2022
RELAZIONE ANNUALE AL PARLAMENTO

2022

RELAZIONE ANNUALE AL PARLAMENTO

sommario

prefazione

La gestione della coda pandemica, la vicinanza del conflitto russo-ucraino, le ricadute che quest'ultimo ha in termini di insicurezza delle rotte energetiche costituiscono talune delle sfide che l'Italia, nel contesto europeo e internazionale, si trova oggi ad affrontare: esse delineano un quadro fragile, al cui interno la tutela degli interessi nazionali è determinata dal concorso di molteplici fattori.

La salvaguardia di tali interessi nello spazio cibernetico – in cui assume un rilievo crescente la richiesta di servizi digitali da parte di cittadini, istituzioni e operatori economici – è accompagnata da un processo di trasformazione digitale, influenzato anche dalla comparsa di nuove tecnologie, tutte bisognose di cautele operative.

Il necessario adeguamento ai continui mutamenti che l'ambiente impone non va disgiunto da un'azione programmatica di lungo termine, che sostenga lo sviluppo di capacità tecnologiche nazionali all'interno di un ecosistema virtuoso, anche ai fini del perseguimento di un'autonomia strategica di settore.

Il mantenimento di elevati livelli di sicurezza e di resilienza cibernetiche contribuisce alla robustezza del sistema produttivo, grazie alla protezione delle infrastrutture critiche, e assicura lo svolgimento di funzioni e servizi essenziali per lo Stato.

L'azione di coordinamento e di regolamentazione condotta dall'Agenzia per la cybersicurezza nazionale, subito dopo l'attivazione delle funzioni a essa attribuite, ha fornito un importante contributo alla complessiva opera di governo e all'impegno politico in tale direzione. Questa relazione ne illustra i termini.

Alfredo Mantovano

introduzione

Nell'anno appena trascorso, caratterizzato dall'accresciuto dinamismo di diverse tipologie di attori e dall'espansione del numero di eventi con impatti sulle infrastrutture digitali nazionali ed europee, il rischio associato alla minaccia di natura cibernetica si è attestato su livelli particolarmente elevati.

Tuttavia, se da una parte è sicuramente cresciuta l'attenzione dell'opinione pubblica verso incidenti e attacchi di varia origine e intensità, dall'altra la piena consapevolezza dei rischi cyber *– specie se comparata al livello di pervasività che le tecnologie dell'informazione hanno raggiunto nella nostra vita quotidiana – è di là da venire.*

L'ACN, in tale contesto, ha operato a tutela degli interessi nazionali nel campo della cybersicurezza, in costante collaborazione con le altre Amministrazioni che compongono l'architettura nazionale, nella ferma convinzione che la sicurezza e la resilienza nello spazio cibernetico si costruisce tramite uno sforzo condiviso e in una logica di sistema.

Nel suo ruolo di Autorità nazionale di cybersicurezza, l'ACN ha condotto una vasta azione di coordinamento, incoraggiando la creazione di una rete di collaborazione e favorendo la concentrazione delle capacità nazionali in materia.

In tale ottica, il confronto supera l'ambito istituzionale e viene anche arricchito da un processo di consultazione continua e bidirezionale con il settore privato e il mondo dell'accademia e della ricerca.
Solo un partenariato efficace con gli operatori strategici può consentire di rafforzare i presidi normativi posti a tutela delle infrastrutture critiche del Paese. Solo un dialogo costruttivo

con le università e le istituzioni scolastiche può favorire lo sviluppo di una workforce *nazionale con competenze specialistiche. Solo il potenziamento della ricerca e il supporto alla nuova imprenditorialità innovativa può garantire l'autonomia tecnologica nel settore della cybersicurezza.*

Lungo una direttrice diversa, l'Agenzia, animata da uguale convinzione, lavora al fianco di omologhe organizzazioni europee, partner *internazionali e Paesi* like-minded*. Attesa l'intrinseca natura internazionale della cybersicurezza, lo scambio informativo e la cooperazione – tanto a livello strategico, quanto in ambito tecnico – diventano strumenti utili a far fronte alla complessità del panorama della minaccia e alla sua sofisticatezza.*

L'evoluzione del contesto geopolitico, in cui l'accesso alle tecnologie – specie quelle emergenti – contribuisce a determinare la gerarchia internazionale, e il ciclico riacutizzarsi di tensioni e conflitti nelle oramai numerose aree di crisi, continueranno a condizionare la sicurezza delle catene di approvvigionamento e influenzare i livelli di rischio cibernetico.
In tale contesto, il mantenimento di uno spazio cibernetico sicuro e resiliente diviene elemento irrinunciabile per la crescita economica, il benessere della popolazione e la tenuta dei valori democratici.

Proprio per questo, l'ACN, conformemente al suo mandato istituzionale, continuerà a operare per garantire la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle Pubbliche Amministrazioni.

Bruno Frattasi

01.

COSTRUZIONE DI UN'AUTORITÀ NAZIONALE COMPETENTE PER LA CYBERSICUREZZA

L'Agenzia per la cybersicurezza nazionale è il fulcro della rete di protezione e sviluppo *cyber* del Paese. Una tappa fondamentale nel percorso di rafforzamento della sicurezza e della resilienza cibernetiche nazionali è rappresentata, quindi, proprio dal processo di costruzione dell'Agenzia, sia dal punto di vista della strutturazione dell'ente, che del suo posizionamento nel panorama istituzionale. L'Agenzia, istituita nella seconda metà del 2021 con l'adozione del decreto-legge 14 giugno 2021, n. 82 – d'ora innanzi decreto-legge – ha iniziato ad esercitare le prime funzioni nel settembre 2021, proseguendo, per gran parte del 2022, nel suo percorso di costruzione e consolidamento, in uno con lo svolgimento, sin da subito, delle competenze prioritarie assegnatele dal decreto-legge. Una parte significativa delle attività che hanno impegnato il 2022 ha, pertanto, riguardato un ampio spettro di attività prodromiche e funzionali, quali l'elaborazione di normativa e procedure interne, l'istituzione degli organi e Comitati previsti dal decreto-legge, il reclutamento del personale necessario all'efficace svolgimento delle funzioni, l'adozione dei bilanci e il posizionamento istituzionale.

Parallelamente al processo di costruzione, l'Agenzia si è subito inserita nel panorama istituzionale quale attore con competenze specialistiche in grado di cooperare attivamente con tutte le altre Amministrazioni interessate dai temi della cybersicurezza. In questo ambito, hanno rivestito un ruolo fondamentale le sedi di raccordo interistituzionale quali, a livello politico, il Comitato interministeriale per la cybersicurezza (CIC), a livello tecnico-operativo, il Nucleo per la cybersicurezza (NCS).

Il CIC[1] svolge rilevanti funzioni d'indirizzo, consulenza e vigilanza, a livello politico, nella materia della cybersicurezza. In particolare, oltre ad esercitare l'alta sorveglianza sull'attuazione della Strategia, è chiamato ad esprimere pareri su atti necessari al funzionamento dell'Agenzia, tra cui i DPCM attuativi del D.L. n. 82/2021 e i bilanci preventivo e consuntivo. Nel corso del 2022 l'Agenzia ha supportato il funzionamento dell'alto consesso – per il quale il Direttore generale dell'Agenzia svolge funzioni di segreteria – predisponendo il materiale prodromico alle riunioni, quello istruttorio e di resoconto finale, a supporto del Presidente del Consiglio, dell'Autorità delegata e dei Ministri.

Nel 2022 si sono svolte 4 riunioni del CIC, nel corso delle quali sono stati sottoposti all'attenzione dei Ministri componenti, in particolare: la Strategia nazionale di cybersicurezza 2022-2026 e il relativo Piano di implementazione, entrambi predisposti dall'Agenzia con il contributo delle altre Amministrazioni NCS, come si avrà modo di illustrare in seguito; i bilanci dell'Agenzia, preventivo 2022 e 2023, e consuntivo 2021; lo schema di DPCM 18 maggio 2022, n. 92, concernente le procedure di accreditamento da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) dei laboratori di prova, nonché i raccordi tra lo stesso CVCN, i Laboratori Accreditati di Prova (LAP) e i Centri di Valutazione (CV) del Ministero dell'interno e del Ministero della difesa; lo schema di DPCM

[1] Istituito dall'art. 4 del D.L. n. 82/2021.

1° settembre 2022, n. 166, recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico (Regolamento c.d. "appalti in deroga").

Particolare rilevanza rivestono questi ultimi due provvedimenti: il primo, inserito nel contesto del passaggio di funzioni tra l'allora Ministero dello sviluppo economico (Ministero delle imprese e del *made in Italy*) e l'ACN – formalmente compiuto con successivo provvedimento – in quanto ha costituito l'ultimo dei provvedimenti di attuazione previsti dal decreto-legge n. 105 del 2019 (c.d. "decreto Perimetro"), essenziale ai fini dell'avvio del CVCN entro il termine, previsto dalla legge; il secondo, in quanto completa il percorso di adozione delle disposizioni regolamentari previste dal D.L. n. 82/2021 per la piena operatività dell'ACN, affiancandosi ai tre provvedimenti già adottati nel 2021 (Regolamento di contabilità, Regolamento di organizzazione e funzionamento e Regolamento del personale) e contribuendo all'attuazione di una specifica *milestone* del PNRR, la cui scadenza era prevista per il mese di dicembre 2022. In particolare, esso disciplina le modalità di svolgimento dell'attività negoziale dell'Agenzia finalizzata alla tutela, nello spazio cibernetico, della sicurezza nazionale. L'Agenzia, pur in coerenza con i principi di economicità, efficacia, tempestività, proporzionalità, correttezza e non discriminazione, potrà operare, laddove ricorrano i presupposti, con procedure più snelle e tempestive, in deroga alle norme in materia di contratti pubblici. Ciò, peraltro, anche al fine di consentire, nell'eventualità, un immediato approvvigionamento di beni e servizi necessari ad affrontare situazioni di crisi nello spazio cibernetico. In ragione dello specifico ambito di attività (la tutela della sicurezza nazionale nello spazio cibernetico) e dell'esercizio delle deroghe sopra richiamate, sono previsti specifici obblighi informativi nei confronti del Comitato parlamentare per la sicurezza della Repubblica (COPASIR).

Il Nucleo per la cybersicurezza, costituito presso l'ACN e presieduto dal suo Direttore generale, è – come detto – la sede di coordinamento interministeriale a livello tecnico-operativo, che opera a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione e alla preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Molteplici sono state le tematiche affrontate nel corso del 2022 in seno al Nucleo – anche alla luce dell'intensificarsi del conflitto russo-ucraino – tra cui la diversificazione tecnologica, la Strategia nazionale di cybersicurezza, le recenti normative in materia *cyber* approvate a livello europeo. In linea generale, tutti gli adempimenti connessi allo svolgimento del Nucleo hanno certamente rappresentato un filone di attività significativo del 2022, di cui si darà atto più dettagliatamente nel prosieguo.

L'Agenzia siede, inoltre, nel Nucleo interministeriale situazione e pianificazione (NISP) in virtù del DPCM 24 febbraio 2022 che, nel modificare il DCPM 5 maggio 2010, ne aumenta il numero dei componenti. Tale ampliamento trova fondamento nella crescente complessità degli scenari sottesi alle attività del NISP, che richiedono l'espressione di competenze diversificate, tra le quali proprio quelle in materia di cybersicurezza. L'Agenzia, a partire dai primi mesi del 2022, ha pertanto potuto offrire il proprio contributo per i profili inerenti alla cybersicurezza e alle crisi di cybersicurezza.

L'architettura istituzionale delineata dal D.L. n. 82/2021 prevede, inoltre, che l'Agenzia sia sottoposta al controllo del Comitato parlamentare per la sicurezza della Repubblica. In tal senso, nel corso del 2022 il Direttore generale è stato udito tre volte dal COPASIR. Inoltre, in attuazione di quanto previsto dall'art. 14 del richiamato decreto-legge, il 30 giugno 2022 è stata presentata la prima relazione sulle attività svolte nel 2021 dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico.

1.1 La strutturazione dell'ACN

Parte essenziale della strutturazione dell'Agenzia è stata l'attività di produzione della normativa interna, volta a consentire la realizzazione della struttura dell'ACN, così come definita con il Regolamento di organizzazione e funzionamento (DPCM n. 223/2021), nonché la concreta attuazione degli istituti e delle procedure previsti dagli altri DPCM di attuazione del D.L. n. 82/2021: il Regolamento di contabilità; il Regolamento del personale; il Regolamento c.d. "appalti in deroga".

L'attività di produzione della normativa interna è risultata nell'adozione di circa 40 provvedimenti attuativi del Direttore generale dell'ACN disciplinanti l'organizzazione e le attività dell'Agenzia[2].

In sede di prima operatività, in considerazione delle risorse umane disponibili, si è provveduto ad attivare progressivamente Servizi, Divisioni e le altre articolazioni necessarie per l'efficace svolgimento delle attività prioritarie, dovendosi affidare provvisoriamente alcune funzioni proprie di Servizi non ancora istituiti, a quelli esistenti, in deroga a quanto previsto dal Regolamento di organizzazione dell'Agenzia.

Il continuo processo di assunzione di nuove risorse umane, portato avanti nel corso dell'anno dall'Agenzia, ha consentito però di modificare progressivamente, con successivi provvedimenti

[2] L'articolo 6 del decreto-legge, nel rimandare ad apposito Regolamento la disciplina di dettaglio, ha previsto la possibilità di istituire fino ad un massimo di otto articolazioni di livello dirigenziale generale, nonché fino ad un massimo di trenta articolazioni di livello dirigenziale non generale. Il decreto del Presidente del Consiglio dei ministri recante il Regolamento di organizzazione ha, quindi, previsto l'articolazione dell'Agenzia in sette uffici di livello dirigenziale generale, denominati Servizi, posti alle dipendenze del Direttore generale dell'Agenzia, confermando il numero massimo di trenta articolazioni di livello dirigenziale non generale. I Servizi previsti dall'articolo 12 del DPCM n. 223/2021 sono: Gabinetto; Autorità e sanzioni; Certificazione e vigilanza; Operazioni; Programmi industriali, tecnologici, di ricerca e formazione; Risorse umane e strumentali; Strategie e cooperazione.

del Direttore generale, la ripartizione delle competenze prevista con il primo provvedimento organizzativo, redistribuendo le attività in funzione del graduale ampliamento sia delle articolazioni, sia dell'organico dell'Agenzia.
Pertanto, alla fine del 2022, la strutturazione interna dell'Agenzia era così articolata:

- 5 Servizi;
- 16 Divisioni, di cui 9 di maggiore complessità, quali articolazioni di livello dirigenziale non generale, in relazione alla particolare delicatezza e rilevanza delle funzioni, che comportano notevoli responsabilità;
- 2 Strutture di missione;
- 1 Unità a supporto del Vice Direttore generale;
- 1 Nucleo di progetto.

In particolare, sono stati attivati i seguenti 5 dei 7 Servizi previsti dal Regolamento di organizzazione e funzionamento:

- Gabinetto;
- Certificazione e vigilanza;
- Operazioni;
- Programmi industriali, tecnologici, di ricerca e formazione;
- Risorse umane e strumentali.

Nel mese di gennaio 2023 è stato attivato anche il Servizio Autorità e sanzioni.
Quanto alle strutture di progetto o missione – la cui costituzione è prevista dal Regolamento di organizzazione e funzionamento per l'attuazione di progetti di durata definita – sono state istituite la Struttura di missione per le relazioni internazionali di carattere strategico, con il fine di consentire l'avvio e l'espansione delle competenze dell'Agenzia in materia di cooperazione internazionale, e la Struttura di missione per lo sviluppo di capacità e competenze, allo scopo di sviluppare le competenze in ambito *cyber.* Queste ultime costituiscono, insieme alla cooperazione, i fattori abilitanti della Strategia nazionale di cybersicurezza.

Sempre con riferimento alla struttura interna dell'Agenzia, con provvedimento del Direttore generale dell'Agenzia del 14 giugno 2022, su deliberazione del Comitato di Vertice, sotto la presidenza dell'Autorità delegata, è stato nominato il Collegio dei revisori dei conti, organo di controllo dell'ACN, composto da un magistrato della Corte dei conti, che lo presiede, da un magistrato del Consiglio di Stato e da un dirigente del Ministero dell'economia e delle finanze. Il Collegio dei revisori dei conti ha sin da subito avviato le attività volte ad effettuare, tra l'altro, il riscontro agli atti della gestione finanziaria, a svolgere verifiche di cassa e di bilancio e ad esprimere i pareri sul progetto di bilancio

preventivo e sul rendiconto annuale.
Il decreto-legge prevede, inoltre, la costituzione di un Comitato tecnico-scientifico "*con funzioni di consulenza e proposta, volto a promuovere la collaborazione con il sistema dell'università e della ricerca e con il sistema produttivo nazionale, nonché a supportare le iniziative pubblico-private in materia di cybersicurezza*", con la cui istituzione è stato posto un altro tassello funzionale alla strutturazione dell'Agenzia. I suoi componenti, scelti nell'ambito dell'Agenzia, nonché tra rappresentanti dell'industria, dell'accademia e dell'associazionismo di settore, sono stati designati con DPCM del 15 giugno 2022, sentito il Comitato di Vertice dell'Agenzia, su proposta del Direttore generale. Essi resteranno in carica per due anni, con possibilità di rinnovo per un ulteriore anno.

Tra le attività svolte nel 2022, rientra anche la progettazione, la gestione e l'implementazione dei sistemi informativi volti ad assicurare, in prima istanza, l'ingegnerizzazione delle procedure necessarie alla fase di strutturazione interna e *startup* delle attività dell'Agenzia, nonché della migrazione dei sistemi a supporto delle funzioni trasferite dalla Presidenza del Consiglio dei ministri, dall'Agenzia per l'Italia Digitale (AgID) e dall'allora MiSE, in materia di cybersicurezza.

Per quanto attiene ai sistemi informativi trasferiti da AgID e MiSE, l'attività si è concentrata sulla definizione e attuazione del progetto di migrazione, individuando la migliore soluzione tecnologica, volta a garantire l'assenza di disservizio nel processo di migrazione dei dati e delle utenze di circa 4.000 utenti dei servizi digitali esposti sul *web* (Sistema di interazione del CVCN www.cvcn.gov.it, Organismo di Certificazione della Sicurezza Informatica www.ocsi.gov.it, *Cloud Marketplace* catalogocloud.acn.gov.it) e dei servizi digitali attualmente in corso di pubblicazione su *web* (sistema di Gestione rischio *cyber*).

Si è, inoltre, proceduto alla migrazione dei sistemi a supporto delle funzioni del CSIRT Italia e del Perimetro di sicurezza nazionale cibernetica (PSNC). Un impegno considerevole è stato anche posto nell'evoluzione di numerosi nuovi servizi, verso la *constituency* afferente alla Pubblica Amministrazione, al settore privato, ai partner UE ed extra UE.

In riferimento ai sistemi interni dell'Agenzia si è proceduto alla realizzazione della piattaforma per l'ottimizzazione dei processi di gestione e di comunicazione ai dipendenti, per l'efficientamento delle attività di gestione del personale[3], per il sistema di contabilità e bilancio e per la gestione dei flussi documentali e dei sistemi di conservazione.

Si è proceduto, infine, alla realizzazione di un apposito modello, messo a disposizione sulla piattaforma PAdigitale2026 del Dipartimento per la trasformazione digitale della Presidenza del

[3] Compresi gli strumenti necessari per la gestione delle presenze, dei *workflow* autorizzativi e per l'elaborazione delle buste paga.

Consiglio dei ministri, a supporto delle Pubbliche Amministrazioni per la classificazione dei propri dati e servizi, che rappresenta un passaggio fondamentale per attuare il processo di migrazione verso il *cloud*, previsto dalla Strategia *Cloud* Italia (vds. Cap. 6.1).

Per la realizzazione degli obiettivi sopra descritti è stata stipulata, una convenzione con SOGEI per il supporto di servizi e infrastrutture IT, ivi incluse le componenti di sicurezza e i servizi di monitoraggio. Molte di queste attività sono state svolte anche nell'ambito dell'Investimento 1.5 *Cybersecurity* del Piano Nazionale di Ripresa e Resilienza (PNRR) sotto la guida progettuale del personale interno all'Agenzia.

1.2 Reclutamento dell'eccellenza e sviluppo del capitale umano

Elemento essenziale della costruzione di un'autorità nazionale in grado di garantire la cybersicurezza del Paese è avere una compagine capace di affrontare le sfide che pone l'era digitale. Ciò richiede un processo di reclutamento di personale che sia non solo competente e qualificato, ma anche in un numero adeguato, tale da poter permettere all'Agenzia di svolgere le sue funzioni in modo efficiente.

Tale processo è stato avviato sin dall'inizio dell'attività dell'Agenzia, si è realizzato attraverso tre diverse modalità di reclutamento e si è dipanato su altrettante principali linee direttrici: 1) reinquadramenti tramite le speciali procedure previste dall'articolo 17, commi 8 e 9, del D.L. n. 82/2021; 2) concorsi pubblici; 3) *vacancy* con l'assunzione tramite contratti di diritto privato a tempo determinato.

In relazione alla prima modalità di reclutamento, il 30 giugno 2022 è stato completato l'inquadramento delle 90 unità messe a disposizione da altre Amministrazioni **al fine di assicurare la prima operatività dell'Agenzia**.

Nel frattempo, a partire da **febbraio 2022**, ha preso avvio un articolato **Piano di reclutamento** per sostenere il percorso di crescita dell'Agenzia e consentirle di raggiungere, in sede di prima applicazione, le 300 unità di dotazione organica iniziale previste dal D.L. n. 82/2021. L'obiettivo è quello di far diventare l'ACN un **polo di eccellenza nazionale** nel campo della cybersicurezza al servizio del Paese, per attrarre i **migliori talenti** presenti sul mercato che, grazie al loro bagaglio di competenze e capacità e al loro spirito di servizio, rappresentano il patrimonio più prezioso di cui dispone un'istituzione pubblica come l'Agenzia.

Oltre ai reinquadramenti previsti dal decreto-legge, che hanno consentito all'Agenzia di poter

avviare le proprie attività sin dal primo giorno, l'alimentazione della compagine dell'Agenzia – che al 31 dicembre 2022 è composta da **165 persone** – è stata perseguita, sia con le assunzioni ordinarie a tempo indeterminato, tramite **concorso pubblico**, sia attraverso i canali di reclutamento, a tempo determinato, previsti dagli articoli 91 e 93 del Regolamento del personale.

In particolare, il 22 febbraio 2022 l'Agenzia ha pubblicato il **primo bando per l'assunzione a tempo indeterminato di 50 laureati da inquadrare nel segmento professionale di Esperto**, articolato in 6 distinti concorsi, ciascuno dei quali destinato ad alimentare specifiche funzioni dell'ACN, per laureati nelle discipline IT con almeno 2 anni di esperienza nello specifico settore oggetto del concorso. Le prove scritte e orali si sono concluse nel mese di **luglio** e i primi ingressi di personale si sono realizzati a partire dal mese di **agosto**. Al 31 dicembre 2022 sono state assunte **48 persone**, in gran parte destinate all'attivazione del CVCN.

Il 28 ottobre 2022 è stato pubblicato un ulteriore bando di **concorso pubblico, articolato in 7 distinti concorsi, per l'assunzione di 60 diplomati** con profilo tecnico *cyber*, necessari per assicurare l'operatività di strutture quali il CSIRT Italia e i laboratori di scrutinio tecnologico, indispensabili per la corretta attuazione della normativa in materia di *Golden Power* e di Perimetro di sicurezza nazionale cibernetica. Hanno presentato domanda di partecipazione complessivamente **860 candidati** che, entro il primo semestre del 2023, saranno chiamati a sostenere due **prove scritte** e, qualora conseguano la votazione minima prevista dal bando di concorso, anche una prova orale.

In seguito alle procedure selettive (***vacancy***) per l'assunzione a tempo determinato con contratto di diritto privato di soggetti in possesso di alta e particolare specializzazione per lo svolgimento di **attività assolutamente necessarie all'operatività dell'Agenzia**, ovvero per la realizzazione di **specifiche progettualità**, hanno preso servizio **9 unità** provenienti da settori professionali variegati, sia per natura, sia per esperienza. In particolare, sono stati assunti: 3 professionisti – che rientravano da un periodo lavorativo svolto all'estero – 2 per lo sviluppo dei Programmi di investimento e dei Programmi industriali, nonché uno per ricoprire il ruolo di *Data Protection Officer*; 1 unità proveniente da una società di consulenza, per le attività correlate al *Cyber risk management*; 4 liberi professionisti per le attività di comunicazione istituzionale e per ricoprire il ruolo di "Responsabile per la transizione digitale"; 1 unità proveniente dal mondo accademico (*Legal advisor*) per l'attuazione di programmi europei e attività di sviluppo tecnologico.

In particolare, dei **57** neoassunti a seguito di concorso pubblico (**48**) e di *vacancy* (**9**), per la quasi totalità in possesso di competenze tecniche *cyber*, il **92%** proviene dall'ambito privato e della ricerca

e un significativo **11%** rientra da posizioni lavorative all'estero. Quest'ultimo dato va correlato alla percentuale di domande effettuate per i concorsi e le *vacancy* da parte di appartenenti alla PA, che risulta essere di **poco inferiore al 30%.**

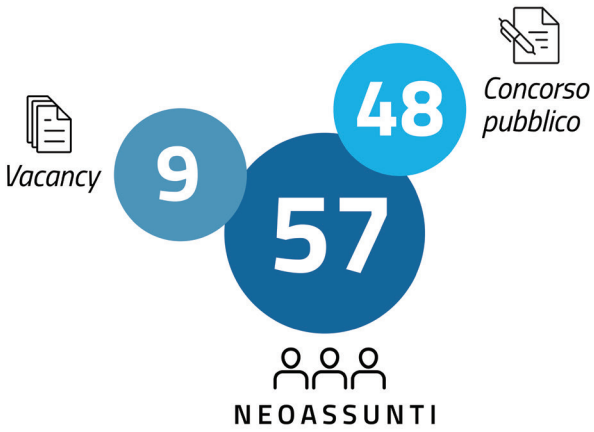


FIGURA 1 – PROVENIENZA DEL PERSONALE ASSUNTO AL 31 DICEMBRE 2022

Inoltre, grazie a specifiche intese con altri Enti e Istituzioni pubbliche, sono stati disposti **distacchi, comandi, fuori ruolo o altre analoghe posizioni**, per **18 unità**.
La distribuzione per titoli di studio del personale assunto mostra una netta prevalenza di persone in possesso di laurea specialistica.

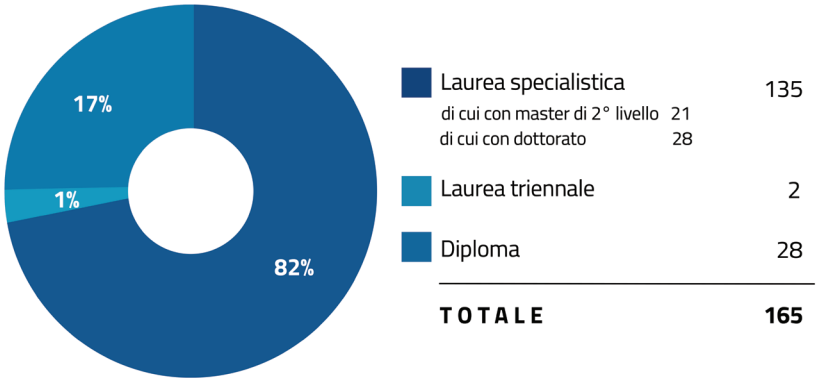


FIGURA 2 – TITOLI DI STUDIO DEL PERSONALE ASSUNTO AL 31 DICEMBRE 2022

A inizio dicembre sono state pubblicate due ulteriori *vacancy*, una per ricoprire il posto di *Project manager* per l'attuazione di programmi industriali e attività di sviluppo tecnologico e l'altra per due *Advisor* per le attività di coordinamento interistituzionale con altri organi dello Stato e/o altre amministrazioni e di sviluppo delle relazioni internazionali.

Non sono stati ancora attivati gli ulteriori due canali di reclutamento previsti, ovvero la possibilità di utilizzare personale proveniente dal Ministero della difesa (da realizzarsi mediante apposito decreto del Presidente del Consiglio dei ministri, come specificamente previsto dal D.L. n. 82/2021), nonché di avvalersi di 50 esperti in possesso di specifica ed elevata competenza nel campo dell'IT.

L'Agenzia è quindi nel pieno del processo di reclutamento di nuovo personale, essenziale per poter garantire l'espletamento delle funzioni istituzionali nel campo della sicurezza e della resilienza cibernetiche. Difatti, sebbene l'Agenzia abbia quasi triplicato, nel corso del 2022, il personale a propria disposizione, è necessario accrescere ulteriormente le risorse umane per garantire la sostenibilità e l'efficacia dei processi lavorativi.

Parimenti, poiché lo sviluppo del capitale umano è un ulteriore fattore determinante per garantire l'assolvimento della *mission* istituzionale dell'Agenzia, valorizzando **l'Accordo del 4 marzo 2022 tra l'ACN e la Banca d'Italia**, entrambe le Istituzioni hanno attivato sinergie per permettere alle rispettive compagini di personale la partecipazione a diverse iniziative formative, consentendo l'avvio di un percorso virtuoso di scambio di esperienze professionali.

In particolare, 12 dipendenti della Banca d'Italia hanno partecipato a seminari dell'ACN e 110 dipendenti dell'Agenzia hanno partecipato ad iniziative e corsi di Banca d'Italia. Con riferimento a questi ultimi, 28 dipendenti con posizioni organizzative sono stati inseriti nel percorso formativo sulla *leadership* personale, presso la Scuola di formazione per dirigenti della Banca d'Italia, con sede a Perugia.

Inoltre, sono state avviate le attività per implementare un articolato **Piano di formazione** volto a mantenere un elevato e aggiornato livello di professionalità e qualificazione del personale, nonché a valorizzare e potenziare le competenze (saperi e capacità) necessarie per far fronte ai fabbisogni di professionalità, attuali e prospettici, dell'Agenzia.

In particolare, l'Agenzia ha lavorato alla pianificazione di percorsi di formazione ed esperienze professionali a beneficio del personale, per lo sviluppo di competenze specialistiche, organizzative e manageriali, che incentivino comportamenti orientati alla collaborazione, alla cultura dell'apprendimento continuo e all'innovazione. In una logica di costante condivisione degli obiettivi strategici dell'Agenzia, il citato Piano di formazione permetterà di armonizzare aspirazioni individuali e obiettivi generali e fidelizzare il personale, con conseguente limitazione del *turnover*.

Principali tappe raggiunte dall'ACN 2022

26 GENNAIO
Avvio collaborazione con il Garante *privacy*

Inizio fase di primo reclutamento
22 FEBBRAIO/1 MARZO

Strategia Nazionale Cybersicurezza 2022-2026
17 MAGGIO

18 MAGGIO
DPCM accreditamento Laboratori di Prova e raccordi tra CVCN, LAP e CV Interno e Difesa

Nomina del Collegio dei revisori dei conti
14 GIUGNO

15 GIUGNO
Nomina del Comitato Tecnico-Scientifico dell'Agenzia

15 GIUGNO
DPCM per il trasferimento di funzioni in materia di cybersicurezza di MiSE

30 GIUGNO
Operatività del CVCN

Determinazioni tecniche in materia di accreditamento dei Laboratori di Prova
11 AGOSTO

1 SETTEMBRE
DPCM Regolamento cd. appalti in deroga

1 SETTEMBRE
DPCM per il trasferimento di funzioni in materia di cybersicurezza di AgID e DTD

14 OTTOBRE
Istituzione Organo ispettivo e di vigilanza

31 OTTOBRE
Relazione al Parlamento sullo stato di attuazione del D.L. n. 82/2021

Relazione annuale al Parlamento sulle attività svolte dall'ACN 2021
30 NOVEMBRE

1.3 Pianificazione strategica e programmazione operativa

Per rispondere in modo efficace, tempestivo e credibile alle sfide connesse al processo di trasformazione digitale che sta interessando anche il nostro Paese, il legislatore ha riconosciuto all'Agenzia una peculiare collocazione istituzionale e un marcato livello di autonomia. Ciò permette all'Agenzia di adottare speciali paradigmi strategici, organizzativi e di gestione del personale che le consentono di fronteggiare le sollecitazioni esterne adattando rapidamente la ***vision* strategica**, le **strutture** e le **professionalità**, attraverso un confronto continuo tra il mutevole contesto di riferimento, le aspettative del Paese e dei diversi *stakeholders*.

In quest'ottica, **Strategia, Persone** e **Organizzazione** sono elementi imprescindibili per il perseguimento della *mission* istituzionale. Conseguentemente, il "**Piano strategico ACN**" intende sintetizzare le sfide più rilevanti verso le quali si indirizzano le risorse dell'Agenzia per anticipare i cambiamenti, ipotizzando i possibili scenari evolutivi.
Esso rappresenta un **documento unico** di programmazione (anche operativa), *governance* e coordinamento, nel quale assumono rilievo trasversale gli **obiettivi strategici**, le esigenze di reclutamento, formazione e sviluppo delle **persone**, in una logica di **continuo miglioramento organizzativo** che esalta **valori e identità dell'ACN**.

Il Piano è al contempo uno strumento di **trasparenza** sugli indirizzi dell'azione e sulle priorità strategiche dell'Agenzia verso cui allocare le risorse, nonché sui miglioramenti organizzativi e gestionali da perseguire per una maggiore efficienza e *performance*, anche attraverso un costante monitoraggio delle misure programmate.

In particolare, il sistema di pianificazione, basato su un'approfondita analisi degli scenari sottesi alle attività svolte, prevede: la definizione della ***vision***, degli **obiettivi strategici** e delle direttrici di sviluppo sulle macro-tematiche; l'identificazione di mirate **linee di azione** in cui si articolano gli obiettivi e le relative **Strutture responsabili**; i *deliverable* e le *milestone*; i tempi e le risorse; i criteri per la **valutazione periodica** dei risultati raggiunti, delle risorse impiegate, dei progressi compiuti.

Ne discende una stretta connessione tra pianificazione strategica, strutture organizzative e sviluppo delle risorse umane in termini di professionalità, tanto che l'assegnazione della responsabilità in ordine al raggiungimento dei risultati strategici previsti nel documento di pianificazione, rappresenta il parametro sul quale misurare il livello di conseguimento degli obiettivi assegnati ai Responsabili delle articolazioni, nonché lo strumento per realizzare il pieno allineamento tra gli obiettivi dell'Istituzione e i comportamenti individuali delle persone che vi lavorano.

Durante il primo semestre del 2022, questo processo è stato sostanzialmente connesso all'attivazione delle funzioni prioritarie e alla progressiva strutturazione, in termini di pianta organica, dei Servizi e delle articolazioni dell'Agenzia, secondo un criterio di sostenibilità e gradualità, in coerenza con il numero e le diverse professionalità presenti.

Nel secondo semestre è stato avviato il vero e proprio processo di pianificazione strategica per il **triennio 2023-2025**. In particolare, le linee strategiche dell'azione dell'ACN prevedono di **creare valore pubblico** accompagnando il processo di ammodernamento delle infrastrutture, potenziando la resilienza cibernetica del Paese, riducendone il grado di vulnerabilità e, al contempo, incrementandone l'autonomia e l'indipendenza tecnologica.

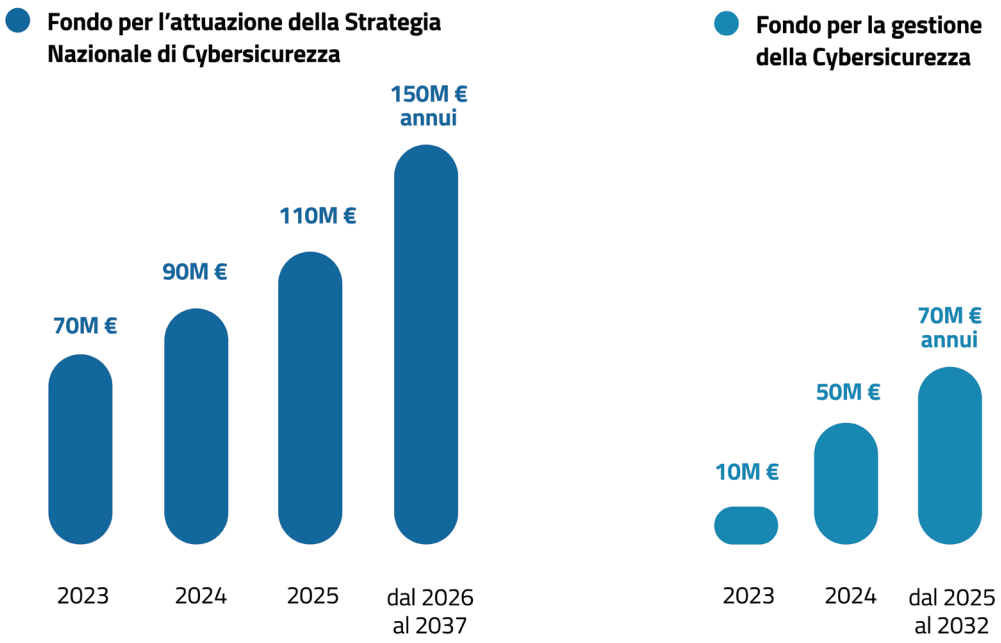
A tal fine, in linea anche con **la Strategia nazionale di cybersicurezza 2022-2026** (vds. Cap. 2) e il relativo **Piano di implementazione**, nel corso del 2023 si concluderà la fase di definizione degli **obiettivi strategici** e delle relative **linee d'azione**, che riguardano i diversi ambiti di intervento dell'Agenzia.

In particolare, con la **programmazione operativa delle attività** è stata predisposta, a livello amministrativo ed economico-finanziario, una scomposizione degli obiettivi di medio-lungo periodo in obiettivi riferiti ad intervalli temporali di minore estensione. Per garantire un maggior raccordo tra la dimensione strategica e quella operativa sono stati analizzati i fabbisogni e le possibili fonti di copertura, i mezzi disponibili e l'eventuale reperibilità di risorse aggiuntive.

A tal fine, nel bilancio sono stati identificati i principali obiettivi strategici, dimensionandoli con la spesa ad essi collegata. La **programmazione annuale e pluriennale delle risorse finanziarie** è stata, pertanto, finalizzata all'efficace ed efficiente raggiungimento degli obiettivi strategici, in coerenza con le maggiori competenze affidate all'Agenzia. In quest'ottica, è stato altresì essenziale il potenziamento dell'attività programmatoria delle acquisizioni di beni e servizi, in linea con la crescita dell'Agenzia e con il PNRR.

Al riguardo, si segnala l'impulso volto all'istituzione – avvenuta ai sensi dell'articolo 1, comma 899, della Legge n. 197/2022 "*Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025*" – del **Fondo per l'attuazione della Strategia nazionale di cybersicurezza**, provvisto di una dotazione complessiva di oltre 2 miliardi di euro, per gli anni dal 2023 al 2037, destinato a finanziare gli investimenti per il conseguimento dell'autonomia tecnologica in ambito digitale e all'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali, nonché all'istituzione del **Fondo per la gestione della cybersicurezza**, destinato a finanziare le correlate attività di gestione operativa degli investimenti di cui sopra, con una dotazione prevista in 10 milioni di euro per l'anno 2023, 50 milioni di euro per l'anno 2024 e di 70 milioni di euro annui a decorrere dal 2025.

All'Agenzia è affidato il compito di coordinare e monitorare l'attuazione degli interventi che saranno realizzati con tali fondi, la cui assegnazione alle Amministrazioni individuate come attori responsabili nell'ambito del predetto piano avverrà con decreti del Presidente del Consiglio dei ministri adottati su proposta dell'ACN, d'intesa con il Ministero dell'economia e delle finanze.



Coordina e monitora l'attuazione degli interventi

Fondi assegnati alle Amministrazioni con DPCM, adottati su proposta dell'ACN, d'intesa con il MEF

FIGURA 3 – FONDI ISTITUITI CON LEGGE DI BILANCIO 2023

1.4 Politiche di bilancio e di approvvigionamento

Il D.L. n. 82/2021 attribuisce all'Agenzia autonomia contabile e finanziaria, oltre ad un sistema contabile ispirato a principi civilistici e improntato al principio di competenza economica. Tale assetto è finalizzato a favorire l'efficace ed efficiente raggiungimento degli obiettivi strategici, in coerenza con le competenze affidate dal legislatore all'Agenzia.

Nel corso dell'anno 2022, in parallelo con la progressiva strutturazione organizzativa dell'Agenzia, è stato predisposto il primo **bilancio preventivo** (*budget* economico 2022), adottato il 24 giugno 2022 con delibera del Direttore generale e approvato dal Presidente del Consiglio con DPCM del 28 luglio 2022.

Successivamente, il 9 settembre 2022, è stato adottato il **bilancio consuntivo** per l'anno 2021, approvato dal Presidente del Consiglio dei ministri con DPCM del 19 dicembre 2022. Il bilancio di esercizio al 31 dicembre 2021 ha registrato un avanzo di 1.768.035 di euro, destinato ad una riserva di patrimonio netto per la copertura delle eventuali spese derivanti dal subentro dell'Agenzia in rapporti giuridici preesistenti.

Il 30 ottobre 2022, infine, è stato adottato, nei termini previsti dal Regolamento di contabilità dell'Agenzia, il **bilancio preventivo** per l'anno 2023, approvato dal Presidente del Consiglio dei ministri con DPCM del 19 dicembre 2022.

Entrambi i documenti di bilancio hanno acquisito il parere positivo del Collegio dei revisori dei conti e del Ministero dell'economia e delle finanze.

Dal punto di vista finanziario, al termine del 2022 sono stati registrati introiti per complessivi 104.048.942 di euro (Figura 4).

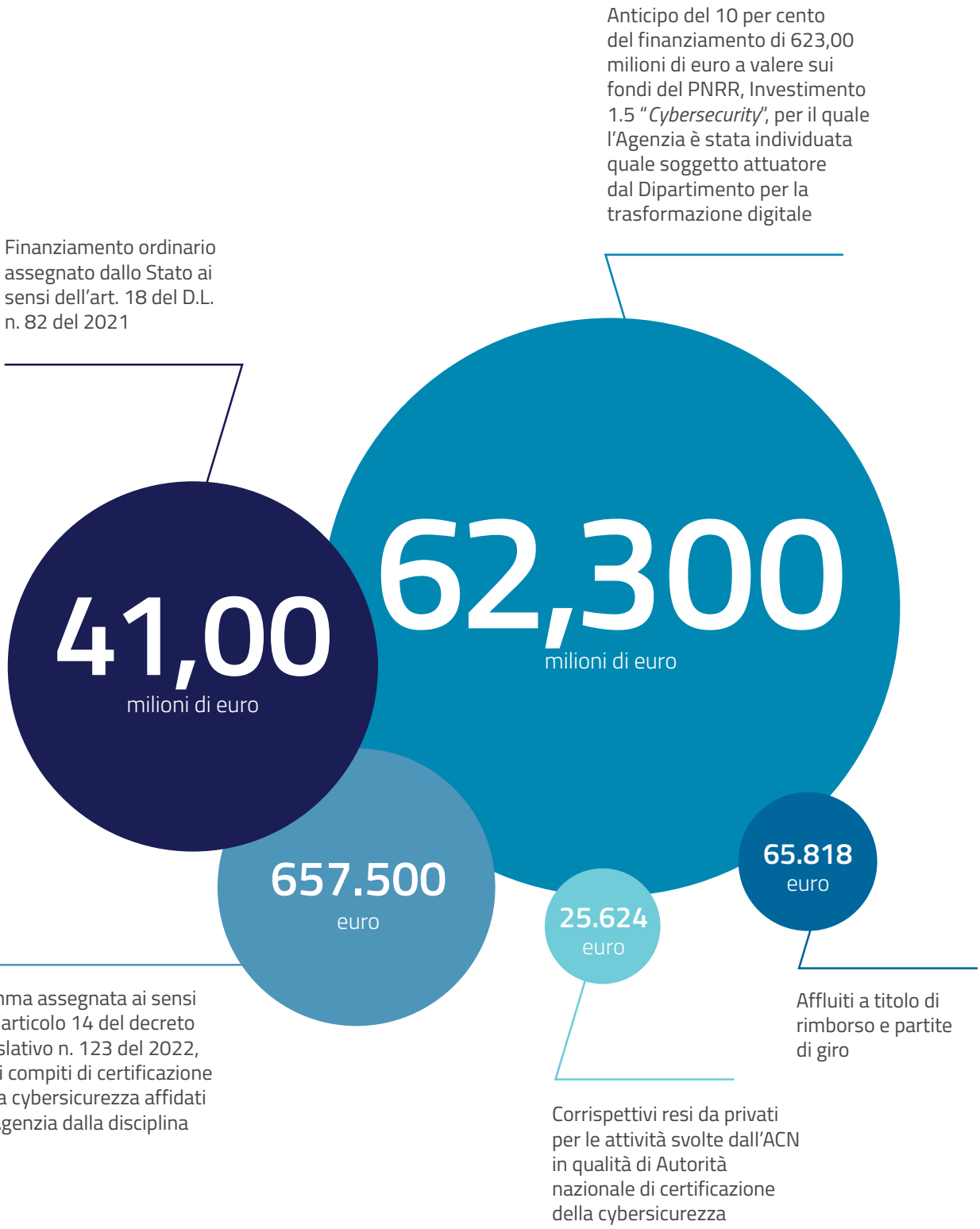


FIGURA 4 – GLI INTROITI DELL'AGENZIA

Tali risorse sono destinate a sostenere la spesa corrente dell'Agenzia, nonché a finanziare gli investimenti, in particolare i progetti del PNRR direttamente realizzati dall'Agenzia (c.d. interventi a titolarità) ovvero affidati ad altre Pubbliche Amministrazioni, cui sono trasferiti i fondi (c.d. interventi a regia)[4].

Infine, nell'anno 2022, per assicurare la prima operatività dell'Agenzia, sono stati altresì impiegati i fondi previsti dall'articolo 17, comma 7, del D.L. n. 82/2021, pari a complessivi 2,1 milioni di euro, per l'acquisto di beni e servizi per l'avvio delle attività istituzionali, nonché per le spese logistiche della sede.

Nei primi mesi dell'anno, al fine di consentire il tempestivo avvio dell'operatività dell'Agenzia, l'attività di ***procurement*** è stata improntata all'approvvigionamento di beni e servizi, ricorrendo prevalentemente a procedure di affidamento diretto nonché alle Convenzioni e agli Accordi Quadro Consip. Inoltre, nell'ottica di garantire l'efficienza e la tracciabilità dei flussi informativi, è stata adottata una disciplina delle procedure di spesa per l'acquisizione di beni e servizi che stabilisce un quadro di regole comuni da applicare a tutti i processi, compresi quelli relativi ai progetti finanziati per il raggiungimento dei *milestone* e dei *target* richiesti dal PNRR (linea di investimento 1.5) dei quali l'Agenzia è Soggetto Attuatore.

1.5 Proiezione esterna: accordi di collaborazione e attività di promozione dell'Agenzia

L'efficacia dell'azione istituzionale dell'Agenzia e l'innalzamento dei livelli di resilienza cibernetica del Paese passano inevitabilmente dalla costruzione di una rete di collaborazione che operi tanto sul versante pubblico quanto su quello privato, a beneficio dei vari *stakeholders* e a tutela degli *asset* ICT strategici.

In tale ottica, il coinvolgimento di amministrazioni pubbliche, università, istituzioni scolastiche, enti di ricerca e operatori privati (incluse piccole imprese e *startup*) va sostenuto tramite specifiche intese e iniziative di collaborazione mirate.

Per tale motivo, conformemente alle funzioni attribuite dalla legge e in linea con le misure previste dal Piano di implementazione della Strategia nazionale di cybersicurezza, l'Agenzia ha riservato particolare attenzione alla sottoscrizione di accordi, intese e convenzioni volte all'avvio di cooperazioni strategiche e di partenariati sul territorio nazionale con soggetti pubblici e privati.

[4] Vds. Cap. 4.

Sul fronte degli accordi con le Pubbliche Amministrazioni e le Autorità amministrative indipendenti, sono state privilegiate iniziative legate alla tutela dei dati e dei servizi pubblici, comprensive delle attività di supporto per la prevenzione, il monitoraggio del rischio cibernetico e il trattamento degli attacchi informatici. Allo stesso tempo, gli accordi prevedono iniziative di formazione e consapevolezza *cyber* destinate ad aumentare le competenze dei dipendenti.

Con riferimento agli accordi stipulati con il mondo privato, la prospettiva ha riguardato azioni comuni tese a prevenire attacchi informatici, a supporto della resilienza cibernetica e della sicurezza digitale del Paese, attraverso lo scambio informativo in tema di *cyber threat intelligence* e la formazione specialistica per varie categorie professionali.

Nel periodo di riferimento l'ACN ha sottoscritto **47** tra **accordi bilaterali**, **protocolli d'intesa** e **convenzioni**, di cui **28** connessi ai progetti PNRR.

FIGURA 5 – ACCORDI BILATERALI, PROTOCOLLI D'INTESA E CONVENZIONI

In particolare, nell'ambito delle attività svolte dall'ACN in qualità di Soggetto attuatore dell'Investimento 1.5 "*Cybersecurity*" della Missione 1 Componente 1 del PNRR, l'Agenzia ha sottoscritto 28 tra accordi di esecuzione e atti d'obbligo, rientranti nella documentazione tecnica necessaria alla partecipazione/implementazione delle progettualità ammesse a godere dei fondi PNRR. In tale ambito, l'Agenzia ha promosso le iniziative legate al PNRR, in stretto raccordo con il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri. Le attività di divulgazione delle opportunità fornite dall'Investimento 1.5 per innalzare il potenziamento *cyber* delle amministrazioni e delle imprese sono consistite in campagne di comunicazione dedicate a interlocutori istituzionali e destinatari degli interventi, anche organizzate unitamente al Dipartimento e ad altre organizzazioni.

Sul fronte della divulgazione delle iniziative strategiche, l'Agenzia ha riservato ampio spazio alla presentazione della Strategia Nazionale di Cybersicurezza 2022-2026, con l'organizzazione dapprima di una conferenza stampa, per poi proseguire il dialogo con gli organi di informazione. In questo percorso divulgativo sono state tratteggiate le linee programmatiche, oltre che gli strumenti relativi alla sua concreta implementazione, sottolineando come la stessa coniughi sicurezza e sviluppo nella tutela e nell'interesse del Paese.

Pur innestandosi nella fase di avvio dell'operatività dell'Agenzia, l'azione di comunicazione istituzionale ha svolto un ruolo fondamentale nel fornire un'informazione chiara e accurata sulle attività e le competenze dell'Agenzia.

Se da un lato l'attività si è concentrata sulla creazione dei canali di comunicazione istituzionali, quali la versione *beta* del sito internet e la pagina LinkedIn, dall'altra lo stretto contatto con i media nazionali e internazionali ha privilegiato una narrativa volta a promuovere la conoscenza del ruolo e delle competenze dell'Agenzia, assicurando un'ampia e corretta informazione verso gli interlocutori istituzionali e le aziende private, principali destinatari delle attività dell'Agenzia.

La comunicazione digitale dell'Agenzia si è focalizzata sulla produzione di contenuti multimediali, circa 250 tra notizie, comunicati stampa, interviste e oltre 90 *post social* sulla pagina istituzionale LinkedIn, perseguendo il duplice fine di promuovere le attività dell'Agenzia e mettere in campo una corposa campagna di *employer branding*. La forte spinta divulgativa che ha interessato il percorso di reclutamento previsto dal D.L. 14 giugno 2021, n. 82, ha visto l'Agenzia raggiungere risultati importanti in termini di visibilità all'interno delle comunità professionali di interesse.

La comunicazione sui *social* ha generato, nel primo anno di presenza *online*, 2 milioni di visualizzazioni dei *post*, 110 mila visualizzazioni della pagina istituzionale e il raggiungimento della quota di 30.500 *follower*.

FIGURA 6 – I NUMERI DELL'ATTIVITÀ DI PROMOZIONE DELL'AGENZIA

02.

LA STRATEGIA NAZIONALE DI CYBERSICUREZZA

L'adozione di una nuova Strategia nazionale di cybersicurezza rappresentava, da tempo, un obiettivo strategico per l'intero Paese al fine di identificare i giusti traguardi da raggiungere per far fronte alle più evolute sfide del mondo digitale, oltre ad essere parte integrante dell'attuazione della nuova architettura di cybersicurezza. Pertanto, un importante filone di attività è stato incentrato sulla predisposizione di questo fondamentale documento, compito che il D.L. n. 82/2021 attribuisce espressamente all'Agenzia, ai fini della sua adozione da parte del Presidente del Consiglio dei ministri, sentito il CIC.

La predisposizione della Strategia ha richiesto non solo un lavoro di elaborazione interna all'Agenzia, ma anche un coordinamento con le altre Amministrazioni, in particolare quelle facenti parte del Nucleo per la cybersicurezza, che, ciascuna per le parti di rispettiva competenza, hanno contribuito a definire gli obiettivi strategici al cui raggiungimento dovranno concorrere.

La Strategia nazionale di cybersicurezza 2022-2026 e l'annesso Piano di implementazione sono stati adottati dal Presidente del Consiglio il 17 maggio 2022, **a soli 8 mesi dall'avvio della prima operatività dell'Agenzia**. Essi mirano ad affrontare una pluralità di sfide che vanno dal rafforzamento della resilienza nella transizione digitale del sistema Paese, al conseguimento dell'autonomia strategica nella dimensione cibernetica, dall'anticipazione dell'evoluzione della minaccia *cyber*, alla gestione di crisi cibernetiche e al contrasto della disinformazione *online*.

Per fronteggiare al meglio le citate sfide per il sistema-Paese, sono stati individuati tre obiettivi fondamentali, **protezione, risposta** e **sviluppo**, e le relative misure funzionali ad assicurare la concreta attuazione della Strategia dal punto di vista organizzativo, di *policy* e prettamente operativo.

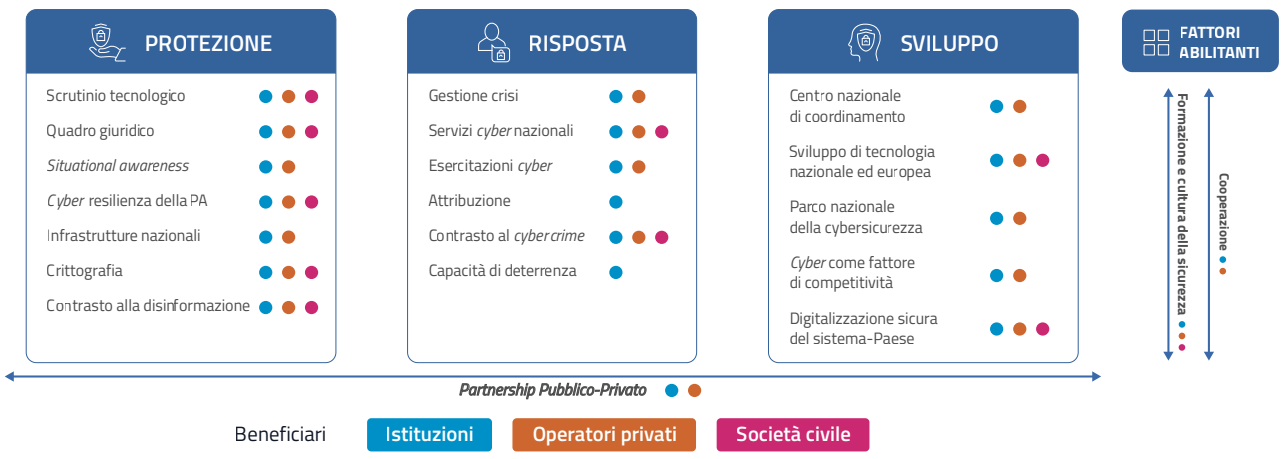


FIGURA 7 – OBIETTIVI DELLA STRATEGIA NAZIONALE DI CYBERSICUREZZA

Nell'impostazione della Strategia, la protezione degli *asset* strategici nazionali viene perseguita 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.

Sotto tale aspetto, 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, oltre alla promozione della crittografia commerciale lungo l'intero ciclo di vita dei sistemi e servizi ICT.

Per quel che concerne la risposta alle minacce, agli incidenti e alle crisi *cyber* nazionali, la Strategia prevede lo sviluppo di elevate capacità nazionali di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale. Ciò richiede azioni mirate riguardo alla gestione delle crisi cibernetiche, alle esercitazioni di sicurezza cibernetica e resilienza, al contrasto al *cybercrime*, alla definizione del posizionamento e della procedura nazionale in materia di attribuzione di attività cibernetiche ostili, nonché al rafforzamento delle capacità di deterrenza in ambito cibernetico e all'integrazione degli attuali servizi *cyber* nazionali. A quest'ultimo riguardo, rientrano gli interventi finanziati con i fondi del Piano Nazionale di Ripresa e Resilienza (PNRR).

Quanto, infine, all'adozione consapevole e sicura delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato, 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 essi 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, sono previsti interventi volti a sviluppare il ruolo del Centro di Coordinamento Nazionale svolto dall'ACN – quale punto di contatto per il Centro Europeo di Competenza sulla Cybersicurezza (ECCC) – nonché 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, supporti lo sviluppo di competenze e il trasferimento tecnologico. Ciò nell'ottica di potenziare la ricerca scientifica nello specifico settore e sviluppare tecnologia nazionale ed europea, così da ridurre la dipendenza da tecnologie extra-UE, specie con riguardo a prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore.

Centro europeo di competenza in *cybersecurity* - ECCC e rete dei Centri nazionali di coordinamento - NCC

- Regolamento (UE) 2021/887 -

Principali strumenti dell'UE per concentrare gli investimenti di sviluppo industriale, tecnologico e ricerca in *cybersecurity* e attuare progetti e iniziative in tale ambito. Ai sensi del D.L. n. 82/2021, l'ACN è designata quale NCC nazionale e attua le funzioni a questo assegnate dal Regolamento (UE) 2021/887.

Per poter realizzare fattivamente gli obiettivi descritti, la Strategia attribuisce grande rilevanza ai seguenti fattori abilitanti: **formazione, promozione della cultura della sicurezza cibernetica** e **cooperazione**.

Le iniziative di **formazione** mirano a stimolare la creazione di una solida forza lavoro nazionale, 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. Ciò può avvenire con varie modalità, ad esempio, il mese di luglio 2022 l'Agenzia, insieme alla Scuola Nazionale dell'Amministrazione e al Dipartimento per la Funzione Pubblica della Presidenza del Consiglio dei ministri, ha organizzato la *Summer School in Cybersicurezza* rivolta a figure apicali nelle Amministrazioni centrali dello Stato (vds. Cap. 6.5).

Altro fattore abilitante, che si muove in parallelo con le esigenze di formazione, è la **promozione della cultura della cybersicurezza**, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce *cyber*. Tale obiettivo viene conseguito anche attraverso la promozione della gestione consapevole del cd. rischio residuo, mediante strumenti di autovalutazione basati su specifici *cyber index*, che consentono alle organizzazioni una gestione autonoma del livello di esposizione. A tal fine, un apposito Protocollo d'intesa è stato sottoscritto, nel settembre 2022, tra l'ACN, Confindustria e la società Generali Italia S.p.A.

Da ultimo, vi è il rafforzamento della **cooperazione**, sia sul fronte nazionale, a livello governativo, nel rapporto pubblico-privato, pubblico-pubblico, e con accademia e ricerca – con l'obiettivo di creare maggiori sinergie tra le Pubbliche Amministrazioni e l'industria – sia in ambito internazionale, partecipando in modo proattivo alle iniziative europee e internazionali, nonché promuovendo collaborazioni bilaterali.

La Strategia è corredata del Piano di implementazione, che contiene 82 misure che specificano le puntuali aree di intervento attraverso cui raggiungere i 3 obiettivi di protezione, risposta e sviluppo. Buona parte delle 82 misure sono caratterizzate da un approccio *whole-of-society* che, attraverso lo strumento del partenariato, vede agire in maniera sinergica il settore pubblico con quello privato, con la società civile, 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.

In seguito all'adozione della Strategia nazionale di cybersicurezza e dell'annesso Piano di implementazione, si è provveduto a dare in primo luogo attuazione alla misura n. 82, concernente la definizione di metriche e di *Key Performance Indicator* (KPI), ovvero degli indicatori chiave atti a misurare il conseguimento degli obiettivi.

In tale ambito, per calcolare i citati KPI, sono stati definiti un modello e un piano di lavoro per l'elaborazione degli indicatori di misurazione. A tal fine, nel mese di luglio 2022 si è svolto un *kick-off meeting* che ha visto il coinvolgimento di circa 50 referenti in rappresentanza delle 17 Amministrazioni individuate come attori responsabili per l'attuazione della Strategia[5]. A questo primo incontro, tra settembre e ottobre ne sono seguiti altri, sempre con le stesse Amministrazioni, ma suddivise in gruppi sulla base di *cluster* omogenei in termini di titolarità e *focus* tematici. Tali riunioni hanno avuto l'obiettivo di:

- definire le metriche e gli indicatori di misurazione proposti dall'ACN e finalizzati a misurare l'effettivo grado di implementazione della Strategia;
- identificare le misure di prioritaria attuazione, individuando l'anno di prevalente implementazione, tenendo in considerazione le tempistiche imposte da adempimenti normativi (con riguardo, tra gli altri, alla trasposizione della nuova Direttiva UE sulla sicurezza delle reti e dei sistemi informativi, cd. "NIS 2", nell'ordinamento nazionale) e il piano di lavoro del PNRR, nonché della propedeuticità tra le stesse.

In esito ai citati incontri con le Amministrazioni responsabili, è stato finalizzato il **Manuale operativo** – validato anche dal Comitato tecnico-scientifico dell'ACN – che declina, per ogni misura, le metriche e gli indicatori di misurazione individuati e l'anno di prevalente implementazione. In totale, per le 82 misure sono stati identificati ben **261 indicatori**.

[5] Oltre a quelle che compongono il CIC, la Presidenza del Consiglio dei ministri (Dipartimento Affari Giuridici e Legislativi, Dipartimento per l'Informazione e l'Editoria, Dipartimento delle Informazioni per la Sicurezza, Dipartimento per la Trasformazione Digitale e Dipartimento della Protezione Civile), l'Ufficio del Consigliere Militare del Presidente del Consiglio, il Ministero dell'Istruzione, il Consorzio Interuniversitario Nazionale per l'Informatica e Atenei.

L'impianto degli indicatori, unitamente ai *target* specifici definiti per ciascuno di essi, espressi in termini numerici, consentirà di elaborare, a partire dal secondo anno di implementazione (2023), dei *KPI* che permetteranno di registrare i progressi effettivi rispetto agli obiettivi della Strategia e di identificare i *trend* delle prestazioni. Il Manuale intende costituire un documento soggetto a periodici aggiornamenti e revisioni, nel quale riportare anche le linee guida elaborate per la concreta implementazione delle singole misure, che saranno progressivamente arricchite di maggiori dettagli in relazione ai livelli di attuazione, anche attraverso la realizzazione di un circuito virtuoso fondato su analisi dei risultati e lezioni apprese.

Finalità misure	N. Misure	N. Indicatori
Protezione	24	68
Risposta	21	46
Sviluppo	13	42
Fattori Abilitanti	24	105
TOTALE	**82**	**261**

FIGURA 8 – PROSPETTO DELLE MISURE PREVISTE DAL PIANO DI IMPLEMENTAZIONE

Con riguardo ai fondi istituiti con la Legge di bilancio per l'anno 2023, di cui si è già fatto cenno, l'Agenzia – che indirizza, coordina e monitora l'attuazione del Piano di implementazione della Strategia nazionale di cybersicurezza – ha sviluppato un modello di *governance* che, in stretta sinergia con le Amministrazioni responsabili, le consente di rilevarne i fabbisogni finanziari, così da poter ripartire i citati fondi tra le stesse, sulla base delle rispettive progettualità. Tali fondi serviranno a finanziare tutte quelle iniziative per le quali non ne siano già stati allocati altri promananti dal bilancio ordinario dell'Amministrazione, dal PNRR o da eventuali bandi dell'UE nell'ambito dei programmi *Horizon Europe*-HEU e *Digital Europe*-DEP.

03.

PREVENZIONE E GESTIONE DI INCIDENTI E ATTACCHI CIBERNETICI

Nel corso del 2022, è stato osservato, a livello globale, un deciso aumento di attività malevole ai danni di settori governativi e infrastrutture critiche.

Tale fenomeno, acuito dai riflessi della crisi in atto in Ucraina (rispetto al quale l'Agenzia ha svolto sin da subito attività finalizzata ad elevare il livello di allerta degli operatori pubblici e privati), si è registrato anche in Italia che, allo stato, risulta tra i Paesi maggiormente interessati dalla diffusione generalizzata di *malware* e da attacchi cibernetici mirati, specie in danno del comparto sanitario e di quello energetico.

In tale contesto l'Agenzia, attraverso la componente operativa del CSIRT Italia, ha adottato strumenti e procedure – sempre in costante sviluppo e aggiornamento – per svolgere le funzioni sia nell'ambito del monitoraggio preventivo, sia per la risposta in caso di incidenti.

A ciò si affianca l'azione svolta dal già citato Nucleo per la cybersicurezza (NCS), sede privilegiata di scambio informativo e coordinamento interministeriale in materia *cyber*, nel cui ambito – in ragione delle rafforzate prerogative assegnate al consesso – sono stati, tra l'altro, promossi interventi legislativi volti al rafforzamento della sicurezza e della resilienza cibernetiche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Tra questi, l'adozione della circolare in materia di diversificazione tecnologica per le Pubbliche Amministrazioni di cui si dirà più avanti.

3.1 Principali eventi cibernetici nel periodo di riferimento

Nell'ambito delle funzioni istituzionali attribuite dalla legge – che includono sia attività di natura proattiva, finalizzate al monitoraggio e all'identificazione precoce della minaccia cibernetica, sia di natura reattiva, volte alla mitigazione dei rischi e al contenimento degli impatti sulle infrastrutture digitali nazionali derivanti dagli incidenti cibernetici – le articolazioni tecnico-operative dell'ACN, *in primis* il CSIRT Italia, hanno adottato processi tecnici e analitici per la raccolta e la valorizzazione, in chiave di protezione, delle informazioni relative ad eventi malevoli o potenziali tali.

BOX 1

DEFINIZIONI E METODOLOGIA

È utile definire i concetti utilizzati e fornire una breve descrizione della metodologia che è alla base del lavoro operativo svolto dall'Agenzia, con particolare riferimento alla modalità di rilevazione di eventi e incidenti cibernetici e alla loro successiva trattazione.

DEFINIZIONI

Segnalazione
le comunicazioni previste per legge per i soggetti appartenenti al Perimetro di sicurezza nazionale cibernetica, per gli Operatori di Servizi Essenziali e Fornitori di Servizi Digitali (Direttiva NIS), e per gli operatori di comunicazione (D.M. Telco).
Le Segnalazioni vengono trattate direttamente come **eventi *cyber***

Comunicazione ricevuta
e-mail ricevute dal CSIRT Italia relative ad informazioni contenenti profili di natura *cyber* anche generiche, sottoposte a valutazione preliminare per determinare l'apertura di *case* o meno

***Asset* potenzialmente compromessi**
sistemi o servizi esposti su Internet da soggetti italiani, rilevati dalle attività di monitoraggio proattivo e per i quali vengono inviate specifiche comunicazioni

Triage
la fase in cui gli operatori analizzano le segnalazioni, le comunicazioni ricevute e ogni possibile evento *cyber* di cui il CSIRT Italia viene a conoscenza, anche a seguito di attività di monitoraggio proattivo, al fine di identificare i potenziali impatti e classificare quindi l'informazione come evento *cyber* e proseguire o meno con le ulteriori fasi di trattazione

Case
un avvenimento d'interesse per il CSIRT Italia, opportunamente approfondito al fine di identificare il possibile impatto e valutare la necessità di azioni di resilienza. I *case* possono diventare **eventi *cyber***

Evento *cyber*
un *case* con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, CSIRT Italia dirama *alert* e/o supporta, eventualmente anche in loco, i soggetti colpiti. Qualora fosse confermato l'impatto dalla vittima, l'evento *cyber* viene considerato **incidente**

Richieste di informazioni
richieste effettuate dal CSIRT Italia al soggetto potenzialmente impattato da un evento *cyber* per acquisire ulteriori elementi, come ad esempio la conferma di una possibile compromissione (e la conseguente classificazione dell'evento *cyber* quale incidente)

Comunicazione inviata
alert, anche massivi, inviati a Pubbliche Amministrazioni e soggetti privati potenzialmente interessati da **eventi *cyber***

Constituency
l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici

Portale di *collaboration*
il portale di *collaboration* è riservato ai membri della *constituency* del CSIRT Italia e costituisce lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati

Portale pubblico
è il sito web del CSIRT Italia accessibile all'intera comunità

METODOLOGIA

CSIRT Italia, articolazione tecnico-operativa dell'Agenzia, è *hub* nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (Perimetro di sicurezza nazionale cibernetica, Direttiva NIS, D.M. Telco). Collaziona, altresì, informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali e internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni costituiscono un ampio **cono di visibilità** di cui l'Agenzia dispone sullo stato della minaccia *cyber* a danno del sistema Paese e forniscono all'Agenzia, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Dal punto di vista quantitativo, al fine di intercettare quei fenomeni che non emergono a seguito di obblighi di legge o nell'ambito più ampio delle attività tecniche svolte, l'Agenzia sta ampliando il citato cono di visibilità attraverso l'attuazione di un programma teso a formalizzare la collaborazione con soggetti pubblici e privati, per rafforzare lo scambio di informazioni e realizzare sinergie per la protezione dalla minaccia *cyber* (vds. Cap. 3.5) nonché attraverso la progettazione ed implementazione dei servizi *cyber* nazionali (HyperSOC, ISAC, Rete CERT, vds. Cap. 3.6).
Tutte le informazioni collazionate vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di *triage* le analizzano e classificano come eventi *cyber*; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento. In particolare, il CSIRT Italia:

- approfondisce le informazioni a disposizione, analizzando i contenuti anche dal punto vista strettamente tecnico quale lo studio dei *malware*, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti;
- se necessario invia **richieste di informazioni** ai soggetti;
- fornisce supporto da remoto o *in loco* ai soggetti impattati;
- invia comunicazioni ai soggetti impattati oppure a tutti i soggetti potenzialmente impattati dall'evento *cyber*;
- pubblica *alert* o bollettini.

Si noti che un evento *cyber* viene considerato **incidente** solo qualora l'impatto fosse confermato dalla vittima a seguito del supporto diretto ovvero in risposta a una richiesta di informazioni da parte del CSIRT Italia.

La raccolta delle informazioni di interesse è avvenuta utilizzando, oltre alle segnalazioni indirizzate al CSIRT Italia dalla *constituency* di riferimento, fonti pubblicamente disponibili e fonti non pubbliche, ma reperibili nell'ambito di attività di cooperazione con articolazioni tecniche di altre Amministrazioni ed enti nazionali, omologhe Agenzie estere e internazionali, nonché *provider* di sicurezza.

Su tali basi, l'ACN ha dato origine ad un'intensa attività di *alerting* e divulgazione sui principali rischi, sia in chiave pubblica, sia tramite comunicazioni puntuali ai soggetti direttamente esposti alle minacce (vds. BOX 2).

BOX 2

I numeri dello CSIRT Italia

portali, comunicazioni e attività reattive

PORTALE PUBBLICO

Alert	Bollettini
379	31

PORTALE *COLLABORATION*

Alert	Bollettini
30	8

COMUNICAZIONI

Inviate	Ricevute	Richieste Info
38.745	5.974	185

ATTIVITÀ REATTIVE

Case	Eventi *cyber*	Incidenti
2.643	1.094	126

Sul fronte delle comunicazioni ricevute dal CSIRT Italia, sono state registrate **81 segnalazioni derivanti da obblighi di legge**, quali la normativa sul Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), dalla normativa di attuazione della c.d. Direttiva NIS (D. Lgs. n. 65/2018) e dal cd. Decreto Telco (Decreto del Ministro dello Sviluppo Economico 12 ottobre 2018).

Nel periodo di riferimento, il CSIRT Italia ha trattato **1.094 eventi *cyber***, per una media di circa **90 eventi al mese**, con un picco di **118** a febbraio 2022 (vds. figura 9). Di questi, **126** hanno avuto un impatto confermato dalla vittima, per una media di **10,5 incidenti al mese** (vds. figura 10).

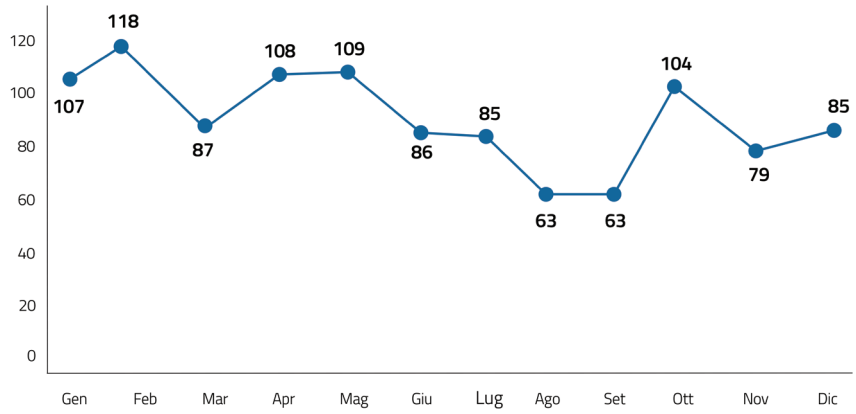


FIGURA 9 – DISTRIBUZIONE TEMPORALE DI EVENTI CYBER
CON IMPATTO SUL TERRITORIO NAZIONALE NEL 2022

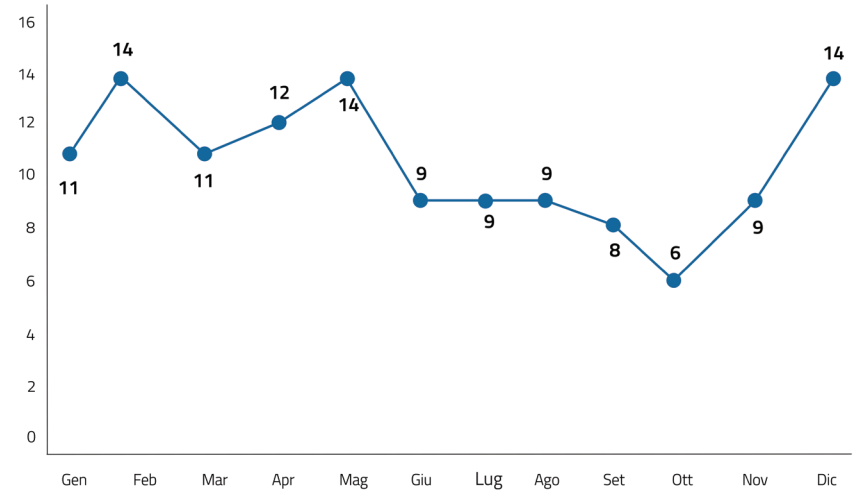


FIGURA 10 – DISTRIBUZIONE TEMPORALE DEGLI INCIDENTI CON IMPATTO CONFERMATO DALLA VITTIMA

I NUMERI DELLE ATTIVITÀ OPERATIVE DELL'ACN NEL 2022

Dall'analisi e dalla successiva classificazione dei 1.094 eventi *cyber* è stato possibile individuare le **tipologie** riportate in Figura 11. Si noti che ognuno dei citati eventi può essere stato associato ad una o più tipologie[6] :

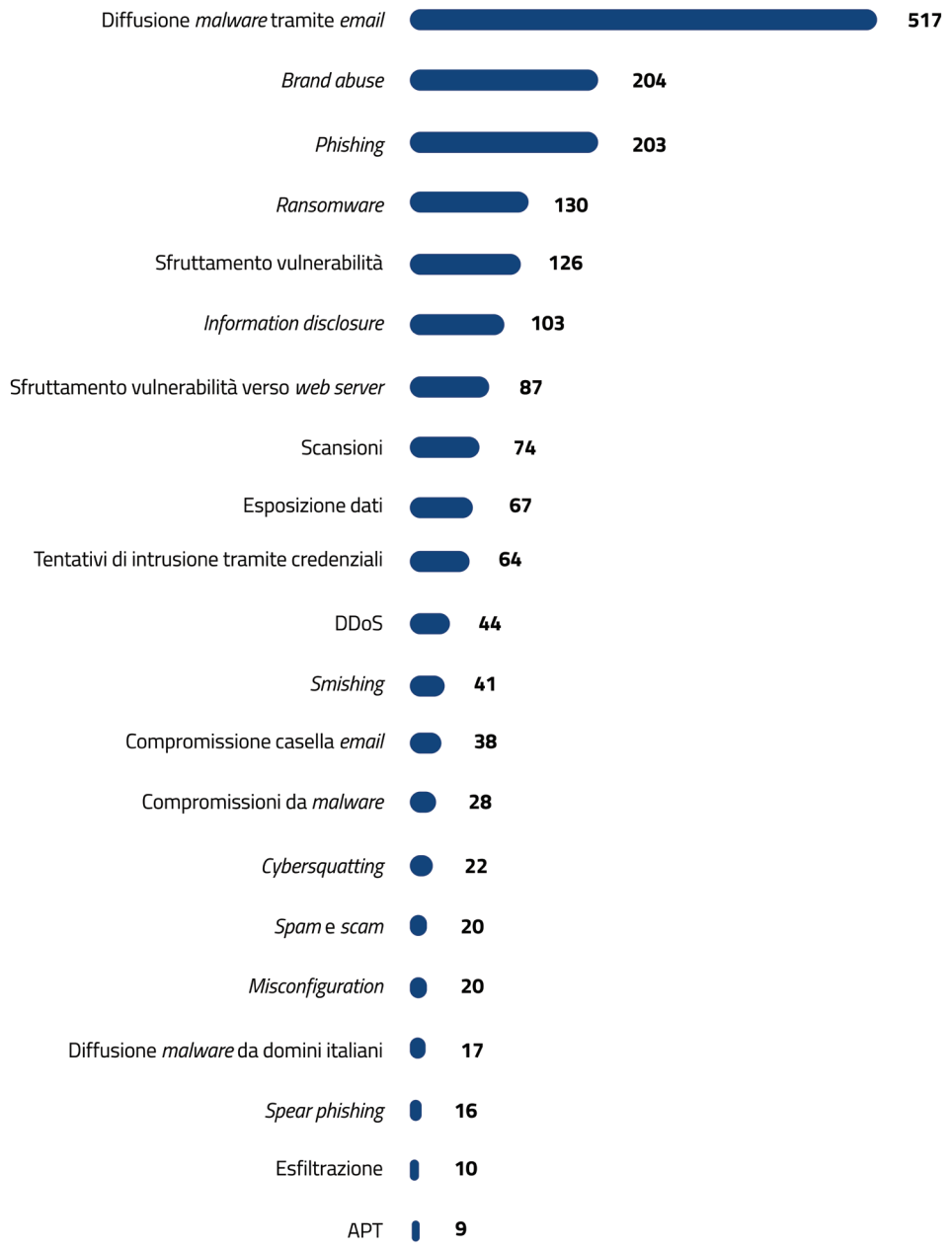


FIGURA 11 – TIPOLOGIE DI EVENTI *CYBER* TRATTATI NEL 2022

[6] Ad esempio, un evento di *phishing* spesso è finalizzato anche alla diffusione di un *malware*, che può essere a sua volta un evento di tipo *ransomware*.

3.1.1 *Focus* su attività connesse al conflitto russo-ucraino

Per quanto attiene al contesto del conflitto in corso tra Russia e Ucraina, l'Agenzia ha svolto sin da subito attività finalizzate ad elevare il livello di allerta degli operatori pubblici e privati rispetto al rischio *cyber* derivante dalla situazione internazionale.

L'attività di natura operativa dell'Agenzia si è intensificata, e ciò ha determinato una crescita delle comunicazioni verso i soggetti della *constituency*, tanto che, nel periodo compreso tra il 26 febbraio e il 29 marzo 2022, sono state inviate circa **19.500 comunicazioni** dirette prevalentemente a soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica. Ancora, in due distinti periodi temporali riferibili, il primo, ai giorni del 17 e 18 maggio 2022 e, il secondo, al 28 giugno 2022, sono state inviate circa **1.000 comunicazioni** aventi rispettivamente ad oggetto l'individuazione di attività di preparazione ad attacchi *Distribuited Denial of Service* (DDoS) contro soggetti nazionali e attacchi DDoS ai danni di organizzazioni europee.

Nel medesimo contesto, sono stati, altresì, condivisi elementi informativi tecnici (Indicatori di Compromissione), al fine di sensibilizzare la *constituency* relativamente a possibili attacchi di tipo DDoS, la cui incidenza straordinaria (vedasi paragrafo 3.1.3 *Focus su eventi DDoS*), osservata a maggio 2022, lasciava ipotizzare che detti attacchi, nell'ambito di un conflitto ibrido, potessero essere una conseguenza del sostegno italiano all'Ucraina in ambito UE e NATO.

L'analisi di tali eventi ha consentito al CSIRT Italia di identificare le peculiari metodologie utilizzate per condurre tali attacchi, in relazione ai quali sono stati pubblicati, in una sezione dedicata del sito *web* istituzionale[7], gli elementi informativi e operativi necessari per la pianificazione delle attività di mitigazione sui rischi *cyber* connessi.

Sul medesimo portale del CSIRT Italia, è stato reso pubblico uno specifico *report* sulle vulnerabilità più sfruttate dagli attori di matrice statuale, e sono stati emessi **13** ***alert*** su minacce *cyber* e altri eventi rilevanti, utili per attuare specifiche azioni di prevenzione, contenimento e mitigazione.

[7] https://www.csirt.gov.it/contenuti?tags=Ucraina

3.1.2 *Focus* su eventi *ransomware*

Nel periodo di riferimento, il *ransomware* si è confermato tra le minacce più impattanti. L'Agenzia, nel corso del 2022, ha osservato **130 eventi** *ransomware* in danno a Pubbliche Amministrazioni e operatori privati, la cui distribuzioni temporale è mostrata in Figura 12.

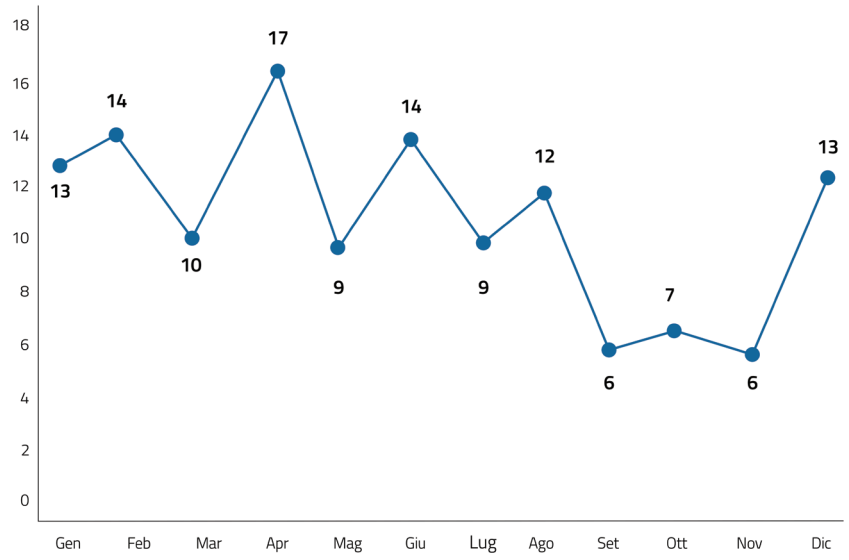


FIGURA 12 - EVENTI *RANSOMWARE* RILEVATI NEL 2022

Il dato rappresenta, tuttavia, solo una parte del numero complessivo di attacchi *ransomware* effettivamente avvenuti, poiché in taluni casi le vittime – specie se appartenenti al tessuto produttivo delle Piccole Medie Imprese, spesso sprovviste di *know-how* e strutture interne dedicate – sono inclini a non segnalare l'evento, gestendolo in autonomia.

Nell'82% dei casi le vittime appartengono al settore privato, a fronte di un rimanente 18% di vittime appartenenti alla Pubblica Amministrazione (Figura 13).

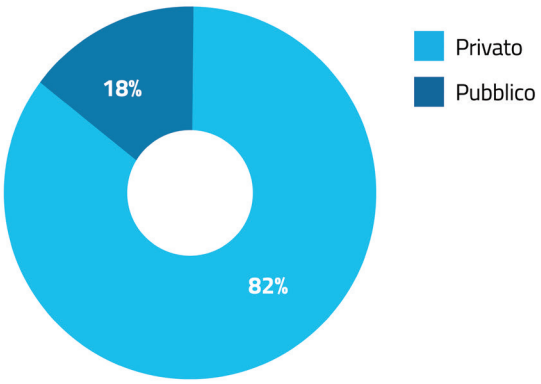


FIGURA 13 - EVENTI *RANSOMWARE* PER TIPOLOGIA DI VITTIMA: PUBBLICO/PRIVATO

Per quanto attiene alla dimensione aziendale dei soggetti privati colpiti, il 31% degli eventi *ransomware* ha interessato grandi imprese, il 28% ha visto coinvolte medie imprese, mentre il restante 41% ha riguardato le piccole imprese (Figura 14).

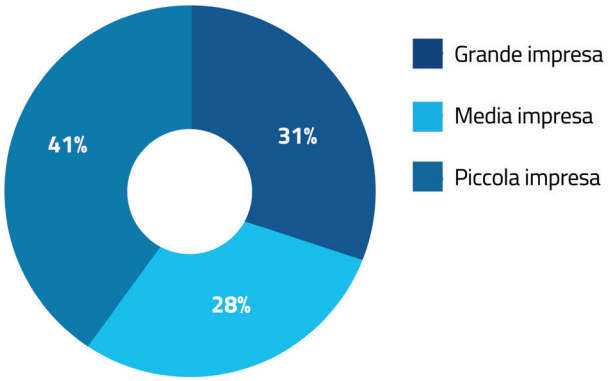


FIGURA 14 – EVENTI *RANSOMWARE* PER DIMENSIONE AZIENDALE

Classificando le vittime in base ai settori di attività economica, emerge come il settore manifatturiero sia stato il più colpito, seguito da quello tecnologico, dal *retail* e dal settore sanitario (Figura 15).

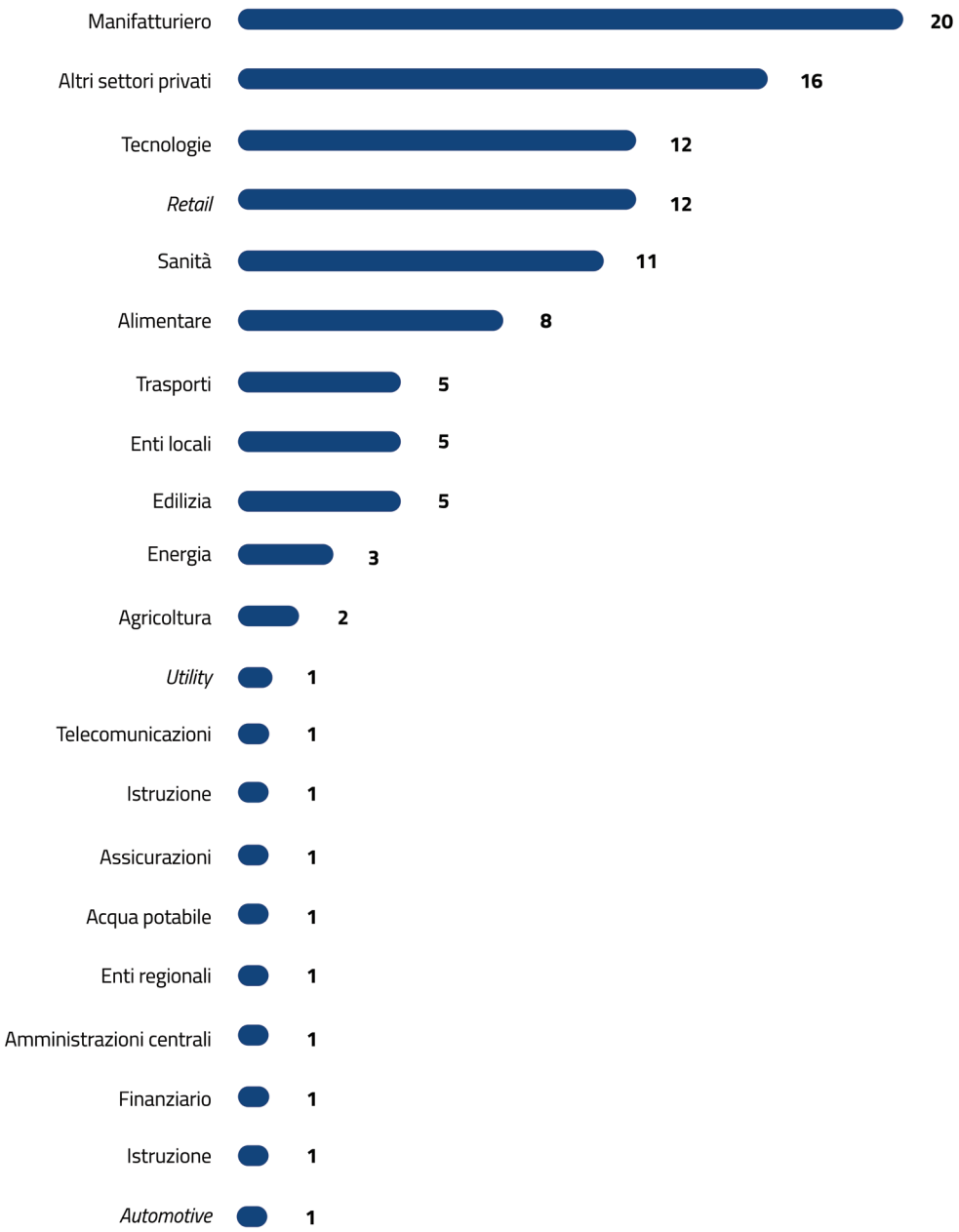


FIGURA 15 – *RANSOMWARE* PER SETTORE DI ATTIVITÀ ECONOMICA DELLA VITTIMA

Da un punto di vista geografico, le zone più interessate dal fenomeno corrispondono alle grandi aree metropolitane di Roma, Milano, Torino e ai distretti manifatturieri del Nord Ovest e Nord Est (Figura 16). Tale contesto è presumibilmente determinato dalla maggiore presenza, in tali zone, di imprese operanti nel settore manifatturiero.

Box 3

GLI ATTACCHI *RANSOMWARE*

In questo tipo di minaccia l'attaccante, di regola, cifra i dati di un'organizzazione al fine di ottenere il pagamento di un riscatto. Recentemente, con l'aumentare della complessità degli attacchi, spesso l'attaccante procede anche a:

1. esfiltrare i dati e minacciarne la pubblicazione salvo pagamento del riscatto (*Double extortion*);
2. pretendere un riscatto anche nei confronti di soggetti terzi (come clienti, fornitori e *partner* dell'organizzazione compromessa) a cui i dati esfiltrati si riferiscono, pena la loro pubblicazione (*Triple extortion*);
3. effettuare contestualmente altri tipi di attacco, come il DDoS al fine di compromettere ulteriormente l'operatività dell'organizzazione.

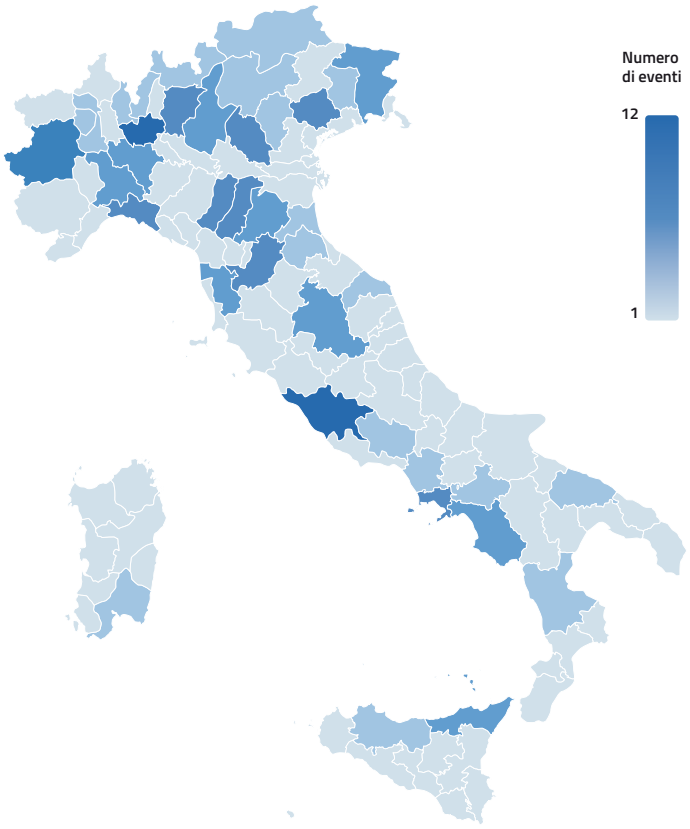


FIGURA 16 – LOCALIZZAZIONE GEOGRAFICA DELLE VITTIME DI EVENTI *RANSOMWARE*

Con riferimento ai *Threat Actors*, nel 2022 gli attacchi sono principalmente stati condotti da **20 diverse *gang* di criminali**, tra le quali le più attive sono risultate "LockBit", "Conti" e "AlphaVM", responsabili della metà degli attacchi totali (Figura 17).

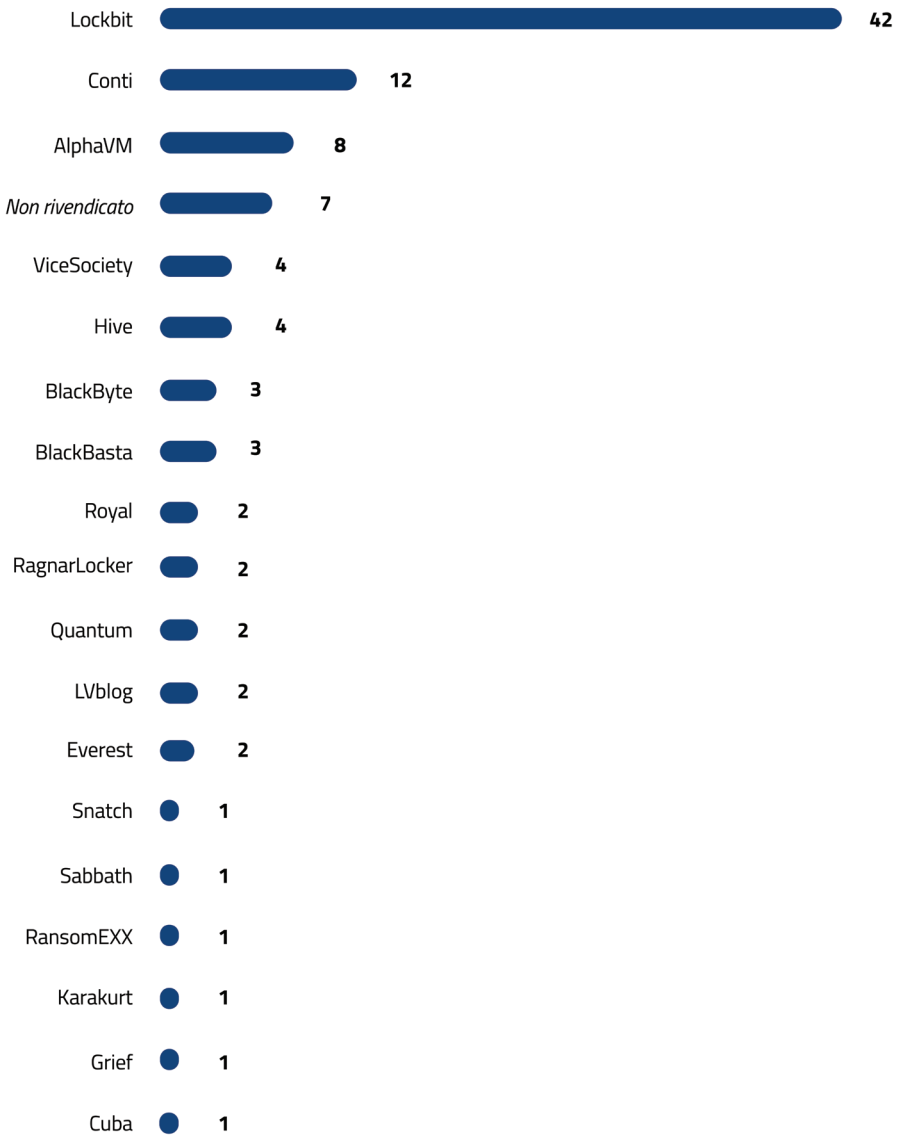


FIGURA 17 – *CYBER GANG* CHE HANNO CONDOTTO ATTACCHI *RANSOMWARE* RILEVATI IN ITALIA NEL 2022

3.1.3 *Focus* su eventi DDoS

A livello internazionale il 2022 è stato caratterizzato da un forte aumento degli attacchi di tipo DDoS (vds. BOX 4). Tale incremento, che ha riguardato anche il nostro Paese, è stato registrato a partire dallo scoppio del conflitto russo-ucraino ed è da ascrivere, per lo più, ai gruppi noti come "Killnet" e "NoName057(16) " (vds. BOX 5) a fini dimostrativi e non distruttivi.

Box 4

GLI ATTACCHI DDOS

Con il termine *Denial of Service* (DoS) si indica un tipo di attacco che mira a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria, senza alcun impatto sull'integrità o confidenzialità dei dati. Nella versione distribuita (*Distributed DoS*) l'attacco proviene da un gran numero di dispositivi ed è diretto verso un *target*. Le *botnet* sono uno strumento per condurre un attacco DDoS.

In base alla specifica risorsa colpita possono essere individuate le seguenti categorie di attacco:

1. **volumetrico**: mira al consumo della disponibilità di banda di rete dell'infrastruttura *target*;
2. **esaurimento di stato**: mira al consumo delle risorse di calcolo e/o di memoria dei dispositivi;
3. **applicativo**: mira al consumo dei processi *software*, del numero di *thread*, del numero connessioni, dello spazio su disco, del *budget* a disposizione (nel caso, ad esempio, in cui il *target* acceda a servizi terzi a pagamento).

Per ulteriori approfondimenti: https://www.csirt.gov.it/contenuti/attacchi-ddos-tipologie-e-azioni-di-mitigazione

Box 5

KILLNET E NONAME057(16)

Killnet è un collettivo *hacker* filo-russo noto per i suoi attacchi DDoS contro istituzioni governative e società private in diversi Paesi, avvenuti durante l'invasione russa dell'Ucraina del 2022.

NoName057(16) è un gruppo *hacker* filo-russo che, a partire da marzo 2022, ha rivendicato attacchi informatici nei confronti di *siti web* ucraini, statunitensi ed europei. Tale gruppo ha dichiarato il proprio sostegno alla Federazione Russa nel conflitto in corso con l'Ucraina, anche mediante un manifesto che definisce le attività condotte nel dominio *cyber* come un atto di vendetta per la guerra contro la Russia.

Anche il sito *web* istituzionale dell'Agenzia, all'indomani dell'attacco russo all'Ucraina, ha subito un attacco di tipo *DDoS* di considerevole entità, che è stato, però, totalmente mitigato dai sistemi di sicurezza preposti.

Nel 2022, gli eventi significativi di tipo DDoS trattati dal CSIRT Italia in danno di soggetti italiani sono stati **44**, distribuiti nel tempo come rappresentato in Figura 18.

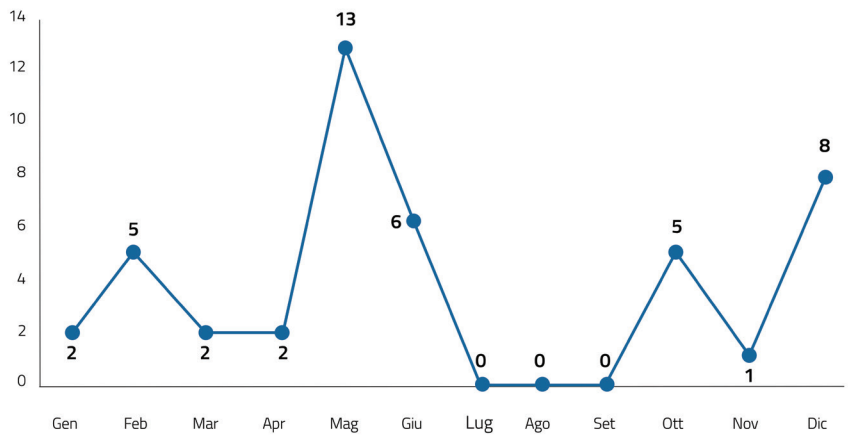


FIGURA 18 – NUMERO DI DDoS RILEVANTI TRATTATI NEL 2022

In Figura 19 è riportata la distribuzione delle vittime di attacchi DDoS nei settori di riferimento. Si noti come circa il 35% dei DDoS abbia colpito settori afferenti alla Pubblica Amministrazione.

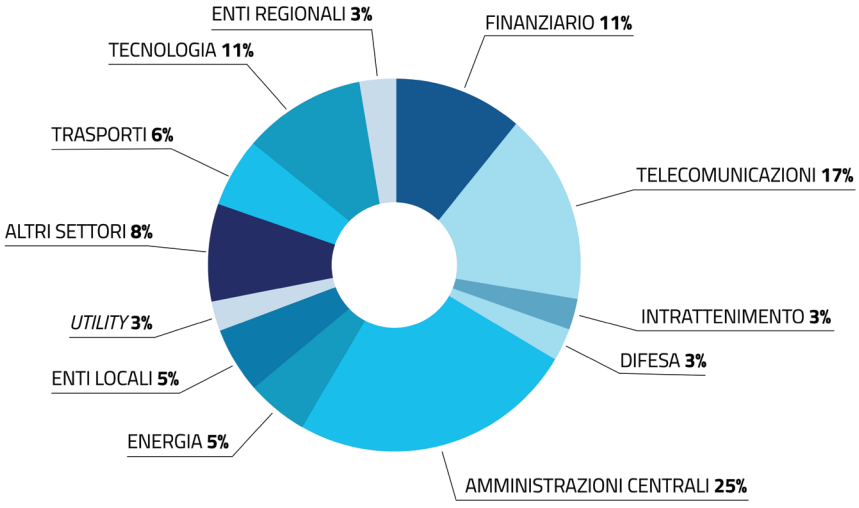


FIGURA 19 – DISTRIBUZIONE DELLE VITTIME DI DDoS NEI SETTORI

3.1.4 *Focus* sulla Pubblica Amministrazione

Nel corso del 2022, l'ACN ha gestito **160 eventi** *cyber* in danno di istituzioni pubbliche nazionali. Di questi, 57 hanno avuto un impatto confermato dai soggetti colpiti, procurando talvolta il malfunzionamento dei sistemi e conseguenti ritardi nell'erogazione dei servizi. Le tipologie di tali incidenti sono rappresentate in Figura 20.

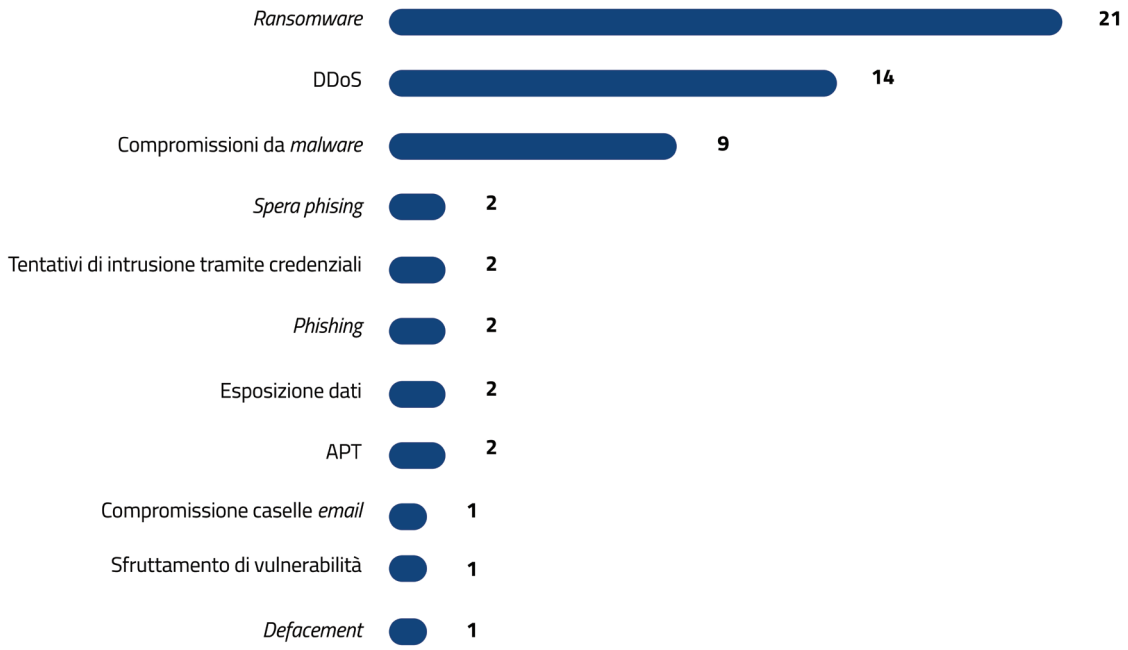


FIGURA 20 – INCIDENTI CONFERMATI DALLE VITTIME IN DANNO DELLA PUBBLICA AMMINISTRAZIONE ORGANIZZATI PER TIPOLOGIA

Considerando la frequenza e l'impatto (una media di oltre un incidente a settimana) delle diverse tipologie di eventi, emerge come il *ransomware* sia l'attività più sfruttata per recare attacchi nei confronti delle istituzioni pubbliche, seguita da attacchi di tipo DDoS e dall'infezione dei sistemi tramite altri tipi di *malware*.

Di seguito, la Figura 21 mostra le tipologie di attacco rapportate alle diverse tipologie delle istituzioni pubbliche[8].

[8] Ricavato dal "Censimento permanente delle Istituzioni pubbliche" dell'ISTAT.

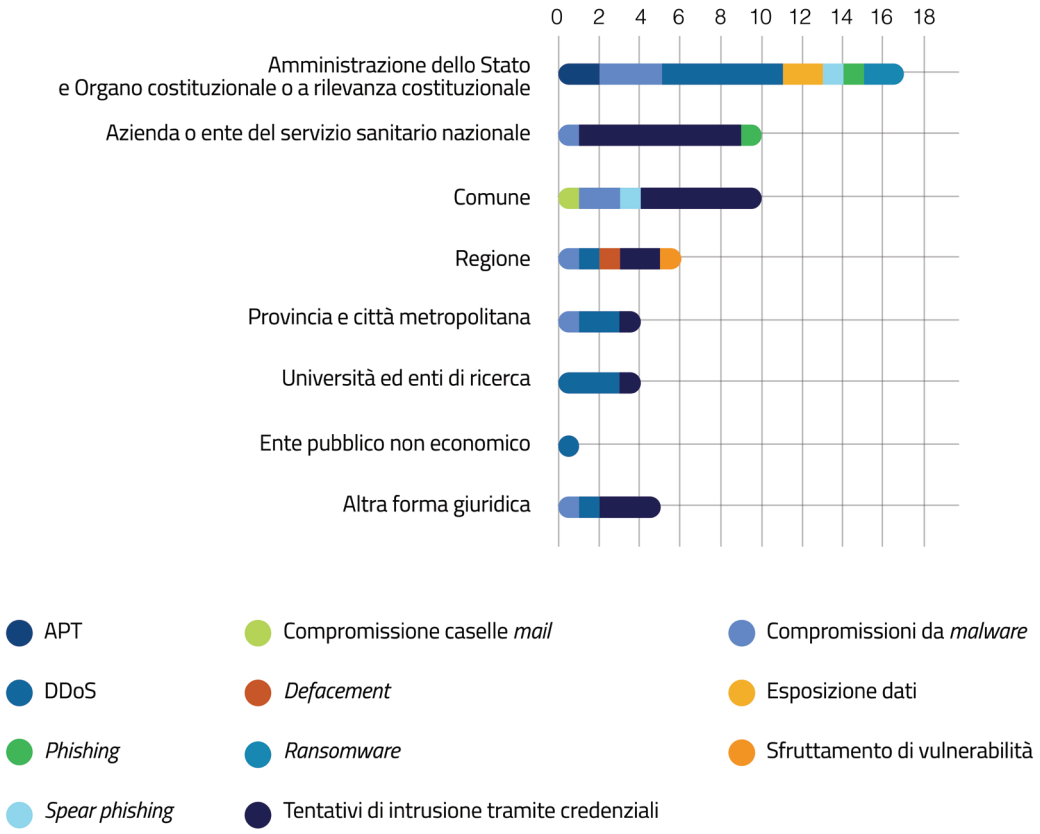


FIGURA 21 – DISTRIBUZIONE DELLE TIPOLOGIE DI INCIDENTI CONFERMATI DALLA VITTIMA RISPETTO ALLE DIVERSE ISTITUZIONI PUBBLICHE

È possibile osservare che, mentre le Amministrazioni Centrali dello Stato sono state colpite in prevalenza da DDoS, il settore sanitario, i Comuni e le Regioni sono oggetto principalmente di *ransomware*.

3.2 Interventi a supporto delle vittime di attacchi *cyber*

Tra i compiti attribuiti all'ACN figura l'intervento diretto in caso di incidente, per i fini di resilienza, di cui l'Agenzia è responsabile, che può avvenire anche in forma di supporto alle vittime di incidenti e attacchi *cyber*. Esso viene garantito dalle articolazioni tecnico-operative dell'Agenzia e consiste principalmente nell'individuazione e nell'implementazione delle azioni da attuare nell'immediato per il contenimento dell'incidente, nonché di quelle volte al ripristino di una efficiente erogazione dei servizi. Nei casi più complessi il supporto può avvenire tramite l'intervento in *loco* di un *team* di specialisti DDFIR (*Deployable Digital Forensic Incident Response*), in raccordo con la Polizia postale e delle comunicazioni, che nel corso del 2022 è intervenuto in **10 diversi incidenti** – tutti avvenuti sul territorio nazionale (Figura 22).

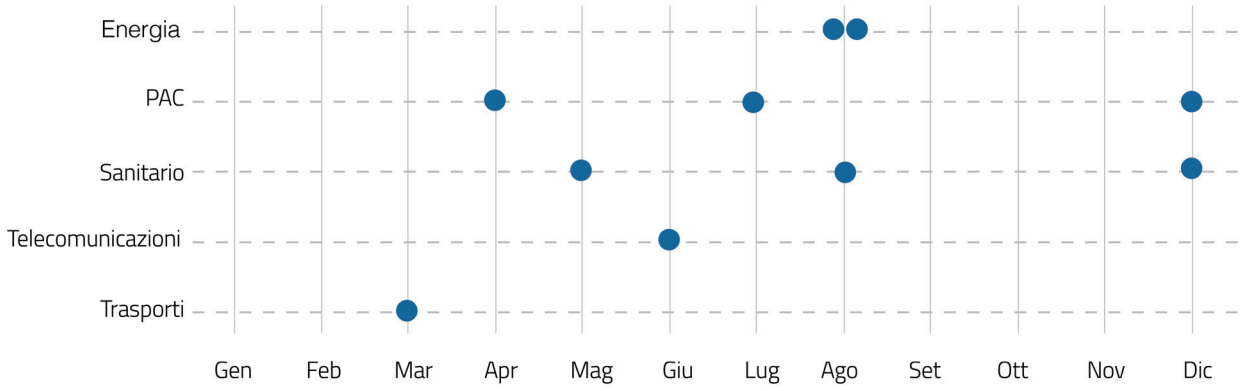


FIGURA 22 – INTERVENTI: INDICAZIONE DEI SETTORI DI OPERATIVITÀ DELLE VITTIME.

3.2.1 Principali criticità riscontrate

Le analisi e le interazioni avute con i soggetti colpiti hanno consentito di identificare le **principali criticità** che hanno determinato tali incidenti, ovvero:

errate politiche di sicurezza e gestione delle credenziali di accesso, più in particolare:

- presenza di credenziali pubblicamente esposte, talvolta oggetto di precedenti *data breach* o dovuta alla presenza di infrastrutture già compromesse in precedenza da altri attaccanti e per le quali non sono state effettuate attività di mitigazione; ad essa si aggiunge l'assenza di utilizzo di meccanismi di autenticazione forte (ad esempio, multifattore) per l'accesso ai servizi;

- mancata cifratura delle *password* necessarie per l'accesso a sistemi/servizi critici e loro memorizzazione in *file* accessibili dall'esterno, tramite servizi interrogabili senza autenticazione;

fattori di **obsolescenza di sistemi e dispositivi** utilizzati. In particolare, tale obsolescenza riguarda non soltanto prodotti IT, ma anche OT (cd. *Operational Technology*, per il monitoraggio e/o il controllo dei processi industriali) e specifiche apparecchiature di settore, per le quali i produttori non forniscono più il servizio di assistenza e manutenzione risultando più esposti ad attacchi informatici;

non conformità a *best practice* di settore, che rendono di fatto vulnerabili anche infrastrutture moderne. In particolare:

- assenza di *policy* di gestione e profilazione degli *account* utente (ad esempio, la gestione dei privilegi amministrativi, che permettono il pieno controllo dell'infrastruttura, risulta spesso carente);
- mancato aggiornamento dei sistemi;
- *design* architetturale non sicuro (si riscontra frequentemente l'assenza di soluzioni di segregazione[9] a livello di rete);
- procedure interne carenti rispetto a gestione, manutenzione e implementazione dei servizi (nella maggior parte dei casi gli attacchi avvengono sfruttando vulnerabilità nei sistemi già note e non corrette denotando forti carenze per gli aspetti di *patch management*);
- mancata conservazione dei *log*;
- assenza di procedure e piani per la mitigazione e la risposta agli incidenti;

alle due precedenti criticità si aggiungono **la carenza di *know-how* e la scarsa formazione**, rilevate anche in presenza di adeguate architetture di sicurezza, da imputarsi principalmente alla mancanza di investimenti relativi alla formazione del personale tecnico e all'impossibilità di reperire, all'interno dell'organizzazione, figure con capacità adeguate alla gestione dei sistemi stessi.

[9] Suddivisione delle reti in compartimenti separati fornendo a ciascuno specifici controlli e servizi di sicurezza.

3.3 Attività di monitoraggio proattivo

Nel corso del 2022 è stato compiuto un importante sforzo al fine di avviare servizi operativi per incrementare la sicurezza degli *asset* di pertinenza dei soggetti maggiormente critici della *constituency*. Ciò si è tradotto in specifiche attività di monitoraggio volte all'individuazione di fattori di rischio, come, ad esempio, mis-configurazioni, potenziali infezioni o disponibilità di credenziali di accesso.

Al riguardo, è stato dato un supporto puntuale a numerosi soggetti, producendo, ove opportuno, dettagliati *report* aventi ad oggetto non solo l'analisi dello spazio di indirizzamento IP, ma anche l'eventuale presenza di errori nelle configurazioni dell'infrastruttura *Domain Name System* (DNS) utilizzata e sugli *account* potenzialmente compromessi.

Sempre nell'ambito di tali attività a favore dei soggetti della *constituency*, sono state inviate comunicazioni massive verso Pubbliche Amministrazioni e imprese che esponevano su *internet* servizi affetti da vulnerabilità critiche, notoriamente sfruttate dagli attaccanti per ottenere accesso alle reti.

L'attività preventiva ha inoltre permesso di identificare **764 *asset* nazionali** con segnali di potenziale compromissione e per i quali, di seguito alle doverose interazioni con i soggetti che esponevano detti sistemi, sono state effettuate le opportune azioni di mitigazione.

Tra le attività svolte in tema di monitoraggio delle minacce *cyber* va sottolineato, in particolare, lo studio di attori cd. *Advanced Persistent Threats*, che hanno condotto tentativi di infezione, tramite campagne di *phishing* o tecniche di *social engineering*, in particolare verso **5 soggetti rilevanti**. Al riguardo, sono stati prontamente condivisi – con i citati soggetti e, ove necessario, con altre Istituzioni – gli elementi informativi utili a rilevare tali campagne, al fine di attuare le necessarie azioni di mitigazione.

Infine, durante i mesi di agosto e settembre 2022, sono state svolte specifiche attività a supporto del Dipartimento per gli Affari Interni e Territoriali (DAIT) del Ministero dell'interno, finalizzate a garantire la cybersicurezza delle elezioni politiche 2022 (vds. BOX 6).

Box 6

ATTIVITÀ DI MONITORAGGIO PROATTIVO DURANTE LE ELEZIONI POLITICHE 2022

Al fine di monitorare e ridurre i profili di rischio cibernetico collegati alle elezioni, l'Agenzia ha avviato una specifica attività di monitoraggio a supporto del Dipartimento per gli Affari Interni e Territoriali (DAIT) del Ministero dell'Interno che gestisce il Sistema Informativo Elettorale (SIEL), il sistema informatico che raccoglie e distribuisce in tempo reale i dati relativi ai risultati dello spoglio dei voti.

L'Agenzia ha così pianificato e concordato con il DAIT una serie di attività preventive e di monitoraggio finalizzate alla individuazione delle criticità sul perimetro esposto del SIEL, e dei sistemi informativi contigui, al fine di rilevare eventuali eventi cibernetici nei giorni precedenti la consultazione elettorale, nonché durante lo svolgimento delle procedure di voto e le successive attività di spoglio, che avrebbero potuto causare una compromissione o una indisponibilità del SIEL.

L'Agenzia ha garantito la presenza di personale 24/7 dedicato esclusivamente a queste attività, facendosi promotrice di un'azione coordinata tra le diverse istituzioni con la costituzione, presso l'ACN, di una "*war-room*" permanente, durante il fine settimana elettorale, cui ha preso parte personale di ACN in costante raccordo con DAIT e Polizia postale e delle comunicazioni/CNAIPIC.

3.4 Prevenzione e preparazione a situazioni di crisi cibernetica

I principali strumenti attraverso cui viene esercitata, ai sensi del decreto-legge, l'attività di prevenzione e preparazione a situazioni di crisi cibernetica, di cui si darà atto nel presente paragrafo, sono costituiti, da un lato, dall'azione di coordinamento del Nucleo per la cybersicurezza, dall'altro, dalla partecipazione alle esercitazioni.

A livello ancora più operativo, vi è l'attività di pianificazione e lo svolgimento delle esercitazioni, anche di carattere multi-settoriale e/o multi-dominio, quale strumento utile non solo alla preparazione e alla gestione delle crisi *cyber*, ma anche per collaudare i meccanismi e le procedure predisposte, nonché addestrare il personale preposto.

3.4.1 Attivazioni del Nucleo per la cybersicurezza

Quale sede primaria di coordinamento interministeriale, a livello tecnico-operativo, in materia di cybersicurezza e resilienza nazionale nello spazio cibernetico, il Nucleo per la cybersicurezza (NCS) ha confermato, nel corso del 2022, il suo ruolo centrale ai fini della prevenzione e della gestione di incidenti e attacchi cibernetici (vds. BOX 7), avvalendosi di procedure di condivisione informativa snelle, di un formato di funzionamento agile e della preziosa collaborazione istituzionale assicurata dalle Amministrazioni componenti (Figura 23).

FIGURA 23 – AMMINISTRAZIONI DEL NUCLEO PER LA CYBERSICUREZZA

L'insorgere di eventi critici per la sicurezza nazionale nello spazio cibernetico – in misura crescente derivanti dal contesto geopolitico attuale – contribuisce alle numerose attivazioni del Nucleo. In particolare, tra le principali cause di tali eventi spiccano la rapida evoluzione del panorama della minaccia cibernetica, popolato da attori sempre più sofisticati, e, non da ultimo, il rischio tecnologico legato alle catene di approvvigionamento e alla continua scoperta di nuove, insidiose vulnerabilità di sicurezza.

In relazione al già menzionato contesto di crisi russo-ucraina, l'Agenzia ha, infatti, convocato specifiche sedute dell'NCS, anche in composizione ristretta, al fine di instaurare tra le Amministrazioni coinvolte un coordinamento continuativo, e promuovere campagne di sensibilizzazione pubblica sui rischi *cyber* potenzialmente innescabili dallo sviluppo della crisi stessa. In tale ottica, sono state previste specifiche sedute allargate alla partecipazione di circa **50 operatori dei settori energetico, finanziario** e **delle telecomunicazioni**. Sempre nel medesimo contesto, l'ACN ha provveduto a verificare, per il tramite della Farnesina, la presenza di aziende strategiche italiane in territorio ucraino, al fine di prevenire eventuali ripercussioni sugli *asset* nazionali, causati dalla maggiore esposizione delle infrastrutture digitali in uso ai rami esteri delle citate aziende.

Più importante e certamente innovativo – anche per effetto delle accresciute funzioni attribuite sul piano delle *policy* dalla normativa vigente – il ruolo svolto dal Nucleo ai fini dell'adozione di alcune disposizioni normative[10] volte a rafforzare la sicurezza nazionale nello spazio cibernetico. Tra esse, quella che prevede che le Pubbliche Amministrazioni procedano alla diversificazione tecnologica di prodotti e servizi tecnologici di sicurezza informatica di aziende produttrici legate alla Federazione Russa (di cui si dirà, più nel dettaglio, al successivo Cap. 4.5). Intervento, questo, che nel confermare l'ampiezza dell'azione di coordinamento interministeriale esercitata dal Nucleo, a livello tecnico-operativo, è anche una dimostrazione del ruolo dell'alto consesso, concepito sempre più quale "piattaforma interattiva e partecipata" grazie alla collaborazione fra le Amministrazioni portatrici di competenze fondamentali nei loro ambiti di attività.

Più in generale giova evidenziare come, già a partire dal 2021, il consesso sia stato attivato anche in modalità preventiva, a seguito di segnalazioni giunte da operatori strategici per il sistema-Paese, nonché in concomitanza con la scoperta di vulnerabilità gravanti su prodotti di sicurezza informatica, anche al fine di prevenire potenziali impatti connessi alla robustezza della catena di approvvigionamento.

[10] Confluite nel decreto-legge 21 marzo 2022, n. 21, recante *"Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina".*

Nel periodo 1° gennaio-31 dicembre 2022, il Nucleo per la cybersicurezza si è riunito **27 volte**.

Box 7

IL NUCLEO PER LA CYBERSICUREZZA

Istituito in via permanente presso l'ACN, il Nucleo per la cybersicurezza (NCS) opera a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi cibernetica e per l'attivazione delle procedure di allertamento.

L'NCS è presieduto dal Direttore generale dell'ACN ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del Dipartimento delle informazioni per la sicurezza-DIS, dell'Agenzia informazioni e sicurezza esterna-AISE, dell'Agenzia informazioni e sicurezza interna-AISI, di ciascuno dei Ministeri rappresentati nel Comitato interministeriale per la cybersicurezza-CIC e dal Dipartimento della Protezione civile della Presidenza del Consiglio dei ministri, nonché integrato, per la trattazione di informazioni classificate, da un rappresentante dell'Ufficio centrale per la segretezza-UCSe del DIS.

Il Nucleo può essere convocato in composizione ristretta con la partecipazione delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi che coinvolgono aspetti di cybersicurezza.

3.4.2 Esercitazioni

All'avvio della Presidenza di turno francese dell'UE, si è svolta la "sequenza esercitativa" denominata EU *Cyber Crisis Linking Exercise on Solidarity* (EU CyCLEs), che ha abbracciato tutto il primo quadrimestre del 2022. Tale esercizio si pone l'obiettivo di rafforzare il coordinamento tra le comunità addette alla gestione delle crisi *cyber* e la componente diplomatica[11], anche con il coinvolgimento del livello politico nazionale.

La partecipazione nazionale a EU CyCLES è stata assicurata dal MAECI in stretto raccordo con l'ACN, il cui Direttore generale ha preso parte alla riunione riservata ai membri di vertice (c.d. *Executive*) del *Cyber Crisis Liaison Organisation Network* (CyCLONe).

In particolare, lo scenario in cui si è giocata l'esercitazione prevedeva un attacco su larga scala alla catena di approvvigionamento, con impatti intersettoriali e transnazionali, caratterizzato da un graduale inasprimento della situazione, fino a sfociare in un incidente di portata tale da saturare le capacità di risposta di uno Stato membro e minacciarne seriamente diversi altri, con danni materiali e perdita di vite umane.

[11] In particolare, lato istituzioni europee, vi hanno preso parte il Comitato dei Rappresentanti Permanenti, il Comitato Politico e di Sicurezza e l'*Horizontal Working Party on Cyber Issues* (HWPCI) del Consiglio dell'UE, nonché il *Cyber Crises Liaison Organisation Network* (CyCLONe).

La prima fase dell'esercizio si è focalizzata sulla dimensione interna della crisi a livello UE, con l'obiettivo di identificare le modalità di supporto al decisore politico attraverso la rete CyCLONe (specie con riferimento ai meccanismi di solidarietà e mutua difesa, con l'eventuale attivazione dell'articolo 42.7 del Trattato sull'Unione europea-TUE[12]). La seconda fase ha, invece, avuto ad oggetto la dimensione esterna, con l'attivazione di tutti gli strumenti di risposta a disposizione dell'UE, incluso il cd. *cyber diplomacy toolbox*[13] e l'attivazione dell'articolo 42.7 del TUE.
Allo scopo di testare l'aggiornamento delle procedure CyCLONE, anche nel 2022 si è tenuto l'annuale evento UE di alto livello ***Blueprint***[14] ***Operational Level Exercise*** **(Blue OLEx)**, a cui partecipano gli *Executive*, nonché gli omologhi delle Istituzioni, Organi e Agenzie dell'UE (EUIBA) coinvolti. La quarta edizione di Blue OLEx si è svolta nel novembre del 2022 a Vilnius (Lituania) ed è stata l'occasione per approfondire i temi del mutuo soccorso, nonché del ruolo delle EUIBA nella gestione di una crisi di natura cibernetica con impatti multi-settoriali e transfrontalieri, nonché con attacchi *cyber* ai danni delle principali Istituzioni europee.

Nell'ambito della *Counter Ransomware Initiative* (vds. Cap. 7.2), si è svolta, nel settembre 2022, la *Ransomware Resilience Exercise* (RRE), esercitazione di tipo *scenario-based discussion*, promossa da India e Regno Unito con la partecipazione di 16 Paesi e incentrata sulla gestione di un imponente attacco *ransomware* alle infrastrutture del settore energia. L'esercizio si prefiggeva di collaudare le capacità di risposta dei Paesi partecipanti, nel più ampio contesto della collaborazione internazionale.

L'Agenzia ha coordinato la partecipazione nazionale, che ha visto il coinvolgimento, per i profili di rispettiva competenza, del MAECI, del Ministero dell'interno, del Ministero della difesa e del Ministero dell'ambiente e della sicurezza energetica.

Sempre con riferimento alla risposta coordinata agli incidenti e alle crisi cibernetiche su vasta scala delineata nella citata *Blueprint*, nella prima parte del 2022 sono proseguite le attività di pianificazione relative all'esercitazione *cyber* promossa da ENISA – l'Agenzia europea per la cybersicurezza – denominata ***Cyber Europe*** **2022**, mediante il coinvolgimento di tutti gli attori in occasione di 5 riunioni interministeriali e di vere e proprie sessioni per la preparazione dei 6 "giocatori nazionali" e la produzione di tutta la documentazione necessaria per procedere in maniera strutturata e coordinata in fase preparatoria e in quella di esecuzione (in totale 9 incontri).

[12] "…Qualora uno Stato membro subisca un'aggressione armata nel suo territorio, gli altri Stati membri sono tenuti a prestargli aiuto e assistenza con tutti i mezzi in loro possesso, in conformità dell'Art. 51 della Carta delle Nazioni Unite. Ciò non pregiudica il carattere specifico della politica di sicurezza e di difesa di taluni Stati membri.
Gli impegni e la cooperazione in questo settore rimangono conformi agli impegni assunti nell'ambito dell'Organizzazione del trattato del Nord-Atlantico che resta, per gli Stati che ne sono membri, il fondamento della loro difesa collettiva e l'istanza di attuazione della stessa."

[13] Si tratta di una raccolta di strumenti per sistematizzare le possibili azioni diplomatiche a disposizione dell'UE per prevenire o rispondere ad azioni malevole, al fine di mantenere la pace e la stabilità dello spazio cibernetico. Tra queste spicca la possibilità di adottare misure restrittive contro individui o enti ritenuti responsabili di azioni malevole ai danni di uno o più Stati dell'UE.

[14] Con "*Blueprint*", si fa riferimento alla Raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi cibernetiche su vasta scala.

A valle dell'attività preparatoria, l'8 e il 9 giugno 2022 si è tenuta l'esercitazione che ha visto il coinvolgimento, a livello europeo, dei CSIRT e delle autorità *cyber* degli Stati membri, della rete CyCLONe, della rete CSIRT, della Commissione e del CERT-EU, nonché, a livello nazionale, dell'ACN, del Ministero dell'interno (CNAIPIC), del Ministero della difesa (COR), del Ministero della salute, nonché di altri attori istituzionali e operatori del settore sanitario di tre Regioni.

Tutti gli attori si sono potuti confrontare in uno scenario in cui venivano simulati attacchi *cyber* su vasta scala ai danni di operatori del settore sanitario, analizzando gli incidenti e i *malware* simulati, e testando l'attivazione di EU CyCLONE e la rete degli CSIRT europei.

Nel periodo di svolgimento, presso l'ACN è stata costituita la cabina di regia nazionale, che ha assicurato il coordinamento, in uno con la cabina di regia UE (istituita presso ENISA), nonché il monitoraggio a livello nazionale dell'esercizio, il raccordo con i pianificatori delle altre Amministrazioni coinvolte e il supporto ai giocatori per le problematiche legate al corretto svolgimento dell'esercizio.

L'evento ha offerto un'utile occasione non solo per collaudare, in un contesto sfidante di minaccia *cyber* che vede coinvolto uno dei settori sottoposti alla disciplina della Direttiva UE NIS, la cooperazione nell'ambito della gestione degli incidenti e delle crisi su vasta scala a livello UE (sia sul piano operativo, attraverso la rete CyCLONe, sia su quello tecnico con la rete degli CSIRT), ma anche per verificare, a livello nazionale, la capacità di cooperazione tra gli attori governativi centrali (in primo luogo le Amministrazioni del Nucleo per la cybersicurezza coinvolte nella specifica esercitazione) e quelli locali, nonché con gli operatori del settore salute, testando le capacità di risposta delle articolazioni tecniche governative e degli operatori coinvolti.

Nel contesto delle esercitazioni multi-dimensionali, promosse a livello nazionale dal Nucleo interministeriale situazione e pianificazione (NISP), nel corso del 2022 sono state portate a termine le attività di pianificazione della componente *cyber* di **PACE EU Integrated Resolve 2022 (IR22)**, esercitazione guidata congiuntamente dal Consiglio dell'Unione europea, dalla Commissione e dal Servizio Europeo per l'Azione Esterna, con l'obiettivo di verificare la capacità dell'Unione e degli Stati membri di rispondere a crisi transfrontaliere e minacce ibride (che includono il vettore *cyber* e quello terroristico), coinvolgendo i livelli operativo e politico-strategico, nonché di testare la cooperazione con la NATO.

Anche in questo caso, la preparazione è stata intensa e ha visto il coinvolgimento degli attori istituzionali in 4 riunioni interministeriali, 12 incontri di coordinamento a livello UE e 1 seminario preparatorio.

Nel mese di novembre, si è quindi tenuta la fase reattiva dell'esercitazione (cd. fase *livex*), per la durata complessiva di 5 giorni, che ha visto la partecipazione, per l'Italia, dell'Ufficio del Consigliere militare, in rappresentanza del NISP, che detiene la titolarità dell'esercizio a livello nazionale, dell'Agenzia per le attivazioni sul piano *cyber*, del Ministero delle infrastrutture e dei trasporti, nonché del personale della Rappresentanza permanente d'Italia presso l'UE. Questa è stata preceduta da una cd. fase *non-livex*, nel corso della quale è stata simulata a Bruxelles la predisposizione di una missione in ambito PSDC (Politica di sicurezza e di difesa comune) che non ha richiesto contributi inerenti alla resilienza *cyber.*

In ambito NATO, l'Agenzia segue le attività promosse dall'Ufficio del *Chief Information Officer* NATO, nonché, nel contesto del NISP, contribuisce alla predisposizione della narrativa *cyber* nelle esercitazioni. Nel citato programma congiunto UE-NATO PACE, è di particolare rilievo la ***Crises Management Exercise***, la quale è volta a migliorare la preparazione e i processi decisionali strategici dell'Allenza e degli Alleati in situazioni di crisi multi-dominio. A tale, ultimo riguardo, nell'anno del periodo di riferimento, è stata assicurata la partecipazione alle riunioni di pianificazione per gli aspetti *cyber*.

3.5 Collaborazione con soggetti pubblici e privati

In uno scenario globale caratterizzato da un costante inasprimento della minaccia *cyber*, l'Agenzia ha avviato un programma teso a formalizzare la collaborazione con soggetti pubblici e privati, anche attraverso la stipula di specifici protocolli d'intesa/accordi con cui entrambe le parti si impegnano a cooperare per innalzare il livello di resilienza cibernetica, scambiando informazioni e realizzando sinergie per la protezione dalla minaccia *cyber*, secondo il paradigma della "difesa partecipata".

È volontà dell'Agenzia proseguire il programma anche nei prossimi anni, nella piena consapevolezza che solo attraverso lo scambio di esperienze e informazioni è possibile incrementare le capacità

di prevenzione e contrasto alle minacce *cyber*. Continueranno, inoltre, le interlocuzioni con diverse organizzazioni che condividono, a titolo gratuito, informazioni su scala nazionale, utili a rafforzare la sicurezza degli *asset* esposti su *internet* e delle credenziali degli utenti.

Nell'ambito dello sviluppo e del mantenimento delle capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta degli incidenti di sicurezza informatica, l'Agenzia ha altresì avviato un processo di **partecipazione** del CSIRT Italia alla rete professionale CSIRT promossa da ***Trusted Introducer***[15]. Questa partecipazione permetterà a CSIRT Italia di conseguire e gestire un livello efficace di cooperazione internazionale, aumentando lo *standard* generale di sicurezza, tanto in termini di risposta ad attacchi informatici, quanto di condivisione di informazioni relative a minacce emergenti. Il **24 maggio 2022**, con la conclusione della prima fase, CSIRT Italia è diventato un *team* accreditato presso *Trusted Introducer*.

Lo scoppio del conflitto in Ucraina ha dato, infine, avvio a numerose attività di *info-sharing*, focalizzate su specifiche minacce *cyber*, con omologhe Agenzie estere, oltre ad aver reso necessario un approfondimento di alcune tematiche per poter incrementare la resilienza ad attacchi di particolare complessità. In tale ambito è stato avviato uno studio mirato sui protocolli di *routing* inter-dominio, sulle relative attività malevole ad essi collegate, come, ad esempio, il c.d. BGP *hijacking*, ossia il dirottamento intenzionale del traffico *internet*, che gli *Internet Exchange Point* (IXP) scambiano tra loro a livello nazionale e mondiale. In tale contesto, l'Agenzia ha avviato attività di coordinamento con gli IXP nazionali, con l'obiettivo di disporre di una rete pronta a gestire simili attacchi, che sarà ulteriormente consolidata in accordo alle specifiche misure previste dalla Strategia Nazionale di Cybersicurezza 2022-26.

[15] Il servizio del *Trusted Introducer* (TI) è stato fondato in Europa nel 2000, con l'obiettivo di favorire e rendere efficace la cooperazione tra *team*, aumentando conseguentemente il livello generale di sicurezza, grazie alla possibilità di rispondere con rapidità agli attacchi informatici e alle nuove minacce emergenti.

3.6 Servizi nazionali *cyber*: HyperSOC, ISAC, Rete CERT

Nel 2022 l'Agenzia ha avviato l'analisi e la progettazione (Figura 21) dei servizi *cyber* nazionali ai fini del potenziamento della *cyber*-resilienza del Paese. Tale attività, peraltro, oltre ad essere in linea con gli obiettivi dell'Investimento 1.5 *Cybersecurity* della Missione 1 Componente 1 del PNRR, darà attuazione ad alcune misure previste dal Piano di implementazione della Strategia nazionale di cybersicurezza.

Per ogni servizio sono stati declinati e formalizzati il modello di servizio, i processi operativi e i requisiti delle piattaforme tecnologiche che ne supportano l'erogazione.

In particolare, tali servizi *cyber* nazionali includono:

- un **HyperSOC**[16] , volto ad assicurare servizi di monitoraggio della *constituency* e delle minacce *cyber* d'interesse. Tale servizio si basa su un sistema di raccolta, correlazione e analisi di dati, sia di quelli già a disposizione dell'Agenzia (tramite *partnership*, dati commerciali, capacità autonoma, ecc.), che di quelli provenienti da soggetti esterni accreditati. Per il tramite dell'HyperSOC, l'Agenzia sarà in grado di erogare servizi non solo di **tipo preventivo**, miranti a ridurre i profili di rischio degli *asset* della *constituency*, tramite la condivisione di informazioni minacce o specifiche criticità rilevate, ma anche di **rilevamento di eventi di sicurezza**, che permetteranno di ottenere un quadro situazionale integrato a livello nazionale, utilizzando, ad esempio, l'incrocio dei dati condivisi dai vari soggetti.

- una **rete di CERT nazionali integrati**[17], federati con il CSIRT Italia, al fine di condividere procedure, processi, strumenti e supporto nella risposta alle minacce emergenti e agli incidenti. Mediante la formalizzazione di una *governance* strutturata, la rete italiana dei CERT potenzierà le capacità di quelli esistenti/nuovi con l'obiettivo di rafforzare la resilienza informatica nazionale attraverso una stretta collaborazione tra il settore pubblico e quello privato. Per la rete di CERT nel corso del 2022 è stata avviata l'attività di analisi tecnico-giuridica per la pianificazione degli avvisi/bandi da pubblicare a valere sul PNRR.

- un ***Information Sharing and Analysis Center*-ISAC centrale presso l'ACN, integrabile con una rete di ISAC settoriali**[18], finalizzato al potenziamento dello scambio di informazioni a valore aggiunto, utili all'innalzamento del livello *cyber*-resilienza del Paese (quali ad

[16] Misura #30 del Piano di implementazione della Strategia nazionale.
[17] Misura #33 del Piano di implementazione della Strategia nazionale.
[18] Misure #34 e #35 del Piano di implementazione della Strategia nazionale.

esempio *best practices* di settore, linee guida, raccomandazioni), oltre che alla promozione di una cultura della cybersicurezza e alla sensibilizzazione sui rischi informatici. Nel 2022 l'Agenzia ha completato la progettazione complessiva dell'ISAC Italia e ha avviato iniziative di promozione per la creazione di ISAC settoriali integrati con ISAC Italia, anche creando una rete di attori pubblici e privati attivi in settori diversi, ma che condividono obiettivi e interessi comuni.

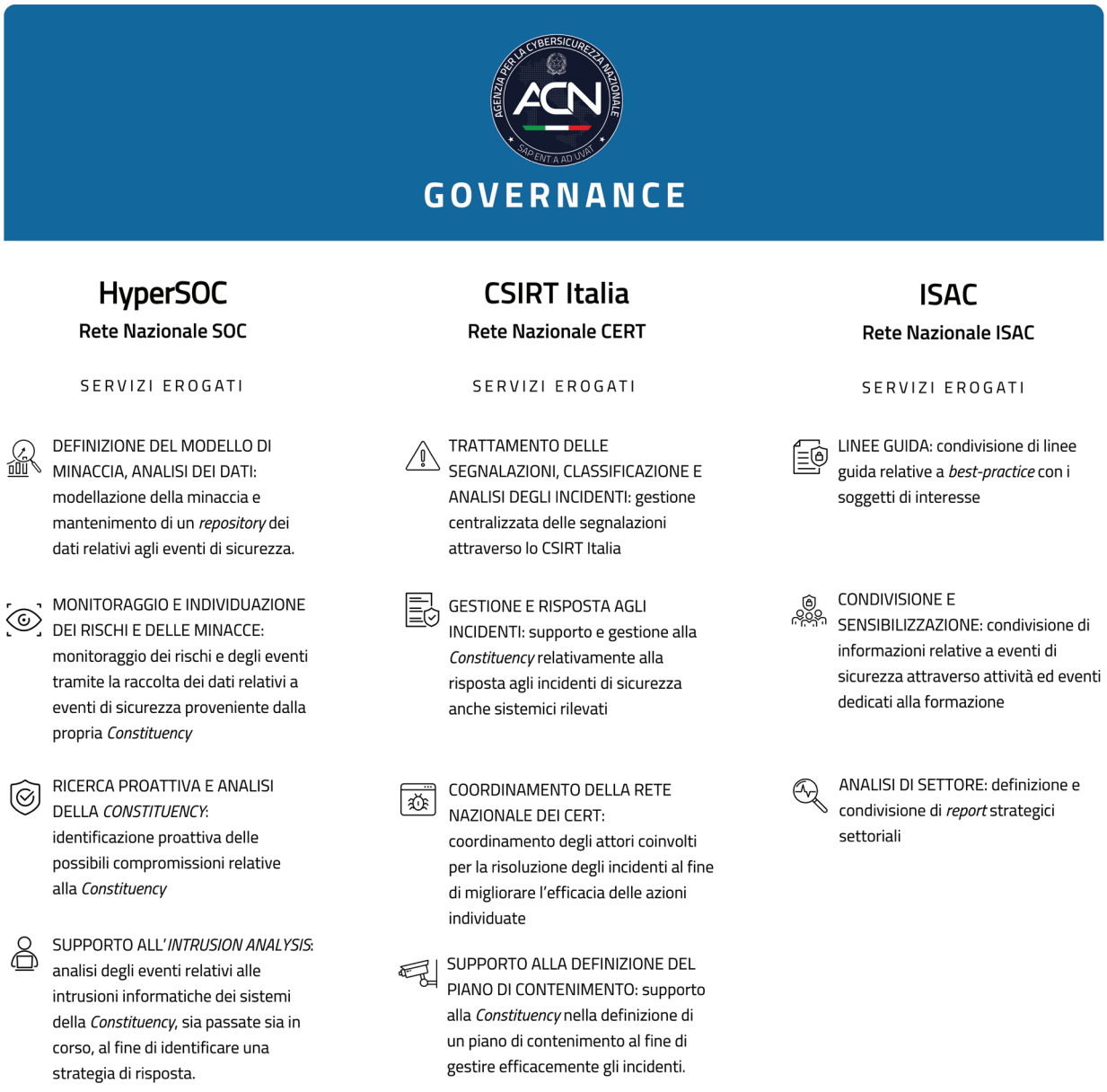


FIGURA 24 – SERVIZI NAZIONALI *CYBER*

04.

LA PROTEZIONE DEGLI ASSET ICT CRITICI E DELLE FUNZIONI E SERVIZI ESSENZIALI DEL PAESE

Oltre alla gestione degli eventi cibernetici, è chiaro che la tutela della resilienza nazionale nello spazio cibernetico richiede l'attuazione di una serie di misure, diverse e complementari, che agiscono in chiave preventiva al verificarsi di attacchi che provochino un pregiudizio allo svolgimento di funzioni e servizi essenziali del Paese e alla sicurezza nazionale nello spazio cibernetico, nonché in chiave funzionale al raggiungimento di un'autonomia strategica.

In tal senso, l'Agenzia è stata impegnata nell'attività di regolamentazione, attuazione e supervisione in relazione alle normative di settore che stabiliscono misure di cybersicurezza, come il decreto-legge 21 settembre 2019, n. 105 ("decreto-legge perimetro") o la direttiva europea relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che stabiliscono specifiche misure di sicurezza, essenziali per avere infrastrutture ICT sicure e resilienti.

L'Agenzia ha, altresì, posto significativo impegno nell'attività di scrutinio tecnologico e certificazione di cybersicurezza, sia attraverso l'avvio delle strutture preposte allo svolgimento delle suddette attività, sia attraverso l'emissione delle certificazioni stesse. Quest'attività è fondamentale nel contribuire alla sicurezza dell'intera catena di approvvigionamento, consentendo di scoprire e, prontamente correggere, eventuali vulnerabilità individuate.

Ulteriore e fondamentale filone di attività per la protezione degli *asset* critici, nonché strategici, del Paese, è stato incentrato sulla partecipazione ai procedimenti relativi all'esercizio del c.d. *Golden Power*, al fine di assicurare una valutazione di affidabilità in relazione alle componenti ad alta intensità tecnologia, tra cui il *cloud computing* e il 5G.

4.1 Il Perimetro di sicurezza nazionale cibernetica

Nel 2022 è stato concluso il percorso di attuazione della normativa del Perimetro di sicurezza nazionale cibernetica (PSNC), delineato dal D.L. 21 settembre 2019, n. 105 (D.L. Perimetro) con l'approvazione, e la successiva adozione e pubblicazione, del DPCM 18 maggio 2022, n. 92, concernente le procedure, le modalità e i termini da seguire in ordine alla gestione dei raccordi del Centro di valutazione e certificazione nazionale (CVCN) con i Laboratori Accreditati di Prova (LAP) e i Centri di Valutazione (CV) del Ministero dell'interno e del Ministero della difesa, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio.

CVCN

Il **Centro di Valutazione e Certificazione Nazionale**-CVCN è la struttura tecnica dell'ACN che, con il supporto di una rete di laboratori accreditati, si occupa di verificare la sicurezza e l'assenza di vulnerabilità note in reti, sistemi e servizi ICT delle infrastrutture da cui dipende l'esercizio di una funzione o l'erogazione di un servizio essenziale per il Paese.

CV

I **Centri di valutazione** del Ministeri dell'interno e della difesa verificano le condizioni di sicurezza e l'assenza di vulnerabilità note relativamente alle forniture di beni, sistemi e servizi ICT da impiegare sulle reti, sui sistemi informativi e sui servizi informatici - individuati ai sensi della normativa Perimetro - dei rispettivi Ministeri.

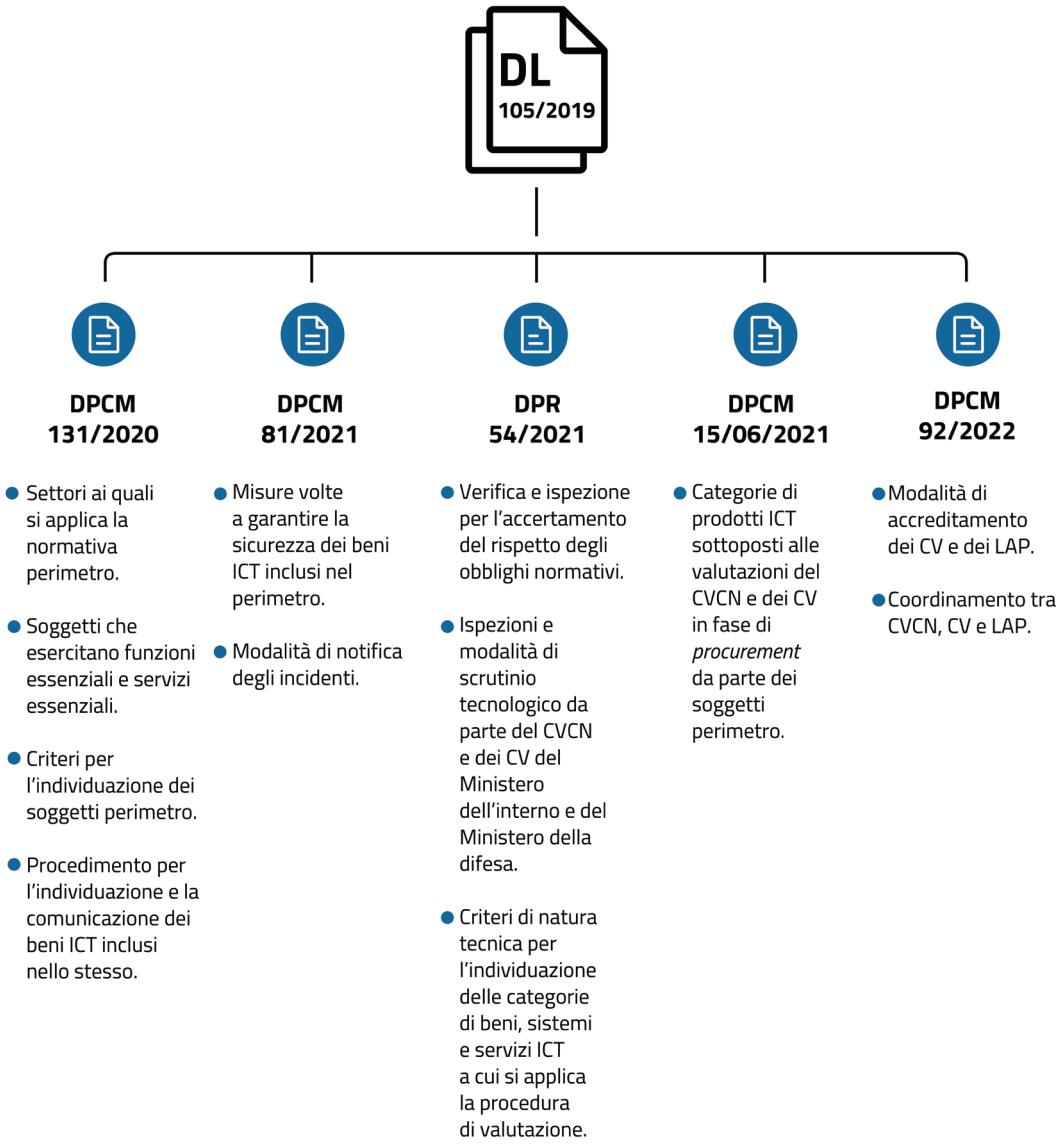


FIGURA 25 – LA NORMATIVA PERIMETRO

L'aggiornamento della normativa ha riguardato anche lo stesso D.L. Perimetro, relativamente alla estensione degli obblighi di notifica già previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica (c.d. beni ICT Perimetro). Nello specifico, l'obbligo è stato esteso agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro, ma che sono comunque di pertinenza di soggetti inclusi nello stesso. L'intervento normativo, che si è sostanziato nell'introduzione del comma 3-bis all'articolo 1 del D.L. n. 105 del 2019, è stato finalizzato a rafforzare il sistema di tutela della sicurezza nazionale nello spazio cibernetico e a consentire all'Agenzia di poter disporre di un quadro tecnico-situazionale aggiornato e completo sugli eventi in corso, così da favorire l'attività di *alerting* e prevenzione (vds. Cap. 4.6).

Con riferimento agli adempimenti in capo ai soggetti Perimetro, nel 2022 si sono succedute tre importanti scadenze legate agli obblighi imposti dalla normativa: due relative all'obbligo di trasmissione all'ACN dell'elenco dei beni ICT Perimetro, e una relativa all'adozione delle misure di sicurezza. I termini decorrono, per ciascun soggetto, a partire dalla data di notifica di iscrizione nell'elenco dei soggetti Perimetro.

A **giugno 2022** sono decorsi, pertanto, i termini[19] per la trasmissione dell'elenco aggiornato dei beni ICT Perimetro per i soggetti che hanno ricevuto la notifica di iscrizione nel 2020, nonché quelli[20] per l'adozione delle misure di sicurezza di categoria A (BOX 8), ivi inclusi quelli per la designazione degli incaricati e dei referenti tecnici. Al contempo, entro il medesimo termine, i soggetti che hanno ricevuto la notifica di iscrizione nel 2021, hanno condiviso con l'Agenzia le relative modalità di implementazione.

Box 8

LE MISURE DI SICUREZZA DEL PERIMETRO

Ai sensi del D.L. 105/2019 i soggetti iscritti nel Perimetro sono tenuti ad adottare misure di sicurezza a protezione dei propri beni ICT.

Le suddette misure sono contenute nell'allegato B al DPCM 81/2021 e sono suddivise in due categorie:

1. le misure di categoria A, di carattere più organizzativo e procedurale, richiedono principalmente l'adozione formale di processi e procedure. Queste devono essere adottate dai soggetti entro 6 mesi dalla trasmissione dell'elenco dei Beni ICT;
2. le misure di categoria B, prevedendo anche l'impiego di infrastrutture e soluzioni tecniche, risultano in generale di carattere più oneroso e, pertanto, la loro adozione è richiesta entro 30 mesi dalla trasmissione dell'elenco dei Beni ICT.

A **dicembre 2022** è, invece, decorso il termine per la trasmissione dell'elenco aggiornato dei beni ICT Perimetro per i soggetti che hanno ricevuto la notifica di iscrizione nel giugno 2021.
Al contempo, sono stati avviati i lavori preparatori per l'aggiornamento dell'elenco dei soggetti Perimetro e, più in generale, dell'impianto regolamentare, così come previsto dal D.L. n. 105/2019. Sono, inoltre, proseguite le attività di supporto ai soggetti coinvolti nell'attuazione delle relative disposizioni sia attraverso oltre 100 interlocuzioni dirette, sia mediante l'aggiornamento delle "FAQ PSNC", ovvero l'elaborato pubblicato sul portale ad accesso controllato dedicato di facile consultazione, a beneficio dei soggetti Perimetro, che raccoglie i riscontri ai quesiti emersi con maggiore frequenza nelle attività in oggetto, integrandovi, in particolare, gli aspetti inerenti all'avvio del CVCN.

[19] Previsti dal DPCM n. 131/2020.
[20] Previsti dal DPCM n. 81/2021.

4.2 Scrutinio tecnologico e certificazione di cybersicurezza

Le attività di scrutinio tecnologico di cybersicurezza sono fondamentali per il conseguimento dell'autonomia tecnologica riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Esse, peraltro, costituiscono una delle prime funzioni che il decreto-legge istitutivo dell'Agenzia attribuisce alla stessa.

Nel corso del 2022, l'Agenzia ha, quindi, profuso notevole impegno nello svolgimento delle attività propedeutiche al potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica, anche in attuazione del Piano di Implementazione della Strategia nazionale di cybersicurezza, che dedica specifiche misure a tale attività.

LAP

I **Laboratori Accreditati di Prova**-LAP sono strutture tecniche altamente specializzate, istituite presso soggetti pubblici e privati, che supportano il CVCN e i CV nelle attività di scrutinio tecnologico e test di sicurezza degli assetti ICT in uso presso i soggetti del PSNC.

Al riguardo, l'Agenzia ha attivato importanti, quanto eterogenee, iniziative che ruotano attorno all'avvio, a partire dal 30 giugno 2022 (in coerenza con quanto previsto dal D.L. n. 105/2019), del Centro di Valutazione e Certificazione Nazionale e all'adozione delle relative metodologie di valutazione della sicurezza, cui si aggiungono l'elaborazione delle aree di accreditamento e dei relativi requisiti tecnico-logistici e di competenza dei Laboratori Accreditati di Prova e il contributo alla definizione delle procedure per l'accreditamento dei Laboratori di Prova a supporto del CVCN e dei CV, adottate tramite il DPCM 18 maggio 2022, n. 92.
Un'altra linea di azione importante riguarda il reclutamento del personale tecnico, altamente specializzato, per le attività di scrutinio e valutazione di sicurezza di beni ICT conferiti al Perimetro, di cui si è già dato conto in apertura di Relazione (vds. Cap. 1.2)

4.2.1 Avvio del CVCN

Il Centro di Valutazione e Certificazione Nazionale (già istituito nel 2019 presso l'allora MiSE e trasferito all'ACN ai sensi del D.L. n. 82/2021) è un componente fondamentale dell'architettura nazionale di cybersicurezza e svolge un ruolo centrale ai fini dell'innalzamento dei livelli di cyber-resilienza del Paese.

Il CVCN, infatti, ai sensi dell'articolo 1, comma 6, lettera a), del D.L. 21 settembre 2019, n. 105, svolge una **valutazione preventiva** sui livelli di sicurezza degli *asset* ICT conferiti al Perimetro di sicurezza nazionale cibernetica e, dunque, impiegati da soggetti che svolgono una funzione essenziale dello Stato ovvero assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato.

Unitamente al trasferimento delle funzioni, sono state acquisite dall'ACN le dotazioni strumentali che hanno consentito di allestire i laboratori per eseguire test su *software* e apparati di rete, nonché un primo laboratorio di elettronica per i test su dispositivi *hardware*.

Il CVCN – attivo dal 30 giugno 2022, in concomitanza con l'avvio dell'obbligo, a carico dei soggetti Perimetro, di comunicare l'intenzione di acquisire tramite procedure di affidamento specifici beni ICT destinati agli *asset* Perimetro – si coordina con gli omologhi Centri di Valutazione-CV istituiti presso il Ministero della difesa e il Ministero dell'interno e accredita laboratori esterni (Laboratori Accreditati di Prova), ai quali può demandare l'esecuzione di test di sicurezza (Figura 26).

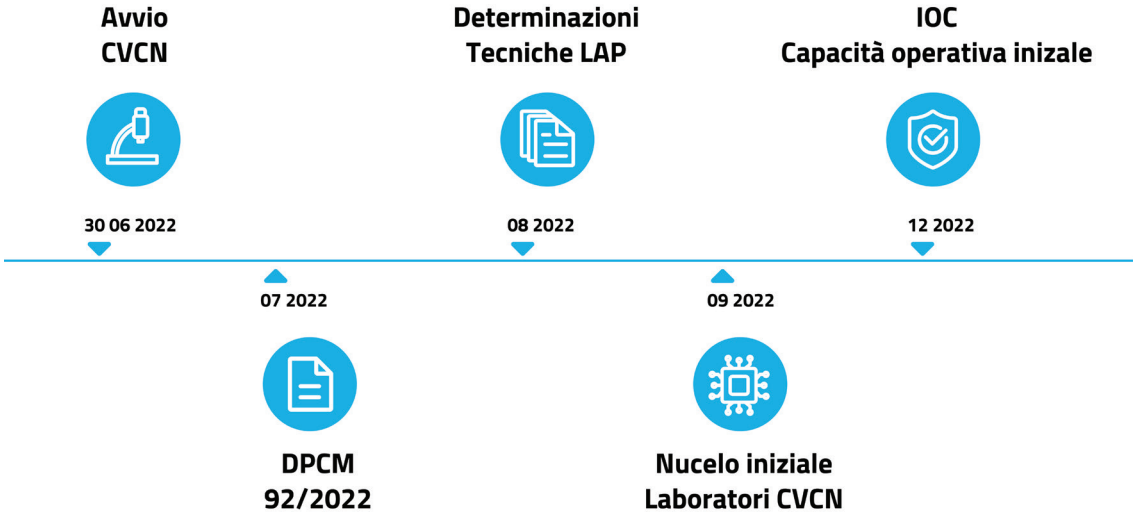


FIGURA 26 - *TIMELINE* AVVIO CVCN

Fin dal suo avvio, il CVCN ha fatto leva sulle unità di personale tecnico che hanno costituito il nucleo iniziale dell'ACN e su quelle trasferite dal MiSE. La dotazione di personale è stata ulteriormente potenziata con l'assunzione degli esperti che hanno superato le prove del concorso concluso nel primo semestre del 2022 (vds. Cap. 1.2). Questa prima fase di reclutamento dell'Agenzia ha avuto infatti come obiettivo prioritario proprio quello di assumere personale rientrante tra i profili destinati alle attività del CVCN (certificatori/ispettori, tecnici *hardware* e TLC, tecnici *software* e crittografi). L'ingresso del nuovo personale in Agenzia ha consentito al CVCN di raggiungere, già nel corso del mese di dicembre, la capacità operativa iniziale.

Nel corso del 2022 il CVCN ha operato secondo il principio di gradualità definito dal DPR 5 febbraio 2021, n. 54, affinando le proprie procedure interne, incrementando progressivamente le dotazioni strumentali e tecnologiche, e avviando progetti di potenziamento della rete dei LAP per mezzo dei fondi PNRR.

Il CVCN ha adottato le metodologie da impiegare nel processo di valutazione, come quella per la predisposizione dell'analisi del rischio, che i soggetti inclusi nel Perimetro devono adottare per redigere la documentazione da allegare alle comunicazioni di affidamento.

Nei primi 6 mesi di attività, il CVCN ha gestito **63 procedimenti** scaturiti da altrettante comunicazioni di affidamento da parte dei soggetti inclusi nel Perimetro (Figura 27).

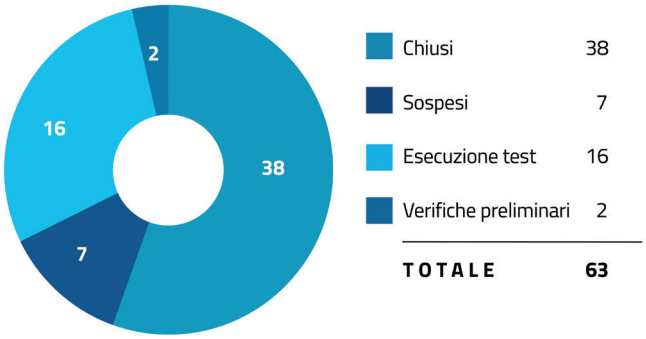


FIGURA 27 - STATISTICHE SULLO STATO DEI PROCEDIMENTI DEL CVCN AL 31 DICEMBRE 2022

La Figura 27 riporta una fotografia, a fine anno, dello stato dei procedimenti CVCN del 2022. In particolare, 38 procedimenti, pari al 60% del totale, sono stati chiusi autorizzando il Soggetto a proseguire con le procedure d'acquisizione di assetti ICT e la successiva installazione, fornendo però raccomandazioni di sicurezza di carattere tecnico; per 16 procedimenti il CVCN ha imposto l'esecuzione di test di sicurezza, attualmente in carico ai laboratori interni dell'Agenzia. Dei

restanti procedimenti, 2 risultavano ancora nella fase di verifiche preliminari, mentre 7 erano sospesi, in attesa di integrazione documentale.

Nel mese di luglio 2022, è stato pubblicato il DPCM 18 maggio 2022, n. 92, che definisce le modalità di accreditamento dei LAP e il raccordo tra il CVCN e i CV del Ministero dell'interno e del Ministero della difesa. Con la pubblicazione del decreto – alla cui elaborazione l'Agenzia ha fornito un importante contributo – è stata ammessa la possibilità, per enti pubblici e privati, di accreditarsi come LAP, dando di fatto avvio alla costituzione della rete a supporto dei Centri (CVCN e CV).

In attuazione del citato DPCM, inoltre, l'Agenzia ha elaborato le determinazioni tecniche – adottate mediante decreto del Direttore generale – che definiscono i requisiti tecnico-professionali e le competenze tecniche dei LAP, nonché le aree tecnologiche di accreditamento per cui possono specializzarsi nell'esecuzione di *test*.

Nel mese di ottobre 2022, al fine di potenziare la rete dei LAP tramite l'attivazione di nuovi laboratori, l'Agenzia ha pubblicato un avviso per l'erogazione di contributi nell'ambito del PNRR. L'avviso si è concluso a fine novembre e ha visto l'adesione dai **34 potenziali LAP**.

4.2.2 OCSI

Con l'adozione del DPCM 15 giugno 2022, che ha disciplinato il trasferimento di funzioni, beni strumentali e documentazione dall'allora MiSE all'ACN, sono transitate, con decorrenza 1° luglio 2022, anche le funzioni dell'Organismo di Certificazione della Sicurezza Informatica-OCSI – già operante ai sensi del DPCM 30 ottobre 2003 – che gestisce lo Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione. Tale schema certifica, in particolare, la sicurezza informatica di prodotti ICT in base allo *standard* ISO/IEC 15408, cd. *Common Criteria*, avvalendosi di una rete di laboratori nazionali ed esteri da esso accreditati.

Nell'ambito dello Schema Nazionale, i soggetti pubblici e/o privati possono sottoporre a certificazione di sicurezza prodotti e sistemi IT, che vengono valutati da laboratori competenti e indipendenti, accreditati da OCSI stesso, al fine di determinare il soddisfacimento di specifici requisiti di sicurezza nei limiti dei livelli di garanzia richiesti (*Evaluation Assurance Level*-EAL).

Al 31 dicembre 2022 sono **11** i **Laboratori per la Valutazione della Sicurezza (LVS)** accreditati dall'OCSI.

A seguito del citato passaggio di competenze, l'OCSI ha ereditato **11 processi di certificazione in corso**, già avviati presso il MiSE, cui si aggiungono ulteriori **8 procedimenti di certificazione** avviati nel corso del 2022 in ACN.

A settembre 2022, OCSI ha emesso **1 certificato** con livello di garanzia EAL5+ (su una scala che va da 1 a 7, così come definito nei *Common Criteria*) e ha concluso **4 valutazioni** approvando, a dicembre 2022, i Rapporti di Fine Valutazione emessi dai LVS coinvolti. I certificati per tali prodotti sono stati emessi nel primo trimestre del 2023.

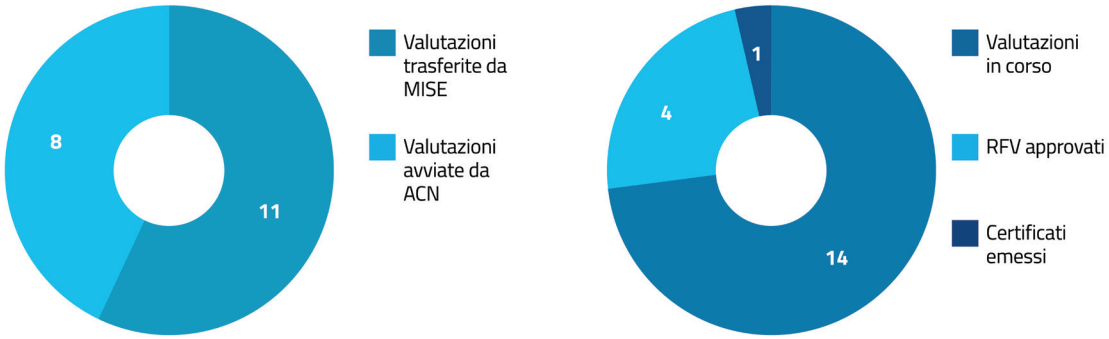


FIGURA 28 – CERTIFICAZIONI DI SICUREZZA SECONDO LO SCHEMA NAZIONALE

L' OCSI, nell'ambito dello Schema Nazionale, aderisce inoltre agli accordi di mutuo riconoscimento internazionale CCRA (*Common Criteria Recognition Arrangement*) ed europeo SOGIS-MRA (*Senior Officials Group Information Systems Security – Mutual Recognition Agreement*), con lo scopo di riconoscere certificati afferenti a tutti gli Schemi internazionali aderenti ai suddetti accordi di mutuo riconoscimento.

SOGIS
Senior Officials Group
Information Systems Security

In particolare, in ambito internazionale l'OCSI ha partecipato, nel corso del 2022, alle riunioni del CCRA tenutesi a Toledo, ricoprendo il ruolo di *chairman* del *Common Criteria Development Board* (CCDB), e agli incontri del SOGIS di Berlino di ottobre 2022. In particolare, nell'ambito delle

attività di coordinamento del CCDB, l'OCSI ha assicurato la preparazione della nuova versione dello standard CC:2022 e CEM:2022 e la sua successiva adozione da parte del CCRA all'incontro di Toledo.

L'OCSI è anche l'organo designato dal Regolamento (UE) n. 910/2014 sull'identità digitale (*electronic IDentification, Authentication and Signature*-eIDAS), nonché ente responsabile in Italia per l'accertamento della conformità di un dispositivo per la creazione di una firma elettronica qualificata o di un sigillo elettronico qualificato, conformemente ai requisiti di sicurezza espressi nell'Allegato II al suddetto regolamento.

4.3 Contributo dell'ACN nelle procedure in materia di "Golden Power"

Tra le funzioni acquisite dall'Agenzia, si evidenzia inoltre la partecipazione al Gruppo di coordinamento che cura le istruttorie per l'esercizio dei poteri speciali del Governo, di cui al decreto-legge 15 marzo 2012, n. 21 (cd. D.L. *Golden Power*). L'Agenzia partecipa per gli aspetti di propria competenza che comprendono, oltre alle notifiche in materia di reti 5G, quelle riguardanti, più in generale, operazioni societarie che impattano su attivi[21] strategici in ambito ICT e di cybersicurezza.

Golden Power

Potere speciale che consente al Governo di imporre condizioni e prescrizioni o apporre il veto ad operazioni societarie con impatto su attivi strategici e ad acquisizioni di tecnologia 5G.

In particolare, nel corso del 2022 ACN ha fornito supporto tecnico nella fase istruttoria di **64 notifiche *Golden Power***, di cui **16 relative a tecnologia 5G**.

Con riferimento alla tecnologia 5G, va evidenziato come, a seguito dell'adozione del "D.L. Ucraina" (decreto-legge n. 21/2022) che ha modificato l'art. 1-bis al D.L. *Golden Power* (vds. par. 4.6), la disciplina dei poteri speciali inerenti ai servizi di comunicazione elettronica a banda larga con tecnologia 5G, basati sulla tecnologia *cloud* e altri attivi sia stata fortemente innovata. L'oggetto delle notifiche, infatti, riguarda ora **piani annuali di sviluppo**, piuttosto che singole

[21] Ai sensi della normativa di settore si fa riferimento a servizi, beni, rapporti, attività e tecnologie.

acquisizioni di componenti specifici, con la conseguenza che, ad un ridotto numero di notifiche, fa ora da contraltare una maggiore complessità delle stesse.

Per quanto riguarda le notifiche relative ad altri settori tecnologici, l'ACN viene ingaggiata prevalentemente nei casi che riguardano beni e rapporti nei settori della cybersicurezza, del trattamento dei dati con piattaforme ICT e, in generale, delle tecnologie digitali.

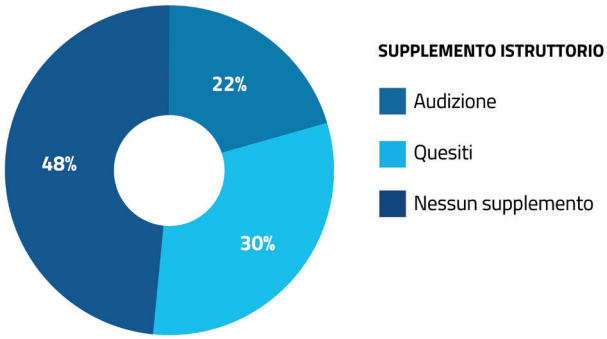


FIGURA 29 – PROCESSI ISTRUTTORI E RELATIVI SUPPLEMENTI

A dimostrazione della complessità dei casi trattati con il supporto tecnico dell'ACN, si noti che in oltre la metà dei casi trattati è stato necessario un supplemento istruttorio, tramite l'invio di quesiti o l'audizione dei soggetti notificanti e/o di terze parti (Figura 29).

Con riferimento ai casi trattati dall'ACN, in **7 occasioni** il Governo ha esercitato i poteri speciali nella forma di **prescrizioni**, che l'ACN ha contribuito a redigere, per gli aspetti di propria competenza, insieme all'amministrazione referente e alle altre amministrazioni del Gruppo di coordinamento, mentre in **un caso** è stato esercitato il potere di **veto**.

Oltre al contributo tecnico assicurato in sede istruttoria tramite la propria partecipazione al Gruppo di coordinamento, l'Agenzia è impegnata nelle attività del Comitato di monitoraggio, istituito per vigilare sull'ottemperanza alle prescrizioni imposte nei casi di esercizio dei poteri speciali nel settore delle reti 5G.

In tal senso, l'ACN fornisce supporto nell'analisi delle relazioni di ottemperanza periodicamente inoltrate dagli operatori del settore delle telecomunicazioni.

In particolare, su attivazione del Comitato di monitoraggio, l'Agenzia ha prodotto, nel mese di marzo 2022, un rapporto sulle relazioni di ottemperanza ricevute nel tempo, analizzando un totale di **98 relazioni**. Tale studio ha consentito di identificare le prescrizioni-tipo incluse nei provvedimenti di esercizio dei poteri speciali e di classificarle per livello di attuazione e impatto.

4.4 Attivazione dell'Organo ispettivo e di vigilanza

Nel mese di ottobre 2022, in seno all'ACN è stato istituito l'Organo ispettivo e di vigilanza con il compito di svolgere attività di verifica tecnico-documentale e ispezione, concernenti gli adempimenti di cybersicurezza attribuiti all'Agenzia dalla normativa vigente, nei confronti dei soggetti pubblici e privati. L'Organo rappresenta, di fatto, l'Unità Centrale Ispettiva che è una delle *milestone* previste dal PNRR (vds. cap. 5).

All'articolazione è stato assegnato personale proveniente da altre amministrazioni dello Stato, oltre alle unità selezionate tramite concorso pubblico.
In tale contesto, l'Organo ispettivo e di vigilanza ha predisposto e formalizzato un sistema di gestione della qualità in conformità alla norma relativa agli Organismi di Ispezione (UNI CEI EN ISO/IEC 17020), al fine, anzitutto, di stabilire una struttura logica e coerente per tutte le procedure, le istruzioni operative, i modelli, i registri e le liste di riscontro che consentano una gestione, sia documentale che operativa, efficace ed efficiente. L'adozione di un sistema strutturato di gestione della qualità è, inoltre, garanzia di imparzialità, indipendenza e riservatezza rispetto alle attività ispettive, nonché di miglioramento continuo dei processi.

Il sistema di gestione è articolato nei seguenti tre livelli:

1. il primo livello è costituito dal **manuale di qualità**, che descrive il sistema di gestione della qualità l'Organo ispettivo e di vigilanza, e dal **modello di erogazione dei servizi**;
2. il secondo livello racchiude **documenti di carattere generale** (procedure, istruzioni operative, modelli e registri) comuni alle varie tipologie di attività erogate;
3. il terzo livello comprende i **documenti specifici** per i vari contesti nei quali opera l'Organo, tra cui quelli relativi all'accreditamento dei Laboratori Accreditati di Prova (LAP) in ambito CVCN e dei laboratori di valutazione della sicurezza (LVS) in ambito OCSI, nonché quelli relativi alla verifica dell'implementazione delle misure di sicurezza in ambito PSNC e NIS.

L'Organo ha, inoltre, definito un primo insieme di processi e strumenti per la conduzione delle attività di verifica e ispezione, dei procedimenti di accreditamento dei laboratori di prova, nonché per le verifiche delle misure di sicurezza relative al PSNC.

4.5 Sicurezza delle reti in attuazione della normativa europea

A dicembre 2020, in concomitanza con l'adozione della "Strategia dell'Unione europea in materia di cybersicurezza per il decennio digitale" volta a rafforzare la resilienza collettiva dell'UE contro le minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili, la Commissione ha presentato la proposta di Direttiva recante misure per un livello comune elevato di cybersicurezza nell'Unione (cd. **NIS2**).

Con riferimento alle fasi negoziali e all'adozione della Direttiva NIS2, l'ACN ha garantito un'assidua partecipazione ai lavori in sede europea al fianco del MAECI, al fine di rappresentare le istanze nazionali in un'ottica di costante dialogo tra la dimensione europea e nazionale della sicurezza cibernetica, anche attraverso il raccordo, in sede bilaterale, con altri Stati membri.

La Direttiva NIS2, che ha abrogato la Direttiva UE 2016/1148, intende garantire un livello di sicurezza cibernetica comune più elevato grazie all'armonizzazione delle norme applicabili ai diversi operatori negli Stati membri e al rafforzamento dei livelli *standard* di sicurezza rispetto a quelli previsti dalla disciplina vigente. Ciò incidendo, in via prioritaria, sulla capacità degli Stati membri in termini di architettura istituzionale, strategia nazionale e piani di gestione delle crisi cibernetiche, ma anche, a livello più operativo, sulla gestione del rischio da parte degli operatori, con misure di sicurezza adeguate e un sistema di notifica di incidenti efficace e reattivo e sulla cooperazione e condivisione di informazioni, attraverso diverse modalità di scambio, a livello europeo e nazionale.

Il negoziato della Direttiva NIS2 si è svolto in parallelo a quello del Regolamento europeo sulla resilienza operativa digitale per il settore finanziario (***Digital Operational Resilience Act*-DORA**), nonché alla Direttiva sulla resilienza dei soggetti critici (***Critical Entities Resilience***).

La contiguità applicativa di tali norme UE ha richiesto un intenso coordinamento interministeriale al fine di garantire dei testi complementari e armonici. A testimonianza del forte raccordo tra gli stessi, tutti i richiamati atti, compresa la direttiva NIS 2, sono stati pubblicati nella medesima

edizione della Gazzetta ufficiale dell'Unione europea (L 333 del 27 dicembre 2022).

I prossimi anni vedranno una intensa attività di tutte le amministrazioni impattate dagli effetti della NIS 2, non solo in relazione al recepimento della stessa, il cui termine è fissato per **ottobre 2024**, ma anche per il necessario coordinamento nell'applicazione dei tre importanti atti normativi unionali.

Con il più volte citato DPCM 15 giugno 2022, relativo al trasferimento di funzioni dall'allora MiSE all'ACN, viene, altresì, perfezionato il passaggio di competenze all'ACN, quale autorità competente NIS per il settore delle infrastrutture digitali e per i fornitori di servizi digitali (FSD), di cui al D.Lgs. n. 65/2018 (cd. decreto NIS), nonché le competenze in materia di sicurezza delle reti e dei servizi di comunicazione elettronica, ai sensi del D.Lgs. n. 207/2021 (provvedimento con cui è stato recepito il nuovo Codice europeo delle comunicazioni elettroniche-Direttiva 2018/1972[22]). Conseguentemente, l'ACN è subentrata all'allora MiSE nei relativi tavoli europei quale rappresentante nazionale (*Work Stream on Digital Service Providers* e il *Work Stream on Digital Infrastructures*, partecipando a 2 riunioni nelle quali sono stati approfonditi aspetti relativi all'applicazione della direttiva NIS e della direttiva NIS2 nel settore delle infrastrutture digitali e agli FSD). Analogamente, l'ACN ha partecipato a 2 riunioni – a giugno, affiancando il MiSE in vista dell'avvicendamento, e a ottobre – del gruppo di esperti *European Competent Authorities for Secure Electronic Communication*. Inoltre, al fine di promuovere il rapido inserimento dell'ACN nella comunità unionale attinente al settore Telco, è stata assicurata la partecipazione alla seconda edizione dell'ENISA *Telecom Security Forum* (giugno).

[22] E con il quale è stata aggiornata la materia, intervenendo in maniera sostanziale sul D.Lgs. n. 259/2003, redistribuendo, in considerazione delle funzioni attribuite all'ACN, i compiti relativi alla sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche.

Box 9

LA DIRETTIVA (UE) 2022/2555

Il processo co-legislativo europeo ha visto il Parlamento europeo adottare la propria relazione sulla proposta della Commissione il 22 novembre 2021, seguito dal cd. *general agreement* del Consiglio il 3 dicembre 2021.
Esaurita la fase più dinamica del negoziato con il raggiungimento del citato *general agreement* in Consiglio UE nel corso del 2021, il *core* delle attività, nel 2022, ha riguardato il raggiungimento di una posizione condivisa tra Parlamento, Consiglio e Commissione. In tale fase, la dialettica si è principalmente sviluppata sui temi della proporzionalità delle misure di sicurezza in relazione al rischio a cui i destinatari delle disposizioni sono esposti, delle modalità di inclusione della Pubblica Amministrazione nell'ambito di applicazione della direttiva, nonché dell'affinamento dell'innovativo impianto relativo alla gestione delle crisi *cyber*.
Infine, all'esito dell'accordo politico raggiunto il 13 maggio 2022 in fase di trilogo, nonché a valle di ulteriori affinamenti di carattere tecnico-giuridico-linguistico, la Direttiva (UE) 2022/2555, cd. NIS2, è stata approvata il successivo 14 dicembre e pubblicata nella Gazzetta Ufficiale dell'Unione Europea L 333 del 27 dicembre 2022.

In particolare, il nuovo impianto supera e rafforza quanto già previsto dalla precedente Direttiva 2016/1148, facendo tesoro dell'esperienza acquisita nella sua applicazione, in relazione ai seguenti ambiti:

1. **revisione del meccanismo di identificazione dei soggetti** quali entità importanti o essenziali, per mezzo di un **criterio** omogeneo di identificazione dei soggetti **basato sulla dimensione** (cd. *size-cap rule*), che estende l'applicazione della direttiva a tutte le medie e grandi imprese che operano nei settori identificati. Ciò al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri;
2. **allargamento dell'ambito di applicazione**, con un aumento significativo dei settori di applicazione e l'introduzione di un approccio "*all-hazards*" alla cybersicurezza, con l'inclusione di profili di sicurezza fisica delle infrastrutture ICT;
3. **rafforzamento dei poteri di supervisione**, con indicazioni più dettagliate per la definizione delle misure di sicurezza e l'inasprimento delle sanzioni;
4. **estensione delle funzioni dei CSIRT nazionali**, che fungeranno, tra l'altro, da intermediari di fiducia tra i soggetti segnalanti e i fornitori di prodotti e servizi ICT nell'ambito del quadro per la divulgazione coordinata delle vulnerabilità;
5. **gestione delle crisi**, con la previsione di quadri nazionali in materia e l'istituzionalizzazione di EU-CyCLONe (vds. Cap. 3.4.2 e Cap. 7.2), per la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala.

4.6 Interventi normativi in materia di resilienza cibernetica

Tra le attività poste in essere dall'ACN nell'ottica del rafforzamento della sicurezza e della resilienza cibernetiche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, anche alla luce dell'attuale scenario internazionale, si segnalano alcuni interventi normativi di particolare rilievo.

Attività legate alla situazione in Ucraina. Circolare sulla diversificazione. Con l'**articolo 29 del decreto-legge n. 21 del 2022, c.d. D.L. Ucraina-*bis***, il legislatore ha introdotto talune disposizioni volte a rafforzare la sicurezza cibernetica. L'evoluzione della situazione internazionale e del contesto geopolitico, infatti, ha richiesto di valutare il rischio tecnologico derivante da prodotti e servizi di sicurezza informatica che, per loro caratteristiche intrinseche e a prescindere dagli elevati

livelli prestazionali, possono costituire un vettore di minaccia. È stato, quindi, previsto che le Pubbliche Amministrazioni, al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi, provvedano alla diversificazione dei prodotti informatici e dei servizi di sicurezza in uso, allorché tali prodotti e servizi siano erogati da aziende produttrici legate alla Federazione Russa. Ciò anche al fine di prevenire possibili pregiudizi per la sicurezza nazionale nello spazio cibernetico. L'individuazione delle categorie di prodotti e servizi da diversificare e delle relative aziende produttrici o fornitrici, è stata demandata ad una circolare dell'Agenzia. In attuazione di tali disposizioni, è stata adottata, anche tenendo conto delle indicazioni del Nucleo per la cybersicurezza, la circolare 21 aprile 2022, n. prot. 4336. Nell'ambito della predetta circolare dell'ACN, sono state, altresì, dettate disposizioni per la semplificazione delle procedure di acquisto di altri prodotti o servizi di sicurezza informatica e raccomandazioni per l'adozione di tutte le misure e le buone prassi.

Perimetro di sicurezza nazionale cibernetica (PSNC). Il **richiamato articolo 29, al comma 5, introduce una modifica all'articolo 5 del D.L. Perimetro** in materia di determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica. Tale ultima disposizione prevede che il Presidente del Consiglio – su deliberazione del Comitato interministeriale per la sicurezza della Repubblica – in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati. In particolare, la modifica è volta a precisare che le determinazioni del Presidente del Consiglio dei ministri in parola, possono essere adottate in deroga alle disposizioni vigenti, nel rispetto dei princìpi generali dell'ordinamento giuridico; in tali ipotesi le relative determinazioni in deroga devono contenere l'indicazione delle principali norme a cui si intende derogare e la specifica motivazione. Tali provvedimenti presidenziali, anche in ragione dell'urgenza di tutelare la sicurezza nazionale, non sono soggetti al controllo preventivo di legittimità. Alla luce dell'acuirsi della crisi russo-ucraina, l'intervento normativo si è reso necessario per una duplice finalità: consentire al Presidente del Consiglio dei ministri di poter disporre, oltre che la disattivazione totale o parziale di determinati apparati o prodotti, anche eventuali ulteriori misure necessarie e connesse (ad es. al fine di garantire la continuità dei servizi); permettere l'adozione di provvedimenti più efficaci, attribuendo anche il potere di andare in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico.

Sempre in materia di PSNC, si segnalano le disposizioni di cui all'**articolo 37-*quater* del decreto-legge n. 115 del 2022**, c.d. D.L. Aiuti-bis. Con emendamento presentato al disegno di legge di

conversione del predetto D.L. n. 115 del 2022, è stato introdotto il comma 3-*bis* all'articolo 1 del D.L. Perimetro che dispone l'estensione degli obblighi di notifica attualmente previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica (c.d. beni ICT), agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (diversi quindi dai beni ICT), ma che sono comunque di pertinenza di soggetti inclusi nel medesimo.

L'intervento normativo in parola è finalizzato a rafforzare il sistema di tutela della sicurezza nazionale nello spazio cibernetico posto in essere dal Perimetro di sicurezza nazionale cibernetica e ad avere un quadro tecnico-situazionale aggiornato e completo sugli eventi in corso, anche al fine di prevenire possibili conseguenti impatti sui beni tecnologici rilevanti inseriti nel Perimetro. La disposizione introdotta prevede, inoltre, che, con determinazioni tecniche del Direttore generale dell'Agenzia per la cybersicurezza nazionale, venga indicata la tipologia degli incidenti di cui al nuovo comma 3-*bis* dell'articolo 1 del D.L. Perimetro e possano essere dettate specifiche modalità di notifica. In attuazione di tale disposizione è stata adottata la Determina 3 gennaio 2023, recante "Tassonomia degli incidenti che debbono essere oggetto di notifica".

Disciplina sull'esercizio poteri speciali del Governo. L' **articolo 28 del decreto-legge n. 21 del 2022, c.d. D.L. Ucraina-*bis***, ha sostituito interamente l'**art. 1-*bis*** del decreto-legge n. 21 del 2012, al fine di prevedere la ridefinizione dei poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G e *cloud*. In particolare, quanto all'ambito di applicazione oggettivo della disposizione in parola, il nuovo comma 1 dell'articolo 1-*bis*, nel confermare che i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G costituiscono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, ai fini dell'esercizio dei poteri speciali, consente, inoltre, di individuare ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia *cloud*, con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con i Ministri competenti, e sentita l'Agenzia per la cybersicurezza nazionale. Inoltre, è stato stabilito che il Gruppo di coordinamento in materia includa, tra gli altri, rappresentanti dell'Agenzia e che si possa avvalere anche del CVCN, per le valutazioni tecniche della documentazione relativa al piano annuale e ai suoi eventuali aggiornamenti, propedeutiche all'esercizio dei poteri speciali e relative ai beni e alle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività rilevanti, nonché ad altri possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi. È stato, altresì, previsto che l'Agenzia partecipi al Comitato di monitoraggio per le attività tese alla verifica dell'osservanza delle prescrizioni e delle condizioni

impartite con il provvedimento dei poteri speciali, e che per tali attività di monitoraggio il comitato si avvale anche del CVCN.

Decreto-legge 27 gennaio 2022, n. 4, recante misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico. L'articolo 21 del provvedimento, in materia di fascicolo sanitario elettronico e governo della sanità digitale, prevede che, al fine di garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale, il Ministero della salute, d'intesa con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, assicurando l'adeguatezza delle infrastrutture tecnologiche e la sicurezza cibernetica in raccordo con l'Agenzia per la cybersicurezza nazionale, curi la realizzazione dell'Ecosistema Dati Sanitari (EDS), i cui contenuti, le modalità di alimentazione, nonché i soggetti che vi hanno accesso, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati, sono individuati con decreto del medesimo Ministro della salute, adottato di concerto con il Ministro delegato per l'innovazione tecnologica e la transizione digitale e con il Ministero dell'economia e delle finanze, e acquisiti i pareri dell'Autorità garante per la protezione dei dati personali e dell'Agenzia per la cybersicurezza nazionale.

05.

RAFFORZAMENTO DELLA RESILIENZA CYBER DELLE PUBBLICHE AMMINISTRAZIONI

Come già più volte illustrato, l'Agenzia è stata individuata quale soggetto attuatore dell'Investimento 1.5, stipulando, a tal fine, un accordo di collaborazione con il Dipartimento per la trasformazione digitale (DTD) della Presidenza del Consiglio dei ministri.

L'Investimento 1.5 "*Cybersecurity*" della Missione 1 – Componente 1 – Asse 1 del PNRR, con una dotazione di 623 milioni di euro, ha come fulcro il **rafforzamento dell'ecosistema digitale nazionale**, il relativo **potenziamento dei servizi di gestione della minaccia *cyber* e lo sviluppo dell'autonomia tecnologica nazionale**, nonché il **supporto all'avvio e all'incremento delle capacità dell'ACN.**

In particolare, l'Investimento 1.5 mira ad incrementare il livello di maturità della Pubblica Amministrazione in termini di postura di sicurezza secondo i requisiti del Perimetro di sicurezza nazionale cibernetica (PSNC) e dei più recenti orientamenti normativi nazionali e dell'Unione europea.

Pertanto, in qualità di Soggetto Attuatore dell'investimento in parola, l'Agenzia è stata impegnata, nel 2022, a coordinare le iniziative che hanno contribuito a raggiungere con successo le *milestone* e i *target* PNRR per l'anno di riferimento (Figura 30). In tale contesto, si inseriscono le azioni intraprese nel corso del 2022 dall'Agenzia, volte al supporto dei soggetti pubblici nella realizzazione di interventi di potenziamento della postura di sicurezza.

T4 2022	M1C1-05	Attivazione dell'Agenzia per la cybersicurezza nazionale
	M1C1-06	Dispiego **iniziale** dei **servizi *cyber* nazionali**
	M1C1-08	Attivazione di un'**unità centrale di ispezione** per le misure di sicurezza PSNC e NIS
T4 2024	M1C1-20	Dispiego **integrale** dei servizi ***cyber* nazionali**
	M1C1-22	Esecuzione di almeno **30 ispezioni** per le misure di sicurezza PSNC e NIS
T4 2022	M1C1-09	Potenziamento delle capacità *cyber*: realizzazione di almeno **5 interventi di potenziamento** *cyber* per le PP.AA.
T4 2024	M1C1-19	Potenziamento delle capacità *cyber*: realizzazione di almeno **50 interventi di potenziamento** *cyber* per le PP.AA.
T4 2022	M1C1-07	Attivazione di almeno **1 laboratorio** di scrutinio tecnologico e certificazione
T4 2024	M1C1-21	Attivazione di almeno **10 laboratori** di scrutinio tecnologico e certificazione, del **CVCN** e dei **Centri di Valutazione di Interno e Difesa**

FIGURA 30 – *MILESTONE* E *TARGET* PNRR M1C1|1.5

5.1 Strategie di finanziamento per la *cyber* resilienza della PA

Per raggiungere gli scopi previsti dal PNRR, finanziati con l'Investimento più volte citato, l'Agenzia ha adottato una metodologia di coinvolgimento "multilivello" di tutti i principali attori nazionali, pubblici e privati, del mondo della *cybersecurity*. Ciò al fine di assicurare lo sviluppo di adeguati livelli di sicurezza per i dati e i servizi dei cittadini e, in tal modo, irrobustire le infrastrutture e i servizi digitali, nonché le competenze specialistiche necessarie a garantire elevati livelli di *cyber*-resilienza per il sistema-Paese.

Le azioni realizzate dall'Agenzia hanno riguardato sia le attività trasversali relative alla *governance* dell'Investimento, sia quelle concernenti la programmazione, l'attuazione e il controllo dei progetti, ponendo in essere, in qualità di Soggetto Attuatore dell'Investimento, anche tutte le attività propedeutiche[23].

La modalità di attuazione degli interventi è stata di volta in volta articolata sulla base della distinzione tra operazioni **"a titolarità"** e **"a regia"** In particolare:

- gli interventi **"a titolarità"** prevedono una modalità di attuazione diretta degli interventi da parte dell'Amministrazione centrale titolare di interventi PNRR, o suo delegato, facendo ricorso all'impiego delle proprie strutture amministrative all'uopo preposte, e operando direttamente in veste di Soggetto Attuatore del progetto incluso all'interno dell'Investimento. Nella fattispecie, quindi, l'Agenzia è responsabile degli adempimenti amministrativi connessi alla realizzazione dei progetti, nonché di quelli propedeutici e consequenziali connessi alla gestione, monitoraggio, controllo amministrativo e rendicontazione delle spese sostenute durante le fasi di attuazione (rientra in tale fattispecie l'Avviso Pubblico 2/2022, di cui si dirà oltre);
- gli interventi **"a regia"** fanno riferimento ai progetti di competenza di altri organismi pubblici, selezionati dall'Amministrazione centrale titolare di interventi PNRR, o suo delegato, secondo le modalità e gli strumenti amministrativi ritenuti più idonei dall'Amministrazione stessa, in base alle caratteristiche dell'intervento da realizzare e in linea con quanto indicato all'interno del PNRR. In tale ambito, l'Agenzia ha scelto questa tipologia di attuazione, di tipo indiretto, ricorrendo alle seguenti modalità di selezione:

  a) espletamento di procedure di selezione tramite Avviso Pubblico a ristoro finalizzato

[23] Si menzionano, tra gli altri, il rispetto del principio di sana gestione finanziaria (in particolare in materia di prevenzione dei conflitti di interessi, delle frodi, della corruzione e recupero dei fondi indebitamente assegnati) e il rispetto della normativa nazionale ed europea afferente agli aiuti di stato.

alla concessione di sovvenzioni, contributi, sussidi, ausili finanziari e l'attribuzione di vantaggi economici di qualunque genere, subordinata alla predeterminazione dei criteri e delle modalità cui i destinatari degli interventi devono attenersi[24]. L'individuazione dei progetti da finanziare è avvenuta, in tale ambito, mediante lo svolgimento di procedure ad evidenza pubblica di tipo:

i. **valutativa con graduatoria**, definita sulla base di appositi criteri per l'attribuzione dei relativi punteggi di merito, e sulla base della quale sono finanziati i progetti fino ad esaurimento delle risorse disponibili (rientrano in tale fattispecie l'Avviso Pubblico 1/2022 e l'Avviso Pubblico 3/2022, di cui si dirà oltre);

ii. **a sportello**, in base alla quale vengono ammesse tutte le proposte progettuali conformi ai requisiti minimi di partecipazione e individuate quelle da finanziare secondo l'ordine cronologico di presentazione delle istanze e fino al raggiungimento di eventuali valori soglia e/o ad esaurimento delle risorse disponibili (rientra in tale fattispecie l'Avviso Pubblico 4/2022, di cui si dirà oltre);

b) adozione di Accordi tra Pubbliche Amministrazioni: si tratta di accordi stipulati tra Pubbliche Amministrazioni in virtù della possibilità conferita all'Agenzia, in qualità di Soggetto Attuatore dell'Investimento 1.5, di coinvolgere altre Pubbliche Amministrazioni e/o enti pubblici per il raggiungimento delle *milestone* e dei *target* associati alla misura di riferimento. Si fa riferimento, in particolare, alle c.d. progettualità *cyber-defence*, per le quali, grazie a specifici accordi, sono state individuate le seguenti Amministrazioni attuatrici: Ministero dell'interno, Ministero della giustizia, Ministero della difesa, Arma dei Carabinieri, Guardia di Finanza e Consiglio di Stato.

La complessità dei sopra descritti programmi di investimento ha richiesto un notevole sforzo in termini di analisi, segnatamente con riguardo agli aspetti concernenti la validità tecnica e la tenuta economica e finanziaria delle proposte ricevute (ad esempio quanto alla coerenza delle proposte ricevute, al piano finanziario di copertura delle spese, ai flussi finanziari, agli obiettivi da raggiungere, ecc.).

Di seguito, la Figura 31 mostra l'elencazione degli Avvisi Pubblici conclusi al 31 dicembre 2022, per i quali l'Agenzia ha svolto l'intera attività di *governance* dell'Investimento, nonché quella legata alla loro programmazione e attuazione.

[24] Procedura consentita dall'art. 12 della Legge n. 241/1990 e declinata, in particolare, dalla Circolare del Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria generale dello Stato - Servizio centrale per il PNRR 14 ottobre 2021, n. 21, recante "Piano Nazionale di Ripresa e Resilienza – Trasmissione alle Amministrazione centrali dello Stato delle Istruzioni tecniche per la selezione dei progetti PNRR", nonché dalle linee guida dell'Amministrazione centrale titolare.

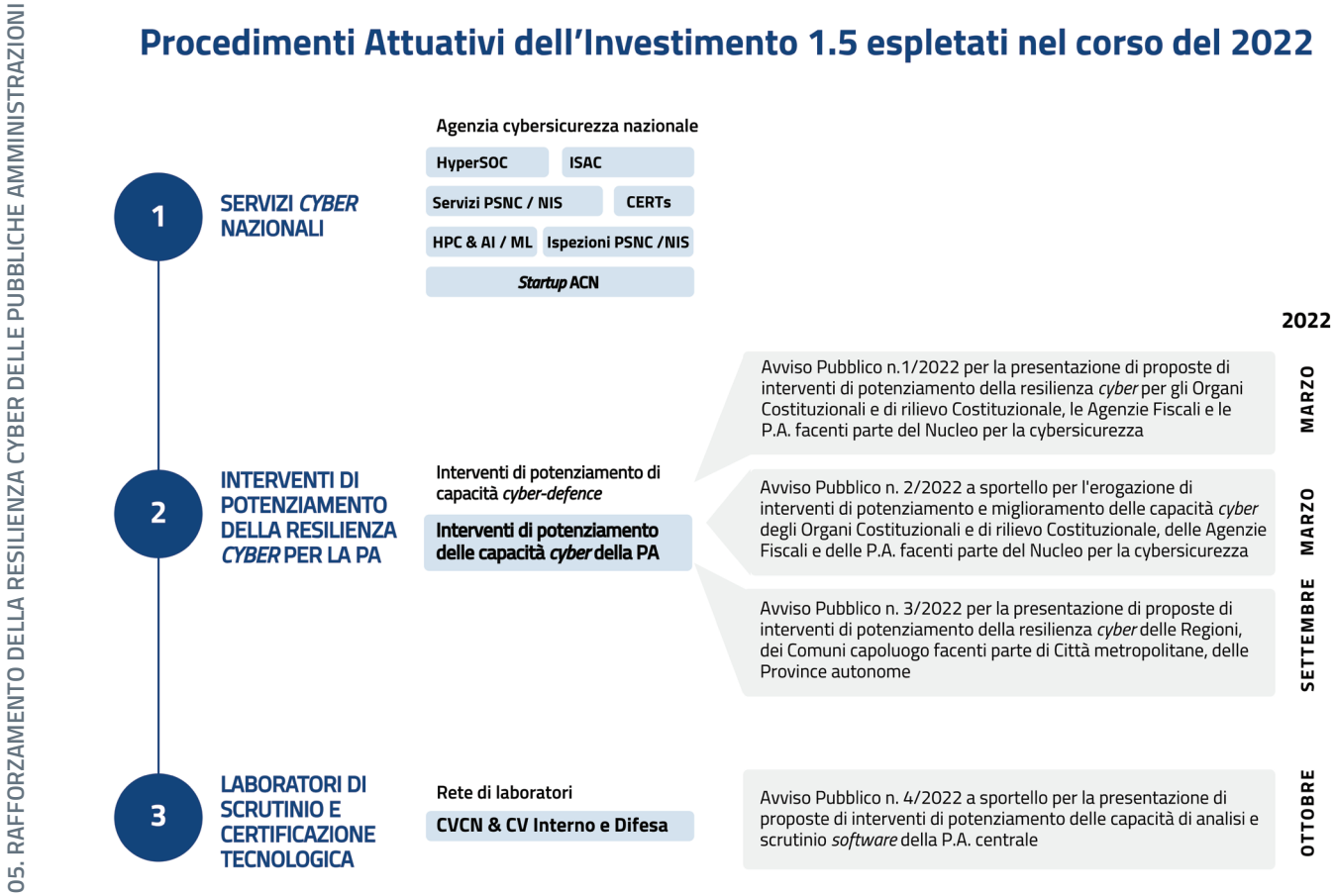


FIGURA 31 – PROCEDIMENTI ATTUATIVI DELL'INVESTIMENTO 1.5 ESPLETATI NEL CORSO DEL 2022

Nella Figura 32 sono sinteticamente rappresentate le fasi procedurali, dando evidenza degli *output* tecnici e amministrativi realizzati dall'Agenzia in qualità di Soggetto Attuatore dell'Investimento.

FIGURA 32 – PROCESSO DI *GOVERNANCE* AMMINISTRATIVA PER I DISPOSITIVI AD EVIDENZA PUBBLICA ESPLETATI NEL CORSO DEL 2022 PNRR M1C1|1.5

Allo scopo di accompagnare i Soggetti interessati agli interventi verso una corretta attuazione dei progetti, l'Agenzia ha realizzato due Manuali Operativi-Linee Guida, rispettivamente a beneficio delle Amministrazioni interessate agli accordi *cyber-defence* e a supporto dei soggetti individuati tramite avvisi pubblici[25].

[25] In linea con i dispositivi di attuazione e le Linee guida, disposizioni e indirizzi dell'Amministrazione centrale titolare e Unità di Missione (DTD).

Tale manualistica offre ai rispettivi destinatari a finanziamento indirizzi e strumenti operativi finalizzati a svolgere i necessari adempimenti di gestione, monitoraggio e controllo, fino alla rendicontazione delle spese e al raggiungimento degli obiettivi intermedi e finali, in linea con le decisioni e gli orientamenti provenienti dagli Organi dell'Unione Europea, dal MEF, e dall'Unità di Missione del PNRR del DTD.

Da un punto di vista funzionale, l'Agenzia ha adottato un modello organizzativo interno che vede articolazioni e risorse specificamente dedicate allo svolgimento dei compiti di monitoraggio e controllo delle attività concernenti l'Investimento 1.5.

5.2 Iniziative e obiettivi raggiunti

Al fine di individuare i Soggetti pubblici interessati alle progettualità riguardanti la realizzazione di interventi di potenziamento della resilienza *cyber*, l'Agenzia ha ritenuto opportuno procedere progressivamente coinvolgendo dapprima gli Organi costituzionali, a rilevanza costituzionale e le Pubbliche Amministrazioni Centrali (PAC) e successivamente le Pubbliche Amministrazioni Locali, ampliandone gradualmente il relativo perimetro, come di seguito illustrato.

Riassumendo, nel corso del 2022, l'Agenzia ha gestito complessivamente:

- **6 accordi** che hanno determinato l'avvio di progettualità volte al potenziamento delle capacità di ***cyber defence* di altrettante Amministrazioni;**
- **4 Avvisi Pubblici**, che hanno determinato l'ammissione al finanziamento di **129 progettualità** rivolte a **51 Amministrazioni**, di cui **16 centrali** e **35 locali,** come dettagliato nella tabella sottostante (Figura 33)[26] .

[26] Per ogni Avviso sono stati ammessi a finanziamento uno o più progetti per singola Pubblica Amministrazione, compatibilmente con i vincoli previsti.

AVVISO	Destinatari	Dotazione finanziaria	Finanziamento ammesso	N. soggetti finanziati	N. progetti finanziati
1/2022 (ristoro)	ORGANI COST.LI, A RILIEVO COST.LE E PAC	15 M €	15 M €	12	20
2/2022 (servizio)	ORGANI COST.LI, A RILIEVO COST.LE E PAC	10 M €	7,85 M €	12	57
3/2022 (ristoro)	PAL	45 M €	45 M €	35	51
4/2022 (ristoro)	PAC	15 M €	1,16 M €	1	1

FIGURA 33 – AVVISI PUBBLICI DEL 2022

Come si evince dalle Figure 34 e 35, gli interventi finanziati nel 2022 a valere sull'Investimento 1.5 coprono parte degli Organi costituzionali e a rilevanza costituzionale, la quasi totalità dei Ministeri e delle Agenzie Fiscali, 19 Regioni e le 2 Province Autonome, nonché 14 Comuni capoluogo facenti parte di Città Metropolitane ai sensi della Legge n. 56/2014, i Comuni capoluogo delle Città Metropolitane istituite nelle Regioni a Statuto speciale e le Provincie autonome.

FIGURA 34 – DESTINATARI DEGLI INTERVENTI TRA GLI ORGANI COSTITUZIONALI,
A RILEVANZA COSTITUZIONALE E LE PA CENTRALI, PNRR M1C1|1.5

FIGURA 35 – DESTINATARI DEGLI INTERVENTI TRA LE PA LOCALI

Entrando più nello specifico, nel corso del 2022 l'ACN ha pubblicato **3 Avvisi Pubblici rivolti agli Organi costituzionali, a rilevanza costituzionale e alle PAC:**

- **Avviso Pubblico 1/2022** per la presentazione di proposte di interventi di potenziamento della resilienza *cyber*;
- **Avviso Pubblico 2/2022**, a sportello, per l'erogazione di interventi di potenziamento e miglioramento delle capacità *cyber*;
- **Avviso Pubblico 4/2022**, a sportello, per la presentazione di proposte di interventi di potenziamento delle capacità di analisi e scrutinio *software* della P.A. centrale.

Di seguito sono riportate, per ciascun Avviso Pubblico, le principali caratteristiche e le attività svolte nel corso dell'ultimo anno, unitamente ad un dettaglio dei soggetti interessati agli interventi e delle progettualità ammesse a finanziamento, con i relativi importi assegnati.
Avviso Pubblico 1/2022. Il primo procedimento espletato per l'attuazione degli investimenti finalizzati alla **realizzazione di interventi di potenziamento della resilienza *cyber* per gli Organi costituzionali e a rilevanza costituzionale e per la P.A. Centrale** è stato pubblicato a marzo 2022, con lo scopo di individuare, mediante una **procedura valutativa selettiva con graduatoria**, Amministrazioni attuatrici di **progetti c.d. "a regia"**.

L'Avviso Pubblico, la cui dotazione finanziaria complessiva ammonta a **15 milioni di euro a valere sull'Investimento 1.5**, costituisce una delle iniziative che l'Agenzia ha attuato nei confronti di Organi Costituzionali e a rilevanza costituzionale, di Agenzie Fiscali[27] e di tutte le Amministrazioni facenti parte del Nucleo per la cybersicurezza, per il finanziamento delle seguenti tipologie di interventi[28]:

- analisi della postura di sicurezza dei servizi e delle infrastrutture digitali delle PP.AA. e definizione di un Piano di potenziamento delle capacità *cyber*;
- analisi, miglioramento e potenziamento dei processi di gestione del rischio *cyber*;
- rafforzamento delle competenze e della consapevolezza delle persone nella gestione del rischio *cyber*;
- progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio *cyber.*

L'intera fase di **progettazione** della metodologia di selezione e di **predisposizione degli atti** è avvenuta **in soli 2 mesi** dall'approvazione del documento di indirizzo strategico denominato "Strategia di finanziamento mediante Avvisi Pubblici – Procedure operative per la selezione di progetti 'a regia', mediante l'espletamento di un Avviso Pubblico". L'Agenzia ha, inoltre, gestito l'intero *iter* procedimentale – dalla fase di istruttoria alla valutazione tecnica delle proposte progettuali pervenute – giungendo all'individuazione dei Soggetti destinatari dell'importo complessivo stanziato **in 6 mesi dalla data di pubblicazione**.

L'efficiente gestione dell'*iter* ha consentito il tempestivo avvio delle progettualità ammesse a finanziamento, consentendo di raggiungere con puntualità i *target* previsti a dicembre 2022, contribuendo altresì a quelli previsti per il 2024 (Figura 36).

[27] Individuate ai sensi del Titolo II del D. Lgs. 300/1999.
[28] Per maggiori informazioni si rimanda al sito ItaliaDomani al seguente link https://www.italiadomani.gov.it.

FIGURA 36 – AVVISO PUBBLICO N.1/2022 PNRR M1C1|1.5 – RISULTANZE AMMISSIONE A FINANZIAMENTO

Avviso Pubblico 2/2022. Parallelamente alla progettazione dell'Avviso Pubblico 1/2022, e a beneficio dei medesimi soggetti, l'Agenzia ha pianificato ed espletato un procedimento per **l'erogazione "a titolarità" di interventi di potenziamento e miglioramento delle capacità *cyber* degli Organi Costituzionali e di rilievo Costituzionale, delle Agenzie Fiscali e delle Amministrazioni facenti parte del Nucleo per la cybersicurezza.**

L'Avviso Pubblico 2/2022[29] ha consentito – mediante l'espletamento di una **procedura a sportello** – di individuare soggetti destinatari di specifici servizi, erogati da parte della stessa Agenzia, nei seguenti ambiti:

- censimento dei livelli di maturità della postura di sicurezza dei servizi e delle infrastrutture digitali delle PP.AA.;
- realizzazione di un piano programmatico di potenziamento, sia a breve che a medio-lungo termine, delle capacità *cyber* volto a supportare il percorso di trasformazione digitale sicura della PA;
- realizzazione di interventi di potenziamento a medio-breve termine dei servizi e delle infrastrutture in essere della P.A.

L'Avviso Pubblico (Figura 37), la cui dotazione finanziaria complessiva ammonta a **10 milioni di euro a valere sull'Investimento 1.5**, è stato **pubblicato a marzo 2022**. L'intero *iter* amministrativo

[29] Per maggiori informazioni si rimanda al sito ItaliaDomani al seguente link https://italiadomani.gov.

propedeutico all'individuazione delle istanze ammesse a finanziamento si è concluso ad aprile. Anche in questo caso, grazie all'efficienza e alla tempestività nella definizione della graduatoria, l'Agenzia ha potuto stipulare le Convenzioni e avviare nell'anno appena concluso, anche mediante l'esternalizzazione dei servizi, **l'85% della totalità degli interventi finanziati.**

FIGURA 37 – AVVISO PUBBLICO N.2/2022 PNRR M1C1|1.5 – RISULTANZE AMMISSIONE A FINANZIAMENTO

Avviso Pubblico 4/2022. Tale Avviso Pubblico è orientato, in particolare, alla **creazione e attivazione di laboratori di analisi e scrutinio *software*, interni alla P.A.**, anche in raccordo con il Centro di Valutazione e Certificazione Nazionale (CVCN).

L'Avviso Pubblico 4/2022[30], la cui dotazione finanziaria complessiva ammonta a **15 milioni di euro a valere sull'Investimento 1.5**, è stato espletato al fine di supportare un percorso virtuoso di **identificazione, valutazione e mitigazione di potenziali fattori di rischio dei *software* in uso presso le PAC**, gli Organi costituzionali e a rilevanza costituzionale.

Il procedimento in oggetto, espletato mediante **procedura a sportello**, concorre al raggiungimento degli obiettivi PNRR, grazie al finanziamento di **progetti "a regia"** finalizzati a:

- l'acquisizione e messa in produzione di strumenti e piattaforme di analisi e valutazione delle vulnerabilità dei *software* delle PP.AA.;

[30] Per maggiori informazioni si rimanda al sito ItaliaDomani al seguente link https://www.italiadomani.gov.it.

- lavori di adeguamento logistico e infrastrutturale per la creazione di ambienti dedicati alle attività del laboratorio che possano garantire adeguate misure di sicurezza fisica;
- la definizione e l'implementazione di procedure e processi in linea con gli *standard* e le prassi nazionali e internazionali di pertinenza;
- il reclutamento di personale dedicato alle attività di avvio del laboratorio;
- lo sviluppo delle competenze e delle professionalità per il personale del laboratorio.

La stipula dell'atto d'Obbligo con il Amministrazione attuatrice individuata è avvenuta **a solo 1 mese dalla pubblicazione dell'Avviso Pubblico**. Ciò ha consentito di avviare entro il 2022 gli interventi ammessi a finanziamento, le cui risultanze sono riportante nella Figura 38.

FIGURA 38 – AVVISO PUBBLICO N.4/2022 PNRR M1C1|1.5 – RISULTANZE AMMISSIONE A FINANZIAMENTO

In continuità rispetto ai primi procedimenti attuativi dell'Investimento 1.5 espletati, e coerentemente con le linee di indirizzo strategico adottate, nel corso del 2022 l'Agenzia ha inoltre pubblicato il primo degli Avvisi rivolti alle **Pubbliche Amministrazioni Locali**, estendendo progressivamente il perimetro delle Amministrazioni cui finanziare interventi di potenziamento del livello di resilienza *cyber* dei sistemi informativi, per la messa in sicurezza dei dati e dei servizi per i cittadini.

La progettazione dell'**Avviso Pubblico 3/2022** ha consentito all'Agenzia di ampliare la platea di soggetti ammessi a presentare le proprie progettualità, individuando quali Soggetti destinatari le Regioni, i Comuni capoluogo facenti parte di Città Metropolitane ai sensi della Legge n. 56/2014, i Comuni capoluogo delle Città Metropolitane istituite nelle Regioni a statuto speciale e le Province autonome.

A luglio, l'Agenzia ha, quindi, indetto l'**Avviso Pubblico 3/2022**[31] volto a supportare la realizzazione di un percorso virtuoso di gestione del rischio *cyber* delle PP.AA. Locali, mediante lo stanziamento di una dotazione finanziaria complessiva di **45 milioni di euro a valere sull'Investimento 1.5.**

I progetti finanziati **"a regia"**, individuati mediante una **procedura valutativa selettiva con graduatoria**, hanno ad oggetto le medesime tipologie di interventi già finanziati per le PP.AA. Centrali, e concorreranno al raggiungimento degli obiettivi PNRR previsti per il 2024. In particolare, essi riguardano:

- analisi della postura di sicurezza e definizione di un piano di potenziamento strategico;
- miglioramento dei processi e dell'organizzazione di gestione della *cybersecurity*;
- miglioramento della consapevolezza delle persone;
- progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio *cyber*.

Nonostante l'alto tasso di partecipazione all'Avviso in oggetto (79 istanze progettuali pervenute per 36 Soggetti richiedenti), l'Agenzia ha **portato a compimento in tre mesi l'intero *iter* di istruttoria amministrativa**, adottando a dicembre 2022 la determina di ammissione ed esclusione delle istanze progettuali pervenute. La Commissione all'uopo incaricata **ha tempestivamente avviato, prima della chiusura dell'anno, le attività di valutazione delle proposte progettuali ammesse,** concludendo l'intero iter valutativo propedeutico alla formalizzazione della graduatoria nei primi giorni di gennaio 2023 i cui esiti sono sintetizzati nella Figura 39.

[31] Per maggiori informazioni si rimanda al sito ItaliaDomani al seguente link https://www.italiadomani.gov.it.

AVVISO PUBBLICO 3/2022: RISULTANZE AMMISSIONE A FINANZIAMENTO

35 Amministrazioni ammesse a finanziamento
51 Progetti finanziati

45 Tot. finanziato **mln/€**

Regione Marche 1/2 progetti — **0,99** mln/€	Regione Veneto 2/2 progetti — **2,00** mln/€	Provincia autonoma di Trento 1/2 progetti — **0,95** mln/€
Regione Molise 1/1 progetti — **1,00** mln/€	Comune di Messina 2/2 progetti — **1,56** mln/€	Regione Abruzzo 1/2 progetti — **0,99** mln/€
Regione Piemonte 2/2 progetti — **1,97** mln/€	Comune di Milano 2/2 progetti — **1,99** mln/€	Regione Basilicata 1/2 progetti — **1,00** mln/€
Regione Puglia 2/2 progetti — **1,99** mln/€	Comune di Napoli 1/3 progetti — **0,66** mln/€	Comune di Torino 2/2 progetti — **1,99** mln/€
Comune di Bari 2/2 progetti — **1,81** mln/€	Comune di Palermo 1/2 progetti — **0,99** mln/€	Regione Lombardia 2/2 progetti — **2,00** mln/€
Comune di Bologna 2/2 progetti — **1,99** mln/€	Comune di Reggio Calabria 1/1 progetti — **0,99** mln/€	Roma Capitale 2/3 progetti — **1,85** mln/€
Comune di Cagliari 1/2 progetti — **0,99** mln/€	Comune di Genova 1/1 progetti — **0,64** mln/€	Regione Campania 1/2 progetti — **0,96** mln/€
Comune di Catania 1/2 progetti — **1,00** mln/€	Regione Sicilia 2/2 progetti — **1,99** mln/€	Regione Emilia Romagna 2/3 progetti — **1,40** mln/€
Comune di Firenze 3/3 progetti — **2,00** mln/€	Regione Calabria 1/2 progetti — **0,96** mln/€	Regione Friuli-Venezia Giulia 1/3 progetti — **0,66** mln/€
Regione Toscana 1/2 progetti — **1,00** mln/€	Regione Sardegna 1/2 progetti — **1,00** mln/€	Regione Lazio 2/3 progetti — **1,22** mln/€
Regione Umbria 1/2 progetti — **1,00** mln/€	Comune di Venezia 1/3 progetti — **0,24** mln/€	Regione Liguria 1/2 progetti — **0,99** mln/€
Regione Valle d'Aosta 1/2 progetti — **0,92** mln/€	Provincia autonoma di Bolzano 2/3 progetti — **1,20** mln/€	

FIGURA 39 – AVVISO PUBBLICO N. 3/2022 PNRR M1C1|1.5 – RISULTANZE AMMISSIONE A FINANZIAMENTO

5.3 Evidenze dello stato della postura di sicurezza della PA

È di tutta evidenza come l'avvio di interventi PNRR di rafforzamento della resilienza *cyber* delle PP.AA. consenta di perseguire uno degli obiettivi fondamentali della Strategia nazionale di cybersicurezza 2022-2026, ovvero la protezione degli *asset* strategici nazionali da realizzare attraverso l'adozione di un approccio sistemico orientato alla gestione e mitigazione del rischio, volto a garantire la transizione digitale e migliorare la resilienza del Paese, anche in linea con i requisiti di sicurezza definiti dalle normative PSNC e NIS.

In particolare, con i primi interventi avviati e completati, grazie ad una accurata **analisi della postura di sicurezza** di diverse Pubbliche Amministrazioni Centrali, sono state individuate mirate **opportunità di miglioramento** tarate rispetto ai **livelli di maturità** presenti in ogni specifico contesto, consentendo una distribuzione ragionata delle risorse disponibili. Le aree di miglioramento identificate includono: la razionalizzazione dei modelli di *governance* della *cybersecurity*; la standardizzazione dei processi e tematiche di formazione e *awareness*; la definizione di un approccio strutturato di valutazione del rischio *cyber*; la gestione automatizzata degli *asset* aziendali; la formalizzazione di processi strutturati per la gestione e la risposta agli incidenti informatici.

Dando immediato seguito ai risultati delle attività di analisi condotte dall'Agenzia, sono già state svolte **iniziative *ad hoc*** presso svariate Amministrazioni interessate dagli interventi che, ad oggi, hanno già consentito di:

- migliorare e/o definire un **programma di *cybersecurity*** in maniera strutturata e integrata, fondato sulla gestione del rischio *cyber*, che possa essere implementato in presenza di modelli preesistenti di governo della sicurezza *cyber* o al fine di formalizzane uno, laddove non presente;
- agevolare e facilitare la **comunicazione con i vertici dell'Amministrazione** e con gli interlocutori esterni ed istituzionali.

È, inoltre, emerso con evidenza che, oltre all'attivazione di iniziative *ad hoc* finalizzate a realizzare specifici **programmi di trasformazione ed evoluzione dei presidi in essere**, per poter rendere effettive le opportunità di miglioramento individuate occorre guidare le Amministrazioni verso la scelta di più **adeguati strumenti contrattuali** attraverso cui attivare progetti di rilevanza strategica. In tale contesto,

le Convenzioni pubbliche Consip, sembrano rappresentare lo strumento preferenziale per l'attuazione di tali potenziamenti.

In tale contesto, per garantire il **necessario coordinamento nella rilevazione dei bisogni** e nell'uniformità di attuazione tra le diverse Amministrazioni **nella conseguente definizione degli interventi strategici di *cybersecurity***, **l'Agenzia** può e intende configurarsi quale **soggetto facilitatore al fine di veicolare, verificare e integrare le richieste** per garantire un catalogo di servizi il più possibile completo rispetto alle esigenze cogenti.

Il Piano di implementazione della Strategia nazionale di cybersicurezza rappresenta certamente un importante strumento per guidare l'Agenzia nel percorso collaborativo a supporto della P.A., nonché per offrire nuovi strumenti di finanziamento per la realizzazione delle opportunità di potenziamento identificate.

06.

AUTONOMIA STRATEGICA

Il raggiungimento di un'autonomia strategica è non solo uno dei compiti dell'Agenzia, assegnato dal D.L. n. 82/2021, ma anche uno degli obiettivi della Strategia dell'UE in materia di cybersicurezza per il decennio digitale a livello europeo. Infatti, lo sviluppo di tecnologie proprie, in collaborazione con il settore privato, la presenza di una forza lavoro adeguatamente formata e una diffusa consapevolezza sui rischi *cyber*, consentono di rafforzare significativamente lo scudo protettivo del Paese in relazione a possibili attacchi e minacce *cyber*.

Pertanto, l'Agenzia sta simultaneamente portando avanti attività su tutti questi fronti con il fine di consentire il raggiungimento dell'autonomia strategica.

6.1 Attuazione Strategia Cloud Italia

Nell'ambito delle misure volte a rafforzare la postura di cybersicurezza della Pubblica Amministrazione e del Paese è certamente ricompresa l'attuazione della Strategia *Cloud* Italia, volta a promuovere la sovranità e l'autonomia tecnologica del nostro Paese e dell'Unione europea nella gestione dei dati dei cittadini e delle aziende europee, a partire dal settore pubblico. Difatti, con il DPCM 1° settembre 2022, recante modalità e termini per assicurare il trasferimento delle funzioni, dei beni strumentali e della documentazione dall'Agenzia per l'Italia digitale e dal Dipartimento per la trasformazione digitale all'Agenzia per la cybersicurezza nazionale, l'ACN è subentrata ad AgID nella qualificazione dei servizi *cloud* per la Pubblica Amministrazione secondo il processo definito dal Regolamento "*Cloud* per la PA".

Il documento di indirizzo delinea tre obiettivi che pilotano un percorso di trasformazione digitale sicuro:

- incentivare l'adozione del modello *Cloud* della P.A., nell'ottica di proporre un'offerta di servizi digitali e infrastrutture tecnologiche sicure, efficienti, affidabili e autonome, in linea con i principi di tutela della *privacy* e le raccomandazioni destinate all'intero mercato digitale europeo;
- costituire il Polo Strategico Nazionale, quale infrastruttura a garanzia della sicurezza degli *asset* strategici per il Paese;
- valorizzare le Amministrazioni e la loro capacità di offrire servizi digitali.

Nel 2022 l'Agenzia è stata impegnata a consentire la realizzazione degli obiettivi di questa Strategia adottando due Determinazioni implementative del c.d. Regolamento *cloud*.

La prima (Determinazione n. 306/2022) definisce il modello per la predisposizione dell'elenco e della **classificazione** dei dati e dei servizi pubblici. La classificazione costituisce il passo abilitante per individuare un compromesso bilanciato tra costi e sicurezza. In tale contesto, in base ai possibili effetti di una loro compromissione in termini di disponibilità, confidenzialità e integrità, i dati e i servizi della P.A. sono classificati su tre livelli:

FIGURA 40 – CLASSIFICAZIONE DEI DATI E DEI SERVIZI PUBBLICI

- **strategici**, la cui compromissione può avere impatto sulla sicurezza nazionale, che includono quelli ricompresi nel D.L. n. 105/2019, i servizi essenziali ai sensi del D.Lgs. n. 65/2018 erogati a livello nazionale e le banche dati a carattere nazionale;
- **critici**, la cui compromissione potrebbe determinare un pregiudizio per il mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese, che includono i servizi essenziali ai sensi del D.Lgs. n. 65/2018 erogati a livello locale, nonché quelli che trattano grandi moli di dati personali;
- **ordinari**, i rimanenti dati e servizi.

Al fine di supportare tale esercizio, primo nel suo genere a livello nazionale, il modello di classificazione prevede due elementi: un questionario e degli "elenchi pre-classificati di servizi", ospitati sulla piattaforma PAdigitale2026 alla quale tutte le Amministrazioni possono accedere per avviare la propria pratica di classificazione.

Il questionario consiste in 23 domande tramite le quali è possibile caratterizzare i servizi erogati dalle Amministrazioni. In considerazione dell'elevatissima quantità di dati oggetto di analisi, è stato sviluppato da ACN un algoritmo di classificazione che ha consentito di determinare la classe (ordinario, critico o strategico) del servizio e dei dati trattati, applicando una combinazione di soglie in base alla tipologia dell'ente, al punteggio raggiunto con le risposte, nonché al volume e alla qualità dei dati.

Gli "elenchi pre-classificati di servizi" consistono in elenchi di servizi in cui viene proposta una classificazione predefinita, che l'Amministrazione può accettare o modificare compilando il citato questionario. È inoltre possibile eliminare servizi o inserirne di nuovi.

L'attività preparatoria svolta dall'ACN ha permesso di rendere disponibili 7 elenchi pre-classificati:

- i servizi tipici della P.A., sia di carattere interno (come il protocollo) che esterno (come l'albo pretorio);
- i servizi delle Regioni e delle Province Autonome;
- i servizi delle Città Metropolitane;
- i servizi delle Province;
- i servizi dei Comuni;
- i servizi delle ASL e delle Aziende Ospedaliere;
- i servizi delle Scuole.

In tale contesto, è risultato estremamente prezioso il contributo apportato dai 4 gruppi pilota di Amministrazioni locali e i 2 gruppi pilota di Amministrazioni centrali che si sono resi disponibili a supportare l'Agenzia nel primo semestre del 2022.

Dall'avvio del processo di classificazione, avvenuto ad aprile, nel corso dell'anno sono state evase, tramite la piattaforma PAdigitale2026, le pratiche di classificazione per circa gli 80% degli enti. In relazione a tale copertura, la Figura 41 riporta la percentuale di servizi classificati come ordinari, critici e strategici per le diverse categorie della PA.

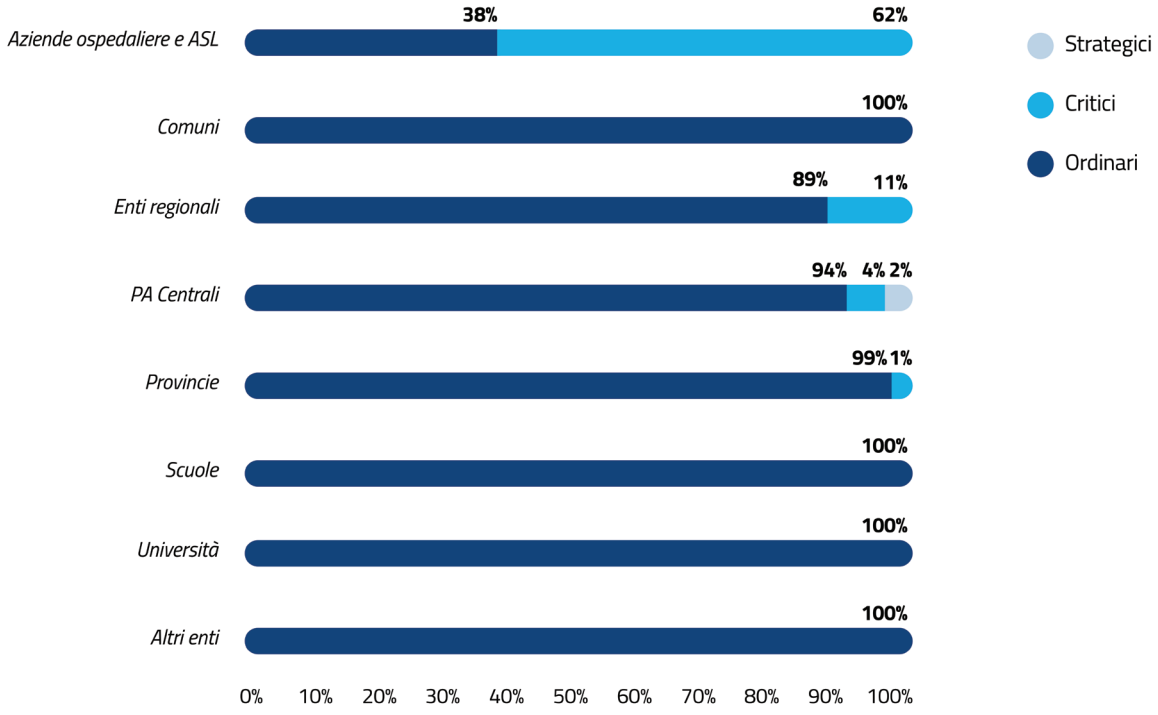


FIGURA 41 – PERCENTUALE DI SERVIZI CLASSIFICATI COME ORDINARI, CRITICI E STRATEGICI, PER CATEGORIE DI PA

Quale elemento complementare alla classificazione, la seconda Determinazione n. 307/2022 ha stabilito inoltre:

- i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali;
- le caratteristiche di qualità, di sicurezza, di *performance* e scalabilità, interoperabilità, portabilità dei servizi *cloud*;
- le modalità del procedimento di qualificazione dei servizi *cloud*.

In relazione ai livelli minimi e alle caratteristiche dei servizi *cloud*, si è provveduto ad elaborare un insieme di misure coerente con l'impianto regolamentare esistente in materia *cyber*, che impone obblighi gradualmente crescenti per le 3 classi di dati e servizi identificati nell'esercizio di cui sopra. In particolare, si è teso ad allineare le misure per il **livello ordinario** a quanto già previsto da AgID per i CED pubblici di classe A[32]. Per quanto riguarda, invece, il **livello strategico**, le misure sono coerenti con le previsioni del DPCM n. 81/2021, mentre quelle di **livello critico** si pongono su

[32] Ai sensi della circolare 1/2019 di AgID.

un piano intermedio, secondo un criterio di gradualità. La matrice da cui sono derivate le misure è, infatti, il *Framework Nazionale per la Cybersecurity e la Data Protection*, in continuità con quanto stabilito in relazione alle misure fissate nella normativa relativa al PSNC e alla NIS, al fine di agevolare gli enti, tra i quali quelli inseriti nel Perimetro, tenuti al rispetto di molteplici normative.

In tal senso, gli allegati tecnici della Determinazione n. 307/2022 recano 57 misure per il livello ordinario, 8 misure aggiuntive per il livello critico, nonché 2 ulteriori misure aggiuntive per il livello strategico, declinate in relazione alle infrastrutture digitali e ai servizi *cloud* (Figura 42).

Allegati tecnici della Determinazione n. 307/2022

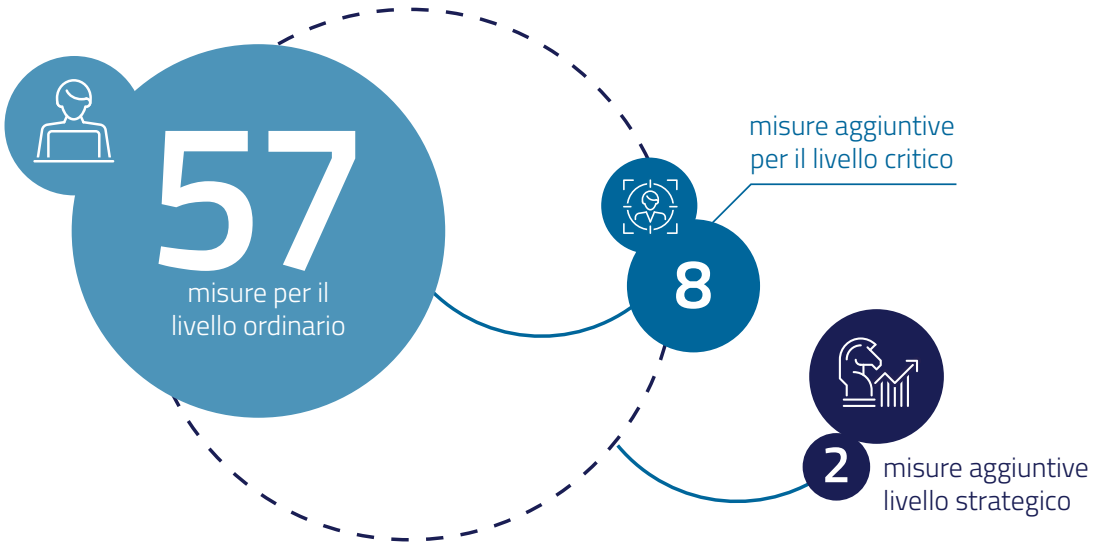


FIGURA 42 – ALLEGATI TECNICI DELLA DETERMINAZIONE N. 307/2022

Il processo di **qualificazione**, invece, è lo strumento che consente all'Agenzia di svolgere le verifiche preventive sull'adeguatezza dei servizi *cloud* offerti da operatori privati dei quali si possono avvalere le Pubbliche Amministrazioni. I requisiti di qualificazione sono organizzati in **4 livelli crescenti**, tesi a promuovere un maggior controllo sui dati da parte degli enti pubblici, che si basano sui livelli minimi per le infrastrutture e sulle caratteristiche dei servizi *cloud* di cui sopra.

In linea con lo spirito che guida l'azione dell'Agenzia, è stato avviato un processo di supporto a beneficio di tutti gli attori interessati, svolgendo nel corso dell'anno **oltre 50 incontri** a favore di numerosi enti pubblici e privati, ciò unitamente ad interventi pubblici e alla concertazione con associazioni di settore.

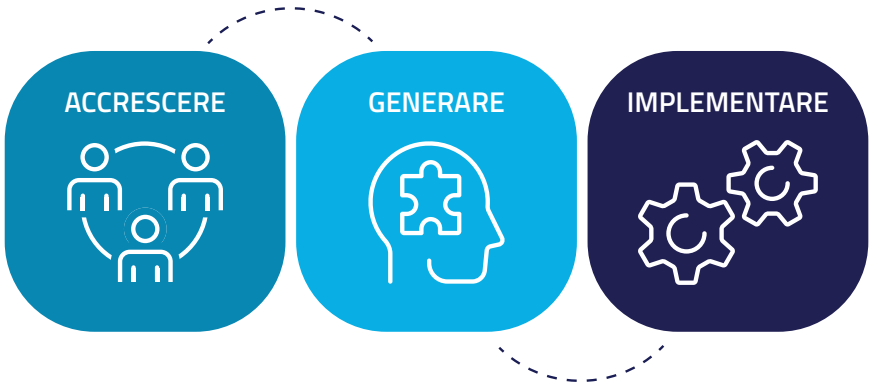
6.2 Programmi a supporto dell'imprenditoria nella *cybersecurity*

Il tema del raggiungimento di un'autonomia tecnologica è centrale per il sistema Paese. Il suo conseguimento, come evidenziato anche nella Strategia Nazionale di Cybersicurezza 2022-2026, 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*".

A tal riguardo, l'Agenzia ha definito un programma di azioni sinergiche tra ricerca, *startup* e sviluppo, al fine di sostenere l'innovazione, il rafforzamento tecnologico e industriale del sistema Paese, attraverso l'impegno nella valorizzazione della ricerca e nella creazione di nuove aziende tecnologiche.

Il Programma, che è stato progettato nel 2022, si basa sul modello della ***Cyber Innovation Network***, ovvero la costruzione di una rete di collaborazioni dell'Agenzia con primari Operatori dell'ecosistema dell'innovazione (incubatori per *spin-off* e *startup* tecnologiche, acceleratori di *startup* innovative, strutture impegnate nel trasferimento tecnologico, ecc.), per definire e implementare programmi congiunti di supporto e accelerazione dell'innovazione nelle aree tecnologiche di interesse. In particolare, sono stati definiti i seguenti obiettivi nel dominio *cyber*:

1. **accrescere**, attraverso la collaborazione stabile con Operatori qualificati, la visibilità e l'accesso a portafogli rilevanti e qualificati di *startup* innovative, *spin-off* universitari, risultati della ricerca, per contribuire ad accelerarne lo sviluppo;
2. **generare**, con la definizione di programmi congiunti tra Agenzia e Operatori, un'offerta integrata e ad alto valore aggiunto per le *startup* innovative e i gruppi ricerca;
3. **implementare** un approccio di collaborazione e integrazione tra l'Agenzia e l'ecosistema dell'innovazione, consentendo di accelerare i processi di trasferimento e adozione di nuove tecnologie nel sistema produttivo e industriale italiano.



Nelle more dell'avvio della *Cyber Innovation Network*, pianificato in prima fase per Acceleratori e Incubatori e, a seguire, per *Technology Transfer Office* (TTO) in ambito universitario e ambiti di ricerca, l'Agenzia ha anche definito e attivato un piano, sostenuto con progettualità e finanziamenti afferenti al PNRR – Investimento 1.5, volto a sostenere la creazione di strutture tecniche nel mondo privato a supporto dell'attivazione delle capacità di scrutinio tecnologico.

In quest'ottica l'Agenzia, nel corso del 2022, ha sviluppato e pubblicato il primo intervento di **finanziamento** rivolto **ai soggetti privati** intenzionati a realizzare un laboratorio di prova per lo **svolgimento di attività di valutazione e scrutinio tecnologico sui beni, servizi e sistemi ICT** utilizzati dai Soggetti che erogano servizi essenziali per il Paese e che rientrano nel Perimetro nazionale di sicurezza cibernetica.

A tal fine, l'impegno dell'Agenzia non si è limitato esclusivamente alla progettazione della strategia di selezione dei Soggetti Sub-attuatori, bensì si è esteso anche alla fase di definizione, a monte, dei requisiti tecnici e logicistici, delle misure di sicurezza informatica, e dei requisiti di competenza ed esperienza necessari per l'accreditamento dei laboratori, mediante adozione delle relative Determinazioni Tecniche.

L'**Avviso Pubblico n. 5/2022**, è stato pubblicato a novembre 2022, e ha riguardato l'individuazione di **proposte progettuali c.d. "a regia"** che possano contribuire al processo di attivazione di una rete di Laboratori Accreditati di Prova (LAP), a supporto del Centro di Valutazione e Certificazione Nazionale (CVCN) istituito presso l'ACN, e in stretta collaborazione con i Centri di Valutazione (CV) del Ministero della difesa e del Ministero dell'interno, al fine di assicurare una gestione efficiente, a livello nazionale, dei procedimenti di scrutinio tecnologico, come previsto dall'art. 7 del decreto del Presidente del Consiglio 18 maggio 2022, n. 92.

In particolare, il suddetto Avviso Pubblico, la cui dotazione finanziaria complessiva ammonta a **5 milioni di euro a valere sull'Investimento 1.5**, mira a supportare la realizzazione di interventi di rafforzamento delle dotazioni tecnico-professionali dei Soggetti sub-attuatori, in termini di strumentazione, protezione degli ambienti di test, misure di sicurezza informativa e competenza del personale, mediante il finanziamento delle seguenti tipologie di attività:

- progettazione, sviluppo e messa in produzione di nuovi sistemi per l'esecuzione di analisi e scrutinio del *software*;
- lavori di adeguamento logistico e infrastrutturale;
- realizzazione e miglioramento dell'organizzazione e dei processi operativi del laboratorio;

- reclutamento di personale a tempo determinato dedicato esclusivamente all'attivazione del laboratorio;
- miglioramento delle competenze tecniche e delle professionalità del personale preposto al funzionamento del laboratorio.

Il finanziamento erogato **sarà concesso secondo il Regolamento "*de minimis*"**[33], in forma di sovvenzione diretta e nel rispetto dei massimali previsti secondo il suddetto regime, pari a 200.000 euro per Soggetto.

L'Avviso Pubblico, per il quale non è ancora conclusa la fase di istruttoria tecnico-amministrativa, contribuirà, insieme ai successivi che saranno pubblicati, a supportare realtà imprenditoriali con un profilo già specializzato nel campo della sicurezza *cyber*, orientandole e specializzandole ulteriormente nel campo dello scrutinio e certificazione tecnologica e creando una rete di laboratori funzionale al raggiungimento degli obiettivi strategici nazionali e degli impegni in ambito PNRR, con particolare riferimento alla *milestone* **M1C1-21 "Completamento della rete dei laboratori e del CVCN"**.

6.3 Programmi a supporto della ricerca nella *cybersecurity*

Durante il periodo in esame, i programmi a supporto della ricerca nella sicurezza cibernetica sono stati articolati in due principali linee di intervento: (i) attività propedeutiche alla stesura di un'Agenda di ricerca e innovazione (R&I) e (ii) iniziative di collaborazione nazionali ed europee in ambito ricerca sulla *cybersecurity.*

Quanto alle attività propedeutiche alla stesura dell'Agenda di ricerca e innovazione, in linea con il Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026, sono state proposte diverse misure per promuovere la ricerca e l'innovazione tecnologica attraverso la collaborazione tra soggetti pubblici e privati italiani. Nel 2022 l'ACN ha identificato una tabella di marcia per il perseguimento, entro il 2026, di tali misure riguardanti la ricerca, che si articola in tre fasi:

- nella **Fase#1** verrà definita un'Agenda di ricerca e innovazione per la cybersicurezza, che consideri le specificità del contesto nazionale italiano. Tale Agenda ha come obiettivo la creazione di una base di conoscenza condivisa per progettare e realizzare politiche di R&I in materia di cybersicurezza, a favore sia del settore pubblico sia di quello privato;

[33] Regolamento (UE) n. 1407/2013 relativo agli aiuti «de minimis», che disciplina gli aiuti di Stato di modesto importo (c.d. «de minimis») che sono dispensati dal controllo sugli aiuti di Stato in quanto si ritiene che essi non abbiano alcuna incidenza sulla concorrenza e sugli scambi nel mercato interno dell'Unione europea.

- nella **Fase#2** verrà creata una rete di soggetti di ricerca, pubblici e privati, che l'ACN intende coinvolgere al fine di cooperare nell'ottica di rafforzamento della postura dell'Italia sulla ricerca e innovazione in ambito cybersicurezza;
- nella **Fase#3** verrà progettato un piano di investimenti per le attività di R&I che, estendendo la già avviata *Cyber Innovation Network* ai TTO delle Università e a primari Centri di ricerca, consentirà di sviluppare programmi congiunti finalizzati ad incentivare il trasferimento tecnologico nel campo della cybersicurezza, sostenendo e indirizzando, laddove necessario, la ricerca applicata negli ambiti, individuati dall'agenda, per i quali risulta necessario un potenziamento delle capacità nazionali.

Attività propedeutiche alla stesura di un'Agenda di ricerca e innovazione (R&I)

FIGURA 43 – ATTIVITÀ PROPEDEUTICHE ALLA STESURA DI UN'AGENDA DI RICERCA E INNOVAZIONE (R&I)

L'ACN ha quindi dato inizio, nel 2022, alla Fase#1 con una serie di attività propedeutiche alla stesura dell'Agenda di R&I per la cybersicurezza, quali:

- la definizione della metodologia per la redazione dell'Agenda;
- l'analisi preliminare del panorama della ricerca nazionale in materia di cybersicurezza;
- lo studio del posizionamento di ACN nel quadro della ricerca internazionale.

Entro la fine del periodo in esame, tali attività propedeutiche hanno portato **ai seguenti risultati:**

- l'avvio di una collaborazione con il Ministero dell'Università e della Ricerca (MUR) e di contatti preliminari con la nuova Fondazione "SERICS – *Security and Rights in CyberSpace*[34]", al fine di allineare le rispettive priorità e coordinare le attività e gli sforzi di R&I per la sicurezza cibernetica;

- l'identificazione di importanti riferimenti internazionali riguardo il dominio di conoscenza sulla cybersicurezza redatti da (i) ENISA – *European Union Agency for Cybersecurity*, (ii) *Joint Research Centre* e (iii) un gruppo di lavoro costituito da esperti di fama internazionale, coordinato dal Regno Unito, per la redazione di un *Cybersecurity Body Of Knowledge* (CyBOK);
- l'identificazione di 6 aree della conoscenza sulla sicurezza cibernetica e 18 sub-aree al loro interno che definiscono le priorità di R&I.

Si prevede di concludere la Fase#1 con la definizione dell'Agenda, entro la prima metà del 2023.

L'ACN ritiene di importanza fondamentale stabilire collaborazioni con i soggetti di ricerca che operano sia sul territorio nazionale sia in ambito europeo ed internazionale. Nel corso del 2022 sono state avviate diverse attività finalizzate a stabilire tali collaborazioni e a condurre progetti di ricerca su temi di rilevanza comune.

Sul piano nazionale, nel corso del 2022 è stato sottoscritto un accordo tra ACN e il Consorzio Interuniversitario Nazionale per l'Informatica (CINI), su tematiche di collaborazione con il Laboratorio Nazionale di Cybersecurity[35], che consta di 64 nodi con sedi presso Università, Istituti ed Enti italiani di ricerca. In particolare l'ACN, nell'ambito delle attività legate all'evoluzione del quadro normativo, regolamentare e tecnico relative al PSNC, ha avviato attività di ricerca e sviluppo finalizzate all'aggiornamento e incremento del livello di maturità del c.d. modello perimetro, per la descrizione dell'architettura e della componentistica relativa ai beni ICT individuati negli elenchi di cui all'articolo 7 del DPCM 30 luglio 2020, n. 131, e di altri aspetti connessi, quali l'analisi del rischio di cybersicurezza.

Sul piano internazionale, l'ACN ha promosso diverse attività di collaborazione sul fronte della ricerca. Tra queste si evidenzia un'iniziativa di analisi congiunta su temi di Intelligenza Artificiale con il *Natural Sciences and Engineering Research Council of Canada*[36] e il MUR, anche in chiave di rafforzamento della cooperazione bilaterale con il Governo canadese.

[34] Soggetto attuatore del partenariato esteso nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU. Ulteriori informazioni disponibili al link: https://serics.eu/.

[35] https://cybersecnatlab.it/.

[36] https://www.nserc-crsng.gc.ca/index_eng.asp

6.4 Sviluppo *workforce* e capacità nazionali

Un problema ben noto al quale è necessario dare risposta è quello che vede, da un lato, una grande carenza di esperti di cybersicurezza a tutti i livelli e, dall'altro, di un possesso limitato di competenze in materia di cybersicurezza da parte di molti di coloro che hanno responsabilità decisionale (siano esse operative, intermedie o dirigenziali).

Sin dal 2022, con lo scopo di colmare tali lacune, ma anche di accrescere le competenze di cybersicurezza di tutti coloro che sono impegnati nella attività lavorative e la consapevolezza di tutti i cittadini sui rischi *cyber*, l'ACN ha avviato attività volte a promuovere, nel Paese, le iniziative di formazione nel settore della cybersicurezza ai vari livelli. Per rendere armonico e coerente il percorso di sviluppo di nuova forza lavoro e di competenze nel settore della cybersicurezza, è in corso di elaborazione una strategia complessiva che dovrà prevedere la promozione di un insieme variegato e articolato di iniziative da sviluppare secondo diverse coordinate. In particolare, essa si svolgerà secondo due fondamentali direttive: la prima è costituita dall'**ambito** di applicazione (scolastico, universitario, di formazione professionale); la seconda dal ***focus***, che può essere più o meno ampio e più o meno tecnico o anche relativo alle sole problematiche di sensibilizzazione o di generale cultura della cybersicurezza.

Molte delle attività che saranno poi inquadrate nella strategia della formazione, in corso di elaborazione, sono state già avviate nel corso del 2022.

L'Agenzia ha, infatti, già intrapreso una serie di interlocuzioni con numerosi Atenei e con la Conferenza dei Rettori delle Università Italiane (CRUI), per concordare attività da svolgere in collaborazione, al fine di supportare le attività didattiche e di ricerca nel settore della cybersicurezza e di contribuire alla loro definizione. A tal proposito sono state già stipulate alcune convenzioni.

Con riferimento al livello accademico più avanzato, l'Agenzia ha collaborato all'attivazione e alla promozione del nuovo corso di Dottorato nazionale in Cybersicurezza, proposto da oltre venti atenei e istituzioni di ricerca, sotto il coordinamento della Scuola IMT Alti Studi di Lucca, con cui è in via di stipula una convenzione. Nel contesto di tale dottorato, è stata programmata la partecipazione di dirigenti e funzionari dell'Agenzia alle attività di docenza, che si è contribuito a definire.

Per quanto riguarda i corsi di laurea e laurea magistrale, è stata avviata un'interlocuzione con il Laboratorio Nazionale di *Cybersecurity* del CINI, finalizzata ad una ricognizione dell'offerta formativa e successivamente a valutare la possibilità di definire, nel rispetto delle competenze degli altri soggetti istituzionalmente competenti per l'approvazione e l'accreditamento, una forma di riconoscimento dei corsi di studio in cybersicurezza, o in altre discipline (in particolare, informatica o ingegneria informatica) con contenuti significativi di cybersicurezza.

Una specifica attenzione è stata dedicata agli ITS, gli Istituti Tecnologici Superiori, che costituiscono un segmento di formazione di livello post-secondario non universitario, realizzato da Fondazioni *ad hoc* costituite, in ambito regionale, da soggetti di diverse categorie (istituti scolastici, atenei, aziende, enti di formazione professionale) che stanno già collaborando a realizzare percorsi in settori tecnologicamente avanzati, che permetteranno un più rapido inserimento nel mondo del lavoro di figure professionali di livello intermedio.

La realtà degli ITS ha, in Italia, una dimensione ancora abbastanza piccola (circa 20.000 studenti in tutto il Paese, rispetto ai 420.000 studenti universitari delle aree scientifiche e tecnologiche), mentre in altri paesi la situazione è diversa: in Germania, ad esempio, le istituzioni di livello paragonabile (*Fachhochschulen*) hanno un numero di studenti inferiore di solo il 50% rispetto a quello dei corsi universitari di area tecnico scientifica. Negli ultimi anni, Parlamento e Governo hanno dedicato una specifica attenzione agli ITS, con una legge che li ha definiti in modo più sistematico e con finanziamenti significativi, in particolare nel contesto del PNRR. Ciò risulta di particolare importanza oggi, in quanto nel campo della cybersicurezza il mercato del lavoro richiede sempre più spesso, fra le varie figure professionali, proprio quelle tecniche specializzate di livello intermedio, che possono essere formate attraverso i percorsi degli ITS.

L'Agenzia ha, pertanto, partecipato attivamente alla costituzione di una rete di collaborazione con il Ministero dell'istruzione, il Ministro dell'innovazione tecnologica e della trasformazione digitale *pro-tempore*, cinque regioni (Emilia-Romagna, Lombardia, Umbria, Liguria e Puglia), INDIRE, Confindustria e altri soggetti, volta a promuovere e coordinare le iniziative relative agli ITS sul tema della cybersicurezza e su quello correlato del *cloud computing*. Sono stati, inoltre, avviati contatti con altre Regioni per estendere l'iniziativa a tutto il territorio nazionale. Anche in questo contesto, così come in quello universitario, e con tempi auspicabilmente più veloci, si intende promuovere un'iniziativa volta al riconoscimento formale dei percorsi di cybersicurezza, avviando, allo scopo, interlocuzioni con il Ministero dell'istruzione e del merito.

Sempre con riferimento alla formazione non universitaria, sono state sostenute specifiche iniziative nell'ambito di quella professionale, in particolare con la Regione Lazio. Al riguardo, grazie ad un apposito accordo di collaborazione con quest'ultima, sono stati finalizzati la progettazione e l'avvio dei corsi della neo-istituita Accademia per la Cybersicurezza del Lazio, frutto dell'accordo di collaborazione tra l'ACN e quella Regione, volta a formare e qualificare figure professionali in grado di rispondere alle sfide della sicurezza informatica e della protezione dei sistemi informativi attraverso specifici programmi di formazione rivolti a studenti delle scuole superiori, diplomati e laureati, organizzati sotto la supervisione tecnico-scientifica dell'Agenzia. Sono stati avviati, inoltre, contatti con altre Regioni finalizzati alla definizione di profili e all'avvio di percorsi di formazione.

La promozione della formazione nel settore della cybersicurezza è stata portata avanti anche attraverso la partecipazione di esponenti dell'Agenzia a numerosi eventi e seminari presso istituzioni nazionali, nonché con l'interazione con numerose aziende. Tra le varie iniziative si segnala quella, ancora in fase preliminare, denominata Repubblica Digitale, promossa dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio, e con ANITEC-ASSINFORM, sul tema della formazione delle competenze avanzate ICT.

In tutte le iniziative sopra citate, oltre a prestare attenzione ai profili specialistici, è stata enfatizzata la necessità di promuovere la crescita delle competenze di *cybersecurity* anche secondo una prospettiva di natura trasversale. In questo contesto, è molto importante perseguire un approccio alla formazione che favorisca il dialogo multidisciplinare, con esperti con competenze di base diverse, ad esempio giuridica, economica o manageriale, che siano in grado di interagire con gli specialisti di area tecnologico-informatica e viceversa. L'Agenzia, coerentemente, sta contribuendo a promuovere tali iniziative formative.

L'Agenzia ha, altresì, collaborato alla promozione di una serie di competizioni nel settore della cybersicurezza, con il duplice obiettivo di stimolare l'interesse specifico da parte dei giovani e di contribuire alla diffusione di una maggiore consapevolezza della gestione del rischio e della minaccia *cyber*. In particolare, ha offerto il proprio contributo a due iniziative mirate, la prima promossa da Cassa Depositi e Prestiti e *Maker Faire Rome*, la seconda da *Cyber4.0* e Leonardo. Ha, inoltre, collaborato con il più volte citato Laboratorio Nazionale di *Cybersecurity* del CINI, con riguardo alle iniziative promosse sotto il nome complessivo di "*Big Game*", che includono *CyberChallenge* (prevalentemente per universitari e universitarie), *OliCyber* (rivolta a studentesse e studenti delle scuole superiori) e *CyberTrials* (rivolta specificamente a studentesse, senza prerequisiti tecnici). Quest'ultima, in particolare, mira a contribuire alla riduzione del cosiddetto

"*gender gap*", in quanto cerca di avvicinare alla *cybersecurity* anche le ragazze, che, per vari motivi, tendono a non privilegiare le discipline scientifico-tecnologiche.

È importante segnalare che le attività sono state svolte anche partendo dall'analisi del panorama internazionale. Anzitutto, per quanto riguarda la tematica relativa al riconoscimento dei corsi di studio, sono state esaminate con attenzione le esperienze di altri Paesi, in particolare la Francia, il Regno Unito e gli USA, che hanno già avviato da diversi anni iniziative sul tema. Sono stati, inoltre, avviati contatti con l'agenzia europea ENISA, che ha recentemente definito una serie di profili professionali tipici del settore della *cybersecurity* per classificare in dettaglio le competenze in materia *cyber*. Quest'ultimo esercizio, in particolare, potrà essere di grande utilità per l'Agenzia, che ha in animo la definizione di un quadro di riferimento di competenze a vario livello di specializzazione e varia ampiezza di spettro. In tale attività, oltre a fare riferimento ai profili definiti da ENISA, si potrà ricorrere alle classificazioni di aree e tematiche predisposte da associazioni scientifiche, quali la *Association for Computing Machinery* e l'*Institute of Electrical and Electronics Engineers*, e a quanto utilizzato dai vari soggetti che, sul mercato, offrono certificazioni a livello professionale, ivi inclusi gli enti di standardizzazione, fra cui, a livello italiano, UNINFO, con cui è stato avviato un contatto preliminare.

6.5 Cultura della cybersicurezza e iniziative di consapevolezza

Come evidenziato nei paragrafi precedenti, il tema della promozione della cultura della cybersicurezza e delle iniziative in tema di consapevolezza (*awareness*) risulta strettamente collegato a quello della formazione. Da un lato, infatti, la consapevolezza costituisce un primo livello di competenza, dall'altro, proprio attraverso la consapevolezza è possibile dare visibilità al settore e generare attrazione, in particolare fra i giovani, verso gli studi in cybersicurezza e più in generale verso le discipline informatiche e le altre di natura tecnico-scientifica. In quest'ultima categoria rientra anche la promozione delle competizioni nel settore della cybersicurezza, citata nel paragrafo precedente.

Nel corso del 2022 le iniziative sul tema sono state condotte secondo un approccio di crescita graduale, partendo da esperienze concrete, anche se sperimentali, per tendere poi verso un approccio sistematico da realizzare negli anni successivi sulla base dell'impostazione definita nella predisposizione della Strategia nazionale di cybersicurezza.

Per quanto riguarda le iniziative specifiche, si possono citare:

- la *Summer School in Cybersicurezza* organizzata nel mese di luglio dall'Agenzia insieme alla Scuola Nazionale dell'Amministrazione e al Dipartimento per la Funzione Pubblica della Presidenza del Consiglio dei ministri. Quest'ultima esperienza ha avuto un rilievo particolare in quanto ideata con l'obiettivo di offrire a chi ricopre ruoli apicali nelle Amministrazioni centrali dello Stato un'occasione di approfondimento intensivo sui rischi connessi alla sicurezza cibernetica e sugli strumenti per riconoscerli, prevenirli e contrastarli. Sono stati, in particolare, condivisi e analizzati casi concreti, con riferimento ai quattro pilastri tecnico-operativi della Strategia nazionale di cybersicurezza: cybersicurezza e resilienza; prevenzione e contrasto della criminalità informatica; difesa e sicurezza militare dello Stato; ricerca ed elaborazione informativa. Le attività sono state sviluppate con un'ampia partecipazione dei dirigenti dell'Agenzia, e con esponenti del Ministero della difesa, del Ministero degli affari esteri e della cooperazione internazionale, del Dipartimento delle Informazioni per la Sicurezza, del Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei ministri, della Polizia Postale e delle Comunicazioni, della Scuola Nazionale dell'Amministrazione e della *Cyber & Security Academy* di Leonardo;

- la partecipazione a ITASEC 2022, conferenza di riferimento della comunità italiana di ricerca in *cybersecurity*, alla quale ACN ha offerto il suo supporto, oltre a contribuire alla definizione delle attività scientifiche. Nel corso dell'evento l'Agenzia ha, altresì, partecipato a numerosi *workshop* per approfondire le molteplici competenze di ACN, dall'autonomia tecnologica, alle capacità nazionali di monitoraggio e risposta agli incidenti, ai temi della cultura della cybersicurezza e delle nuove certificazioni del Centro di Valutazione e di Certificazione Nazionale (CVCN);

- partecipazione alle sessioni formative di *Cybersecurity Awareness*, organizzate nell'ambito dell'Avviso Pubblico 02/2022 (vds Cap. 5.2), tenute da personale dell'ACN a beneficio di personale dipendente, sia a livello direttivo che dirigenziale, di Pubbliche Amministrazioni e Organi Costituzionali. L'obiettivo dei corsi è stato quello di introdurre la platea alle

principali tematiche nell'ambito della cybersicurezza e sensibilizzarla rispetto alle minacce informatiche più rilevanti nei contesti governativi e della Pubblica Amministrazione, indicando, anche tramite esempi concreti, i corretti comportamenti che ogni lavoratore può adottare nella quotidianità lavorativa per minimizzare il rischio di danni al patrimonio informatico delle proprie amministrazioni.

Sono stati, infine, avviati contatti con diversi soggetti nel mondo della comunicazione e della scuola e con esponenti del mondo produttivo, con l'obiettivo di esplorare le possibilità di promozione di iniziative di sensibilizzazione e le relative modalità.

A livello più sistematico, anche sulla base delle esperienze appena citate, sono state portate avanti iniziative volte alla promozione della cultura della cybersicurezza. In particolare, nella seconda parte dell'anno è stata avviata una riflessione, con il coinvolgimento della Presidenza del Consiglio (Dipartimento per l'Informazione e l'Editoria, Dipartimento per la trasformazione digitale), del Ministero dell'interno, del Ministero dell'università e della ricerca e del Ministero dell'istruzione e del merito, con l'obiettivo di predisporre e attuare iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e comportamenti responsabili nello spazio cibernetico, anche con riferimento a particolari fasce della popolazione.
Specifiche iniziative sono previste nel mondo della scuola e dell'università, al fine di coinvolgere tutta la popolazione giovanile.

07.

PROIEZIONE INTERNAZIONALE

Come evidenziato nella prefazione di questa Relazione, elemento essenziale per il rafforzamento della cybersicurezza del Paese è la cooperazione con gli altri Paesi, in particolare quelli c.d. "*like-minded*", e il posizionamento nelle organizzazioni intergovernative di cui fa parte l'Italia. La cooperazione con gli altri Stati consente, ad esempio, di amplificare la conoscenza di minacce e vulnerabilità, attraverso lo scambio informativo che avviene sia a livello bilaterale, sia all'interno di reti di CSIRT.

Allo stesso modo, è fondamentale la presenza e l'attiva partecipazione ai consessi multilaterali nei quali vengono discusse tematiche *cyber* al fine di incidere, in particolare, nella definizione delle *policy* e degli atti normativi che avranno un impatto sul territorio nazionale.

Per tali ragioni, l'ACN ha sin da subito lavorato per accreditarsi nel contesto internazionale, presentando la propria attività, contribuendo all'organizzazione di eventi di rilevanza strategica come la "*Cyber Defence Pledge Conference*" (vds. Cap. 7.2), nonché contribuendo alla definizione di importanti atti normativi, come la Direttiva NIS 2.

7.1 *Engagement* bilaterale

La cybersicurezza è un tema, per sua intrinseca natura, transnazionale e sempre più al centro delle agende di Stati e di organismi sovranazionali, in ragione dei rilevanti riflessi o ricadute che esso produce dal punto di vista della sicurezza, della resilienza, dello sviluppo e del progresso a livello interno ed internazionale.

Nella consapevolezza della dimensione transnazionale della *cybersecurity* e conformemente al suo mandato istituzionale, l'ACN ha avviato e rafforzato, sulla base di un dettagliato piano di proiezione internazionale, il dialogo e la collaborazione bilaterale con i principali interlocutori del settore, tra cui omologhe agenzie/autorità e competenti organizzazioni intergovernative. Ciò è stato possibile anche grazie allo svolgimento di visite istituzionali e incontri di vertice con esponenti apicali delle diverse controparti coinvolte, sia in formato virtuale, sia attraverso missioni all'estero e la partecipazione a conferenze internazionali. Tali incontri – che si sono anche svolti presso rappresentanze diplomatiche straniere in Italia ovvero presso la sede stessa dell'Agenzia – hanno beneficiato in termini di pianificazione e organizzazione della collaborazione e del supporto del MAECI.

Complessivamente, nel periodo di riferimento, i vertici dell'Agenzia hanno svolto:

- **5** missioni internazionali di vertice – Bruxelles (aprile 2022), Stati Uniti (giugno e ottobre 2022), Israele (giugno 2022) e Canada (novembre 2022) – nell'ambito delle quali si sono svolti mirati incontri con autorità e rappresentanti governativi locali o di organizzazioni internazionali con sede in tali Paesi (NATO e UE),
- **19** incontri bilaterali (15 dei quali svolti in presenza in Italia) con rappresentanti di autorità di *cybersecurity* estere o rappresentanti governativi di oltre 15 Paesi (inclusi Stati terzi all'UE);
- **4** incontri bilaterali con rappresentanti di organizzazioni intergovernative (UE, NATO, IILA).

FIGURA 44 – MISSIONI INTERNAZIONALI DI VERTICE

Tali missioni e incontri, che sono stati funzionali alla proiezione internazionale dell'ACN e al rafforzamento della posizione dell'Italia in materia di cybersicurezza e resilienza nell'arena internazionale, hanno interessato rappresentanti dei seguenti Paesi: Arabia Saudita, Belgio, Brasile, Canada, Estonia, Francia, Germania, Giordania, Israele, Montenegro, Oman, Paesi Bassi, Qatar, Slovenia, Regno Unito e USA.

In particolare, per quanto riguarda gli interlocutori esteri con i quali è stato stabilito un proficuo dialogo strategico, che fa da cornice e contribuisce ad alimentare specifiche forme di cooperazione bilaterale a livello tecnico-operativo, si segnalano, a titolo meramente esemplificativo:

Nord America:

- USA - il *Deputy National Security Advisor for Cyber and Emerging Technologies* per le attività del *National Security Council*, il *National Cyber Director*, l'*Under Secretary of Commerce for Standards and Technology* e Direttore del *National Institute of Standards and Technology*-NIST, il Direttore della *Cybersecurity and Infrastructure Security Agency*, nonché rappresentanti del *Bureau of Cyberspace and Digital Policy* del Dipartimento di Stato.
- Canada – il Ministro *de la Cybersécurité et du Numérique* del Quebec, il Direttore del *Canadian Centre for Cyber Security* (CCCS), il Direttore generale del *National Cybercrime Coordination Centre*.

Europa: i direttori del *Bundesamt für Sicherheit in der Informationstechnik*-BSI tedesco, dell'*Agence nationale de la sécurité des systèmes d'information* francese, del *Center for Cybersecurity Belgium*, del *Government Information Security Office* della Repubblica di Slovenia;

MENA: il Direttore dell'*Israel National Cyber Directorate*, del *Cyber Defence Center dell'Oman*, del *National Cybersecurity Council* della Giordania;

Organizzazioni internazionali: il Vice Segretario Generale della NATO, il *Deputy Assistant Secretary General for Emerging Security Challenges* (DASG ESC) della NATO, il Direttore del NATO *Cooperative Cyber Defence Centre of Excellence*, il Direttore della NATO *Communications and Information Agency*, il Segretario Generale e il Direttore Esecutivo dell'Organizzazione Internazionale Italo-Latino Americana (IILA), diversi rappresentati di vertice delle Istituzioni e agenzie europee (es. Commissione europea, Servizio Europeo per l'Azione Esterna, l'Agenzia per la *cybersecurity* ENISA).

A livello di contenuti, l'attività di promozione di relazioni internazionali strategiche ha avuto ad oggetto molteplici tematiche afferenti alla salvaguardia e alla promozione della cybersicurezza e della resilienza *cyber* nazionale e internazionale, nonché allo sviluppo e all'innovazione tecnologica. Oltre a far conoscere ai diversi interlocutori esteri la rinnovata architettura nazionale *cyber* e presentare le capacità di cui il Paese dispone in materia – compresi gli strumenti di *policy* (es. Strategia nazionale di cybersicurezza e Strategia Cloud Italia), normativi (es. legge sul Perimetro di sicurezza nazionale cibernetica) e organizzativi-tecnici (es. CVCN e scrutinio tecnologico) – queste attività hanno permesso di confrontarsi a livello strategico con le controparti sullo stato della minaccia *cyber* (anche nel contesto della situazione in Ucraina), sui *gaps and needs* del settore (es. carenza di forza lavoro specializzata, di una catena di approvvigionamento sicura, di una diffusa cultura della cybersicurezza) e di ragionare su come farvi fronte. In tale ottica, questo approccio ha consentito di avviare o promuovere iniziative comuni che mirano ad incrementare lo scambio informativo, la condivisione di migliori pratiche, esperienze e lezioni apprese, e a sostenere la ricerca e lo sviluppo di tecnologie e conoscenze per la cybersicurezza, nell'obiettivo ulteriore di valorizzare le eccellenze nazionali. Ad esempio, l'interlocuzione di vertice con il direttore del CCCS canadese ha consentito di dare avvio ad una collaborazione bilaterale in tema di *cyber threat intelligence*, sia da un punto di vista di scambio informativo, sia di metodologie e strumenti di analisi, anche in relazione allo sviluppo del progetto HyperSOC, di cui l'ACN è promotrice. Rilevante è stato anche il supporto ad iniziative dirette ad accrescere il coordinamento strategico tra i presidi nazionali e internazionali della cybersicurezza (es. *Counter Ransomware Initiative*-CRI – vds. Cap. 7.2).

Più in generale e in un'ottica di sistema, l'*engagement* bilaterale ha affiancato o integrato la partecipazione operativa dell'ACN a diversi consessi di cooperazione multilaterale. In diversi casi, si è rivelato funzionale alla ricerca e mantenimento di intese o alleanze su specifici temi, che si sono talvolta consolidate in posizioni comuni o condivise, fatte valere nei pertinenti tavoli internazionali, conferendo maggiore forza alla capacità negoziale nazionale.

7.2 Definizione *policy* europee e internazionali

Sul fronte **NATO**, l'Agenzia, oltre a seguire, in raccordo con la Rappresentanza Permanente d'Italia presso il Consiglio Atlantico, i negoziati dei documenti di *cyber defence policy* per gli aspetti di resilienza cibernetica trattati nell'ambito del *Cyber Defence Committee*, ha supportato, in coordinamento con il Ministero della difesa e le altre amministrazioni nazionali competenti,

il MAECI nella preparazione e nello svolgimento dei lavori della NATO *Cyber Defence Pledge Conference* (Roma, 10 novembre 2022), co-organizzata, da Italia e Stati Uniti d'America, con il supporto dell'*International Staff* della NATO.

La Conferenza, focalizzata sul tema della resilienza e della preparazione alla risposta alle minacce *cyber* contro le infrastrutture critiche, si è svolta presso la Farnesina e ha visto la partecipazione delle delegazioni dei 30 Paesi Alleati. Il successo dell'evento ha contribuito a valorizzare il ruolo e l'immagine dell'Italia quale interlocutore strategico – anche per le tematiche *cyber* – nei confronti dell'Alleanza e dei singoli Stati che ne fanno parte.

In ambito **OSCE**, l'Agenzia ha assicurato l'attiva partecipazione alle periodiche riunioni plenarie dell'*Informal Working Group*, che, nel corso del 2022, si è riunito per 3 volte e che ha visto la partecipazione delle delegazioni nazionali dei 57 Stati partecipanti tra Nord America, Europa e Asia.

In particolare, *a latere* di uno degli incontri, si è tenuto un *workshop* nel quale sono state illustrate alcune iniziative nazionali in materia di partenariato pubblico-privato in ambito *cybersecurity.* Nell'occasione, il nostro Paese ha illustrato il progetto dell'Accademia di Cybersicurezza Lazio (ACL) (vds. Cap. 6.4).

Sempre in ambito OSCE, attivo supporto è stato inoltre fornito dall'Agenzia al MAECI, nell'implementazione delle *Confidence Building Measures*. In particolare:

- la n. 14[37], nell'ambito della quale l'ACN ha potuto presentare alcune esperienze nazionali in materia di *partnership* pubblico-privato illustrando, in particolare, quelle in materia di formazione, tra cui il citato progetto realizzato con la Regione Lazio (ACL) e la realizzazione della rete di coordinamento nazionale degli Istituti Tecnologici Superiori (ITS *Academy*) per la transizione digitale;

- la n. 15[38], rispetto alla quale l'ACN ha contribuito al rapporto "*Cyber Incident Classification: A Report on Emerging Practices within the OSCE region*", che compendia le pratiche nazionali per la classificazione degli incidenti *cyber*, identificando le procedure comuni tra gli Stati partecipanti dell'OSCE.

[37] «Gli Stati partecipanti, su base volontaria e conformemente alla legislazione nazionale, promuoveranno partenariati pubblico-privati e svi lupperanno meccanismi per lo scambio di migliori prassi per quanto concerne le risposte alle sfide comuni alla sicurezza derivanti dall'uso delle TIC.». Misura adottata da Italia, Austria, Belgio, Estonia, Finlandia e Svezia.

[38] «Gli Stati partecipanti, su base volontaria, incoraggeranno, faciliteranno e/o parteciperanno alla cooperazione regionale e subregionale tra autorità legalmente autorizzate che sono preposte alla protezione delle infrastrutture critiche, al fine di discutere le opportunità e affrontare le sfide alle reti nazionali e transfrontaliere di TIC da cui dipendono tali infrastrutture critiche.».

L'Agenzia, infine, in qualità di punto di contatto (PoC) tecnico, ha preso parte, in raccordo con il MAECI, al periodico *communication check*, svoltosi dal 3 al 6 ottobre 2022 e volto a testare la prontezza nella risposta da parte dei PoC nazionali e facilitare l'interazione tra organismi nazionali competenti ed esperti.

Nel contesto delle attività multilaterali, l'Agenzia ha coordinato la partecipazione nazionale alla ***Counter Ransomware Initiative*-CRI**, iniziativa promossa dallo *US National Security Council* al fine di consolidare la cooperazione internazionale nel contrasto ai *ransomware*, minaccia sempre più pervasiva e impattante nel panorama *cyber*. Le attività erano già state avviate nell'ottobre 2021 con la riunione virtuale dei Ministri e dei rappresentanti di 31 Stati e dell'UE – per l'Italia era presente il Direttore generale dell'ACN – in esito alla quale il nostro Paese ha appoggiato un *joint statement* per il contrasto alla minaccia *ransomware* lungo quattro direttrici: *resilience*; *countering illicit finance*; *disruption* (a livello di *law enforcement*) e *diplomacy.* Successivamente, nel 2022, sono stati costituiti gruppi di lavoro – presidiati per l'Italia dall'Agenzia, nel ruolo di coordinatore, nonché, per i rispettivi profili di competenza, da MAECI, Ministero dell'interno e MEF. Nell'ambito della CRI, l'Italia ha preso parte a una specifica esercitazione, la RRE (vds. Cap. 3.4.2). Le attività sono poi culminate con il vertice tenutosi a Washington dal 31 ottobre al 1° novembre, alla presenza di 36 Stati e dell'Unione europea, cui l'Italia ha preso parte con una delegazione guidata dal Direttore generale dell'ACN. In tale occasione i partecipanti hanno confermato l'impegno nella lotta al *ransomware* con la sottoscrizione di un nuovo *joint statement*, che prevede: l'istituzione di una *task force* internazionale (*International Counter Ransomware Task Force*), finalizzata a favorire le sinergie tra i diversi domini coinvolti e rendere più operativo il consesso; la ricerca di un maggiore coinvolgimento del settore privato, anche attraverso lo sviluppo di una piattaforma per lo scambio informativo e di strumenti di *capacity building*; lo svolgimento di esercitazioni *cyber* su base biennale.

Nel contesto dell'**Unione europea**, l'Agenzia ha assicurato, in stretto raccordo con il MAECI, la partecipazione ai lavori dell'*Horizontal Working Party on Cyber Issues* (HWPCI), gruppo di lavoro del Consiglio dell'UE nel quale sono discusse la politica e le attività legislative in materia di cybersicurezza. In quel consesso, sono stati trattati, in particolare, anche in coordinamento con le altre Amministrazioni nazionali competenti, i temi relativi a:

- il negoziato, nel corso del trilogo, per giungere all'accordo politico sulla Direttiva NIS2 (vds. Cap. 4.5);

- l'avvio del negoziato relativo al *Cyber Resilience Act*;
- il negoziato relativo alla proposta di Regolamento che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione per addivenire al cd. *general agreement* del Consiglio;
- le *Council Conclusions on developing the Union's cyber posture, c.d. Cyber Posture*;
- le *Council Conclusions on the Special Report No. 03/2022 by the European Court of Auditors* intitolato "*5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved*";
- le *Council Conclusions on ICT supply chain security*;
- la Raccomandazione del Consiglio su un approccio coordinato dell'Unione per rafforzare la resilienza delle infrastrutture critiche;
- lo sviluppo della gestione crisi *cyber*, sostenendo le iniziative già avviate e sviluppando delle analisi circa gli elementi mancanti o che richiedono ulteriore sviluppo.

Box 10

CYBER RESILIENCE ACT

Lo schema del regolamento CRA ha il fine di armonizzare i requisiti di cybersicurezza per i prodotti con elementi digitali e rimuovere gli ostacoli alla libera circolazione delle merci. A tal fine, sono stati individuati quattro obiettivi specifici:

1. garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita secondo un approccio di *security by design*;
2. garantire un quadro coerente in materia di cybersicurezza, facilitando la conformità per i produttori di *hardware* e *software*;
3. migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali;
4. consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

La proposta trae le basi dalla Strategia dell'Unione europea per la cybersicurezza per il decennio digitale, che evidenzia come sia fondamentale garantire che i componenti *hardware* e *software* prodotti nell'UE e nei Paesi terzi, usati da servizi e infrastrutture critiche e dai dispositivi mobili, siano affidabili, sicuri e garantiscano la protezione dei dati personali. Per costruire un mercato unico dei prodotti ICT sicuro è quindi necessario che tutti, nella catena di approvvigionamento (produttori, sviluppatori di *software*, fornitori di servizi della società dell'informazione) facciano della cybersicurezza una priorità. Sono, inoltre, necessari adeguati requisiti, che devono essere rispettati lungo tutta la catena di approvvigionamento dei prodotti ICT utilizzati in Europa.

Box 11

REGOLAMENTO SULLA CYBERSICUREZZA DELLE ISTITUZIONI, DEGLI ORGANI E DELLE AGENZIE UE

La proposta di Regolamento avanzata dalla Commissione istituisce un quadro per garantire norme e misure comuni in materia di cybersicurezza nelle Istituzioni, negli Organi e nelle Agenzie dell'Unione (c.d. EUIBA) allo scopo di migliorare le capacità di resilienza e di risposta agli incidenti.

Il Regolamento rappresenterà un'importante occasione per consentire alle EUIBA di allinearsi, in maniera orizzontale e omogenea, alle migliori pratiche realizzate dagli Stati membri. Inoltre, la proposta, attualmente in fase di negoziato, rivede il quadro giuridico relativo al CERT-UE e tiene conto degli sviluppi e dell'aumento della digitalizzazione nelle EUIBA negli ultimi anni e dell'evolversi del panorama della minaccia *cyber*.

Il negoziato in Consiglio ha permesso di definire con maggior precisione le aree di intervento e le finalità del regolamento e individuare efficaci modalità di allineamento rispetto alle previsioni della direttiva NIS2, la quale si applica anche alla Pubblica Amministrazione centrale degli Stati membri.

Box 12

UN APPROCCIO COORDINATO DELL'UNIONE PER RAFFORZARE LA RESILIENZA DELLE INFRASTRUTTURE CRITICHE

In stretto raccordo con l'UCM, è stata negoziata, per quanto concerne i profili di cyber resilienza, la Raccomandazione del Consiglio recante "*Union-wide coordinated approach to strengthen the resilience of critical infrastructure*". Questa evidenzia la necessità di accelerare e, se del caso, anticipare, le previsioni delle direttive CER e NIS2, nonché di implementare senza ritardo le altre iniziative in materia di protezione delle infrastrutture critiche, nel dominio fisico e *cyber*. Per quanto attiene alla cybersicurezza viene richiesto di: dotarsi di una regolamentazione adeguata; aggiornare le strategie di cybersicurezza nazionali; sfruttare la piattaforma offerta dall'ECCC (vds. par. 7.3); avvalersi dei servizi di cybersicurezza offerti da ENISA; assicurare la partecipazione a CyCLONe; rafforzare il CSIRT nazionale; impegnarsi nelle azioni discendenti della *Nevers Call* e delle Conclusioni del Consiglio sulla *Cyber Posture*.
La raccomandazione, inoltre, prospetta lo svolgimento di *stress test* sulle infrastrutture critiche e impegna la Commissione a fornire il supporto di competenza, nonché a produrre in tempi rapidi una proposta per il fondo UE di emergenza per la cybersicurezza (*Cybersecurity Emergency Response Fund*).

Sempre a livello UE, l'Agenzia ha designato propri rappresentanti che, in qualità di delegati nazionali, siedono nell'ambito del *Management Board* dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA), quale organo di governo interno. L'ACN ha altresì designato proprio personale nella veste di *National Campaign Coordinator* delle iniziative per la promozione della cybersicurezza nell'ambito del mese europeo della sicurezza informatica, nonché di *National Liaison Officer* (NLO), con il compito di agevolare la condivisione di informazioni tra ENISA e gli Stati membri e nel supportare l'Agenzia europea nella diffusione delle sue attività e dei relativi risultati.

In quest'ultima veste, anche nell'ambito di dedicati gruppi di lavoro istituiti all'interno della rete degli NLO, i delegati dell'ACN hanno contribuito a:

- elaborare lo *European Cyber Security Index*, volto a valutare e incrementare – in linea con la Strategia di Sicurezza Cibernetica dell'Unione e con il relativo contesto normativo[39] – i livelli di maturità dell'Unione e degli Stati membri nelle seguenti aree: *policy*, capacità, operatività, sviluppo del mercato e del settore industriale. Da ultimo, l'Agenzia ha preso parte alla fase pilota dell'esercizio, che verrà avviato ufficialmente nella seconda metà del 2023;
- fornire elementi sugli aspetti di *governance* concernenti l'implementazione della Strategia nazionale di cybersicurezza, riversati da ENISA nel rapporto "*Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies*";
- testare il prototipo della piattaforma InfoHUB sviluppata dall'Agenzia europea, destinata a fornire al pubblico informazioni (notizie, eventi, statistiche) in materia di cybersicurezza, disponibili in diverse lingue dell'UE;
- elaborare osservazioni e riscontri su rapporti e studi di volta in volta elaborati dall'Agenzia europea.

L'ACN ha inoltre preso parte attiva ai lavori del Gruppo di Cooperazione NIS (NIS *Cooperation Group*-NISCG), istituito dalla Direttiva NIS, volto al rafforzamento della cooperazione e dello scambio informativo relativo alle *policy* di cybersicurezza tra Paesi dell'Unione. Oltre a presidiare le **4 riunioni** plenarie trimestrali del NISCG svoltesi nel periodo di riferimento, l'Agenzia ha coordinato, in qualità di co-presidente, le attività del *Work Stream on Large Scale Cyber Incident and Crisis* (WSLSCIC) del *Work Stream on 5G Cybersecurity* (WS5G), nonché del neo

[39] In particolare, con il *Cyber Security Act* e la Direttiva NIS 2.

costituito *work stream* dedicato all'implementazione di quanto previsto dalle citate Conclusioni del Consiglio sulla *Cyber Posture*, prendendo parte a **14 incontri di coordinamento** e presenziando a **6 riunioni plenarie**.

Inoltre, è stata assicurata la partecipazione, d'intesa con le Autorità di settore interessate, a **15 ulteriori riunioni** relative:

- al *Work Stream on Cyber Risk and Vulnerability Management;*
- al *Work Stream on Digital Service Providers;*
- al *Work Stream on Digital Infrastructures;*
- al *Work Stream on Energy;*
- al *Work Stream on Incident Reporting;*
- al *Work Stream on Supply Chain Security;*
- alla *Coordinated Vulnerability Disclosure Task Force;*
- al *WS5G Subgroup on Standardization and Certification.*

FIGURA 45 – RIUNIONI DEL NIS *COOPERATION GROUP*-NISCG

Oltre alle specifiche tematiche dei gruppi di lavoro, in quei consessi sono stati trattati, in particolare, i seguenti temi:

- lo sviluppo della gestione crisi *cyber*;
- il confronto con l'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (ACER) circa il *Network Code for cybersecurity aspects of cross-border electricity flows*;
- l'implementazione delle raccomandazioni di competenza espresse dalla *European Court of Auditors* nella relazione "*5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved*", tra cui l'aggiornamento dello stato di attuazione del *Toolbox* di cybersicurezza per il 5G;
- l'analisi del rischio e la formulazione di raccomandazioni per il settore delle telecomunicazioni in senso lato, come richiesto con la c.d. *Nevers Call* dai Ministri UE delle telecomunicazioni a marzo 2022. In tale contesto, è stato elaborato un questionario somministrato, a livello nazionale, agli operatori di settore, i cui esiti sono stati aggregati dall'Agenzia e trasmessi al NISCG per la successiva analisi a livello europeo, svolta con il supporto di ENISA;
- la definizione degli scenari di rischio *cyber* a cui è esposta l'Unione prevista dalle citate Conclusioni del Consiglio sulla *Cyber Posture*;
- la preparazione all'attuazione della Direttiva NIS2.

In tema di risposta coordinata a incidenti e crisi cibernetiche su larga scala, essa ha occupato una parte significativa dell'agenda europea in materia *cyber*, con numerose iniziative che si sono susseguite a livello di Consiglio e di Commissione.

Al riguardo, il quadro di riferimento è fornito dalla Raccomandazione UE 2017/1584 (cd. *Blueprint*), che organizza la cooperazione su tre livelli:

- politico, che gestisce la risposta strategica alle crisi, adottando, ad esempio, misure diplomatiche, nella più ampia cornice dei dispositivi integrati per la risposta politica alle crisi (*Integrated Political Crisis Response Mechanism*-IPCR) del Consiglio dell'Unione europea;
- operativo, implementato tramite una rete europea per la gestione coordinata degli incidenti e delle crisi *cyber* transfrontalieri su vasta scala (C*yber Crisis Liaison Organisation Network*-CyCLONe), promossa congiuntamente nel 2020 da Italia e Francia;
- tecnico, per il monitoraggio degli incidenti di elevata criticità e l'analisi delle minacce e dei rischi cibernetici, tramite le funzioni svolte dal c.d. CSIRT *Network*.

Nel corso del 2022, si è quindi osservata una progressiva maturazione dei meccanismi esistenti,

nonché l'avvio di attività volte a rendere organica la risposta dell'Unione, con un maggior coinvolgimento di istituzioni e agenzie europee e un rafforzamento della cooperazione tra le comunità di *cyber-resilience e cyber-diplomacy*.

L'Italia, coerentemente al quadro delineato dal legislatore europeo, si è dotata di un'architettura nazionale di cybersicurezza strutturata sui livelli politico, operativo e tecnico, in cui assume particolare rilevanza il ruolo dell'ACN. In seno all'Agenzia, infatti, sono incardinate sia la struttura di livello tecnico (CSIRT Italia), sia quella di livello operativo (NCS), e ad essa sono attribuiti i ruoli di Autorità nazionale competente e Punto di contatto unico per le finalità di cui al D.Lgs. NIS. L'ACN è inoltre referente nazionale per CyCLONe, anche ai fini della potenziale attivazione dei meccanismi previsti dall'IPCR.

In tale contesto, l'Agenzia ha preso parte alle 4 riunioni plenarie di CyCLONe e ha co-coordinato il *Working Group on Standard Operating Procedures* (WGSOP) di CyCLONe, partecipando a 10 riunioni di coordinamento con la Presidenza di turno e 7 incontri con i *partner* europei. Il WGSOP ha prodotto un aggiornamento delle procedure interne nel primo semestre del 2022, incorporandovi le lezioni apprese in relazione alla compromissione di *SolarWinds* e di *Microsoft Exchange*, nonché dalla gestione delle tensioni derivanti dall'attuale scenario internazionale. Una seconda revisione è poi stata portata a termine tenendo conto delle lezioni apprese nel corso di *Cyber Europe* 2022 (vds. par. 3.4.2). Il livello di visibilità della rete, inoltre, ha determinato la necessità di un significativo coordinamento circa le attività esercitative nel quale è stato richiesto il coinvolgimento di CyCLONe.

Al contempo, l'ACN ha partecipato ai lavori del gruppo che sovraintende il coordinamento della Rete europea dei CSIRT, riunitosi in 3 riunioni plenarie per promuovere, anch'esso, lo sviluppo delle procedure operative *standard*, ma ad un ritmo meno serrato in ragione della maggiore maturità di questo consesso rispetto a CyCLONe, nonché per definire la programmazione e pianificazione delle esercitazioni di carattere tecnico/procedurali utili a rafforzare la preparazione degli Stati membri in materia di gestione degli incidenti.

Infine, il decreto legislativo 3 agosto 2022, n. 123 – all'elaborazione del quale l'ACN ha lavorato congiuntamente all'allora MiSE – nello stabilire misure volte ad adeguare la normativa nazionale al nuovo quadro europeo di certificazione della cybersicurezza – introdotto mediante le

disposizioni del Titolo III del Regolamento (UE) 2019/881 – definisce ulteriormente le attività di ACN quale Autorità nazionale di certificazione per la cybersicurezza.

Nell'esercizio di tali funzioni, coerentemente con il più volte citato passaggio di competenze dal MiSE all'ACN, l'Agenzia ha partecipato ai lavori dello *European Cybersecurity Certification Group* (ECCG).

In particolare, il personale di ACN ha preso parte al *workshop certification week* di ENISA tenutosi a Bruxelles dal 22 al 24 novembre 2022 e all'incontro dell'ECCG del 25 novembre 2022 a Bruxelles. Durante il *workshop* è stato presentato da ENISA lo stato delle attività per l'elaborazione dei nuovi sistemi europei di certificazione della cybersicurezza, con particolare riferimento agli European *Common Criteria*-EUCC, *European Cloud Services* (EUCS) e *European* 5G *networks* (EU5G), presentando la politica di transizione al nuovo standard *Common Criteria* 2022 (CC:2022) adottato nell'ambito degli accordi di mutuo riconoscimento internazionale (CCRA).
Durante il citato incontro dell'ECCG, la Commissione europea ha discusso lo stato di elaborazione dei citati sistemi di certificazione (EUCC, EUCS ed EU5G), aggiornando i lavori sui prossimi sviluppi per l'adozione dell'atto di esecuzione per lo schema EUCC, al primo semestre del 2023.

7.3 Centro Nazionale di Coordinamento

È istituito presso l'ACN il Centro Nazionale di Coordinamento (NCC), quale interfaccia verso il Centro di competenza europeo in *cybersecurity* (**ECCC**) di cui al Regolamento (UE) 2021/887, con l'obiettivo di concentrare gli investimenti in sviluppo industriale, tecnologico e della ricerca in *cybersecurity* e per l'attuazione di progetti e iniziative in tali ambiti.

In particolare, la missione dell'ECCC è quella di:

- potenziare l'autonomia strategica dell'UE in materia di cybersicurezza;
- sostenere le capacità, i mezzi e le competenze *cyber* dell'UE nell'ambito industriale, tecnologico e della ricerca;
- aumentare la competitività globale dell'industria *cyber* europea, garantendo *standard* elevati e trasformando la cybersicurezza in un vantaggio competitivo per altri settori industriali dell'Unione.

A tal fine, l'ECCC attua le azioni relative alla cybersicurezza contenute nei programmi di finanziamento ***Horizon Europe*-HEU** e ***Digital Europe*-DEP** [40].

In particolare, nel periodo di riferimento, l'NCC ha monitorato costantemente le progettualità in corso, veicolando alcune opportunità ai settori di interesse e avviando un percorso di divulgazione e supporto per le realtà pubbliche e private nazionali che intendono applicare alle *call* europee.

Nello specifico, nell'assicurare l'attuazione delle funzioni a questo assegnate dal Regolamento (UE) 2021/887, l'NCC ha rappresentato l'Italia presso il **Governing Board** dell'ECCC, partecipando attivamente alle sue attività e a quelle realizzate dai *Working Group* istituiti al suo interno (tra cui quelli relativi all'avvio della *Community* dell'ECCC e all'agenda strategica del Centro). Nel 2022 hanno, infatti, avuto inizio gli incontri in presenza del *Board*, a cui hanno partecipato, in qualità di rappresentanti nazionali, due designati di ACN nominati con il DPCM 28 febbraio 2022. Tra le attività di maggior rilievo portate avanti dal *Governing Board* nel corso del 2022 vi sono l'adozione del *budget* pluriennale dell'ECCC per i periodi 2022-2024 e 2023-2025, nonché l'approvazione della normativa interna e procedurale, funzionale ad assicurare la piena operatività del Centro.

L'NCC ha, inoltre, ottenuto il riconoscimento da parte della Commissione UE della propria capacità di gestire fondi UE, prerequisito essenziale per poter partecipare ai progetti europei e ricevere il relativo supporto finanziario dall'ECCC.

Sono state, altresì, avviate le istruttorie per la predisposizione delle proposte progettuali per rispondere a due *Call for projects* 2022 in ambito *Digital Europe* ("*Deploying the Network Of National Coordination Centres With Member States*" e "*Capacity building of Security Operation Centres*"), individuate come prioritarie per supportare la prima fase di *start-up* dell'Agenzia nel corso del 2022. In particolare, la prima è volta a supportare la piena capacità operativa dell'NCC, mentre la seconda è volta a sviluppare, a livello UE, le progettualità in materia *Security Operation Center* (SOC), già avviate a livello nazionale con il PNRR.

Importante è stata l'attività di promozione e monitoraggio della partecipazione nazionale ai progetti europei gestiti dall'ECCC. In particolare, con riferimento alle attività di promozione, l'NCC ha avviato una serie di interlocuzioni, a livello nazionale, per avviare iniziative congiunte di comunicazione sui programmi di finanziamento *Digital Europe* e *Horizon Europe* veicolati dall'ECCC.

Parallelamente sono state svolte attività di comunicazione e disseminazione sulle proprie attività, nonché sulle principali azioni e risultati dell'ECCC, della rete di NCC e della *Community* mediante il

[40] Per il 2022, l'ECCC ha implementato esclusivamente le azioni del DEP.

sito *web* dell'Agenzia – su cui è presente una pagina dedicata alle attività dell'NCC, costantemente alimentata e aggiornata – e i suoi canali *social* – con particolare riferimento al profilo LinkedIn dell'ACN, su cui sono regolarmente postate le notizie di maggior rilievo in tali ambiti. Ciò anche al fine di promuovere la partecipazione degli *stakeholder* che compongono l'ecosistema nazionale di cybersicurezza alle attività dell'ECCC, della rete di NCC e della *Community*.

Numerosi sono stati gli incontri bilaterali con la Commissione UE e con gli altri NCC, principalmente finalizzati alla condivisione di informazioni e buone pratiche, nonché allo sviluppo di iniziative di collaborazione anche nell'ambito di progetti europei gestiti dall'ECCC.

Sono, infine, state avviate le attività per la definizione di procedure volte a consentire il pieno esercizio della funzione di punto di contatto nazionale per la *Community*, anche con riferimento alla ricezione e valutazione delle richieste di partecipazione alla stessa da parte degli enti nazionali.

Dati NCC 2022	
Budget DEP *Cybersecurity Work Programme* 2021-2022	269M€
Riunioni del *Governing Board* nel 2022	4 + 4 *ad hoc meetings*
Working Groups attivi del *Governing Board*	7
Altre riunioni/*webinar*/*workshop*	21

FIGURA 46 – ATTIVITA' DEL CENTRO NAZIONALE DI COORDINAMENTO

08.

ACRONIMI

Acronimi

A	ACL	Accademia di cybersicurezza Lazio
	AgID	Agenzia per l'Italia digitale
B	BGP	*Border Gateway Protocol*
	Blue OLEx	*Blueprint Operational Level Exercise*
C	CCCS	*Canadian Centre for Cyber Security*
	CCDB	*Common Criteria Development Board*
	CCRA	*Common Criteria Recognition Arrangement*
	CERT	*Computer Emergency Response Team*
	CIC	Comitato interministeriale per la cybersicurezza
	CINI	Consorzio interuniversitario nazionale di informatica
	CNAIPIC	Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche
	CSIRT	*Computer Security Incident Response Team*
	CV	Centro di valutazione
	CVCN	Centro valutazione e certificazione nazionale
	CyCLONe	*Cyber Crises Liaison Organisation Network*

D	**DAIT**	Dipartimento per gli affari interni e territoriali
	DDoS	*Distributed Denial of Service*
	DEP	*Digital Europe Programme*
	DoS	*Denial of Service*
	DTD	Dipartimento trasformazione digitale
E	**EAL**	*Evaluation Assurance Level*
	ECCC	*European Cybersecurity Competence Centre*
	ECCG	*European Cybersecurity Certification Group*
	ENISA	*European Network and Information Security Agency*
	EU CyCLEs	*Eu Cyber Crisis Linking Exercise on Solidarity*
	EU5G	*European 5G Networks*
	EUCC	*European Common Criteria*
	EUCS	*European Cloud Services*
	EUIBA	*EU Institutions, Bodies and Agencies*
H	**HWPCI**	*Horizontal Working Party on Cyber Issues*
I	**ICT**	*Information Communication Technology*
	IILA	Organizzazione internazionale italo-latino americana
	IPCR	*Integrated Political Crisis Response*
	ISAC	*Information Sharing and Analysis Center*

I	ITS	Istituti tecnologici superiori
K	KPI	*Key Performance Indicator*
L	LAP	Laboratori accreditati di prova
	LVS	Laboratori di valutazione della sicurezza
M	MAECI	Ministero degli affari esteri e della cooperazione internazionale
	MEF	Ministero dell'economia e delle finanze
	MiSE	Ministero dello sviluppo economico
	MUR	Ministero dell'università
N	NCS	Nucleo per la cybersicurezza
	NIS	*Network Information Security*
	NISCG	NIS *Cooperation Group*
	NISP	Nucleo interministeriale situazione e pianificazione
	NLO	*National Liaison Officer*
O	OCSI	Organismo di certificazione della sicurezza informatica
	OSCE	Organizzazione per la sicurezza e la cooperazione in Europa

P	PACE	*Parallel and Coordinated Exercise*
	PAC	Pubbliche amministrazioni centrali
	PNRR	Piano nazionale di ripresa e resilienza
	POC	Punto di contatto
	PSNC	Perimetro di sicurezza nazionale cibernetica
R	RRE	*Ransomware Resilience Exercise*
S	SERICS	*Security and Rights in Cyberspace*
	SIEL	Sistema informativo elettorale
	SOC	*Security Operation Center*
T	TUE	Trattato sull'Unione europea
W	WGSOP	*Work Group on Standard Operating Procedures*
	WS5G	*Work Stream on 5G Cybersecurity*


REPVBBLICA ITALIANA
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT