EXECUTIVE SUMMARY

CAPITOLO 1
Lo stato della cibersicurezza in Europa e in Italia

La costante e ingente evoluzione dell'ecosistema digitale ha generato una vasta gamma di nuove opportunità per individui e imprese. Allo stesso tempo, al crescente impiego delle nuove tecnologie si è accompagnata l'intensificazione di rilevanti rischi, in particolare, quelli riconducibili alla minaccia cibernetica. Dai dati Clusit si evince come negli ultimi anni **il numero di cyberattacchi annuali a livello globale sia cresciuto di oltre il 60%**, passando dalle 1.554 del 2018 alle 2.489 del 2022. Inoltre, anche **i valori inerenti il primo semestre del 2023 appaiono preoccupanti**, in quanto si è raggiunta una quota di 1382 attacchi, ben **637 in più rispetto al primo semestre del 2018**.

Negli ultimi tre anni si è instaurata una tendenza che ha visto prevalere **gli attacchi con severity "Critica"**, ovvero che hanno prodotto effetti dannosi importanti per le vittime, tra cui ingenti perdite economiche e di dati. Si è passati dal **32% nel 2021, al 36% nel 2022 e al 40% nel primo semestre del 2023**. In merito alla **distribuzione geografica delle vittime**, nel primo semestre del 2023 i numeri più elevati sono quelli riconducibili al continente americano, **mentre l'Europa si posiziona seconda attraendo il 22% delle azioni dei cybercriminali**.

A livello italiano, nel primo semestre 2023 sono stati registrati **132 attacchi di particolare gravità**, che si traducono in una **media mensile di 22**, circa **dieci volte più elevata rispetto a quella rilevata nel 2018** (2,5). Il settore industriale che ha attratto il maggior numero di attacchi in Italia è la Pubblica Amministrazione (23%), seguita a breve distanza da target multipli e dalla manifatturiera (17%). In termini di severity, il dato italiano nel primo semestre del 2023 assume un andamento particolare, in quanto a **differenza di quello mondiale (40%) gli incidenti con impatto "Critico" costituiscono il 21%.** La quota più elevata di attacchi è ricondotta a una severity "Alta" (48% in Italia/38% globale) e "Media" (30% in Italia/21% mondiale), mentre una severity "Bassa" attiene solo al 2% degli episodi.

In un contesto come quello appena delineato, gli **investimenti in cybersicurezza** assumono un ruolo di significativa importanza, in quanto rappresentano la prima risposta, in termini preventivi, alle esigenze che incombono sulle imprese e che derivano dalle nuove dinamiche del cyberspazio. Secondo quanto emerso dall'ultima versione del rapporto NIS Investments", **in UE le organizzazioni francesi sono quelle che spendono di più in sicurezza informatica in valore mediano** (€6,30 milioni), **seguite dalle italiane e spagnole** che riportano una spesa rispettivamente pari a **€4,80 e €3,80 milioni**. Questi investimenti rappresentano nel caso della Francia e della Spagna il 6,7% del budget IT, mentre **per l'Italia corrispondono al 7,6%**.

CAPITOLO 2
L'ecosistema normativo sulla cybersecurity

In un contesto socioeconomico sempre più incentrato sull'offerta di servizi digitali è irrinunciabile per gli Stati apprestare misure normative e organizzative che siano in grado di far fronte ai rischi della digitalizzazione, predisponendo tutele efficaci per le risorse (umane, finanziarie e tecnologiche) a disposizione di enti pubblici e imprese da un lato, e per i diritti e le libertà fondamentali degli individui, dall'altro. Se si rivolge lo sguardo sul contesto globale, **nel mese di dicembre del 2016, la Cina ha pubblicato una propria strategia nazionale**, nella quale è rinvenibile un riferimento interessante circa l'importanza del dominio cibernetico, secondo cui esso costituirebbe un mezzo attraverso il quale promuovere la salvaguardia della pace mondiale e, al contempo, la sicurezza e gli

interessi di sviluppo nazionale. Per quanto riguarda il lato più prettamente normativo, **la cibersicurezza in Cina è regolamentata da tre atti principali: la *Cybersecurity Law* (2017), la *Data Security Law* (2021) e la *Personal Information Protection Law* (2021)**. Anche gli **USA** si sono attivati già da diverso tempo nella definizione di una propria strategia di cibersicurezza, **puntando particolarmente su una politica estera in ambito cyber**, la quale – naturalmente – si è evoluta col tempo. Tra gli ultimi interventi, **a marzo 2023 l'amministrazione Biden ha chiarito la strategia di cybersecurity** che guiderà gli Stati Uniti per i prossimi anni, **mentre lo scorso 30 ottobre è stato reso noto l'*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* nell'ambito del quale è possibile rintracciare un focus dedicato alla cybersicurezza**.

