AGENDA DI RICERCA E INNOVAZIONE

PER LA CYBERSICUREZZA

2023 – 2026

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

MUR
Ministero dell'Università e della Ricerca

Versione 1.0
(2023)

Autori:

Indice

Prefazione

"La cybersicurezza è una branca del sapere considerevolmente estesa poiché include diverse discipline quali l'informatica e l'ingegneria ma anche discipline umanistiche, sociologiche, economiche e legali. Inoltre, all'interno di ogni area sono presenti molte subaree e argomenti che contribuiscono all'avanzamento della frontiera della ricerca, sia di base che applicata.

*In tale contesto, un'**agenda di ricerca e innovazione (R&I) per la cybersicurezza** svolge il ruolo chiave di fissare gli argomenti di R&I prioritari per l'ecosistema italiano della ricerca sulla sicurezza cibernetica".*

Anna Maria Bernini
Ministro dell'Università e della Ricerca

*"Le tecnologie emergenti stanno progressivamente pervadendo il mondo fisico, le cui frontiere con lo spazio cibernetico diventano sempre più indefinite, ponendo nuove sfide nel preservare la Sicurezza Nazionale. **Proteggere il nostro Paese dalle minacce cibernetiche** è di vitale importanza ed è necessario farsi trovare pronti dinanzi a queste nuove sfide.*

*Per questo, dobbiamo **governare gli investimenti in R&I sulla cybersicurezza** nella direzione di costruire capacità che sono necessarie a proteggere l'Italia e, allo stesso tempo, **rafforzarne l'autonomia strategica e digitale**".*

Alfredo Mantovano
Sottosegretario di Stato alla Presidenza del Consiglio, Autorità Delegata per la Sicurezza della Repubblica

1 Introduzione

1 Introduzione

Vivere in un mondo digitale nel quale si interagisce con sistemi informativi e di comunicazione per ottimizzare le attività quotidiane rappresenta una straordinaria opportunità: la trasformazione digitale, infatti, abilita nuove modalità di lavoro, intrattenimento, viaggio e interazione. Assieme a questa positiva evoluzione delle nostre abitudini, però, sono emersi nuovi rischi di natura cibernetica, che continuano ad evolversi e a moltiplicarsi. In particolare, è possibile individuare due macrocategorie di rischi che devono essere tempestivamente gestite: i rischi tecnologici e i rischi connessi ad attacchi cibernetici.

I rischi tecnologici sono legati al grado di affidabilità (*trustworthiness*) di un fornitore di prodotti hardware e software. Anche per il nostro Paese, la produzione globalizzata di componenti per la tecnologia dell'informazione ha creato un sempre maggior numero di dipendenze che, se venissero meno, causerebbero un'interruzione delle catene di approvvigionamento con conseguenze negative sulla nostra economia. Per fronteggiare questi rischi, è importante mettere in campo azioni che puntino ad un rafforzamento dell'autonomia tecnologica strategica in ambito nazionale ed europeo, investendo sulla progettazione e sullo sviluppo di tecnologie affidabili, i cui anelli critici della catena di approvvigionamento si trovano su suolo italiano o in Paesi *like-minded*.

Riguardo agli attacchi cibernetici, il panorama delle minacce, sia in Italia che a livello mondiale, diventa di giorno in giorno più complesso e include svariati attori. Nello specifico, i singoli criminali cibernetici o i gruppi del cybercrimine organizzato conducono attività di hackeraggio per finalità economiche o di altro genere. Un esempio per tutti è quello del *ransomware*, ovvero quella particolare tipologia di malware utilizzata per crittografare i dati di un'organizzazione a scopo estorsivo: ad oggi è una delle minacce più diffuse sia in Italia[1] che in Europa[2]. In aggiunta, le tensioni geopolitiche continuano ad avere ricadute rilevanti in campo cibernetico: attori statuali ostili possono realizzare, ad esempio, campagne di disinformazione online oppure compromettere la capacità dello Stato di garantire servizi essenziali quali energia, acqua e trasporto a cittadini ed imprese. Tale scenario rende sempre più urgente il rafforzamento

[1] Si veda https://www.acn.gov.it/documents/ACN_Rel_Parlamento_2021.pdf.

[2] Disponibile (in inglese) al sito https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

degli strumenti a difesa delle infrastrutture critiche nazionali.

Per fronteggiare efficientemente ed efficacemente i rischi cibernetici, è necessario che le organizzazioni pubbliche e private investano nello sviluppo di capacità collettive per la tutela della cybersicurezza, che rappresenta un dominio vasto, estremamente interdisciplinare e in costante evoluzione. Le diverse aree di conoscenza della sicurezza cibernetica, dalla sicurezza dei dati agli aspetti di governo, sono tra loro interconnesse e determinano uno scenario complesso che richiede sforzi collegiali da parte di tutti i soggetti coinvolti nell'ecosistema della ricerca e innovazione (R&I) per tenere il passo con i rapidi cambiamenti delle nuove minacce presenti nel cyberspazio. Inoltre, gli avanzamenti tecnologici procedono speditamente e un Paese sviluppato come l'Italia, come anche il resto d'Europa, gioca un ruolo primario nella ricerca, sviluppo e industrializzazione di tecnologie emergenti quali l'intelligenza artificiale, il cloud e il *quantum computing*.

A questo proposito, l'Italia possiede straordinarie risorse di ricerca e industriali in tutti i settori: la sfida più grande è che tali risorse remino nella stessa direzione, collaborando sulla base di un piano strategico che renda (e mantenga) il nostro Paese un posto *cyber*-sicuro per la società. All'interno della "Strategia Nazionale di Cybersicurezza 2022-2026 – Piano di Implementazione"[3] redatta dall'Agenzia per la Cybersicurezza Nazionale (ACN) e adottata dal Presidente del Consiglio dei Ministri, diverse misure puntano a favorire la ricerca e l'innovazione tecnologica tramite collaborazioni tra entità pubbliche e private in Italia. Le due misure principali sono:

MISURA #53: *Promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.*

MISURA #54: *Favorire la ricerca e lo sviluppo, specialmente nelle nuove tecnologie, promuovendo l'inclusione dei principi di cybersicurezza e supportando, anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione, progetti di sicurezza cibernetica da parte del settore privato – con particolare riferimento alle startup e alle PMI innovative – e dei Centri di competenza e di ricerca attivi sul territorio nazionale.*

[3] Disponibile al sito https://www.acn.gov.it/ACN_Implementazione.pdf.

L'obiettivo finale è che il Governo Italiano, l'industria, il mondo accademico e l'intera società collaborino su iniziative di R&I atte a consolidare ed espandere le capacità nazionali nell'ambito della cybersicurezza, creando un ecosistema che sia in grado di migliorare le linee di difesa del Paese contro i possibili attacchi di origine cibernetica perpetrati da attori ostili.

Tra le entità responsabili per l'implementazione di queste misure strategiche c'è la stessa ACN, in qualità di Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nello spazio cibernetico secondo il D.L. 82/2021[4], la quale agisce in stretta cooperazione con i Ministeri e i soggetti governativi italiani interessati. In questo contesto, ACN ha identificato una tabella di marcia per il perseguimento degli obiettivi di R&I stabiliti dal documento di Strategia[3] che comprende tre fasi:

1. **La Fase#1** prevede la definizione di un'Agenda di R&I per la cybersicurezza che consideri le specificità del contesto nazionale. L'Agenda ha come obiettivo la creazione di una base di conoscenza condivisa da utilizzare per governare le attività di ricerca nazionali, fornendo cioè un riferimento per pianificare politiche di R&I in materia di cybersicurezza sia a favore del settore pubblico sia di quello privato.
2. **La Fase #2** prevede la creazione di una rete di soggetti di ricerca pubblici e privati con cui ACN intende cooperare nell'ottica di rafforzare la postura dell'ecosistema nazionale della R&I sulla cybersicurezza.
3. **La Fase #3** consiste nella creazione di un piano di investimenti per le attività di R&I basato su diversi strumenti e opportunità di finanziamento, con l'obiettivo di sviluppare nuove capacità e competenze nelle imprese e di colmare le carenze tecnologiche esistenti nel campo della cybersicurezza.

Il presente documento conclude la **Fase#1** con la pubblicazione dell'Agenda di R&I, frutto della collaborazione tra ACN e il Ministero dell'Università e della Ricerca (MUR). L'Agenda è caratterizzata da una lista di argomenti prioritari per le attività di R&I sulla sicurezza cibernetica, con un'attenzione specifica al contesto nazionale e con un orizzonte temporale che guarda al 2026. L'Agenda di R&I potrà essere aggiornata sulla base delle interazioni che avverranno in futuro con i soggetti coinvolti nelle diverse fasi di implementazione della tabella di marcia, oltre che, naturalmente, in relazione a nuovi argomenti che potrebbero emergere nel panorama della ricerca nazionale e internazionale. Pertanto, una versione aggiornata dell'Agenda sarà resa disponibile entro i primi tre mesi dell'anno a partire dal 2024 fino al 2026, con potenziali revisioni minori nel corso dei singoli anni.

Il documento è principalmente rivolto a tutti gli attori che operano direttamente o beneficiano della ricerca sulla cybersicurezza, sia nel settore pubblico (ad esempio, università, organizzazioni e consorzi di ricerca, pubbliche amministrazioni e organizzazioni anche europee e internazionali) sia del settore

[4] Disponibile al sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14;82.

privato (imprese e associazioni industriali).

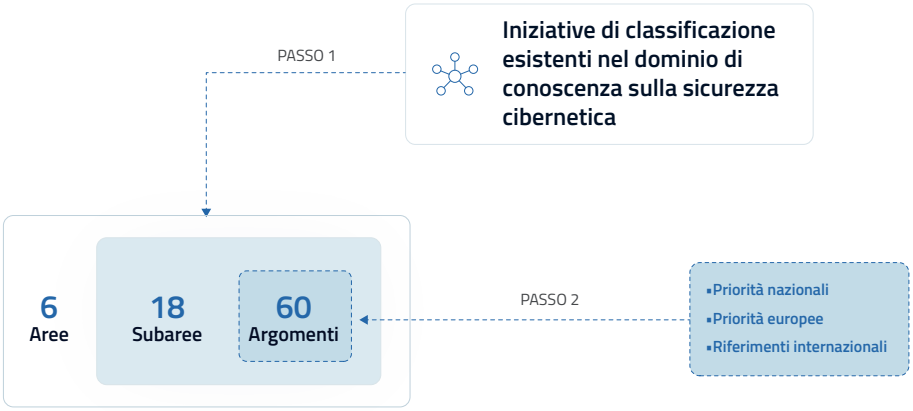
1.1. Metodologia

La predisposizione dell'Agenda di R&I è il risultato di un'attività di *desktop research* cui hanno preso parte articolazioni interne ad ACN e il MUR; a seguire sono stati raccolti riscontri da membri del Laboratorio Nazionale di Cybersecurity del CINI e dal comitato tecnico-scientifico dell'ACN, nonché da selezionati ricercatori che hanno fornito un contributo in fase di perfezionamento del documento. Come esplicitato nel seguito, sono state prese in considerazione come fonti le direzioni di ricerca sulla cybersicurezza individuate in Italia e in Europa; sono stati, inoltre, esaminati molti riferimenti internazionali su aree specifiche.

La metodologia di costruzione dell'Agenda è essenzialmente articolata in due passi:

- *l'identificazione delle aree* tramite raggruppamento ed indicazione delle corrispondenze con le iniziative di classificazione esistenti nel dominio di conoscenza della cybersicurezza[5];
- *la definizione delle subaree e dei relativi argomenti* tramite la valutazione sia delle priorità italiane ed europee[6] sia di riferimenti rilevanti sul piano internazionale.

Figura 1-1: Metodologia adottata.



[5] Il dettaglio della relazione tra le aree di R&I identificate e le iniziative di classificazione della conoscenza della cybersicurezza considerate si trova in appendice.

[6] Per quanto riguarda le priorità nazionali, il riferimento fondamentale è costituito dal Programma Nazionale per la Ricerca (PNR) (https://www.mur.gov.it/sites/default/files/2021-01/Pnr2021-27.pdf) del MUR, in particolare l'allegato esteso sulla sicurezza dei sistemi sociali (https://www.mur.gov.it/sites/default/files/2021-08/3.AllegatoEsteso_Sicurezza.pdf). Il MUR presenterà un aggiornamento del PNR nel corso del 2023, sottolineando ulteriori priorità in materia di sicurezza cibernetica. Per quanto riguarda le priorità europee, sono state considerate le indicazioni contenute nell'ultima versione del *Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation Needs and Priorities* (https://www.enisa.europa.eu/publications/research-and-innovation-brief) e in altri riferimenti dell'Agenzia dell'Unione Europea per la Cibersicurezza (ENISA).

Una rappresentazione grafica della metodologia descritta è illustrata in Figura 1-1, che riporta altresì una quantificazione delle aree, delle subaree e degli argomenti individuati, nello specifico:

- **6 aree;**
- **18 subaree**;
- **60 argomenti**.

Inoltre, è stata identificata una lista di cosiddette ***Emerging and Disruptive Technology*** **(EDT),** selezionate come rilevanti per la cybersicurezza in generale e utili ad indirizzare lo studio degli argomenti di ricerca proposti.

1.2. Struttura del documento

Il resto del documento è organizzato come segue.

- La Sezione 2 introduce le aree, le subaree e gli argomenti di R&I identificati.
- La Sezione 3 descrive le EDT rilevanti e le mette in corrispondenza con le subaree di R&I.
- Lista degli acronimi.
- Appendice.

2 Aree di Ricerca e Innovazione

2

Aree di Ricerca e Innovazione

Le aree di R&I sulla cybersicurezza identificate sono:

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

Le aree di R&I sono raffigurate in Figura 2–1, la quale evidenzia anche il ruolo trasversale che le EDT rivestono rispetto alle stesse.

Figura 2–1: relazione tra aree di R&I e EDT.

Di seguito, ogni area di R&I è presentata nel dettaglio.

2.1. Area#1: Sicurezza dei Dati e Privacy

La sicurezza dei dati è il processo che consente di preservare la riservatezza, l'integrità e la disponibilità (la cosiddetta triade RID) dei dati nel mondo digitale, in aggiunta ad altre caratteristiche quali l'autenticità, la responsabilità (*accountability*) e il non ripudio (*non repudiation*). In un numero sempre maggiore di casi, i servizi digitali che usiamo tutti i giorni, come ad esempio i servizi di acquisto online, i servizi di localizzazione per la navigazione, o le reti sociali, utilizzano dati personali[7] – anche detti *personally identifiable information* (PII[8]). Sebbene forniscano molti vantaggi ai loro utenti, questi servizi introducono rischi legati al trattamento dei dati, siano essi personali o meno. Questi rischi non possono essere trascurati, ma vanno accuratamente gestiti, soprattutto quando legati a servizi che sono parte di processi articolati in cui monitorare tutti i soggetti coinvolti diventa molto complesso.

L'area *Sicurezza dei Dati* e *Privacy* include tre subaree, descritte a seguire.

2.1.1. SUBAREA #1.1: INGEGNERIA DELLA PROTEZIONE DEI DATI

La protezione dei dati *by design* è un obbligo di legge in Europa a partire dalla piena operatività del GDPR nel 2018. Dal punto di vista tecnologico, sono adottate sempre più frequentemente nuove soluzioni per preservare la privacy, comunemente indicate come *Privacy-Enhancing Technology* (PET). Tuttavia, garantire un'efficace protezione dei dati *by design* richiede un approccio globale che contempli l'intero processo di elaborazione dei dati e sfrutti le PET in maniera corretta e tempestiva.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#1.1.1]** l'*elaborazione privacy-preserving dei dati*, basata su tecniche come, ad esempio, la crittografia omomorfica, la *Secure Multi-party Computation* (SMC), la *differential privacy*, la generazione di dati sintetici e soluzioni basate su sicurezza hardware come *Trusted Execution Environment* (TEE) (cfr. Sezione 2.4.1);
- **[Argomento#1.1.2]** la *memorizzazione privacy-preserving dei dati*, che prevede tecniche crittografiche applicate all'hardware (cfr. Sezione 2.4.1) e al software che gestisce i supporti di memorizzazione (cfr. Sezione 2.3.1);
- **[Argomento#1.1.3]** *l'autenticazione, l'autorizzazione e il controllo di accesso con garanzie di privacy aggiuntive,* sfruttando tecniche che aumentano il livello di protezione dei dati come, ad esempio, le *zero-knowledge proofs*.

[7] La definizione di dati personali secondo il GDPR è disponibile al sito https://gdpr.eu/article-4-definitions/.

[8] La definizione di PII secondo lo "US Office of Privacy and Open Government" è disponibile (in inglese) al sito https://www.osec.doc.gov/opog/privacy/PII_BII.html.

2.1.2. SUBAREA #1.2: CRITTOGRAFIA

La promozione dell'uso della crittografia, così come lo sviluppo di sistemi di crittografia nazionali in ambito non classificato, sono esplicitamente menzionati nella "Strategia Nazionale di Cybersicurezza 2022-2026 – Piano di Implementazione"[3,9]. Di recente, il campo della crittografia sta affrontando sfide importanti che derivano dai progressi del *quantum computing*. In questo campo, gli argomenti prioritari sono:

- **[Argomento#1.2.1]** la ricerca di nuove *primitive, algoritmi e protocolli per Post-Quantum Cryptography* (PQC)[10], che si focalizza sulla progettazione e sullo sviluppo di soluzioni adottabili dagli attuali elaboratori e dispositivi elettronici ma robuste nei confronti della crittoanalisi sia tradizionale sia quantistica. È di interesse anche studiare metodologie per identificare soluzioni crittografiche non resistenti ad attacchi di origine quantistica (*non-quantum-resistant*) e pianificare le relative strategie di migrazione in maniera agile. A tal proposito, si fa riferimento alla recente legislazione statunitense che affronta il tema della migrazione dei sistemi informatici delle agenzie esecutive alla PQC[11];
- **[Argomento#1.2.2]** studio della *crittografia quantistica*, che, al contrario della PQC, sfrutta le proprietà della fisica dei quanti per realizzare procedure crittografiche. Una delle sfide maggiori è la distribuzione di chiavi quantistiche (*Quantum Key Distribution* – QKD), che ha l'obiettivo di fornire una modalità per lo scambio di chiavi crittografiche con garanzie di sicurezza.

In aggiunta, meritano attenzione le soluzioni di crittografia omomorfica (*homomorphic encryption*), che rappresentano una forma di crittografia robusta rispetto ad attacchi quantistici (*quantum-safe*) e permettono di effettuare elaborazioni direttamente sui dati crittografati, senza la necessità di effettuare una preventiva decrittazione. In questo campo, l'argomento prioritario è:

[9] In particolare: Misura #22 (*Promuovere l'uso della crittografia in ambito non classificato, quale impostazione predefinita e comunque fin dalla fase di progettazione di reti, applicazioni e servizi, in conformità ai principi della sicurezza e della tutela della vita privata, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea*) e Misura #23 (*Sviluppo di tecnologie/sistemi di cifratura nazionale in ambito non classificato. A sostegno di tale iniziativa è prevista la creazione di un ecosistema nazionale per il suo mantenimento ed evoluzione*).

[10] Si veda il sito (in inglese) https://csrc.nist.gov/projects/post-quantum-cryptography.

[11] Si veda https://www.congress.gov/bill/117th-congress/house-bill/7535 (in inglese), diventato *Public Law* il 21/12/2022.

- **[Argomento#1.2.3]** la ricerca di schemi per la *Fully Homomorphic Encryption* (FHE), che possono essere applicati in scenari pratici come, ad esempio, nell'ambito del cloud computing.

Infine, come parte della continua evoluzione dello stato dell'arte degli algoritmi crittografici, si propone un ulteriore argomento prioritario riguardante

- **[Argomento#1.2.4]** nuove *funzioni crittografiche di hashing*, le quali, tra i possibili utilizzi, possono essere elementi costitutivi di alcuni schemi di crittografia omomorfica e sono impiegate nelle *blockchain* (cfr. Sezione 2.3.3).

2.1.3. SUBAREA #1.3: TRUSTED INFORMATION SHARING

La proposta di "Data Act"[12], come parte della strategia europea complessiva sui dati, è un importante passo in avanti per utilizzare pienamente il potenziale dei moderni ecosistemi di dati, in particolare facilitando la condivisione orizzontale tra diversi settori. Il regolamento rende obbligatoria la condivisione di dati per scopi ben definiti di pubblica utilità, vincolandola allo stesso tempo a determinate garanzie di diritti e interessi degli individui a cui i dati si riferiscono. Inoltre, nel'ambito della strategia europea sui dati, il "Data Governance Act"[13] introduce i *common European data space* come soluzioni specifiche per abilitare la condivisione ed il riuso dei dati.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#1.3.1]** l'*arricchimento delle soluzioni standard di interoperabilità semantica con controlli di sicurezza*, ad esempio, per garantire la confidenzialità e l'integrità dei dati;
- **[Argomento#1.3.2]** l'analisi di *soluzioni architetturali per trusted information sharing e storage*, sia per un settore specifico che per la condivisione dei dati tra settori, ad esempio tramite l'uso di PET che permettono di accedere ai dati in maniera *privacy-preserving* (cfr. Sezione 2.1.1). In particolare, le soluzioni di *trusted information storage* sono di estremo interesse con riferimento ad infrastrutture su scala nazionale che memorizzino copie sicure di dati pubblici e privati per garantire il ripristino da condizioni di disastro causate da incidenti cibernetici (cfr. Sezione 2.2.3).

[12] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

[13] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?pk_campaign=todays_OJ&pk_content=Regulation&pk_keyword=data+governance+act&pk_medium=TW&pk_source=EURLEX&uri=CELEX%3A32022R0868.

2.2. Area#2: Gestione delle Minacce Cibernetiche

Come riportato nell'ultimo rapporto sul "Threat Landscape" pubblicato dall'ENISA[2], gli attacchi cibernetici sono aumentati nella seconda metà del 2021 e nel 2022, non solo in termini di vettori e numerosità, ma anche in relazione all'entità dell'impatto causato, evidenziando una serie di minacce informatiche nuove, ibride ed emergenti. Il rapporto rileva le principali minacce e categorizza gli attori coinvolti, enfatizzando la crescita (i) dell'impatto della geopolitica sul panorama delle minacce alla sicurezza cibernetica, (ii) delle capacità degli attaccanti, (iii) del numero di attacchi contro la disponibilità dell'informazione e (iv) dell'impatto delle nuove minacce. In questo contesto, il ruolo dei *Security Operation Center* (SOC) è cruciale e necessita di essere ulteriormente rafforzato, come peraltro raccomandato anche dalla "Strategia Nazionale di Cybersicurezza 2022-2026 – Piano di Implementazione"[3,14].

L'area *Gestione delle Minacce Cibernetiche* include le quattro subaree descritte nel seguito.

2.2.1. SUBAREA #2.1: ATTACCO E DIFESA

Questa subarea tratta le tecniche che consentono il rilevamento degli attacchi cibernetici e le reazioni ad essi mirate a preservare l'operatività dei sistemi impattati.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#2.1.1]** le nuove *tecniche di attacco e misure di difesa* che possono essere applicate nelle diverse fasi di un attacco cibernetico quali, ad esempio, nuove misure di difesa contro attacchi di tipo Distributed Denial of Service (DDoS);
- **[Argomento#2.1.2]** *rilevamento e risposta contro i malware*, incluse tecniche specifiche per offuscare, de-offuscare e analizzare i malware, così come quadri procedurali per eseguire tali tecniche in maniera non bloccante sui sistemi impattati. Inoltre, in generale, sono da investigare nuove tecniche per l'identificazione di attività maliziose al fine di riconoscere prontamente tipologie di malware non ancora note, con l'inclusione di modelli di analisi statistica;

[14] Nello specifico, si veda la Misura #30 (*Realizzare un sistema di raccolta e analisi HyperSOC per aggregare, correlare ed analizzare eventi di sicurezza di interesse al fine di individuare precocemente eventuali "pattern" di attacco complessi, nonché abilitare una gestione del rischio cyber in chiave preventiva e integrata tra molteplici sorgenti dati, sfruttando anche infrastrutture di High Performance Computing e tecnologie di Intelligenza Artificiale e il machine learning*).

- **[Argomento#2.1.3]** la *messa in sicurezza di algoritmi e modelli per il machine learning*, studiando tecniche per migliorarne la robustezza rispetto a minacce quali gli *adversarial attacks*, ad esempio l'*adversarial model inference,* o la manipolazione dei dati utilizzati dai sistemi di machine learning come, ad esempio, il *data poisoning* e la *data exfiltration*[15];
- **[Argomento#2.1.4]** la ricerca sul cosiddetto *adversarial behaviour*, al fine di analizzare le motivazioni e le capacità degli attaccanti con particolare riferimento a tecniche e tecnologie utilizzate nelle attività ostili da loro condotte (delegando invece gli aspetti umani all'Area#5, cfr. Sezione 2.5.1).

2.2.2. SUBAREA#2.2: CYBERTHREAT INTELLIGENCE

Questa subarea si focalizza sulla raccolta e l'analisi informativa al fine di caratterizzare possibili minacce cibernetiche. La creazione di un servizio nazionale di monitoraggio delle minacce cibernetiche è esplicitamente menzionata nella "Strategia Nazionale di Cybersicurezza 2022-2026 – Piano di Implementazione"[3,16].

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#2.2.1]** l'utilizzo del *machine learning per la cyberthreat intelligence*, dove il *machine learning* è da intendersi in generale, a ricomprendere anche il cosiddetto *deep learning*. Sono incluse tecniche di machine learning per l'individuazione di malware, spam e tentativi di intrusione nei sistemi, oltre che altri utilizzi finalizzati in generale al contrasto degli attacchi cibernetici. In aggiunta, le tecniche di machine learning possono essere usate anche per la costruzione e l'aggiornamento di *knowledge graph* che, ad esempio, rappresentino e organizzino la conoscenza relativa agli attori ostili o alla cosiddetta impronta digitale (*digital footprint*) di un'organizzazione. Le soluzioni basate su machine learning necessitano di adeguati controlli di qualità e correttezza che devono essere applicati sia nelle fasi di addestramento che in quelle di identificazione delle *feature* dei modelli. Il machine learning può essere anche usato per potenziare strategie di attacco e sviluppare strategie di difesa: in questa accezione, sarà trattato nella Sezione 2.2.3. Questo argomento è esplicitamente menzionato nella "Strategia Nazionale di Cybersicurezza 2022-2026 – Piano di Implementazione"[3,17];

[15] Si faccia riferimento al sito https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms (in inglese).

[16] In particolare, si veda la Misura #13 (*Realizzare un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale, al fine di comunicare l'effettivo livello della minaccia, nonché di informare adeguatamente i processi decisionali*).

[17] In particolare, si veda la Misura #32 (*Creare un'infrastruttura di High Performance Computing dedicata alla cybersecurity nazionale per il potenziamento dei servizi cyber nazionali dell'Agenzia, nonché lo sviluppo di strumenti di simulazione, basati sull'Intelligenza Artificiale e il machine learning, per supportare le fasi di prevenzione, scoperta, risposta e predizione degli impatti di attacchi cyber di natura sistemica*).

- **[Argomento#2.2.2]** la ricerca di nuove *metodologie per monitorare la disinformazione*, come parte di una strategia globale per mitigare l'impatto delle *fake news* o di altri tipi di contenuti falsi, anche di tipo audio, video e fotografico (ad esempio, i cosiddetti *deepfakes*), creati e condivisi da attori ostili per destabilizzare l'opinione pubblica. Sono incluse come metodologie di interesse le recenti proposte basate su modelli generativi del linguaggio[18];
- **[Argomento#2.2.3]** le metodologie per l'*attribuzione di attacchi alla sicurezza cibernetica*, finalizzate al tracciamento e all'identificazione delle attività dell'attaccante, anche nell'ottica di supportare operazioni di profilazione nell'ambito di indagini investigative (cfr. Sezioni 2.2.1 e 2.5.1).

2.2.3. SUBAREA #2.3: GESTIONE DEGLI INCIDENTI E OPERAZIONI DI SICUREZZA

Secondo il recente "Threat Landscape" dell'ENISA[2], i beni ICT, e in generale la popolazione europea, sono ormai oggetto di un numero di incidenti cibernetici rilevati stabilmente elevato. In particolare, sono state registrate operazioni cibernetiche ostili contro infrastrutture critiche al fine primario di ottenere informazioni confidenziali, ma anche di diffondere nuovo malware e interrompere servizi e funzioni essenziali. Pertanto, in questo contesto, è importante stabilire e perfezionare approcci destinati a (i) rispondere agli incidenti e (ii) condurre operazioni efficaci di rafforzamento della sicurezza su sistemi cibernetici e cyber-fisici.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#2.3.1]** la *resilienza dei sistemi cyber-fisici*, che comprende (i) il rafforzamento della consapevolezza situazionale (*situational awareness*) tramite il miglioramento delle attuali (o nuove) metodologie che consentano una percezione aumentata del contesto per il personale operativo, sfruttando strumenti quali, ad esempio, sistemi SIEM – *Security Information and Event Management* e SOAR – *Security Orchestration, Automation and Response*; (ii) la progettazione di processi e procedure per gestire la risposta agli incidenti di sicurezza contro i sistemi cyber-fisici, incluse le infrastrutture critiche;

[18] Per approfondimenti, si veda, ad esempio, l'articolo (in inglese) di R. M. Samant, M. R. Bachute, S. Gite and K. Kotecha, "Framework for Deep Learning-Based Language Models Using Multi-Task Learning in Natural Language Understanding: A Systematic Literature Review and Future Directions," in IEEE Access, vol. 10, pp. 17078-17097, febbraio 2022.

- **[Argomento#2.3.2]** l'*automazione via machine learning dei sistemi tradizionali*, inclusi, ad esempio, i SIEM e i sistemi antintrusione (*Intrusion Prevention Systems* – IPS), al fine di migliorarne sia l'efficacia (ad esempio, rimuovendo le dipendenze da controlli statici secondo regole predefinite) che l'efficienza, grazie a funzioni più automatizzate;
- **[Argomento#2.3.3]** le nuove *strategie di difesa* da adottare a valle di fasi di progettazione già condotte o in contesti ibridi quali, ad esempio, il telelavoro, utilizzando sistemi di gestione delle infrastrutture digitali resilienti e adattativi. Questo argomento include anche le strategie di difesa in risposta ad attacchi potenziati dal machine learning, che presentano una combinazione di velocità, scala, automazione e sofisticazione tale da richiedere risposte innovative.

2.2.4. SUBAREA #2.4: SCIENZE FORENSI DIGITALI

A seguito di un incidente di sicurezza, si attua dapprima una fase di reazione che comporta decisioni e azioni di contenimento e successivamente un'ulteriore fase che consiste nell'analisi a posteriori di ciò che si è verificato, per scopi investigativi e al fine di migliorare la postura cibernetica dell'infrastruttura impattata dall'incidente. Questa importante fase di analisi è effettuata sfruttando tecniche di scienze forensi digitali, ossia procedure informatiche e investigative che esaminano prove digitali garantendo autorità, catena di custodia, utilizzo di strumenti validati, ripetibilità e sfruttando reportistica, verifiche matematiche e testimonianze di esperti[19]. Le tecniche a garanzia delle prove digitali da utilizzare nell'ambito di procedure legali sono trattate anche dalla comunità di standardizzazione[20].

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#2.4.1]** i nuovi approcci per gestire la complessità dei *processi di scienze forensi digitali*, i quali debbono far fronte all'acquisizione, all'archiviazione e all'elaborazione di una grande quantità di prove digitali, nonché alla dispersione delle informazioni in diversi luoghi fisici o virtuali;
- **[Argomento#2.4.2]** lo sviluppo di *contromisure per aggirare le tecniche antiforensi* che impediscono alle forze dell'ordine di indagare sui criminali cibernetici.

19 Definizione tratta dal sito https://csrc.nist.gov/glossary/term/digital_forensics (in inglese).

20 Si veda, per esempio, https://www.etsi.org/deliver/etsi_ts/103600_103699/103643/01.02.01_60/ts_103643v010201p.pdf (in inglese).

2.3. Area#3: Sicurezza del Software e delle Piattaforme

Il software sta progressivamente permeando tutti gli aspetti della vita quotidiana e, specialmente in alcuni contesti importanti quali, ad esempio, la guida autonoma, la sua affidabilità è sempre più essenziale. Infatti, le vulnerabilità che affliggono il codice sorgente o che possono essere introdotte tramite dipendenze da terze parti potrebbero danneggiare severamente gli utilizzatori finali, al punto tale da metterne a rischio l'incolumità fisica. A tal riguardo, è necessario ricordare che gli sviluppi di software e piattaforme nativamente nazionali o europei sono limitati.

L'area *Sicurezza del Software e delle Piattaforme* include tre subaree, descritte di seguito.

