Stato della ricerca sulla cybersicurezza in Italia

Un'analisi basata sulla Valutazione della Qualità della Ricerca (VQR) 2020-2024

anvur

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

Stato della ricerca sulla cybersicurezza in Italia

Un'analisi basata sulla Valutazione della Qualità della Ricerca (VQR) 2020-2024

Agenzia nazionale di valutazione del sistema universitario e della ricerca

Agenzia per la cybersicurezza nazionale

Indice

Prefazione

Come è noto, la diffusione delle tecnologie digitali ha determinato una profonda trasformazione dell'economia e della società, creando nuove opportunità ma anche rischi. Ogni giorno, miliardi di persone generano dati personali, navigano sulla rete, utilizzano applicazioni e piattaforme, interagiscono con dispositivi connessi. Oltre a imprese e consumatori, anche Stato centrale, enti territoriali e Pubbliche Amministrazioni si avvalgono costantemente di infrastrutture digitali, ponendo in essere attività spesso dematerializzate e trasferendo e adoperando enormi quantità di informazioni.

Dinanzi a tali fenomeni, fondamentale appare la protezione di sistemi informatici, di reti come anche di dati non solo al fine di impedire disfunzioni e inefficienze (data breach e interruzioni di rete), tattiche di hacking e soprattutto per garantire diritti fondamentali di libertà (riservatezza e tutela dell'identità personale), interessi economici, interesse pubblico e democrazia. In questo contesto la cybersecurity diviene funzione pubblica (si veda il Cybersecurity Act del 2019, che stabilisce il quadro regolatorio europeo per la sicurezza informatica di prodotti, servizi e processi digitali) e viene istituita l'Agenzia per la cybersicurezza nazionale (ACN) con il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico (cfr, D.l. n. 82/2021), di prevenire attacchi cibernetici e promuovere sovranità e autonomia tecnologica. In questo ambito, particolare rilevanza assume la ricerca sia in considerazione della continua evoluzione tecnologica, sia per il numero sempre crescente di dispositivi connessi (smart home, auto, sensori, ecc.) e quindi di minacce digitali e attacchi ibridi.

Il libro bianco che ho l'onore di presentare risponde all'esigenza di rappresentare lo stato attuale della ricerca sulla cybersicurezza da parte di Università e enti di ricerca anche al fine di cogliere punti di forza e di debolezza, offrendo preziosi strumenti conoscitivi al decisore pubblico. Esso nasce dalla proficua e intensa collaborazione avviata di recente in forza di una convenzione tra ACN e Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR) nella consapevolezza della rilevanza di un comune impegno nel censire l'esistente, apprezzare i risultati della ricerca scientifica di qualità e delineare percorsi e strumenti di valorizzazione industriale della stessa, consolidando vocazioni e competenze del nostro sistema e riducendo dipendenze tecnologiche da altri Paesi.

Il valoroso gruppo di lavoro, a cui va il mio sincero ringraziamento, ha in primo luogo condiviso la metodologia dell'indagine, consistente nella ricognizione dei lavori scientifici in materia di sicurezza cibernetica e dai casi studio e iniziative di trasferimento tecnologico e valorizzazione della conoscenza sempre sugli stessi ambiti conferiti dalle Università ed enti di ricerca nell'ambito della valutazione periodica condotta dall'ANVUR, cosiddetta VQR-Valutazione della Qualità della Ricerca 2020/2024. Sebbene si tratta di temi nuovi, l'analisi evidenzia risultati interessanti. Tra i 1154 lavori scientifici censiti, il 27 per cento riguarda la gestione delle minacce cibernetiche, il 21 per cento la sicurezza del software e delle piattaforme e il 19 per cento la sicurezza dei dati e la privacy. Più distaccate, altri ambiti come la sicurezza delle infrastrutture digitali, gli aspetti di *governance, ecc*. I risultati offrono anche dati omogenei su tutto il territorio nazionale pur con un maggiore attivismo delle istituzioni del Nord con una percentuale complessiva del 42%; tuttavia, anche le altre macroaree geografiche hanno conferito buone percentuali di pubblicazioni a fronte del 38 per cento di Sud e isole e 18 per cento centro (mento

attive le Università telematiche anche per la natura dell'offerta formativa erogata e per la composizione del corpo docente). Anche i dati riguardanti i corsi di dottorato di ricerca sono confortanti, evidenziando una qualche prevalenza di concentrazione nel Nord Italia (49%) ma anche una buona tenuta di tutte le altre aree territoriali.

Rinviano a dati e tabelle presentati nel libro bianco, posso esprimere la soddisfazione per un lavoro, primo in Italia e in Europa, che si segnala per la completezza della mappatura della ricerca nei diversi ambiti della cybersicurezza e la forte vitalità del sistema della ricerca nel Nostro Paese. Un lavoro che lascia ben sperare per le prospettive di sviluppo della conoscenza in materia; riprendendo Sant'Agostino una conoscenza "che si rinnova continuamente e che rivela il carattere dinamico dell'esistenza umana", una "speranza che è compagna del viaggio della vita e che è forza che non si spegne.

Last but not least, un sincero ringraziamento va alla Prof.ssa Alessandra Celletti, vicepresidente di ANVUR, infaticabile e valorosa responsabile della VQR che, con il prof. Massimo Tronci, componente del consiglio direttivo dell'agenzia, dott. Marco Malgarini, dirigente dell'area ricerca e Dott.ssa Paola Costantini, responsabile UO Statistica, hanno svolto, per conto dell'agenzia, il complesso lavoro di raccolta e sistemazione dei dati, e, per ACN, il prof. Mario Caligiuri, che ha ispirato e fortemente promosso la collaborazione tra le nostre agenzie e la stesura del rapporto e le dott.sse Monica Scannapieco, Carola Aiello, il dott. Marco Centenaro e il dott. Danilo D'Elia per il rigore e l'attenzione con la quale hanno partecipato alla raccolta e analisi dei dati.

Infine, un vivo ringraziamento al sottosegretario Alfredo Mantovano, autorità delegata per la sicurezza della Repubblica, alla Ministra dell'Università e della ricerca Sen. Prof. Annamaria Bernini, e al prefetto Bruno Frattasi, direttore di ACN per il costante sostegno e l'attenzione con la quale hanno seguito il progetto che ci auguriamo tutti possa proseguire anche nei prossimi anni.

Antonio Felice Uricchio
Presidente ANVUR

Il Rapporto “Stato della ricerca sulla cybersicurezza in Italia” rappresenta una prima ricognizione sistematica sulla ricerca in cybersicurezza in Italia, realizzata nel solco della missione dell’Agenzia per la cybersicurezza nazionale: promuovere la conoscenza scientifica e diffondere una cultura della sicurezza digitale come fondamento della resilienza del Paese.

Si tratta di un lavoro frutto di una concreta collaborazione istituzionale con l’Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca, presieduta da Antonio Felice Uricchio. Abbiamo insieme segnato un passaggio essenziale, perché il rapporto consente per la prima volta di disporre di una visione organica e comparabile di un ambito strategico che, oltre a supportare le attività di ACN e ANVUR, offre al decisore pubblico strumenti concreti per orientare politiche e investimenti.

Viviamo in una dimensione in cui la cybersicurezza non è più un settore specialistico, ma una condizione generale dell’esistenza contemporanea. Infatti, la cybersicurezza è un tema che riguarda tutti, sia i cittadini, sia le imprese e le istituzioni, coinvolgendo ogni dimensione umana. Proteggere lo spazio cibernetico significa garantire continuità operativa, fiducia nei servizi digitali e tutela dei diritti fondamentali, in un equilibrio sempre più delicato tra innovazione e sicurezza.

La mappatura, realizzata con l’ANVUR nell’ambito dell’esercizio della Valutazione della Qualità della Ricerca (VQR) nel periodo 2020–2024, offre un quadro articolato e interessante. Su oltre 200.000 pubblicazioni analizzate, 1.154 sono attinenti alla cybersicurezza e di queste: il 27% riguarda la gestione delle minacce cibernetiche, il 21% la sicurezza del software e delle piattaforme e il 19% la sicurezza dei dati e della privacy, il 12% la sicurezza delle infrastrutture digitali, l’11% gli aspetti della società e il 10% gli aspetti di governo. Sono dati che evidenziano una buona capacità di risposta alle minacce più immediate, ma anche la necessità di rafforzare ambiti meno presidiati.

Nel complesso, tuttavia, nei dati VQR osservati, la cybersicurezza rappresenta ancora meno dell’1% della produzione scientifica totale nazionale, quota che resta inferiore al 4% anche considerando le aree disciplinari più vicine. Questo dato impone una riflessione strategica: non è più rinviabile un investimento strutturale che aumenti massa critica, qualità e impatto della ricerca in un settore determinante per la sicurezza nazionale e quindi per la vita dei cittadini.

L’analisi tematica evidenzia, inoltre, squilibri significativi. La sicurezza delle infrastrutture digitali registra circa il 57% di contributi in meno rispetto alla gestione delle minacce, mentre risultano ancora marginali le scienze forensi digitali. Negli aspetti sociali prevale la dimensione giuridica (46%), mentre restano più deboli le componenti umane, culturali e formative, che costituiscono, come è noto, il primo livello di difesa nello spazio cibernetico. Sul piano dell’innovazione, le tecnologie quantistiche mostrano segnali di crescita ma incidono per meno dell’8% negli ambiti prioritari. Procedono più lentamente anche le ricerche su sistemi cyber-fisici e reti di nuova generazione, contesti cruciali per la protezione delle infrastrutture critiche e per il rafforzamento dell’autonomia strategica nazionale. In tale quadro, porre in sicurezza i sistemi e le infrastrutture significa proteggere economia, democrazia, sviluppo futuro e qualità della ricerca.

La distribuzione territoriale mostra una prevalenza del Nord (42% delle pubblicazioni), ma anche una partecipazione significativa di Sud e Isole (38%) e del Centro (18%). Si delinea così una diffusione

nazionale, che tuttavia necessita di maggiore integrazione e coordinamento, anche sul piano della ricerca dottorale. Permane, inoltre, un divario di genere nei temi di cybersicurezza a connotazione prevalentemente STEM, con una presenza femminile tra il 15% e il 20% nelle aree più tecniche, segnale di un potenziale ancora non pienamente valorizzato.

Nel complesso, questa prima ricognizione restituisce l'immagine di un sistema vitale ma ancora in fase di consolidamento. Le iniziative di valorizzazione e trasferimento tecnologico, pur limitate, indicano una traiettoria promettente che deve essere rafforzata, trasformando la ricerca in capacità operativa e vantaggio competitivo. È da qui che occorre proseguire, con continuità e visione. Perché, la cybersicurezza è ormai una leva fondamentale per la crescita economica e la qualità della democrazia. Investire nella ricerca in cybersicurezza, in ultima analisi, significa investire nella sicurezza, nella libertà e nel futuro del Paese.

Bruno Frattasi
Direttore Generale ACN

Sintesi

La cybersicurezza costituisce un ambito di crescente rilevanza per il sistema-Paese italiano, anche in virtù dell'attuale quadro geopolitico internazionale. Al fine di mantenere la competitività nelle tecnologie ad alto impatto economico e strategico per la sicurezza nazionale, è necessario poter contare su un ecosistema della ricerca e dell'innovazione capace di produrre risultati della ricerca scientifica di qualità, e allo stesso tempo di trasformare tali risultati in soluzioni industriali, riducendo dipendenze tecnologiche e rafforzando la resilienza nazionale.

In questo contesto, l'Agenzia per la cybersicurezza nazionale (ACN) e l'Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR) hanno avviato una collaborazione con l'obiettivo di far emergere lo stato attuale della ricerca sulla cybersicurezza, al fine di individuare eventuali criticità e punti di forza e supportare l'assunzione di decisioni volte al rafforzamento della capacità scientifica e tecnologica del Paese.

In particolare, sono state analizzate le pubblicazioni scientifiche sottoposte dalle principali Istituzioni di ricerca italiane alla valutazione periodica condotta dall'ANVUR, cosiddetta VQR-Valutazione della Qualità della Ricerca, per caratterizzarle in relazione alle tematiche inerenti alla cybersicurezza. Sono state inoltre prese in esame le principali iniziative di trasferimento tecnologico in materia di sicurezza cibernetica effettuate dagli atenei e dagli enti di ricerca, nonché i corsi di dottorato inerenti alla cybersicurezza attivati su territorio nazionale.

L'analisi, nel suo complesso, ha consentito di produrre una prima mappatura delle tematiche di cybersicurezza affrontate dalle Istituzioni di ricerca che operano in Italia. I risultati dell'analisi, presentati in questo rapporto, sono diretti all'intero ecosistema della ricerca pubblica e privata, e anche alle Amministrazioni e Organizzazioni pubbliche italiane impegnate nella definizione di politiche per la ricerca.

1 Introduzione

La ricerca nel campo della cybersicurezza rappresenta un pilastro essenziale per consolidare l'autonomia strategica dell'Italia, soprattutto in un quadro geopolitico in rapida evoluzione, nel quale diventa imprescindibile investire con decisione in tecnologie nazionali ed europee. Solo così è possibile mantenere il ritmo dell'innovazione globale e, quando le condizioni lo permettono, assumere una posizione di vantaggio rispetto ad altri Paesi impegnati nella stessa competizione tecnologica. In questo scenario, orientare in modo mirato ed efficace le risorse dedicate alla ricerca diventa un fattore determinante: una gestione strategica degli investimenti consente infatti di ottenere risultati significativi in tempi ridotti e di rafforzare la capacità del sistema Paese di misurarsi con successo con le sfide e le opportunità del settore.

L'Agenzia per la cybersicurezza nazionale (ACN), in qualità di Autorità nazionale per la cybersicurezza ai sensi del D.L. n. 82 del 14 giugno 2021 e ss.mm.ii., ha il mandato di salvaguardare gli interessi strategici del Paese in questo ambito e di accrescerne la capacità di resistere e reagire alle minacce cibernetiche. Per perseguire questi obiettivi, l'Agenzia promuove lo sviluppo della ricerca, favorisce l'innovazione e sostiene la competitività del settore industriale legato alla cybersicurezza, operando in stretta collaborazione con il mondo accademico, con i centri di eccellenza, con le imprese e con le istituzioni pubbliche.

L'Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR), istituita con D.P.R. n. 76 del 2010 e ss.mm.ii., è chiamata a misurare la qualità e l'efficacia delle attività svolte dalle università e dagli enti di ricerca italiani. ANVUR rappresenta un attore istituzionale la cui azione incide direttamente sulla comprensione e sul miglioramento del sistema scientifico nazionale, e riveste un ruolo centrale e altamente significativo nel definire il profilo e l'evoluzione della ricerca in Italia.

La collaborazione istituzionale tra ACN e ANVUR prende forma a partire dall'esigenza di disporre di una rappresentazione più ampia, accurata e misurabile del panorama nazionale dedicato alla ricerca nell'ambito della cybersicurezza. L'obiettivo finale è costruire una fotografia approfondita e affidabile che permetta di comprendere le dinamiche del settore, individuare eventuali carenze o punti di forza e supportare decisioni strategiche per il rafforzamento della capacità scientifica e tecnologica del Paese nel campo della cybersicurezza.

1.1 Obiettivi del documento

Il presente documento costituisce un rapporto congiunto tra ACN e ANVUR e si rivolge all'ecosistema della ricerca e innovazione con l'obiettivo generale di caratterizzare lo stato della ricerca in cybersicurezza in Italia, con riferimento al quinquennio 2020-2024, assumendo come fonte principale la selezione dei prodotti scientifici trasmessi dalle università nell'ambito della VQR-Valutazione della Qualità della Ricerca, che costituisce un esercizio svolto periodicamente dall'ANVUR nei confronti delle istituzioni di ricerca italiane volto a valutare la qualità della ricerca scientifica.

Per selezionare la ricerca specifica in cybersicurezza, un rilevante punto di partenza è stato il documento strategico denominato Agenda di Ricerca e Innovazione per la Cybersicurezza, redatto da ACN in collaborazione con il Ministero dell'Università e della Ricerca. Tale documento partiziona il dominio di conoscenza della cybersicurezza in sei aree, che coprono la sicurezza dei dati, le minacce cibernetiche, la sicurezza del software e delle infrastrutture digitali, gli aspetti di sicurezza legati alla società e quelli di governo della cybersicurezza.

Il presente rapporto permette di delineare in modo chiaro le caratteristiche della ricerca di qualità a livello nazionale nel settore della cybersicurezza, adottando come chiave di lettura l'Agenda di Ricerca e Innovazione (nel seguito anche Agenda di R&I). Attraverso questa prospettiva, il rapporto non solo evidenzia le aree tematiche maggiormente presidiate in termini di qualità dei risultati prodotti dalla comunità scientifica italiana, ma mette anche in relazione i risultati emersi con le priorità strategiche e gli orientamenti futuri del Paese. Nello specifico, il rapporto analizza (i) i prodotti di ricerca inerenti alla cybersicurezza, (ii) le iniziative di valorizzazione della ricerca sulla cybersicurezza e, principalmente in relazione a (i) e (ii), (iii) i ricercatori e le istituzioni di ricerca, con particolare riferimento ai corsi di dottorato operanti sui temi della cybersicurezza.

Il rapporto è un documento che sarà aggiornato, non solo sulla base delle evoluzioni intrinseche delle unità oggetto dell'analisi, ma anche sulla base di nuove esigenze di analisi che possano utilmente andare a completare il quadro presentato e che derivano dal panorama dinamico delle politiche, della ricerca e dell'innovazione in materia di cybersicurezza. I risultati presentati costituiscono un primo esercizio di mappatura dello stato della ricerca italiana in cybersicurezza che potrà essere esteso e integrato in futuro, come riportato nella Sezione 7.

I destinatari di questo studio sono tutti gli attori che gestiscono, svolgono o traggono beneficio dalle attività di ricerca in ambito cybersicurezza. Ne fanno parte l'intero ecosistema della ricerca pubblica e privata — università, imprese ed enti di ricerca — oltre alle amministrazioni e organizzazioni pubbliche italiane impegnate nella definizione di politiche per la ricerca. D'altro canto, il documento può essere un'utile lettura anche per un pubblico più ampio, non specializzato, che abbia interesse ad informarsi sullo stato della ricerca cyber.

1.2 Struttura del documento

La Sezione 2 contiene una descrizione sintetica dei risultati e delle osservazioni basate sulle analisi effettuate. Nella restante parte del documento si trovano, invece, le analisi di dettaglio. In particolare:

- la Sezione 3 descrive il quadro di riferimento delle due Agenzie coinvolte in questo studio e la metodologia adottata per effettuare le analisi;
- i risultati dell'analisi delle pubblicazioni si trovano nella Sezione 4;
- la caratterizzazione dei ricercatori e delle Istituzioni di ricerca attivi su tematiche di cybersicurezza è riportata nella Sezione 5;
- la Sezione 6 contiene i risultati dell'analisi delle iniziative di valorizzazione della ricerca;
- infine, la Sezione 7 riassume il contesto della collaborazione istituzionale tra ACN e ANVUR e ne delinea i potenziali sviluppi futuri.

1.3 Definizioni

Si fornisce di seguito una raccolta dei principali concetti e termini utilizzati nel resto del rapporto.

Area scientifico-disciplinare	Raggruppamento di discipline accademiche simili, definito a livello ministeriale in Italia per organizzare l'istruzione di livello universitario.
Corso di dottorato	Corso del più alto grado di istruzione previsto nell'ordinamento accademico italiano volto all'acquisizione delle competenze necessarie

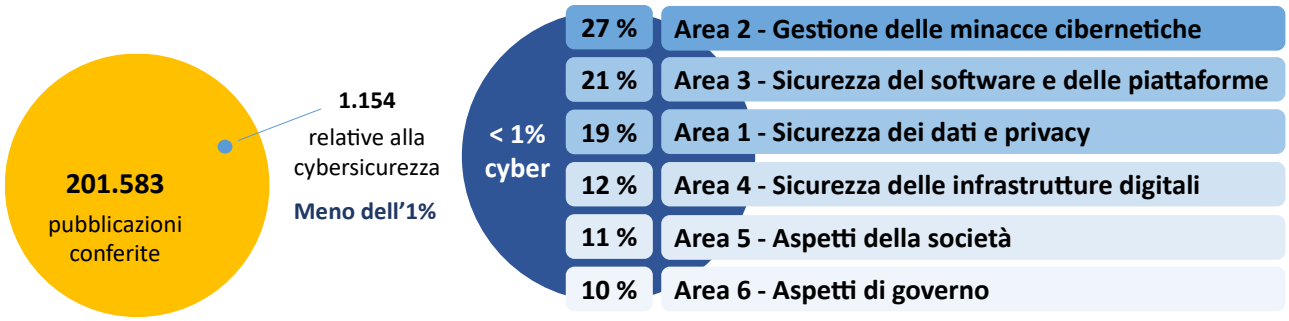
	per esercitare attività di ricerca di alta qualificazione presso Università, enti pubblici e soggetti privati.
Domini tecnologici prioritari	Insiemi di tecnologie emergenti considerati ad elevato impatto perché caratterizzati da un rapido avanzamento e/o della loro sempre più estesa adozione in ampi settori della popolazione e dell'industria.
Istituzioni di ricerca	Università legalmente riconosciute, comunque denominate, ivi compresi gli istituti universitari ad ordinamento speciale e le Università telematiche, gli Enti Pubblici di Ricerca (EPR) vigilati dal MUR, nonché istituzioni diverse che svolgono attività di ricerca e che, a differenza delle precedenti, partecipano alla Valutazione della qualità della ricerca (VQR) su base volontaria.
Prodotti della ricerca conferiti	Prodotti della ricerca così come definiti nel Bando VQR (Decreto n. 8 del 31/10/2023), prevalentemente costituiti da pubblicazioni scientifiche, e conferiti all'ANVUR nell'ambito dell'esercizio periodico di valutazione della qualità della ricerca (VQR).
Ricercatori	Personale che svolge attività di ricerca impiegato presso le Istituzioni partecipanti alla VQR. Comprende sia le qualifiche accademiche che quelle proprie degli Enti di ricerca nonché le figure a queste equivalenti in servizio presso le Istituzioni volontarie.
Tematiche di ricerca e innovazione	Argomenti di ricerca e innovazione da attenzionare nel contesto della cybersicurezza, afferenti ad aree che vanno dalla sicurezza dei dati agli aspetti di *governance* della sicurezza cibernetica.
Valorizzazione della ricerca	Attività di valorizzazione delle conoscenze, intesa come il processo con cui si crea valore economico e/o sociale a partire dalle conoscenze, collegando aree e settori diversi e trasformando i dati, le competenze tecniche e i risultati della ricerca in prodotti, servizi, soluzioni e politiche sostenibili basate sulla conoscenza e che portano vantaggi alla società. Rappresentata, ai fini della VQR, dai cosiddetti "casi di studio" conferiti dalle Istituzioni di ricerca.
Valutazione della qualità della ricerca (VQR)	Esercizio condotto periodicamente dall'ANVUR che valuta i risultati scientifici delle Istituzioni di ricerca italiane ai fini di migliorare la qualità della ricerca, orientare i finanziamenti pubblici e valorizzare l'impatto sul territorio. L'attuale quarto ciclo (2020-2024), avviato col D.M. 998/2023, valuta prodotti della ricerca (prevalentemente pubblicazioni scientifiche), valorizzazione delle conoscenze, infrastrutture di ricerca, progetti di ricerca.

Al termine del documento è stata, inoltre, predisposta una lista degli acronimi utilizzati.

2 Presentazione schematica dei risultati e commento

La collaborazione tra l'ACN e l'ANVUR ha consentito di avviare un percorso condiviso di analisi e confronto, producendo risultati concreti e significativi per il coordinamento della ricerca in cybersicurezza. Essa rappresenta un rilevante esempio di collaborazione istituzionale strutturata, espressamente finalizzata alla realizzazione di studi settoriali dedicati alla valutazione e alla promozione della ricerca di qualità, che potrebbe trovare ulteriori ambiti di applicazione.

Il quadro d'insieme fornito da questo rapporto descrive quanto le tematiche contenute nell'Agenda di Ricerca e Innovazione per la Cybersicurezza (cfr. Sezione 3.1.1) sono trattate dall'ecosistema della ricerca italiana, basandosi principalmente sulle evidenze relative ai prodotti della ricerca conferiti dalle Istituzioni di ricerca nazionali all'ANVUR nell'ambito dell'esercizio di valutazione della qualità di ricerca per il periodo 2020-2024 (cfr. Sezione 3.1.2).



L'analisi delle pubblicazioni conferite (cfr. Sezione 4) evidenzia che meno dell'1% del totale è relativo a tematiche di cybersicurezza. La prevalenza si trova nell'ambito dell'Area 2 - Gestione delle minacce cibernetiche (27%), seguita dall'Area 3 - Sicurezza del software e delle piattaforme (21%) e dall'Area 1- Sicurezza dei dati e privacy (19%). Più distaccate, si trovano pubblicazioni che trattano l'ultima branca delle tematiche di cybersicurezza nel cosiddetto ambito STEM (*Science, Technology, Engineering and Mathematics*), ovvero l'Area 4 - Sicurezza delle infrastrutture digitali (12%), seguono, infine, gli impatti della cybersicurezza sulla società con l'Area 5 -Aspetti della società (11%) e gli aspetti di *governance* della cybersicurezza con l'Area 6 – Aspetti di governo (10%).

Dal punto di vista delle aree scientifico-disciplinari delle Istituzioni di ricerca che pubblicano articoli su tematiche di cybersicurezza, invece, emergono le Scienze matematiche e informatiche e l'Ingegneria industriale e dell'informazione, che insieme coprono oltre l'80% dei contributi scientifici, seguite dalle Scienze giuridiche e dalle Scienze fisiche. Restringendo l'analisi alle prime due aree scientifico-disciplinari, i contributi inerenti alla cybersicurezza salgono dall'1% al 4% circa del totale.

Nella Figura 1 si riporta una panoramica dell'andamento temporale delle pubblicazioni nei diversi ambiti e la loro distribuzione su temi più specifici (cfr. Sezione 4.2).

Il rapporto analizza anche quattro domini tecnologici prioritari per la cybersicurezza, ovvero intelligenza artificiale, tecnologie quantistiche, *cyber-physical systems* e reti *wireless* di prossima generazione – cfr. Sezione 3.1.1. Rimandando alla Sezione 4.3 per i risultati di dettaglio sulle singole tecnologie, in questa sezione ci limitiamo a riportare che il *trend* delle pubblicazioni nel periodo 2020-2024 è in crescita per le tecnologie quantistiche, stazionario per l'intelligenza artificiale e in discesa sia per *cyber-physical systems* sia per reti *wireless* di prossima generazione. Tuttavia, le tecnologie quantistiche contribuiscono per meno dell'8% al totale delle pubblicazioni relative alla cybersicurezza nei domini tecnologici prioritari.

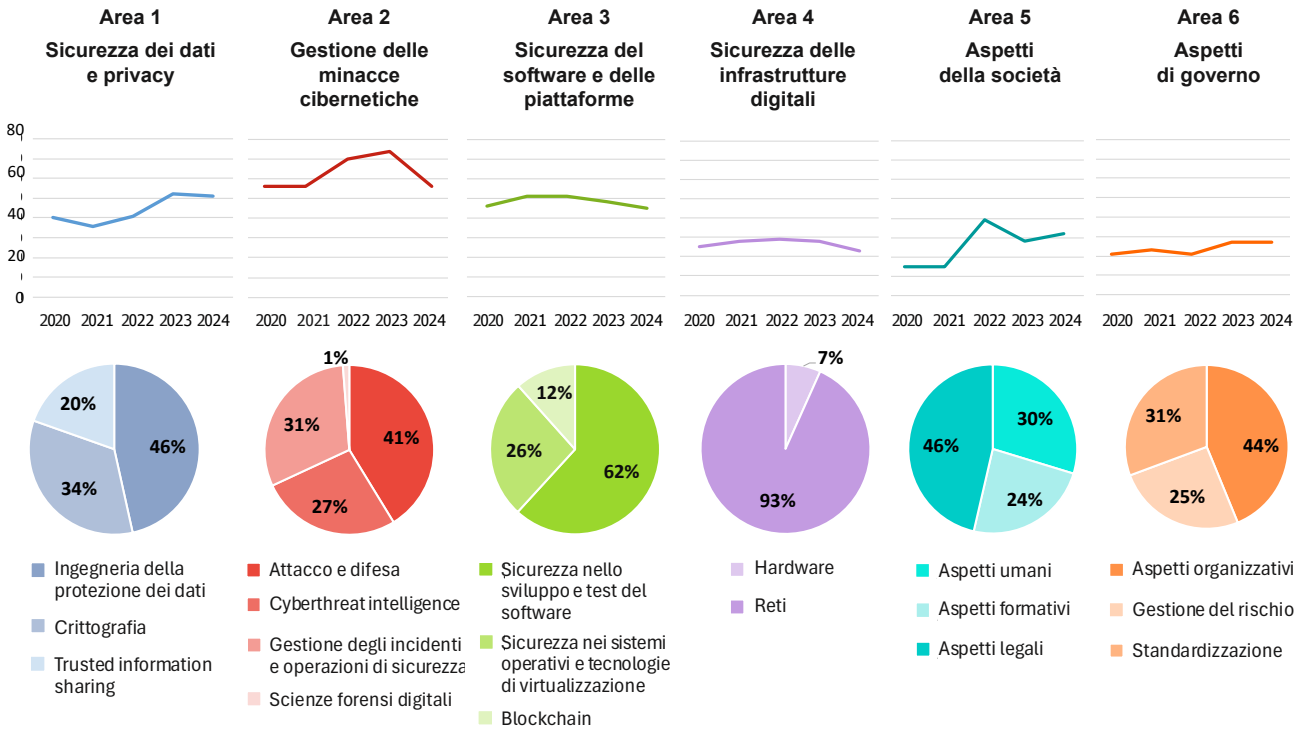


Figura 1: Panoramica dell'andamento temporale delle pubblicazioni e della relativa distribuzione sugli ambiti tematici specifici.

Passando alla caratterizzazione delle Istituzioni di ricerca attive sulla cybersicurezza (cfr. Sezione 5), dalla Figura 2 si può notare che la macro-area geografica del Nord è quella maggiormente attiva, con una percentuale complessiva del 42%, tuttavia anche le altre macro-aree geografiche hanno conferito buone percentuali di pubblicazioni.

Altri risultati salienti sono riassunti dalla panoramica fornita in Figura 3, la quale evidenzia come la ricerca sugli aspetti di cybersicurezza dei 4 domini tecnologici prioritari sia svolta nella grande maggioranza dei casi dagli atenei statali, seguiti dagli enti pubblici di ricerca. Si sottolinea, però, che su tematiche di cybersicurezza trattate nell'ambito delle tecnologie quantistiche, il peso degli enti pubblici di ricerca è più marcato rispetto alle altre tecnologie. Inoltre, analizzando la distribuzione territoriale degli atenei statali e non, emerge una prevalenza della macro-area Sud e Isole insieme a quella del Nord Italia per intelligenza artificiale e *cyber-physical systems* e del solo Nord per le tecnologie quantistiche, mentre su tematiche di reti i contributi scientifici sono piuttosto distribuiti su tutto il territorio nazionale.

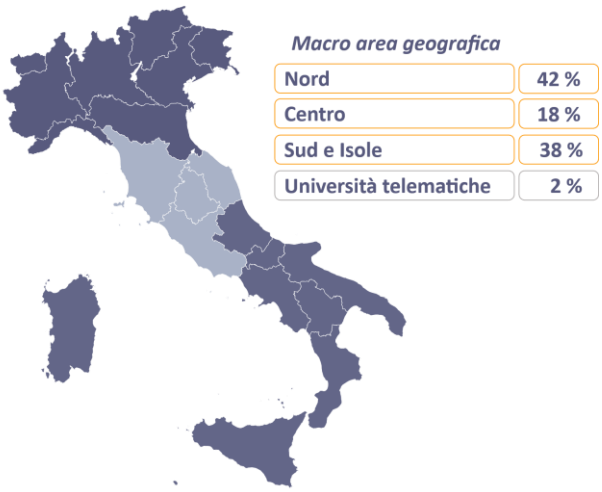


Figura 2: Distribuzione territoriale delle pubblicazioni conferite su base macro-area geografica.

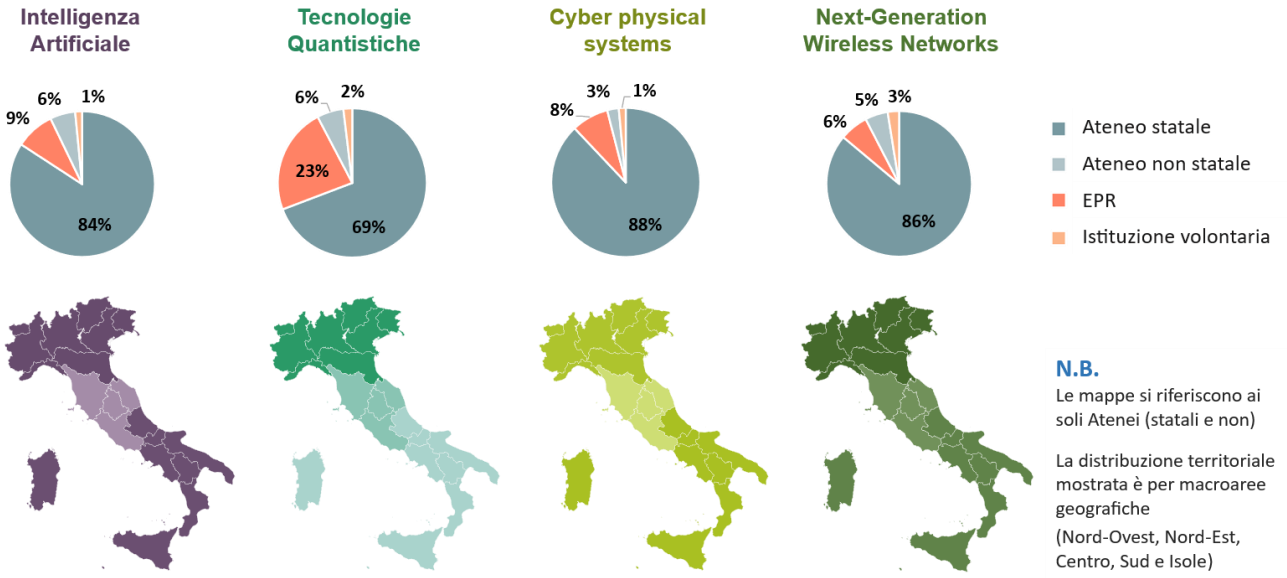


Figura 3: Panoramica dello stato della ricerca sui quattro domini tecnologici prioritari in relazione alla cybersicurezza.

Per quanto riguarda, invece, le analisi dei ricercatori attivi su tematiche di cybersicurezza (cfr. Sezione 5.1), la Figura 4 presenta le qualifiche dei ricercatori che hanno conferito pubblicazioni inerenti alla cybersicurezza, evidenziando in particolare le stesse rispetto a pubblicazioni presentate in aree dell'Agenda di R&I a prevalenza STEM (Aree 1-4) e a prevalenza NON-STEM (Aree 5-6).

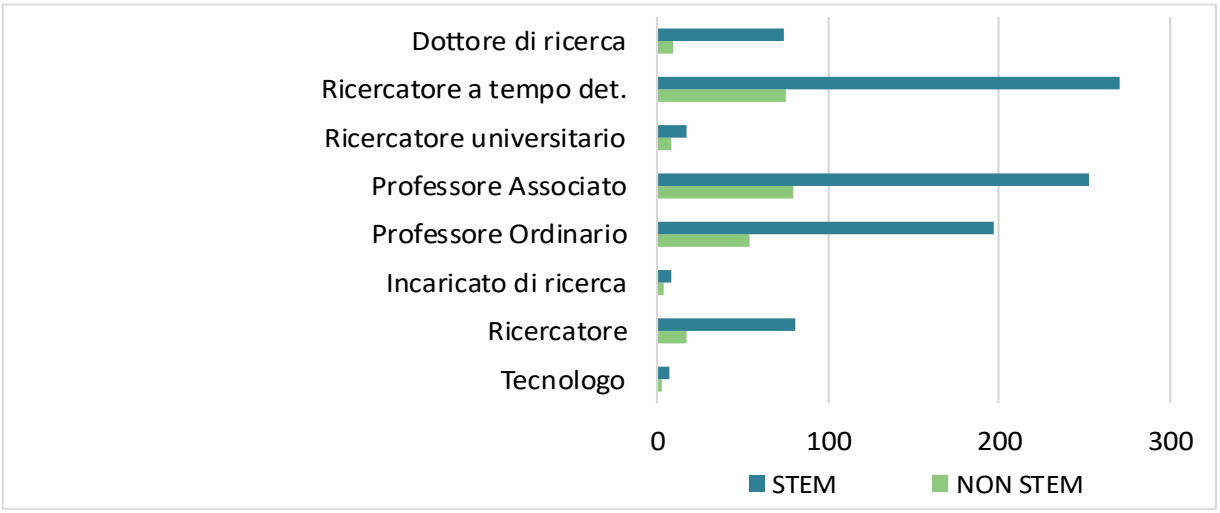


Figura 4: Qualifiche dei ricercatori per aree dell'Agenda di R&I a prevalenza STEM (Aree 1-4) e NON STEM (Aree 5-6).

Si nota nello specifico il contributo non trascurabile dei Dottori di Ricerca che però appare più marcato per le aree STEM.

Da un punto di vista di genere (cfr. Sezione 5.1), la Figura 5 illustra come le aree dell'Agenda di R&I a prevalenza STEM abbiano una netta predominanza di ricercatori uomini, mentre gli studi sugli aspetti della società e della *governance* di cybersicurezza, a prevalenza NON STEM, registrino una percentuale di ricercatrici più alta rispetto alle precedenti.

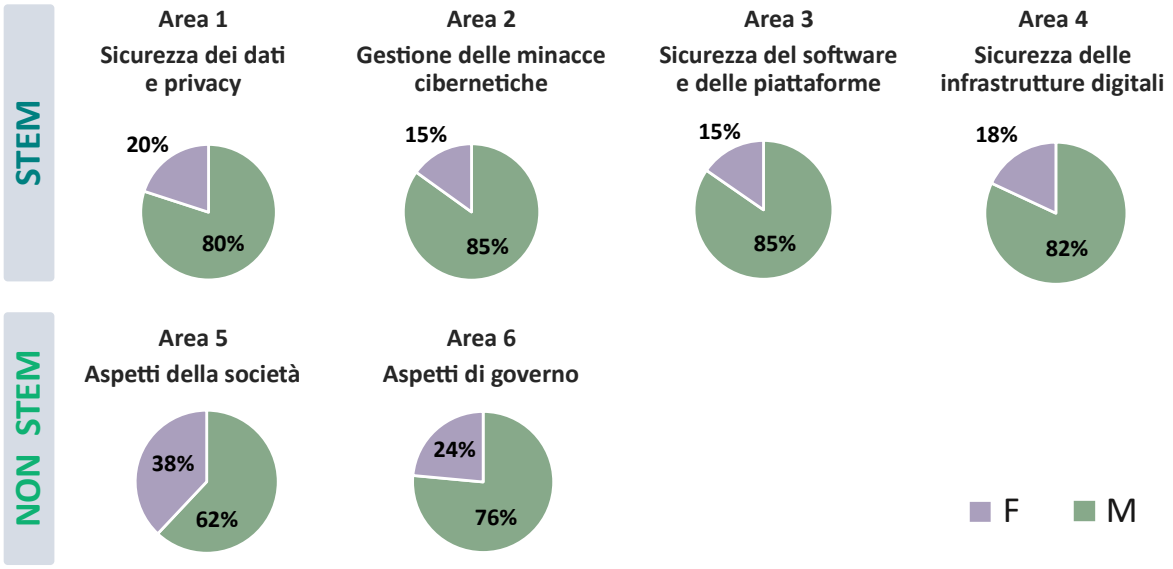


Figura 5: Genere dei ricercatori attivi su tematiche di cybersicurezza.

Inoltre, l'analisi dei corsi di dottorato di ricerca (cfr. Sezione 5.4), in analogia con la distribuzione territoriale delle pubblicazioni (Figura 2), mostra una prevalenza di concentrazione nel Nord Italia (49%); tuttavia, complessivamente la distribuzione dei corsi è buona anche per le altre macro-aree geografiche – cfr. Figura 6.

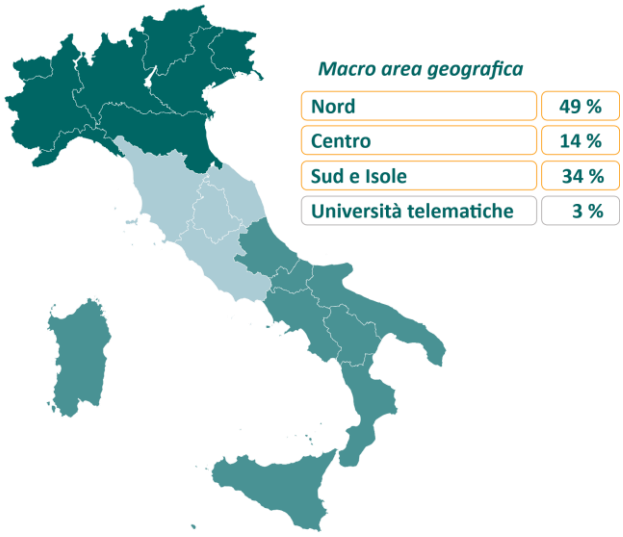


Figura 6: Distribuzione territoriale dei corsi di dottorato inerenti alla cybersicurezza.

Infine, in relazione alle iniziative di valorizzazione della ricerca (cfr. Sezione 6), i risultati principali dell'analisi portano ad osservare come le tematiche di ricerca e innovazione più presenti siano quelle dedicate agli aspetti della società (in particolare, gli aspetti connessi alla formazione) e alla sicurezza delle infrastrutture digitali (con l'ambito hardware preponderante rispetto alle reti di telecomunicazioni). D'altro canto, in relazione alla distribuzione territoriale delle iniziative di valorizzazione sulla cybersicurezza, emerge la prevalenza degli atenei del Nord Italia – cfr. Figura 7.

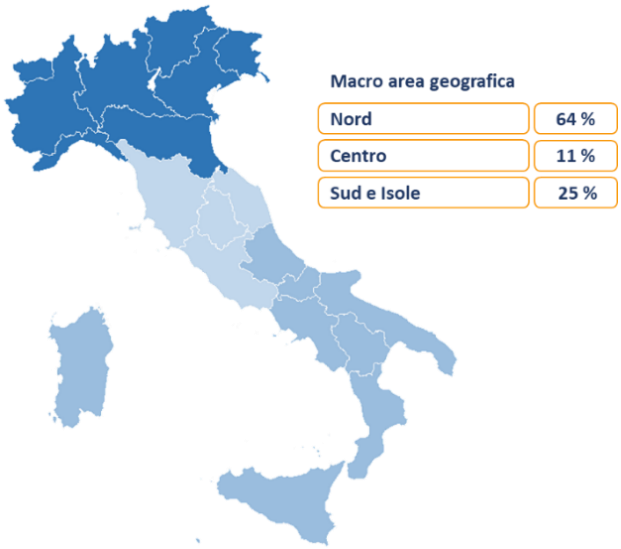


Figura 7: Distribuzione territoriale delle iniziative di valorizzazione inerenti alla cybersicurezza.

Da quanto illustrato in precedenza e dettagliato nelle sezioni successive, questo studio evidenzia le seguenti peculiarità della ricerca nella cybersicurezza in Italia come emergono dai dati conferiti per la VQR 2020-2024, sulla base delle quali è possibile formulare alcune prime considerazioni a supporto delle iniziative di promozione e valorizzazione della ricerca sulla cybersicurezza.

- ***Potenziamento della ricerca sulla cybersicurezza*** – Le pubblicazioni scientifiche relative alle tematiche di cybersicurezza rappresentano meno dell'1% delle pubblicazioni totali conferite ad ANVUR, nell'ambito della VQR 2020-2024. Anche limitando l'analisi delle pubblicazioni scientifiche provenienti dalle aree scientifico-disciplinari maggiormente attive e interessate dalle tematiche di cybersicurezza[1], i contributi relativi alla cybersicurezza rappresentano una quota pari a meno del 4%. Tali risultati mettono in luce la necessità di un potenziamento mirato della ricerca di alto livello in questo settore strategico, al fine di aumentarne l'impatto scientifico e la rilevanza all'interno del sistema nazionale della ricerca.
- ***Tematiche di ricerca in cybersicurezza emerse come carenti*** – La distribuzione delle pubblicazioni rispetto alle aree dell'Agenda di R&I fa emergere come maggiormente carente l'area della sicurezza delle infrastrutture digitali, che, nonostante la numerosità degli argomenti di afferenza, sia in ambito reti di telecomunicazioni sia in ambito hardware, ha circa il 57% di contributi in meno rispetto all'area della gestione delle minacce cibernetiche, che risulta essere l'area maggiormente contribuita. D'altro canto, con riferimento all'ambito della gestione delle minacce cibernetiche, spicca il contributo estremamente limitato relativo alle scienze forensi digitali. Nell'area aspetti della società, gli aspetti umani e quelli formativi sono meno presidiati degli aspetti legali, questi ultimi contribuendo da soli al 46% delle pubblicazioni dell'area. Infine, nel contesto degli aspetti di governo, si rileva l'importanza di sostenere gli argomenti afferenti alla gestione del rischio e alla standardizzazione, soprattutto per consentire di massimizzare gli aspetti di gestione dell'impatto delle tecnologie emergenti.
- ***Andamento della ricerca sulla cybersicurezza relativa ai domini tecnologici prioritari*** – Lo studio ha consentito di analizzare la composizione in termini di tecnologie emergenti e caratterizzare la tendenza temporale delle pubblicazioni ad essi relative. In termini di contributi

[1] Nello specifico, Scienze matematiche e informatiche e Ingegneria industriale e dell'informazione.

nei domini prioritari, le tecnologie quantistiche emergono come in crescita ma da potenziare ulteriormente, contribuendo per meno dell'8% alle pubblicazioni classificate rispetto ai domini tecnologici prioritari. In relazione alle tecnologie quantistiche è altresì rilevante rimarcare il ruolo di primo piano svolto dagli enti pubblici di ricerca per la ricerca di settore. Risulta invece crescere in misura minore rispetto alle tecnologie quantistiche, sia la ricerca sulla cybersicurezza dei sistemi cyber fisici, sia quella sulla cybersicurezza delle reti del futuro. Nello specifico, il ruolo della ricerca *cyber* nel primo ambito è particolarmente importante per fronteggiare le minacce alle infrastrutture e ai servizi critici del Paese. Invece, le reti di prossima generazione rappresentano un insieme di tecnologie di estrema importanza ai fini del rafforzamento dell'autonomia tecnologica nazionale.

- ***Aspetti territoriali della ricerca in cybersicurezza*** – L'analisi territoriale mostra una prevalente concentrazione delle istituzioni di ricerca che contribuiscono alle pubblicazioni in ambito di cybersicurezza nella macro-area settentrionale del Paese. Per quanto riguarda i domini tecnologici prioritari, l'intelligenza artificiale e i sistemi cyber-fisici risultano maggiormente rappresentati dagli atenei statali e non statali del Sud e delle Isole oltre che del Nord Italia, mentre le tecnologie quantistiche sono oggetto di una più intensa attività di ricerca da parte degli atenei della sola macro-area del Nord. Le reti di prossima generazione presentano una distribuzione più equilibrata tra le università sull'intero territorio nazionale. Infine, con riferimento ai corsi di dottorato sulla cybersicurezza, rispetto al totale dei corsi di dottorato offerti, emerge una maggiore concentrazione degli stessi nelle macro-aree geografiche del Nord e Sud e Isole.
- ***Gender gap*** – Il divario di genere presente nelle discipline STEM, tradizionalmente a prevalenza maschile, si conferma nelle analisi relative al dominio della cybersicurezza, con le aree dalla 1 alla 4 dell'Agenda di R&I, prevalentemente contribuite dalle discipline STEM, che presentano percentuali delle ricercatrici che variano da un minimo del 15% (Sicurezza del software e delle piattaforme) ad un massimo del 20% (Sicurezza dei dati e privacy). Invece, sono più alte le percentuali di ricercatrici nelle aree prevalentemente NON STEM, nello specifico aspetti della società (38%) e di governo (34%).
- ***Iniziative di valorizzazione***. Le analisi condotte sulle iniziative di valorizzazione confermano una preponderanza di tali iniziative negli atenei del Nord Italia ed evidenziano una prevalenza di iniziative nell'area aspetti della società, soprattutto in relazione alle iniziative di formazione e nell'area della sicurezza delle infrastrutture digitali. Si osserva, tuttavia, come i risultati facciano riferimento ad un numero limitato di iniziative relative alla cybersicurezza provenienti dalla fonte VQR 2020-2024. Per questo motivo, in questo documento si è avviato un processo di integrazione con altre fonti disponibili che, auspicabilmente, potrebbe proseguire nel corso di sviluppi futuri (cfr. Sezione 7).

3 Quadro di riferimento

In questa sezione è presentato il contesto in cui questo studio si colloca, oltre alla metodologia di analisi dei dati adottata.

3.1 Contesto

Una parte importante della missione istituzionale dell'ACN consiste nella pianificazione e gestione di programmi di promozione e valorizzazione della ricerca sulla cybersicurezza, perseguendo l'obiettivo di potenziare l'autonomia strategica tecnologica nazionale. A supporto di tali attività, l'ACN si avvale dell'*Agenda di Ricerca e Innovazione per la Cybersicurezza*.

Similmente, la missione istituzionale dell'ANVUR include la valutazione della ricerca delle Università e degli Enti di ricerca, con l'obiettivo di assicurare la qualità e incentivare l'eccellenza accademica e scientifica. A tal fine, come precedentemente introdotto, l'ANVUR effettua un esercizio periodico di valutazione, chiamato *Valutazione della Qualità della Ricerca* (VQR).

Nel seguito di questa sezione, i quadri di riferimento delle due Agenzie verranno descritti in dettaglio.

3.1.1 Agenda di ricerca e innovazione per la cybersicurezza

L'ACN, in collaborazione con il Ministero dell'Università e della Ricerca (MUR), ha pubblicato nel 2023 l'Agenda di Ricerca e Innovazione per la Cybersicurezza, un documento strategico che definisce una base di conoscenza condivisa per governare le attività di ricerca nazionali. L'Agenda di R&I, aggiornata nel 2026[2], ha una struttura ad albero in cui sono state identificate:

- 6 aree derivate dall'analisi di iniziative di classificazioni esistenti, che partizionano il dominio di conoscenza della cybersicurezza;
- 18 subaree e 61 argomenti relativi, individuati valutando le priorità italiane ed europee, ma anche di riferimenti rilevanti sul piano internazionale;
- 32 sottoargomenti, che specializzano ulteriormente gli argomenti prioritari, per evidenziare le principali sfide aperte della ricerca e fornire punti focali per l'investigazione futura.

Ai fini di questo rapporto, ci si focalizzerà sulle 6 aree, ovvero

- 1 – Sicurezza dei dati e *privacy*,
- 2 – Gestione delle minacce cibernetiche,
- 3 – Sicurezza del software e delle piattaforme,
- 4 – Sicurezza delle infrastrutture digitali,
- 5 – Aspetti della società,
- 6 – Aspetti di governo

[2] Disponibile al sito https://www.acn.gov.it/portale/agenda-di-ricerca-e-innovazione.

e le relative subaree dell'Agenda, indicate nella Figura 8. Si noti che le prime 4 aree raggruppano le tematiche di ricerca proprie delle discipline scientifico-tecnologiche, c.d. STEM (*Science, Technology, Engineering and Mathematics*), mentre le ultime due aree riguardano principalmente le discipline umanistiche.

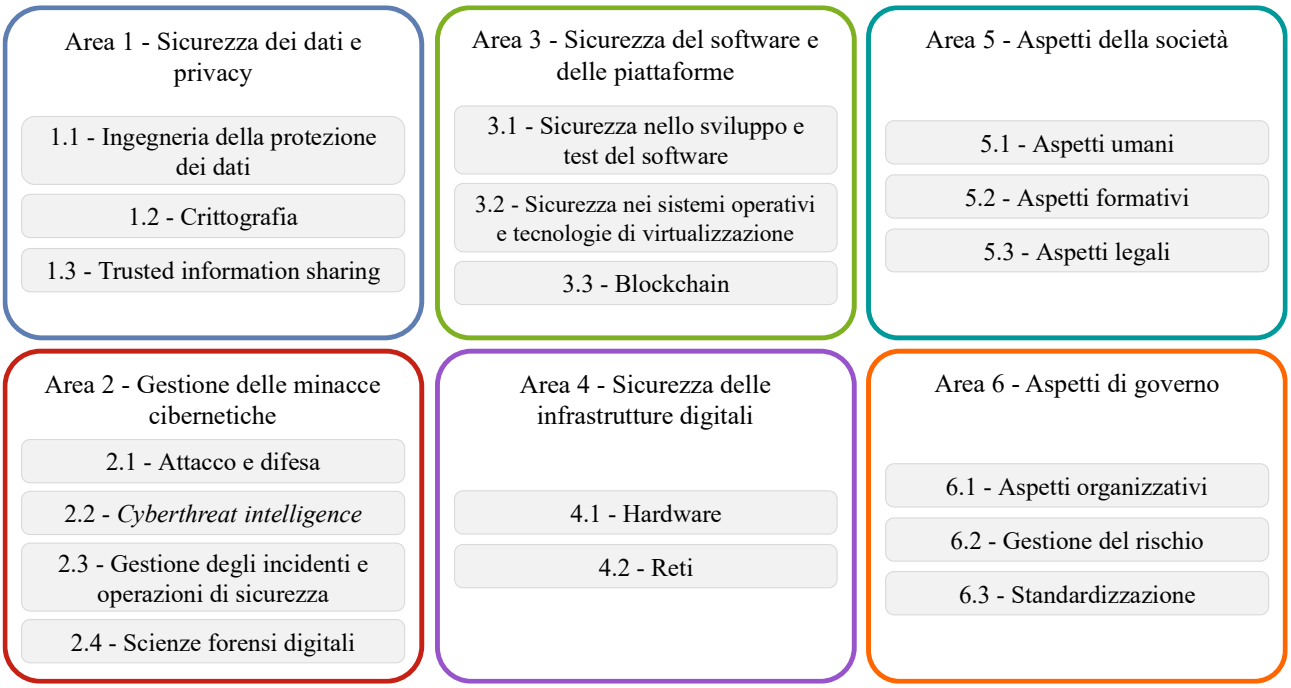


Figura 8: Aree e subaree identificate nell'Agenda di R&I.

Nell'Agenda di R&I è stata, inoltre, identificata una lista di 20 *Emerging and Disruptive Technology* (EDT) rilevanti per lo studio degli argomenti di ricerca sulla cybersicurezza individuati all'interno delle 18 subaree – cfr. Figura 9. Si noti che le EDT considerate sono per la maggior parte attribuibili al contesto dell'ICT e appartengono a diversi livelli di astrazione, spaziando da generici paradigmi a tecniche di dettaglio. L'avanzamento tecnologico sempre più spedito richiede, infatti, un costante aggiornamento sullo stato dell'arte per poterne comprendere i rischi e le opportunità dettati dal loro utilizzo. Per questo motivo, è importante identificare e quindi stimolare sinergie tra esperti delle tecnologie e ricercatori in cybersicurezza, al fine di favorire lo scambio di competenze e specializzare così gli argomenti di ricerca agli aspetti di cybersicurezza della singola tecnologia. A tal fine, nell'Agenda le EDT sono messe in relazione con le subaree, evidenziando come esse contribuiscono ad indirizzare lo studio degli argomenti all'interno di ciascuna subarea.

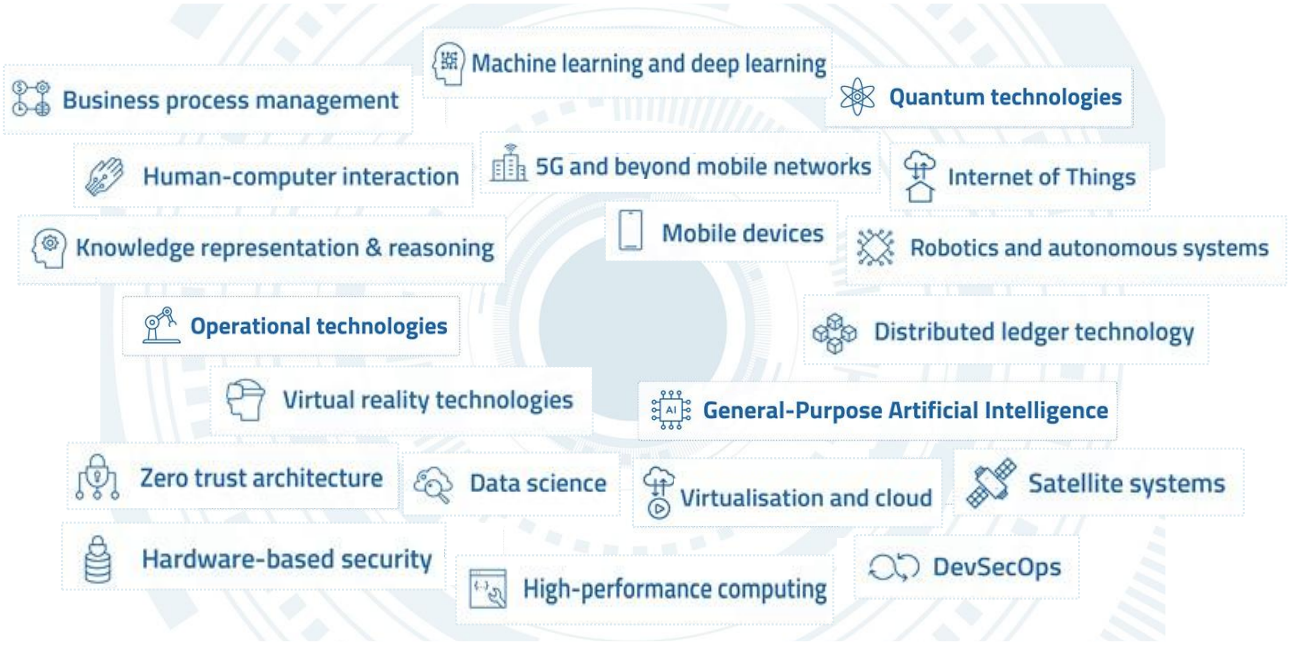


Figura 9: EDT identificate dall'Agenda di R&I.

Ai fini di questo rapporto, non saranno sempre considerate le singole EDT dell'Agenda di R&I, quanto piuttosto quattro *domini tecnologici prioritari*, considerati ad elevato impatto perché caratterizzati da un rapido avanzamento e/o della loro sempre più estesa adozione in ampi settori della popolazione e dell'industria. Tali domini sono:

- le tecnologie per l'intelligenza artificiale (IA) – da intendersi come unione delle EDT *data science*, *machine learning and deep learning*, rappresentazione della conoscenza e *general-purpose artificial intelligence* (GPAI);
- le tecnologie quantistiche (TQ), interamente rappresentate dall'EDT omonima. L'importanza strategica dello sviluppo di tecnologie per il calcolo, la sensoristica e la comunicazione *quantum* è stata recentemente evidenziata dall'elaborazione della Strategia italiana per le TQ[3];
- le tecnologie per i sistemi *cyber*-fisici (*cyber-physical systems*, CPS) – da intendersi come unione di *operational technologies* (OT), Internet delle cose (*Internet of things*, IoT) e robotica e sistemi autonomi. A questo dominio si rifanno le tecnologie per i sistemi di controllo industriale (*industrial control system*, ICS) e, più in generale, delle infrastrutture critiche in diversi settori quali, ad esempio, trasporti ed energia;
- le tecnologie per reti *wireless* di prossima generazione (*next-generation wireless networks*, NGWN) – da intendersi come unione di reti mobili di quinta generazione (5G) e successive, dispositivi mobili e sistemi satellitari.

3.1.2 Valutazione della qualità della ricerca

Rivolta ad università, enti pubblici di ricerca vigilati dal MUR e, su base volontaria, ad istituzioni diverse che svolgono attività di ricerca, la VQR ha l'obiettivo di analizzare la qualità dei risultati della ricerca scientifica realizzati in un determinato periodo temporale. Inoltre, i risultati della VQR vengono utilizzati per la distribuzione della quota premiale del Fondo di Finanziamento Ordinario delle università. ANVUR ha il compito di definire le linee guida e i criteri di valutazione, organizzare le procedure operative,

[3] Disponibile al sito https://www.mur.gov.it/it/strategia-italiana-le-tecnologie-quantistiche.

gestire la raccolta dei dati, coordinare i Gruppi di Esperti Valutatori (GEV), elaborare e diffondere i risultati finali.

Il primo esercizio di valutazione della ricerca venne condotto dal Comitato di Indirizzo per la Valutazione della Ricerca (CIVR) nel 2007 e ha riguardato la ricerca scientifica svolta nel periodo 2001-2003. Successivamente ANVUR ha effettuato le VQR relative al periodo 2004-2010 (svolta nel 2011-2013), 2011-2014 (svolta nel 2015-2017), 2015-2019 (svolta nel 2020-2022). Il D.M. n. 998 del 1° agosto 2023 ha avviato la VQR relativa al periodo 2020-2024, che si concluderà a giugno 2026. La VQR persegue molteplici obiettivi, come descritto all'art. 2 del Bando VQR 2020-2024, di cui riportiamo alcune finalità:

- promuovere la qualità della ricerca italiana, stimolando i ricercatori alla partecipazione attiva alla ricerca,
- incentivare il miglioramento della qualità delle scelte per il reclutamento e le progressioni di carriera,
- incrementare la visibilità internazionale, nonché la partecipazione a progetti internazionali,
- incrementare le attività di valorizzazione delle conoscenze,
- incentivare le azioni di trasferimento tecnologico,
- valorizzare le infrastrutture di ricerca,
- promuovere il miglioramento della qualità della formazione dottorale,
- incrementare le collaborazioni tra il sistema della ricerca e le imprese,
- promuovere l'accessibilità dei dati e le pubblicazioni in modalità di accesso aperto.

Nella VQR relativa al periodo 2020-2024 sono oggetto di valutazione:

- i prodotti della ricerca scientifica,
- le attività di valorizzazione delle conoscenze (c.d. casi di studio),
- le infrastrutture di ricerca,
- l'entità finanziaria dei progetti internazionali ottenuti su base competitiva tramite una revisione tra pari.

I principali prodotti della ricerca sono gli articoli pubblicati su riviste scientifiche internazionali indicizzate nelle principali banche dati (Web of Science, Scopus). I prodotti valutabili includono anche monografie, capitoli di libri, edizioni critiche di testi, contributi in atti di convegno, curatele, brevetti, opere artistiche, progetti architettonici, software e banche dati originali. Per ciascuna Istituzione viene valutata una selezione di prodotti della ricerca, in numero commisurato alle dimensioni dell'Istituzione (2,5 volte il numero dei ricercatori in servizio).

La valorizzazione delle conoscenze include, invece, le attività con cui le Istituzioni entrano in contatto con la società, interagendo attraverso diverse iniziative. Precisamente, il D.M. 998/2023, art. 1, comma 3, lettera b, specifica che per "valorizzazione delle conoscenze" si intende il processo con cui si crea valore economico e/o sociale a partire dalle conoscenze risultanti dall'attività di ricerca, collegando aree e settori diversi e trasformando i dati, le competenze tecniche e i risultati della ricerca in prodotti, servizi, soluzioni e politiche sostenibili basate sulla conoscenza e che portano vantaggio alla società. La VQR 2020-2024 prevede che la valorizzazione delle conoscenze sia suddivisa nelle seguenti cinque tematiche, ciascuna delle quali è stata ulteriormente declinata in cinque campi di azione: i) trasferimento tecnologico, produzione, gestione di beni pubblici, ii) *public engagement*, iii) scienze della vita e salute, iv) sostenibilità ambientale, v) inclusione e contrasto alle diseguaglianze, con particolare riferimento agli obiettivi dell'Agenda ONU 2030.

Per ciascuna Università è consentito sottoporre un caso di studio ogni 100 ricercatori in servizio, mentre per gli EPR e le Istituzioni volontarie tale limite si abbassa a 50.

Inoltre, i soli Enti pubblici di ricerca (EPR) vigilati dal MUR e le Istituzioni volontarie possono presentare alla valutazione una infrastruttura di ricerca. Si tratta di strutture, anche distribuite, localizzate sul territorio dei paesi dell'Unione Europea (UE) (incluse quelle su territorio italiano), dell'Associazione europea di libero scambio (*European free trade association*, EFTA) e del Regno Unito, caratterizzate da apertura all'utilizzo da parte della comunità scientifica e di altri utenti, ai fini della conduzione di ricerche di alta qualità.

Infine, alle Istituzioni è stata richiesta la presentazione di progetti assegnati da enti di natura pubblica o privata non nazionali o locali sulla base di una selezione competitiva internazionale, tramite revisione tra pari con un ammontare minimo di finanziamento per l'Istituzione conferente pari o superiore a 50.000 Euro.

Al fine di valutare quanto conferito dalle istituzioni di ricerca, nel seguito anche IdR, in ciascuna delle precedenti categorie, vengono costituiti, per ciascuna area disciplinare del Consiglio Universitario Nazionale (CUN), uno o più Gruppi di Esperti Valutatori (GEV) – cfr. Tabella 1. Ogni GEV è composto da ricercatori di riconosciuto prestigio nazionale e internazionale selezionati in base alla competenza scientifica, all'esperienza nella valutazione della ricerca e alla reputazione accademica.

Tabella 1: Corrispondenza tra GEV e aree CUN.

ID GEV	GEV	ID Area CUN corrispondente	Area CUN corrispondente
1	Scienze matematiche e informatiche	1	Scienze matematiche e informatiche
2	Scienze fisiche	2	Scienze fisiche
3	Scienze chimiche	3	Scienze chimiche
4	Scienze della Terra	4	Scienze della Terra
5	Scienze biologiche	5	Scienze biologiche
6	Scienze mediche	6	Scienze mediche
7	Scienze agrarie e veterinarie	7	Scienze agrarie e veterinarie
8a	Architettura	8	Ingegneria civile ed architettura
8b	Ingegneria civile	8	Ingegneria civile ed architettura
9	Ingegneria industriale e dell'informazione	9	Ingegneria industriale e dell'informazione
10	Scienze dell'antichità, filologico-letterarie e storico-artistiche	10	Scienze dell'antichità, filologico-letterarie e storico-artistiche
11a	Scienze storiche, filosofiche e pedagogiche	11	Scienze storiche, filosofiche, pedagogiche e psicologiche
11b	Scienze psicologiche	11	Scienze storiche, filosofiche, pedagogiche e psicologiche
12	Scienze giuridiche	12	Scienze giuridiche
13a	Scienze economiche e statistiche	13	Scienze economiche e statistiche
13b	Scienze economico-aziendali	13	Scienze economiche e statistiche
14	Scienze politiche e sociali	14	Scienze politiche e sociali

La valutazione considera sia la dimensione quantitativa (quanti prodotti vengono conferiti da ciascuna istituzione) sia la dimensione qualitativa (ovvero se i prodotti sono eccezionali, eccellenti, standard, sufficienti, scarsi o non accettabili). I membri dei GEV hanno il compito di valutare i prodotti della ricerca tramite revisione tra pari; laddove appropriato, la peer review può essere supportata dall'eventuale utilizzo di indicatori bibliometrici (impatto della rivista e numero di citazioni ricevute). È opportuno sottolineare che gli indicatori citazionali non possono sostituirsi ad un'accurata valutazione di merito

del prodotto della ricerca. La valutazione di prodotti in aree specifiche o per i quali siano necessarie competenze altamente specializzate può coinvolgere anche revisori esterni, italiani o stranieri.

Ogni prodotto o caso di studio conferito da ciascuna istituzione viene classificato dai GEV in base ai seguenti tre criteri: originalità, metodologia e impatto. Per i casi di studio conferiti nell'ambito delle attività di valorizzazione delle conoscenze, i criteri sono quattro, e precisamente:

a) dimensione sociale, economica e culturale dell'impatto, considerando la capacità di valorizzare le conoscenze anche collegando aree e settori diversi;
b) rilevanza rispetto al contesto di riferimento;
c) valore aggiunto per i beneficiari;
d) contributo scientifico, organizzativo e/o gestionale della struttura proponente.

Sulla base di tali criteri, i prodotti o i casi di studio vengono assegnati ad una delle seguenti categorie di merito: eccezionale, eccellente, standard, sufficiente oppure di scarsa rilevanza o non accettabile.

3.2 Metodologia di analisi

Questo rapporto si propone di analizzare, nell'ambito dei temi di ricerca e innovazione (R&I) d'interesse per la cybersicurezza:

- le pubblicazioni scientifiche conferite;
- le iniziative di valorizzazione della ricerca;
- i ricercatori e le Istituzioni di Ricerca (IdR).

3.2.1 Pubblicazioni scientifiche conferite

L'obiettivo dell'analisi delle pubblicazioni scientifiche inerenti alla cybersicurezza è individuare su quali tematiche di R&I si concentra la produzione scientifica. Ai fini di questo studio, sono state, pertanto, analizzate le circa 160000 pubblicazioni conferite per la VQR 2020-2024, le quali rappresentano la quasi totalità dei prodotti della ricerca raccolti, ovvero articoli su rivista, monografie, contributi in volume (capitoli di libri o saggi) e contributi in atti di convegno – cfr. Sezione 3.1.2. Tali pubblicazioni, pur non rappresentando la totalità della ricerca pubblica italiana sul periodo di riferimento, sono utili ai fini di una prima analisi della ricerca poiché provengono da tutte le IdR italiane, nonché da tutte le aree disciplinari, oltre a coprire un arco temporale di 5 anni. Con riferimento alle aree disciplinari, si ricorda che, ai sensi del D.M. n. 639 del 02/05/2024, le aree CUN sono suddivise in Gruppi Scientifico-Disciplinari (GSD), i quali a loro volta sono articolati in Settori Scientifico-Disciplinari (SSD), raffinando ulteriormente la granularità delle tematiche trattate all'interno dell'area.

Si ricorda, inoltre, che, come riportato dal Bando VQR 2020-2024 (Decreto n. 8 del 31/10/2023), le pubblicazioni sono valutate sulla base dei seguenti criteri di qualità:

a) *originalità*, da intendersi come la capacità del prodotto di introdurre un nuovo modo di pensare e/o interpretare o nuovi metodi in relazione all'oggetto della ricerca, anche introducendo metodi sino a quel momento propri di altre discipline;
b) *metodologia*, da intendersi come la capacità del prodotto di presentare in modo chiaro gli obiettivi della ricerca e il loro valore scientifico, la letteratura utilizzata e i risultati ottenuti, favorendo altresì, ove applicabile, la riproducibilità dei risultati, la trasparenza rispetto a metodi e procedure adottate e l'accesso ai dati utilizzati, nella logica di valorizzare l'intero processo che ha portato alla realizzazione del prodotto della ricerca;

c) *impatto*, da intendersi come la capacità del prodotto di generare, nel breve, medio o lungo periodo, un effetto o beneficio per la comunità scientifica nazionale e internazionale, e/o sul contesto economico e sociale.

Le pubblicazioni considerate dal presente studio rappresentano *le pubblicazioni di maggiore qualità* selezionate ai fini della VQR dalle Istituzioni conferenti, ovvero con l'obiettivo di massimizzare la valutazione rispetto alle definizioni e ai criteri sopra esposti.

3.2.2 Iniziative di valorizzazione della ricerca

L'obiettivo dell'analisi delle iniziative di valorizzazione della ricerca è ricostruire una fotografia il più possibile fedele delle attività prossime al trasferimento tecnologico, valutando in che misura la ricerca italiana in cybersicurezza sia in grado di tradurre risultati scientifici in soluzioni utilizzabili, attraverso strumenti di valorizzazione della proprietà industriale e intellettuale (ad esempio brevetti, software, licenze, spin-off, contratti con imprese). Questa dimensione è cruciale per due ragioni. Da un lato, consente di comprendere quanto l'ecosistema nazionale sia "pronto" a sostenere una filiera dell'innovazione completa, dalla ricerca di frontiera fino all'adozione industriale. Dall'altro, è un elemento direttamente connesso agli obiettivi di autonomia strategica: mettere a disposizione ricerca orientata all'innovazione significa ridurre dipendenze tecnologiche, rafforzare capacità nazionali ed europee, e aumentare la resilienza del sistema-Paese rispetto a minacce e vulnerabilità. In questa prospettiva, la valorizzazione non è un esito accessorio, ma un moltiplicatore di impatto che trasforma conoscenza in capacità, prodotti e servizi di cybersicurezza.

Ai fini di questo rapporto, le iniziative di valorizzazione della ricerca analizzate consistono primariamente nei casi di studio raccolti dalla VQR 2020-2024 – cfr. Sezione 3.1.2. D'altro canto, l'esercizio basato sui risultati VQR è stato esteso con un primo esempio di approfondimento, integrando l'analisi con una ulteriore banca dati *open source*, per ampliare la copertura informativa e migliorare la lettura complessiva delle traiettorie di trasferimento tecnologico. Tale banca dati è *KnowledgeShare*[4], la più grande piattaforma a livello nazionale dedicata alla valorizzazione della ricerca pubblica. Il portale è nato con l'obiettivo di rendere disponibili in modo chiaro e comprensibile informazioni relative a progetti che rappresentano l'eccellenza del *know-how* scientifico delle Università italiane e dei Centri di Ricerca, al fine di risolvere le principali criticità legate al processo di trasferimento tecnologico e di fornire uno strumento consolidato per canalizzare e semplificare le interazioni tra mondo della ricerca, quello delle imprese e degli investitori.

3.2.3 Ricercatori e istituzioni di ricerca

L'obiettivo dell'analisi di ricercatori e IdR è di caratterizzare chi fa e dove si fa R&I su tematiche di cybersicurezza a livello nazionale. Nello specifico, ai fini di questo rapporto, l'analisi dei dati relativi alle pubblicazioni scientifiche di qualità e alle iniziative di valorizzazione delle conoscenze consentono di derivare informazioni importanti sui ricercatori e sulle IdR attive sul territorio nazionale; tali informazioni possono essere integrate da una panoramica dell'offerta di corsi di dottorato che trattano argomenti riconducibili alle Aree e ai domini tecnologici prioritari per la cybersicurezza. Com'è noto, infatti, i corsi di dottorato fanno parte del 3° ciclo della Formazione Superiore e hanno l'obiettivo di preparare alla metodologia per la ricerca scientifica avanzata. I corsi di dottorato di ricerca sono erogati solamente dagli atenei, statali e non, a valle del processo di accreditamento gestito dal MUR e dall'ANVUR, ai sensi di quanto previsto dal D.M. n. 226 del 14 dicembre 2021. La nuova normativa ha

[4] Disponibile al sito https://www.knowledge-share.eu/it.

infatti introdotto rilevanti innovazioni, prevedendo la possibilità di istituire corsi di dottorato svolti in organica collaborazione con le imprese (i cosiddetti dottorati industriali), che si affiancano ai più tradizionali dottorati svolti con un co-finanziamento industriale (dottorati in collaborazione con le imprese). Il D.M. 226/2021 ha anche introdotto per la prima volta i dottorati di interesse nazionale, svolti in modo associato da università e imprese e caratterizzati dalla erogazione di almeno 30 borse di studio, focalizzate su temi di interesse strategico nazionale.

Ai fini di questo rapporto, sono stati presi in considerazione i 1.241 corsi di dottorato accreditati per il XLI ciclo, disponibili in una banca dati del consorzio interuniversitario CINECA la quale contiene informazioni relative al progetto formativo e agli obiettivi di ciascun corso.

3.2.4 Fasi dell'analisi

Riassumendo, questo rapporto considera le unità di analisi e le relative fonti riportate in Tabella 2.
L'analisi dei dati è stata effettuata sulle diverse fonti in due fasi:

1. filtraggio dei dati tramite parole chiave al fine di identificarne l'attinenza all'ambito della cybersicurezza. Nello specifico, sono stati definiti due insiemi di parole chiave a partire dalle tematiche trattate dalle subaree (cfr. Figura 10) e dalle EDT dell'Agenda di R&I (cfr. Figura 11). Le parole chiave sono state definite sia in lingua italiana sia in lingua inglese, al fine di poterle utilizzare in maniera appropriata sulla base della lingua delle singole pubblicazioni;
2. elaborazione di dettaglio delle singole unità di analisi, al fine di estrarre le statistiche presentate nelle prossime sezioni.

Tabella 2: Lista dei dati considerati per il presente studio con relative fonti.

Unità di analisi	Fonti
Pubblicazioni scientifiche	VQR
Ricercatori e IdR	VQR, CINECA- Corsi di Dottorato XLI Ciclo
Iniziative di valorizzazione della ricerca	VQR, *KnowledgeShare*

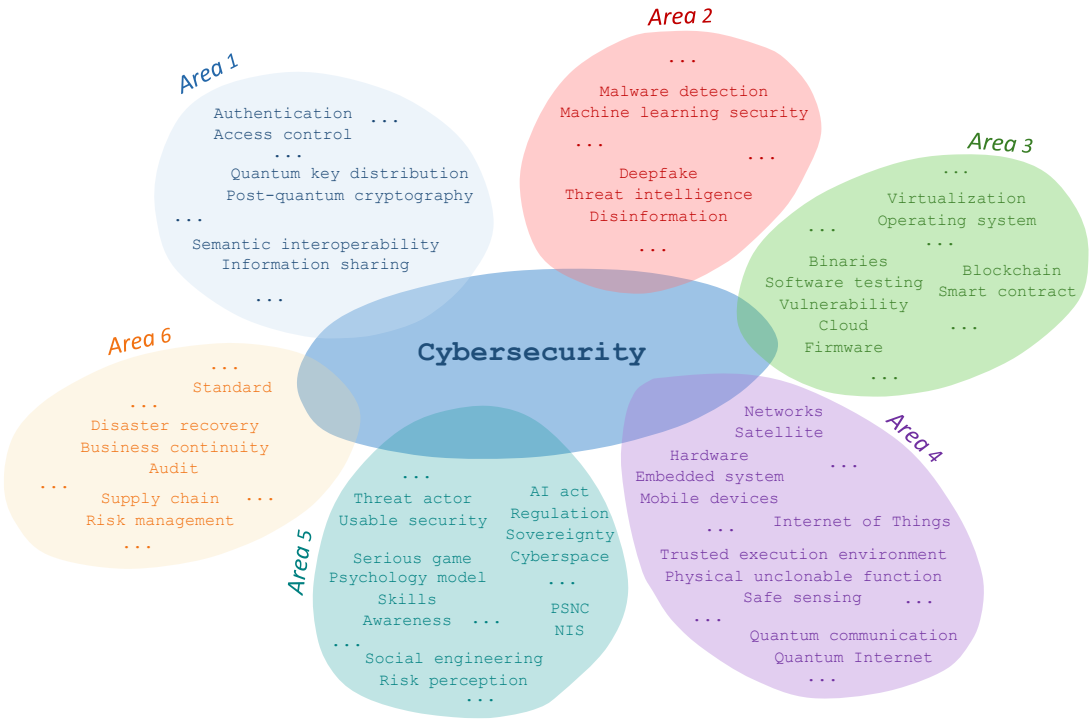


Figura 10: Esempi di parole chiave in lingua inglese utilizzate per individuare le pubblicazioni e le iniziative di valorizzazione inerenti alle diverse aree dell'Agenda di R&I.

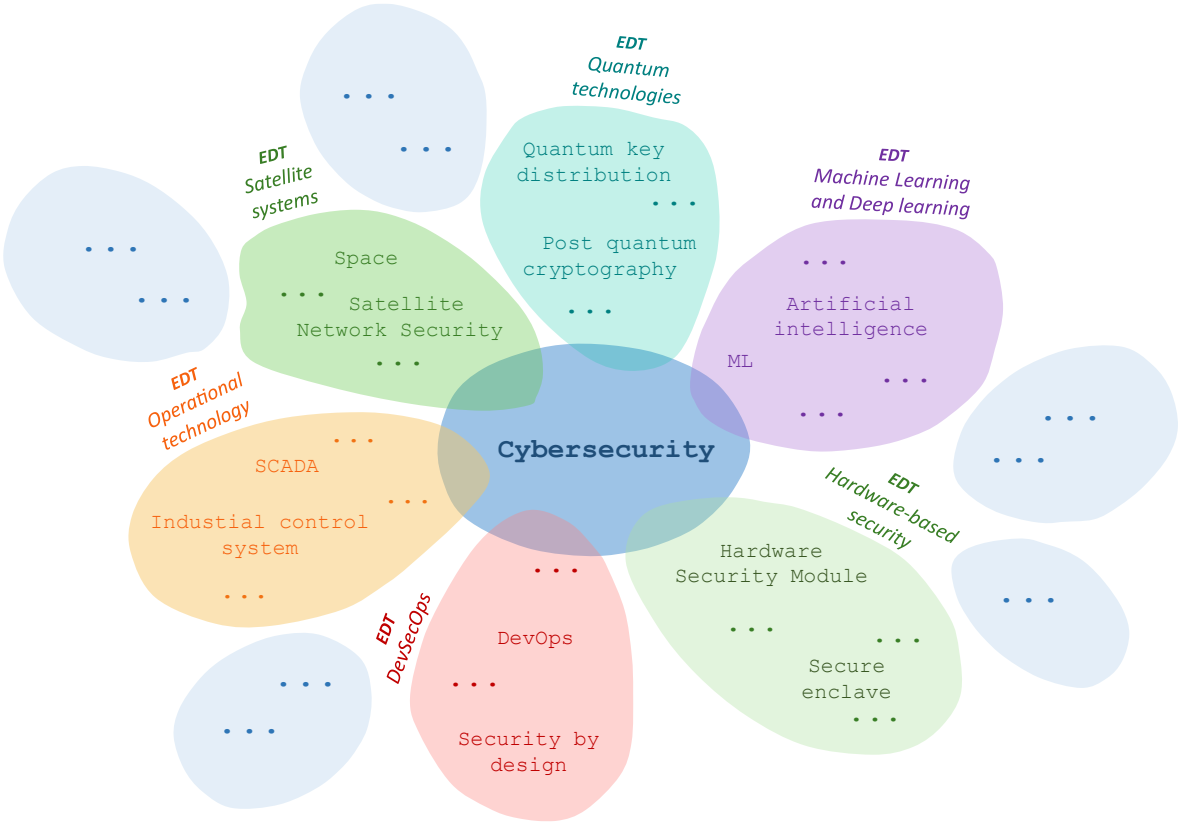


Figura 11: Esempi di parole chiave in lingua inglese utilizzate per individuare le pubblicazioni e le iniziative di valorizzazione inerenti alle diverse EDT dell'Agenda di R&I.

In relazione all'analisi delle pubblicazioni scientifiche conferite, è utile far notare che, per come è strutturato l'esercizio della VQR, una determinata pubblicazione, cui è assegnato un identificativo unico, può essere presente in più GEV o più volte in un dato GEV – ciò a seconda di quanti co-autori hanno presentato lo specifico prodotto ai fini della valutazione. Per questo motivo, l'analisi delle pubblicazioni è stata effettuata secondo la procedura seguente:

1. il filtraggio dei prodotti della ricerca è stato eseguito sulla lista dei prodotti unici, senza considerare i duplicati, di modo da selezionare tutti i prodotti inerenti alla cybersicurezza. Per tali prodotti, è stato possibile produrre statistiche sull'appartenenza alle subaree e alle EDT dell'Agenda, a prescindere dal GEV di origine;
2. grazie ai codici identificativi univoci dei prodotti selezionati, sono stati ricostruiti eventuali conferimenti multipli dello stesso prodotto in più GEV o all'interno di un certo GEV;
3. sulla base della mappa completa dei conferimenti (ovvero, che include i duplicati), sono state effettuate le analisi riportate in seguito.

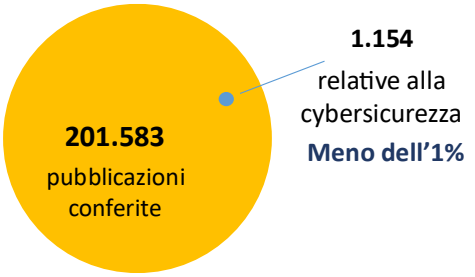
Inoltre, in relazione ai corsi di dottorato analizzati nell'ambito dei ricercatori e delle IdR, si osserva che il filtraggio è stato effettuato sulla base della denominazione del corso, della descrizione del progetto e degli obiettivi del corso.

4 Analisi delle pubblicazioni conferite

In questa sezione sono presentate le analisi delle pubblicazioni raccolte tramite la VQR 2020-2024 in relazione alle tematiche di R&I sulla cybersicurezza.

4.1 Relazione tra tematiche di R&I e settori scientifico-disciplinari

Il primo risultato che riguarda l'analisi delle pubblicazioni è che meno dell'1% del totale è relativo a tematiche di R&I sulla cybersicurezza. Ciò premesso, è utile, anzitutto, considerare la classificazione delle pubblicazioni pertinenti lungo la dimensione delle 6 aree dell'Agenda di R&I per avere una immediata rappresentazione di quanto sono trattati i temi di cybersicurezza – cfr. Figura 12.



Le Aree 1, 2, e 3 sono quelle che emergono come le aree di maggiore produzione della ricerca di qualità in cybersicurezza, con l'Area 2 – Gestione delle minacce cibernetiche che rappresenta l'area con più contributi, come peraltro ragionevole dato il ruolo centrale che i temi costituenti la stessa rivestono nel settore della cybersicurezza. Tuttavia, l'Area 4 – Sicurezza delle infrastrutture digitali ha invece meno

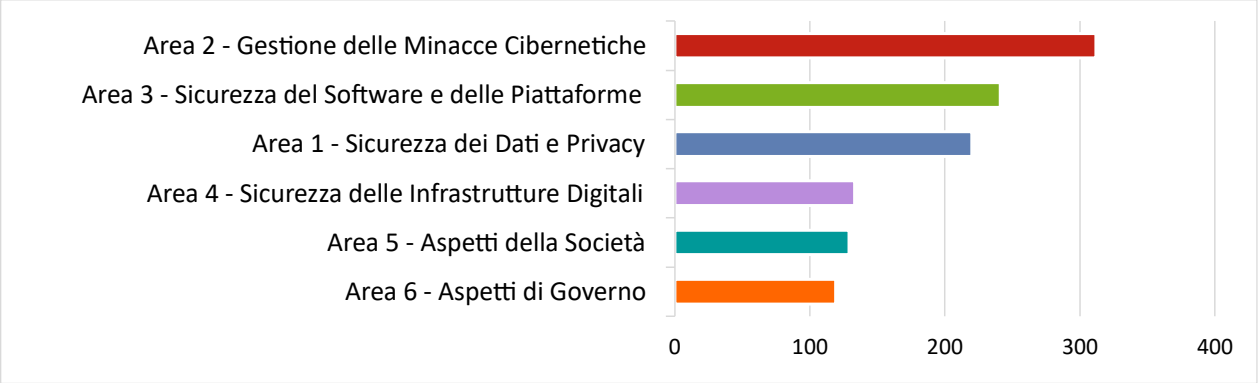


Figura 12: Statistiche delle pubblicazioni pertinenti la sicurezza cibernetica, classificate per Area.

della metà dei contributi dell'Area 2, nonostante la rilevanza dell'area e l'estensione della stessa in termini di temi, visto che l'Area 4 include sia la Subarea 4.1 – Hardware, sia la Subarea 4.2 – Reti. Le Aree 5 e 6, come aree prevalentemente non STEM, presentano invece un numero più limitato di contributi. D'altro canto, è utile valutare la pertinenza dei GEV alle tematiche di interesse per la cybersicurezza, basandosi sul numero delle pubblicazioni risultanti dal filtraggio di tutte le pubblicazioni valutate dai diversi GEV secondo le aree e le EDT dell'Agenda. Dalla Tabella 3, la quale riporta le percentuali più significative di pubblicazioni inerenti alla cybersicurezza rilevate tra tutte quelle conferite per i diversi GEV, emergono, come aree scientifico-disciplinari più rappresentate, il GEV1 – Scienze matematiche e informatiche, il GEV2 – Scienze fisiche, il GEV9 – Ingegneria industriale e dell'informazione e il GEV12 – Scienze giuridiche.

Tabella 3: Distribuzione delle pubblicazioni pertinenti sui GEV più rappresentati.

ID GEV	Denominazione GEV	Percentuale su base Aree	Percentuale su base EDT
1	Scienze matematiche e informatiche	26,74%	25,15%
2	Scienze fisiche	5,48%	7,22%
9	Ingegneria industriale e dell'informazione	56,42%	61,24%
12	Scienze giuridiche	6,15%	4,12%

Si noti che, se si rapporta il totale delle pubblicazioni inerenti alla cybersicurezza al totale delle pubblicazioni conferite nei soli due GEV più pertinenti, ovvero GEV9 e GEV1, si osserva che la percentuale di prodotti inerenti a tematiche di ricerca sulla cybersicurezza aumenta, ma di misura, passando da meno dell'1% a meno del 4%.

Nel seguito di questa sezione, verranno analizzate nel dettaglio le 6 aree di R&I sulla cybersicurezza (cfr. Sezione 4.2) e i quattro domini tecnologici prioritari, ovvero IA, QT, CPS e NGWN (cfr. Sezione 4.3).

4.2 Analisi relativa alle aree dell'Agenda di R&I

Da un punto di vista generale, l'analisi dei prodotti sulla base delle aree dell'Agenda di R&I dimostra che la tipologia di pubblicazione più frequente in tutte le aree è l'articolo in rivista (in un intervallo compreso tra il 93% in Area 3 – Sicurezza del software e delle piattaforme e l'81% in Area 5 – Aspetti della società). A seguire, si trovano tipicamente i contributi in atti di convegno, compresi tra il 5% in Area 3 e il 7% in Area 4 – Sicurezza delle infrastrutture digitali. Fa eccezione l'Area 5, che dopo gli articoli su rivista presenta, nel 9% dei casi, monografie o trattati scientifici. Seguono, infine, in tutte le aree, i contributi in volume (capitoli o saggi).

Dall'analisi dei dati si evince, inoltre, come tali pubblicazioni siano rese a disposizione ad accesso aperto (*open access*) nella maggior parte dei casi in tutte le aree (in un intervallo compreso tra il 92% in Area 1 – Sicurezza dei dati e privacy e il 57% in Area 6 – Aspetti di governo). A seguire, emergono le seguenti casistiche per le quali la pubblicazione non è disponibile in *open access* per una delle seguenti cause: i) i diritti sono stati ceduti all'Editore, ii) è stata invocata la protezione dei risultati ex D.Lgs. 30/2005 (Codice della proprietà industriale) e iii) è stato posto un embargo oltre il 30/06/2026[5].

Di seguito, sarà presentata l'analisi di dettaglio relativa alle 6 aree dell'Agenda di R&I.

4.2.1 Area 1 – Sicurezza dei dati e privacy

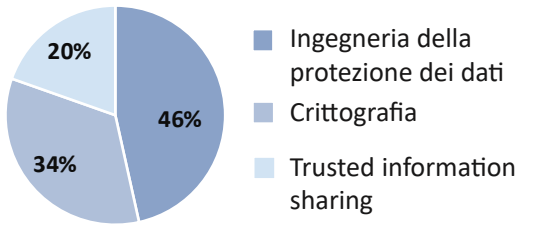


Figura 13: Statistiche per subaree dell'Area 1.

Dalla Figura 13 si nota che la distribuzione delle pubblicazioni conferite in Area 1 nelle subaree costitutive della stessa è abbastanza equilibrata: la Subarea 1.1 – Ingegneria della protezione dei dati, che raggruppa le tecniche emergenti di *privacy-preserving data management* risulta essere quella con il maggior numero di pubblicazioni, seguita subito dalla Subarea

[5] Si ricorda che la lista delle pubblicazioni conferite per la VQR 2020-2024 sarà pubblicata dall'ANVUR dopo il 30/06/2026.

1.2 – Crittografia e, infine, dalla Subarea 1.3 – *Trusted information sharing*, che comprende i temi di cybersicurezza più direttamente legati alla distribuzione geografica dei dati.

Analogamente, è interessante visualizzare lo spaccato degli SSD su cui le pubblicazioni selezionate come inerenti all'Area 1 sono state valutate dai rispettivi GEV. Come si può notare nella Figura 14, le tematiche di interesse per l'Area 1, riguardanti le *privacy-enhancing technology* e le sfide più attuali nell'ambito della crittografia e della condivisione sicura delle informazioni, sono trattate principalmente dagli SSD in ambito ingegneria informatica, scienze informatiche, fisica e ingegneria delle telecomunicazioni.

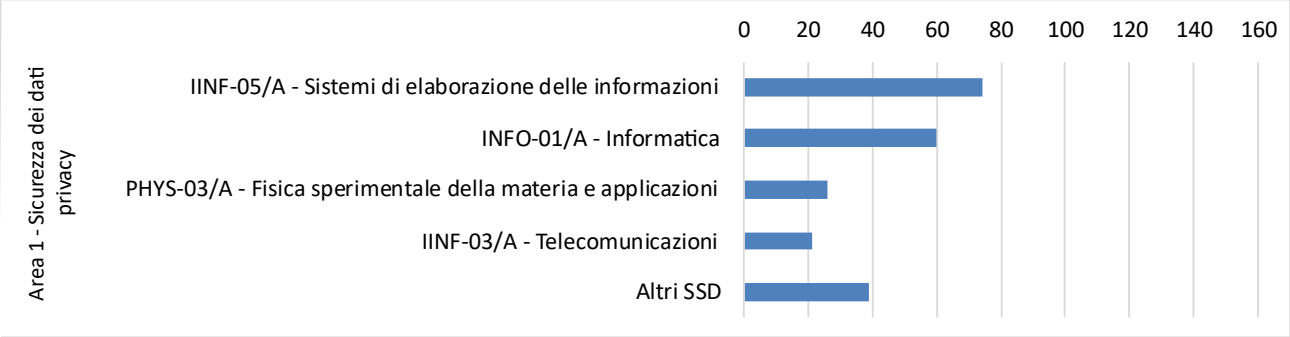


Figura 14: SSD valutazione per Area 1.

Segue, infine, la lista delle 10 riviste più utilizzate per le pubblicazioni selezionate per l'Area 1:

1. *Future Generation Computer System*;
2. *IEEE Access*;
3. *Computer Networks*;
4. *IEEE Internet of Things Journal*;
5. *IEEE Transactions on Dependable and Secure Computing*;
6. *Journal of Network and Computer Applications*;
7. *Nature Communications*;
8. *Sensors*;
9. *Information Sciences*;
10. *IEEE Transactions on Industrial Informatics*.

4.2.2 Area 2 – Gestione delle minacce cibernetiche

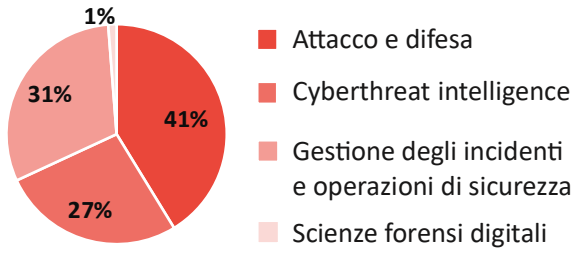


Figura 15: Statistiche per subaree dell'Area 2.

Dalle statistiche raffigurate in Figura 15, la Subarea 2.1 – Attacco e difesa risulta essere quella a cui è riferito il maggior numero di articoli, come prevedibile data la centralità degli argomenti di afferenza, seguita dalla Subarea 2.3 – Gestione degli incidenti e delle operazioni di sicurezza, e dalla Subarea 2.2 – *Cyberthreat intelligence*. Delle 4 subaree componenti l'Area 2, risulta spiccatamente poco contribuita la Subarea 2.4 – Scienze forensi digitali.

La Figura 16 mostra, invece, come le pubblicazioni inerenti all'Area 2 si distribuiscono su svariati SSD. Si può apprezzare, infatti, come i contributi alla ricerca su tecniche di attacco e difesa, *cyberthreat intelligence* e gestione degli incidenti e delle operazioni di sicurezza provengano da diversi settori dell'Ingegneria industriale e dell'informazione (a partire dai sistemi di elaborazione delle informazioni

e delle telecomunicazioni, fino ai sistemi elettrici per l'energia e all'automatica), ma anche dalle Scienze matematiche e informatiche (con la peculiare presenza dell'SSD relativo all'Algebra), dalle Scienze fisiche e da quelle giuridiche.

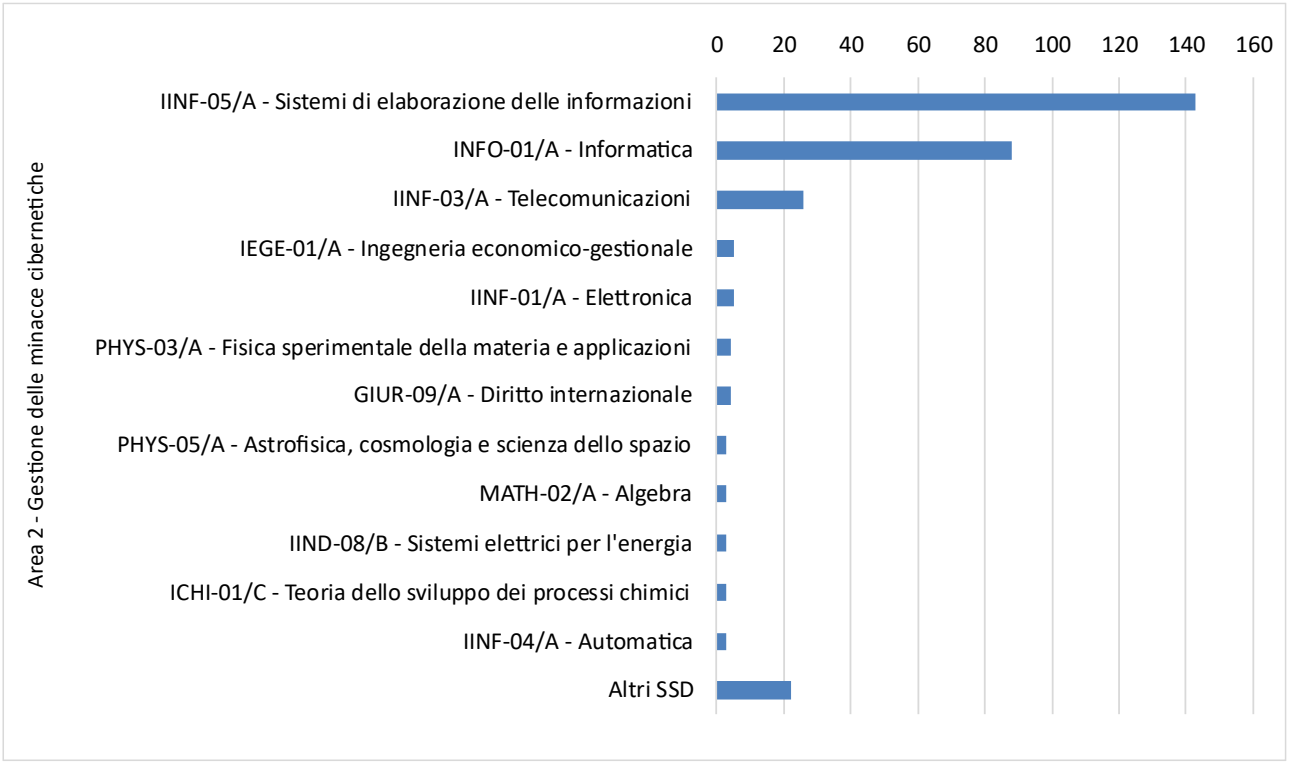


Figura 16: SSD valutazione per Area 2.

Infine, le 10 riviste principali su cui sono stati pubblicati i contributi conferiti identificati come inerenti all'Area 2 sono:

1. *Computers & Security*;
2. *IEEE Access*;
3. *Sensors*;
4. *Computer Networks*;
5. *Journal of Information Security and Applications*;
6. *IEEE Transactions on Information Forensics and Security*;
7. *Expert Systems with Applications*;
8. *IEEE Transactions on Networks and Service Management*;
9. *IEEE Transactions on Dependable and Secure Computing*;
10. *Future Generation Computer System*.

4.2.3 *Area 3 – Sicurezza del software e delle piattaforme*

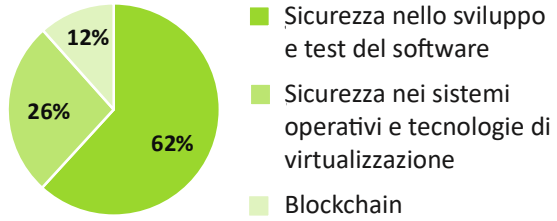


Figura 17: Statistiche per subaree dell'Area 3.

Nell'Area 3, emerge la percentuale abbastanza limitata, solo il 26%, delle pubblicazioni afferenti alla Subarea 3.2 – Sicurezza dei Sistemi operativi e delle tecnologie di virtualizzazione – cfr. Figura 17.

Come si può evincere dalla Figura 18, le statistiche sugli SSD su cui sono state valutate le pubblicazioni rilevate come attinenti all'Area 3, la quale si focalizza sullo sviluppo e test sicuro del software e sulla sicurezza dei sistemi operativi, delle tecnologie di virtualizzazione e delle blockchain, sono simili a quelle per l'Area 2 – cfr. Sezione 4.2.2. Si noti l'aggiunta di Statistica tra gli SSD più frequenti.

Infine, la lista delle 10 riviste più utilizzate per pubblicazioni su tematiche di Area 3 è:

1. *Future Generation Computer Systems*;
2. *Computers & Security*;
3. *IEEE Access*;
4. *Sensors*;
5. *IEEE Internet of Things Journal*;
6. *Internet of Things*;
7. *Computer Networks*;
8. *Computer Communications*;
9. *Journal of Information Security and Applications*;
10. *Information Fusion*.

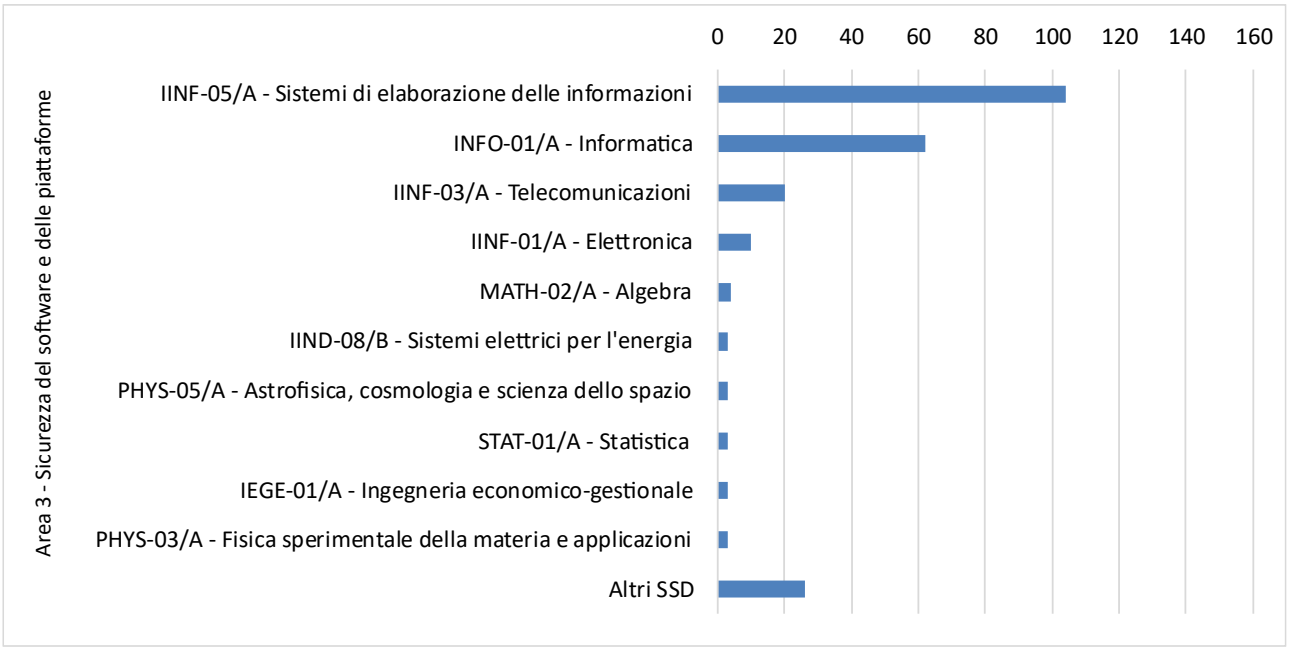


Figura 18: SSD valutazione per Area 3.

4.2.4 *Area 4 – Sicurezza delle infrastrutture digitali*

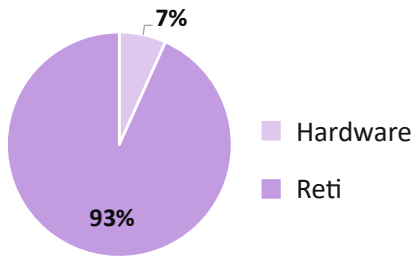


Figura 19: Statistiche per subaree dell'Area 4.

Dalla Figura 19 si può notare che, in termini di pubblicazioni conferite, la Subarea 4.1 – Reti è preponderante, con un significativo 93%, rispetto all'ulteriore subarea costitutiva dell'Area 4, ossia la Subarea 4.2 – Hardware.

Per quanto riguarda gli SSD su cui tali pubblicazioni sono state valutate, la distribuzione è molto più ristretta ad aree scientifico-disciplinari proprie dell'Ingegneria e delle Scienze matematiche e informatiche: nello specifico, spiccano Sistemi di elaborazione delle informazioni, informatica e telecomunicazioni – cfr. Figura 20. Le tematiche trattate in questa area, infatti, sono relative alla sicurezza degli apparati hardware e di rete che compongono le infrastrutture digitali, tipicamente trattate da tali SSD.

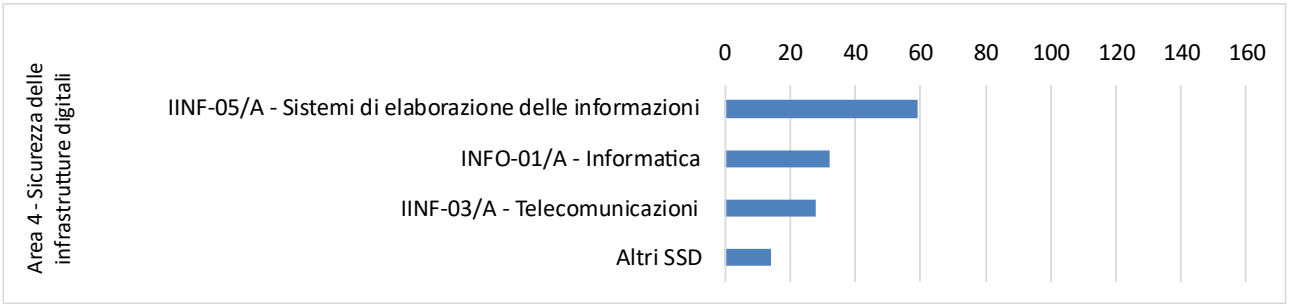


Figura 20: SSD valutazione per Area 4.

Infine, la lista delle 10 riviste più utilizzate in Area 4 è la seguente:

1. *IEEE Internet of Things Journal*;
2. *IEEE Transactions on Information Forensics and Security*;
3. *Computer Networks*;
4. *Computer Communications*;
5. *IEEE Access*;
6. *Ad Hoc Networks*;
7. *Journal of Information Security and Applications*;
8. *Information Fusion*;
9. *Internet of Things*;
10. *IEEE Communications Surveys and Tutorials*.

4.2.5 *Area 5 – Aspetti della società*

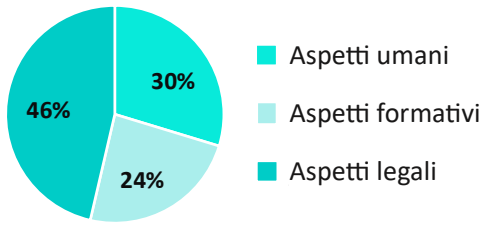


Figura 21: Statistiche per subaree dell'Area 5.

Come si può vedere nella Figura 21, delle tre subaree componenti l'Area 5, la subarea prevalente risulta essere la 5.3 – Aspetti Legali, seguita dalla Subarea 5.1 – Aspetti umani e, in coda, dalla Subarea 5.2 – Aspetti formativi. Gli argomenti afferenti alla Subarea 5.3 sono di estrema importanza, data la necessità crescente di avere una legislazione che segua gli sviluppi tecnologici con riferimento agli aspetti di cybersicurezza.

L'analisi degli SSD (cfr. Figura 22) su cui sono state valutate le pubblicazioni inerenti all'Area 5 riflette quanto osservato in relazione alle subaree, ovvero una folta rappresentanza di Scienze giuridiche (nello specifico, Diritto internazionale, Filosofia del diritto, Diritto amministrativo e pubblico, Diritto privato, Diritto costituzionale e pubblico, Diritto dell'Unione Europea e Diritto penale) e Scienze politiche e sociali. Gli SSD più rappresentati, però, continuano ad essere di tipo STEM (Sistemi di elaborazione delle informazioni e Informatica), a testimonianza della necessità di trattare le tematiche di R&I relative agli aspetti della società in maniera interdisciplinare.

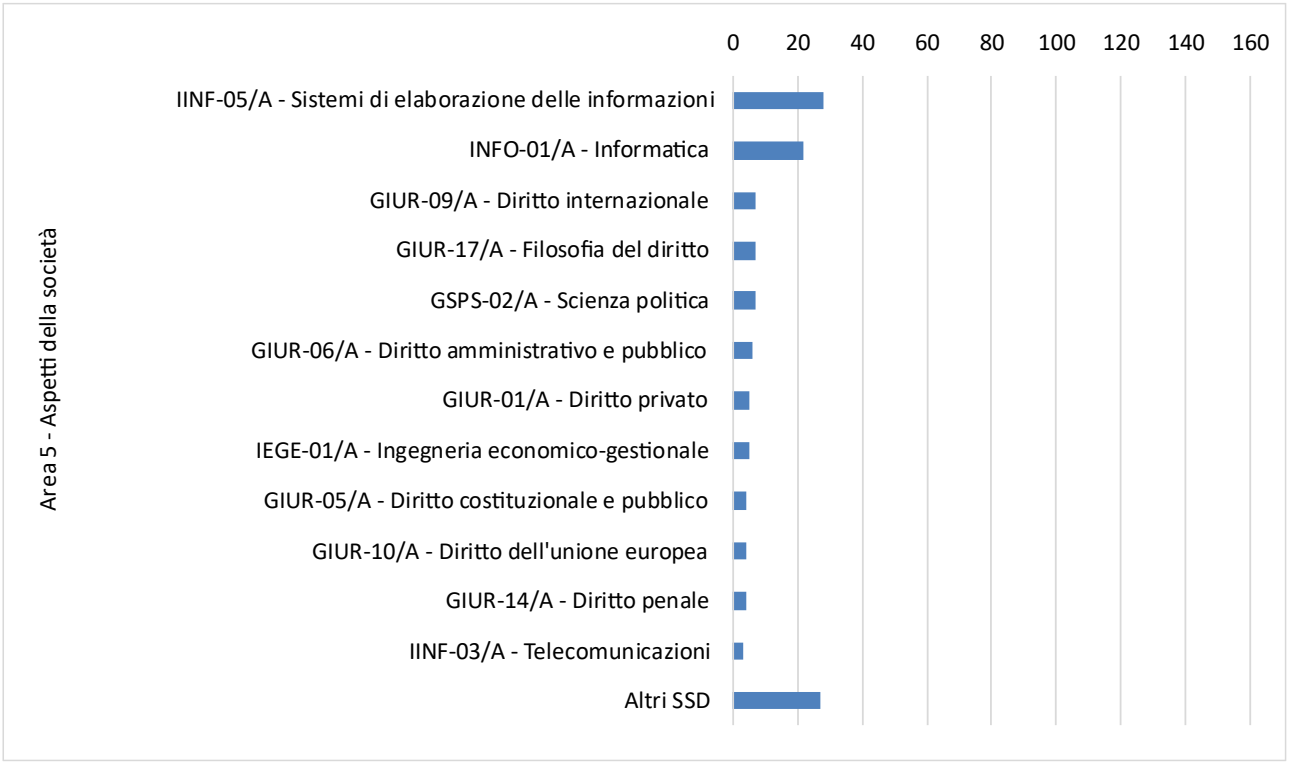


Figura 22: SSD valutazione per Area 5.

Infine, le 10 riviste più utilizzate per la ricerca su tematiche inerenti all'Area 5 sono:

1. *Computers & Security*;
2. *Decision Support Systems*;
3. Rivista Italiana di Politiche Pubbliche;
4. *Computer Networks*;
5. *ACM Computing Surveys*;
6. Rivista del Diritto della Navigazione;
7. *Pattern Recognition Letters*;
8. *IEEE Access*;
9. *European Papers*;
10. *German Law Journal*.

4.2.6 Area 6 – Aspetti di governo

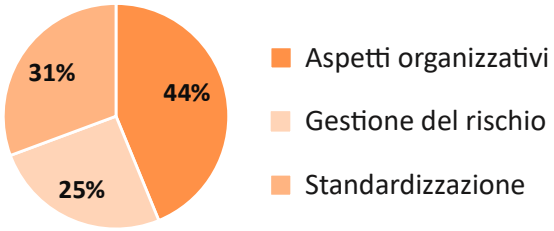


Figura 23: Statistiche per subaree dell'Area 6.

Dal grafico in Figura 23, si evince come la subarea con il maggior numero di pubblicazioni nel contesto dell'Area 6 è la Subarea 6.1 – Aspetti organizzativi, che distanzia non di poco (13 punti percentuali) la Subarea 6.3 – Standardizzazione, seguita dalla Subarea 6.2 – Gestione del rischio. Gli argomenti afferenti alla Subarea 6.3 sono di crescente interesse per consentire di massimizzare l'impatto delle tecnologie emergenti.

La distribuzione degli SSD su cui sono valutate le pubblicazioni inerenti all'Area 6 è fornita in Figura 24. Si può notare come, al netto di Scienza politica e Statistica, gli aspetti di governo sono trattati in larga parte da aree scientifico-disciplinari di tipo ingegneristico.

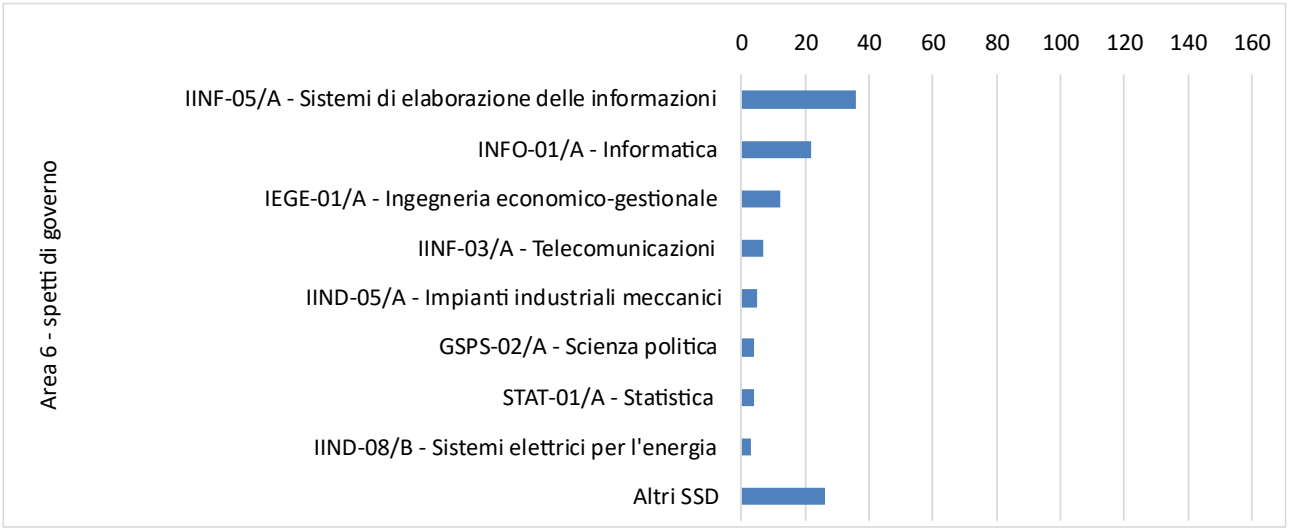


Figura 24: SSD valutazione per Area 6.

Infine, le 10 riviste più utilizzate nell'ambito degli aspetti di governo relativi alla cybersicurezza sono:

1. *Future Generation Computer Systems*;
2. *Computers & Security*;
3. *IEEE Access*;
4. *Computer Communications*;
5. *Journal of Information Security and Applications*;
6. *Decision Support Systems*;
7. *Computer Networks*;
8. *IEEE Transactions on Service Computing*;
9. *IEEE Transactions on Dependable and Secure Computing*;
10. *Computers in Industry*.

4.2.7 Trend temporale

A conclusione della trattazione delle diverse aree di R&I sulla cybersicurezza, è utile confrontare l'andamento delle pubblicazioni negli anni 2020-2024. Come si può vedere dalla Figura 25, il trend è in crescita per le Aree 1, 5 e 6, stazionario per le Aree 3 e 4, mentre per l'Area 2 si osserva una crescita tra il 2021 e il 2023 e una decrescita nel 2024 fino ai livelli del 2020, pur rimanendo l'area con un maggior numero di pubblicazioni conferite in tutto il quinquennio.

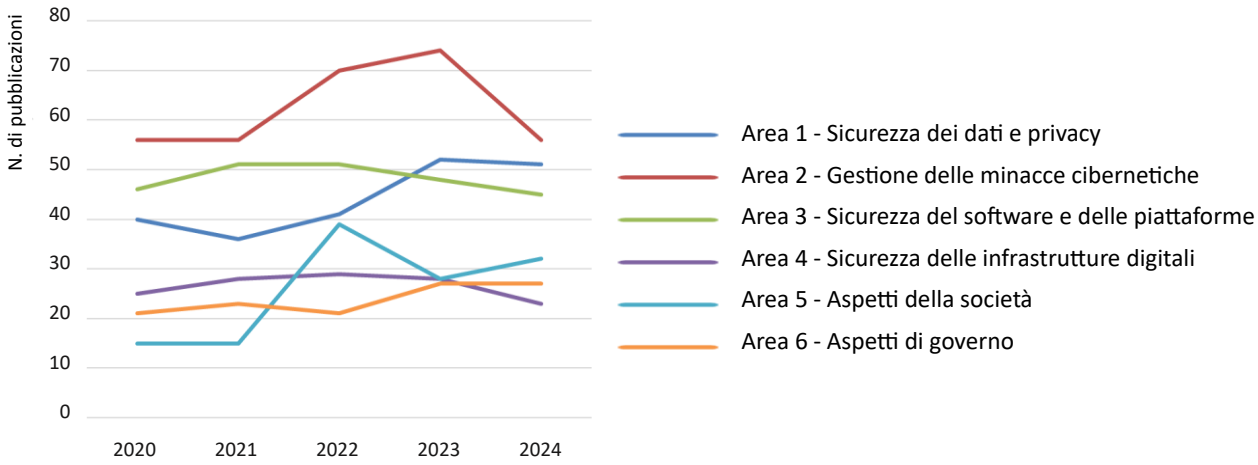


Figura 25: Andamento temporale delle pubblicazioni conferite afferenti alle aree dell'Agenda di R&I.

4.3 Analisi relativa ai domini tecnologici prioritari

Da un punto di vista generale, si presenta a seguire l'analisi delle pubblicazioni sulla base dei 4 domini tecnologici prioritari (IA, QT, CPS e NGWN), che coprono circa l'85% delle pubblicazioni inerenti alla cybersicurezza filtrate sulle EDT.

Si osserva che la tipologia di pubblicazione più frequente in tutti i domini è l'articolo in rivista, con una percentuale superiore al 93%. La parte restante delle pubblicazioni è costituita da contributi in atti di convegno, contributi in volume (capitoli o saggi), monografie o trattati scientifici e curatele.

Dall'analisi dei dati si evince, inoltre, come tali pubblicazioni siano rese a disposizione ad accesso aperto (*open access*) nella maggior parte dei casi in tutte le aree (in un intervallo compreso tra il 75% in ambito TQ e il 65% in ambito CPS). A seguire, emergono le stesse casistiche osservate nell'analisi relativa alle aree di R&I, per cui la pubblicazione non è disponibile in *open access*, ovvero i) i diritti sono stati ceduti

all'Editore, ii) è stata invocata la protezione dei risultati ex D.Lgs. 30/2005 (Codice della proprietà industriale) e iii) è stato posto un embargo oltre il 30/06/2026.

Di seguito, è presentata l'analisi di dettaglio relativa ai quattro domini tecnologici.

4.3.1 Intelligenza artificiale

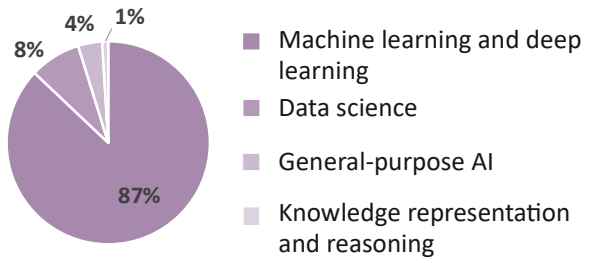


Figura 26: Statistiche per le singole EDT che compongono il dominio tecnologico IA.

Come evidenziato dalla Figura 26, la stragrande maggioranza della ricerca in questo dominio riguarda la relazione tra cybersicurezza e *machine learning and deep learning*. A seguire, *data science*, il nuovo ambito del GPAI e, infine, la rappresentazione della conoscenza. È interessante notare come quest'ultima EDT, che gioca un ruolo importante nell'ambito della c.d. IA simbolica, contribuisca solo per l'1% al dominio IA, laddove, invece, è di particolare importanza per la spiegabilità (*explainability*) e la trasparenza delle soluzioni IA.

Coerentemente con quanto osservato pocanzi, dalla Figura 27 si nota che gli SSD su cui sono valutate le pubblicazioni relative al dominio tecnologico dell'IA sono, a parte Diritto privato, in larga parte legate a discipline ingegneristiche quali Sistemi di elaborazione delle informazioni, Informatica, Telecomunicazioni ed Elettronica.

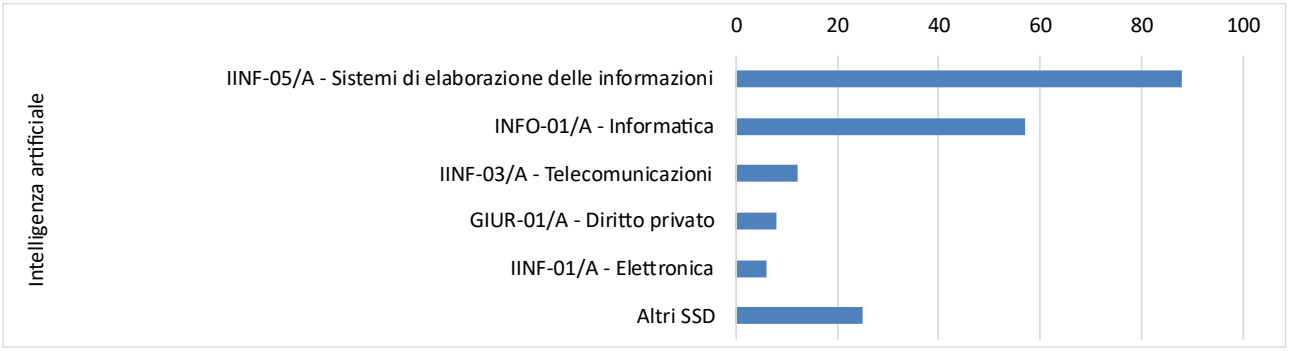


Figura 27: SSD valutazione per il dominio tecnologico Intelligenza artificiale (IA).

Infine, le 10 riviste più utilizzate per pubblicare ricerche sulla sicurezza dell'IA sono:

1. *IEEE Access*;
2. *Computers & Security*;
3. *IEEE Transactions on Network and Service Management*;
4. *Sensors*;
5. *Expert Systems with Applications*;
6. *Future Generation Computer Systems*;
7. *IEEE Transactions on Information Forensics and Security*;
8. *Pattern Recognition Letters*;
9. *Computer Networks*;
10. *IEEE Internet of Things Journal*.

4.3.2 *Tecnologie quantistiche*

Per quanto riguarda le TQ, come atteso (cfr. Figura 28), l'SSD su cui sono state valutate la stragrande maggioranza delle pubblicazioni è nell'ambito delle Scienze fisiche, in particolare Fisica sperimentale della materia e applicazioni. A debita distanza, dopo Fisica teorica della materia, modelli, metodi matematici e applicazioni, troviamo altre discipline STEM quali Informatica, Telecomunicazioni e Sistemi di elaborazione delle informazioni.

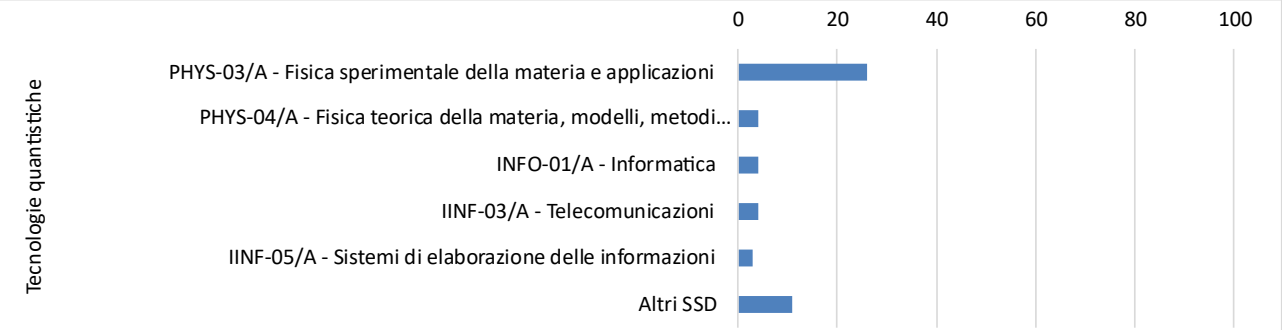


Figura 28: SSD valutazione per il dominio tecnologico Tecnologie quantistiche (TQ).

Per quanto riguarda le riviste su cui si pubblicano articoli sulla sicurezza delle TQ, le prime 10 sono:

1. *Nature Communications*;
2. *Science Advances*;
3. *npj Quantum Information*;
4. *Nature Materials*;
5. *Advances in Optics and Photonics*;
6. *Physical Review Applied*;
7. *Designs, Codes and Cryptography*;
8. *Journal of Optical Communications and Networking*;
9. *Quantum Science and Technology*;
10. *ACS Applied Nano Materials*.

4.3.3 *Sistemi cyber-fisici*

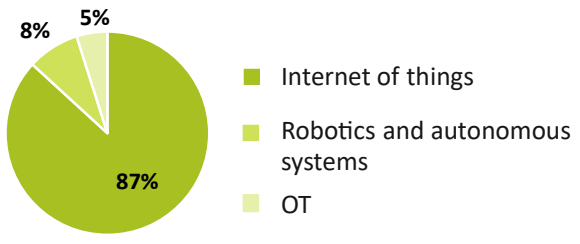


Figura 29: Statistiche per le singole EDT che compongono il dominio tecnologico CPS.

Dalla Figura 29 emerge chiaramente come la stragrande maggioranza della ricerca sulla relazione tra cybersicurezza e CPS riguarda l'Internet delle cose. È, infatti, molto limitato il contributo di OT al dominio CPS (5%).

Similmente a quanto osservato per l'IA, nella distribuzione degli SSD su cui sono valutate le pubblicazioni in ambito CPS le discipline ingegneristiche e applicate risultano essere le più attive – cfr. Figura 30.

Infine, le prime 10 riviste su cui sono apparsi studi relativi alla sicurezza dei CPS sono:

1. *IEEE Internet of Things Journal*;
2. *Computer Networks*;
3. *Computer Communications*;
4. *Sensors*;
5. *IEEE Transactions on Industrial Informatics*;
6. *Future Generation Computer Systems*;
7. *Journal of Information Security and Applications*;
8. *Internet of Things*;
9. *IEEE Access*;
10. *IEEE Transactions on Dependable and Secure Computing*.

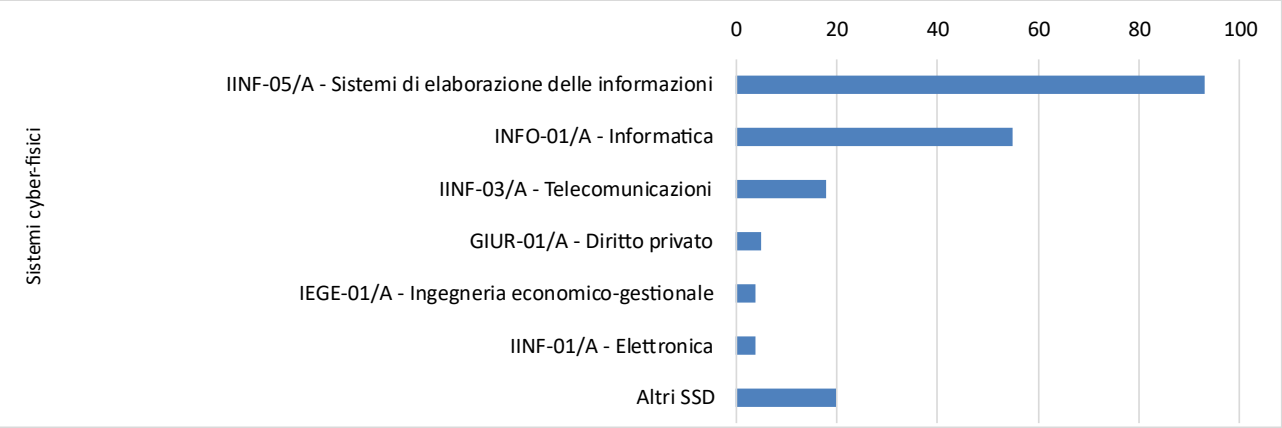


Figura 30: SSD valutazione per il dominio tecnologico Sistemi cyber-fisici (CPS).

4.3.4 Reti wireless di prossima generazione

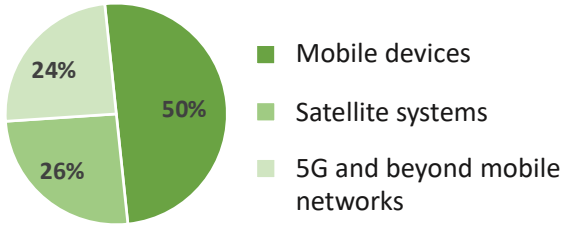


Figura 31: Statistiche per EDT componenti il dominio tecnologico NGWN.

Per quanto riguarda le NGWN, l'EDT più trattata nelle pubblicazioni selezionate risulta essere *mobile devices*, mentre sistemi satellitari e reti mobili si spartiscono in maniera uguale l'altra metà dei lavori scientifici – cfr. Figura 31. In particolare, il contributo pari al 26% dei *"Satellite Systems"* risulta giustamente significativo, anche in considerazione della relativa importanza strategica rispetto all'autonomia tecnologica nazionale.