In questo contesto generale, l'UE sta delineando un ecosistema normativo della cibersicurezza particolarmente articolato. Nel 2020, in particolare, la Commissione europea ha lanciato il "Cybersecurity package", costituito dalla "Strategia dell'UE in materia di cibersicurezza per il decennio digitale", una nuova direttiva sulla resilienza delle entità critiche ed una proposta di direttiva relativa alle misure necessarie per conseguire un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista). Se la strategia ha declinato proposte concrete di iniziative politiche, di regolamentazione e di investimento per rafforzare resilienza, sovranità tecnologica e leadership, sviluppare capacità operative di prevenzione, dissuasione e risposta e promuovere un ciberspazio globale e aperto, il 27 dicembre 2022 è stata pubblicata sulla G.U. dell'UE la Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (Direttiva CER – Resilience of Critical Entities), il cui termine di recepimento per gli Stati membri è fissato al 17 ottobre 2024. Tale direttiva, in particolare, mira ad aumentare la resilienza di soggetti, negli Stati membri, che sono fondamentali per la fornitura di servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno, in una serie di settori che sono alla base del funzionamento di molti altri settori dell'economia dell'Unione e a migliorare la cooperazione internazionale tra le autorità competenti.

Partendo dalla constatazione della frammentazione normativa conseguente al recepimento della direttiva NIS, all'esito di un ampio e complesso dibattito, il 17 gennaio 2023 è entrata in vigore la **Direttiva NIS 2 (Dir. n. 2555/2022)**, che ha ampliato l'ambito di applicazione soggettivo, abbandonando la precedente distinzione tra OSE e DSP, in favore di una suddivisione tra soggetti essenziali e soggetti importanti (introducendo una soglia per l'applicabilità della disciplina alle imprese), ha prescritto l'adozione di misure tecniche, organizzative e operative adeguate e proporzionate, ha declinato obblighi di segnalazione in caso di incidenti significativi, ha previsto misure di vigilanza e individuato misure per garantire la sicurezza della supply chain. Il 14 settembre 2023 la Commissione europea ha pubblicato i primi orientamenti sull'applicazione di alcune norme fondamentali della Direttiva NIS2 nei quali sono fornite importanti indicazioni circa l'implementazione degli obblighi e la compliance al nuovo assetto normativo.

Se la direttiva NIS, oggi superata dalla NIS2, è intervenuta a disciplinare in maniera organica il tema della sicurezza delineando la cornice normativa ed organizzativa nell'UE e rinsaldando la cooperazione tra stati membri ed istituzioni, il **Regolamento n. 881/2019 (Cybersecurity Act)**, al fine di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cybersicurezza, cyberresilienza e fiducia all'interno dell'Unione, ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA e ha delineato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity. Sull'impianto del regolamento sta intervenendo la Commissione che ha lanciato una proposta di regolamento per quanto riguarda i servizi di sicurezza gestiti.

Sempre in attuazione di quanto previsto nella Strategia del 2020, il **15 settembre 2022** la Commissione ha pubblicato una **proposta di regolamento** sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali **(*Cyber Resilience Act* – CRA)**. Nel definire l'ambito applicativo, la proposta si riferisce **ai prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione logica o fisica diretta o indiretta di dati a un dispositivo o a una rete, individuando tra i prodotti con elementi digitali, quelli critici** (suddivisi in Classe I e II) e fissa una serie corposa di obblighi a carico di produttori, importatori e distributori. Sulla proposta della Commissione, Parlamento e Consiglio hanno raggiunto un **accordo provvisorio sul testo il 30 novembre scorso** che, pur mantenendo l'impianto generale proposto dalla Commissione che tuttavia aveva già subito diverse modifiche nel corso dell'*iter*, introduce una metodologia più semplice per la classificazione dei prodotti digitali, fissa in almeno 5 anni il periodo di sostegno per un prodotto digitale (esclusi i prodotti di cui sia previsto un periodo di utilizzo più breve), fissa obblighi di segnalazione relativi alle vulnerabilità attivamente sfruttate e agli incidenti innanzitutto nei confronti delle autorità nazionali competenti anche se è rafforzato il ruolo dell'ENISA, introduce ulteriori misure di sostegno per le piccole imprese e microimprese, comprese specifiche attività di sensibilizzazione e formazione, nonché il sostegno alle procedure di prova e di valutazione della conformità. Quanto al periodo di applicazione delle norme, nella logica di prevedere per i fabbricanti tempistiche di adeguamento idonee, esso è fissato in tre anni dall'entrata in vigore del regolamento. In ultimo, il 17 gennaio 2023 è entrato in vigore – ma si applicherà dal prossimo 17 gennaio – il **Reg. n. 2554/2022 (DORA)**, che si prefigge l'obiettivo di rafforzare e armonizzare i requisiti di cybersecurity di un'**ampia varietà di entità finanziarie**, sia di stampo tradizionale, sia nuovi attori come i fornitori di servizi per le cripto-attività e fornitori di servizi ICT (es: fornitori di servizi cloud), attraverso la prescrizione di una serie di adempimenti suddivisibili in sei pilastri.

Così come l'UE è impegnata nella definizione di un set di regole in grado di assicurare un'efficace tutela della cybersecurity, anche l'Italia è stata fortemente impegnata negli ultimi anni nella creazione di **un nuovo ecosistema normativo ruotante intorno all'istituzione**, in attuazione delle previsioni del PNRR, **dell'Agenzia per la cybersicurezza nazionale (ACN)** individuata come la principale autorità preposta a livello nazionale ed internazionale alla salvaguardia della cybersicurezza. L'ACN, in particolare, oltre a svolgere tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, nonché tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale, è titolare di un'ampia gamma di competenze anche rispetto all'*awareness,* formazione e ricerca.

Un'altra importante sfida in ambito nazionale concerne l'**implementazione della NIS2**. Lo scorso 27 luglio, in particolare, è stato presentato alla Camera il disegno di legge recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023" (Atto Camera 1342), che all'art. 3 si occupa specificamente dei principi e dei criteri per l'esercizio della delega per il recepimento della direttiva NIS2. Il ddl dopo essere stato approvato dalla Camera il 20 dicembre, è attualmente al vaglio del Senato. Nella medesima legge di delegazione europea all'esame del Senato, l'art. 5 definisce princìpi e criteri direttivi specifici per l'esercizio della delega per il recepimento della direttiva CER (2022/2557).

Sempre nella logica di rafforzare l'ecosistema nazionale della cybersecurity, il **21 settembre 2019**, il **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, ha istituito **il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)** al fine di assicurare un livello elevato di

sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori (pubblici e privati aventi una sede nel territorio nazionale), da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Per raggiungere tale obiettivo, la disciplina istitutiva del perimetro ha tracciato un **percorso attuativo frazionato con scadenze temporali diversificate, che si snoda attraverso cinque decreti del Presidente del Consiglio dei ministri e un regolamento governativo di esecuzione e che, seppur in ritardo, è finalmente giunto a completamento**. In virtù della disciplina disegnata, i soggetti pubblici e privati che offrono tali servizi o svolgono funzioni essenziali e che sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici (interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro) dalle Amministrazioni competenti nei rispettivi settori, sono tenuti a predisporre e aggiornare annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT Italia attivo presso la Presidenza del Consiglio. Tali soggetti, inoltre, sono tenuti – dal 30 giugno 2022 – a comunicare al CVCN l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici" (contenuti nell'elenco di beni ICT). A seguito di questa comunicazione, prende inizio il procedimento di verifica e valutazione dinanzi al CVCN, che si suddivide in tre macro fasi: verifiche preliminari, preparazione all'esecuzione dei test ed esecuzione dei test di hardware e software.

Sempre nella logica di accrescere la sicurezza, la **disciplina Golden Power**, che trova origine e fondamento nel decreto-legge 15 marzo 2012, n. 21 (convertito, con modificazioni, in legge 11 maggio 2012, n. 56), negli anni, ha subito numerosissime modifiche ed integrazioni, anche su spinta europea, tutte orientate ad estendere e/o rafforzare l'esercizio dei poteri speciali. Ed infatti, il **D.L. 25 marzo 2019, n. 22** (convertito, con modificazioni, dalla legge n. 41 del 20 maggio 2019), ha introdotto, nel D.L. n. 21 del 2012, **l'articolo 1-*bis***, che disciplina **l'esercizio dei poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G**, mentre il **D.L. 21 settembre 2019, n. 105** (convertito, con modificazioni, dalla legge n. 133 del 18 novembre 2019) **ha esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori strategici**, coordinandolo con l'attuazione del **Regolamento 2019/452** in materia di controllo degli investimenti esteri diretti nell'Unione europea. Inoltre, **il D.L. n. 21/2022** (convertito con legge 20 maggio 2022, n. 51), recante **"Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina", nel Titolo IV ha dedicato il Capo I al Golden Power**, introducendo una serie di importantissime novità che di fatto hanno ridisegnato la disciplina sui poteri speciali. Una novità rilevante per quanto concerne **l'ambito di applicazione della disciplina GP**, è stata introdotta con il **d. l. n. 104/2023 (c.d. Decreto Asset)** autorizza l'applicazione del golden power a tecnologie particolarmente critiche, inclusi l'IA, la cybersecurity e i macchinari per la produzione di chip.

In attuazione dell'art. 2-quater "Misure di semplificazione dei procedimenti e prenotifica", con **DPCM 1° agosto 2022, n. 133**, pubblicato sulla G.U. del 9 settembre ed entrato in vigore il successivo 24 settembre, è stato adottato il Regolamento recante disciplina delle attività di coordinamento della Presidenza del Consiglio dei ministri propedeutiche all'esercizio dei poteri speciali. Tale regolamento, in particolare,

persegue il fine di semplificare la procedura di notifica e ridurre il numero di notifiche che sono passate da 342 a 608 in soli due anni (2020-2022).
Da ultimo, nella logica di valutare l'impatto dell'esercizio dei poteri speciali ed apprestare interventi compensativi a sostegno delle imprese destinatarie delle relative misure, con **D.L. 5 dicembre 2022, n. 187**, recante misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici, convertito con **legge 1° febbraio 2023, n. 10,** si è tornati ad occuparsi del Golden Power prevedendo, all'art. 2, **"Misure economiche connesse all'esercizio del golden power"**, la possibilità, per un'impresa che sia stata destinataria dell'esercizio dei poteri speciali, di presentare istanza al Ministero delle imprese e del made in Italy, al quale è rimessa la relativa valutazione, per l'accesso a misure di sostegno della capitalizzazione dell'impresa.
In un contesto ad elevata complessità in cui la procedura di recepimento della NIS2 è in corso e la disciplina sul perimetro di sicurezza nazionale cibernetica vive le prime stagioni applicative, secondo le notizie apprese e gli annunci pubblicati, il 25 gennaio scorso il Consiglio dei Ministri avrebbe approvato un nuovo disegno di legge sulla cybersicurezza al fine espresso di rafforzare la normativa attuale per riuscire a contrastare l'avanzata offensiva del cybercrimine in Italia. Si tratta di un'iniziativa importante che da un lato inasprisce pene e sanzioni per gli hacker e, dall'altro, allarga il perimetro di soggetti tenuti a dotarsi di sistemi di cybersicurezza includendovi espressamente le regioni e le province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali. Tali soggetti, in particolare, dal punto di vista organizzativo, sarebbero chiamati ad individuare, laddove non presente, un referente per la cybersicurezza, a segnalare senza ritardo ad ACN, e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze ottenute e ad inviare entro settantadue ore a decorrere dal medesimo momento, una notifica completa di tutti gli elementi informativi disponibili, un incidente riconducibile a una delle tipologie individuate. A corredo di tale obbligo, sarebbe previsto, nel caso di reiterata inosservanza dell'obbligo di notifica, una sanzione amministrativa pecuniaria da €25.000 a €125.000.

CAPITOLO 3
Le certificazioni

È ormai opinione diffusa, in particolare nel contesto europeo, che la spinta verso una sempre **maggiore interoperabilità e standardizzazione rappresenti una delle principali chiavi anche per garantire ulteriore affidabilità e sicurezza all'ecosistema digitale e ai prodotti e servizi che in esso vengono forniti**.
La sensibilità su tali argomentazioni a livello internazionale trova la sua origine negli Stati Uniti, con la nascita del *Trusted Computer System Evaluation Criteria* – TCSEC, seguito dall'ITSEC europeo e successivamente dai Common Criteria (CC). A livello tecnico, questi ultimi hanno la funzione di definire dei criteri per rendere misurabili, e quindi comparabili in maniera oggettiva e incondizionata, le proprietà legate alla sicurezza di un prodotto o di un sistema informatico. A tal proposito vengono utilizzati i **principi di imparzialità, ripetibilità, riproducibilità e obiettività**. La documentazione prodotta in ottemperanza di questi criteri evidenzia gli elementi fondamentali dell'oggetto della valutazione, ovvero del *Target of Evaluation* (TOE). Per ottenere la certificazione è necessario identificare gli obiettivi di sicurezza, l'ambiente ed i requisiti funzionali. In numerosi paesi UE **attualmente esistono schemi nazionali con caratteristiche specifiche modellati sulla base della struttura indicata dai *Common Criteria*, così da permettere, sino alla piena operatività dello schema eurounitario EUCC, l'adozione del principio del mutuo riconoscimento**

a livello europeo. Per misurare numericamente il grado di sicurezza del TOE si ricorre agli Evaluation Assurance Level (EAL), 7 livelli di sicurezza, ciascuno dei quali corrisponde ad un pacchetto di sicurezza (SFR) e di garanzia (SAR). L'apprezzamento per i sistemi condivisi di valutazione è cresciuto costantemente negli anni, difatti secondo lo studio Jtsec, **nel 2021 si è raggiunto il valore più alto della storia, rafforzando un trend in forte crescita, particolarmente marcato soprattutto dal 2013**, **anche se va evidenziato che nel 2022 si è registrato un lieve rallentamento in tal senso**, in quanto sono stati certificati 370 prodotti, a fronte dei 399 dell'anno precedente e dei 383 del 2020. L'ottenimento delle certificazioni migliora la competitività sul mercato, può garantire l'accesso a mercati con requisiti minimi e offre ai governi nazionali uno strumento per garantire che i sistemi IT utilizzati nel Paese siano sicuri, consentendo di contrastare rischi sistemici, in attesa di standard comunitari. Allo stesso tempo, è opportuno considerare alcuni importanti fattori: la documentazione richiesta dai sistemi nazionali aumenta considerevolmente i costi della valutazione, oggi a carico del fornitore; il processo richiede l'utilizzo di risorse specializzate; e i tempi di esecuzione sono piuttosto lunghi, in particolare per i livelli dal terzo in poi. Inoltre, **le rigidità alla base dei CC non permettono di mantenere la certificazione per prodotti/sistemi su cui vengono installate nuove patch per aggiornamenti**. In questo contesto, **i dati rilevati da Jtsec indicano per il 2022 l'avvenuta certificazione di 15 prodotti in Italia** (nel 2021 erano stati solo 11). A livello europeo, comprese le esigenze di far combaciare più agilmente la rinnovata e rafforzata attenzione circa i fenomeni di cybersecurity con i ritmi sempre più dinamici e flessibili dei mercati digitali, le istituzioni hanno iniziato a sostenere la creazione di un nuovo sistema di certificazioni di cybersecurity uniforme in tutta l'UE già dal 2019, con la pubblicazione del Cybersecurity Act. Per accompagnare questo percorso, l'ENISA ha istituito un gruppo di lavoro specifico con l'obiettivo di sostenere e promuovere la **stesura di Common Criteria europei, detti EUCC (*Common Criteria based European candidate cybersecurity certification scheme),* sulla base dei *Common Criteria* esistenti**. La versione attualmente disponibile di tali meccanismi di certificazione (Versione 1.1.1) si fonda su un modello ispirato agli schemi ISO/IEC 15408 e ISO/IEC 18045 e ha lo scopo di creare un progetto comunitario volto a sostituire i singoli schemi nazionali, anch'essi basati sui Common Criteria, che operano sotto l'accordo di mutuo riconoscimento SOG-IS MRA. Le novità affrontano direttamente le criticità riscontrate, tra cui tempi e costi, ad esempio favorendo il *Patch Management*, ossia la possibilità di aggiornare, correggere, migliorare un programma, e il "*testing once principle*". **Lo scorso 31 gennaio, la Commissione europea ha adottato l'*Implementing Act*, ossia il regolamento di esecuzione con cui gli EUCC possono finalmente diventare ufficialmente parte della legislazione europea, fissando un periodo di transizione di 12 mesi (che aumentano a 24 se il processo di certificazione prende inizio entro i 12 mesi dall'entrata in vigore del regolamento), al termine del quale le certificazioni nazionali dovrebbero cessare di operare per lasciare spazio agli EUCC**.

CAPITOLO 4
La percezione delle imprese

Al fine di verificare **la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity**, con particolare riferimento al Perimetro di Sicurezza Nazionale Cibernetica (PSNC), **l'Istituto per la Competitività (I-Com) ha condotto un'indagine** (svolta tra agosto e ottobre 2023), avvalendosi anche del sostegno di alcune delle principali associazioni di categoria, che ha coinvolto 145 imprese appartenenti a vari settori.

Innanzitutto, ai soggetti partecipanti è stato chiesto di fornire **una valutazione circa l'impatto degli**

adempimenti prescritti dalle normative in cybersicurezza sulla competitività aziendale. Per le grandi imprese si rilevano maggiormente **gli investimenti tecnico-organizzativi necessari alla compliance** (35 risposte), mentre le aziende di medie dimensioni si concentrano prettamente sulla **numerosità degli oneri burocratici e amministrativi richiesti** (19) e, infine, le piccole imprese si preoccupano prioritariamente **dell'impatto sui rapporti con la supply chain** (6).

Successivamente, è stato chiesto alle imprese intervistate di indicare nello specifico i fattori che rendono più difficoltosa la **compliance rispetto alle norme in materia di cybersecurity** ed è emerso che ciò sarebbe dovuto alla **mancanza di competenze idonee sia internamente, sia sul mercato del lavoro** (60 risposte in totale), seguito dall'incertezza interpretativa della normativa (52 risposte) e alla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (48 risposte).

Considerando l'aggravarsi dello scenario, sia in termini numerici che di impatto, circa le attività malevole a danno delle infrastrutture critiche anche in Italia, nonché dei maggiori adempimenti previsti dalle direttive NIS2 e CER, le quali si applicheranno a partire dal 18 ottobre 2024, è stato chiesto alle aziende partecipanti di fornire indicazioni su un **eventuale incremento delle risorse destinate alla cybersecurity**. Sul punto, si può osservare come **il 51,2% dei rispondenti stia ancora valutando tale eventualità. Diversamente, il 36,1% delle imprese ha già deciso di aumentare gli investimenti in cybersicurezza, mentre il restante 12,6% non stanzierà ulteriori risorse**.

Analizzando le risposte pervenute con riguardo alle **modalità con cui poter migliorare i livelli di sicurezza informatica**, **l'81% delle imprese ritiene che si debba puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze**. Tale opzione è risultata la più selezionata da tutte e tre le classi dimensionali considerate, a conferma del fatto che si tratta di un aspetto particolarmente sentito a livello aziendale. **La seconda scelta (65,5%) è ricaduta sul riservare più aiuti finanziari alle imprese, in quanto ciò è ritenuto necessario per stimolare gli investimenti in cybersecurity, mentre il 43% dei rispondenti sostiene che si debba rafforzare la collaborazione pubblico-privata sin dalle prime fasi del processo normativo.** Quest'ultima opzione non è stata particolarmente selezionata dalle PMI, che piuttosto hanno insistito sullo snellimento degli obblighi imposti dalle normative di cybersicurezza.

In merito all'adozione di una o più **certificazioni volontarie di cybersicurezza**, si può osservare che **la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione**. Tuttavia, **considerando solo le grandi imprese rispondenti, il 36% delle stesse ha già adottato una o più certificazioni di cybersecurity, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno**. Di converso, tra le medie imprese i risultati sono ben diversi, in quanto un mero 11% ha acquisito almeno una certificazione, mentre il 14% intende ottenere la prima certificazione entro un anno. Quanto alle piccole imprese, solo 1 ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno. Tali risultati possono trovare una motivazione negli **ostacoli che sono percepiti dalle imprese con riguardo all'ottenimento di una certificazione volontaria di cybersecurity**. In primo luogo, il principale intralcio (38% dei rispondenti) risiede nei **costi elevati del processo di certificazione**, che **non sono percepiti come proporzionati ai benefici** che ne possono conseguire. In secondo luogo, quasi il 27% sostiene che **i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi**. Il 70% dei rispondenti è parzialmente o totalmente d'accordo in merito al fatto che **standard comunitari** – come gli *European Common Criteria-based cybersecurity certification scheme* (EUCC) **possano incentivare il ricorso a tali strumenti.**

Tra coloro che hanno dichiarato di **aver adottato almeno una certificazione, i principali effetti direttamente riconducibili ad essa sono stati**: un **miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders** (45% dei rispondenti), una **maggiore consapevolezza dei dipendenti e dei collaboratori esterni** (39,7%) e **più possibilità di partecipare a bandi di gara pubblici o** privati (29,5%).

L'ultima sezione dell'indagine riguarda più nello specifico alcuni aspetti connessi al Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e alle attività del Centro di Valutazione e Certificazione Nazionale (CVCN). Più nel dettaglio, la prima domanda chiede alle imprese la loro **percezione rispetto ai test prescritti dal CVCN sui beni, sistemi e servizi Ict** di rispettiva pertinenza ed è emerso che **per il 30% dei rispondenti non si rilevano particolari criticità in tal senso, mentre il 22,7% non ha espresso un'opinione in merito**. La restante quota di feedback pervenuti evidenzia, invece, alcune problematiche: **32 soggetti ritengono che l'esecuzione di frequenti test, che allungano i tempi e incrementano i costi, possa disincentivare l'acquisto di "beni Ict" di ultima generazione; 23 aziende convengono che la necessità di esaminare tali beni Ict nel relativo ambiente operativo determini la ripetizione di test sugli stessi beni; 16 imprese si preoccupano che la parziale incertezza sulle attività di valutazione possa rappresentare un disincentivo dato il rischio reputazionale conseguente a un eventuale ko**.

Relativamente alle diverse posizioni dei rispondenti con riferimento a una **valutazione complessiva della disciplina sul PSNC**, è possibile osservare come **il 20,7%, soprattutto grandi imprese, si ritenga assolutamente soddisfatto dalle regole e dagli adempimenti previsti nell'ambito del Perimetro**. Parallelamente, poco **più del 10% considera tale normativa come eccessivamente gravosa**, recando solo un minimo beneficio per la sicurezza nazionale. Invece, **il restante 68,8% si colloca nel mezzo**. Il maggior numero, 52 imprese, ha una percezione parzialmente positiva, poiché ritiene che gli adempimenti richiesti – seppur meno aderenti alle esigenze aziendali – siano funzionali a garantire la sicurezza nazionale. Di converso, 21 rispondenti hanno denunciato che l'approccio adottato impone adempimenti sproporzionati ai soggetti inclusi nel Perimetro.

L'ultima domanda del questionario richiede agli intervistati di proporre alcuni **aspetti su cui insistere per migliorare l'ecosistema della cibersicurezza in Italia**. Sul punto**, 60 rispondenti ritengono sia opportuno superare la logica del test sul singolo oggetto in favore di una logica di accreditamento dei fornitori affidabili, prevedendo rimedi contrattuali per legge e adeguate forme di responsabilizzazione nei confronti dei fornitori stessi**. Anche la semplificazione dei test obbligatori sui beni ICT, introducendo – ad esempio – un approccio a tempi fissi con tempistiche controllate secondo una valutazione dei rischi basata su criteri standard, ha incontrato un importante consenso tra i rispondenti, precisamente 48, di cui ben 7 piccole imprese.

Con riguardo agli altri approcci proposti dalle imprese intervistate, pare opportuno fare riferimento **all'armonizzazione dei requisiti delle normative in materia di cybersicurezza, a una maggiore considerazione delle certificazioni a norma del Cybersecurity Act per la procedura di valutazione dinanzi al CVCN, oltre che a un effettivo riconoscimento sul mercato del costo necessario per garantire un elevato livello di cibersicurezza dei prodotti e servizi ICT**.

CAPITOLO 5
La cooperazione tra pubblico e privato

Il **Partenariato Pubblico-Privato (PPP)** è inteso dalla Strategia Nazionale di Cybersicurezza 2022-2026 e dal relativo Piano di Implementazione come elemento traversale agli obiettivi di protezione, risposta e sviluppo, nonché ai fattori abilitanti della formazione,

della promozione della cultura della cybersicurezza e della cooperazione. Tale istituto trova una disciplina organica all'interno del **Codice dei Contratti Pubblici**, riformato di recente attraverso il **d. lgs. n. 36/2023**, che era del tutto assente nel d. lgs. n. 163/2006 e meno strutturata nella precedente normativa in materia (d. lgs. n. 50/2016). I-Com ha mappato le principali iniziative nazionali di PPP in cybersecurity avviate negli ultimi anni, tra cui va annoverato il **Polo Strategico Nazionale (PSN)**, ossia l'infrastruttura che ha l'obiettivo di dotare la PA di tecnologie e sistemi cloud che possano beneficiare di elevate garanzie di affidabilità, resilienza e indipendenza. Inoltre, sono stati promossi vari eventi su scala nazionale per rafforzare la consapevolezza e lo scambio di idee, come richiamato dal Piano di Implementazione dell'ACN. Tra questi vi sono "**Itasec**", organizzata dal Cybersecurity National Lab del CINI e "**CyberSec**", evento promosso da Cybersecurity Italia. Il MUR ha selezionato quattordici grandi Partenariati estesi alle università, ai centri di ricerca e alle aziende sul territorio, nell'ambito dei quali è stata avanzata una proposta progettuale dal titolo **"Security and Rights in the CyberSpace" (SERICS)** che definisce un'ampia agenda di ricerca che abbraccia questioni tecniche, legali e sociali relative alla sicurezza e alla privacy. Tra i progetti volti a formare, consapevolizzare e a creare forza lavoro nazionale specializzata in cybersicurezza abbiamo, a titolo di esempio, **"CyberChallenge"**, **"OliCyber"**, **"CyberTrails"**, **"Cyber Harbour"** e il **Primo dottorato nazionale in cybersicurezza** realizzato dalla Scuola IMT Alti Studi di Lucca in collaborazione con il Laboratorio nazionale di Cybersecurity del CINI. Anche gli otto **Competence Center** istituiti dal MISE con funzione di orientamento e formazione alle imprese rientrano tra i partenariati pubbico-privati. Questi presentano focus tematici specifici, tra cui è inclusa la cibersicurezza, offrendo – anche nel caso di centri di competenza con focus differenti – singoli progetti di ricerca e innovazione sul tema.

In tema di collaborazione tra pubblico e privato, vanno considerate anche **le start-up innovative**.

I-Com ha svolto un monitoraggio su quelle che si occupano di cybersicurezza, osservandone **121 sull'intero territorio nazionale**. Per quanto concerne l'anno di costituzione, è possibile **notare un andamento in costante crescita fino al 2019**, a cui è seguito un rallentamento importante nel 2020 – causa pandemia da covid-19 – che è stato successivamente recuperato l'anno seguente, in cui si sono costituite il maggior numero di start-up in cybersicurezza su base annua (35). Tuttavia, **nel 2022 si è assistito a una contrazione significativa, con sole 11 start-up in tale ambito, tendenza calante continuata nel 2023 in cui se ne rilevano appena 4**.

In aggiunta, tra le altre **forme di collaborazione tra pubblico privato sulla cybersecurity** rientrano gli accordi con l'ACN nell'ambito delle proprie funzioni di impulso e, in particolare, le iniziative per il rafforzamento delle sinergie tra l'Agenzia e i **Cluster tecnologici** per agevolare il trasferimento tecnologico verso le PMI.

CAPITOLO 6
Le competenze in cibersicurezza

La formazione degli individui riveste un ruolo fondamentale nell'ambito della cibersicurezza. Nel merito, l'Italia è più indietro rispetto agli altri Paesi europei e presenta una diffusione di competenze digitali altamente variegata a seconda della fascia d'età. Ad esempio, le competenze digitali almeno di base sono diffuse in una quota pari al 45,8% della popolazione. Un dato interessante emerge a proposito della consapevolezza sui pericoli digitali, infatti, **rispetto agli individui che non utilizzano l'Internet of Things per timori legati alla sicurezza, l'Italia presenta quote sensibilmente più basse rispetto alla media UE**. Ciò detto, **nel corso del 2023 si è riscontrato un significativo incremento degli illeciti legati al fenomeno del falso trading online**. Più in generale, l'anno scorso

sono peggiorati numerosi dati emergenti dal report della Polizia Postale: rispetto al 2022 sono maggiori sia i casi trattati che le somme di denaro sottratte. Nell'ambito della formazione ICT delle imprese, il nostro Paese è nuovamente al di sotto della media europea. Addirittura, **la quota di imprese ICT con più di 10 addetti che erogano formazione al proprio personale è diminuita negli ultimi anni**, dal 62,1% del 2019 al 54,7% del 2022. Allo stesso tempo, sempre in Italia, il costo medio delle violazioni di dati è aumentato da 3,6 milioni di dollari nel 2021 a 3,86 nel 2023; nel medesimo periodo lo stesso dato diminuiva sia in Francia che in Germania. Tutti questi elementi segnalano una situazione allarmante per la formazione e consapevolezza dei rischi digitali in Italia, per cui **risulta necessario investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità, indipendentemente dal livello di alfabetizzazione digitale già in loro possesso**. Molte delle iniziative già attive in questo campo nascono e si sviluppano anche grazie al settore privato, spesso in collaborazione e/o col patrocinio di enti pubblici. Appare dunque utile che queste forme di collaborazione pubblico-privato possano essere rafforzate e messe maggiormente a sistema.

Il monitoraggio I-Com delle attività di formazione sulla cibersicurezza in ambito universitario ha evidenziato un interesse decisamente crescente per queste tematiche da parte del mondo accademico, che **a gennaio 2024** presentava **520 tra corsi e insegnamenti relativi alla cibersicurezza rispetto ai 234 individuati a inizio 2023**. Nel dettaglio, l'analisi ha individuato 259 insegnamenti singoli all'interno di corsi di laurea magistrale, 105 insegnamenti singoli in lauree triennali, 44 progetti di ricerca in dottorati, 34 lauree magistrali, a fronte di 22 corsi all'interno di dottorati di ricerca, 26 master, 23 corsi singoli all'interno di master di I e II livello e 7 lauree triennali interamente dedicate alla cybersecurity. Pertanto, il totale delle lauree specifiche (triennali e magistrali) sul tema della cibersicurezza ammonta a 41, ben 15 in più rispetto a quelle rilevate a gennaio 2023. La formazione post-laurea si affianca a quella universitaria con differenze in termini quantitativi piuttosto importanti: tra progetti di ricerca in dottorati e master di primo e secondo livello sono stati conteggiati ben 70 corsi "specializzati". Nel complesso, la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 111 corsi di studio interamente dedicati. Per quanto riguarda la **distribuzione regionale della complessiva offerta formativa**, questa appare piuttosto disomogenea con una forte concentrazione nel Lazio (101 tra corsi e singoli insegnamenti), in Campania (53) e in Lombardia (47). Tuttavia, se si considerano i **dati normalizzati per il numero di Università presenti sul territorio regionale**, la classifica varia mostrando in prima posizione la Liguria con un rapporto 13:1, seguita da Veneto (10,8:1) e Piemonte (9,5:1). A livello regionale, a gennaio 2024 solo Basilicata e Valle d'Aosta risultavano non proporre corsi di questo genere. In relazione alla distribuzione regionale della offerta formativa "specializzata" (lauree triennali, magistrali, master e progetti di ricerca in dottorati), il Lazio si conferma la regione più interessata con 26 percorsi complessivi, catalizzando buona parte dell'offerta sia in termini di lauree dedicate (8 tra magistrali e triennali), sia per quanto concerne la specializzazione post-laurea (10 master e 8 progetti di ricerca in dottorato). **L'elevato numero di master specifici sui temi della cibersicurezza (26) sembra suggerire un'elevata domanda di approfondimento post-laurea su questi temi.** Nell'ambito della formazione superiore, un ruolo di rilievo è rivestito dagli ITS che hanno lo scopo di formare personale tecnico in aree strategiche per lo sviluppo del tessuto economico del Paese. La **Missione 4 del PNRR sottolinea l'importanza della riforma del sistema ITS**, che si è concretizzata attraverso la **l. n. 99 del 15 luglio 2022**, alla quale si sta dando attuazione mediante diversi decreti.

Il rapporto di monitoraggio, pubblicato dall'Istituto Nazionale Documentazione Innovazione Ricerca Educativa (INDIRE), nell'anno 2023 ha registrato sul territorio nazionale ben 142 ITS. **Il 5 ottobre 2022 è stato firmato l'Accordo per la Rete di coordinamento nazionale per lo sviluppo di percorsi formativi specifici in Cybersecurity nell'ambito degli ITS Academy, tra le cui parti rientra l'ACN**. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-Com, **gli ITS che si occupano di cybersicurezza sono il 17,6% rispetto al numero complessivo di quelli attivi**, l'offerta formativa erogata ha visto l'avvio di un numero considerevole di corsi in sicurezza informatica specifici e di singoli insegnamenti sul tema all'interno di corsi attinenti a materie differenti.