STRATEGIA

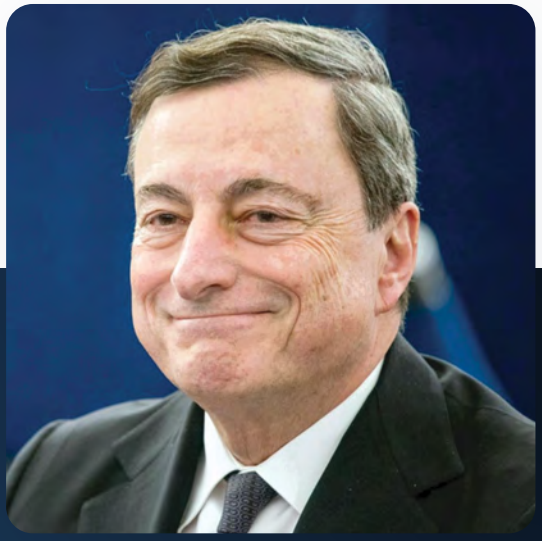
NAZIONALE DI CYBERSICUREZZA

2022 – 2026

Sommario

	Prefazione	2
	Premessa	4
01	Le sfide da affrontare	9
02	Visione strategica: gli obiettivi da perseguire	15
	Elenco degli acronimi	27

Prefazione



Le nuove forme di competizione strategica che caratterizzano lo scenario geopolitico impongono all'Italia di proseguire e, dove possibile, incrementare le iniziative in materia di cybersicurezza. Dobbiamo tenere fede agli impegni assunti nell'ambito delle organizzazioni internazionali a cui l'Italia partecipa, anche tenuto conto dell'elevata qualità e dei massicci investimenti realizzati dai principali alleati e partner internazionali. È dunque necessaria una puntuale rivisitazione nella concezione e nella visione strategica dell'architettura nazionale di cybersicurezza.

La strategia italiana per la cybersicurezza unisce sicurezza e sviluppo, nel rispetto dei valori della nostra Costituzione. È in linea con quanto previsto dalla Strategia dell'Unione europea per la cybersicurezza del dicembre 2020, dalla Bussola Strategica per la sicurezza e la difesa dell'UE del marzo 2022 e dai recenti indirizzi strategici della NATO.

Per realizzare questa nuova visione, l'Italia ha costruito un ecosistema di cybersicurezza fondato sulla collaborazione tra i settori pubblico e privato. Al contributo delle istituzioni, si affianca quello attivo degli operatori economici - in particolare dei gestori delle infrastrutture da cui dipende l'erogazione dei servizi essenziali dello Stato - del mondo dell'università e della ricerca e della società civile. Tutti devono farsi parte attiva nel proteggere i propri assetti informatici, nel rispetto delle norme riconosciute a livello internazionale.

I produttori e fornitori di beni e servizi ICT svolgono un ruolo di primo piano. A loro è richiesto di fornire prodotti e soluzioni tecnologiche che soddisfino adeguati requisiti di cybersicurezza. L'obiettivo è rafforzare la resilienza di dispositivi e apparati ICT, a partire dal 5G e dal cloud, anche al fine di aumentare la fiducia dei cittadini.

È nostra intenzione intensificare i progetti di sviluppo tecnologico per arrivare a disporre di un adeguato livello di autonomia strategica nel settore e quindi garantire la nostra sovranità digitale. Per farlo, sarà cruciale stanziare fondi adeguati, con continuità.

Premessa

Velocità di connessione, numerosità di interazioni tra utenti e accessibilità di dati e informazioni online non sono parametri sufficienti a definire lo sviluppo digitale che caratterizza l'età contemporanea, né riescono a descrivere, nella sua interezza, quell'articolata dimensione che chiamiamo spazio cibernetico.

In tale dominio trovano posto, interconnessi e comunicanti, innumerevoli servizi concepiti per il soddisfacimento delle quotidiane esigenze delle nostre comunità e per lo svolgimento delle relative attività economiche: infrastrutture energetiche, mercati finanziari, forniture di acqua potabile, trasporti di massa, e, non ultime, le funzioni essenziali dello Stato, incluse la sua difesa e integrità. La complessità e l'interdipendenza dei sistemi è cresciuta fino a sfumare la dualità tra la dimensione digitale e il mondo reale, rendendo spesso problematica l'identificazione di confini e rispettive caratteristiche.

Se, da una parte, è l'incessante evoluzione delle moderne tecnologie a rendere più conveniente la "migrazione" verso il digitale, dall'altra, solo la resilienza e la sicurezza delle reti e dei sistemi su cui tali servizi si basano possono garantire, nell'immediato, la sicurezza per la nostra comunità e, in prospettiva, lo sviluppo economico e il benessere dello Stato.

La ricerca scientifica e lo sviluppo industriale determinano, dal canto loro, la diffusione e il progressivo impiego delle cd. *Emerging and Disruptive Technologies* (EDT), nel cui novero rientrano reti e protocolli di comunicazione di ultima generazione (5G/6G), *blockchain*, intelligenza artificiale (IA), *quantum computing, High Performance Computing* (HPC), *Internet of Things* (IoT), robotica, strumenti crittografici evoluti e altre innovazioni di portata dirompente.

I rischi insiti in tale complessità – e le potenziali, molteplici ricadute negli ambiti economico, sociale e politico – spaziano dalla dipendenza tecnologica e perdita di autonomia strategica dello Stato alle minacce di tipo antropico, in cui l'errore umano si somma alle iniziative di attori malevoli, caratterizzati da diverso grado di sofisticazione e mossi da differenti, ma ugualmente dannosi, intenti.

Siano esse volte ad ottenere profitti illeciti (*cyber-crime*), generare vantaggio informativo per fini di competizione geopolitica (*cyber-espionage*), diffondere narrative divisive e polarizzanti in aderenza a specifiche ideologie o motivazioni politiche, nessuna organizzazione, pur tecnologicamente equipaggiata e proceduralmente preparata, può ambire a eliminare del tutto le minacce che promanano dallo spazio cibernetico.

A tale realtà occorre far fronte, agendo secondo un approccio che includa l'adozione di misure di prevenzione e mitigazione del rischio volte a innalzare la resilienza delle infrastrutture digitali. Queste ultime non includono soltanto reti, sistemi e dati, ma anche, e soprattutto, utenti, la cui consapevolezza – siano essi attori istituzionali, imprese private o cittadini – va alimentata attraverso una diffusa cultura della cybersicurezza. Se ad oggi, infatti, esiste una diffusa percezione dei rischi correlati alla sicurezza fisica, per cui ogni individuo pone in essere, nella propria quotidianità, azioni volte a tutelare sé stesso e i propri beni, lo stesso non può dirsi per la dimensione digitale, dei cui rischi non si ha ancora piena consapevolezza.

Tale aspetto, unito alla sempre più ampia disponibilità – a costi relativamente bassi – di strumenti offensivi, all'accresciuto livello di complessità degli attacchi, alla difficoltà tecnica di attribuire gli stessi a un autore certo, nonché alla possibilità che esistano vulnerabilità di sicurezza gravanti su prodotti e soluzioni informatiche, fa registrare un numero complessivo di azioni ostili in costante aumento.

I recenti trend di attacco forniscono evidenze di danni economici e reputazionali per imprese, blocco dell'operatività di infrastrutture energetiche, malfunzionamenti di sistemi informativi impiegati da aziende ospedaliere e sanitarie, diffusione di dati personali che mirano a screditare figure pubbliche, giornalisti e attivisti politici, fino a metterne in pericolo, talvolta, l'incolumità.

Da tale scenario derivano quattro considerazioni imprescindibili:

1. rientra tra i doveri dello Stato la **definizione di adeguate strategie di cybersicurezza** volte a pianificare, coordinare e attuare misure tese a rendere il Paese sicuro e resiliente anche nel dominio digitale, assicurando, al contempo, la fiducia dei cittadini nella possibilità di sfruttarne i relativi vantaggi competitivi, nella piena tutela dei diritti e delle libertà fondamentali;
2. la cybersicurezza, che è divenuta una questione di importanza strategica, deve porsi a fondamento del processo di digitalizzazione del Paese, quale elemento imprescindibile della trasformazione digitale, anche nell'ottica di **conseguire l'autonomia nazionale strategica** nel settore;
3. la stessa deve poi essere percepita non come un costo, ma come un investimento e un **fattore abilitante per lo sviluppo dell'economia e dell'industria nazionale,** al fine di accrescere la competitività del Sistema-Paese a livello globale;
4. la messa in sicurezza di infrastrutture, sistemi e informazioni dal punto di vista tecnico deve essere accompagnata da un progresso culturale ad ogni livello della società, verso un **approccio *"security-oriented",*** tassello indispensabile per tutelare il nostro sistema valoriale e democratico.

Nella consapevolezza di quanto sopra e della velocità e vastità del cambiamento tecnologico che impongono di perseverare nell'opera di adeguamento normativo e adattamento strategico, a partire dal 2013, molto è stato fatto dal nostro Paese nel campo della cybersicurezza.

Nel tempo, infatti, sono stati adottati una serie di provvedimenti sostanzialmente diretti sia ad acquisire, sviluppare e rafforzare le necessarie capacità cyber nazionali, sia a garantire l'unicità istituzionale di indirizzo e di azione rispetto ad un'area di intervento, quella della cybersicurezza, quanto mai trasversale e coinvolgente diversi soggetti portatori di interessi.

Si tratta di finalità, da ultimo, perseguite attraverso la recente riforma dell'architettura nazionale cyber, che è stata attuata attraverso l'adozione del decreto-legge 14 giugno 2021, n. 82. Il decreto ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), con l'obiettivo – nel rispetto delle competenze attribuite dalla normativa vigente ad altre Amministrazioni – di razionalizzare e semplificare il frammentato sistema di competenze, esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

L'Agenzia, in qualità di Autorità nazionale per la cybersicurezza, ha tra i suoi compiti quello di predisporre la strategia nazionale di cybersicurezza. Inoltre, ai sensi del citato decreto-legge, l'ACN è designata quale Autorità nazionale competente in via esclusiva e punto di contatto unico (PoC) per le finalità di cui alla normativa sulla sicurezza delle reti e dei sistemi informativi (NIS), Autorità nazionale di certificazione della cybersicurezza, Centro Nazionale di Coordinamento (NCC) rispetto al Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ed elemento centrale del Perimetro di sicurezza nazionale cibernetica (PSNC). Competenze queste, precedentemente attribuite ad una pluralità di soggetti istituzionali.

I PILASTRI TECNICO-OPERATIVI

La riorganizzazione dell'architettura nazionale di cybersicurezza alla luce del decreto-legge 82/2021

* Polizia Postale e delle Comunicazioni - Organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazioni

Con la creazione dell'ACN si è voluto mettere a sistema l'esperienza accumulata nei precedenti cinque anni di lavoro, nel contesto del DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali", nonché di quella maturata da altri Paesi, riconoscendo autonoma dignità alla sicurezza e alla resilienza cibernetica ponendole sotto la responsabilità del Presidente del Consiglio dei ministri a fondamento del processo di digitalizzazione del Paese, attraverso un più ampio ruolo di sinergia e coordinamento con tutte le Amministrazioni competenti in materia. Si è quindi voluto definire un ulteriore pilastro, attestandolo ad un unico soggetto governativo, a completamento di quelli esistenti di prevenzione e repressione dei reati informatici (di competenza delle Forze di polizia), di difesa e sicurezza militare dello Stato nello spazio cibernetico (di spettanza del Ministero della Difesa) e di ricerca ed elaborazione informativa (di competenza degli Organismi di informazione per la sicurezza). Ciò, con l'obiettivo di assicurare la coerenza delle iniziative, l'efficientamento della spesa, la capacità di fornire un chiaro e aggiornato quadro situazionale all'Autorità politica, nonché identificare un'unica interfaccia incaricata, nel rispetto delle competenze attribuite dalla normativa vigente ad altre Amministrazioni, del coordinamento tra i soggetti pubblici coinvolti in materia di sicurezza cibernetica e resilienza, anche al fine di garantire nei consessi internazionali una postura nazionale unitaria e coerente con le politiche di sicurezza cibernetica e resilienza definite dal Presidente del Consiglio dei ministri.

Per assicurare la cyber-resilience, l'Agenzia mira a divenire una fucina di competenze, sia da innestare nell'ambito di altre Pubbliche Amministrazioni per innalzare la nostra postura cyber nazionale, sia da far crescere al suo interno. Per svolgere i suoi molteplici compiti istituzionali, infatti, l'ACN – quale struttura di eccellenza e asset per il sistema-Paese – necessita di numerose ed elevate professionalità. A partire dal 2022, mirate campagne porteranno al reclutamento di esperti, che raggiungeranno il target delle 800 unità nel 2027. Ciò consentirà anche di arginare la fuga delle competenze verso l'estero e di riportare in Patria alcuni dei nostri talenti, prospettando un percorso di crescita professionale al servizio della sicurezza del loro Paese.

Per quel che concerne le attività di prevenzione e contrasto ai crimini informatici, provvede la Polizia di Stato attraverso il Servizio di Polizia Postale e delle Comunicazioni, al cui interno opera il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), quale unità specializzata nella protezione delle infrastrutture critiche informatizzate dai reati informatici e punto di contatto nazionale per le emergenze in materia di criminalità informatica transnazionale. Nell'ambito del Dipartimento di Pubblica Sicurezza, inoltre, è stata recentemente creata la Direzione Centrale per la polizia scientifica e la sicurezza cibernetica, nella quale confluiscono le attribuzioni di organo centrale del Ministero dell'Interno per la sicurezza e la regolarità delle comunicazioni e quelle di contrasto ai reati di sfruttamento sessuale per via informatica e di prevenzione del terrorismo, in precedenza assicurate dal Servizio polizia postale e delle comunicazioni. Presso la Direzione Centrale per la Sicurezza Cibernetica opererà il Computer Emergency Response Team (CERT) del Ministero dell'Interno, istituito per garantire la sicurezza delle reti e dei sistemi informativi del Dicastero, attraverso la prevenzione e la gestione degli eventi critici.

Per quanto riguarda l'Arma dei Carabinieri, il Reparto Indagini Telematiche del Raggruppamento Operativo Speciale (ROS) costituisce l'articolazione specializzata dell'Arma nel contrasto alla criminalità informatica, nello studio e sperimentazione delle tecnologie per l'esplorazione del web e l'intercettazione dei flussi telematici, mentre per la Guardia di Finanza è il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT) quale Repar-

to Speciale deputato al contrasto delle frodi telematiche ed informatiche, nonché alla tutela della privacy.

In relazione, poi, alla difesa e sicurezza dello Stato, il Ministero della Difesa definisce e coordina la politica militare, la governance e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero. La Difesa, attraverso le articolazioni specialistiche dedicate, conduce operazioni militari cibernetiche offensive e difensive nei casi previsti.

Tale Dicastero, pertanto, assicura, anche in situazioni di crisi di natura cibernetica (sia nazionale sia internazionale), tutti i servizi e le attività necessari, da un lato, a garantire la protezione, la resilienza e l'efficienza delle reti e infrastrutture militari e, dall'altro, a sviluppare le proprie peculiari capacità necessarie all'implementazione di attività di supporto, difesa, reazione e stabilizzazione.

La ricerca ed elaborazione informativa, finalizzata alla tutela degli interessi politici, militari, economici, scientifici e industriali dell'Italia, è affidata al Comparto intelligence, che a tali fini provvede anche alle attività volte alla rilevazione e alla sistematica azione di monitoraggio, prevenzione e contrasto delle minacce cibernetiche più insidiose, perpetrate nel o attraverso l'ambiente digitale, anche attraverso la conduzione di operazioni cyber.

Un ruolo rilevante, trasversale ai citati quattro pilastri, è inoltre costituito dalla cyber diplomacy, intesa come il ricorso a strumenti e iniziative diplomatiche per conseguire gli interessi nazionali del Paese nello spazio cibernetico e come parte delle più ampie attività di politica estera, tenuto conto dell'impatto della tecnologia sulle relazioni internazionali. Tale attività fa capo all'Unità per le politiche e la sicurezza dello spazio cibernetico del Ministero per gli Affari Esteri e la Cooperazione Internazionale (MAECI).

Al di là degli attori istituzionali con competenze in materia cyber – che non si esauriscono in quelli sopra citati[1] – la presente strategia è ispirata ad un approccio "whole-of-society", che vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza. Nella presente visione strategica, infatti, quest'ultima è concepita non solamente come un indiretto beneficiario delle misure contemplate nel Piano di implementazione della strategia, ma anche come parte attiva. L'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso.

[1] Per una disamina dell'ecosistema nazionale di sicurezza cibernetica, si veda la sezione sulla "Governance nazionale" del Piano di implementazione della strategia.

#1

Le sfide da affrontare

#1

Le sfide da affrontare

La rapida evoluzione tecnologica che ormai caratterizza il mondo contemporaneo ha determinato la comparsa di nuovi rischi e ulteriori ne sorgeranno con l'avanzare della stessa e delle tecniche di attacco. A ciò non sempre corrisponde, tuttavia, un adeguato grado di consapevolezza da parte della società.

Tali rischi includono quelli sistemici, connessi a:

- attacchi cyber dovuti a cybercriminali, attivisti o a campagne statuali coordinate, che sfruttano errori software, errate configurazioni, debolezze nei protocolli e/o umane, per sottrarre dati o arrecare danni ai sistemi, come nel caso delle campagne ransomware, le quali hanno un impatto sull'erogazione dei servizi, anche essenziali di un Paese, sul suo PIL e sulla sua reputazione;

- tecnologie impiegate, le quali sono sviluppate e prodotte da grandi realtà aziendali, talvolta controllate o, comunque, influenzate nel loro operato dai Governi in cui hanno sede, con conseguenti possibili ingerenze nella catena degli approvvigionamenti, sia in termini di disponibilità sul mercato delle relative componenti, sia di affidabilità delle stesse;

- diffusione, attraverso lo spazio cibernetico, di fake news, deepfake e campagne di disinformazione che tendono a confondere e destabilizzare i cittadini di un Paese immergendoli in uno spazio informativo estremamente dinamico e orizzontale, caratterizzato da un insieme pressoché infinito di sorgenti di notizie che polarizzano le opinioni cambiando il modo in cui percepiamo la realtà.

In considerazione dei citati rischi, la presente strategia mira ad affrontare le seguenti sfide inerenti il rafforzamento della resilienza nella transizione digitale del sistema Paese, promuovendo un uso sicuro delle tecnologie, indispensabili per la nostra prosperità economica, presente e futura, il conseguimento dell'autonomia strategica nella dimensione cibernetica, l'anticipazione dell'evoluzione della minaccia cyber, la gestione di crisi cibernetiche in scenari geopolitici complessi, nonché il contrasto della disinformazione online, nel rispetto dei diritti umani, dei nostri valori e principi.

SFIDE DA AFFRONTARE

Assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo

Non ci può essere transizione digitale senza un'adeguata resilienza agli attacchi e agli incidenti cyber. La cybersicurezza degli assetti e dei servizi digitali è, infatti, elemento imprescindibile della loro fruibilità da parte del cittadino, il quale sarà, così, non solo incentivato all'utilizzo degli stessi, ma ne farà ricorso in totale fiducia e con la consapevolezza che i suoi dati sono adeguatamente protetti. Va da sé che la resilienza non deve essere intesa solo nell'accezione tecnica, ma anche sotto il profilo della cultura della sicurezza informatica e della disponibilità di un'adeguata forza lavoro qualificata. Senza quest'ultima, infatti, ogni possibilità di raggiungere una sovranità digitale resterebbe pura utopia. A ciò si aggiunge una sfida nella sfida, la questione di genere, in quanto le donne che intraprendono studi informatici o lauree nelle discipline STEM (Scienze, Tecnologia, Ingegneria e Matematica) rappresentano un numero esiguo e ancora meno sono quelle che si specializzano in cybersicurezza.

Autonomia strategica nazionale ed europea nel settore del digitale

A livello UE, l'eccessiva frammentazione e competizione tra gli Stati Membri ha costituito, fino ad oggi, un grosso ostacolo allo sviluppo di tecnologia "made in EU" e alla creazione di grandi aziende di erogazione di servizi digitali. L'UE e, in particolare, l'Italia, si trova in una posizione di dipendenza tecnologica da altri Paesi, leader nella produzione di software e delle cosiddette Emerging and Disruptive Technologies quali, ad esempio, l'Intelligenza Artificiale e il quantum computing. Ciò ha inevitabili ricadute anche sulla possibilità di detenere un controllo diretto sui dati conservati, elaborati e trasmessi attraverso tali tecnologie. Infatti, più si è autonomi dal punto di vista tecnologico e più si possono attuare politiche di sovranità delle informazioni.

Anticipare l'evoluzione della minaccia cyber

A seguito dell'esperienza maturata dal nostro Paese nell'implementazione del "Quadro strategico nazionale per la protezione dello spazio cibernetico" (2013) e dell'annesso "Piano nazionale per la protezione cibernetica e la sicurezza informatica" (aggiornato nel 2017), quali primi documenti strategici nazionali in materia di cybersecurity, è apparso chiaro come sia necessario puntare su tattiche di difesa attiva – che si aggiungono alle buone pratiche di cyber resilienza e due diligence – volte ad aumentare i costi di eventuali attività cyber offensive, così da renderle economicamente svantaggiose. Ciò presuppone, tuttavia, un cambio radicale di paradigma. Se è vero, infatti, che rincorrere la minaccia non è una strategia vincente, è anche vero che stare al passo con essa non è più sufficiente. Occorre, per quanto possibile, anticiparla, ossia prevederla, prevenirla e mitigarne il più possibile gli impatti.

Gestione di crisi cibernetiche

Le ultime tensioni internazionali hanno messo in evidenza l'importanza primaria di un meccanismo efficiente di gestione delle crisi cibernetiche, che consenta, con l'apporto di tutti i soggetti interessati, di graduare le attività sulla base di scenari predefiniti della minaccia cyber – che vanno dalla pre-allerta in vista di possibili eventi cyber sistemici su larga scala, fino al loro verificarsi in maniera conclamata – al ricorrere dei quali viene innescata l'immediata applicazione di strumenti, procedure e norme di linguaggio comuni. La rapidità con cui eventi cyber possono verificarsi e susseguirsi, specie in scenari geopolitici complessi, richiede, infatti, un coordinamento continuativo tra tutti i soggetti pubblici e privati interessati, nonché prontezza nel dispiegamento di un set predefinito di misure.

Contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida

La digitalizzazione di ogni aspetto della vita sociale, volano di crescita economica e sociale dei sistemi democratici occidentali, è sempre più sfruttata per azioni che mirano ad influenzare, interferire o tentare di condizionare il libero esercizio delle libertà fondamentali, specie a ridosso di momenti strategici per i sistemi democratici come quelli connessi allo svolgimento di consultazioni elettorali, allo sviluppo di processi decisionali su questioni di rilevanza strategica ovvero in concomitanza con situazioni di crisi internazionale. Il ricorso sempre più massivo alla disinformazione online richiede, specie quando essa assume connotazioni strutturate, azioni preventive e di contrasto sinergiche e coordinate a livello sia nazionale che internazionale per ostacolare i tentativi di mettere a repentaglio il sistema di valori su cui si base il nostro Paese.

GLI STRUMENTI PER L'IMPLEMENTAZIONE DELLA STRATEGIA

Per implementare la presente strategia e affrontare le richiamate sfide, è previsto un adeguato programma di investimenti e leve finanziarie.

Al di là degli strumenti finanziari già assegnati alle Amministrazioni con competenza in materia cyber, potranno anche essere messi a disposizione appositi fondi previsti di anno in anno dalle leggi finanziarie, per supportare specifici progetti di interesse. A tale fine sarà riservata una quota percentuale degli investimenti nazionali lordi su base annuale. Tali leve finanziarie potranno anche consistere in sgravi fiscali per le aziende o nell'introduzione di aree nazionali a tassazione agevolata per la costituzione, ad esempio, di un "parco nazionale della cybersicurezza" e dei relativi "hub" delocalizzati sull'intero territorio nazionale.

Fondi nazionali
Quota percentuale (1,2%) degli investimenti nazionali lordi su base annuale

Tali risorse saranno dedicate a specifiche progettualità volte a traguardare il conseguimento dell'autonomia tecnologica in ambito digitale, oltre che l'ulteriore innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali.

Vi saranno, inoltre, anche i finanziamenti che l'Agenzia sarà chiamata a gestire in quanto, sempre ai sensi del citato decreto, è designata quale Centro Nazionale di Coordinamento (NCC) ex articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021. Tale atto normativo istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, unitamente alla rete dei centri nazionali di coordinamento, il quale convoglierà in particolare i finanziamenti provenienti dai programmi **Orizzonte Europa** ed **Europa Digitale.**

Orizzonte Europa
Bilancio totale 2021-2027:
95,51 miliardi di Euro

Principale programma di finanziamento dell'UE per facilitare la collaborazione e rafforzare l'impatto della ricerca e dell'innovazione nello sviluppo, nel sostegno e nell'attuazione delle politiche dell'UE, affrontando, nel contempo, le sfide globali. Esso sostiene la creazione e una migliore diffusione di conoscenze e tecnologie di eccellenza.
Inoltre, crea posti di lavoro, impegna pienamente il bacino di talenti dell'UE, stimola la crescita economica, promuove la competitività industriale e ottimizza l'impatto degli investimenti all'interno di uno Spazio europeo della ricerca rafforzato.

Europa Digitale
Bilancio totale 2021-2027:
7,59 miliardi di Euro

Primo piano europeo di finanziamento per espandere le competenze digitali dei cittadini e delle imprese e per velocizzare la ripresa economica e sociale.
Il programma, che mira a colmare il divario tra la ricerca sulle tecnologie digitali e la diffusione sul mercato, finanzia progetti in cinque settori cruciali:

- supercalcolo
- intelligenza artificiale
- cybersicurezza
- competenze digitali avanzate
- uso diffuso delle tecnologie digitali nell'economia e nella società.

Gli investimenti sostengono il duplice obiettivo dell'Unione europea della transizione verde e della trasformazione digitale e rafforzano la resilienza e la sovranità digitale dell'Unione.

IL PIANO NAZIONALE DI RIPRESA E RESILIENZA: INVESTIMENTO 1.5 "CYBERSECURITY"

Ulteriore strumento strategico per affrontare le sfide è il **Piano Nazionale di Ripresa e Resilienza (PNRR).** Nell'ambito della Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", sono incluse le attività di transizione digitale della Pubblica Amministrazione, quali il progetto del Cloud Nazionale e la digitalizzazione dei processi e servizi per i cittadini, la cui realizzazione porterà al potenziamento delle capacità di resilienza delle infrastrutture e dei servizi digitali del Paese. Inoltre, lo specifico Investimento 1.5 "Cybersecurity" - pari a 623 milioni di euro - rimesso all'Agenzia per la Cybersicurezza Nazionale quale Soggetto Attuatore, prevede la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio cyber, con strette connessioni, a livello nazionale e internazionale, con tutti i principali partner della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. Ciò, al fine di conseguire un'autonomia tecnologica nazionale ponendo la cybersicurezza e la resilienza a fondamento della trasformazione digitale della Pubblica Amministrazione.

PNRR (transizione digitale)
Bilancio totale 2021-2026: 122,6 miliardi di Euro

Con il programma Next Generation EU (NGEU), l'Unione prevede investimenti e riforme per accelerare la transizione ecologica e digitale, migliorare la formazione delle lavoratrici e dei lavoratori, e conseguire una maggiore equità di genere, territoriale e generazionale.
L'Italia è la prima beneficiaria dei due principali strumenti del NGEU: il Dispositivo per la Ripresa e Resilienza (RRF) e il Pacchetto di Assistenza alla Ripresa per la Coesione e i Territori d'Europa (REACT-EU). Il dispositivo RRF richiede agli Stati membri di presentare un pacchetto di investimenti e riforme: il Piano Nazionale di Ripresa e Resilienza (PNRR). Il Piano si articola in sei Missioni e 16 Componenti.
Le sei Missioni del Piano sono: digitalizzazione, innovazione, competitività, cultura e turismo; rivoluzione verde e transizione ecologica; infrastrutture per una mobilità sostenibile; istruzione e ricerca; inclusione e coesione; salute.

Il piano di attuazione, d'intesa con il Dipartimento per la Trasformazione Digitale (DTD) nella sua veste di Amministrazione Titolare dell'investimento, è organizzato in tre principali aree d'intervento e, in accordo alle regole tecnico-organizzative del PNRR, coinvolgerà tutti i principali attori nazionali, pubblici e privati, del mondo della cybersecurity:

01 **174 M€**

SERVIZI CYBER NAZIONALI

Contribuendo all'attivazione e piena operatività dell'Agenzia, le reti e i servizi che saranno realizzati potenzieranno le capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione di minacce cyber.

02 **301.7 M€**

INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER PER LA PA

Le capacità cyber della PA sono un elemento fondante per una transizione digitale sicura del Paese, assicurando quindi adeguati livelli di sicurezza per i dati e i servizi dei cittadini.

03 **147.3 M€**

LABORATORI DI SCRUTINIO E CERTIFICAZIONE TECNOLOGICA

Il raggiungimento di un'autonomia tecnologica nazionale passa necessariamente anche dal potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica, in stretta collaborazione con il mondo privato dell'industria e dell'accademia.

#2

Visione strategica: gli obiettivi da perseguire

#2

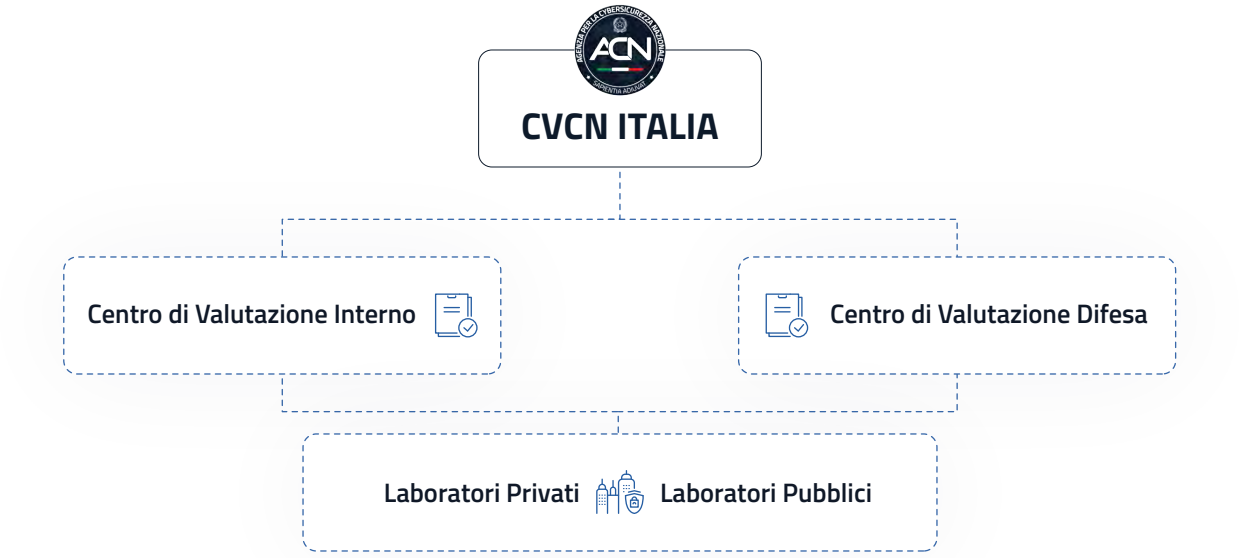
Visione strategica: gli obiettivi da perseguire

Per fronteggiare al meglio le sfide per il sistema-Paese sopra delineate, sono stati individuati **tre obiettivi fondamentali** – protezione, risposta e sviluppo – e relative misure, funzionali ad assicurare la concreta attuazione della strategia, raggruppate per aree tematiche e declinabili sia dal punto di vista organizzativo e di policy che prettamente operativo. Ciascuna misura è stata associata all'obiettivo maggiormente caratterizzante, per ognuna delle quali è indicato il novero degli attori responsabili dell'implementazione e tutti gli altri soggetti a vario titolo interessati, al netto di quelli direttamente beneficiari delle misure.

Rimandando al Piano di implementazione per una descrizione dettagliata delle misure, si intende fornire di seguito una visione d'insieme e il più possibile esaustiva, degli aspetti salienti e della relativa visione strategica alla base dello stesso.

1. OBIETTIVO PROTEZIONE

La **protezione** degli asset strategici nazionali, attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese. Di particolare importanza è lo sviluppo di strategie e iniziative per la verifica e valutazione della sicurezza delle infrastrutture ICT, ivi inclusi gli aspetti di approvvigionamento e supply-chain a impatto nazionale.



Per poter assicurare un livello di protezione efficace e duraturo è, infatti, indispensabile:

A. il **potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale (CVCN)** dell'Agenzia per la Cybersicurezza Nazionale e, negli ambiti di competenza, dei **Centri di Valutazione (CV)** del Ministero dell'Interno e della Difesa, nonché l'integrazione con una rete di Laboratori Accreditati di Prova, permetterà di sviluppare capacità nazionali di valutazione delle vulnerabilità di tecnologie avanzate a servizio degli asset più critici del Paese;

B. la **definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente** in materia di cybersicurezza, che tenga conto degli orientamenti e degli sviluppi in ambito europeo ed internazionale. Tale impianto non ricomprende solamente il livello normativo, quanto anche l'insieme di linee guida, schemi di certificazione e policy settoriali rivolte ai soggetti pubblici e agli operatori privati. In tale contesto, assume rilevanza primaria:

   - il *supporto allo sviluppo di schemi di certificazione e standard europei e internazionali* in materia di cybersicurezza;
   - la *promozione dell'utilizzo di schemi di certificazione europea in materia di cybersicurezza,* da parte delle imprese italiane specializzate, al fine di conseguire un vantaggio competitivo sul mercato;

- l'*adozione di linee guida per le amministrazioni pubbliche*, basate su di un approccio "zero trust" quale cambiamento di paradigma nella gestione del rischio cyber, affinché le relative reti, sistemi e servizi soddisfino elevati standard di cybersicurezza;
- la *valorizzazione dell'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT* della Pubblica Amministrazione;
- la *definizione di una politica nazionale sulla divulgazione coordinata di vulnerabilità*, così da porre il Paese al passo con altre nazioni e con quanto richiesto dalla comunità internazionale;

C. la **conoscenza approfondita del quadro della minaccia cibernetica** e il possesso di adeguati strumenti tecnici, competenze specialistiche e capacità operative, in capo agli attori a vario titolo coinvolti. L'*ulteriore rafforzamento della situational awareness* mediante *il monitoraggio continuo degli eventi cibernetici* e la tempestiva condivisione delle connesse risultanze, secondo gli specifici ambiti di competenza, costituisce, infatti, condizione necessaria ai fini dell'incremento delle capacità nazionali di difesa, resilienza, contrasto al crimine informatico e cyber intelligence. A tal fine, appare essenziale il costante scambio informativo pubblico-privato e pubblico-pubblico, anche mediante l'introduzione di canali di comunicazione protetti e di un sistema integrato di gestione del rischio cyber per identificare e analizzare vulnerabilità, minacce e rischi in chiave previsionale e programmatica;

D. il **potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione**, assicurando una trasformazione digitale sicura e resiliente. A tal fine, la transizione verso il Cloud della Pubblica Amministrazione, sia verso tecnologie di Public Cloud che mediante la creazione di un Polo Strategico Nazionale (PSN), rappresenta un elemento fondante per garantire adeguate garanzie di autonomia tecnologica del Paese. Il consolidamento delle infrastrutture computazionali delle Pubbliche Amministrazioni consente, inoltre, alle stesse, di poter ridurre il numero di esperti in cybersecurity e governance IT a cui fare ricorso. La *migrazione a tecnologie Cloud*, siano esse del PSN o del Public Cloud, sarà guidata e controllata da una metodologia di gestione del rischio il cui elemento principale è la classificazione dei dati e dei servizi della Pubblica Amministrazione (ovvero ordinari, critici e strategici). Al riguardo saranno altresì *coordinati interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber* nella Pubblica Amministrazione;

E. lo **sviluppo di capacità di protezione per le infrastrutture nazionali**, realizzate anche mediante programmi con i privati, tra cui:

- il monitoraggio delle configurazioni Border Gateway Protocol (BGP) mediante lo sviluppo di procedure, processi e strumenti in cooperazione con gli Internet Exchange Point (IXP) nazionali, al fine di aumentare la resilienza delle infrastrutture BGP nazionali;
- un'infrastruttura di risoluzione Domain Name System (DNS) nazionale, con servizi di protezione della navigazione web a uso della PA, per un utilizzo più sicuro della rete Internet;

- il monitoraggio di vulnerabilità e configurazioni erronee dei servizi digitali della PA, sia a livello applicativo che di configurazioni DNS, al fine di ridurre in modo proattivo potenziali superfici di attacco;
- il monitoraggio delle configurazioni dei domini di posta elettronica della PA, supportando e facilitando l'applicazione delle migliori configurazioni di sicurezza contro eventi di phishing o abusi collegati;

F. la ***promozione dell'uso della crittografia*** come strumento di cybersicurezza, favorendo l'impiego di crittografia commerciale lungo l'intero ciclo di vita dei sistemi e servizi ICT, in conformità ai principi della sicurezza e della tutela della privacy, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea. In tale contesto e in settori specifici, l'ACN, anche in sinergia con le altre Amministrazioni, intende sviluppare tecnologie/sistemi di cifratura nazionale, il che ha come prerequisito la creazione di un apposito ecosistema nazionale per il suo mantenimento ed evoluzione;

G. l'***implementazione di un'azione di coordinamento nazionale***, coerente con le iniziative adottate a livello europeo e in sinergia con i Paesi like-minded, per prevenire e contrastare la ***disinformazione online***, che sfruttando le caratteristiche del dominio cibernetico, mira a condizionare/influenzare processi politici, economici e sociali del Paese.

2. OBIETTIVO RISPOSTA

La **risposta** alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale. Una risposta quanto più tempestiva e risolutiva deve, infatti, necessariamente basarsi su:

A. un **sistema di gestione crisi cibernetica nazionale** – assicurato dal Nucleo per la Cybersicurezza (NCS) – **e transnazionale,** che sia fondato su procedure di collaborazione consolidate supportate da costanti flussi informativi ed elementi di conoscenza condivisi anche grazie a reti e infrastrutture nazionali e transnazionali, con il coinvolgimento delle Amministrazioni e degli operatori privati interessati.
In tale ambito dovranno altresì essere assicurati:

- lo sviluppo di un *sistema di coordinamento continuativo* di tutte le Amministrazioni che compongono il NCS, che garantisca una tempestiva e sinergica gestione dei vari possibili scenari di crisi cibernetica, nonché una immediata implementazione delle misure di risposta;

- il *periodico aggiornamento delle procedure operative* relative alle misure di risposta connesse ai vari scenari della minaccia cyber per le determinazioni del Presidente del Consiglio, ai sensi della vigente normativa nazionale, e per la conseguente corretta implementazione da parte dei soggetti interessati;
- una *pronta attività di comunicazione istituzionale* in caso di incidenti cyber rilevanti o di crisi cibernetica, nonché ogni qual volta si renda necessario svolgere azioni di sensibilizzazione nei confronti della popolazione civile;

APPROFONDIMENTO - LA GESTIONE DEGLI INCIDENTI E DELLE CRISI DI CYBERSICUREZZA

L'architettura nazionale per la gestione degli incidenti e delle crisi di cybersicurezza si incardina perfettamente nella piattaforma definita dalla Raccomandazione UE 2017/1584 (c.d. Blueprint), con il livello:

- **politico**, rappresentato dal Presidente del Consiglio dei ministri, dall'Autorità delegata per la sicurezza della Repubblica, ove istituita, e dal Comitato Interministeriale per la Sicurezza della Repubblica (CISR);
- **operativo**, costituito dal NCS, supportato dall'ACN in raccordo con le strutture competenti delle Amministrazioni NCS;
- **tecnico**, realizzato dallo CSIRT Italia, in raccordo con le altre articolazioni tecniche delle Amministrazioni NCS.

L'ACN, con al suo interno lo CSIRT Italia, il PoC NIS e il NCS, ricopre due dei tre livelli funzionali a consentire una prevenzione e risposta adeguata a potenziali attacchi cyber al sistema-Paese, fornendo supporto al livello politico, per il tramite del Direttore Generale, quale coordinatore delle crisi di cybersicurezza. Questa struttura sinergica determina un processo che, in pieno allineamento con gli omologhi europei e internazionali, vede la valorizzazione delle informazioni, delle segnalazioni o delle notifiche acquisite dal livello tecnico operativo in eventi cyber che necessitano l'attivazione del NCS e l'eventuale elevazione del suo stato di funzionamento, fino alla crisi di cybersicurezza.

Tale assetto si completa, inoltre, con il ruolo di collegamento che l'ACN assicura con l'Unione europea. Sul versante comunitario, infatti, l'ACN fa parte della rete CyCLONe (Cyber Crisis Liaison Organisation Network) e della rete europea degli CSIRT.

In particolare, la rete CyCLONe per la risposta rapida alle crisi e agli incidenti cyber transfrontalieri su larga scala, mira ad implementare il relativo meccanismo europeo (c.d. "Blueprint") ed a supportare le strutture di cybersecurity, raccordando il livello politico europeo – ovvero il Consiglio UE, anche tramite i meccanismi integrati per la risposta politica alla crisi (IPCR) – con il livello tecnico, ovvero gli CSIRT nazionali e la rete europea degli CSIRT. Le funzioni di CyCLONe, su base volontaria, comprendono la preparazione, la conoscenza situazionale, la cooperazione nella gestione crisi e il supporto al decisore politico nazionale ed europeo.

B. l'integrazione degli attuali **servizi cyber nazionali** nei seguenti ambiti:

- *identificazione della minaccia* realizzando un "Hyper SOC", ovvero un sistema di raccolta, correlazione e analisi di eventi di interesse da Security Operation Center (SOC), nonché dagli *Internet Service Provider (ISP)* mediante apposite convenzioni, al fine di individuare precocemente eventuali "pattern" di attacco complessi che potrebbero rappresentare minacce emergenti di interesse;
- *assicurare e facilitare modalità di notifica unitaria degli incidenti di sicurezza cibernetica al Computer Security Incident Response Team (CSIRT),* così da rendere più efficace la capacità di risposta e allarme tempestivo;
- *risposta agli incidenti* realizzando una rete di CSIRT/Computer Emergency Response Team (CERT) settoriali federati con lo CSIRT Italia per la condivisione di procedure, informazioni e supporto nella risposta alle minacce emergenti e agli incidenti;
- *condivisione di informazioni* realizzando un Information Sharing and Analysis Center (ISAC) centrale presso l'Agenzia, integrabile con una rete di ISAC settoriali sviluppati mediante iniziative pubblico-private, che possa potenziare la diffusione e l'applicazione di informazioni a maggior valore aggiunto per l'innalzamento del livello di cyber resilience del Paese, quali ad esempio best-practice di settore, linee guida, avvisi di sicurezza e raccomandazioni;
- *qualificazione di aziende in materia di incident response*, in grado di fornire supporto allo CSIRT Italia nel caso in cui dovesse verificarsi una moltitudine di incidenti cyber di natura sistemica.

Queste capacità sono pienamente in linea con l'iniziativa lanciata dalla Strategia di cybersecurity dell'Unione europea di realizzazione di uno "EU CyberShield" e si avvarranno delle più recenti tecnologie di intelligenza artificiale (IA) e machine learning messe a disposizione da un centro di "High Performance Computing" (HPC) realizzato ad hoc, nonché da sistemi integrati di monitoraggio e analisi del rischio cyber nazionale. L'Italia si porrà alla guida, in Europa, del processo di sviluppo e di integrazione con i diversi Stati membri di questi nuovi strumenti tecnologici.

C. *l'organizzazione di periodiche* ***esercitazioni di sicurezza cibernetica e resilienza***, anche nell'ambito del Perimetro di sicurezza nazionale cibernetica, nonché la *promozione e il coordinamento della partecipazione a quelle europee e internazionali;*

D. la ***definizione del posizionamento e della procedura nazionale in materia di attribuzione*** di attività cibernetiche ostili, che specifichi anche i diversi attori coinvolti e il relativo contributo. Il nostro Paese, infatti, quale membro dell'UE e della NATO, è sovente chiamato ad apportare il proprio contributo nei rispettivi consessi, per l'applicazione delle misure di risposta ad attività cyber ostili – incluso il rilascio di dichiarazioni congiunte – contemplate nell'EU Cyber Diplomacy Toolbox e nella NATO Guide for Response Options to Malicious Cyber Activities. È importante evidenziare al riguardo come l'attribuzione costituisca prerogativa nazionale dei singoli Paesi membri, come riconosciuto nei documenti di policy delle citate organizzazioni;

E. il ***contrasto al cybercrime***, declinato nella prevenzione e nel contrasto delle attività criminali di matrice comune, organizzata e terroristica rivolte all'integrità delle infrastrutture critiche informatizzate, erogatrici dei servizi pubblici essenziali; nella prevenzione e nel contrasto ai financial cybercrime ed alle attività illecite dirette a colpire le infrastrutture finanziarie; nell'attività infoinvestigativa condotta, in collaborazione con i competenti Uffici della PS, in materia di tutela dell'ordine pubblico e di contrasto al terrorismo, colti nella loro proiezione cibernetica; nella tutela della persona, con particolare riguardo alla protezione dei minori, dalle aggressioni alla libertà personale e sessuale, alla sicurezza, all'incolumità, alla riservatezza, all'onore ed alla reputazione che si realizzano nella dimensione virtuale, ovvero mediante l'utilizzo di strumenti informatici o telematici;

F. il ***rafforzamento delle capacità di deterrenza in ambito cibernetico***.

3. OBIETTIVO SVILUPPO

Lo **sviluppo** consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato. La costellazione di centri di eccellenza e imprese che compongono, assieme all'accademia, il tessuto della ricerca e dello sviluppo è infatti un patrimonio essenziale per il nostro Paese con importanti potenzialità di espansione. Numerosi sono gli strumenti e le iniziative avviate negli ultimi anni per supportare lo sviluppo delle capacità del sistema nazionale di ricerca, la trasformazione digitale e l'innovazione tecnologica, tra cui si annoverano, in particolare, quelli previsti dal PNRR, dalle ultime leggi di bilancio, e dal Piano Nazionale Impresa 4.0. Per accrescere ulteriormente tale impegno, è pertanto fondamentale:

A. il ruolo del **Centro Nazionale di Coordinamento (NCC)** che, in stretto raccordo con il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC), è chiamato a supportare lo sviluppo e il potenziamento dell'autonomia strategico-tecnologica e digitale dell'Unione europea e del nostro Paese. Ciò, *coordinando le attività di ricerca e sviluppo*, favorendo l'osmosi con il mondo industriale, accademico e della ricerca per l'avvio di progetti e partnership pubblico-private in cybersicurezza, mediante l'*accesso a finanziamenti nazionali ed europei.* In questo senso, risultano fondamentali le *sinergie con i Centri di competenza ad alta specializzazione e i Digital Innovation Hub (DIH)* attivi sul territorio nazionale;

B. lo **sviluppo di tecnologia nazionale ed europea**, così da ridurre la dipendenza da tecnologie extra-UE, attraverso l'avvio di dedicate progettualità che saranno realizzate - grazie a specifici stanziamenti utilizzando sia fondi nazionali che europei - nell'ambito di un "parco nazionale della cybersicurezza" destinato, a tendere, ad inglobare i *Cluster tecnologici* che svolgono attività in materia. Tale tecnologia consentirà di sviluppare un'industria nazionale ed europea competitiva, anche attraverso una specializzazione virtuosa di startup e piccole e medie imprese (PMI) innovative, in grado di fornire tecnologie e servizi abilitanti ad elevato grado di sicurezza, con particolare riguardo alle infrastrutture critiche digitali;

C. la ***realizzazione di un "parco nazionale della cybersicurezza"*** che, mettendo a sistema competenze e risorse provenienti dalla Pubblica Amministrazione, dall'industria e dal mondo accademico e della ricerca, fornisca tutte le infrastrutture tecnologiche necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali quali, a titolo di esempio, l'intelligenza artificiale, il quantum computing & cryptography e la robotica. Con la sua creazione si intende conseguire nel tempo una maggiore autonomia strategica nazionale sulle tecnologie cyber, sostenendo lo sviluppo e la produzione di software e hardware nazionali da impiegare nelle reti e nei sistemi di maggiore rilevanza strategica. Il parco è concepito come un incubatore di capacità e tecnologie, al cui interno giovani talenti e startup possano entrare in contatto con le grandi aziende e con le diverse realtà nazionali che, a vario titolo, operano nel settore. Per tale motivo, il parco deve poter disporre di una struttura "diffusa" nella quale, accanto ad un "hub" centrale, sussistono ramificazioni distribuite sull'intero territorio nazionale;

D. l'introduzione di nuovi meccanismi e soluzioni incentivanti per continuare a supportare lo **sviluppo industriale, tecnologico e della ricerca**, con particolare riferimento allo sviluppo di competenze e al trasferimento tecnologico (specie nei settori avanzati della cybersicurezza).
Ciò, anche con l'obiettivo di:

- continuare a *favorire la competitività del sistema produttivo del Paese,* sostenendo le imprese nella loro transizione digitale ed ecologica, *agevolandone l'internazionalizzazione e l'attrazione di investimenti;*
- *realizzare prodotti e servizi ICT ad alta affidabilità,* anche incoraggiando la creazione di *Product Secu-*

rity Incident Response Team (PSIRT) da parte degli operatori privati, per accrescere le loro capacità di gestire le vulnerabilità di prodotti ICT;

E. il continuo ***impulso all'innovazione tecnologica e alla digitalizzazione*** *della Pubblica Amministrazione e del tessuto produttivo del Paese,* assicurando una costante rispondenza ai principi di cybersicurezza e facendo ricorso alle *risorse messe a disposizione dal PNRR.* Ciò va di pari passo con la promozione di iniziative volte a rafforzare l'autonomia industriale e tecnologica dell'Italia.

FATTORI ABILITANTI

Per poter realizzare fattivamente gli obiettivi descritti, è indispensabile fare riferimento a una serie di **fattori abilitanti** – formazione, promozione della cultura della sicurezza cibernetica e cooperazione – i quali, data la loro trasversalità, sono necessariamente correlati a tutti e tre gli obiettivi sopra delineati, quali elementi imprescindibili per la loro piena attuazione.

In primo luogo, la **formazione** in ambito cyber, con particolare focus sulle nuove tecnologie. Lo sviluppo di nuove iniziative e il rafforzamento di quelle esistenti deve muovere, infatti, dall'esigenza sempre più concreta di stimolare la creazione di una solida forza lavoro nazionale, composta da esperti e giovani talenti in possesso delle capacità e delle competenze necessarie per poter essere applicate a beneficio delle imprese e delle amministrazioni italiane, con riferimento alle tecnologie informatiche in generale e a quelle relative alla sicurezza cibernetica in particolare. Questo deve realizzarsi tramite:

- meccanismi incentivanti che favoriscano la progressiva *familiarizzazione degli studenti con le nuove tecnologie informatiche*, con approccio formativo e di respiro culturale, prima ancora che tecnico e pratico; è opportuno intervenire, prevedendo l'introduzione dell'informatica come disciplina, in tutti i livelli del sistema educativo, dalla scuola primaria all'università e, dalla secondaria di secondo grado in poi, in tutti i contesti, inclusi quelli generalisti e quelli orientati verso professioni non tecniche;
- meccanismi incentivanti che promuovano l'inserimento in carriere tecnico-scientifiche (cercando anche di colmare il divario di genere presente in esse), con particolare riferimento agli aspetti ci cybersicurezza; anche qui sono necessari interventi a vari livelli: i percorsi tecnici e professionali della scuola secondaria di secondo grado; gli *Istituti Tecnici Superiori (ITS)*; i corsi di laurea ad orientamento professionale recentemente introdotti dalla normativa; i corsi di laurea e laurea magistrale tradizionali, i master e i dottorati di ricerca; specifica attenzione va dedicata agli ITS e ai corsi di laurea ad orientamento professionale che, realizzati in collaborazione con realtà produttive, possono favorire il rapido inserimento nel mondo del lavoro e la calibrazione dei profili e quindi dei percorsi formativi;
- il *continuo aggiornamento della didattica e della preparazione del corpo docente*, a tutti i livelli di istruzione scolastica e universitaria, *affinché l'offerta educativa sia al passo con lo sviluppo delle conoscenze e delle tecnologie e con le esigenze dettate dal mercato del lavoro*, secondo un approccio fondato sul binomio, ormai inscindibile, sviluppo e sicurezza;

- il *dispiegamento di fondi per la formazione specialistica e l'aggiornamento professionale nei settori pubblico e privato*, da realizzarsi in modo continuo e multilivello così da favorire la crescita e la qualificazione delle risorse umane operanti nel campo della cybersicurezza e di conseguire una sovranità nazionale digitale delle competenze;
- la realizzazione di un *sistema nazionale di certificazione di tali professionalità* (sia in ambito scolastico/accademico che lavorativo), mediante l'attivazione di percorsi di formazione ad hoc approvati dall'ACN;
- *percorsi di formazione specifici per i non specialisti della materia, rivolti ai dipendenti di Pubbliche Amministrazioni e soggetti privati*, incluse le PMI, ad iniziare dai top manager, così da sensibilizzare gli stessi in merito all'importanza di concepire la cybersicurezza più come un investimento che come un costo;
- il *potenziamento delle capacità di cyber diplomacy*, attraverso percorsi mirati per il personale diplomatico da dispiegare nei principali consessi internazionali sulla tematica e mettersi così al passo con altri Paesi, europei e non.

Le citate azioni saranno sviluppate grazie alla collaborazione con Università, scuole secondarie di secondo grado, Regioni – in base ad appositi accordi – oltre che con Amministrazioni pubbliche e soggetti privati.

Altro fattore abilitante, che si muove in parallelo con le esigenze di formazione, è la **promozione della cultura della sicurezza cibernetica**, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber, le quali includono non solo gli attacchi cibernetici propriamente intesi, ma anche la diffusione di contenuti fake e il fenomeno del cyberbullismo, che, ancorché non nuovo, non cessa di creare allarme sociale.

Al riguardo, è quindi importante che i soggetti pubblici, gli operatori privati e la società civile nel suo complesso, percepiscano il proprio ruolo quale parte attiva e responsabile all'interno del sistema-Paese, attuando comportamenti sicuri e virtuosi nello spazio cibernetico. Ciò deve avvenire:

- attraverso la previsione di un *programma capillare di educazione digitale* – da sviluppare anche online – a beneficio della collettività e diretto all'adozione di buone prassi e all'acquisizione di capacità di verificare i contenuti e le informazioni reperite online avendo contezza di quegli indicatori che consentono di identificare le c.d. "fake news";
- *all'interno delle organizzazioni pubbliche e private*, mediante una forte sensibilizzazione delle risorse – *ad iniziare dai livelli apicali per poi coinvolgere l'intera line* – non soltanto per promuovere una "cyber hygiene" interna, quanto per accrescere la percezione delle esigenze di sicurezza dell'organizzazione e delle minacce a cui questa è esposta, nonché per mettere in campo le azioni di prevenzione più efficaci;
- promuovendo la gestione consapevole del cd. "rischio residuo", anche prevedendo l'adozione di strumenti di autovalutazione basati su specifici "cyber index", che consentono alle organizzazioni una gestione autonoma del livello di esposizione.

Da ultimo vi è la **cooperazione,** da incrementare:

- sul fronte nazionale, a livello governativo, nel rapporto pubblico-privato, pubblico-pubblico, nonché con accademia e ricerca. In tale contesto, è prevista la creazione di tavoli operativi permanenti con i soggetti Perimetro suddivisi per settore, a seconda delle trattazioni ed esigenze contingenti, per creare maggiori sinergie tra le Pubbliche Amministrazioni e l'industria;
- in ambito internazionale, partecipando in modo proattivo alle iniziative europee e internazionali e promuovendo collaborazioni bilaterali.

A livello nazionale, ciascuna componente dell'ecosistema cyber è non solo responsabile, per gli ambiti di competenza, della sicurezza nel dominio digitale, ma è portatrice di esperienze e informazioni cruciali per incrementare le capacità di prevenzione e contrasto alle minacce, promuovere il trasferimento di know-how, tecnologie e risorse umane, nonché per consentire alle imprese innovative di espandersi con maggiore facilità sul mercato. A livello internazionale, l'Italia collabora nella promozione del rispetto dei diritti umani, delle libertà fondamentali e dei valori democratici nel dominio cyber, per far sì che questo rimanga uno spazio globale, aperto, stabile e sicuro, in cui il diritto internazionale ed i principi condivisi siano rispettati. A tal fine, il nostro Paese partecipa alle principali iniziative di cooperazione, di cyber diplomacy e di *capacity building* nei confronti di Paesi partner che stanno sperimentando un rapido sviluppo digitale. Ciò, anche attraverso l'*implementazione di confidence building measure (CBM)* dell'OSCE, al fine di evitare l'emergere di tensioni a livello politico-militare derivanti dall'impiego delle tecnologie ICT. Inoltre, l'Italia condivide le metodologie e gli strumenti di deterrenza e risposta ad attacchi cibernetici definiti a livello UE e NATO. In tale contesto, la partecipazione alle iniziative internazionali e la prosecuzione dei dialoghi e delle relazioni con i Paesi di interesse, sono elementi indispensabili per *rafforzare ulteriormente il posizionamento dell'Italia*, per favorire lo scambio di conoscenze e per promuovere l'internazionalizzazione delle imprese nazionali attive nel settore.

Trasversale ai citati obiettivi di protezione, risposta e sviluppo, nonché ai richiamati fattori abilitanti della formazione, della promozione della cultura della cybersicurezza e della cooperazione, è la **Partnership Pubblico-Privato (PPP),** la quale permea interamente la presente strategia, improntata come già detto ad un approccio "whole-of-society", che vede il settore pubblico agire sinergicamente con quello privato, il mondo accademico e della ricerca, i media, le famiglie e gli individui per rafforzare la resilienza cibernetica della nazione e della società nel suo insieme. Lo spazio cibernetico è, peraltro, costituito da prodotti e servizi ICT realizzati ovvero erogati principalmente da soggetti privati. Per tale ragione, la presente strategia non può prescindere da una piena collaborazione e costante consultazione pubblico-privato, che si traduce in una serie di azioni strutturate come, a titolo di esempio, il monitoraggio dello spazio cibernetico attraverso la cooperazione dei SOC, la mitigazione degli incidenti mediante la collaborazione tra CSIRT e l'incident response qualificato, la rete di laboratori di prova, la formazione e la diffusione della consapevolezza.

METRICHE E KEY PERFORMANCE INDICATORS

Infine, la strategia non può ritenersi completa senza un insieme di ***metriche*** e di ***Key Performance Indicator (KPI)***, quali strumenti che consentano di misurare non solo l'effettiva attuazione della stessa, ma anche tutte quelle azioni, da essa contemplate, la cui effettiva efficacia e impatto resterebbero altrimenti inesplorati.

Acronimi

Elenco degli acronimi

ACN	Agenzia per la Cybersicurezza Nazionale
BGP	Border Gateway Protocol
CBM	Confidence Building Measure
CERT	Computer Emergency Response Team
CISR	Comitato Interministeriale per la Sicurezza della Repubblica
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche della Polizia di Stato
CSIRT	Computer Security Incident Response Team
CVCN	Centro di Valutazione e Certificazione Nazionale
CV	Centro di Valutazione
CyCLONe	Cyber Crisis Liaison Organisation Network
DIH	Digital Innovation Hub
DNS	Domain Name System
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTD	Dipartimento per la Trasformazione Digitale
ECCC	Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (European Cybersecurity Competence Centre)
EDT	Emerging and Disruptive Technologies
EU	European Union
FSD	Fornitori di Servizi Digitali
HPC	High Performance Computing
IA	Intelligenza Artificiale
ICT	Information and Communication Technologies
IoT	Internet-of-Things
IPCR	Integrated Political Crisis Response
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
ITS	Istituti Tecnici Superiori

IXP	Internet Exchange Point
KPI	Key Performance Indicator
MAECI	Ministero degli Affari Esteri e della Cooperazione Internazionale
NATO	North Atlantic Treaty Organization
NCC	Centro Nazionale di Coordinamento (National Coordination Centre)
NCS	Nucleo per la Cybersicurezza
NGEU	Next Generation EU
NIS	Network and Information Security
NSTPFT	Nucleo Speciale Tutela Privacy e Frodi Tecnologiche
OSCE	Organizzazione per la Sicurezza e la Cooperazione in Europa
OSE	Operatori di Servizi Essenziali
PA	Pubblica Amministrazione
PIL	Prodotto Interno Lordo
PMI	Piccole e Medie Imprese
PNRR	Piano Nazionale di Ripresa e Resilienza
PoC NIS	Punto di contatto unico NIS
PPP	Partnership Pubblico-Privato
PS	Polizia di Stato
PSIRT	Product Security Incident Response Team
PSN	Polo Strategico Nazionale
PSNC	Perimetro di sicurezza nazionale cibernetica
REACT-EU	Recovery Assistance for Cohesion and the Territories of Europe
ROS	Raggruppamento Operativo Speciale dell'Arma dei Carabinieri
RRF	Recovery and Resilience Facility
SOC	Security Operation Center
STEM	Science, Technology, Engineering and Mathematics
UE	Unione europea


REPUBBLICA ITALIANA
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT