- Suggerisce azioni di **mitigazione dei rischi**
- Riceve richieste e **fornisce supporto ai referenti SIR**, anche tramite altre istituzioni
- Fornisce **materiale formativo**
- Agisce da **coordinamento nazionale** dei referenti SIR
- Dialoga con il **Centro Europeo SIR**

Referente per la Sicurezza e Integrità della Ricerca
A livello di singola Istituzione [o più Istituzioni consorziate], **esamina i progetti** con indicatori di rischio **sopra soglia** e:
- Fornisce **azioni di mitigazione al responsabile di attività**;
- Fornisce **raccomandazioni alla governance** dell'Istituzione, anche su protocolli per **visite** di ospiti o **viaggi** in paesi con profilo di **rischio alto**
- Si occupa della **formazione** a livello di Istituzione
- Contribuisce all'implementazione delle politiche di **cybersicurezza**
- Contribuisce al rispetto delle politiche su **dual use** ed **exports control**
- Riceve **linee guida e matrici di rischio** dal **Servizio Nazionale**
- Può richiedere **supporto** al **Servizio Nazionale**

Responsabile di attività
- Presenta il **progetto di attività** di ricerca all'istituzione ed eventualmente altre agenzie di finanziamento
- Produce una **autovalutazione dei rischi** con l'aiuto di una **griglia** a livello ministeriale



2 blocchi verticali:
tipologie di azione malevola



2 colonne per blocco:
Valutazioni di **impatto** e **probabilità**

Griglia di valutazione: struttura

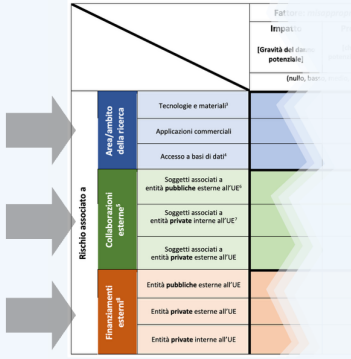
L'area disciplinare e in senso più lato la tematica e la tipologia dell'attività di ricerca (fondamentale, applicata, conto terzi, ecc.); il coinvolgimento o la disponibilità di asset (materiali e immateriali)

Area scientifica o tecnologie critiche o sensibili*

La collaborazione con partner non appartenenti a istituzioni EU

Fonti di finanziamento non provenienti da istituzioni EU

blocchi orizzontali:
3 **aree di rischio**

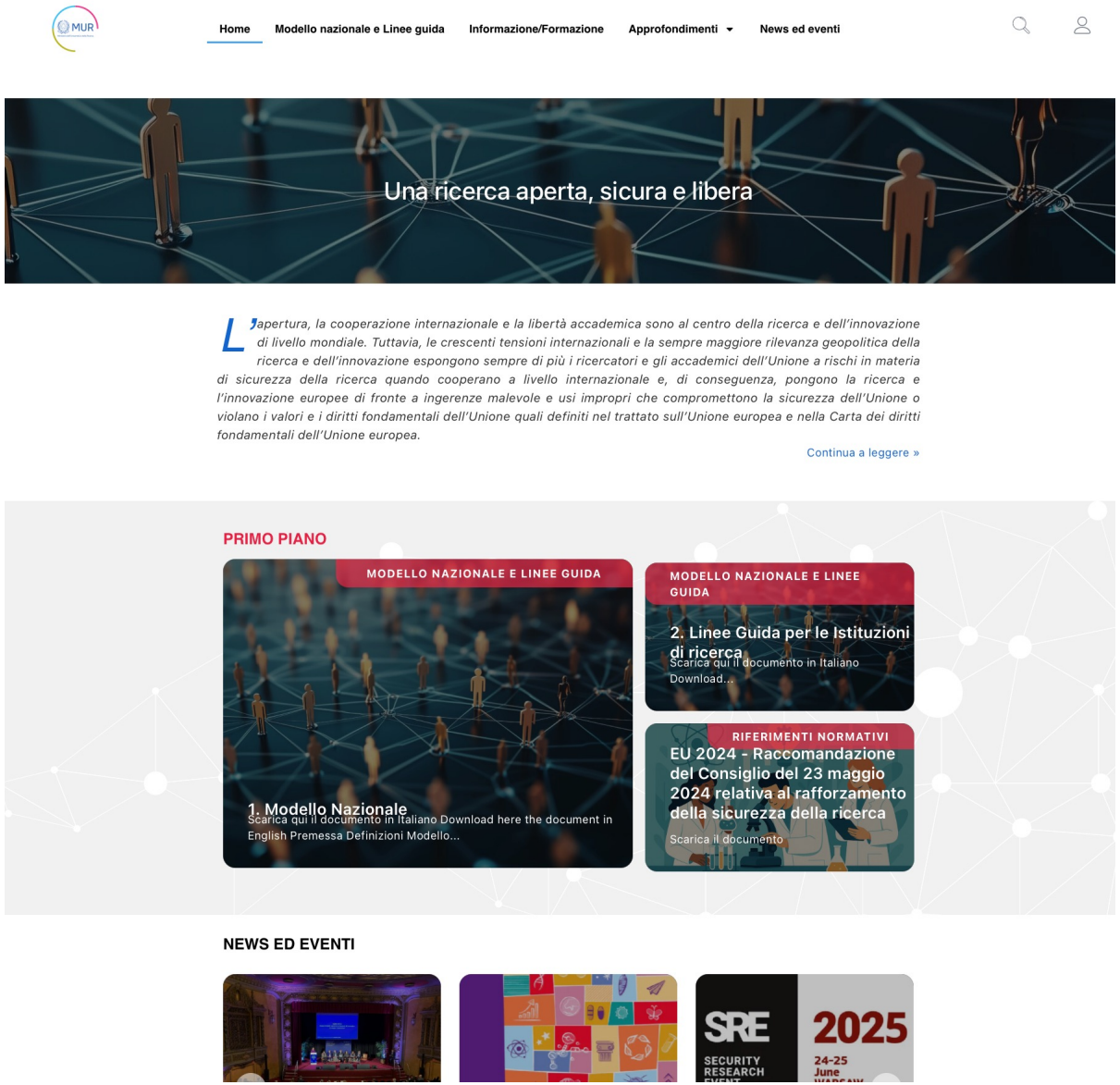


** "ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States", 3 ottobre 2023:*

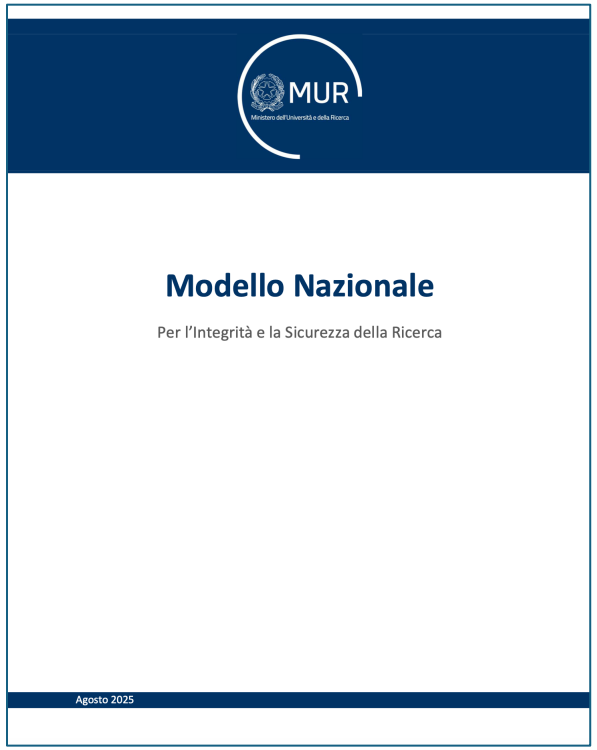
Area Tecnologica	Tecnologie
SEMICONDUTTORI	• Microelettronica, compresi i processori • Tecnologie fotoniche (incluso i laser ad alta energia) • Chip ad alta frequenza • Attrezzature per la produzione di semiconduttori avanzati
INTELLIGENZA ARTIFICIALE	• Calcolo ad alte prestazioni • Cloud computing e edge computing • Tecnologie di analisi dei dati • Visione artificiale, elaborazione del linguaggio, riconoscimento degli oggetti
QUANTISTICA	• Calcolo quantistico • Crittografia quantistica • Comunicazioni quantistiche • Sensori e radar quantistici
BIOTECNOLOGIE	• Tecniche di modifica genetica • Nuove tecniche genomiche • Gene-drive (propulsione genetica) • Biologia sintetica
CONNETTIVITÀ, NAVIGAZIONE E DIGITALI	• Comunicazioni digitali e connettività sicure, come RAN e Open RAN (Radio Access Network) e 6G • Tecnologie di sicurezza informatica, incluse la cyber-sorveglianza, sistemi di sicurezza e intrusioni, informatica forense digitale • Internet delle cose e Realtà Virtuale • Tecnologie di registro distribuito e identità digitale • Tecnologie di guida, navigazione e controllo, incluse l'avionica e il posizionamento marino
SENSORI	• Sensori elettro-ottici, radar, chimici, biologici, di radiazioni e di rilevamento distribuito • Magnetometri, gradiometri magnetici • Sensori di campo elettrico subacquei • Misuratori e gradiometri di gravità
TECNOLOGIE SPAZIALI E DI PROPULSIONE	• Tecnologie specifiche per lo spazio, che vanno dal livello di componente a quello di sistema • Tecnologie per la sorveglianza spaziale e l'osservazione della Terra • Posizionamento spaziale, navigazione e temporizzazione (PNT) • Comunicazioni sicure, compresa la connettività in orbita terrestre bassa (LEO) • Tecnologie di propulsione, incluse l'ipersonica e componenti per uso militare
ENERGIE	• Tecnologie di fusione nucleare, reattori e generazione di energia, tecnologie di conversione/arricchimento/riciclaggio radiologico • Idrogeno e nuovi combustibili • Tecnologie a emissioni zero, incluse le fotovoltaiche • Reti intelligenti e stoccaggio dell'energia, batterie
ROBOTICA E SISTEMI AUTONOMI	• Droni e veicoli (aerei, terrestri, di superficie e subacquei) • Robot e sistemi di precisione controllati da robot • Esoscheletri • Sistemi abilitati dall'intelligenza artificiale
MATERIALI, MANIFATTURA E RICICLAGGIO	• Tecnologie per nanomateriali, materiali intelligenti, materiali ceramici avanzati, materiali stealth, materiali progettati per essere sicuri e sostenibili • Manifattura additiva • Manifattura digitale di micro-precisione, e lavorazione/saldatura laser su piccola scala • Tecnologie per l'estrazione, la lavorazione e il riciclaggio di materiali grezzi critici (inclusa l'estrazione idrometallurgica, la bio-lisciviazione, la filtrazione basata sulla nanotecnologia, la lavorazione elettrochimica e la massa nera)

Linee guida italiane

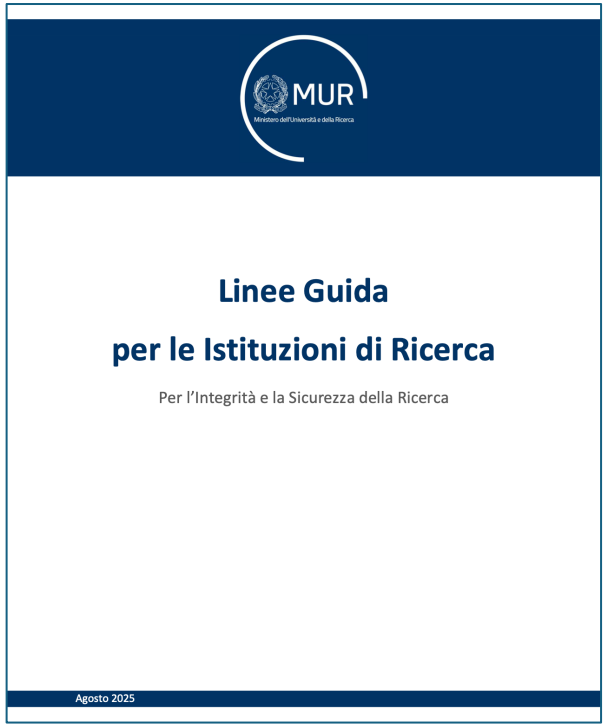
https://www.sicurezzaricerca.mur.gov.it



https://www.sicurezzaricerca.mur.gov.it/wp-content/uploads/2025/08/Modello-Nazionale.pdf



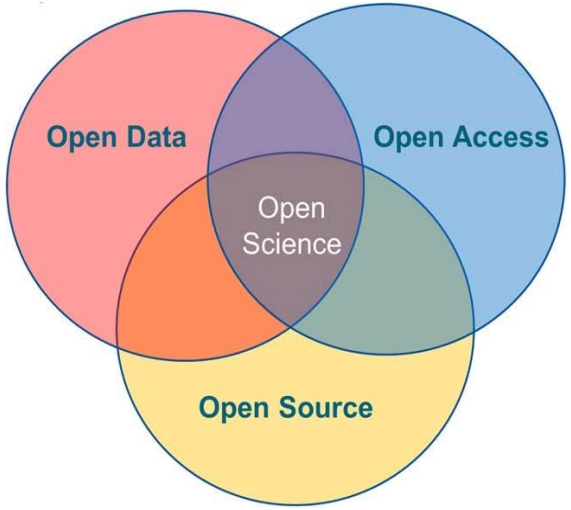
https://www.sicurezzaricerca.mur.gov.it/wp-content/uploads/2025/08/Linee-Guida.pdf



Research Security vs. Open Science

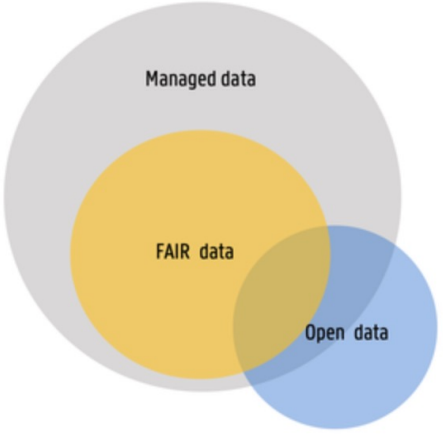
Francesco Priolo
[Bari, Workshop Sicurezza della Ricerca 4/12/2024]

- L'OS è concepito come **potenziale strumento di trasparenza** e di **accountability verso la società**, verso gli stakeholders e verso i cittadini.
- La grande **quantità di dati esistenti** e le interconnessioni disciplinari rendono necessaria una scienza aperta a tutti i contributi (FAIR).
- L'**accesso a dati** e risultati scientifici rappresenta (anche) una «**democratizzazione**» e un contributo allo sviluppo indirizzati a Paesi (o individui) che non possono permettersi costi di ricerca elevati o fuggono da regimi.
- Non ultimo, il **controllo** esercitato dalla **intera comunità scientifica** può fungere da **garanzia** combattendo **fake**, plagi, condotte etiche inappropriate e contribuire alla reputazione della scienza (percezione dell'affidabilità).



In particolare sugli open data

FAIR non significa «**open**» ovvero dati che possono essere **liberamente** usati, modificati e condivisi da **chiunque** e per **qualsiasi uso**



DATI PROPRIETARI

- Dati di terze parti [non generati dalla ricerca]
- Dati protetti da copyright o condivisi con altri soggetti
- Dati con valore economico o commerciale con diritti dell'istituzione o agenzie finanziatrici

DATI SENSIBILI, PERSONALI o CONFIDENZIALI

Dati che riguardano:

- **Salute** [dati clinici, genetici, altri dati sanitari]
- **Finanza** [transazioni, valutazioni economiche, dati bancari]
- **Scienze sociali** [su opinioni, credenze, comportamenti individuali e collettivi, ecc.]

Oltre i principi FAIR

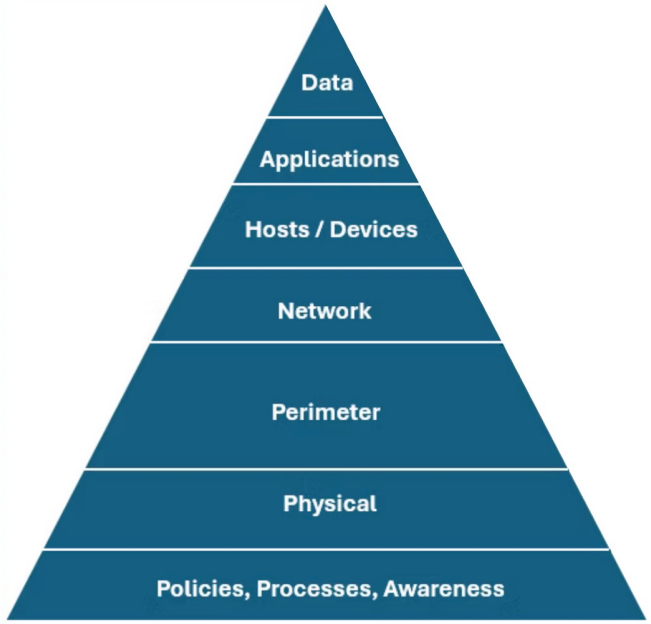
Tra le proposte di **estensione** dei principi **FAIR** ci sono i concetti di:

Extensibility

capacità di espandere un data model dinamicamente con ulteriori capacità, mantenendo la struttura iniziale

Security

- funzionalità legate all'identità: access control implementato a livello dei dati, non [solo] del server, dell'applicazione o della rete
- crittografia
- data governance, ovvero politiche di gestione del dato
- Anonimizzazione e protezione della privacy/dati sensibili
- revisione e controllo periodico [audit e monitoraggio]



Trust

autenticità e affidabilità sono incapsulate nei dati stessi [provenienza, integrità, proprietà, ecc.]

Spunti di riflessione

Bloccare il libero flusso di informazioni rallenta il progresso scientifico e tecnologico:

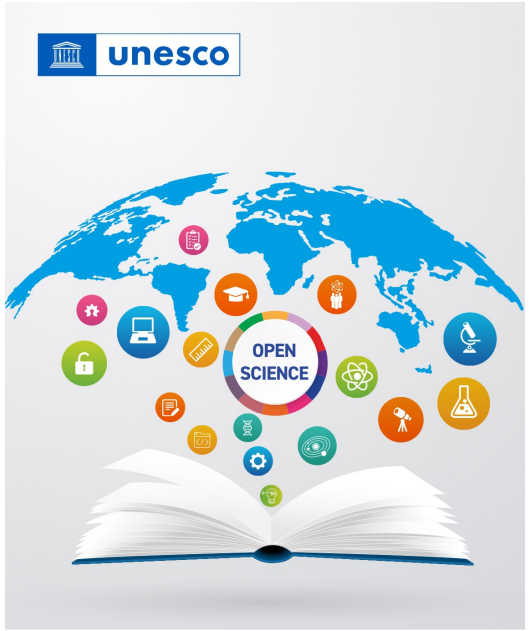
- non è possibile rinunciare alla collaborazione internazionale senza allontanare i ricercatori e le loro istituzioni da preziose partnership globali
- ciò inevitabilmente ridurrebbe la capacità scientifica collettiva e sarebbe di ostacolo nell'affrontare le sfide globali che abbiamo di fronte: cambiamento climatico, energia, salute, invecchiamento, salvaguardia del territorio, ecc.

D'altro canto, non è possibile tornare indietro sulla strada maestra, intrapresa da tempo e convintamente dalle istituzioni europee, della Scienza Aperta:

- nella ERA Policy Agenda, condensata in 20 policy actions, l'Open Science è al primo posto
- A ottobre 2024 è stato inaugurato EOSC, lo European Open Science Cloud, strumento per la federazione e interoperabilità fra i vari «nodi» OS. Open AIRE, infrastruttura digitale finanziata attraverso fondi comunitari, lavora in sinergia con EOSC

Anche UNESCO, che ha pubblicato le proprie raccomandazioni sull'Open Science sottolinea che:

«Access to scientific knowledge should be as open as possible, but sometimes access may need to be restricted, for example to protect human rights, confidentiality, intellectual property rights, personal information, threatened or endangered species, and sacred and secret indigenous knowledge. Open science encourages scientists to develop tools and methods for managing data so that as much data as possible can be shared, as appropriate.»



PRIORITY AREA

DEEPENING A TRULY FUNCTIONING INTERNAL MARKET FOR KNOWLEDGE

ACTIONS

1 **ENABLE THE OPEN SHARING OF KNOWLEDGE AND THE RE-USE OF RESEARCH OUTPUTS, INCLUDING THROUGH THE DEVELOPMENT OF THE EUROPEAN OPEN SCIENCE CLOUD (EOSC)**

The amount of data generated or used in public-funded research and innovation (R&I) activities is growing exponentially. However, a significant part of the data never makes it to a trusted and sustainable repository, is poorly annotated or not formatted in a standardised way that supports machine readability. As a consequence, many experiments conducted on the basis of those data are considered not reproducible. Scientific data and other research digital output, such as codes and software, need to be more open, better managed, machine actionable and extensively re-used.

E quindi?

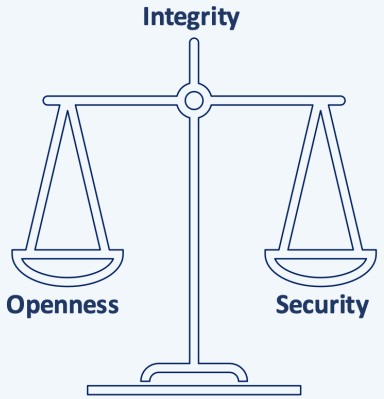
Adottare un approccio equilibrato può migliorare la sicurezza della ricerca e rassicurare i partner, mantenendo al tempo stesso l'apertura essenziale al lavoro della comunità scientifica

Spunti di riflessione

Fulvio Esposito
[Bari, Workshop Sicurezza della Ricerca 4/12/2024]

- **Bilanciare** la politica di sicurezza con la natura aperta della ricerca è delicato, sia dal punto di vista sostanziale, sia formale (Trattati, Costituzione, Leggi, Statuti, ecc.)
- **Fondamentale evitare** di ridurre la questione sicurezza della ricerca a un ennesimo adempimento **puramente burocratico**
- **Evitare** di **scoraggiare le collaborazioni** o peggio discriminare paesi terzi. Applicare correttamente il **principio di reciprocità**.
- **Assicurare** il **coordinamento** a livello **europeo** e oltre (**OCSE**, **G7**): la recente Raccomandazione EU è un passo fondamentale.
- Tenere in conto la **specificità** ed **eterogeneità** delle istituzioni di ricerca, considerando anche l'impegno nella ricerca tecnologica, nella didattica [università] e nel trasferimento di conoscenza al sistema produttivo e alla società, nonché nel servizio e/o consulenza a agenzie e organi governativi e territoriali.
- **Gestire** correttamente il rapporto con gli organi governativi e in particolare con le **agenzie di sicurezza e intelligence**: siamo e dobbiamo restare ricercatori

Tema non del tutto sovrapponibile ma connesso è quello dell'**uso duale**, che meriterebbe **una discussione a parte**



In funzione delle circostanze, il fulcro della bilancia si può spostare in una direzione o nell'altra.

• Lo scambio di idee ed esperienze con colleghe e colleghi animati dagli stessi valori

può essere d'aiuto a prendere decisioni equilibrate (balanced approach, naivety and paranoia…).

• G7-Scienza ha lanciato la Virtual Academy on Research Security and Integrity, ospitata sulla piattaforma SINAPSE della Commissione Europea "to develop a shared understanding of research integrity and security…

…allowing international collaboration to continue with confidence". https://europa.eu/sinapse/sinapse

Spunti di riflessione

A livello di implementazione **nella specifica realtà delle nostre istituzioni** occorre considerare:

- L'alto grado di **internazionalizzazione** della ricerca
- La comunità scientifica, per sua natura **autonoma** e «**ibrida**»: ricercatori e tecnologi, enti e università, pubblico e privato, ecc.
- E quindi attenzione alle **specificità** delle diverse istituzioni e delle loro missioni [università con la didattica, enti non MUR con ricerca istituzionale e di servizio, vocazione al trasferimento tecnologico, ecc.]

Cosa succede **dopo** la predisposizione di **linee guida**?

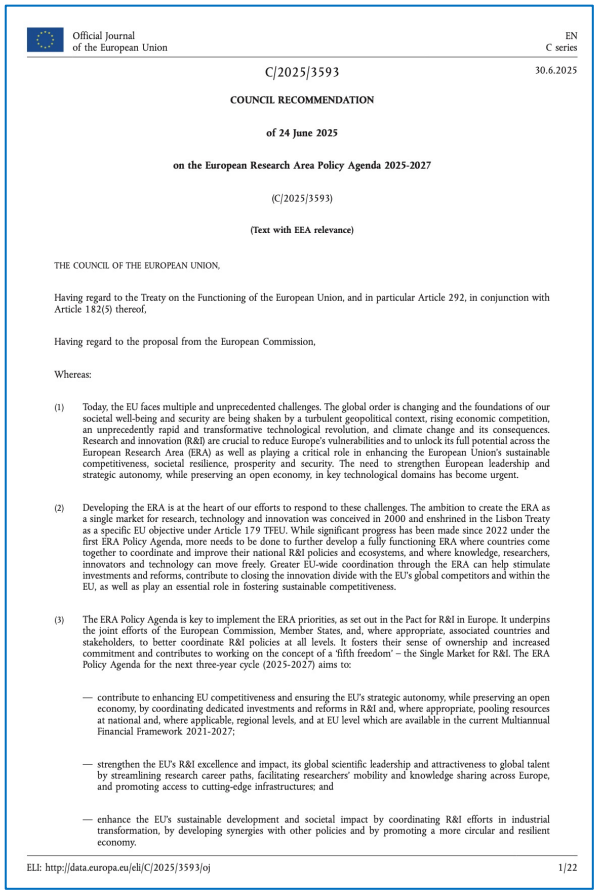
- Supporto del Governo/MUR/agenzie governative su **monitoraggio delle minacce**, «**entity list**», **matrici di rischio**, **strumenti**.

  Per esempio: un **centro nazionale**; **strumenti software** condivisi con i partner EU/G7

- Priorità alla **formazione** per aumentare la consapevolezza della comunità e al tempo stesso diffondere un atteggiamento equilibrato e una metodologia razionale.
- **Sperimentazione** dell'implementazione delle linee guida in alcune istituzioni pilota:
  - Disponibilità di INFN: primo disciplinare per la sicurezza della ricerca in via di approvazione.

Cosa sta succedendo

- **Flagship Conference europea**
- Sicurezza della ricerca inserita nella legislazione EU, in particolare inella proposta legge della Commissione sulla **European Research Area**. Consultazione pubblica sull'**ERA Act**.
- Realizzazione di un **Centro di Competenza EU** entro la fine del 2026: hub per training, tools, comunità di pratica
- Entro il 2026: realizzazione di una **Due diligence EU platform** basata su dati open source, su centri di ricerca stranieri
- Anche Science Europe intende sviluppare una piattaforma di supporto [hub o centro di competenza]
- Riorganizzazione del MUR: nuova Direzione Generale con competenza per la sicurezza della ricerca


Official Journal of the European Union
EN
C series

C/2025/3593
30.6.2025

COUNCIL RECOMMENDATION

of 24 June 2025

on the European Research Area Policy Agenda 2025-2027

(C/2025/3593)

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292, in conjunction with Article 182(5) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Today, the EU faces multiple and unprecedented challenges. The global order is changing and the foundations of our societal well-being and security are being shaken by a turbulent geopolitical context, rising economic competition, an unprecedently rapid and transformative technological revolution, and climate change and its consequences. Research and innovation (R&I) are crucial to reduce Europe's vulnerabilities and to unlock its full potential across the European Research Area (ERA) as well as playing a critical role in enhancing the European Union's sustainable competitiveness, societal resilience, prosperity and security. The need to strengthen European leadership and strategic autonomy, while preserving an open economy, in key technological domains has become urgent.

(2) Developing the ERA is at the heart of our efforts to respond to these challenges. The ambition to create the ERA as a single market for research, technology and innovation was conceived in 2000 and enshrined in the Lisbon Treaty as a specific EU objective under Article 179 TFEU. While significant progress has been made since 2022 under the first ERA Policy Agenda, more needs to be done to further develop a fully functioning ERA where countries come together to coordinate and improve their national R&I policies and ecosystems, and where knowledge, researchers, innovators and technology can move freely. Greater EU-wide coordination through the ERA can help stimulate investments and reforms, contribute to closing the innovation divide with the EU's global competitors and within the EU, as well as play an essential role in fostering sustainable competitiveness.

(3) The ERA Policy Agenda is key to implement the ERA priorities, as set out in the Pact for R&I in Europe. It underpins the joint efforts of the European Commission, Member States, and, where appropriate, associated countries and stakeholders, to better coordinate R&I policies at all levels. It fosters their sense of ownership and increased commitment and contributes to working on the concept of a 'fifth freedom' – the Single Market for R&I. The ERA Policy Agenda for the next three-year cycle (2025-2027) aims to:

— contribute to enhancing EU competitiveness and ensuring the EU's strategic autonomy, while preserving an open economy, by coordinating dedicated investments and reforms in R&I and, where appropriate, pooling resources at national and, where applicable, regional levels, and at EU level which are available in the current Multiannual Financial Framework 2021-2027;

— strengthen the EU's R&I excellence and impact, its global scientific leadership and attractiveness to global talent by streamlining research career paths, facilitating researchers' mobility and knowledge sharing across Europe, and promoting access to cutting-edge infrastructures; and

— enhance the EU's sustainable development and societal impact by coordinating R&I efforts in industrial transformation, by developing synergies with other policies and by promoting a more circular and resilient economy.

ELI: http://data.europa.eu/eli/C/2025/3593/oj
1/22

Altre novità recenti:

- La Svizzera farà partire nel 2026 un National Competence Center for Scientific Integrity.
- Negli USA: SECURE sta preparando uno shared virtual environment per fornire risorse e strumenti di valutazione, SECURE ANALYTICS sta testando una piattaforma dedicata.
- Rapporto OECD "Science, Technology and Innovation (STI) Outlook 2025: Driving Change in a Shifting Landscape" esamina come scienza, tecnologia e innovazione possano sostenere un cambiamento trasformativo nell'economia e nella società e come la cooperazione scientifica viene ridefinita dalle dinamiche geopolitiche.

Ricerca nel settore difesa e dual use

INFN Istituto Nazionale di Fisica Nucleare

CoPER CONSULTA DEI PRESIDENTI DEGLI ENTI DI RICERCA

Tra le tante iniziative:

Quantum Scientists for Disarmament

We are a group of quantum scientists who oppose the ongoing militarization of our societies and the use of quantum research for military purposes. You can read our manifesto below.

If you are a quantum scientist and wish to support our manifesto, you may sign it using the form provided below the list of signatories.

MANIFESTO

The manifesto is also available on arXiv: https://arxiv.org/abs/2601.14282

Signatures

SCIENCE|BUSINESS®

Bringing together industry, research and policy

News ▾ Funding Newswire ▾ Reports Events The Network ▾ Communications Services ▾ About Us ▾

FP10 should focus on 'dual-use by design,' Commission advisory group says

03 Jul 2025 | News

Dual use | Defence | Planning FP10 | R&D Policy

The European Commision is also looking at how dual use research is handled in other parts of the world

By Lola Laws

Photo credits: Anne Davis 773 / Flickr

The EU should integrate dual-use research in FP10, the next Framework programme for research and innovation, and align it with the European Defence Fund, a new report but the European Commission's expert group on the economic and societal impact of research and innovation (ESIR).

"The EU should adopt a 'dual use by design' approach as a vital pillar for ensuring Europe's security, competitiveness and prosperity," the report says. "The persistent division between civilian and defence R&I is leading to a loss of competitive advantages in emerging technologies."

The report suggests that, by pooling resources and leveraging synergies between civilian and military research, the EU could foster new innovations more easily and faster.

The Guild

News & Blog › Blog ›

Horizon Europe must remain civilian

By: Jan Palmowski

The European Commission has proposed that from 2026 the European Innovation Council's Accelerator programme may fund defence technologies. This would end what has until now been a legally mandated focus on purely civilian research and innovation in 40 years of EU funding.

The move also foreshadows the Commission's proposal to open the whole of the next iteration of Horizon Europe—the 10th EU Framework Programme for research and innovation (FP10), beginning 2028—to dual-use and collaborative defence research. What will change if Horizon Europe is no longer a civilian-only research and innovation programme?

There is wide agreement that even in a civilian programme such as Horizon Europe, much, possibly most, research already has dual-use potential. Even so, the changes proposed raise five fundamental concerns.

Budget drain

To begin with, applied dual-use and defence research and innovation may require bigger budgets, not least because such work is subject to more stringent regulations and security controls. Whatever the budget for the next Horizon Europe programme, adding defence and dual-use research would divert money from civilian research.

Second, the Commission already funds military research through the European Defence Fund. Rather than reorient the EIC Accelerator programme, the Commission could and should have changed the EDF's regulation to allow direct equity investment in scale-up companies.

Similarly, the planned European Competitiveness Fund (ECF) is set to spend €125 billon on defence industry research and development alone: that is clearly the place to fund defence research and scaleup, not Horizon Europe.

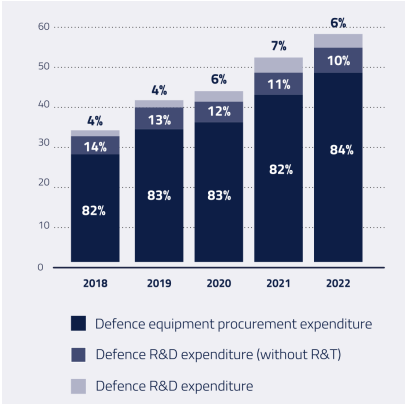
International exclusions

Third, many of the changes envisaged by the Commission for the immediate future of research and innovation policy concern the exclusion of third countries. It proposes to limit defence projects to entities in the EU, the European Economic Area and Ukraine, excluding other countries associated with Horizon Europe such as the UK. Exclusions could also apply to dual-use calls, and to private companies owned by entities outside the EU.

If in future, all of FP10 "may support dual-use actions", as the current draft regulation proposes, how attractive will it be to third countries that have little idea of which parts of the programme they can access? How attractive will it be to top EU researchers if their peers in the UK or Switzerland might be excluded from calls in artificial intelligence or quantum computing?

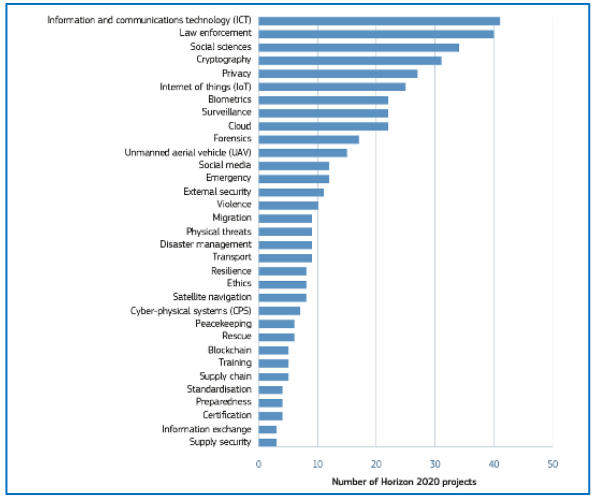
Dual-use calls would impair the programme's openness in terms of publication as well as collaboration. Who will decide what data and results have the potential for military applications and are, therefore, exempt from open science mandates? Opening Horizon Europe to dual-use research could upend 10 years of the Commission-led drive towards open science.

https://research-and-innovation.ec.europa.eu/document/download/7ae11ca9-9ff5-4d0f-a097-86a719ed6892_en?filename=ec_rtd_white-paper-dual-use-potential.pdf



DG Research and Innovation basato su EDA Defence Data 2022

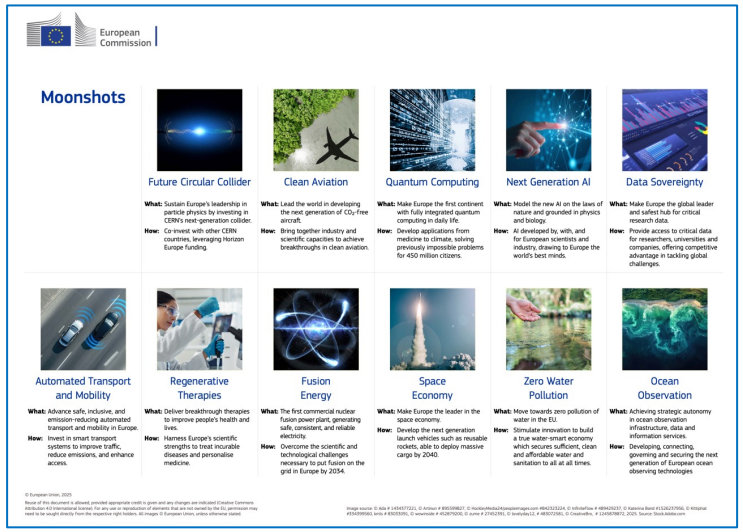
Progetti Horizon 2020 connessi alla dfesa
https://publications.jrc.ec.europa.eu/repository/handle/JRC120636



Framework Program 2028-2034

Proposta per FP 10

Pillar I	Pillar II	Pillar III	Pillar IV
EXCELLENT SCIENCE	COMPETITIVENESS AND SOCIETY	INNOVATION	EUROPEAN RESEARCH AREA
€44.079 BILLION	€75.876 BILLION	€38.785 BILLION	€16.262 BILLION
EUROPEAN RESEARCH COUNCIL	COMPETITIVENESS[1] : 1. Clean Transition and Industrial Decarbonisation 2. Health, Biotech, Agriculture and Bioeconomy 3. Digital leadership 4. Resilience and Security, Defence Industry and Space	EUROPEAN INNOVATION COUNCIL	ERA POLICIES
MARIE SKŁODOWSKA-CURIE ACTIONS	SOCIETY: 1. Global societal challenges 2. EU Missions 3. New European Bauhaus Facility	INNOVATION ECOSYSTEMS AND THE KNOWLEDGE TRIANGLE	RESEARCH AND TECHNOLOGY INFRASTRUCTURES
SCIENCE FOR EU POLICIES			WIDENING PARTICIPATION AND SPREADING EXCELLENCE



- Proposta iniziale della **Commissione** luglio 2025: 175 miliardi, integrazione con European Competitiveness Fund [in particolare per Pillar II], forte subordinazione dei Councils alla Commissione; ECF definisce anche le regole di collaborazione [basate su sicurezza economica principalmente]; ricerca dual use permessa, non chiaro se possibile R&D direttamente connesso alla difesa
- Draft Report della commissione del Parlamento ITRE, **C. Ehler**: non «parts» ma «pillars» [continuità]; ERC e EIC indipendenti; richiami a **Rapporto Draghi** e **Rapporto Heitor**; 220 miliardi e «Fast Track» [to Excellence e to Innovation]; regole sulla sicurezza più chiare
- Moonshots [grandi progetti, molto ambiziosi] al posto delle Missions [ITRE chiede abbiano un ruolo di trasversalità tra strumenti e politiche e non solo di finanziamento]

Altre considerazioni:

- Le norme sulla sicurezza non devono pregiudicare le collaborazioni internazionali nella ricerca fondamentale [futuro di strumenti come MSCA, ERC grants]
- Molti programmi dei Moonshots sono chiaramente dual use
- Quale sarà l'entità dei fondi per la difesa? Quale separazione con FP 10?

Istituto Nazionale di Fisica Nucleare

CoPER CONSULTA DEI PRESIDENTI DEGLI ENTI DI RICERCA

Disciplinare INFN – 1

3. Nel raggiungimento dei propri obiettivi, l'INFN attribuisce fondamentale rilevanza alla libertà della ricerca anche con riguardo alla cooperazione internazionale che considera componente fondamentale per promuovere l'eccellenza scientifica, unitamente alla mobilità internazionale del proprio personale della ricerca come definito nel successivo art. 3, comma 1.6

4. L'INFN ha consapevolezza del contesto internazionale e dei rischi per le collaborazioni nel settore della ricerca connessi a trasferimenti indesiderati di conoscenze e tecnologie verso Paesi terzi che potrebbero utilizzarli per scopi non pacifici con ripercussioni sul rispetto dei valori e diritti fondamentali della persona o sulla sicurezza nazionale ed europea.

5. Accogliendo la Raccomandazione del Consiglio dell'Unione europea del 23 maggio 2024 e tenuto conto del Modello Nazionale e delle Linee-Guida adottate nell'agosto del 2025 dal Ministero dell'Università e Ricerca a seguito di un lavoro congiunto CoPER-CRUI-MUR, l'INFN intende garantire assistenza e sostegno al proprio personale di ricerca affinché possa svolgere la propria attività secondo principi di libertà, apertura e cooperazione, anche internazionale, salvaguardando la sicurezza della ricerca.

6. L'INFN, pur non svolgendo alcun tipo di attività di ricerca a fini militari, è però consapevole che software e tecnologie promosse e finanziate per scopi pacifici e di ricerca scientifica di base potrebbero essere utilizzati in applicazioni nel settore militare da entità, Stati od organismi che hanno fini estranei a quelli pacifici della ricerca o utilizzati impropriamente per scopi contrari agli accordi internazionali, ai regolamenti europei e alle leggi nazionali sul controllo dei prodotti a duplice uso che potrebbero essere impiegati per la progettazione, lo sviluppo, la produzione e l'uso di armi nucleari, chimiche o batteriologiche. Il presente Disciplinare, in linea con le raccomandazioni europee e nazionali in materia, regolamenta anche tali attività a duplice uso.

7. Lo scopo di questo disciplinare, pertanto, non è in alcun modo quello di limitare o vietare attività scientifiche di qualsivoglia natura, se coerenti con la missione scientifica dell'Istituto, ma è quello di sensibilizzare tutti i soggetti coinvolti nell'attività e nella vita dell'INFN ai temi della sicurezza della ricerca e a mettere in atto misure ragionevoli e proporzionate per mitigare i rischi ad essa connessi.

Valori e principi
- Libertà della ricerca
- Condivisione della conoscenza
- Collaborazione internazionale
- Tutela dei diritti della persona
- Sicurezza nazionale ed europea

Rifiuto della ricerca a fini militari

Consapevolezza della possibilità di dual use

Scopo:
- Aumentare consapevolezza
- Mitigare i rischi

Disciplinare INFN – 2

Art. 2 Finalità e ambito di applicazione

1. Il presente Disciplinare è diretto a sollecitare e agevolare la valutazione preliminare delle criticità e rischi di sicurezza eventualmente associati alle attività di ricerca mediante la definizione di un assetto organizzativo adeguato a sostenere il personale della ricerca INFN nell'adozione di decisioni informate per la gestione dei rischi, la conservazione e il rafforzamento della sicurezza della ricerca.
2. La prima applicazione del presente Disciplinare costituisce una sperimentazione volta a dare attuazione ai principi generali enunciati all'articolo 1. I provvedimenti e le raccomandazioni emanati saranno oggetto di verifica dell'efficacia e rispondenza agli obiettivi, nonché di eventuale revisione.
3. L'INFN si coordina con il Ministero dell'Università e della Ricerca ed in particolare con la Direzione generale per la valutazione e la sicurezza della ricerca, con il Centro nazionale per la sicurezza e integrità della ricerca, con gli altri Ministeri e con tutte le Autorità coinvolte nella definizione ed attuazione di strategie e prassi dirette a raggiunge e rafforzare gli obiettivi di sicurezza nazionale.

Un'organizzazione di supporto per:

- Valutare e gestire i rischi
- Prendere decisioni informate
- Rafforzare la sicurezza della ricerca

Coordinamento con il MUR e con gli altri Ministeri e Autorità di settore

Disciplinare INFN – 3

Art. 4 - Referente per la Sicurezza e l'Integrità della Ricerca

1. L'INFN istituisce la figura del Referente per la Sicurezza e l'Integrità della Ricerca (di seguito anche ReSIR).
2. Il ReSIR è nominato dal Presidente dell'INFN, dura in carica quattro anni e può essere rinnovato per una sola volta.
3. Il ReSIR svolge i propri compiti secondo le linee-guida fornite dal Consiglio Direttivo e dalla Giunta Esecutiva dell'INFN ed opera in stretta collaborazione con i Direttori delle Strutture e con i Presidenti delle Commissioni Scientifiche Nazionali, conciliando la propria attività con le esigenze scientifiche, organizzative, tecniche e territoriali delle Strutture. Il Consiglio Direttivo può affiancare al ReSIR un panel di esperti di supporto.
4. Il Referente per la Sicurezza e l'Integrità della Ricerca ha il compito di:
    a. elaborare, in collaborazione con le Commissioni Scientifiche Nazionali e la Giunta Esecutiva, linee-guida relative all'attivazione di collaborazioni con istituzioni di aree con profili di rischio medio-alto e alla gestione di finanziamenti provenienti dalle suddette aree;
    b. definire, unitamente ai responsabili di attività scientifica o tecnologica, misure di mitigazione del rischio per la sicurezza e l'integrità della ricerca proporzionate per le attività con profilo di rischio meritevole di attenzione;
    c. fornire supporto, in collaborazione con la Commissione Calcolo e Reti INFN, la Direzione Sistemi Informativi INFN e le Autorità nazionali competenti, per la definizione di procedure da attuare in caso di rischi per la sicurezza informatica che interferiscano con la sicurezza e l'integrità della ricerca.
    d. proporre al Consiglio Direttivo un modello di protocollo per i visitatori diretto a ridurre eventuali criticità durante la visita alle Strutture INFN, monitorandone l'attuazione in raccordo con i Direttori delle Strutture;
    e. proporre al Consiglio Direttivo un protocollo e un vademecum per le missioni del personale dipendente e associato, in particolare verso aree (di transito o di destinazione) con profili di rischio medio-alto, monitorandone l'attuazione, tenuto conto delle linee-guida e delle indicazioni per i viaggi di lavoro rese disponibili dal Centro nazionale per la sicurezza e integrità della ricerca;
    f. proporre al Consiglio Direttivo politiche per la gestione di conflitti di interessi come definiti all'art. 3, comma 1.7
    g. promuovere attività di informazione e formazione del personale della ricerca sulle tematiche della sicurezza e integrità della ricerca, coordinandosi con la Commissione Nazionale Formazione dell'Istituto e i suoi referenti locali;
    h. curare, in accordo con la Giunta Esecutiva, i rapporti con il Centro Nazionale per la sicurezza e integrità della ricerca, l'Autorità per la Cybersicurezza Nazionale e le altre Autorità e Istituzioni competenti in tema di Sicurezza e Integrità della Ricerca, adottando tempestivamente pratiche di aggiornamento coerenti con l'evoluzione normativa eurounitaria e nazionale;
    i. monitorare potenziali criticità per la sicurezza e l'integrità della ricerca anche mediante la realizzazione di modelli standard per la valutazione dei rischi;
    j. curare la raccolta e gestione dei dati relativi alle collaborazioni esterne dell'INFN, provvedendo al loro costante aggiornamento.

Il Referente per la Sicurezza e l'Integrità della Ricerca

Disciplinare INFN – 4

Art. 5 – La gestione dei rischi per la sicurezza della ricerca

1. Il personale della ricerca che ravvisi rischi per la sicurezza della ricerca si rivolge al Direttore della Struttura di afferenza per ottenere chiarimenti o supporto per la corretta attuazione dei principi contenuti nel presente Disciplinare.
2. Il Direttore di Struttura ha il compito di verificare preventivamente che per ogni attività di ricerca o progetto o collaborazione scientifica o tecnologica con Enti stranieri siano stati valutati i rischi evidenti o le criticità in merito ai contenuti di questo disciplinare al fine dell'applicazione di quanto specificato di seguito.
3. Il Direttore di Struttura, qualora ritenga di avere individuato una questione di particolare complessità o rilievo, può rivolgersi al ReSIR il quale si adopererà per fornire il supporto richiesto anche attraverso il confronto con le Autorità nazionali preposte.
4. Qualora il Direttore o il ReSIR ravvisino elementi di criticità in seguito alle attività di cui ai punti 2. e 3., di comune accordo elaborano una strategia di mitigazione del rischio e la comunicano in forma scritta sia agli organi di governo dell'Ente sia al personale coinvolto nell'attività stessa.
5. Il ReSIR raccoglie le richieste in un'apposita base dati utile a predisporre FAQ per la gestione di successivi casi analoghi.

Art. 6 - Informazione e Formazione

1. L'INFN provvede a un'adeguata informazione e formazione del personale della ricerca sul tema della sicurezza e integrità della ricerca.
2. Il ReSIR, in accordo con la GE, propone linee-guida e vademecum sui temi rilevanti in materia; organizza, coordinandosi con la Commissione Nazionale Formazione, corsi appositi presso le Strutture anche in modalità telematica.

Art. 7 - Attività a duplice uso [dual-use]

1. L'INFN promuove attività di formazione e informazione del personale della ricerca in merito ai rischi inerenti alle attività a duplice uso, privilegiando come strumento primario il criterio dell'autovalutazione informata.
2. Il ReSIR collabora al monitoraggio della corretta e completa applicazione delle norme vigenti in materia di tecnologie a duplice uso.
3. Il ReSIR ha il compito di redigere e proporre all'approvazione della Giunta Esecutiva e del Consiglio Direttivo opportune linee-guida dirette a regolare le attività a duplice uso e ad implementare nell'INFN le norme vigenti in materia.
4. Nel caso di attività di duplice uso le prescrizioni di cui all'art. 5.4 sono sempre necessarie.

Art. 8 - Valutazione dei rischi e controlli

1. Il ReSIR coadiuva e supporta i Direttori delle Strutture nel monitoraggio e nella verifica della corretta attuazione delle disposizioni contenute nel presente Disciplinare.
2. Il personale della ricerca, formato e informato dall'INFN, è tenuto ad attenersi scrupolosamente alle prescrizioni del presente Disciplinare.
3. Il ReSIR organizza, in collaborazione con il Servizio Trasferimento Tecnologico, la Direzione Servizi alla Ricerca, la Commissione Calcolo e Reti e i Direttori delle Strutture, controlli periodici delle attività in corso e in modo particolare dei progetti finanziati su fondi esterni in merito alla corretta applicazione del presente Disciplinare.
4. Il Direttore di Struttura, ove ravvisi condotte adottate in violazione del presente Disciplinare ne dà segnalazione al ReSIR.

Né **naïveté**…

…né **paranoia**

Ma **valutazione** e **mitigazione** del rischio