Come atteso, l'analisi degli SSD in Figura 32 riporta nelle prime posizioni Telecomunicazioni, Sistemi di elaborazione delle informazioni e Informatica. È interessante, però, osservare come trovano spazio anche discipline delle Scienze fisiche, della Bioingegneria e dell'Ingegneria industriale, rendendo il dominio NGWN il più interdisciplinare tra i quattro analizzati in questo rapporto.

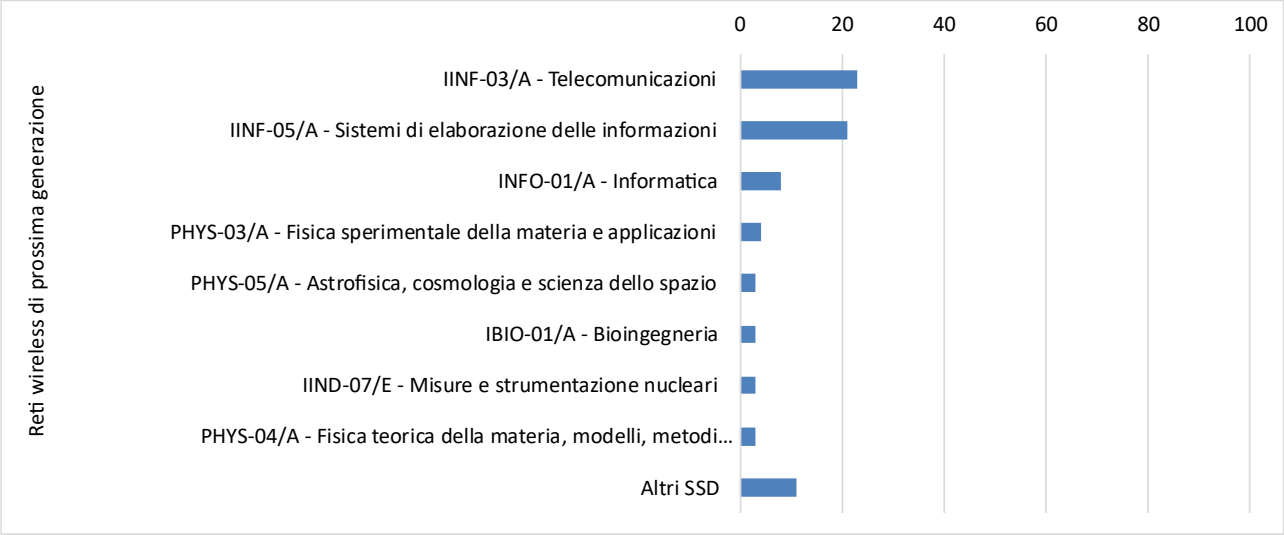


Figura 32: SSD valutazione per il dominio tecnologico Reti wireless di prossima generazione (NGWN).

Infine, le 10 riviste più utilizzate per pubblicare ricerche sulla sicurezza delle NGWN sono:

1. *Sensors*;
2. *The Planetary Science Journal*;
3. *Computer Communications*;
4. *IEEE Internet of Things Journal*;
5. *IEEE Transactions on Vehicular Technology*;
6. *Advances in Optics and Photonics*;
7. *Computers & Security*;
8. *IEEE Transactions on Information Forensics and Security*;
9. *IEEE Access*;
10. *IEEE Transactions on Network and Service Management*.

4.3.5 Trend temporale

A conclusione della trattazione dei quattro domini tecnologici prioritari in relazione alla cybersicurezza, è utile confrontare l'andamento delle pubblicazioni negli anni 2020-2024. Come si può vedere dalla Figura 33, il trend è in crescita per TQ, pur essendo i contributi più limitati rispetto agli altri domini, e in leggera discesa per CPS e NGWN. In relazione all' IA, che si attesta insieme a Cyber-physical systems, come il dominio a maggior numero di contributi negli anni, si osserva una prima variazione in discesa (2020-2021) e poi in risalita dal 2021.

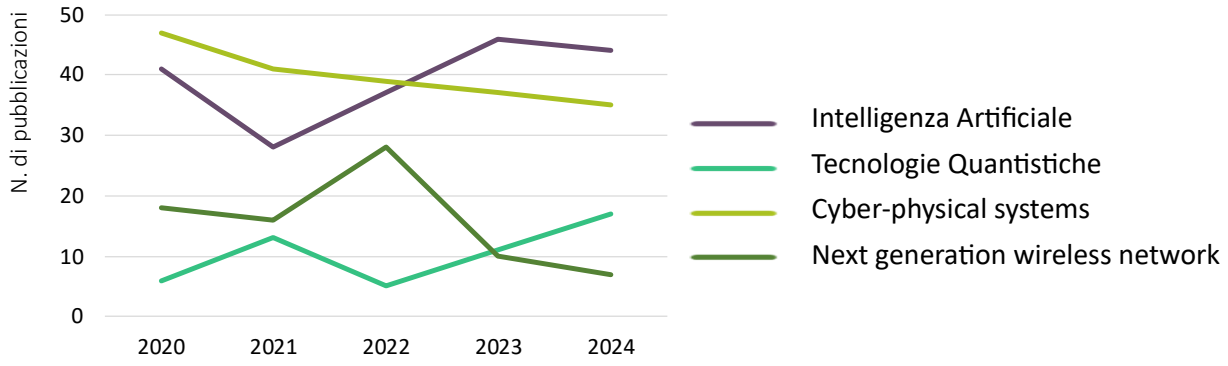


Figura 33: Trend annuale pubblicazioni per dominio tecnologico.

5 Analisi dei ricercatori e istituzioni di ricerca attive

In questa sezione, sono presentate le analisi relative ai ricercatori e alle IdR attive sulla cybersicurezza, utilizzando diverse dimensioni di analisi. Anzitutto, saranno analizzate le categorie dei ricercatori e delle IdR che hanno conferito le pubblicazioni selezionate. Quindi, saranno studiate le distribuzioni territoriali delle pubblicazioni e delle iniziative di valorizzazione della ricerca individuate. Infine, saranno caratterizzati i corsi di dottorato di ricerca inerenti alla cybersicurezza.

5.1 Caratterizzazione dei ricercatori che hanno conferito pubblicazioni

I ricercatori che hanno conferito pubblicazioni alla VQR possono essere caratterizzati dai seguenti parametri:

- profilo. Si distingue principalmente tra i) ricercatori neoassunti o promossi nel periodo 2020-2024, ii) ricercatori permanenti, ovvero che, nel periodo considerato, non hanno ottenuto un avanzamento di carriera e iii) altro;
- genere;
- qualifica. Le qualifiche considerate per gli atenei sono:
    - assistenti,
    - dottori di ricerca;
    - professori di prima fascia (ordinari),
    - professori di seconda fascia (associati),
    - professore straordinario a tempo determinato,
    - ricercatori a tempo determinato,
    - ricercatori universitari.

Le qualifiche per EPR e Istituzioni volontarie, invece, comprendono:

- incaricati di ricerca,
- ricercatori,
- tecnologi.

5.1.1 Per aree dell'Agenda di R&I

Da un punto di vista generale, l'analisi dei ricercatori sulla base delle aree dell'Agenda di R&I dimostra che il profilo più frequente in tutte le aree è il neoassunto (in un intervallo compreso tra il 69% in Area 6 – Aspetti di governo e il 58% in Area 1 – Sicurezza dei dati e privacy). A seguire, si trova il profilo del ricercatore permanente, compreso tra il 34% in Area 1 e il 27% in Area 6.

La Figura 34 illustra le qualifiche dei ricercatori che hanno conferito pubblicazioni relative alla cybersicurezza, distinguendo tra ruoli universitari e ruoli relativi ad enti pubblici di ricerca e altri enti.

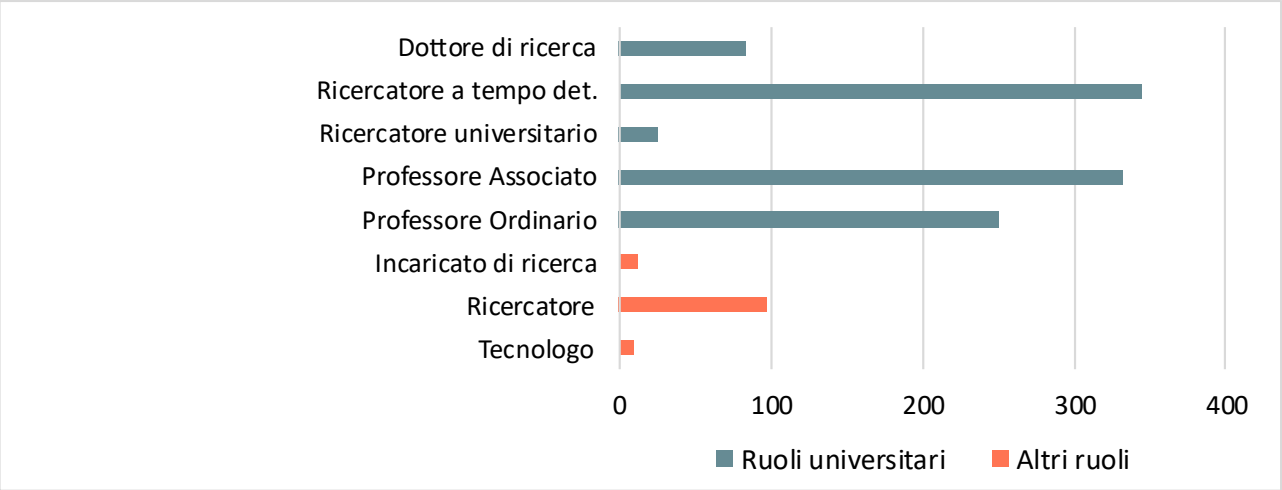


Figura 34: Qualifiche dei ricercatori su base aree dell'Agenda.

La Figura 35 rappresenta la distribuzione delle qualifiche dei ricercatori conferenti in ambito universitario e non sulle diverse aree dell'Agenda di R&I, evidenziando come gli stessi si ripartiscano su tutte le aree, con una prevalenza dell'Area 2 – Gestione delle minacce cibernetiche.

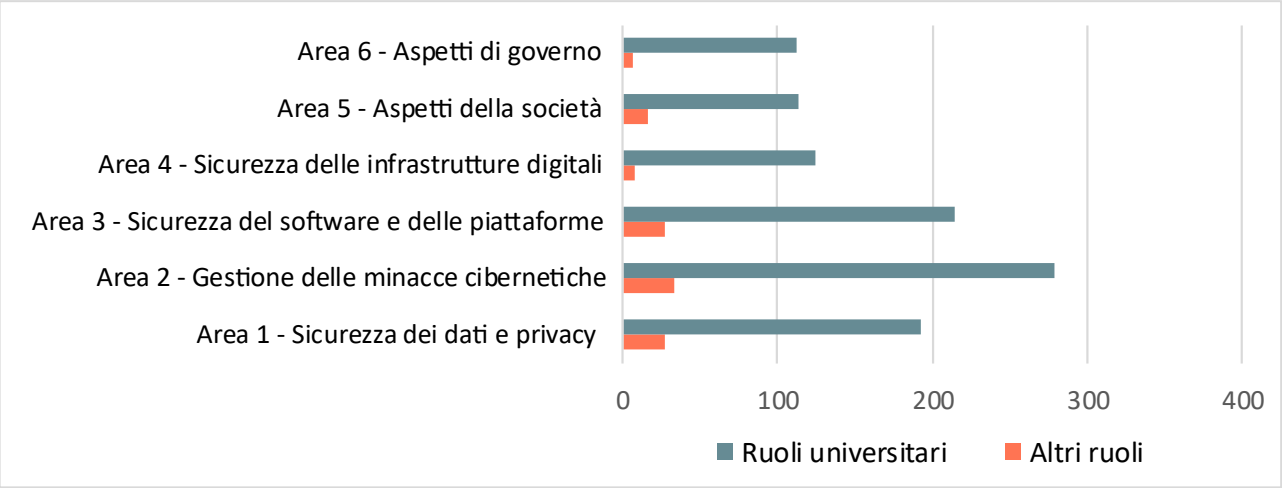


Figura 35: Distribuzione delle qualifiche per aree dell'Agenda.

In Figura 36 è presentato il dettaglio delle singole qualifiche ripartite ciascuna area dell'Agenda di R&I. Da non trascurare, in particolare, che una quota significativa di pubblicazioni inerenti alla cybersicurezza è stata conferita da dottori di ricerca. Si osserva inoltre che il contributo dei dottori di ricerca appare più marcato per le aree STEM. In aggiunta, in Figura 36 è mostrata un'analisi di genere, da cui si evince che nelle aree di R&I afferenti all'ambito STEM, ovvero le Aree 1-4, la percentuale di ricercatrici che hanno conferito le pubblicazioni identificate come inerenti alla cybersicurezza non supera il 20%. Tale percentuale sale nelle Aree 5 e 6, dove, nello specifico per l'Area 5 – Aspetti della società, raggiunge il 38%.

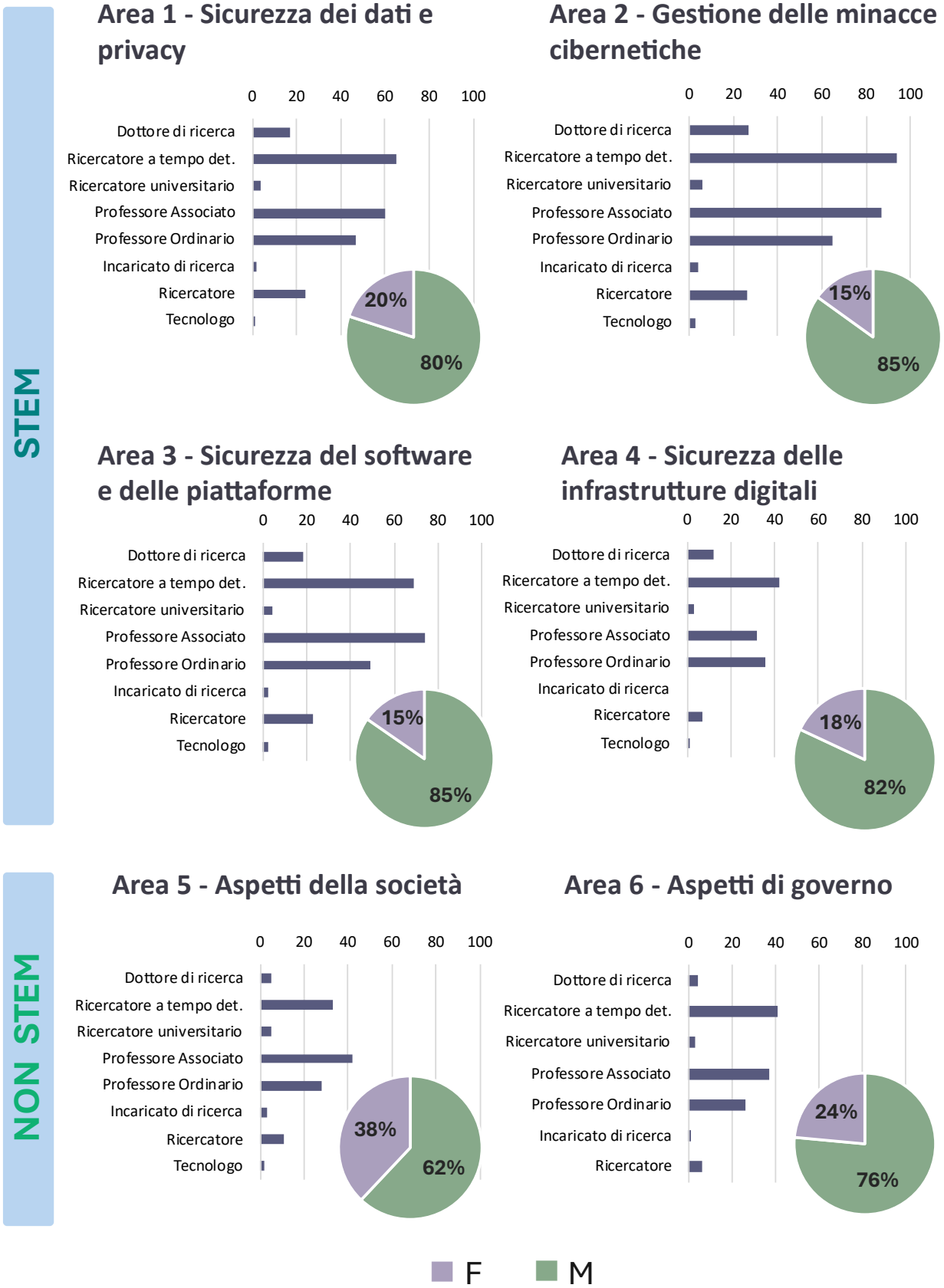


Figura 36: Panoramica dei ricercatori attivi sulla cybersicurezza in termini di qualifica e genere.

5.1.2 *Per domini tecnologici prioritari*

Da un punto di vista generale, l'analisi dei ricercatori su base domini tecnologici prioritari dimostra che il profilo più frequente in tutti i domini è il neoassunto (in un intervallo compreso tra il 70% nel dominio NGWN e il 61% in ambito IA). A seguire, si trova il profilo del ricercatore permanente, compreso tra il 30% in ambito IA e il 20,25% nel dominio NGWN.

Relativamente all'analisi di genere, dai risultati presentati in Figura 37, si evince che nei domini IA e CPS la percentuale di ricercatrici che hanno conferito le pubblicazioni identificate come inerenti alla cybersicurezza non supera il 20%. Tale percentuale sale moderatamente in ambito TQ e NGWN, dove raggiunge in entrambi i casi la soglia del 27%.

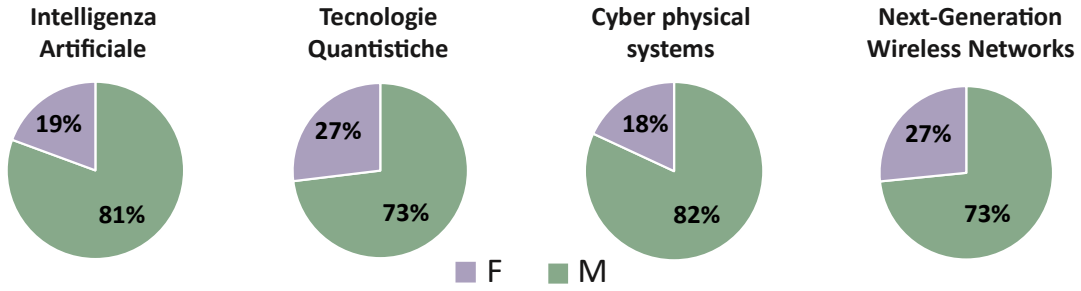


Figura 37: Genere dei ricercatori attivi sui domini tecnologici prioritari.

5.2 Caratterizzazione delle Istituzioni di Ricerca che hanno conferito pubblicazioni

5.2.1 *Per aree dell'Agenda di R&I*

L'analisi delle IdR sulla base delle aree dell'Agenda di R&I dimostra che la tipologia di istituzione più frequente in tutte le aree è l'ateneo pubblico (in un intervallo compreso tra l'89% in Area 4 – Sicurezza delle infrastrutture digitali e 77% in Area 5 – Aspetti della società). A seguire, si trovano gli enti pubblici di ricerca (EPR), con una percentuale compresa tra l'11% dell'Area 1 – Sicurezza dei dati e privacy e il 7% dell'Area 4. La parte restante è costituita da atenei non statali e istituzioni volontarie.

5.2.2 *Per domini tecnologici prioritari*

L'analisi delle IdR sulla base dei domini tecnologici è disponibile in Figura 38. Si può vedere chiaramente che, mentre su IA, CPS e NGWN la tipologia di istituzione più frequente è l'ateneo pubblico, con percentuali comprese tra l'84% e l'86%, tale percentuale scende al 69% nel caso delle TQ. La differenza viene assorbita dagli EPR che, nel caso della ricerca sulla relazione tra TQ e cybersicurezza, recitano un ruolo significativamente più importante rispetto agli altri domini.

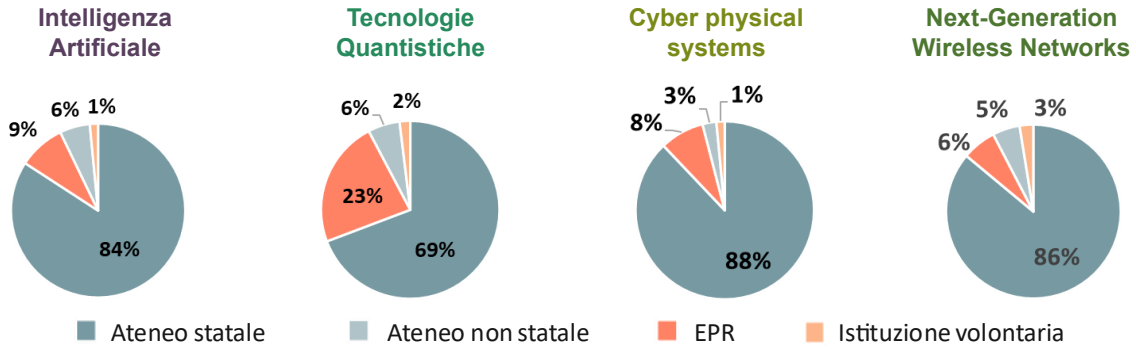


Figura 38: Tipologia di IdR per i domini tecnologici prioritari.

5.3 Distribuzione territoriale delle pubblicazioni conferite

Per le sole pubblicazioni conferite da atenei statali e non statali è possibile individuare la macro-area geografica (Nord, Centro, Sud e Isole) da cui proviene il conferimento.

5.3.1 Per aree dell'Agenda di R&I

Dalla Figura 39, è possibile notare che la macro-area geografica Nord rappresenta quella più attiva nei conferimenti di pubblicazioni inerenti alla cybersicurezza (42%), seguita dal Sud e Isole (38%) e dal Centro (18%). Le università telematiche contribuiscono per il residuale 2%.

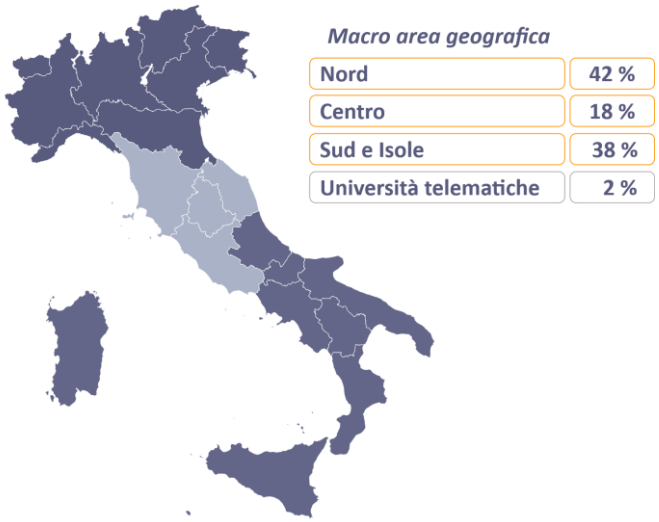


Figura 39: Distribuzione territoriale delle pubblicazioni su base aree dell'Agenda.

5.3.2 Per domini tecnologici prioritari

Dalla Figura 40 alla Figura 43 è possibile notare, invece, che, mentre per IA e CPS le macro-aree geografiche di Nord e Sud e Isole si equivalgono, per TQ le macro-aree geografiche Nord e Centro risultano le più attive. Infine, per il dominio NGWN si registra una distribuzione sostanzialmente uniforme delle pubblicazioni conferite.

Figura 40: Macro-area geografica per IA.

Figura 41: Macro-area geografica per TQ.

Figura 42: Macro-area geografica per CPS.

Figura 43: Macro-area geografica per NGWN.

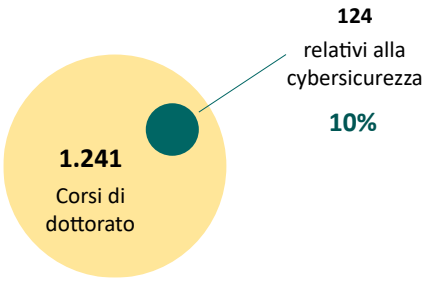
5.4 Corsi di dottorato di ricerca inerenti alla cybersicurezza

È utile, inoltre, arricchire l'analisi su ricercatori e IdR attivi sul territorio nazionale con un approfondimento relativo all'offerta di corsi di dottorato inerenti alla cybersicurezza, al fine di fornire una stima del bacino di potenziali futuri ricercatori e di prodotti della ricerca dottorale inerenti alla cybersicurezza, nonché informazioni utili sulla distribuzione territoriale dei corsi stessi.

I corsi di dottorato sono caratterizzati da una o più aree CUN, con un'area principale ossia quella a cui afferisce la maggioranza relativa dei componenti del Collegio di dottorato.

5.4.1 *Tematiche di R&I trattate*

Dei 1.241 corsi di dottorato analizzati, 124 sono risultati attinenti alle tematiche delle 6 aree dell'Agenda di R&I. La Figura 44 consente una immediata rappresentazione di quanto i temi di cybersicurezza siano trattati nei percorsi formativi di terzo livello: l'Area 5 – Aspetti della società emerge come la più trattata (con oltre 80 corsi di dottorato inerenti), seguita dall'Area 2 – Gestione delle minacce cibernetiche (con più di 60 corsi inerenti) e dall'Area 6 – Aspetti di governo (con oltre 40 corsi inerenti). Più distaccati, troviamo le restanti Aree 1, 3 e 4. Si noti come le aree non-STEM (Aspetti della società e Aspetti di governo) risultano particolarmente trattate rispetto a quanto accade nelle pubblicazioni (cfr. Sezione 4.2).



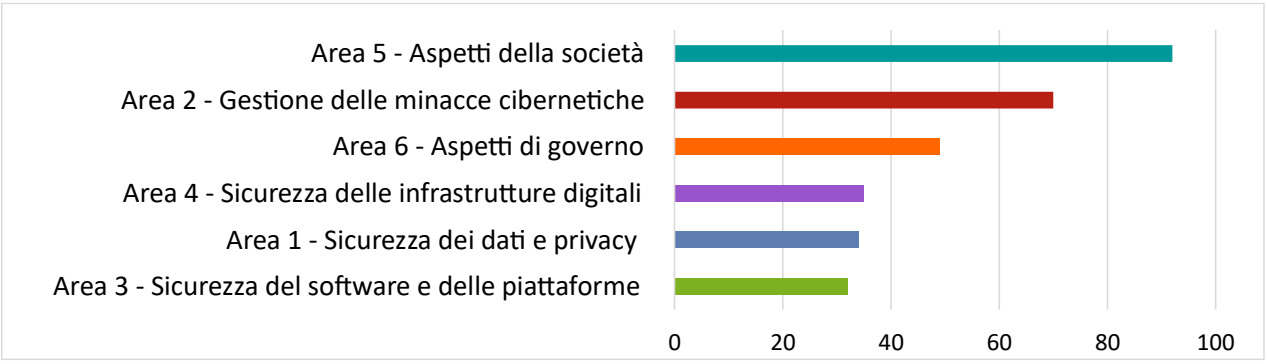


Figura 44: Distribuzione dei corsi di dottorato sulle aree di R&I. Si noti che un singolo corso può trattare più di un'area.

Inoltre, la Figura 45 fornisce la vista per domini tecnologici prioritari, evidenziando la netta prevalenza di corsi di dottorato inerenti aspetti di cybersicurezza relativi all'IA e ai CPS, mentre TQ e NGWN risultano a minore presenza di corsi.

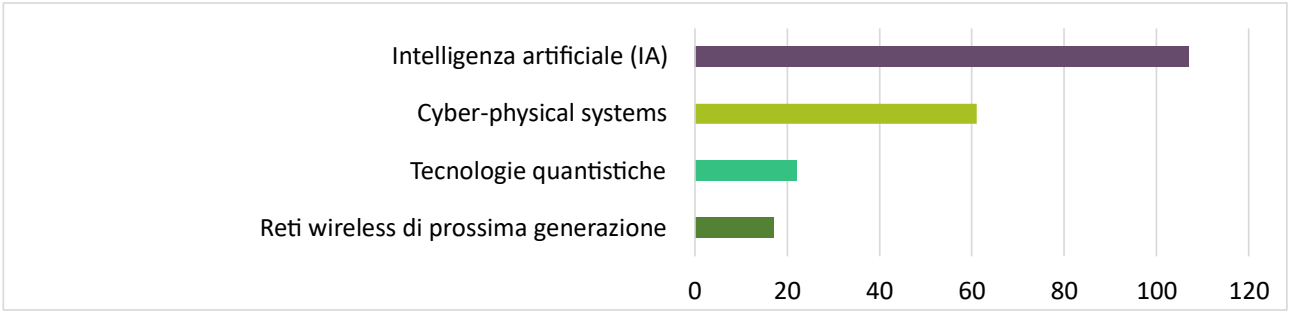


Figura 45: Distribuzione dei corsi di dottorato sui domini tecnologici prioritari.

Infine, dalla Figura 46 è possibile vedere come i corsi di dottorato che risultano inerenti a tematiche di interesse per la cybersicurezza siano riconducibili alle Aree CUN (cfr. Sezione 3.1.2). In particolare, si conferma quanto osservato in Sezione 4.1 e in Tabella 3, ovvero che la maggior parte dei corsi di dottorato inerenti alla cybersicurezza sono caratterizzati da un Collegio di dottorato afferente alle Aree CUN 1 e 9, le quali corrispondono ai GEV1 – Scienze matematiche e informatiche e GEV9 – Ingegneria industriale e dell'informazione. Più distaccate, l'Area CUN 12 – Scienze giuridiche, ma comunque in linea con quanto osservato nelle citate sezioni. Emergono, invece, in maniera più importante le Aree CUN 13 (Scienze economiche e statistiche) e 14 (Scienze politiche), che superano l'Area CUN 2 – Scienze fisiche.

Tali risultati dell'analisi sono coerenti con quanto rappresentato in Sezione 4.1, nella quale era stata analizzata la relazione tra le tematiche di R&I trattate nelle pubblicazioni scientifiche e gli SSD di origine.

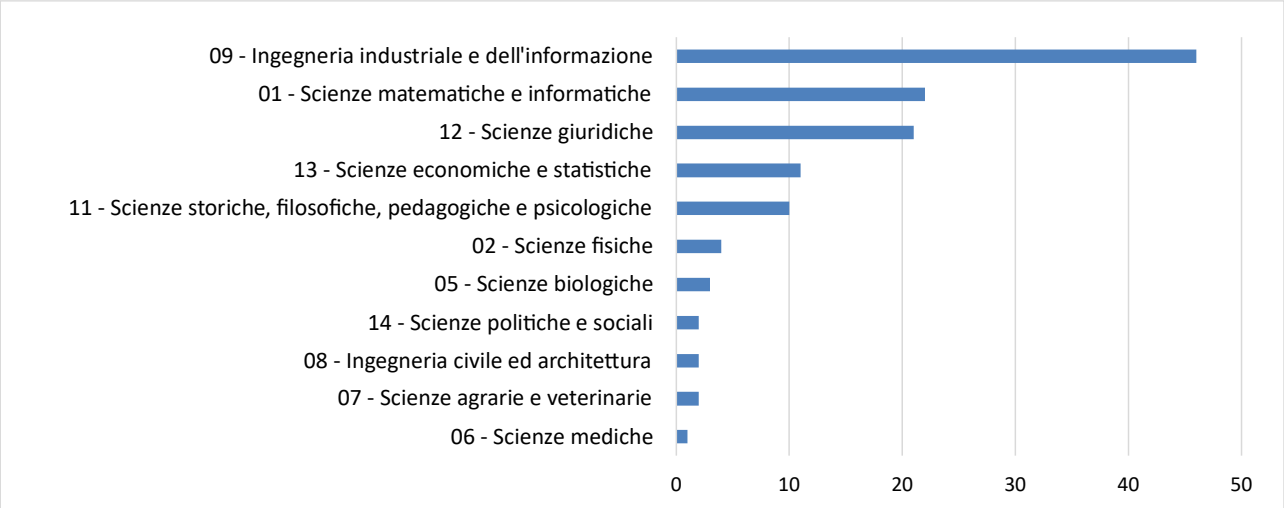


Figura 46: Aree CUN dei corsi di dottorato inerenti alla cybersicurezza.

5.4.2 Distribuzione territoriale

La Figura 47 mostra come i corsi di dottorato inerenti alla cybersicurezza si distribuiscano sulle diverse regioni del territorio nazionale: conduce il Nord con il 49%, seguito dal Sud e Isole con il 34% e dal Centro con il 14%. Le università telematiche costituiscono, infine, il 3% del bacino dei corsi di dottorato individuati.

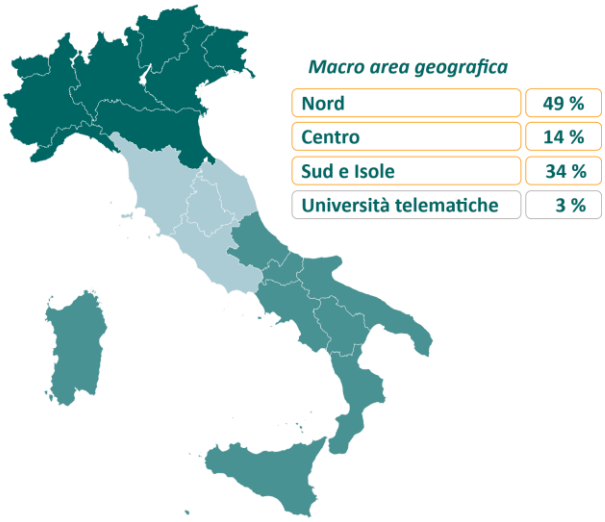


Figura 47: Distribuzione territoriale dei corsi di dottorato inerenti alla cybersicurezza.

6 Iniziative di valorizzazione della ricerca in cybersicurezza

Per mantenere la competitività del Paese nelle tecnologie ad alto impatto economico e strategico per la sicurezza nazionale – come quelle analizzate in questo rapporto – è necessario poter contare su un ecosistema dell'innovazione capace di trasformare i risultati scientifici in soluzioni adottabili, riducendo dipendenze tecnologiche e rafforzando la resilienza nazionale. In questo quadro, diventa centrale una ricerca in cybersicurezza che sappia avvicinarsi al mercato e alle esigenze operative di imprese e istituzioni, valorizzando in modo sistematico competenze, prototipi e proprietà intellettuale. Per questa ragione, il rapporto si è interrogato sullo stato della terza missione nel campo della cybersicurezza, ossia quell'insieme di attività che, accanto alla didattica/formazione (prima missione) e alla ricerca (seconda missione), consente il trasferimento di conoscenze, tecnologie e risultati verso società, istituzioni e sistema produttivo, generando impatto economico, sociale e civile.

In particolare, integrando i 676 casi di studio conferiti nell'ambito della VQR 2020-2024 (cfr. Sezione 3.1.2) con i casi di studio presenti sul portale *KnowledgeShare* (3123), sono state analizzate le iniziative di terza missione del sistema della ricerca pubblica italiana relative a:

- valorizzazione della proprietà intellettuale e industriale quali, ad esempio, brevetti, licenze, software registrato;
- imprenditorialità accademica quale, ad esempio, spin-off e start-up di matrice accademica;
- *cross-innovation* e *cross-fertilization*, con attenzione alle collaborazioni impresa–università e a iniziative congiunte orientate all'adozione industriale.

6.1 Tematiche di R&I trattate dalle iniziative di valorizzazione

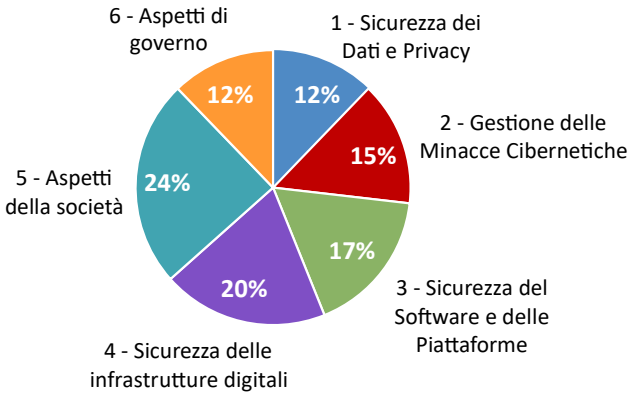


Figura 48: Distribuzione dei casi di studio analizzati sulle Aree.

Con sole 28 iniziative di valorizzazione attinenti al campo della cybersicurezza su un totale di 3799, l'analisi dei dati raccolti evidenzia una limitata produzione di attività legate al trasferimento tecnologico e di avvicinamento all'imprenditorialità accademica.

Come si può vedere in Figura 48, i casi di studio sono distribuiti abbastanza uniformemente sulle 6 aree di R&I sulla cybersicurezza.

Nello specifico, si osserva che:

- l'Area 5 – Aspetti della società rappresenta quasi un quarto dei casi complessivi. Dall'analisi delle subaree, si evince che la maggior parte di essi sono concentrati prevalentemente sulla Subarea 5.2 – Aspetti formativi;
- nell'Area 4 – Sicurezza delle infrastrutture digitali, la seconda per incidenza di casi di studio individuati, la Subarea 4.1 – Hardware è preponderante sulla Subarea 4.2 – Reti, in contrasto con quanto visto per le pubblicazioni (cfr. Sezione 4.2.4);

- l'Area 1 – Sicurezza dei dati e *privacy* è tra le aree relativamente meno rappresentate. Dall'analisi delle subaree, si evince che la maggior parte dei casi di studio inerenti ad essa sono nell'ambito della Subarea 1.2 – Crittografia;
- nell'ambito dell'Area 3 – Sicurezza del software e delle piattaforme, cui afferiscono il 17% dei casi di studio, emergono iniziative principalmente nell'ambito della Subarea 3.1 – Sicurezza nello sviluppo e nel test del software.

Infine, dal punto di vista delle EDT, i casi risultano concentrati soprattutto su *Hardware-based security* e *Mobile device*, a conferma di quanto osservato in precedenza relativamente alla Subarea 4.1 – Hardware, ma anche su *Machine learning e deep learning*.

6.2 Caratterizzazione delle Istituzioni di Ricerca che hanno conferito iniziative

In analogia a quanto visto per le pubblicazioni, la maggior parte delle IdR fa riferimento ad atenei statali (82%), mentre atenei non statali, EPR e Istituzioni volontarie raggiungono complessivamente il 18%. Dal momento che le iniziative di valorizzazione sono in numero limitato, è possibile solamente mostrarne la distribuzione territoriale in maniera aggregata – cfr. Figura 49 – che considera solo gli atenei statali e non. Dalla mappa si può notare come gli atenei del Nord Italia contribuiscano sostanzialmente alle iniziative di valorizzazione della ricerca, raggiungendo una percentuale aggregata del 64%, seguiti da quelli del Sud e Isole col 25% e del Centro con l'11%.

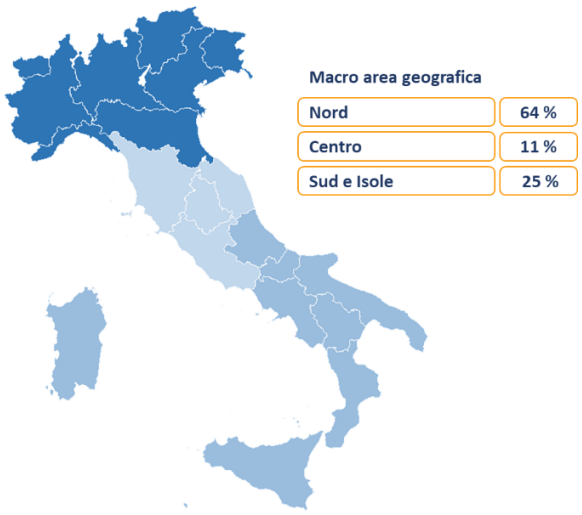


Figura 49: Distribuzione geografica delle iniziative di valorizzazione della ricerca inerenti alla cybersicurezza.

7 Sviluppi futuri

La collaborazione instaurata tra l'Agenzia per la cybersicurezza nazionale (ACN) e l'Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR) ha reso possibile approfondire e specializzare al dominio della cybersicurezza la fotografia complessiva della ricerca italiana derivante dall'esercizio di Valutazione della Qualità della Ricerca (VQR) 2000–2024. Tale lavoro congiunto ha consentito di far emergere significative evidenze quantitative relative al livello di copertura delle diverse aree tematiche della cybersicurezza da parte delle istituzioni di ricerca italiane, nonché informazioni rilevanti riguardanti il profilo dei ricercatori coinvolti e le caratteristiche strutturali degli enti accademici e dei centri di ricerca attivi in questo ambito.

I risultati prodotti offrono quindi un primo quadro sistematico, utile sia per comprendere lo stato dell'arte della ricerca nazionale nel settore sia per orientare future strategie di sviluppo scientifico e di rafforzamento delle competenze nel Paese.

Tale quadro può essere integrato ed esteso in diverse direzioni future.

In primo luogo, risulterebbe auspicabile estendere l'analisi all'insieme completo delle pubblicazioni scientifiche, integrando le pubblicazioni conferite nell'ambito dell'esercizio di Valutazione della Qualità della Ricerca (VQR) con quanto disponibile per altri esercizi condotti dal Ministero dell'Università e della Ricerca. Un simile ampliamento del corpus analizzato consentirebbe di migliorare la rappresentatività e la robustezza delle evidenze prodotte.

In secondo luogo, si ritiene opportuno ampliare il perimetro delle analisi sinora condotte, integrando come ulteriore unità di osservazione i progetti di ricerca aventi pertinenza con il dominio della cybersicurezza, sia di matrice nazionale sia finanziati in ambito europeo. L'inclusione dei progetti di ricerca consentirebbe non solo di arricchire la comprensione dei percorsi di sviluppo scientifico e tecnologico nel settore, ma anche di cogliere con maggiore precisione dinamiche collaborative, capacità di attrazione delle risorse e posizionamento competitivo delle Istituzioni italiane in relazione agli ecosistemi di ricerca europei e internazionali.

Sarebbe inoltre utile collocare le evidenze quantitative prodotte in merito alla ricerca italiana nel settore della cybersicurezza all'interno di un quadro comparativo di ampiezza internazionale, includendo sia il contesto europeo sia quello globale. L'adozione di un *benchmark* multilivello consentirebbe di valutare in modo più rigoroso il posizionamento dell'Italia rispetto agli altri Paesi, identificando differenziali di performance, specializzazioni relative e possibili aree di ritardo o di eccellenza.

In una prospettiva di medio periodo, si prevede di proseguire la collaborazione tra ACN e ANVUR e di rendere periodica la pubblicazione del presente documento di analisi sullo stato della ricerca italiana in materia di cybersicurezza, progressivamente arricchendolo e aggiornandolo nei contenuti, nelle metodologie e nelle fonti utilizzate, in modo da fornire un supporto informativo stabile alle politiche pubbliche e alle decisioni in materia di ricerca in cybersicurezza in Italia.

Lista degli acronimi

5G	Quinta Generazione (di reti mobili)
ACN	Agenzia per la cybersicurezza nazionale
ANVUR	Agenzia nazionale per la valutazione del sistema universitario e della ricerca
CIVR	Comitato di Indirizzo per la Valutazione della Ricerca
CPS	*Cyber physical system*
CUN	Consiglio Universitario Nazionale
D.L.	Decreto Legge
D.Lgs.	Decreto Legislativo
D.M.	Decreto Ministeriale
EDT	*Emerging and Disruptive Technology*
EFTA	*European free trade association*
EPR	Ente pubblico di ricerca
UE	Unione Europea
GEV	Gruppi di Esperti Valutatori
GPAI	*General-purpose artificial intelligence*
GSD	Gruppo Scientifico-Disciplinare
IA	Intelligenza Artificiale
ICS	*Industrial Control System*
IoT	*Internet of Things*
MUR	Ministero dell'Università e della Ricerca
OT	*Operational Technology*
R&I	Ricerca e Innovazione
SSD	Settore Scientifico-Disciplinare
STEM	*Science, Technology, Engineering and Mathematics*
VQR	Valutazione della Qualità della Ricerca

ISBN 978-88-32041-10-1