2.3.1. SUBAREA #3.1: SICUREZZA NELLO SVILUPPO E TEST DEL SOFTWARE

Ad oggi, il paradigma *DevOps* garantisce un aumento del grado di efficienza e automazione dei rilasci delle applicazioni software, che avvengono direttamente in ambiente di produzione, a valle di ogni iterazione di sviluppo. Per questo motivo, la presenza eventuale di vulnerabilità all'interno del software, di natura volontaria o involontaria, può essere estremamente dannosa per l'intero ambiente di produzione, specialmente se parte di infrastrutture critiche digitali (cfr. Sezione 2.4). Standard internazionali quali l'ISO/IEC 27001[21] e la *Special Publication* 800-160[22] del NIST affrontano questo problema.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#3.1.1]** i nuovi *linguaggi di programmazione security-aware*, basati su modelli semantici che consentano di formalizzare, collaudare e certificare i meccanismi di sicurezza adottati *by design*;
- **[Argomento#3.1.2]** le pratiche innovative di *gestione sicura del ciclo di vita del software* (*secure software development lifecycle*), che comprendono strumenti basati su machine learning per l'automazione dei controlli di sicurezza sul codice sorgente (cfr. Sezione 2.2.2), miglioramenti della sicurezza di applicazioni web e browser, anche tramite nuove tecniche per il rilevamento di bug a livello logico, l'applicazione di tecniche di *hardening* del codice e del *software bill of materials* (SBOM). In aggiunta, è di interesse anche l'adozione di *cyber-range* come ambiente sicuro per lo sviluppo e la verifica della postura di sicurezza di nuovi programmi, oltre all'uso primario dei cyber-range che è quello in ambito

[21] Per approfondimenti si veda il sito https://www.iso.org/isoiec-27001-information-security.html (in inglese).

[22] Disponibile al sito https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/final (in inglese).

formativo (cfr. Sezione 2.5.2);

- **[Argomento#3.1.3]** lo studio del *paradigma dell'open cloud*, fattore abilitante del trasferimento del software (*lift-and-shift*) tra cloud privati e pubblici e tra diversi fornitori di cloud pubblico;
- **[Argomento#3.1.4]** le *tecniche per rilevare vulnerabilità di sicurezza nel firmware e nei file binari*, i quali dovrebbero essere approfonditamente vagliati nel momento in cui il codice sorgente non è accessibile, al fine di rilevare bug e *backdoor*, assicurandone così la conformità al comportamento dichiarato o atteso dal fornitore. In particolare, tra le tecniche di interesse si menzionano quelle atte a favorire (i) il rilevamento di vulnerabilità di sicurezza, bug o backdoor utilizzando analisi statica e dinamica di file binari e firmware, (ii) l'analisi dei file binari da parte di uno sviluppatore terzo e (iii) l'hardening dei file binari stessi.

2.3.2. SUBAREA #3.2: SICUREZZA NEI SISTEMI OPERATIVI E TECNOLOGIE DI VIRTUALIZZAZIONE

Oltre ad essere eseguiti su un sistema operativo *host* (installazione su *bare metal*), oggigiorno i programmi sfruttano sempre più il paradigma del *cloud computing*, appoggiandosi a servizi sistemistici infrastrutturali (*Infrastructure* o *Containers-as-a-Service* – IaaS o CaaS, rispettivamente), a servizi di piattaforme computazionali (*Platform-as-a-Service* – PaaS), oppure a servizi applicativi (*Software-as-a-Service* – SaaS).

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#3.2.1]** la *sicurezza dei nuovi approcci alla virtualizzazione*, in grado di orchestrare il carico computazionale dei programmi in maniera sempre più trasparente. Dal punto di vista della sicurezza cibernetica, tali paradigmi divengono di massima importanza nel momento in cui sono utilizzati per orchestrare programmi per il calcolo e la comunicazione nel continuum cloud-edge. Pertanto, essi richiedono studi approfonditi su approcci di sicurezza *by design* che includano, ad esempio, la progettazione e l'applicazione di politiche di controllo degli accessi basate sui ruoli. Si sottolinea che, ai fini della resilienza, è importante focalizzare l'attenzione sull'*edge cloud*, che rappresenta un'infrastruttura vitale per il Paese nell'assicurare la continuità delle applicazioni a bassa latenza a dispetto di potenziali guasti o attacchi alle dorsali di rete internazionali;
- **[Argomento#3.2.2]** la progettazione di nuovi *modelli di protezione per la sicurezza delle piattaforme* e l'aggiornamento continuo dei modelli esistenti, dove quest'ultimo obiettivo costituisce un'attività cruciale data la già menzionata rapida evoluzione dei sistemi operativi e delle piattaforme di virtualizzazione. Pertanto, sono richiesti ulteriori sforzi nell'adozione di approcci di hardening basati su linee guida di implementazione sicura (*Security Technical Implementation Guidelines* – STIG) e nella progettazione di nuovi ed efficaci meccanismi di *observability* per la sicurezza, eventualmente accoppiati con l'hardware sottostante (cfr. Sezione 2.4.1).

2.3.3. SUBAREA #3.3: BLOCKCHAIN

La blockchain costituisce il primo e più diffuso esempio di tecnologia a registro distribuito (*Distributed Ledger Technology* – DLT), ovvero un sistema distribuito che consente ai partecipanti (definiti *nodi*) di inviare, validare e conservare informazioni su una base di dati condivisa, senza dipendere da un nodo centrale. A seconda del modello di autorizzazione adottato per la rete di nodi, una DLT può prevedere libera ammissione (*permissionless DLT*) o restrizioni all'ammissione (*permissioned DLT*)[23] alla rete di nodi. In particolare, la blockchain implementa una DLT in cui gli insiemi di dati conservati formano una catena di blocchi collegati tra loro tramite *hash* crittografici, i quali dimostrano in modo inequivocabile lo storico delle transazioni che avvengono tra i nodi della rete. Dati i numerosi possibili casi d'uso che potrebbero beneficiare della blockchain, la comunità di R&I è estremamente attiva in questo campo[24].

In questa subarea, oltre alle questioni menzionate in precedenza riguardo lo sviluppo sicuro di software e piattaforme, gli argomenti prioritari sono i seguenti:

- **[Argomento#3.3.1]** le soluzioni ai *problemi di sicurezza degli algoritmi di consenso e mining*, ad esempio, *peer flooding*, *network partitioning*, *block reorganization* e *Byzantine faults*;
- **[Argomento#3.3.2]** le *tecnologie per smart contract* che comprendano la progettazione e lo sviluppo di nuovi linguaggi di programmazione sicuri (cfr. Sezione 2.3.1) in grado di assicurare l'efficacia dell'implementazione di *smart contract* nei nodi della blockchain;
- **[Argomento#3.3.3]** le *tecniche di crittografia e anonimizzazione* per blockchain al fine di proteggere, dove applicabile, le transazioni pubblicate sulla blockchain e le identità delle parti coinvolte;
- **[Argomento#3.3.4]** lo studio dell'*economia delle blockchain* che comprenda l'identificazione di casi d'uso appropriati per la blockchain, anche a seconda delle politiche di autorizzazione sopra menzionate.

[23] Si veda, ad esempio, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf (in inglese).

[24] Si veda, ad esempio, https://www.cylab.cmu.edu/research/blockchain/research.html (in inglese).

2.4. Area#4: Sicurezza delle Infrastrutture Digitali

Le infrastrutture digitali ricoprono un ruolo importante per la società dal momento che abilitano lo scambio di informazioni (siano essere caratterizzate dalla presenza di dati personali o meno, cfr. Sezione 2.1) tra diverse istanze di software e piattaforme (cfr. Sezione 2.3). Per questo motivo, è fondamentale tenere in dovuta considerazione la sicurezza degli apparati ICT che compongono le infrastrutture digitali per assicurare la resilienza cibernetica dei sistemi informativi nel loro complesso.

L'area *Sicurezza delle Infrastrutture Digitali* include due subaree, descritte in seguito.

2.4.1. SUBAREA #4.1: HARDWARE

Le infrastrutture digitali sono primariamente costituite da componenti hardware quali dispositivi per gli utenti e apparati per centri di elaborazione dati che offrono servizi *on-premise* oppure in cloud.

Mentre la sicurezza del software e delle piattaforme che operano su tale hardware sono trattate in Sezione 2.3, gli argomenti prioritari riguardanti specificamente la sicurezza hardware sono i seguenti:

- **[Argomento#4.1.1]** lo studio di *vulnerabilità e attacchi indotti dall'hardware* che comprende, ad esempio, la progettazione e lo sviluppo di metodi di test a scatola chiusa (*black box testing*) o aperta (*white box testing*), inclusa la verifica formale dell'hardware, ai fini di rilevare hardware malevolo e *hardware trojan*, e l'identificazione di nuovi attacchi a livello hardware che sfruttino canali laterali (*side channels*) per sottrarre informazioni sensibili;
- **[Argomento#4.1.2]** lo studio di *approcci di sicurezza cibernetica ancorati all'hardware (hardware-anchored)* che possano sostanzialmente rafforzare il senso di fiducia (*trust*) verso algoritmi di autenticazione. I TEE rientrano anch'essi nell'ambito di interesse. È altresì incoraggiato lo sviluppo di primitive di sicurezza hardware, tra cui le funzioni fisiche non clonabili (*physically unclonable functions* – PUF) per la generazione di firme univoche per i circuiti integrati;
- **[Argomento#4.1.3]** la ricerca su nuovi *modelli per il rilevamento sicuro dei dati (safe sensing approaches)*, ai fini di assicurare la generazione sicura di dati da parte di nodi sensori e la loro integrità durante la fase di trasmissione grazie a tecnologie IoT affidabili;
- **[Argomento#4.1.4]** la progettazione di *architetture hardware aperte* ai fini di rafforzare il senso di fiducia nell'hardware e supportare l'ecosistema industriale nazionale e, più in generale, europeo, prevenendo la contraffazione dell'hardware e la dipendenza tecnologica da fornitori non affidabili (*vendor lock-in*).

2.4.2. SUBAREA #4.2: RETI

Le reti di telecomunicazioni consentono lo scambio sicuro di informazioni tra sistemi. Mentre i nodi di una rete consistono sia di componenti hardware (cfr. Sezione 2.4.1) che software (cfr. Sezione 2.3), le reti meritano una considerazione a parte, con una subarea dedicata, a motivo della peculiarità e criticità delle funzioni che svolgono e che le rendono obiettivo di minacce specifiche (cfr. Sezione 2.2.2).

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#4.2.1]** il *miglioramento della sicurezza e della resilienza di rete*, perseguendo diversi obiettivi. Anzitutto, assicurare l'evoluzione della sicurezza nelle tecnologie *wireless* più diffuse come, ad esempio, identificazione a radiofrequenza (*Radio-Frequency Identification* – RFID), *Near-Field Communication* (NFC), sistemi radar e sistemi satellitari globali di navigazione (*Global Navigation Satellite Systems* – GNSS). In secondo luogo, accelerare l'adozione dei principali standard Internet e la progettazione di nuovi meccanismi per il rilevamento degli attacchi cibernetici, compresi approcci basati su capacità di machine learning, al fine di incorporarli in nuovi protocolli di rete *by design.* Infine, favorire la creazione di servizi di rete diversificati quali, ad esempio, il Domain Name System (DNS), per il rafforzamento dell'autonomia tecnologica;
- **[Argomento#4.2.2]** nuovi *approcci per la sicurezza dei sistemi IoT*, che comprendono, ad esempio, la sicurezza degli aggiornamenti firmware *over-the-air* (OTA), il rilevamento di attacchi di *jamming* e relative contromisure, approcci per la sicurezza allo strato fisico (*physical layer security*) la diversificazione delle piattaforme IoT, il tutto al fine di stabilire canali di comunicazione autenticati e resilienti considerando i tipici vincoli IoT in termini di energia, *storage,* latenza e larghezza di banda;
- **[Argomento#4.2.3]** il *rafforzamento della sicurezza delle reti di telecomunicazioni cellulari*, favorendo l'adozione della sicurezza *by design* a livello di specifiche tecniche (cfr. Sezione 2.6.3) e a livello implementativo, sviluppando, ad esempio, sistemi di collaudo atti a rilevare potenziali vulnerabilità legate alle caratteristiche della tecnologia di rete mobile;
- **[Argomento#4.2.4]** lo *sviluppo di infrastrutture per la comunicazione quantistica* (*quantum communication infrastructures* – QCI) allo scopo di costruire una rete con tecnologia nazionale e, in generale, europea, la quale consenta di trasmettere informazioni tramite crittografia ultrasicura (QKD, cfr. Sezione 2.1.2) proteggendosi da attacchi cibernetici.

2.5. Area#5: Aspetti della Società

Come menzionato dal "Threat Landscape" dell'ENISA[2], secondo il *Verizon Data Breach Investigations Report* (DBIR[25]) l'82% delle violazioni cibernetiche coinvolge il fattore umano e non meno del 60% delle violazioni in Europa, Medio Oriente e Africa coinvolge la componente di ingegneria sociale (*social engineering*), per mezzo della quale gli attaccanti adescano gli utenti facendo loro aprire documenti, file o e-mail, visitare pagine web o concedere accesso a sistemi o servizi a persone non autorizzate. Lo scopo di tali attacchi di ingegneria sociale è quello di ottenere accesso a informazioni specifiche, ma anche di realizzare profitto illecitamente.

L'area *Aspetti della Società* include tre subaree, descritte in seguito.

2.5.1. SUBAREA #5.1: ASPETTI UMANI

Questa subarea si focalizza principalmente sulle persone come soggetti che rischiano di subire un attacco cibernetico, cercando modi per migliorare la loro postura di cybersicurezza. D'altro canto, questo non può prescindere da un'analisi delle motivazioni e degli incentivi che si celano dietro i comportamenti degli attaccanti, richiedendo un approccio interdisciplinare con un forte accoppiamento con la tecnologia (cfr. Sezione 2.2.1).

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#5.1.1]** la *ridefinizione dei confini dell'interazione uomo-macchina* e i relativi rischi di sicurezza;
- **[Argomento#5.1.2]** il *miglioramento della percezione del rischio* di attacchi cibernetici da parte dei cittadini, sfruttando, ad esempio, modelli psicologici;
- **[Argomento#5.1.3]** le *metodologie per la prevenzione degli attacchi di ingegneria sociale* e riduzione dei rischi legati all'uomo, anche considerando i recenti avanzamenti nei modelli generativi del linguaggio[18] che, ad esempio, permettono di creare messaggi e-mail maliziosi in maniera automatica (cfr. Sezione 2.2.2);
- **[Argomento#5.1.4]** *favorire l'accettazione di politiche e tecnologie di sicurezza da parte degli utenti finali*, prendendo in considerazione il paradigma della "sicurezza utilizzabile" (*usable security*) ed estendendo l'approccio basato sulla tecnologia con aspetti psicologici;

25 Disponibile al sito https://www.verizon.com/business/resources/reports/dbir/ (in inglese).

- **[Argomento#5.1.5]** la *profilazione dell'attaccante*, identificando le categorie di attaccanti e utilizzando tale informazione in fase sia di prevenzione che di risposta.

2.5.2. SUBAREA #5.2: ASPETTI FORMATIVI

La forza lavoro nel dominio della cybersicurezza manca di un sufficiente numero di professionisti che siano dotati delle competenze e della formazione necessarie ad affrontare le sfide correnti. Ciò comporta un enorme rischio per le imprese, il Governo Italiano e l'intera società.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#5.2.1]** la definizione di *metodologie per la valutazione e lo sviluppo di competenze di cybersicurezza e per l'identificazione delle competenze per le professioni legate alla cybersicurezza*;
- **[Argomento#5.2.2]** lo studio di nuovi *modelli e strumenti per la consapevolezza* (awareness) *della cybersicurezza*, quali, ad esempio, *serious games*, che possano sostenere dal punto di vista tecnologico campagne informative atte a sensibilizzare i cittadini nelle loro esperienze quotidiane di sperimentazione dello spazio cibernetico, andando verso una cultura dello *zero trust*;
- **[Argomento#5.2.3]** lo studio di nuovi *modelli e strumenti per la formazione sulla cybersicurezza*, in considerazione della complessità di tale mondo, che sempre più richiede strumenti didattici dedicati come, ad esempio, i cyber-range, che forniscano un ambiente sicuro e legale per acquisire competenze pratiche sulla sicurezza cibernetica.

2.5.3. SUBAREA #5.3: ASPETTI LEGALI

Sta emergendo con forza la necessità di iniziative di carattere normativo che contrastino l'utilizzo improprio della tecnologia, la distribuzione illecita di materiale sottratto durante una violazione dei dati (*data breach*), potenzialmente coperto da diritti di proprietà intellettuale, e il cybercrimine.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#5.3.1]** *regole e principi etici per uno spazio cibernetico sicuro*, che riguardino, ad esempio, i confini nell'utilizzo di applicazioni di intelligenza artificiale come previsto dall'"AI Act"[26];

[26] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

- **[Argomento#5.3.2]** *modelli e regole per favorire l'autonomia strategica* quali, ad esempio, lo "European Chips Act"[27] e le "US reviews of critical supply chains"[28];
- **[Argomento#5.3.3]** *modelli e regole per il governo del cyberspazio* inclusivi, ad esempio, di una disciplina normativa del rischio, di disposizioni sulla disinformazione nello spazio cibernetico, di regolamenti internazionali ed europei che garantiscano una *leadership* del cyberspazio sicuro e regole per meglio gestire scenari transfrontalieri (cfr. Sezione 2.2.4).

[27] Disponibile al sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0046.

[28] Si faccia riferimento ai rapporti disponibili al sito https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf e al sito https://www.commerce.gov/sites/default/files/2022-02/Assessment-Critical-Supply-Chains-Supporting-US-ICT-Industry.pdf (entrambi in inglese).

2.6. Area#6: Aspetti di Governo

In considerazione della varietà di minacce alla sicurezza cibernetica e della complessità del loro trattamento (cfr. Sezione 2.2), sono stati proposti diversi sistemi di gestione della sicurezza delle informazioni tra i quali si segnalano lo standard ISO/IEC 27001 (e correlati)[21], il *Cybersecurity Framework* del NIST[29] e il Framework Nazionale per la Cyber Security e la Data Protection[30]. Si evidenzia come l'efficacia di tali sistemi di gestione è massima solo se essi sono applicati a tutti i processi di un'organizzazione e dal numero maggiore possibile di organizzazioni sia del settore pubblico che di quello privato.

L'area *Aspetti di Governo* include tre subaree, descritte di seguito.

2.6.1. SUBAREA #6.1: ASPETTI ORGANIZZATIVI

Questa subarea tratta le politiche di indirizzo, i processi e le procedure che, tramite appropriate metodologie e strumenti, garantiscono che un sistema di gestione della sicurezza delle informazioni persegua obiettivi di sicurezza fissati.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#6.1.1]** la ricerca sull'*economia dell'ecosistema della cybersicurezza e*, in particolare, *delle catene di approvvigionamento* (*supply chain*);
- **[Argomento#6.1.2]** l'innovazione nelle *metodologie per il raggiungimento degli obiettivi di cybersicurezza*, al fine di implementare politiche di governo che includano, ad esempio, la possibilità di avvalersi della difesa attiva contro gli attacchi cibernetici;
- **[Argomento#6.1.3]** l'innovazione nelle *metodologie per gli audit di cybersicurezza*;
- **[Argomento#6.1.4]** l'innovazione nei modelli a supporto della *continuità operativa* (*business continuity*) *e* del *recupero dal disastro* (*disaster recovery*) per rafforzare la resilienza cibernetica.

[29] Si veda il sito https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide (in inglese).

[30] Si veda il sito https://www.cybersecurityframework.it/framework2.

2.6.2. SUBAREA #6.2: GESTIONE DEL RISCHIO

Come parte degli aspetti di governo, una subarea cruciale è la gestione dei rischi associati alla possibilità che una o più minacce alla sicurezza cibernetica (cfr. Sezione 2.2) sfruttino vulnerabilità presenti su uno o più apparati ICT, causando quindi un danno al singolo individuo o all'intera organizzazione, sia essa parte del settore pubblico o privato.

In questa subarea, gli argomenti prioritari sono i seguenti:

- **[Argomento#6.2.1]** lo studio e il miglioramento continuo dei *quadri procedurali per la valutazione del rischio*[31], al fine di facilitare l'identificazione, l'analisi e la quantificazione del rischio rendendo quindi più efficace il relativo piano di trattamento (e l'accettazione del rischio ove ragionevole). In particolare, rientrano in questo argomento di R&I i modelli per la valutazione d'impatto;
- **[Argomento#6.2.2]** lo studio e il miglioramento continuo della misurazione di *key performance indicator* (KPI) *sulla sicurezza cibernetica*, inclusi strumenti per la loro raccolta e visualizzazione al fine di facilitare il monitoraggio e la revisione del rischio;
- **[Argomento#6.2.3]** la *gestione del rischio e* l'*analisi delle reti di catene di approvvigionamento* (*supply chain network*), al fine di sviluppare modelli di rischio che considerino i possibili effetti a cascata derivanti da eventi avversi cibernetici che coinvolgono tali reti. Questi modelli dovrebbero evidenziare rilevanti dipendenze funzionali tra soggetti e prodotti sfruttando, ad esempio, le SBOM dei prodotti ICT (cfr. Sezione 2.3.1) e, in questo modo, essere applicabili anche a livello nazionale e internazionale (cfr. Sezione 2.2.3). Tali studi completano le analisi strategiche menzionate in precedenza, dipingendo un quadro esaustivo del rischio per settore economico, incluso quello legato alla catena d'approvvigionamento (cfr. Sezioni 2.5.3 and 2.6.1).

2.6.3. SUBAREA #6.3: STANDARDIZZAZIONE

Molti sistemi complessi del mondo digitale richiedono che valga il requisito di interoperabilità tra diversi produttori. Al fine di assicurare il raggiungimento dell'interoperabilità è necessario promuovere e supportare politiche e standard aperti internazionali quali, ad esempio, le specifiche tecniche emanate dal 3GPP per le reti di telecomunicazioni cellulari.

In questa subarea, gli argomenti prioritari sono i seguenti:

[31] Importanti quadri procedurali esistenti sono l'ISO/IEC 27005 (https://www.iso.org/standard/80585.html), il "Digital Operational Resilience Act" (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554), le *Special Publication* del NIST 800-30 (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final), 800-53 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final), 800-82 (https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final), e lo standard ISA 62443 (3-2) (https://www.isa.org/products/ansi-isa-62443-3-2-2020-security-for-industrial-a).

- **[Argomento#6.3.1]** l'innovazione nella *standardizzazione dei processi aziendali per la cybersicurezza*, sfruttando, ad esempio, i *Capability Maturity Model* (CMM) e i modelli di sicurezza *zero trust*;
- **[Argomento#6.3.2]** lo *sviluppo di standard di sicurezza cibernetica specifici per le singole tecnologie*, al fine di monitorare e rilevare proattivamente possibili vulnerabilità *by design* introdotte nelle specifiche tecniche da attori ostili[32];
- **[Argomento#6.3.3]** la *formalizzazione delle specifiche tecniche* scritte in linguaggio naturale attraverso linguaggi formali.

[32] Si veda il rapporto del CISA alla pagina https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf (in inglese).

3 Aree di R&I e EDT

3

Aree di R&I e EDT

A valle dell'illustrazione delle aree di R&I, identifichiamo a seguire la lista delle EDT che sono rilevanti per lo studio dei vari argomenti facenti parte delle aree. 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. Si sottolinea che alcune EDT potrebbero essere considerate come argomenti di ricerca a sé stanti, come ad esempio il machine learning; tuttavia, è stato ritenuto d'interesse trattarle indipendentemente dagli argomenti di R&I identificati per rendere esplicito come esse contribuiscono alla ricerca sulla sicurezza cibernetica. Inoltre, alcune EDT sono parte di domini più ampi: ad esempio, machine learning, rappresentazione della conoscenza, robotica e sistemi autonomi contribuiscono al dominio più ampio dell'*intelligenza artificiale*.

In questa sezione è disponibile prima di tutto una lista di EDT ritenute rilevanti, assieme ad una descrizione per ciascuna di esse. Quindi, le EDT sono messe in relazione con le subaree di R&I, evidenziando come esse contribuiscono ad indirizzare (o supportando o vincolando) gli argomenti all'interno delle subaree.

3.1. EDT Rilevanti: Descrizioni

La Tabella 3-1 contiene la lista delle EDT con la rispettiva descrizione.

Tabella 3-1: descrizioni delle EDT.

EDT (ordine alfabetico in inglese)	Descrizione
***5G and beyond mobile networks* – Reti mobili 5G e successive**	La quinta generazione delle reti wireless a lungo raggio per terminali mobili ha migliorato la qualità del servizio a banda larga e introdotto il supporto nativo per l'IoT industriale (si veda descrizione dell'IoT come EDT a sé stante) e l'utilizzo delle reti mobili a scopo non pubblico (*non-public networks*). Le successive generazioni (ovvero 5G-Advanced e sesta generazione) amplieranno ulteriormente le capacità della tecnologia al fine di mantenere la promessa dell'*Internet of Everything*[33].

[33] Per approfondimenti, si veda la pagina https://www.3gpp.org/ftp/Inbox/Marcoms/3GPP_Poster%20v2.pdf (in inglese).

EDT (ordine alfabetico in inglese)	Descrizione
Business Process Management (BPM) – Gestione dei processi aziendali	Insieme di principi, metodi e strumenti per progettare, analizzare e monitorare i processi aziendali, ovvero raccolte di eventi, attività e decisioni che coinvolgono un gran numero di attori e risorse e che portano collettivamente ad un risultato di valore per l'organizzazione o i suoi clienti[34].
Data science	Approcci di analisi dei dati, inclusi modelli statistici e di machine learning (quest'ultimo anche trattato come EDT a sé stante); metodi di preparazione dei dati (*data preparation*), di qualità e integrazione dei dati, nonché di memorizzazione degli stessi.
DevSecOps	Sebbene introdotta recentemente, la pratica *DevOps* è stata ampiamente adottata da industrie e governi grazie all'agilità che offre per mantenere il ritmo dell'innovazione. In particolare, l'approccio *DevSecOps* garantisce che la sicurezza sia affrontata in tutte le parti di tale pratica, incorporando controlli di sicurezza e generando automaticamente artefatti conformi alle regole di sicurezza.
Distributed Ledger Technology (DLT) – Tecnologia a registro distribuito	Sistema distribuito che consente ai partecipanti (chiamati nodi) di inviare, validare e conservare informazioni su una base di dati condivisa, senza dipendere da un nodo centrale. A seconda del modello di autorizzazione adottato per la rete di nodi, una DLT può prevedere libera ammissione (*permissionless DLT*) o restrizioni all'ammissione (*permissioned DLT*)[24] alla rete di nodi.
Hardware-based security – Sicurezza basata sull'hardware	Dominio tecnologico che mira a preservare la sicurezza di un bene ICT e dell'informazione ivi contenuta tramite componenti hardware ad hoc. Specifiche tecnologie che appartengono a questo dominio sono, ad esempio, *Hardware Security Module (HSM)* e *secure enclave*.
High-Performance Computing (HPC) – Calcolo ad elevate prestazioni	Pratica che consiste nell'aggregare potenza di calcolo in modo tale da raggiungere prestazioni molto superiori rispetto a quelle che si potrebbero ottenere da un computer tradizionale o una workstation, al fine di risolvere problemi complessi in ambito scientifico, ingegneristico o di business.

[34] Definizione tratta dal libro intitolato "Fundamentals of Business Process Management" di M. Dumas, M. La Rosa, J. Mendling, H. A. Reijers. Per approfondimenti, si faccia riferimento alla pagina: http://fundamentals-of-bpm.org/supplementary-material/lectures/ (in inglese).

EDT (ordine alfabetico in inglese)	Descrizione
***Human-Computer Interaction (HCI)* – Interazione uomo-computer**	Studio dell'interazione tra persone e computer. Comprende (i) *tecnologie di visualizzazione dei dati e delle informazioni*, ovvero, rappresentazioni computazionali, visuali e interattive dei dati allo scopo di dare loro un significato, acquisire conoscenza, scoprire nuove informazioni e/o presentare efficacemente i risultati; (ii) *interfacce uomo-macchina*, ovvero, componenti hardware o software che consentono all'operatore umano di monitorare lo stato di un processo, modificare le configurazioni di controllo per cambiarne l'obiettivo ed escludere manualmente le operazioni di controllo automatico in caso d'emergenza[35].
***Industrial Control System (ICS)* – Sistema di controllo industriale**	Sistema informativo che comprende tecnologie quali, ad esempio, sistemi SCADA – *Supervisory Control And Data Acquisition* e sistemi di controllo distribuiti, utilizzati per il controllo dei processi industriali[36].
***Internet of Things (IoT)* – Internet delle Cose**	Interconnessione di oggetti e dispositivi in grado di trasmettere e ricevere dati su una rete, offrendo così un nuovo livello di interazione e di controllo a distanza che fornisca soluzioni a richieste socioeconomiche, presenti o future, di servizi di rilevamento e monitoraggio, nonché di nuove applicazioni, modelli di business e settori industriali. Quando i dispositivi sono impiegati in processi industriali che richiedono una qualità del servizio molto alta, il paradigma viene definito come *Industrial IoT (IIoT).*
***Knowledge representation and reasoning* – Rappresentazione della conoscenza**	Campo di studio pertinente il dominio dell'*intelligenza artificiale* che si occupa di utilizzare simboli formali per rappresentare una raccolta di proposizioni ritenute vere da un agente[37].
Machine learning and deep learning	Il machine learning è il sottocampo dell'*intelligenza artificiale* definito come la capacità di una macchina di imitare un comportamento umano intelligente. Al momento della stesura di questo documento, una delle direzioni più promettenti consiste nelle reti neurali profonde (*deep neural network*) e i modelli generativi del linguaggio basati su di esse.

[35] Descrizione tratta in parte da https://csrc.nist.gov/glossary/term/Human_Machine_Interface (in inglese).

[36] Descrizione tratta in parte da https://csrc.nist.gov/glossary/term/industrial_control_system (in inglese).

[37] Descrizione tratta in parte dal libro intitolato "Knowledge Representation and Reasoning" di R. Brachman, and H. Levesque, The Morgan Kaufmann Series in Artificial Intelligence, Morgan Kaufmann Publishers, 2004 (in inglese).

EDT (ordine alfabetico in inglese)	Descrizione
Mobile devices – Dispositivi mobili	Un dispositivo mobile è da intendersi come un dispositivo informatico portatile che: (i) ha un ridotto fattore di forma che permette che il dispositivo possa essere trasportato da un singolo individuo; (ii) è progettato per operare senza una connessione fisica (ad esempio, è in grado di trasmettere o ricevere informazioni wireless); (iii) possiede supporti di archiviazione dati locali, non rimovibili; e (iv) è in grado di rimanere acceso per lunghi periodi di tempo grazie ad una fonte di alimentazione autonoma[38].
Quantum technologies	Dominio tecnologico che sfrutta le proprietà della meccanica quantistica quali, ad esempio, entanglement quantistico, sovrapposizione quantistica ed effetto tunnel, per innovare campi quali il calcolo, il monitoraggio e la crittografia.
Robotics and autonomous systems – Robotica e sistemi autonomi	Dominio tecnologico dell'*intelligenza artificiale*; comprende architetture di sistema, algoritmi e strumenti software che mirano a realizzare procedure avanzate di automazione e agenti autonomi che siano in grado di adattarsi al cambiamento di condizioni, della conoscenza e dei vincoli che li circondano[39].
Satellite systems – Sistemi satellitari	Classe di sistemi di comunicazione senza fili che sfrutta costellazioni di satelliti artificiali al fine di creare canali di comunicazione tra trasmettitore e ricevitore posizionati in diversi punti sulla Terra, i quali non possono comunicare tra loro sfruttando tecnologie di rete terrestri. Recentemente, i sistemi satellitari stanno passando dalla tradizionale condizione di integrazione verticale ad un aggregato di segmenti di proprietà e gestione indipendenti che determinano un sistema satellitare che include anche reti terrestri[40].
Virtual reality technologies – Tecnologie per la realtà virtuale	Classe di tecnologie che includono elementi visuali, uditivi e sensoriali, combinati per creare un'interfaccia verso un ambiente cibernetico completamente separato dal mondo reale.

38 Descrizione tratta in parte da https://csrc.nist.gov/glossary/term/mobile_device (in inglese).

39 Descrizione tratta in parte da https://www.nasa.gov/isd-autonomous-systems-and-robotics (in inglese).

40 Si veda https://www.nccoe.nist.gov/projects/hybrid-satellite-networks-cybersecurity (in inglese).

EDT (ordine alfabetico in inglese)	Descrizione
Virtualisation and cloud – Virtualizzazione e cloud	La virtualizzazione è una tecnologia che consente agli utenti di creare molteplici ambienti simulati o di dedicare risorse a partire da un singolo sistema hardware fisico. Il paradigma del *cloud computing* si riferisce ad un ambiente informatico che consente l'astrazione, il raggruppamento e la scalabilità delle risorse fisiche attraverso una rete. A seconda del modello di risorse computazionali offerte, l'ambiente cloud fornisce diversi livelli di virtualizzazione quali IaaS, CaaS, PaaS e SaaS. Con riferimento ad un ICS, architetture *SCADA-as-a-Service* rientrano nell'ambito cloud. Si parla di *edge computing* quando l'elaborazione è eseguita da un ambiente cloud in prossimità di una particolare origine dati per minimizzare la latenza.
Zero trust architecture	La proliferazione di alcune delle precedenti EDT quali, ad esempio, cloud computing, dispositivi mobili e IoT, ha comportato la dissoluzione dei tradizionali confini di rete basati su perimetro. Il paradigma di cybersicurezza della z*ero trust* prevede di spostare le linee di difesa da uno statico perimetro esterno di rete ai singoli utenti, ai beni ICT e alle risorse, assumendo che la fiducia non può essere concessa sulla base della sola posizione fisica o in rete[41].

[41] Descrizione tratta in parte da https://www.nist.gov/publications/zero-trust-architecture (in inglese).

3.2. Proposta di Corrispondenza tra Subaree e EDT

In Tabella 3–2 e Tabella 3–3 viene fornita una corrispondenza tra subaree di R&I e EDT. La risultante mappa è rappresentata in due modi per consentirne una fruizione agevolata sotto diverse prospettive: la Tabella 3–2 mette in relazione ogni subarea con le EDT rilevanti per il suo studio, mentre la Tabella 3–3 riporta per ciascuna EDT le subaree che ne sono interessate.

Tabella 3–2: relazioni tra ogni subarea di R&I e le EDT.

Aree	Subaree	Argomenti	EDT (in inglese)
1. SICUREZZA DEI DATI E PRIVACY	**1.1. Ingegneria della protezione dei dati**	**1.1.1.** Elaborazione *privacy-preserving* dei dati **1.1.2.** Memorizzazione *privacy-preserving* dei dati **1.1.3.** Autenticazione, autorizzazione e controllo di accesso con garanzie di privacy aggiuntive	▪ BPM ▪ Data science ▪ Hardware-based security ▪ ICS ▪ IoT ▪ Knowledge representation and reasoning ▪ Machine learning and deep learning ▪ Mobile devices ▪ Satellite systems ▪ Virtualisation and cloud ▪ Zero trust architecture
	1.2. Crittografia	**1.2.1.** Primitive, algoritmi e protocolli per PQC **1.2.2.** Crittografia quantistica **1.2.3.** Schemi di FHE **1.2.4.** Funzioni crittografiche di hashing	▪ DevSecOps ▪ DLT ▪ Hardware-based security ▪ HPC ▪ Mobile devices ▪ Quantum technologies ▪ Satellite systems ▪ Virtualisation and cloud
	1.3. Trusted information sharing	**1.3.1.** Arricchimento delle soluzioni standard di interoperabilità semantica con controlli di sicurezza **1.3.2.** Soluzioni architetturali per *trusted information sharing* e *storage*	▪ BPM ▪ Data science ▪ HCI ▪ Knowledge representation and reasoning ▪ Machine learning and deep learning ▪ Mobile devices ▪ Virtualisation and cloud ▪ Zero trust architecture

Aree	Subaree	Argomenti	EDT (in inglese)
2. GESTIONE DELLE MINACCE CIBERNETICHE	**2.1. Attacco e difesa**	**2.1.1.** Tecniche di attacco e misure di difesa **2.1.2.** Rilevamento e risposta contro i malware **2.1.3.** Messa in sicurezza di algoritmi e modelli per il machine learning **2.1.4.** *Adversarial behaviour*	▪ 5G and beyond mobile networks ▪ BPM ▪ Data science ▪ HPC ▪ HCI ▪ IoT ▪ Knowledge representation and reasoning ▪ Machine learning and deep learning ▪ Mobile devices ▪ Robotics and autonomous systems ▪ Virtualisation and cloud ▪ Zero trust architecture
	2.2. Cyberthreat intelligence	**2.2.1.** Machine learning per la *cyberthreat intelligence* **2.2.2.** Metodologie per monitorare la disinformazione **2.2.3.** Attribuzione di attacchi alla sicurezza cibernetica	▪ Data science ▪ HPC ▪ HCI ▪ IoT ▪ Knowledge representation and reasoning ▪ Machine learning and deep learning ▪ Robotics and autonomous systems
	2.3. Gestione degli incidenti e operazioni di sicurezza	**2.3.1.** Resilienza dei sistemi cyber-fisici **2.3.2.** Automazione via machine learning dei sistemi tradizionali **2.3.3.** Strategie di difesa	▪ 5G and beyond mobile networks ▪ BPM ▪ Data science ▪ DevSecOps ▪ DLT ▪ HCI ▪ ICS ▪ IoT ▪ Knowledge representation and reasoning ▪ Machine learning and deep learning ▪ Mobile devices ▪ Robotics and autonomous systems ▪ Virtualisation and cloud ▪ Zero trust architecture

Aree	Subaree	Argomenti	EDT (in inglese)
	2.4. Scienze forensi digitali	**2.4.1.** Processi di scienze forensi digitali **2.4.2.** Contromisure per aggirare le tecniche antiforensi	▪ 5G and beyond mobile networks ▪ BPM ▪ Data science ▪ DLT ▪ Machine learning and deep learning ▪ Mobile devices
3. SICUREZZA DEL SOFTWARE E DELLE PIATTAFORME	**3.1. Sicurezza nello sviluppo e test del software**	**3.1.1.** Linguaggi di programmazione *security-aware* **3.1.2.** Gestione sicura del ciclo di vita del software **3.1.3.** Paradigma dell'open cloud **3.1.4.** Tecniche per rilevare vulnerabilità di sicurezza nel firmware e nei file binari	▪ 5G and beyond mobile networks ▪ BPM ▪ DevSecOps ▪ DLT ▪ ICS ▪ IoT ▪ Machine learning and deep learning ▪ Mobile devices ▪ Robotics and autonomous systems ▪ Virtual reality technologies ▪ Virtualisation and cloud
	3.2. Sicurezza nei sistemi operativi e tecnologie di virtualizzazione	**3.2.1.** Sicurezza dei nuovi approcci alla virtualizzazione **3.2.2.** Modelli di protezione per la sicurezza delle piattaforme	▪ 5G and beyond mobile networks ▪ BPM ▪ DevSecOps ▪ Hardware-based security ▪ IoT ▪ Mobile devices ▪ Robotics and autonomous systems ▪ Virtual reality technologies ▪ Virtualisation and cloud ▪ Zero trust architecture

Aree	Subaree	Argomenti	EDT (in inglese)
	3.3. Blockchain	3.3.1. Problemi di sicurezza degli algoritmi di consenso e *mining* 3.3.2. Tecnologie per *smart contract* 3.3.3. Tecniche di crittografia e anonimizzazione 3.3.4. Economia delle blockchain	▪ BPM ▪ DLT ▪ HPC
4. SICUREZZA DELLE INFRASTRUTTURE DIGITALI	4.1. Hardware	4.1.1. Vulnerabilità e attacchi indotti dall'hardware 4.1.2. Approcci di sicurezza cibernetica ancorati all'hardware 4.1.3. Modelli per il rilevamento sicuro dei dati 4.1.4. Architetture hardware aperte	▪ 5G and beyond mobile networks ▪ DevSecOps ▪ Hardware-based security ▪ HPC ▪ ICS ▪ IoT ▪ Machine learning and deep learning ▪ Mobile devices ▪ Quantum technologies ▪ Robotics and autonomous systems ▪ Virtual reality technologies ▪ Zero trust architecture
	4.2. Reti	4.2.1. Miglioramento della sicurezza e della resilienza di rete 4.2.2. Approcci per la sicurezza dei sistemi IoT 4.2.3. Rafforzamento della sicurezza delle reti di telecomunicazioni cellulari 4.2.4. Sviluppo di infrastrutture per la QCI	▪ 5G and beyond mobile networks ▪ DevSecOps ▪ Hardware-based security ▪ HPC ▪ ICS ▪ IoT ▪ Machine learning and deep learning ▪ Mobile devices ▪ Quantum technologies ▪ Robotics and autonomous systems ▪ Satellite systems ▪ Virtual reality technologies ▪ Virtualisation and cloud ▪ Zero trust architecture

Aree	Subaree	Argomenti	EDT (in inglese)
5. ASPETTI DELLA SOCIETÀ	**5.1. Aspetti umani**	**5.1.1.** Ridefinizione dei confini dell'interazione uomo-macchina **5.1.2.** Miglioramento della percezione del rischio **5.1.3.** Metodologie per la prevenzione degli attacchi di ingegneria sociale **5.1.4.** Favorire l'accettazione di politiche e tecnologie di sicurezza da parte degli utenti finali **5.1.5.** Profilazione dell'attaccante	▪ BPM ▪ Data science ▪ HCI ▪ IoT ▪ Machine learning and deep learning ▪ Mobile devices ▪ Robotics and autonomous systems ▪ Virtual reality technologies ▪ Zero trust architecture
	5.2. Aspetti formativi	**5.2.1.** Metodologie per la valutazione e lo sviluppo di competenze di cybersicurezza e per l'identificazione delle competenze per le professioni legate alla cybersicurezza **5.2.2.** Modelli e strumenti per la consapevolezza della cybersicurezza **5.2.3.** Modelli e strumenti per la formazione sulla cybersicurezza	▪ BPM ▪ HCI ▪ Mobile devices ▪ Virtual reality technologies ▪ Zero trust architecture
	5.3. Aspetti legali	**5.3.1** Regole e principi etici per uno spazio cibernetico sicuro **5.3.2.** Modelli e regole per favorire l'autonomia strategica **5.3.3.** Modelli e regole per il governo del cyberspazio	▪ 5G and beyond mobile networks ▪ BPM ▪ Data science ▪ DLT ▪ HCI ▪ Machine learning and deep learning ▪ Robotics and autonomous systems ▪ Virtualisation and cloud ▪ Zero trust architecture

Aree	Subaree	Argomenti	EDT (in inglese)
6. ASPETTI DI GOVERNO	**6.1. Aspetti organizzativi**	**6.1.1.** Economia dell'ecosistema della cybersicurezza e delle catene di approvvigionamento **6.1.2.** Metodologie per il raggiungimento degli obiettivi di cybersicurezza **6.1.3.** Metodologie per gli audit di cybersicurezza **6.1.4.** Continuità operativa e recupero dal disastro	▪ BPM ▪ DLT ▪ Virtualisation and cloud ▪ Zero trust architecture
	6.2. Gestione del rischio	**6.2.1.** Quadri procedurali per la valutazione del rischio **6.2.2.** KPI sulla sicurezza cibernetica **6.2.3.** Gestione del rischio e analisi delle reti di catene di approvvigionamento	▪ 5G and beyond mobile networks ▪ BPM ▪ Data science ▪ DLT ▪ HCI ▪ ICS ▪ IoT ▪ Knowledge representation and reasoning ▪ Mobile devices ▪ Robotics and autonomous systems ▪ Virtual reality technologies ▪ Virtualisation and cloud ▪ Zero trust architecture
	6.3. Standardizzazione	**6.3.1.** Standardizzazione dei processi aziendali per la cybersicurezza **6.3.2.** Sviluppo di standard di sicurezza cibernetica specifici per le singole tecnologie **6.3.3.** Formalizzazione delle specifiche tecniche	▪ 5G and beyond mobile networks ▪ BPM ▪ Data science ▪ DevSecOps ▪ DLT ▪ Hardware-based security ▪ ICS ▪ IoT ▪ Knowledge representation and reasoning ▪ Machine learning ▪ Mobile devices ▪ Quantum technologies ▪ Virtualisation and cloud ▪ Zero trust architecture

Tabella 3–3: relazioni tra ogni EDT (in inglese) e le subaree di R&I.

	Area#1 – Sicurezza dei dati e privacy			Area#2 – Gestione delle minacce cibernetiche				Area#3 – Sicurezza del SW e piatt.		
	Ing. della protezione dei dati	Critto-grafia	Trusted info sharing	Attacco e difesa	Cyber-threat in-telligence	Gest. degli incid. e oper. di sic.	Scienze forensi digitali	Sic. nello sviluppo e test del SW	Sic. nei sist. oper. e tecn. di virt.	Block-chains
5G and beyond mobile networks				X		X	X	X	X	
BPM	X		X	X		X	X	X	X	X
Data science	X		X	X	X	X	X			
DevSecOps		X				X		X	X	
DLT		X				X	X	X		X
Hardware-based security	X	X							X	
HPC		X		X	X					X
HCI			X	X	X	X				
ICS	X					X		X		
IoT	X			X	X	X		X	X	
Knowledge representation and reasoning	X		X	X	X	X				
Machine learning and deep learning	X		X	X	X	X	X	X		
Mobile devices	X	X	X	X		X	X	X	X	
Quantum technologies		X								
Robotics and autonomous systems				X	X	X		X	X	
Satellite systems	X	X								
Virtual reality technologies								X	X	
Virtualisation and cloud	X	X	X	X		X		X	X	
Zero trust architecture	X		X	X		X			X	

	Area#4 – Sic. delle infr. dig.		Area#5 – Aspetti della società			Area#6 – Aspetti di governo		
	HW	Reti	Aspetti umani	Aspetti formativi	Aspetti legali	Aspetti organizzativi	Gestione del rischio	Std
5G and beyond mobile networks	X	X			X		X	X
BPM			X	X	X	X	X	X
Data science			X		X		X	X
DevSecOps	X	X						X
DLT					X	X	X	X
Hardware-based security	X	X						X
HPC	X	X						
HCI			X	X	X		X	
ICS	X	X					X	X
IoT	X	X	X				X	X
Knowledge representation and reasoning							X	X
Machine learning and deep learning	X	X	X		X			X
Mobile devices	X	X	X	X			X	X
Quantum technologies	X	X						X
Robotics and autonomous systems	X	X	X		X		X	
Satellite systems		X						
Virtual reality technologies	X	X	X	X			X	
Virtualisation and cloud		X			X	X	X	X
Zero trust architecture	X	X	X	X	X	X	X	X

Lista degli Acronimi

3GPP	Third Generation Partnership Project
5G	Quinta Generazione (di reti mobili)
ACN	Agenzia per la Cybersicurezza Nazionale
BPM	Business Process Management
CaaS	Containers-as-a-Service
CINI	Consorzio Interuniversitario Nazionale per l'Informatica
CISA	(US) Cybersecurity and Infrastructure Security Agency
CMM	Capability Maturity Model
DDoS	Distributed Denial of Service
D.L.	Decreto Legge
DLT	Distributed Ledger Technology
DNS	Domain Name System
EDT	Emerging and Disruptive Technology
ENISA	Agenzia dell'Unione Europea per la Cibersicurezza
EU	European Union
FHE	Fully Homomorphic Encryption
GDPR	(EU) General Data Protection Regulation
GNSS	Global Navigation Satellite Systems
HCI	Human-Computer Interaction
HPC	High-Performance Computing
HSM	Hardware Security Module
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPS	Intrusion Prevention System
JRC	(EU) Joint Research Centre

KPI	Key Performance Indicator
MUR	Ministero dell'Università e della Ricerca
NATO	North Atlantic Treaty Organization
NFC	Near-Field Communication
NIST	(US) National Institute of Standards and Technology
OS	Operating System
OTA	Over-the-air
PaaS	Platform-as-a-Service
PET	Privacy-Enhancing Technology
PII	Personally Identifiable Information
PMI	Piccole e Medie Imprese
PNR	Programma Nazionale per la Ricerca
PQC	Post-Quantum Cryptography
PUF	Physically Unclonable Function
QCI	Quantum Communication Infrastructure
QKD	Quantum Key Distribution
R&I	Ricerca e Innovazione
RFID	Radio-Frequency Identification
RID	Riservatezza, Integrità, Disponibilità
SaaS	Software-as-a-Service
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SMC	Secure Multi-party Computation
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
STIG	Security Technical Implementation Guideline
TEE	Trusted Execution Environment
UK	United Kingdom
US	United States of America

Appendice

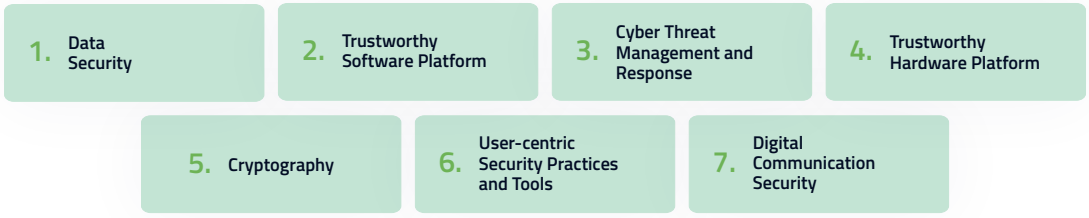
Le fonti utilizzate per classificare le aree principali del dominio di conoscenza della cybersicurezza sono principalmente le quattro che seguono:

- le attività in corso a livello nazionale da parte dei partenariati pubblico-privati che stanno implementando la Componente 2 ("Dalla Ricerca all'Impresa") della Missione 4 ("Istruzione e Ricerca") di *Italia Domani* – Piano Nazionale di Ripresa e Resilienza[42], in particolare il progetto SERICS – *Security and Rights in the CyberSpace* [43];
- *Cybersecurity Research Directions for the EU's Digital Strategic Autonomy*[44] dell'ENISA;
- *European Cybersecurity Centres of Expertise Map – Definitions and Taxonomy*[45] del JRC;
- *CyBOK*[46], un'iniziativa internazionale coordinata dal Regno Unito.

In particolare,

la classificazione di SERICS è la seguente:

la classificazione di ENISA è la seguente:



[42] Per approfondimento veda: https://italiadomani.gov.it/content/sogei-ng/it/en/il-piano/missioni-pnrr/istruzione-e-ricerca.html.

[43] Si veda il sito https://serics.eu/.

[44] Disponibile (in inglese) al sito https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy.

[45] Disponibile (in inglese) al sito https://publications.jrc.ec.europa.eu/repository/handle/JRC111441.

[46] Disponibile (in inglese) al sito https://www.cybok.org/. w3e4w.

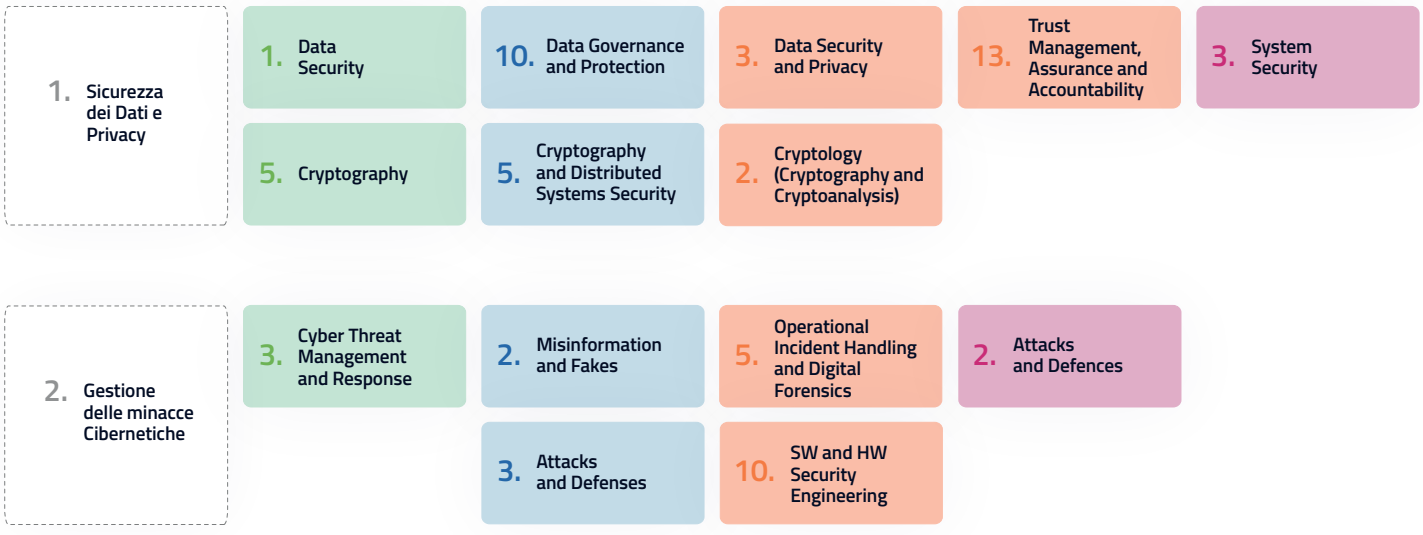
la classificazione del JRC è la seguente:

1. Assurance, Audit and Certification
2. Cryptology (Cryptography and Cryptoanalysis)
3. Data Security and Privacy
4. Education and Training
5. Operational Incident Handling and Digital Forensics
6. Human Aspects
7. Identify and Access Managements (IAM)
8. Security Management and Governance
9. Network and Distributed Systems
10. SW and HW Security Engineering
11. Legal Aspects
12. Theoretical Foundations
13. Trust Management, Assurance and Accountability

la classificazione del CyBOK è la seguente:

1. Human, Organisational & Regulatory Aspects
2. Attacks and Defences
3. System Security
4. Software and Platform Security
5. Infrastructure Security

La corrispondenza tra le iniziative di classificazione menzionate in precedenza e le aree di R&I identificate in questo documento è mostrata nelle figure seguenti.



Legenda: ENISA SERICS JRC CyBOK

3. Sicurezza del Software e delle Piattaforme	2. Trustworthy Software Platform	5. Cryptography and Distributed Systems Security	10. SW and HW Security Engineering	12. Theoretical Foundations	3. System Security
	4. Operating Systems and Virtualization security	6. Software and Platform Security	7. Identify and Access Managements (IAM)	13. Trust Management, Assurance and Accountability	4. Software and Platform Security
4. Sicurezza delle Infrastrutture Digitali	4. Trustworthy Hardware Platform	7. Infrastructure Security	9. Network and Distributed Systems	5. Infrastructure Security	
	7. Digital Communication Security	9. Securing Digital Transformation	10. SW and HW Security Engineering		
5. Aspetti della Società	6. User-centric Security Practices and Tools	6. Human Aspects	5. Operational Incident Handling and Digital Forensics	1. Human, Organisational & Regulatory Aspects	
	1. Human, Social and Legal Aspects	11. Legal Aspects	4. Education and Training		
6. Aspetti di Governo	8. Risk Management and Governance	8. Security Management and Governance	1. Human, Organisational & Regulatory Aspects		
		1. Assurance, Audit and Certification			

Legenda: ENISA SERICS JRC CyBOK


REPVBBLICA ITALIANA
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT
MUR
Ministero dell'Università e della Ricerca