2021

RELAZIONE ANNUALE AL PARLAMENTO

ai sensi dell'art. 14, comma 1, del D.L. 14 giugno 2021, n. 82

Sommario

Premessa

Il decreto-legge 14 giugno 2021, n. 82, nel procedere al riordino delle competenze in materia di cybersicurezza precedentemente poste in capo a una pluralità di attori istituzionali, ha disposto l'istituzione dell'Agenzia per la cybersicurezza nazionale, quale Autorità nazionale per la cybersicurezza.

Il citato decreto-legge, inoltre, dispone precisi oneri informativi nei confronti del Parlamento, prevedendo, tra l'altro, che il Presidente del Consiglio dei ministri presenti una relazione al Parlamento sulle attività svolte dall'Agenzia nell'anno precedente.

Mentre il termine di scadenza "ordinario" della Relazione annuale è Mentre il termine di scadenza "ordinario" della relazione annuale è fissato, dall'art. 14, comma 1, del decreto-legge, al 30 aprile successivo all'anno di riferimento, in sede di prima applicazione, il termine di trasmissione al Parlamento è fissato, ai sensi dell'articolo 17, comma 10-bis, al 30 novembre 2022.

La presente Relazione, pertanto, nell'assolvere ai citati obblighi informativi, illustra le attività svolte dall'Agenzia nell'arco temporale che si estende dal 1° settembre al 31 dicembre 2021.

Nel prosieguo, dopo aver sinteticamente descritto la ridefinizione dell'architettura nazionale *cyber*, si darà atto della strutturazione iniziale dell'ACN e di quanto realizzato nella fase di cd. prima operatività (capitolo 1). La Relazione darà conto delle attività di resilienza svolte a tutela degli interessi nazionali nel campo della cybersicurezza, nonché di quelle in relazione alla prevenzione e preparazione a eventuali situazioni di crisi (capitolo 2) e passerà in rassegna le iniziative per lo sviluppo della resilienza delle infrastrutture tecnologiche del Paese (capitolo 3). Da ultimo, verranno descritte le attività svolte nell'ambito della cooperazione internazionale in materia di cybersicurezza (capitolo 4).

#1

Ridefinizione dell'architettura nazionale

Ridefinizione dell'architettura nazionale

Nel solco delle iniziative, che, già a partire dal 2013, hanno promosso lo sviluppo e il rafforzamento delle capacità nazionali in materia di cybersicurezza, il decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109 (d'ora innanzi decreto-legge), ha proceduto al riordino dell'architettura nazionale *cyber* e istituito l'Agenzia per la cybersicurezza nazionale.

L'istituzione dell'Agenzia mira a razionalizzare e semplificare, nel rispetto delle prerogative attribuite dalla normativa vigente ad altre Amministrazioni, il novero delle competenze in materia di cybersicurezza – precedentemente poste in capo a una pluralità di soggetti istituzionali – con l'obiettivo di garantire l'unicità di indirizzo e di azione rispetto ad un'area di intervento per definizione complessa e ramificata. Ciò al fine di innalzare il livello di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Il decreto-legge definisce, pertanto, il nuovo ecosistema nazionale di cybersicurezza. Esso include:

- il **Presidente del Consiglio dei ministri**, che esercita l'alta direzione e detiene la responsabilità generale delle politiche di cybersicurezza. Il Presidente può delegare le funzioni a lui attribuite in via non esclusiva all'**Autorità delegata per la sicurezza della Repubblica**, di cui all'art. 3 della L. 3 agosto 2007, n. 124;

- il **Comitato interministeriale per la cybersicurezza-CIC**, istituito presso la Presidenza del Consiglio dei ministri, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Il Comitato è presieduto dal Presidente del Consiglio dei ministri e, ai sensi del decreto-legge, è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico (ora "delle imprese e del *made in Italy*"), dal Ministro della transizione ecologica (ora "dell'ambiente e della sicurezza energetica"), dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale (non previsto a livello di Ministro nell'attuale Governo) e dal Ministro delle infrastrutture e della mobilità sostenibili (ora "delle infrastrutture e dei trasporti"). Il Direttore generale dell'ACN svolge le funzioni di segretario del Comitato;

- l'**Agenzia per la cybersicurezza nazionale-ACN**, designata quale Autorità nazionale per la cybersicurezza e deputata alla salvaguardia della cybersicurezza e della resilienza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;

- i **Ministeri e le istituzioni** con competenze trasversali in ambito *cyber* che interagiscono con l'ACN-Autorità nazionale per la cybersicurezza;

- il **Nucleo per la cybersicurezza-NCS**, consesso interministeriale, istituito presso l'ACN e presieduto dal suo Direttore generale, che supporta il Presidente del Consiglio nella materia della cybersicurezza per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il Nucleo formula proposte di iniziativa in materia di cybersicurezza e costituisce una piattaforma di cooperazione a livello operativo anche sulle tematiche di *policy*;

- gli **operatori economici privati**, l'**accademia** e la **ricerca** e, non ultima, la **società civile**, considerati elementi imprescindibili per la resilienza del sistema-Paese e, pertanto, parte dell'ecosistema nazionale di cybersicurezza. In tal senso, un ruolo centrale è affidato allo strumento del partenariato pubblico-privato, essenziale per innalzare la resilienza e tramite il quale l'ACN "accompagna" anche le aziende nazionali verso l'efficace applicazione della normativa settoriale *cyber* e dei relativi obblighi e misure.

In tale contesto, l'ACN assicura il coordinamento tra i soggetti pubblici nazionali coinvolti nella materia della cybersicurezza e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore.

Più in particolare, nella rinnovata architettura istituzionale, l'ACN ha assunto un ruolo centrale anche per l'attuazione della normativa relativa al **Perimetro di sicurezza nazionale cibernetica-PSNC** di cui al decreto-legge 21 settembre 2019, n. 105 (cd. D.L. Perimetro). Il decreto-legge, infatti, assegna all'ACN le funzioni regolamentari, di certificazione, ispezione, vigilanza e sanzionatorie, precedentemente attribuite a Dipartimento delle informazioni per la sicurezza-DIS, MiSE (ora Ministero delle imprese e del *made in Italy*) e Presidenza del Consiglio dei ministri-MITD (approfondimento nel prosieguo della Relazione, nella sezione dedicata al Perimetro di sicurezza nazionale cibernetica).

L'ACN, inoltre, è designata:

- Autorità nazionale competente in via esclusiva e punto di contatto unico per le finalità della normativa sulla sicurezza delle reti e dei sistemi informativi di cui alla Direttiva (UE) NIS;

- Autorità nazionale di certificazione della cybersicurezza;

- Centro Nazionale di Coordinamento, in attuazione del Regolamento (UE) 2021/887, che ha istituito il Centro europeo di competenza in *cybersecurity*-ECCC e la rete dei Centri nazionali di coordinamento-NCC.

Dal quadro sopra delineato, appare chiaro come, alla luce dell'esperienza accumulata nei precedenti cinque anni di lavoro nel contesto della normativa previgente[1], la riforma ha riconosciuto autonoma dignità alla sicurezza e alla resilienza cibernetica ponendole sotto la responsabilità del Presidente del Consiglio dei ministri a fondamento del processo di digitalizzazione del Paese.

Per tale ragione, nell'ambito delle proprie attività istituzionali, l'ACN esercita le funzioni di coordinamento ad essa attribuite dalla legge tramite un'azione sinergica che coinvolge tutte le Amministrazioni con competenze istituzionali in materia, e, più in particolare:

- le Forze di polizia, cui spetta la prevenzione e la repressione dei reati informatici;
- il Ministero della Difesa, che assicura la difesa e la sicurezza militare dello Stato nello spazio cibernetico;
- gli Organismi di informazione per la sicurezza, che mantengono la prerogativa esclusiva delle attività di ricerca ed elaborazione informativa;
- il Ministero degli affari esteri e della cooperazione internazionale, cui fanno capo le funzioni di *cyber diplomacy*, volte al conseguimento degli interessi nazionali del Paese nello spazio cibernetico nella più ampia cornice della politica estera nazionale.

In tal senso, la riforma mira ad assicurare la coerenza delle iniziative, l'efficientamento della spesa, la capacità di fornire un chiaro e aggiornato quadro situazionale all'Autorità politica, nonché identificare un'unica interfaccia incaricata del coordinamento tra i soggetti pubblici coinvolti in materia di sicurezza cibernetica e resilienza, anche al fine di garantire, nei consessi internazionali, una postura nazionale unitaria e coerente con le politiche in materia di cybersicurezza definite dal Presidente del Consiglio dei ministri.

A completamento del quadro sopra delineato, la Strategia nazionale di cybersicurezza 2022-2026 – adottata dal Presidente del Consiglio a maggio 2022 e alla cui redazione l'ACN ha iniziato a lavorare già nel periodo in esame – ha individuato 3 obiettivi fondamentali (protezione, risposta e sviluppo) e una serie di fattori abilitanti (cooperazione e formazione, promozione della cultura della sicurezza) che consentiranno al sistema-Paese di affrontare le sfide connesse al processo di digitalizzazione. Le relative misure (82), funzionali ad assicurare la concreta attuazione della strategia, sono state raggruppate per aree tematiche nel Piano di implementazione annesso al citato documento strategico.

[1] Di cui al DPCM 17 febbraio 2017 ("Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali").

Strutturazione dell'Agenzia e prima operatività

La nascita dell'Agenzia a livello normativo, avvenuta il 14 giugno 2021, è stata quasi contestuale all'avvio della sua operatività, il 1° settembre 2021.

Allo scopo di assicurare sin da subito la funzionalità dell'Agenzia, a poche settimane dalla conversione in legge del D.L. n. 82/2021, il DIS ha messo a disposizione una prima aliquota di personale ai sensi dell'art. 17, comma 8, lett. *a)*, che è stata progressivamente ampliata e integrata anche da personale messo a disposizione da altre amministrazioni dello Stato.

In particolare, a valle dell'adozione del DPCM 16 settembre 2021 – che ha disposto il trasferimento all'ACN delle funzioni in materia di cybersicurezza già assicurate dal DIS e di cui si darà atto nel prosieguo della Relazione – l'Agenzia, al fine di esercitare le plurime e complesse attività connesse al proprio mandato istituzionale, nelle more dell'adozione dei Regolamenti interni, anche tenuto conto del personale e delle competenze disponibili, ha proceduto all'attivazione transitoria delle Funzioni:

- **Gabinetto**, responsabile per gli affari giuridico-legislativi, i rapporti interistituzionali (comprese le Segreterie del Comitato interministeriale per la cybersicurezza-CIC, del Nucleo per la cybersicurezza-NCS e del cd. Tavolo attuazione Perimetro), la cooperazione internazionale e la gestione dei flussi documentali e informativi, degli archivi e del protocollo informatico;

- **Operazioni**, con il ruolo di coordinamento del CSIRT Italia e delle articolazioni tecniche deputate al monitoraggio, analisi e impiego di strumenti tecnici *cyber*, nonché allo scrutinio tecnologico di soluzioni e prodotti ICT;

- **Segreteria e Rapporti istituzionali del Direttore generale**, **Comunicazione istituzionale e Cerimoniale**;

- **Strategia, Programmi e Ricerca**, cui sono state ricondotte le attività in ambito *policy cyber*, progetti e infrastrutture IT e quelle relative al Piano Nazionale di Ripresa e Resilienza-PNRR e allo sviluppo del *cloud* nazionale, nonché i rapporti con lo *European Cybersecurity Competence Centre*.

Successivamente, nell'ottica della graduale attuazione delle funzioni attribuite dal decreto-legge, il 6 ottobre 2021 è stata attivata la Funzione **Risorse umane e strumentali**, incaricata di assicurare la corretta ed efficace gestione del personale, garantire l'applicazione del D.Lgs. 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza sui luoghi di lavoro, sovraintendere, inoltre, alle politiche di bilancio, agli obblighi contabili e agli adempimenti fiscali e gestire le attività di carattere logistico.

Il 30 dicembre 2021, infine, è stata attivata la **Funzione Certificazione e vigilanza**, con il compito di sovraintendere ai processi di certificazione, qualificazione e valutazione, avviare le attività funzionali all'attivazione del Centro di valutazione e certificazione nazionale (illustrato nelle pagine seguenti) presso l'ACN, nonché curare l'attività ispettiva e di verifica.

Inoltre, ai sensi del Decreto del Presidente del Consiglio dei ministri del 6 novembre 2015, n. 5 (così come modificato dal DPCM 2 ottobre 2017, n. 3), è stato istituito presso l'Agenzia l'**Organo centrale di sicurezza**, per la trattazione e la gestione della documentazione classificata.

Nel quadro sopra delineato, la fase di cd. prima operatività dell'Agenzia è coincisa anche con il processo di posizionamento istituzionale, che ha incluso, tra l'altro, la predisposizione di appositi Protocolli d'intesa con altre amministrazioni dello Stato (firmati, poi, nel periodo successivo a quello di riferimento), nonché l'ingaggio delle controparti tecniche sia pubbliche, sia private. In particolare, il 28 dicembre 2021, l'ACN ha aderito al Protocollo d'intesa precedentemente sottoscritto tra la Autorità nazionale anticorruzione (ANAC), l'Autorità garante della concorrenza e del mercato (AGCM), la Banca d'Italia, la Commissione nazionale per la società e la borsa (CONSOB) e l'Istituto per la vigilanza sulle assicurazioni (IVASS), per la gestione in comune delle procedure di appalto congiunte, finalizzato all'individuazione di strategie per l'acquisizione di lavori, servizi e forniture e per il conseguimento di risparmi di spesa.

La fase di cd. prima operatività dell'ACN è stata, inoltre, caratterizzata dall'espletamento di funzioni riferite al proprio mandato istituzionale (inclusi gli scambi, in ambito nazionale, con le altre Amministrazioni coinvolte nella materia e, sul piano della cooperazione internazionale, con le omologhe Autorità *cyber* di altri Paesi), sia da attività direttamente connesse alla nascita dell'amministrazione, riguardanti aspetti di carattere logistico-organizzativo (come, ad esempio, l'attivazione dell'infrastruttura IT e delle postazioni di lavoro, la registrazione del marchio dell'Agenzia e del dominio *web* 'acn.gov.it') e di natura gestionale-amministrativa (quali, ad esempio, la disciplina degli obblighi del personale e la definizione delle procedure di *procurement*).

Inoltre, nel periodo in esame, sul versante della produzione normativa e provvedimentale (concretizzatasi, tra l'altro, nella redazione del DPCM per il trasferimento di funzioni dal Dipartimento delle informazioni per la sicurezza e dei Regolamenti interni), ha assunto particolare rilievo l'elaborazione di 8 pareri su provvedimenti normativi. In particolare, si segnalano, quali più significativi, il parere sull'iniziativa di novella del decreto-legge 15 marzo 2012, n. 21, in relazione alle disposizioni sul ruolo dell'Agenzia previsto dall'articolo 1-bis con riferimento al ricorso al cd. *Golden Power* in materia di tecnologie 5G, nonché quello sul Codice delle comunicazioni elettroniche – decreto legislativo 8 novembre 2021, n. 207 – in merito al ruolo dell'Agenzia in tale ambito.

APPROFONDIMENTO - PRIMA OPERATIVITÀ: SISTEMI IT ACN

Tra le attività svolte dal 15 settembre 2021 al 31 dicembre 2021, rientra anche la progettazione dei primi sistemi informativi dell'Agenzia necessari per il funzionamento dei servizi di base e per migrare i sistemi in trasferimento dalla Presidenza del Consiglio, allo scopo di assicurare la continuità dell'operatività del CSIRT e dei servizi *cyber* collegati.
Per quanto attiene ai servizi di base, l'attività si è concentrata sulla progettazione del *data center*, della rete e del prospetto di distribuzione delle postazioni di lavoro, nonché dell'allestimento delle sale riunioni.

In riferimento ai primi sistemi IT da attivare, si è proceduto alla progettazione del nuovo sito dell'Agenzia, del dominio utenti e del sistema di posta elettronica e *collaboration* (per 150 utenti), nonché della definizione delle *policy* di sicurezza. Inoltre, si è proceduto alla redazione del piano dei fabbisogni per l'attivazione della connettività e dei servizi di fonia, oltre che del supporto alle attività di progettazione, analisi e implementazione dei servizi *cyber* nazionali. Infine, si è proceduto alla progettazione del *data center* e dei sistemi IT per la trattazione delle informazioni classificate.

Per quanto attiene ai beni IT oggetto di trasferimento dalla Presidenza del Consiglio, l'attività si è concentrata sulla definizione del progetto di migrazione dei sistemi. In particolare, si è proceduto ad individuare la soluzione per garantire l'assenza di disservizio, la migrazione dei dati e la migrazione delle utenze esterne (circa 800 tra soggetti pubblici e privati) dei portali esposti (Portale CSIRT 'www.csirt.gov.it', Portale *Collaboration* 'www.portale.csirt.gov.it', Portale Perimetro – 'www.perimetro.csirt.gov.it').

In tale contesto, mediante uno sforzo di sistema improntato alla più stretta collaborazione interistituzionale e reso possibile dall'irrinunciabile contributo, oltre che dell'Agenzia, anche di CIC, COPASIR e Commissioni Parlamentari competenti – sono stati adottati, nel corso della seduta del CIC del 9 dicembre 2021, tre dei quattro regolamenti interni dell'ACN[2]. In particolare, il *Regolamento di contabilità dell'Agenzia per la cybersicurezza nazionale* (DPCM 9 dicembre 2021, n. 222) è stato pubblicato nella Gazzetta Ufficiale del 24 dicembre 2021, mentre il *Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale* (DPCM 9 dicembre 2021, n. 223) e il *Regolamento del personale dell'Agenzia per la cybersicurezza nazionale* (DPCM 9 dicembre 2021, n. 224) in quella del 27 dicembre 2021.

[2] Rimanendo da definire il Regolamento cd. appalti in deroga, ai sensi dell'art. 11, comma 4 del decreto-legge, successivamente adottato nel 2022.

APPROFONDIMENTO - REGOLAMENTI DELL'ACN

Con riferimento al funzionamento dell'Agenzia, il D.L. 82/2021, nel dotare l'ACN di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, ha previsto l'adozione di 4 Regolamenti di attuazione:

1. "Organizzazione e funzionamento" (art. 6);
2. "Contabilità" (art. 11, comma 3);
3. cd. Appalti in deroga (art. 11, comma 4);
4. "Personale" (art. 12).

Al riguardo, il legislatore ha inteso demandare la disciplina di tali materie a veri e propri atti normativi, per i quali sono stati previsti, nell'ambito dei diversi *iter* di adozione, specifici momenti di **controllo parlamentare**: i pareri delle Commissioni parlamentari competenti e quello del COPASIR. In particolare, giova evidenziare come il controllo esercitato da quel Comitato corrisponda all'esigenza di controbilanciare la possibilità che tali discipline siano approvate anche in deroga alle vigenti disposizioni di legge, pur nel rispetto dei principi generali dell'ordinamento giuridico e tenuto conto delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia.

La medesima procedura di adozione ha previsto, inoltre, il coinvolgimento dei Ministri membri del CIC, i quali intervengono nella *governance* della cybersicurezza italiana. Essi, infatti, sono stati "sentiti" dal Presidente del Consiglio dei ministri prima della formale adozione.

Trasferimento di funzioni, risorse umane, beni e dotazioni

Al fine di conferire unitarietà di indirizzo e azione alle politiche in materia di cybersicurezza, il legislatore, nel procedere al riordino dell'architettura nazionale di cybersicurezza, ha disposto, coerentemente con l'istituzione di un'unica Autorità nazionale, il trasferimento di una serie di funzioni precedentemente in capo a una pluralità di soggetti istituzionali.

In tale ottica, in attuazione all'art. 17, comma 5, del decreto-legge, e, in particolare, per dettare termini e modalità volte ad assicurare, mediante opportune intese, la prima operatività dell'Agenzia con l'individuazione di spazi e il trasferimento delle funzioni del DIS all'ACN, nonché per il trasferimento della documentazione, anche di natura classificata, attinente alle funzioni trasferite, è stato adottato il decreto del Presidente del Consiglio dei ministri del 16 settembre 2021.

Con tale provvedimento è stato, pertanto, disposto, con decorrenza dalla medesima data, il passaggio all'ACN delle funzioni in materia di cybersicurezza, incluse quelle volte alla tutela della sicurezza nazionale nello spazio cibernetico, in precedenza assicurate dal DIS, contestualmente alla messa a disposizione di una ulteriore aliquota di personale (addetto all'espletamento delle funzioni oggetto di trasferimento), che ha integrato l'organico già reso disponibile a partire dal 1° settembre. Nella suddetta fase di prima operatività, inoltre, oltre al personale distaccato dal DIS, l'Agenzia si è avvalsa anche del supporto di figure professionali provenienti da altre amministrazioni dello Stato, e, più segnatamente, i Ministeri dell'interno, della giustizia, della difesa e di Banca d'Italia.

Per effetto di tale trasferimento, l'Agenzia ha assunto, altresì, le funzioni derivanti dal decreto-legge 21 settembre 2019, n. 105 recante *Disposizioni urgenti in materia di Perimetro di sicurezza nazionale cibernetica,* cd. decreto Perimento, e dai relativi provvedimenti attuativi (del cui esercizio si darà conto nel prosieguo della Relazione, nella sezione dedicata alla attività di resilienza a tutela degli interessi nazionali nel campo della cybersicurezza), quelle previste dal decreto legislativo 18 maggio 2018, n. 65, di attuazione della Direttiva (UE) 2017/1148 sulla sicurezza delle reti e dei sistemi informativi, cd. Direttiva NIS, ivi incluso il ruolo di punto di contatto unico, nonché in ragione della funzione di coordinamento della cooperazione internazionale in materia attribuita all'Agenzia[3], quelle relative alla definizione delle politiche e alla partecipazione ai consessi multilaterali nei quali vengono discusse tematiche di cybersicurezza, di cui si dirà più compiutamente nella sezione dedicata alle attività internazionali.

Con il medesimo provvedimento è stata garantita la prima operatività del *Computer Security Incident Response Team*-CSIRT Italia, la struttura tecnica di prevenzione, coordinamento e risposta agli eventi e incidenti informatici con impatto, effettivo o potenziale, sul territorio nazionale, incardinata presso l'ACN. Infatti, con l'istituzione dell'Agenzia per la cybersicurezza nazionale, i compiti fino ad allora in capo al CSIRT operativo presso il DIS sono contestualmente transitati nella sfera di competenza dell'ACN (vds. 3.1). Vale evidenziare come il trasferimento di tale funzione sia avvenuta in maniera tale da garantire la piena operatività della struttura, i cui servizi hanno continuato ad essere erogati senza soluzione di continuità.

Tra le funzioni, che ai sensi del decreto-legge sono oggetto di trasferimento da altre amministrazioni vi sono, poi, quelle precedentemente incardinate presso il Ministero dello Sviluppo Economico (ora "delle imprese e del *made in Italy*"), che afferiscono alle materia delle certificazioni di cybersicurezza e dello scrutinio tecnologico di apparati ICT, alla normativa di attuazione del Perimetro di sicurezza nazionale cibernetica, alla sicurezza e all'integrità delle comunicazioni elettroniche e alla sicurezza delle reti e dei sistemi informativi di cui al decreto legislativo NIS.

[3] Tale funzione viene esercita in stretto raccordo con il MAECI, fatta eccezione per i casi in cui la legge attribuisce competenze esclusive ad altre Amministrazioni. In tali, ultimi casi è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri.

In tale contesto, si è, tra l'altro, realizzato il trasferimento di due organismi: l'Organismo di Certificazione della Sicurezza Informatica (OCSI) e il Centro di Valutazione e Certificazione Nazionale (CVCN).

Il trasferimento di tali funzioni è demandato, per la parte esecutiva, ad un apposito decreto del Presidente del Consiglio dei ministri, la cui elaborazione ha fortemente impegnato l'Agenzia e il MiSE. Tale trasferimento – avvenuto successivamente al periodo in esame – ha regolato anche il passaggio di carico di documentazione, assetti finanziari e beni strumentali.

In particolare, OCSI è operativo dal 2003 e rilascia certificazioni di sicurezza cibernetica su prodotti ICT, in conformità allo schema di certificazione nazionale adottato con decreto del Presidente del Consiglio dei ministri nell'ottobre del 2003. Tale schema si applica su base volontaria, nel senso che un produttore di apparati ICT può rivolgersi ad OCSI per ottenere una certificazione riconosciuta a livello internazionale dai Paesi che aderiscono, insieme all'Italia, ad accordi di mutuo riconoscimento. Lo stesso schema di certificazione è basato su *standard* e norme internazionali. Per le attività di *test*, OCSI si avvale di laboratori esterni (i Laboratori di Valutazione della Sicurezza – LVS).

Il CVCN è stato istituito nel 2019 presso l'allora MiSE, in attuazione del DPCM 17 febbraio 2017 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. Tale struttura, incardinata, in seguito alla riforma operata dal decreto-legge, in seno all'ACN, ha il compito di effettuare valutazioni preventive su particolari categorie di *asset* ICT (definite con DPCM 15 giugno 2021), destinati ad essere impiegati dai soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica per l'erogazione di funzioni e servizi essenziali. Il CVCN si coordina con i Centri di Valutazione (CV) istituiti presso il Ministero della difesa e il Ministero dell'interno ed accredita laboratori esterni (Laboratori Accreditati di Prova-LAP), ai quali può demandare l'esecuzione di test di sicurezza.

OCSI

Organismo di Certificazione della Sicurezza Informatica. Organismo traferito dal Ministero dello Sviluppo Economico all'Agenzia per la cybersicurezza nazionale, con il compito di emettere certificazioni di sicurezza su prodotti ICT. Opera su richiesta dei produttori e applica lo schema di certificazione nazionale, adottato con DPCM 30 ottobre 2003. OCSI partecipa ad accordi di mutuo riconoscimento che fanno sì che i certificati emessi siano riconosciuti anche negli altri Paesi che partecipano agli stessi accordi.

CVCN

Centro di Valutazione e Certificazione Nazionale. Trasferito dal MiSE ad ACN, valuta la sicurezza e può eseguire test su asset ICT da impiegare sul Perimetro.

LAP ed LVS

Laboratori accreditati che operano a supporto, rispettivamente, del CVCN e di OCSI. Eseguono test di sicurezza su asset ICT: i LAP in ambito Perimetro, gli LVS secondo lo schema di certificazione nazionale.

In relazione, poi, alla sicurezza delle comunicazioni elettroniche, si segnala il trasferimento di una ulteriore competenza dall'allora MiSE all'ACN. In particolare, il D.Lgs. 207/2021 – alla cui predisposizione l'Agenzia ha fornito il suo contributo – ha recepito nell'ordinamento nazionale, nel novembre 2021, la normativa europea di settore[4], novellando il Codice delle comunicazioni elettroniche nazionale (D.Lgs. 259/2003) e prevedendo, in particolare, l'adozione di misure di sicurezza che dovranno sostituire il decreto ministeriale del Ministro dello sviluppo economico del 12 dicembre 2018 in materia di misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi.

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.

Tra le funzioni attribuite all'Agenzia, si evidenzia, inoltre, la partecipazione al Gruppo di coordinamento che cura le istruttorie per l'applicazione dei poteri speciali, cd. *Golden Power*. Fin dalla sua prima operatività, infatti, l'Agenzia ha fornito supporto tecnico al Gruppo di coordinamento *Golden Power*, per gli aspetti di propria competenza, in presenza di notifiche inerenti alle reti di telecomunicazione a banda larga con tecnologia 5G, e, più in generale, a operazioni societarie che impattano su attivi strategici in ambito ICT e di cybersicurezza. Nel periodo di riferimento, in particolare, l'ACN ha preso parte a 5 riunioni del Gruppo di coordinamento *Golden Power*.

Con riferimento agli aspetti logistici, ai sensi del DPCM 16 settembre 2021, il DIS e l'ACN hanno proceduto all'individuazione di spazi idonei a ospitare gli uffici dell'Agenzia, al fine di assicurarne la prima operatività. In tempi estremamente serrati, sono stati eseguiti lavori di adattamento, funzionali a rendere operativa la sede dell'Agenzia con, tra l'altro, circa 150 postazioni di lavoro.

Nel periodo in esame, inoltre, data la crescita di personale stimata (e in parte già raggiunta nel 2022), sono state immediatamente avviate tutte le attività di studio e pianificazione volte ad individuare una sede dell'Agenzia in grado di rispondere a tutte le esigenze, dai laboratori alle postazioni di lavoro adeguate all'organico che l'ACN dovrà raggiungere.

Inoltre, al medesimo fine – come anticipato – una prima aliquota di personale del Dipartimento delle Informazioni per la sicurezza è stata messa a disposizione a partire dal 1° settembre 2021 ai sensi dell'art 17, comma 8, lett. *a)*, del decreto-legge. Tale contingente, in precedenza impiegato nelle funzioni oggetto di trasferimento, è stato successivamente inquadrato nel ruolo del personale a tempo indeterminato, con decorrenza 1° gennaio 2022.

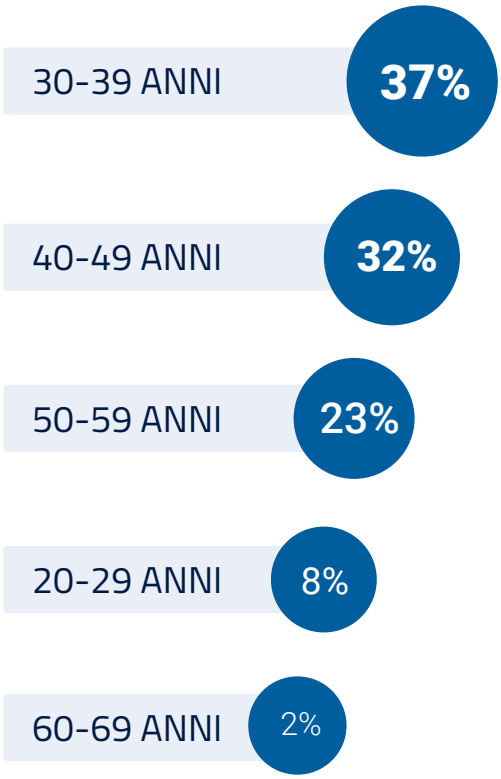
[4] In data 4 novembre 2021, il Consiglio dei ministri ha approvato il decreto di attuazione della Direttiva 2018/1972.

Al predetto contingente si è aggiunta un'ulteriore aliquota di personale che, a partire dal mese di ottobre 2021, è stata messa a disposizione da altre amministrazioni, ai sensi dell'art. 17, comma 8, lett. *b)*, del decreto-legge. Trattasi di personale che è stato successivamente inquadrato nel ruolo del personale a tempo indeterminato dell'Agenzia, a seguito del superamento della procedura selettiva prevista decreto-legge.

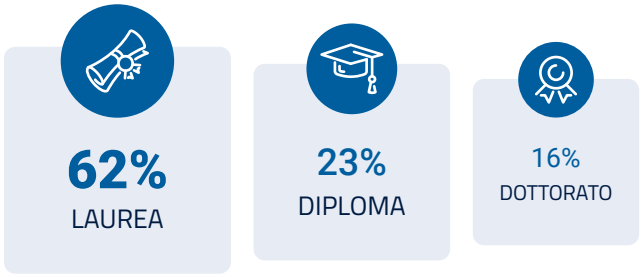
Infine, a seguito di intese con la Banca d'Italia, l'Agenzia, nel periodo in riferimento, si è avvalsa di ulteriori 3 persone, rese disponibili tramite distacco.

RISORSE UMANE DELL'ACN

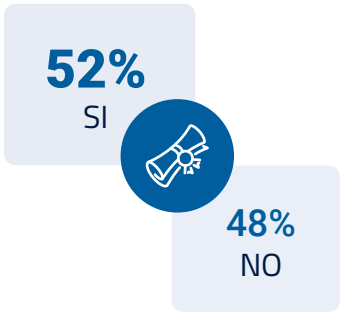
FASCIA D'ETÀ



TITOLO DI STUDIO



LAUREA STEM *



ETÀ MEDIA

*** STEM**

Acronimo di *Science, Technology, Engineering and Mathematics*. Indica specifici ambiti disciplinari cui sono ricondotti percorsi accademici ad alto valore aggiunto per lo sviluppo e l'innovazione.

In relazione agli aspetti patrimoniali, il decreto-legge assegna all'Agenzia una dotazione finanziaria di 2.000.000 di euro per l'anno 2021, 41.000.000 di euro per l'anno 2022, 70.000.000 di euro per l'anno 2023, 84.000.000 di euro per l'anno 2024, 100.000.000 di euro per l'anno 2025, 110.000.000 di euro per l'anno 2026 e 122.000.000 di euro annui a decorrere dall'anno 2027. L'articolo 11 del citato decreto-legge prevede, inoltre, che la legge di bilancio determini un ulteriore stanziamento a favore dell'Agenzia sulla base del fabbisogno annuo che viene indicato dal Presidente del Consiglio dei ministri. Tali assegnazioni sono da intendersi, ad esempio, per la realizzazione di specifici progetti, volti a perseguire l'autonomia tecnologica, nonché il rafforzamento della sicurezza e resilienza cibernetiche nazionali (in linea con quanto previsto dalla Strategia nazionale di cybersicurezza).

Le entrate dell'Agenzia sono, altresì, costituite dai corrispettivi per servizi a soggetti pubblici o privati; proventi derivanti dallo sfruttamento della proprietà intellettuale, dei prodotti dell'ingegno e delle invenzioni dell'ACN; proventi delle sanzioni irrogate ai sensi delle normative *cyber* vigenti. Esse comprendono, inoltre, i contributi dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione. In tale contesto, l'ACN, in qualità di Centro di coordinamento nazionale di cui al Reg. UE 2021/887, ha accesso ai fondi europei stanziati da *Horizon Europe* e *Digital Europe* per l'implementazione di specifiche progettualità in ambito *cyber*.

Il bilancio preventivo e il bilancio consuntivo, adottati dal Direttore generale dell'Agenzia, sono approvati con decreto del Presidente del Consiglio dei ministri, previo parere del Comitato interministeriale per la cybersicurezza e sono trasmessi alla Corte dei conti, che esercita il controllo previsto dall'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20.

La pianificazione, la programmazione e il *budgeting* dell'Agenzia sono regolati dal DPCM 9 dicembre 2021, n. 222, che prevede anche i termini di presentazione della citata documentazione. Relativamente al primo documento da presentare in ordine temporale, ossia il bilancio di previsione, che, ai sensi del DPCM citato dovrebbe essere presentato entro il 31 ottobre dell'anno precedente, nel quadrimestre di riferimento si è provveduto – sulla base di una opportuna pianificazione strategica – alla elaborazione della programmazione finanziaria, poi confluita nel bilancio approvato nell'anno successivo.

Da ultimo, si segnala che il Dipartimento per la trasformazione digitale-DTD della Presidenza del Consiglio dei ministri, in qualità di "Amministrazione Titolare", ha designato l'ACN quale "Soggetto attuatore" per la realizzazione dell'investimento 1.5 *Cybersecurity*, nell'ambito della Missione 1-Componente 1 del PNRR, volto al potenziamento delle capacità di resilienza delle infrastrutture e dei servizi digitali del Paese, dotato di risorse pari a 623 milioni di euro (approfondimento nel prosieguo della Relazione, nella sezione dedicata).

#2

Le attività di resilienza a tutela degli interessi nazionali nel campo della cybersicurezza

Le attività di resilienza a tutela degli interessi nazionali nel campo della cybersicurezza

Come già indicato in esordio, ai sensi del decreto-legge, il mandato istituzionale dell'Agenzia include la tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della sicurezza nazionale nello spazio cibernetico.

La vastità del cambiamento tecnologico – legata al processo di digitalizzazione che sta attraversando il sistema-Paese – pone di fronte a una serie di rischi, anche di carattere sistemico, che investono le dimensioni economica, sociale e politica. Essi riguardano, tra l'altro: attacchi *cyber* in grado di produrre potenziali impatti sull'erogazione dei servizi, anche essenziali, di un Paese; affidabilità e robustezza della catena di approvvigionamento tecnologico; tentativi di ingerenza e destabilizzazione del dibattito pubblico, anche attraverso il dispiegamento di campagne disinformative e narrative distorte e/o polarizzanti.

In tale contesto, ai sensi del decreto-legge, l'Agenzia assicura – nel rispetto delle prerogative attribuite dalla normativa vigente ad altre amministrazioni – il coordinamento tra i soggetti pubblici coinvolti nella materia della cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la resilienza e la sicurezza cibernetiche per lo sviluppo e la digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni.

Al riguardo, le attività finalizzate a innalzare il livello di resilienza e sicurezza cibernetiche, svolte dall'ACN nel periodo in esame, hanno riguardato: le attività del CSIRT Italia, che includono sia quella in risposta a incidenti informatici sia quella divulgativa, finalizzata, tra l'altro, alla prevenzione dei rischi derivanti da incidenti *cyber*; l'attivazione del Nucleo per la cybersicurezza e le iniziative promosse in relazione alla prevenzione e preparazione a situazioni di crisi che coinvolgono aspetti di cybersicurezza, inclusa l'attivazione delle procedure di allertamento; l'attuazione della normativa in materia di Perimetro di sicurezza nazionale cibernetica.

Attività del CSIRT Italia

COLLABORATION

Il portale di *collaboration* è riservato ai membri della *constituency* del CSIRT Italia. Costituisce lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati.

Nel periodo di riferimento, l'Agenzia, attraverso il CSIRT Italia (vedasi approfondimento - CSIRT Italia), ha svolto attività di natura preventiva e reattiva nei confronti della *constituency* (vedasi approfondimento - *Constituency* del CSIRT Italia). La prima, realizzata attraverso il monitoraggio della rete Internet al fine di rilevare rischi potenziali e incidenti ai danni di soggetti pubblici e privati nazionali, si è tradotta nella produzione di *alert*, bollettini tecnici e comunicazioni dirette, a favore dei soggetti interessati. I prodotti generalmente riferiti all'intera comunità e pubblicamente ostensibili sono stati resi disponibili sul portale pubblico (https://www.csirt.gov.it), mentre quelli pubblicamente non ostensibili[5], riferiti a singoli o gruppi di operatori, sono stati condivisi tramite il portale ad accesso ristretto, cd. portale di *collaboration* (https://portale.csirt.gov.it). A tali contenuti, si aggiungono anche le numerose comunicazioni (2.316) inviate direttamente a soggetti interessati. Per quanto attiene invece alle attività di natura reattiva, ovvero innescate da specifiche comunicazioni ricevute dal CSIRT Italia[6], nel periodo di riferimento sono state trattate 10.249 comunicazioni, sottoposte a *triage* e correlate con gli esiti delle attività di monitoraggio interno, che hanno determinato l'apertura di 337 "*case*", ovvero eventi con potenziali profili di criticità, sottoposti ad approfondimento e gestione (vds. Figura 1).

Figura 1: I portali del CSIRT Italia

PORTALE PUBBLICO
Numero di alert pubblicati **109**
Numero di bollettini pubblicati **20**

PORTALE COLLABORATION
Numero di alert pubblicati **109**
Numero di bollettini pubblicati **20**

COMUNICAZIONI
10.249 comunicazioni ricevute dal CSIRT Italia, di cui 337 riferite ad eventi con potenziali profili di criticità
2.316 comunicazioni inviate dal CSIRT Italia verso la Constituency

[5] Secondo le *best practice* comunemente adottate, le informazioni che vengono scambiate tra articolazioni tecniche *cyber* (vulnerabilità, compromissioni, minacce ecc.), in relazione alla loro sensibilità, sono sottoposte a criteri di condivisione che possono più o meno limitarne la diffusione, la quale può essere quindi pubblica o limitata a singoli o gruppi di soggetti secondo il criterio della "necessità di conoscere".

[6] Tra tali comunicazioni rientrano le segnalazioni di eventi cibernetici trasmesse, in conformità alla normativa vigente, dalla *constituency* tramite la specifica pagina del portale pubblico (https://www.csirt.gov.it/segnalazione), oppure *feed* informativi ricevuti da aziende operanti nel campo della sicurezza informatica sulla base di specifici accordi stipulati con l'Agenzia.

APPROFONDIMENTO - CSIRT ITALIA

La principale fonte normativa che dettaglia i compiti e le funzioni del CSIRT è il Decreto Legislativo 18 maggio 2018, n. 65.

In particolare, i compiti del CSIRT Italia includono:

- il monitoraggio degli incidenti a livello nazionale;
- l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- l'intervento in caso di incidente;
- l'analisi dinamica dei rischi e degli incidenti;
- la sensibilizzazione situazionale;
- la partecipazione alla rete dei CSIRT europei.

A tal fine il CSIRT Italia stabilisce relazioni di cooperazione con il settore privato e promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Il CSIRT Italia rappresenta, quindi:

- la struttura tecnica di prevenzione, coordinamento e risposta agli eventi e incidenti informatici con impatto, effettivo o potenziale, sul territorio nazionale;
- il punto di riferimento per le notifiche degli incidenti occorsi in danno di tutte le infrastrutture digitali della pubblica amministrazione e private, con particolare riferimento alle notifiche – previste ai sensi di legge – ad opera dei soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica-PSNC ovvero per gli operatori di servizi essenziali e fornitori di servizi digitali individuati dalla Direttiva NIS e per i soggetti sottoposti a obbligo di notifica ai sensi del Codice delle comunicazioni elettroniche;
- uno dei membri della rete composta dai CSIRT europei (CSIRT *Network*) avente quale finalità quella di contribuire a sviluppare la fiducia tra gli Stati membri dell'UE e promuovere la cooperazione operativa in ambito internazionale.

Elemento di novità introdotto dal D.L. 14 giugno 2021, n. 82 è l'attribuzione della qualifica di pubblico ufficiale al personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni. Nello specifico, il legislatore ha precisato che, in relazione all'obbligo di denuncia di notifiche di incidenti che costituiscono reati perseguibili d'ufficio (art. 331 del c.p.p.), ricevuti dal personale del CSIRT Italia nell'esercizio o a causa delle proprie funzioni, tale assolvimento sia adempiuto con la trasmissione delle predette notifiche all'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7 *bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

APPROFONDIMENTO - *CONSTITUENCY* DEL CSIRT ITALIA

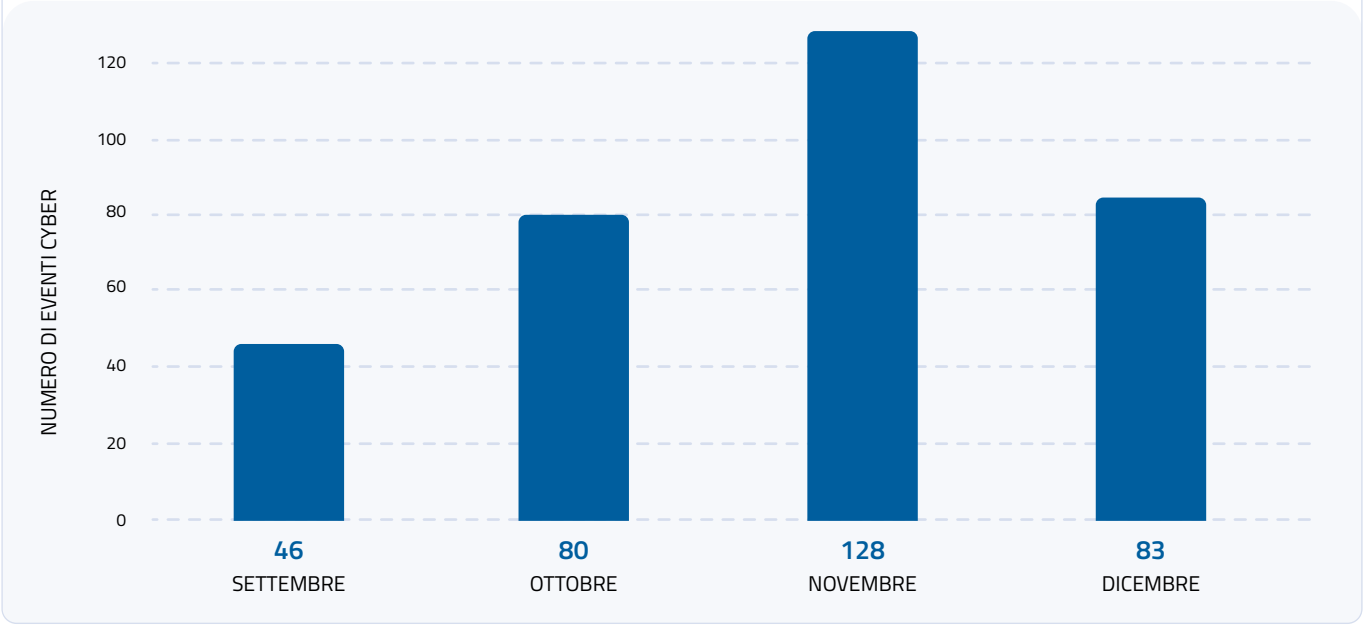
La *constituency* è l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di **prevenzione, monitoraggio, rilevamento, analisi e risposta** al fine di prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici.

Di seguito si riportano i riferimenti normativi, nel testo in vigore nel periodo di riferimento della presente relazione, che considerano il CSIRT Italia quale *hub* nazionale per la ricezione delle notifiche di incidenti, per la loro gestione, nonché per tutte le attività di *alerting* rispetto alle minacce gravanti su soggetti pubblici o privati:

- **D.L. n. 105/2019** e relativi provvedimenti attuativi, che stabilisce, per i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, obblighi di notifica di incidenti;
- **D.Lgs. n. 65/2018** che individua gli Operatori di Servizi Essenziali e i Fornitori di Servizi digitali quali soggetti con obbligo di notifica d'incidente;
- **D.L. n. 259/2003**, così come modificato dal D.Lgs. n. 207/2021 e relativo "DM Telco", che impone obblighi di notifica ai soggetti imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico;
- **D.L. n. 82/2005** (Codice dell'Amministrazione Digitale–CAD) che definisce i soggetti pubblici per i quali il CSIRT Italia coordina le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici.

La distribuzione nel tempo degli eventi è riportata in Figura 2, da cui emerge una media di circa 80 eventi al mese, con un picco a novembre 2021 di 128 eventi.

Figura 2: Eventi *cyber* nel periodo di riferimento



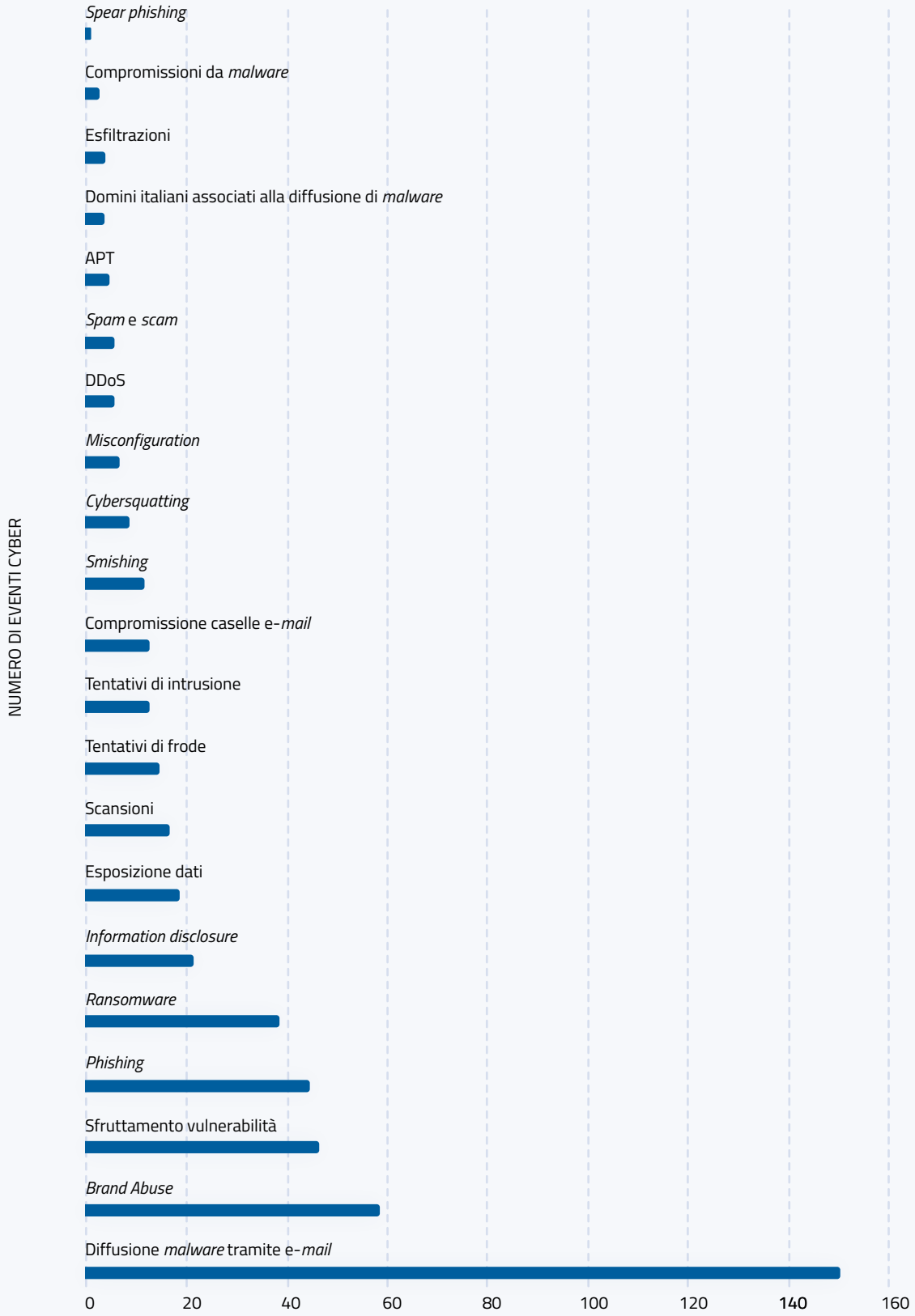
Dall'analisi e dalla successiva classificazione degli eventi rilevati, emergono le seguenti 5 tipologie più frequenti:

1. Diffusione di *malware*: **151 occorrenze**;
2. *Brand abuse*: **59 occorrenze**;
3. Sfruttamento vulnerabilità: **47 occorrenze**;
4. *Phishing*: **45 occorrenze**;
5. *Ransomware*: **39 occorrenze**.

L'elenco completo delle tipologie individuate è riportato in Figura 3. Ognuno dei citati 337 "*case*", riferiti ad eventi con potenziali profili di criticità, può essere stato associato ad una o più tipologie di evento[7].

[7] 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*.

Figura 3: Tipologia di eventi *cyber* nel periodo di riferimento



APPROFONDIMENTO - CAPACITÀ TECNICO-OPERATIVE

Nella fase di cd. prima operatività, anche al fine di sviluppare capacità tecniche connesse alle funzioni previste dal proprio mandato istituzionale, l'Agenzia ha inteso perseguire i seguenti obiettivi:

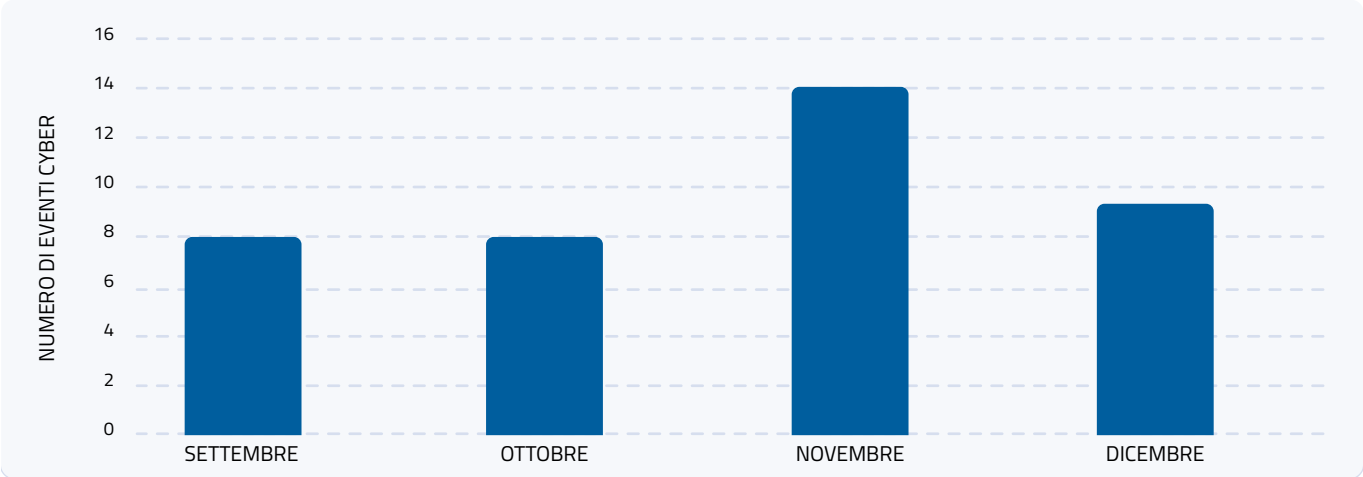
- **strutturare e incrementare le capacità di risposta e ripristino** in capo al CSIRT Italia in previsione dell'aumento sensibile degli eventi cibernetici derivanti dalle nuove sfide;
- **contribuire all'incremento della consapevolezza relativa alla minaccia** nei soggetti della *constituency* mantenendo e incrementando le capacità di pubblicazione di *alert*, bollettini ed *early warning*;
- **consolidare e potenziare le capacità di monitoraggio tecnico *cyber***, necessarie per erogare verso la *constituency* servizi di *early warning* in merito, ad esempio, alla postura di sicurezza degli *asset* esposti dai soggetti, all'individuazione di eventi anomali o di compromissione connessi alle reti degli stessi, oltre che alle campagne ostili ed agli attori *cyber* ostili d'interesse (*cyber threat intelligence*);
- **assicurare una capacità di analisi specialistica** su tematiche di *malware analysis*, *digital forensics* e analisi vulnerabilità, per supportare adeguatamente gli incidenti gestiti dal CSIRT Italia ed il monitoraggio delle minacce *cyber*, oltre che specifiche attivazioni su tematiche tecniche d'interesse;
- **gestire in forma integrata il bagaglio informativo tecnico sulla *constituency* e sulle minacce *cyber*** al fine di ottenere una visione unitaria utile ad assicurare una situation *awareness*, anche attraverso l'elaborazione di modelli e tecniche di valorizzazione dei dati;
- **istituire e consolidare nuove collaborazioni** con omologhi organismi e CSIRT internazionali, anche tramite la certificazione e l'accreditamento a reti di collaborazioni esistenti (come *First* e *Trusted Introducer*) e tramite la partecipazione e l'organizzazione di esercitazioni *cyber*;
- **curare le collaborazioni esistenti ed i rapporti tecnici con soggetti pubblici e privati** volti allo scambio di dati ed istituirne di nuove, ponendo in chiara luce la necessità di elevare il livello di reputazione dell'Agenzia anche adottando strategie di comunicazione e relazioni con i soggetti esterni e sui canali di comunicazione del CSIRT Italia;
- **istituire una capacità di gestione rischio nazionale**, al fine di stimare il rischio *cyber* del Paese e settoriale, anche analizzando i dati provenienti dai soggetti del Perimetro di sicurezza nazionale cibernetica, le segnalazioni ricevute dal CSIRT Italia, nonché tutte le sorgenti di dati acquisite anche tramite collaborazioni;
- **istituire una capacità di analisi** per poter fornire statistiche, *trend* e analisi previsionali;
- **curare lo sviluppo ed il mantenimento delle capacità nazionali** di prevenzione, monitoraggio, rilevamento, analisi e risposta degli incidenti informatici, declinando gli obiettivi strategici dell'Agenzia in termini di servizi, requisiti, architetture e processi.

Focus su eventi *ransomware*

Nel periodo di riferimento, il *ransomware* (vds. approfondimento - Il *Ransomware*) è stato tra le minacce più insidiose per l'operatività delle vittime analizzate. Il CSIRT Italia in quattro mesi ha gestito 39 eventi *ransomware* in danno di aziende e organizzazioni italiane[8], distribuiti nel tempo come mostrato in Figura 4.

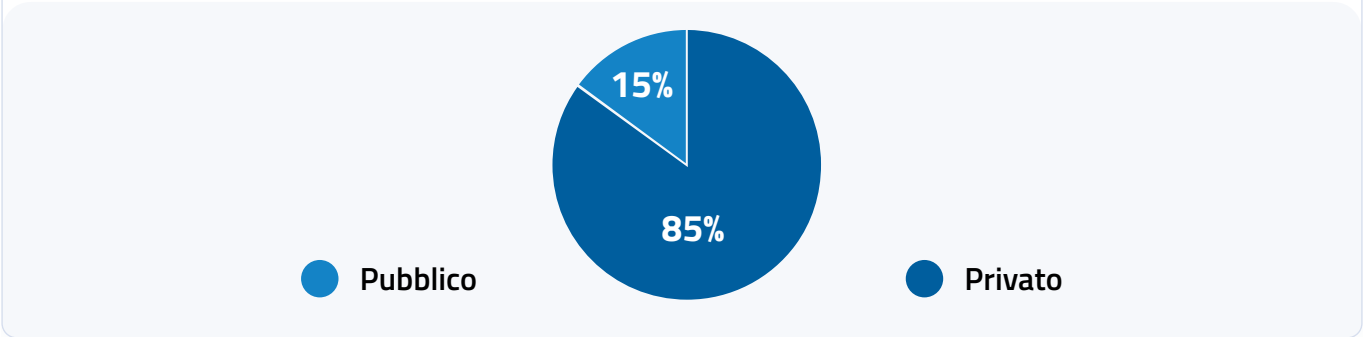
In alcuni casi, particolarmente critici, il personale del CSIRT Italia ha fornito supporto diretto ai soggetti suggerendo gli opportuni elementi informativi e operativi ai fini delle idonee attività di mitigazione.

Figura 4: Eventi *ransomware* nel periodo di riferimento



Le vittime di questi eventi ricadono per l'85% nel settore privato a fronte di un 15% ricompreso tra le pubbliche amministrazioni (Figura 5).

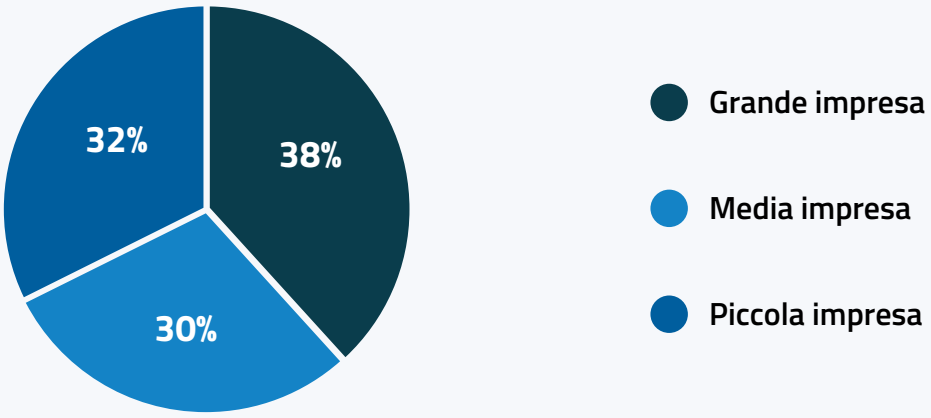
Figura 5: Ripartizione dei *ransomware* per tipo di vittima pubblico/privato



[8] Il dato rappresenta solo una parte del numero complessivo di attacchi *ransomware* effettivamente avvenuti, poiché in diversi casi le vittime, tipicamente soggetti appartenenti al tessuto produttivo delle PMI, non denunciano l'accaduto e gestiscono l'evento in autonomia.

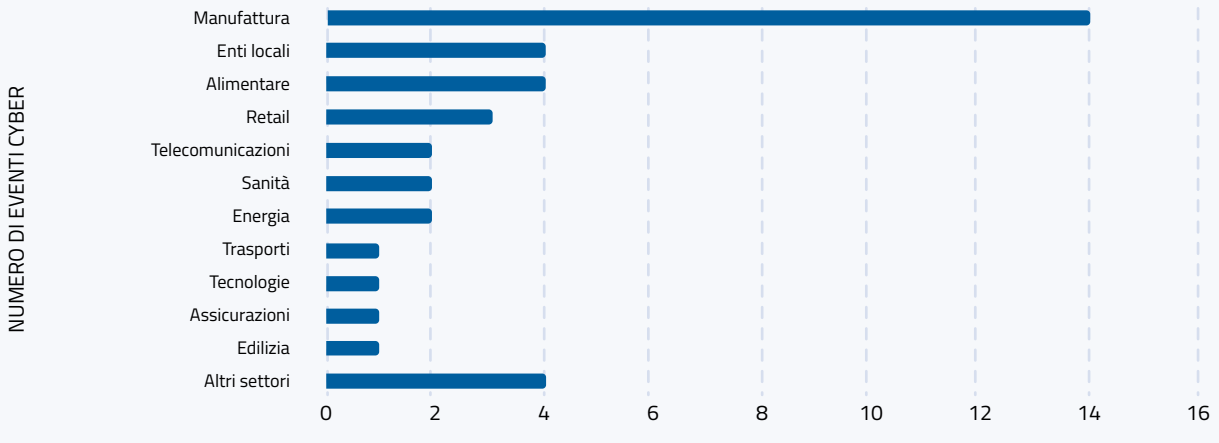
Per quanto attiene alla dimensione aziendale dei soggetti privati colpiti, il 38% degli eventi *ransomware* ha interessato grandi imprese, il 30% ha visto coinvolte medie imprese, mentre il restante 32% ha riguardato le piccole imprese (Figura 6).

Figura 6: Ripartizione eventi *ransomware* per dimensione aziendale



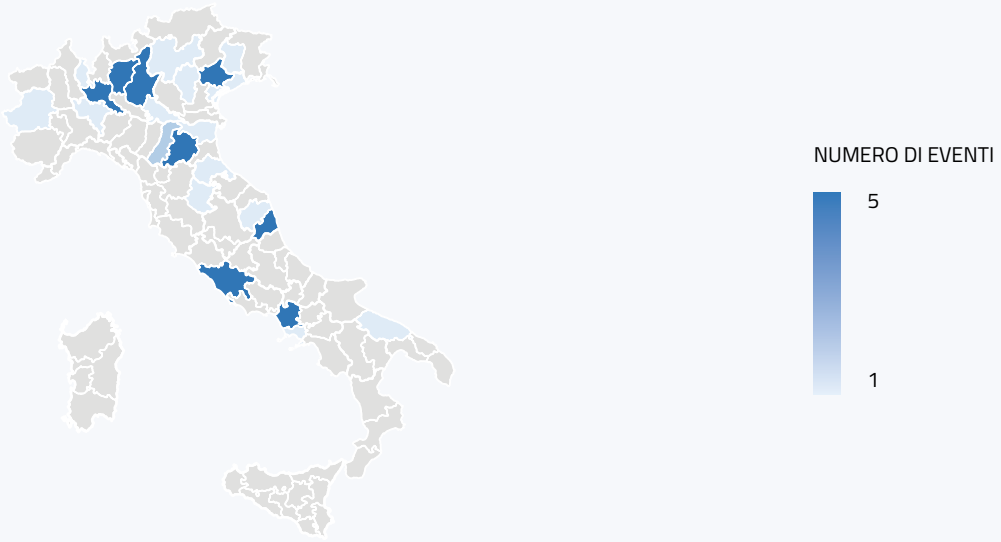
Classificando le vittime in base ai settori di attività economica (Figura 7), emerge come il settore manifatturiero sia stato il più colpito, seguito dalla pubblica amministrazione locale, dal settore alimentare e da quello del *retail*. Giova evidenziare come, ai fini dell'analisi, il manifatturiero costituisca un settore di notevole ampiezza, che ricomprende al suo interno una pluralità di mercati e di ambiti produttivi differenti.

Figura 7: Eventi *ransomware* per settore di attività economica



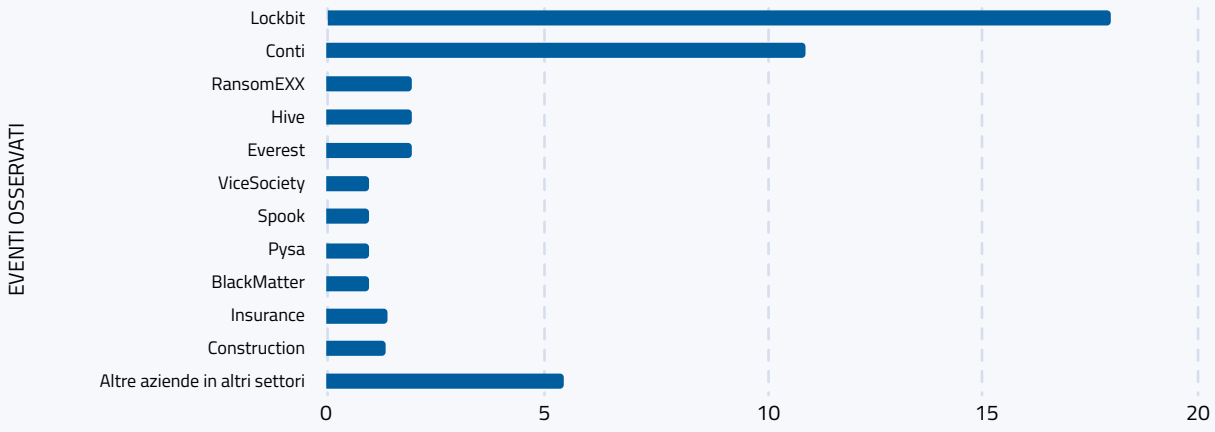
Da un punto di vista geografico, le zone più interessate dal fenomeno corrispondono alle grandi aree metropolitane di Roma e Milano e ai distretti manifatturieri del Nord Ovest e Nord Est (Figura 8). Tale contesto è plausibilmente determinato dalla maggiore presenza, in tali zone, di imprese operanti nel settore manifatturiero.

Figura 8: Localizzazione geografica delle vittime di eventi *ransomware* in base alla provincia del soggetto



Nel periodo d'analisi, gli attacchi sono stati condotti da 9 diversi "*Threat Actors*", tra i quali i più attivi sono risultati Conti, LockBit e Hive, responsabili del 75% degli attacchi totali (Figura 9).

Figura 9: Gruppi *ransomware* rilevati in Italia nel periodo di analisi



APPROFONDIMENTO - IL *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:

- esfiltrare i dati e minacciarne la pubblicazione salvo pagamento del riscatto (*Double extortion*);
- 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*);
- effettuare contestualmente altri tipi di attacco, come il DDOS al fine di compromettere ulteriormente l'operatività dell'organizzazione.

Secondo il recente rapporto dell'Agenzia Europea per la cybersicurezza (Enisa *Threat Landscape for Ransomware Attacks*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks/@@download/fullReport), l'Italia risulta il quarto Paese al mondo più colpito da tale minaccia, dopo Stati Uniti, Germania e Francia.

APPROFONDIMENTO - *CYBERGANG* CRIMINALI

Conti, Hive e Lockbit sono tre tra le più attive organizzazioni *cyber*-criminali responsabili di attacchi *ransomware* a danni di amministrazioni pubbliche e private in tutto il mondo.

Dotate di una struttura organizzativa molto articolata, operano lungo tutta la filiera dell'attacco *cyber*, dalla scelta della vittima, intrusione nel suo sistema informatico, infezione, sino alla richiesta e negoziazione del riscatto.

Ciascun gruppo è caratterizzato da un proprio *modus operandi*, associato all'utilizzo di strumenti di infezione solitamente sviluppati in proprio.

Prevenzione e preparazione a situazioni di crisi e attivazione delle procedure di allertamento

Nell'ambito della rinnovata architettura nazionale *cyber*, è stato istituito, in via permanente, presso l'ACN, il Nucleo per la cybersicurezza-NCS, che 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. Esso è presieduto dal Direttore generale dell'ACN ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del 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, 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.

In particolare, il rinnovato Nucleo per la cybersicurezza è un organismo collegiale che supera, alla luce delle rafforzate competenze sul piano delle *policy*[9] e dell'ampliato novero di soggetti istituzionali coinvolti[10], il precedente Nucleo per la sicurezza cibernetica di cui al DPCM 17 febbraio 2017, e si configura quale sede primaria di coordinamento interministeriale, a livello tecnico-operativo, sul tema, anche a beneficio del Vertice politico.

Nel periodo in esame, contestualmente alla predisposizione delle attività necessarie alla strutturazione di tale consesso e all'avvio dei lavori ordinari, l'Agenzia ha dovuto sin da subito attivare il Nucleo in considerazione di eventi e segnalazioni potenzialmente critici ai fini della sicurezza nazionale nello spazio cibernetico, nonché alla luce del rapido evolversi del panorama delle minacce di natura cibernetica e della numerosità di sempre nuove vulnerabilità di sicurezza informatica quotidianamente identificate. In relazione a tale esigenza, il Nucleo è stato, infatti, convocato anche in composizione ristretta ai sensi dell'art. 8, comma 4, del decreto-legge, mediante il coinvolgimento delle amministrazioni con competenze specifiche in materia.

[9] In particolare, il Nucleo può formulare proposte di iniziative in materia di cybersicurezza del Paese anche nel quadro del contesto internazionale.

[10] Si fa riferimento all'inclusione del Ministero della transizione ecologica (ora "dell'ambiente e sicurezza energetica"), del Ministero dell'università e della ricerca, di un rappresentante del Ministro delegato per l'innovazione tecnologica e la transizione digitale (non previsto a livello di Ministro nell'attuale Esecutivo) e del Ministero delle infrastrutture e della mobilità sostenibile (ora "delle infrastrutture e dei trasporti").

Da ultimo, al fine di prevenire potenziali impatti di natura sistemica derivanti, in parte, da una non sufficiente robustezza delle catene di approvvigionamento, il Nucleo si è ulteriormente riunito in concomitanza con la diffusione mondiale di una vulnerabilità critica, denominata Log4Shell, gravante sul prodotto Log4J di Apache Foundation. In tale occasione, l'Agenzia, nell'assolvere alla funzione di *alerting*, ha indicato le principali misure di mitigazione rispetto al caso di specie e ha verificato il livello di esposizione del settore pubblico, anche con riferimento all'efficacia delle azioni intraprese dalle amministrazioni per risolvere tale vulnerabilità.

Nel periodo 1° settembre-31 dicembre 2021, il Nucleo per la cybersicurezza si è riunito, in composizione ordinaria e in composizione ristretta, per un totale di 7 volte.

La gestione delle crisi in ambito UE e internazionale

Il quadro europeo per la risposta coordinata agli incidenti e alle crisi *cyber* su vasta scala, delineato dalla Raccomandazione UE 2017/1584 (cd. *Blueprint*), rappresenta la componente *cyber* dei meccanismi dell'Unione europea per la gestione delle crisi cinetiche. In particolare, il *Blueprint* organizza la cooperazione su tre livelli:

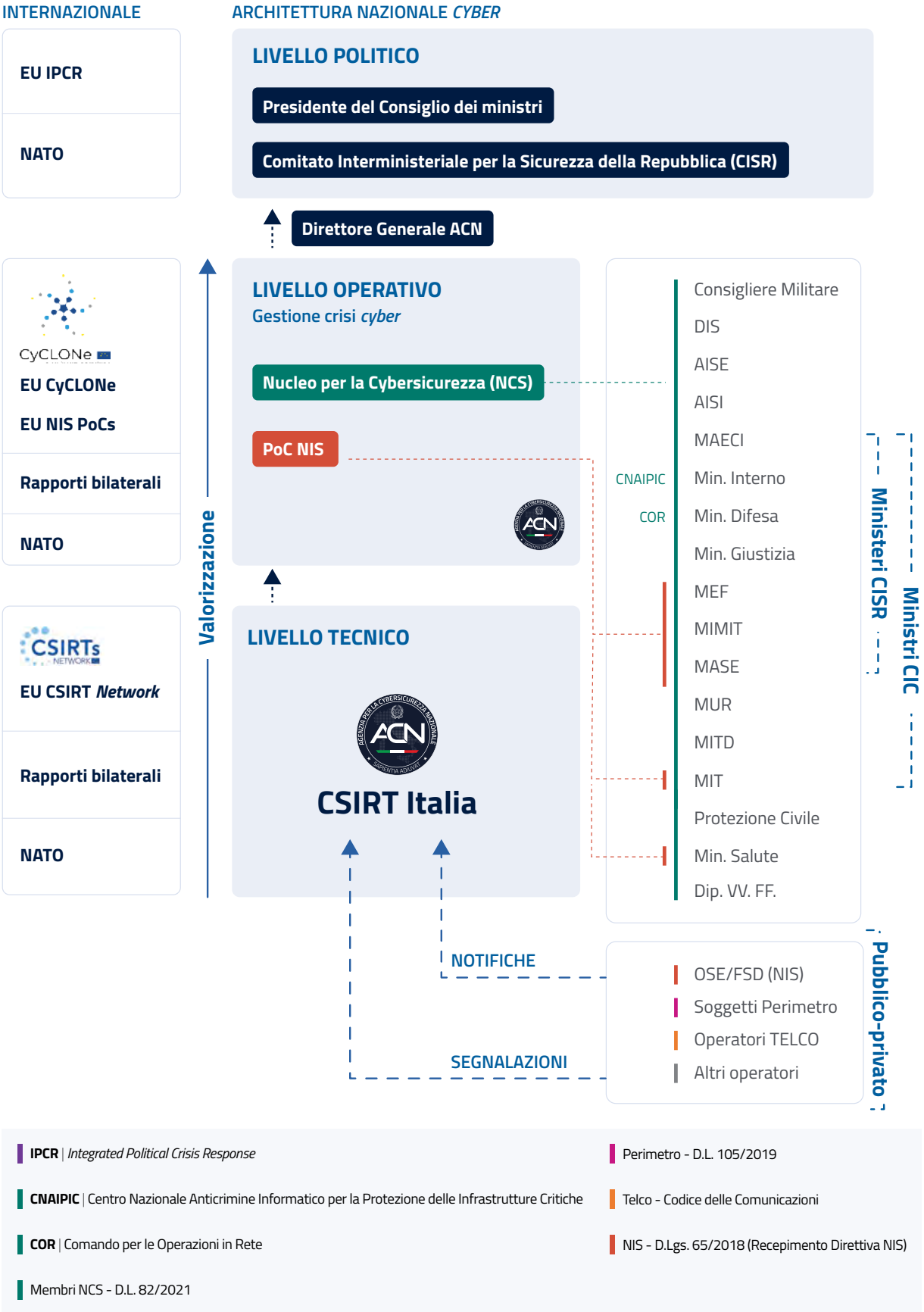
- il livello politico, che gestisce la risposta strategica alle crisi, adottando, ad esempio, misure diplomatiche, nella più ampia cornice dei dispositivi integrati per la risposta politica alle crisi (*Integrated Political Crisis Response Mechanism*-IPCR) del Consiglio dell'Unione europea;

- il livello operativo, che svolge il ruolo di raccordo tra il livello politico e tecnico, implementato tramite la *Cyber Crisis Liaison Organisation Network*-CyCLONe, la rete europea per la gestione coordinata degli incidenti e delle crisi *cyber* transfrontalieri su vasta scala, promossa congiuntamente nel 2020 da Italia e Francia;

- il livello tecnico, che monitora e tratta gli incidenti di elevata criticità, effettuando l'analisi delle minacce e dei rischi cibernetici. Queste funzioni sono svolte dalla rete europea dei CSIRT (cd. CSIRT *Network*) formata dai CSIRT degli Stati Membri.

Giova evidenziare come, coerentemente al quadro delineato dal legislatore europeo, anche l'Italia si sia dotata di un'architettura nazionale di cybersicurezza strutturata sui livelli politico, operativo e tecnico (Figura 10).

Figura 10: Architettura nazionale *cyber* e relativo inquadramento nel contesto internazionale e dell'UE



IPCR | *Integrated Political Crisis Response*

CNAIPIC | Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

COR | Comando per le Operazioni in Rete

Membri NCS - D.L. 82/2021

Perimetro - D.L. 105/2019

Telco - Codice delle Comunicazioni

NIS - D.Lgs. 65/2018 (Recepimento Direttiva NIS)

In tale contesto assume particolare rilevanza il ruolo dell'ACN, al cui interno, come già menzionato, sono incardinate sia la struttura di livello tecnico (CSIRT Italia), sia quella di livello operativo (NCS), rivestendo, al contempo, il ruolo di referente nazionale per CyCLONe, che rappresenta l'infrastruttura transfrontaliera di coordinamento tra il Presidente del Nucleo per la cybersicurezza (*Executive*[11] per l'Italia in CyCLONe) e i suoi omologhi europei, anche ai fini della potenziale attivazione dei meccanismi previsti dall'IPCR.

Più in particolare, CyCLONe prevede la partecipazione di rappresentanti delle Autorità nazionali competenti per la gestione delle crisi *cyber* ed è volta a garantire la preparazione, la *situational awareness*, nonché un efficace raccordo nella gestione delle crisi, offrendo supporto al livello politico sia in ambito nazionale che europeo. Nel periodo in esame, in aggiunta alle consuete attività di scambio informativo, l'Agenzia ha preso parte alla quarta e alla quinta riunione degli *officer*[12] di CyCLONe, svoltesi, rispettivamente, nei mesi di settembre e novembre 2021.

Particolare rilevanza assume, inoltre, lo svolgimento di esercitazioni volte a rafforzare la capacità globali di risposta agli incidenti e innalzare il grado di preparazione in situazioni di crisi.

Al riguardo, sempre in ambito europeo, con il supporto della Commissione europea e dell'Agenzia europea per la sicurezza informatica-ENISA, viene organizzato con cadenza annuale il *Blueprint Operational Level Exercise*-Blue OLEx, volto a testare e rafforzare le capacità dell'Unione in situazioni di crisi *cyber* su vasta scala e migliorare la cooperazione tra le Autorità nazionali *cyber* degli Stati Membri e le Istituzioni europee. La terza edizione di Blue OLEx si è svolta nell'ottobre del 2021 in Romania, con lo scopo di testare le procedure operative *standard* di CyCLONe a livello di *Executive*. Tale edizione è stata collegata – attraverso la condivisione dello scenario, nonché degli esiti – ad ulteriori esercizi svolti in ambito europeo, di cui uno all'inizio del mese di ottobre, che ha visto la partecipazione dell'Agenzia (CyberSOPEx 2021, esercitazione di livello tecnico, con il coinvolgimento della rete europea dei CSIRT).

Sul piano internazionale si è svolta, a fine ottobre 2021, in ambito G7 Energia, un'esercitazione tecnica rivolta ad esperti del settore privato (*G7 Hands-on Cybersecurity for Digital Energy Infrastructure Systems*).

[11] Tale ruolo è ricoperto dai Vertici delle Autorità nazionale *cyber* degli Stati membri.

[12] Si tratta dei rappresentanti degli Stati membri a livello di funzionari.

L'Agenzia ha contribuito alla fase di pianificazione, ingaggiando gli operatori nazionali che hanno partecipato all'esercitazione con i propri esperti, e ha inoltre assicurato il ruolo di osservatore nazionale. L'esercizio ha visto i giocatori dei Paesi partecipanti cooperare per rispondere ad una varietà di attacchi *cyber* condotti in danno di un operatore del settore energia.

In ambito NATO l'Agenzia ha partecipato, in qualità di osservatore, su invito del Ministero della difesa – Amministrazione responsabile per la pianificazione a livello nazionale – all'esercitazione NATO *Cyber Coalition* 2021, fornendo unità tecniche in qualità di giocatori. L'esercitazione ha fornito l'occasione per aumentare il grado di conoscenza dei meccanismi di risposta agli incidenti *cyber* in ambito NATO, nonché acquisire utili elementi esperenziali circa le relative procedure.

L'Agenzia ha inoltre fornito il proprio contributo alle attività di pianificazione dell'edizione *Cyber Europe* 2022, evento promosso da ENISA per il rafforzamento dei meccanismi europei di gestione degli incidenti e delle crisi di cybersicurezza su vasta scala, così come delineati dal *Blueprint*.

Inoltre, nell'ambito del programma esercitativo congiunto UE-NATO *Parallel and Coordinated Exercise*-PACE[13], l'Agenzia – sotto il coordinamento dell'Ufficio del Consigliere Militare della Presidenza del Consiglio dei ministri, che detiene la titolarità dell'esercizio a livello nazionale – ha seguito le attività di pianificazione della componente *cyber* di PACE EU *Integrated Resolve* 2022 (avviate nel dicembre 2021), evento promosso dal Servizio Europeo per l'Azione Esterna, congiuntamente al Consiglio dell'UE e alla Commissione Europea, con l'obiettivo di esercitare le capacità dell'Unione di rispondere a crisi transfrontaliere e minacce ibride, coinvolgendo i livelli operativo e politico-strategico, nonché di testare la cooperazione con la NATO.

[13] L'iniziativa è stata realizzata per la prima volta nel biennio 2017-2018, con lo svolgimento, lato NATO, della *Crisis Management Exercise*-CMX17 e, lato UE, della EU *Hybrid Exercise Multilayer* 18 (PACE).

Il Perimetro di Sicurezza Nazionale Cibernetica

Nella rinnovata architettura istituzionale, come detto, l'Agenzia ha assunto un ruolo centrale anche per l'attuazione del Perimetro di sicurezza nazionale cibernetica-PSNC, in quanto ha accentrato le funzioni regolamentari, di certificazione, ispezione, vigilanza e sanzionatorie, precedentemente attribuite a DIS, all'allora MiSE e alla Presidenza del Consiglio dei ministri-MITD.

Il PSNC è stato istituito dal decreto-legge 21 settembre 2019, n. 105, al fine di assicurare un elevato livello di sicurezza delle reti, sistemi informativi e servizi informatici degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziale, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. A tal fine, è costituito presso l'ACN e presieduto dal Direttore generale, il cd. Tavolo Perimetro, a supporto del CIC, per assicurare il coordinamento interministeriale, specie in relazione all'individuazione delle funzioni e dei servizi essenziali dello Stato, nonché dei soggetti che li erogano.

Oltre al citato decreto-legge n. 105, la normativa PSNC consta di cinque provvedimenti attuativi, di cui quattro già in vigore nel periodo in esame. Essi definiscono, rispettivamente:

- i settori ai quali si applica la normativa, le nozioni di funzioni e servizio essenziale, i criteri per l'individuazione dei soggetti inclusi nel Perimetro e il procedimento per l'individuazione e la comunicazione dei beni ICT inclusi nello stesso (DPCM n. 131/2020);

- la tassonomia degli incidenti, le misure di sicurezza volte a garantire la sicurezza dei beni ICT inclusi nel PSNC e le modalità di notifica degli incidenti (DPCM n. 81/2021);

- le modalità di esecuzione delle attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi di normativi, di esecuzione dello scrutinio tecnologico da parte del Centro di valutazione e certificazione nazionale-CVCN e dei centri di valutazione-CV del Ministero dell'interno e del Ministero della difesa, nonché dei criteri di natura tecnica per l'individuazione delle categorie di beni, sistemi e servizi ICT a cui si applica lo scrutinio tecnologico (DPR n. 54/2021);

- le categorie di prodotti ICT sottoposti allo scrutinio tecnologico del CVCN e dei CV (DPCM 15 giugno 2021).

Le modalità di accreditamento dei Laboratori di prova-LAP e di raccordo tra il CVCN, i laboratori di prova accreditati e i CV del Ministero dell'interno e del Ministero della difesa sono state definite con un regolamento approvato dal DPCM 18 maggio 2022, n. 92, alla cui elaborazione – avvenuta anche nel periodo di riferimento – l'Agenzia ha dato un importante contributo.

In tale contesto, l'Agenzia ha proseguito l'attività di "accompagnamento" dei soggetti inclusi nel PSNC nel processo di implementazione degli obblighi normativi, ai fini di una corretta interpretazione delle disposizioni ancora in fase di "prima applicazione".

A beneficio di tali soggetti, anche al fine di fornire un supporto più strutturato, l'Agenzia ha elaborato un documento di facile consultazione, che raccoglie i riscontri ai quesiti emersi con maggiore frequenza nelle interlocuzioni con i soggetti (cd. FAQ PSNC).

Nel documento sono state fornite informazioni di carattere generale attinenti alle finalità e all'ambito di operatività del Perimetro, agli adempimenti e ai termini da rispettare, nonché alle modalità di comunicazione con l'Agenzia.

In ragione della centralità che rivestono nell'architettura PSNC, specifica attenzione è stata accordata alle modalità e ai criteri di individuazione, descrizione e comunicazione all'Agenzia dei beni ICT da inserire nel Perimetro.

Un altro punto sviluppato nelle FAQ è quello relativo alle misure di sicurezza, rispetto a cui sono stati descritti sia gli elementi di carattere generale, sia le modalità di implementazione di specifiche misure. Inoltre, sono state illustrate le modalità di descrizione e trasmissione per l'assolvimento dell'obbligo di comunicare all'ACN l'avvenuta implementazione delle misure stesse. Sono state, poi, prese in considerazione le modalità e le tempistiche di notifica degli incidenti.

Il citato documento è stato pubblicato nel portale ad accesso controllato dedicato ai soggetti (https://perimetro.csirt.gov.it) e viene integrato ogni volta che nuovi quesiti frequenti o di rilevanza generale emergono.

Sullo stesso fronte sono state predisposte delle linee guida relative agli obblighi, stabiliti nell'ambito delle citate misure di sicurezza, di comunicazione al CSIRT Italia degli esiti dei *penetration test* e dei *vulnerability assessment*. In particolare, il documento chiarisce aspetti di ordine pratico, specie in riferimento al contenuto tecnico delle relazioni periodiche, alle relative modalità di comunicazioni al CSIRT Italia, nonché alle tempistiche. Ciò al fine di individuare un bilanciamento tra la quantità e la qualità delle informazioni condivise dai soggetti con l'ACN.

L'Agenzia ha inoltre provveduto a elaborare un modello per la descrizione delle modalità di implementazione delle misure di sicurezza. Tale modello richiede di specificare per ogni misura di sicurezza:

- lo stato di implementazione, compreso di una sintesi descrittiva delle modalità di realizzazione dal punto di vista organizzativo, tecnologico e di processo;
- il livello di maturità raggiunto nell'implementazione, secondo una scala di valutazione definita dal modello;
- una stima della complessità, in termini di sforzo sostenuto dal soggetto per realizzare la relativa misura;
- i riferimenti alla documentazione interna ad evidenza di quanto descritto.

È prevista, inoltre, la possibilità di fornire facoltativamente ulteriori informazioni, in relazione:

- alle tecnologie e agli strumenti utilizzati per l'implementazione;
- alle metodologie e agli standard di riferimento impiegati a supporto dell'adozione delle misure;
- ad eventuali interventi di rafforzamento già programmati, volti ad innalzare il livello di maturità delle misure, e, se del caso, ai relativi impatti.

Con riferimento agli adempimenti in capo ai soggetti inclusi nel Perimetro, si sono succedute nel periodo in riferimento, due importanti scadenze (vedasi Figura 10)[14]:

- 16 dicembre 2021, termine per la trasmissione dell'elenco dei beni ICT per i soggetti che hanno ricevuto la notifica di iscrizione nel giugno 2021;
- 25 dicembre 2021, termine per l'adozione delle misure di sicurezza di categoria A[15], con successiva trasmissione delle relative modalità di implementazione per i soggetti che hanno ricevuto la notifica di iscrizione nel dicembre 2020.

[14] La normativa Perimetro prevede che i soggetti trasmettano all'ACN l'elenco dei beni ICT, nonché le modalità di adozione delle misure di sicurezza, secondo i termini dettati dai citati decreti, i quali decorrono per ciascun soggetto a partire dalla data di notifica di iscrizione nell'elenco dei soggetti Perimetro.

[15] Le misure di sicurezza individuate dal DPCM n. 81/2021 sono classificate in due gruppi: quelle di categoria A, con un termine di adozione di 6 mesi, sono quelle di più agevole implementazione; quelle di categoria B, con un termine di 30 mesi, sono quelle la cui implementazione, invece, risulta più onerosa in termini organizzativi ed economici.

Figura 10: Successione temporale dei termini per gli adempimenti previsti dalla normativa Perimetro

#3

Sviluppo della resilienza delle infrastrutture tecnologiche del Paese

Sviluppo della resilienza delle infrastrutture tecnologiche del Paese

Progettualità PNRR

Come già accennato, nell'ambito dell'attuazione delle progettualità connesse al PNRR, il Dipartimento per la trasformazione digitale-DTD della Presidenza del Consiglio dei ministri, in qualità di "Amministrazione Titolare", ha designato l'ACN quale "Soggetto Attuatore" dell'Investimento 1.5 *Cybersecurity* rientrante nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo" - Componente 1 "Digitalizzazione, innovazione e sicurezza nella PA". Tale designazione è stata formalizzata con la definizione del piano operativo di attuazione delle progettualità connesse all'investimento e la successiva stipula, il 15 dicembre 2021, dell'accordo tra DTD e ACN.

In accordo al citato piano operativo, l'Agenzia ha quindi definito una pianificazione delle iniziative progettuali da realizzare, in accordo agli obiettivi e traguardi definiti per il PNRR con la Commissione europea. Le iniziative, finanziate per un importo pari a euro 623 milioni, permetteranno di rafforzare l'ecosistema digitale nazionale potenziando i servizi di gestione della minaccia *cyber*, nonché supportando l'avvio e il potenziamento delle capacità dell'ACN. Nel dettaglio, l'investimento si articola sui seguenti obiettivi strategici:

- rafforzare le capacità di *cyber resilience* del Paese in modo diffuso, favorendo sinergie e l'interconnessione delle capacità di monitoraggio, condivisione di informazioni e risposta agli eventi di natura *cyber*;

- sviluppare le capacità nazionali di scrutinio tecnologico e certificazione, al fine di valutare e certificare beni, sistemi e servizi ICT, nell'ambito dell'attivazione del CVCN, istituito presso l'ACN, e per la costituzione di una rete di laboratori nazionali;

- innalzare le capacità *cyber* della pubblica amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini.

Ciò, anche in vista dell'attivazione, avvenuta successivamente al periodo in riferimento, di varie iniziative progettuali direttamente realizzate dall'Agenzia stessa (cd. a titolarità), nonché avvisi pubblici coordinati dall'ACN volti alla distribuzione di fondi verso soggetti terzi (cd. a regia).

Tra le iniziative a titolarità, l'Agenzia, nel periodo in esame, ha proceduto a identificare una serie di progettualità prioritarie da realizzare, tra le quali un HyperSOC nazionale e una rete di condivisione e analisi di informazioni *cyber* (ISAC). Favorendo l'opportuno coinvolgimento del settore privato e delle amministrazioni pubbliche, queste progettualità si inseriscono nell'ambizioso piano di raggiungimento di un'autonomia

tecnologica nazionale mediante lo sviluppo di competenze e strumenti di individuazione, analisi e contenimento di potenziali minacce ed eventi di interesse.

Di contro, tra le iniziative a *regia*, l'Agenzia ha individuato diversi ambiti prioritari per il finanziamento di nuove progettualità, tra cui:

1. interventi di identificazione, analisi e innalzamento del livello di maturità della gestione del rischio *cyber* nella pubblica amministrazione, sia centrale che locale, favorendo una più sistematica definizione di piani di investimento strategici per la cybersicurezza della PA;

2. interventi rivolti a supportare la creazione e il potenziamento della rete nazionale di scrutinio tecnologico e certificazione, favorendo lo sviluppo di capacità di identificazione e analisi di potenziali fattori di rischio.

Scrutinio tecnologico e Certificazione

Il raggiungimento di un'autonomia tecnologica nazionale passa necessariamente anche dal potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica.

SCRUTINIO TECNOLOGICO

Analisi su componenti *hardware* e *software* di sistemi e prodotti al fine di valutarne gli aspetti di sicurezza, anche tramite l'utilizzo di tecniche di simulazione di attacchi informatici (*ethical hacking*).

In quest'ottica l'Agenzia mira a costituire una rete di personale tecnico altamente specializzato, con capacità di analisi e valutazione degli aspetti di cybersicurezza nelle tecnologie più innovative e strategiche per il Paese. La crescita, a livello nazionale, di tali capacità di analisi costituirà un volano per acquisire competenze tecnico/ingegneristiche specifiche e consentire la crescita in settori tecnologici ad oggi appannaggio di Paesi stranieri, riducendo al contempo la dipendenza dell'Italia dalle tecnologie estere.

Al fine di garantire elevati *standard* di affidabilità e ripetibilità delle valutazioni svolte, la competenza tecnica deve essere necessariamente affiancata da schemi di certificazione che con-

SCHEMA DI CERTIFICAZIONE DI SICUREZZA

L'insieme di procedure, metodologie e regole necessarie per la valutazione della sicurezza informatica e la certificazione di sistemi o prodotti ICT. Esempi di schemi di certificazione sono lo schema nazionale, istituito con il DPCM del 30 ottobre 2003 e i sistemi europei che saranno adottato ai sensi del Regolamento (UE) 2019/881 "*Cybersecurity Act*".

sentano di ottenere un'indicazione chiara, oggettiva e universalmente riconosciuta circa il livello di sicurezza di un sistema o prodotto. Tali schemi devono essere costantemente aggiornati ed integrati per far fronte all'evoluzione sia della tecnologia sia delle minacce cibernetiche.

A tal fine, quale Autorità nazionale per la certificazione della cybersicurezza, l'Agenzia partecipa attivamente a gruppi di lavoro internazionali ed europei dedicati allo sviluppo e al raffinamento di schemi e sistemi di certificazione di sicurezza specifici per le differenti aree tecnologiche. In particolare, l'Agenzia partecipa alle attività volte all'elaborazione di sistemi di certificazione europei, ai sensi del Regolamento (UE) 2019/881 "*Cybersecurity Act*", dedicati alla certificazione di tecnologie fondamentali per lo sviluppo del Paese, quali le reti mobili di quinta generazione (5G) e le tecnologie di *cloud computing*.

Strategia Cloud Italia

L'adozione della Strategia Cloud Italia rappresenta una delle principali azioni di *policy* volte ad innalzare i livelli di cybersicurezza della pubblica amministrazione. La Strategia Cloud Italia si pone quale precursore di iniziative volte alla costruzione della sovranità e dell'autonomia tecnologia dell'Unione europea nella gestione dei dati dei cittadini e delle aziende europee, a partire dal settore pubblico.

Il documento di indirizzo è stato presentato il 7 settembre 2021 dal Ministro per l'innovazione tecnologica e la transizione digitale *pro tempore*, dall'Autorità delegata per la sicurezza della Repubblica *pro tempore* e dal Direttore generale dell'Agenzia per la cybersicurezza nazionale. Tale documento, elaborato dal DTD e dall'ACN, è parte integrante del PNRR.

La Strategia Cloud Italia, individua tre obiettivi strategici che caratterizzano il percorso di trasformazione:

- incentivare le amministrazioni all'adozione di soluzioni basate sul *cloud computing*, attraverso il modello cloud della PA, 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 europeo;

- garantire la sicurezza degli *asset* strategici per il Paese, mediante lo sviluppo di un'infrastruttura ad alta affidabilità promossa dalla Presidenza del Consiglio dei ministri, consentendo il consolidamento dei *data center* delle amministrazioni centrali;

- valorizzare le amministrazioni e la loro capacità di offrire servizi digitali.

Con riferimento all'implementazione della citata Strategia, l'ACN offre supporto agli attori coinvolti in relazione agli aspetti di cybersicurezza. In particolare, l'ACN, d'intesa con il DTD:

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

- individua le modalità del procedimento di qualificazione dei servizi;

- definisce un modello per l'elencazione e la classificazione dei dati e dei servizi digitali della pubblica-amministrazione.

Tale ultimo punto rappresenta, in particolare, un primo esercizio volto a individuare l'opportuno bilanciamento tra requisiti e costi, svolgendo un censimento dei servizi digitalizzati della PA da collocare nelle seguenti tre classi:

- servizi strategici, la cui compromissione può arrecare pregiudizio alla sicurezza nazionale;

- servizi critici, la cui compromissione può compromettere il mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;

- servizi ordinari, non rientranti nei casi di cui sopra.

In tale contesto, l'Agenzia ha contribuito sostanzialmente all'elaborazione del cd. Regolamento Cloud, adottato ai sensi dell'articolo 33-*septies* del D.L. 179/2012, da AgID con Determinazione del 15 dicembre 2021, n. 628[16], ed ha, inoltre, avviato la predisposizione delle previste Determinazioni implementative dell'ACN e dei processi interni necessari per la trattazione delle pratiche di classificazione dei servizi di circa 22.000 enti pubblici in un lasso temporale estremamente ambizioso.

[16] Ciò nelle more del passaggio di competenze all'ACN previsto dal decreto-legge.

#4

La cooperazione internazionale

La cooperazione internazionale

Come anticipato, a valle della riforma operata dal decreto-legge, l'ACN è divenuta titolare del coordinamento, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale-MAECI, della cooperazione internazionale in materia di cybersicurezza, assicurando, con riferimento all'ambito istituzionale di competenza, l'interazione con organismi, istituzioni ed enti a livello europeo e internazionale.

Alla luce della natura intrinsecamente transnazionale della minaccia *cyber*, l'ACN ha avviato e rafforzato, fin dalla fase di prima operatività, i contatti con i principali interlocutori internazionali del settore – tra cui omologhe agenzie/autorità nazionali e competenti organizzazioni intergovernative – intessendo una fitta e solida rete di collaborazioni e rapporti, basata, *in primis*, sulla cooperazione bilaterale e multilaterale tra Paesi *like-minded*.

Il posizionamento internazionale dell'ACN

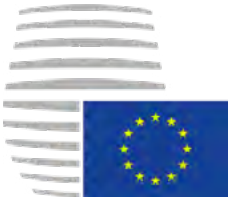
In questa prospettiva, l'Agenzia ha sviluppato, sulla base di un dettagliato piano di *reach out* verso *partner* e Autorità nazionali omologhe, proficue interlocuzioni internazionali tanto a livello multilaterale, continuando ad assicurare la presenza dell'Italia nei principali consessi in materia *cyber*, quanto a livello bilaterale, rinnovando o aprendo nuovi canali di comunicazione e collaborazione con enti, istituzioni od analoghe Agenzie straniere – tra cui, a titolo esemplificativo, la *Cybersecurity and Infrastructure Security Agency*-CISA statunitense, il *Bundesamt für Sicherheit in der Informationstechnik*-BSI tedesco, l'*Agence nationale de la sécurité des systèmes d'information*-ANSSI francese, nonché con la *DG Connect*, l'*European External Action Service* (EEAS) della Commissione europea e la NATO. Di rilievo è stata, poi, la partecipazione ai tavoli multilaterali.

Ciò è stato possibile anche grazie allo svolgimento, fin dai primi mesi di attività, di visite istituzionali e incontri di vertice con esponenti di spicco delle diverse controparti coinvolte, sia in formato virtuale, sia accogliendo delegazioni straniere presso la sede dell'Agenzia ovvero tramite le rispettive rappresentanze diplomatiche. Queste attività, condotte in fase di prima operatività e, dunque, a regime ridotto di risorse, hanno nondimeno dato vita ad un fruttuoso interscambio di esperienze, *know-how* e *best practice* tra i diversi organismi dei Paesi *partner* di volta in volta rappresentati e l'ACN, contribuendo in ultima analisi a rafforzare e consolidare il già ampiamente riconosciuto posizionamento internazionale dell'Italia in ambito *cyber*.

In tale contesto, l'ACN ha assicurato, in costante raccordo con le Amministrazioni di volta in volta inte-

ressate, la partecipazione, in particolare, a oltre 50 riunioni a livello multilaterale e 15 in forma bilaterale, prevalentemente in videoconferenza.

La cooperazione in ambito europeo



Sul versante europeo, l'Agenzia ha garantito, in raccordo con il MAECI, la partecipazione ai lavori dell'*Horizontal Working Party on Cyber Issues*-HWPCI, consesso istituito in seno al Consiglio dell'UE per l'elaborazione e l'implementazione delle *policy* in materia di cybersicurezza. In tale sede sono stati negoziati documenti quali le *Council Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises* e la proposta della cd. Direttiva NIS 2.

Al fine, infatti, di capitalizzare i successi raccolti nell'implementazione della prima Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, cd. NIS, gli Stati membri e le istituzioni europee sono state impegnate nel processo di revisione della stessa, in linea con la EU *Cybersecurity Strategy for the Digital Decade* del dicembre 2020. Tale processo ha visto un intenso coordinamento a livello nazionale, numerose interlocuzioni con organi internazionali interessati (come l'ICANN), nonché dinamiche discussioni nei consessi preposti del Consiglio e della Commissione, con l'adozione di una posizione formale del Consiglio UE Trasporti, Telecomunicazioni ed Energia-TTE il 3 dicembre 2021.

La revisione della Direttiva NIS si pone degli obiettivi ambiziosi per elevare ulteriormente la resilienza *cyber* dell'UE, tra cui:

- un significativo allargamento dei settori di competenza, nel rispetto della sovranità nazionale, e una omogeneizzazione delle modalità di identificazione degli operatori soggetti alla norma;
- l'adozione di strategie nazionali per la gestione delle crisi *cyber* e l'istituzione formale del *Cyber Crises Liaison Organisation Network*-CyCLONe, la rete di cooperazione in situazione di crisi transfrontaliera in materia (vds. Sezione 2.2.1);
- l'introduzione di un meccanismo di *Coordinated Vulnerability Disclosure*-CVD e l'elaborazione di analisi del rischio, a livello europeo, sulla catena di approvvigionamento di prodotti ICT ritenuti critici;
- un rafforzamento delle misure di sicurezza, con un approccio *all-hazards* e il ricorso alle certificazioni di cybersicurezza europee previste dal *Cybersecurity Act*, nonché dei relativi poteri di supervisione e sanzione.

L'Agenzia ha partecipato attivamente ai lavori del NIS *Cooperation Group*-NISCG, istituito dalla Direttiva NIS, volto alla cooperazione e lo scambio informativo relativo alle *policy* di cybersicurezza tra Paesi dell'Unione. Anche tenuto conto del citato negoziato sulla Direttiva NIS2, il gruppo si è focalizzato sull'aggiornamento del proprio programma di lavoro e sulle nuove sfide poste dalla proposta di Direttiva. Oltre a presidiare le riunioni plenarie trimestrali del NISCG, l'ACN ha coordinato, in qualità di co-presidente, le attività del *Work Stream on Large Scale Cyber Incident and Crises* e del *Work Stream on 5G Cybersecurity*. Con riferimento a quest'ultimo, l'ACN, nel periodo in esame ha partecipato a due riunioni, nel corso delle quali, oltre che al consueto accompagnamento alle attività di implementazione del *Toolbox* 5G negli Stati membri e delle relative misure di sicurezza, i lavori del gruppo si sono incentrati sull'analisi dei rischi e delle opportunità offerte dall'architettura *Open Radio Access Network*-RAN, nonché sulle iniziative in corso sull'elaborazione di un apposito sistema di certificazione europeo (EU5G).

In tale contesto, di concerto con l'allora Ministero della transizione ecologica[17], l'Agenzia ha anche preso parte al *Work Stream on Energy* del NISCG, specie per seguire il processo di adozione e negoziale della proposta di *Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows* avanzata da ENTSO-E e EU DSO[18] ai sensi dei Regolamenti UE 2019/942 e 2019/943[19]. In tali occasioni, l'Agenzia ha svolto il ruolo di catalizzatore delle posizioni espresse dalla maggior parte degli Stati membri, ottenendo alcuni primi affinamenti del testo.

Sempre in ambito UE, particolarmente intensa è stata la collaborazione con ENISA. In particolare, l'ACN ha fornito un proprio contributo alla predisposizione del rapporto *Raising Awareness on Cybersecurity. A Key Element of National Cybersecurity Strategies*, contenente una serie di raccomandazioni per accrescere l'efficacia delle campagne nazionali di sensibilizzazione sulla *cybersecurity*, nonché alla definizione del *Cybersecurity Index* dell'UE, volto a valutare – in linea con la Strategia di Sicurezza Cibernetica dell'Unione e con il relativo contesto normativo – i livelli di maturità dell'Unione e degli Stati Membri in termini di *policy*, capacità e operatività, nonché di maturità del mercato e del settore industriale.

[17] Anche nelle more del passaggio di competenze relativo alle funzioni di Autorità competente NIS ai sensi del D.Lgs. 65/2018.

[18] Rispettivamente l'*European Network of Transmision System Operators*, l'associazione degli operatori di trasmissione energetica (TSO) dei Paesi UE e limitrofi, e l'analoga associazione degli operatori di gestione di energetica elettrica (*Distribution System Operator*).

[19] Rispettivamente il Regolamento che istituisce un'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia (ACER) e il Regolamento sul mercato interno dell'energia elettrica.

In ambito certificazioni di cybersicurezza UE, in raccordo con il Ministero dello sviluppo economico (ora "delle imprese e del *made in Italy*")[20] e il Dipartimento per la transizione digitale della Presidenza del Consiglio dei ministri, l'Agenzia ha, in particolare, seguito lo sviluppo dello schema di certificazione di cybersicurezza per i fornitori di servizi *cloud*. Si tratta del secondo schema di certificazione elaborato ai sensi del *Cybersecurity Act* [21] da ENISA, la cui prima versione è stata pubblicata a dicembre 2020, volto a elevare la cybersicurezza e ridurre la frammentazione nel mercato del *cloud computing* identificando tre livelli di certificazione. In linea con i principi espressi dalla citata Strategia Cloud Italia e dai discendenti atti implementativi volti ad affermare la sovranità europea dei dati (vds. Sezione 3.3), l'Agenzia, in raccordo con le omologhe entità di alcuni Stati membri allineati, ha promosso un rafforzamento del livello di certificazione più stringente in ambito bilaterale, multilaterale, nonché nel *Ad-Hoc Working Group* dedicato di ENISA.

Le attività internazionali

Nell'ambito delle attività internazionali, per quel che concerne le Nazioni Unite, l'Agenzia ha partecipato al Gruppo di lavoro interministeriale sul *cybercrime*, riunitosi per la prima volta il 28 settembre 2021, sotto il coordinamento del MAECI, volto a definire la posizione nazionale nell'ambito dei negoziati della Convenzione internazionale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali, in vista della prima sessione dei lavori, tenutasi a New York dal 17 al 28 gennaio 2022. Nel contesto del citato consesso si è provveduto a garantire una posizione nazionale unitaria e coerente con le politiche di cybersicurezza del nostro Paese, anche alla luce delle norme internazionali a cui l'Italia ha aderito, Convenzione di Budapest *in primis*, nonché in ossequio al principio della neutralità tecnologica, al fine di assicurare che le norme penali non divengano obsolete con l'avanzare dello sviluppo tecnologico, rafforzando, al contempo, la cooperazione internazionale, le attività di assistenza tecnica e *capacity building*.

In relazione, poi, all'*International Telecommunication Union*-ITU – agenzia dell'ONU specializzata nelle tecnologie dell'informazione e della comunicazione – l'ACN non ha mancato di fornire un proprio contributo per l'aggiornamento del questionario in base al quale sarà predisposta, da quell'organizzazione, la quinta edizione del *Global Cybersecurity Index*, suddiviso in 5 aree tematiche: misure legali, tecniche, organizzative, di sviluppo capacitivo e cooperazione.

[20] Anche nelle more del passaggio di competenze relativo alle funzioni di Autorità di certificazione nazionale ai sensi del *Cybersecurity Act*.

[21] Regolamento UE 2019/881 relativo all'ENISA e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione.

Nel contesto dell'Organizzazione per la sicurezza e la cooperazione in Europa-OSCE, in occasione della riunione dell'*Informal Working Group*-IWG sul *cyber* del 9 novembre 2021, il nostro Paese ha adottato la *Confidence Building Measures*-CBM n. 14[22], focalizzata sulla partnership pubblico-privato. Il nostro Paese è divenuto così membro attivo del gruppo di lavoro - attualmente composto anche da Austria, Belgio, Estonia, Finlandia e Svezia - dopo averne seguito i lavori per circa un anno in veste di osservatore.

CBMs

Confidence Building Measure(s) for Cyberspace. In ambito OSCE, il termine indica un set di misure che mira a innalzare la fiducia tra Stati e ridurre i potenziali conflitti derivanti dall'utilizzo delle tecnologie ICT.

Sempre in ambito OSCE, l'Agenzia ha inoltre preso parte al *meeting* annuale dei Punti di contatto-PoC stabiliti dalla CBM n. 8, tramite personale del CSIRT Italia, designato quale PoC tecnico nazionale, in supporto del PoC "politico" individuato nell'ambito dell'Unità per le politiche e la sicurezza dello spazio cibernetico del MAECI. Al riguardo, nel mese di ottobre 2021, si è tenuto il periodico *Communication Check*, volto a testare la prontezza della risposta da parte dei citati PoC, sottoponendo loro dei quesiti che, nell'occasione, erano volti ad esplorare eventuali *policy* nazionali e linee-guida in materia di *Coordinated Vulnerability Disclosure*-CVD, e relativa applicazione.

L'ACN ha fornito un concreto contributo anche a livello NATO, con la quale sono state condivise le esperienze nazionali in materia di gestione incidenti e crisi cibernetiche, oltre che di strategia nazionale di cybersicurezza. Contributi sono stati, altresì, forniti nell'ambito dei negoziati dei documenti di *policy cyber*.

Sono state, inoltre, avviate interlocuzioni di vertice, al fine di stabilire e consolidare una proficua collaborazione in tema di resilienza e cybersicurezza.

[22] La quale prevede che «Gli Stati partecipanti, su base volontaria e conformemente alla legislazione nazionale, promuovano partenariati pubblico-privati e sviluppino meccanismi per lo scambio di migliori prassi per quanto concerne le risposte alle sfide comuni alla sicurezza derivanti dall'uso delle tecnologie dell'informazione e della comunicazione».

Infine, nel contesto delle attività multilaterali e delle relazioni con gli Stati Uniti, l'Agenzia ha coordinato la partecipazione nazionale alla cd. *Counter Ransomware Initiative*-CRI, iniziativa promossa dal *National Security Council* di quel Paese, al fine di cementare la cooperazione internazionale nel contrasto ai *ransomware*, minaccia sempre più pervasiva e impattante nel panorama *cyber* (vds. Sezione 2.1). A valle delle attività preparatorie, il 13 e 14 ottobre 2021 si sono riuniti virtualmente i Ministri e i rappresentanti di 31 Stati e dell'UE – per l'Italia era presente il Direttore generale dell'ACN – per sottoscrivere un *joint statement* e affermare l'impegno ad affrontare la minaccia su quattro direttive: *resilience, countering illicit finance, dirsuption (law enforcement)* e *diplomacy*.


REPUBBLICA ITALIANA
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT