IV COMMISSIONE PERMANENTE

(Difesa)

S O M M A R I O

SEDE REFERENTE

Mercoledì 2 aprile 2025. — Presidenza del presidente Antonino MINARDO. – Interviene il sottosegretario di Stato per le imprese e il made in Italy *Massimo Bitonci.*

La seduta comincia alle 8.30.

Disposizioni per l'esercizio della libertà sindacale del personale delle Forze armate e delle Forze di polizia a ordinamento militare, nonché di proroga della delega di cui all'articolo 9, comma 15, della legge 28 aprile 2022, n. 46.

C. 2171 Governo, approvato dal Senato.

(Seguito dell'esame e conclusione).

La Commissione prosegue l'esame del provvedimento, rinviato nella seduta di mercoledì 26 marzo scorso.

Antonino MINARDO, *presidente*, avverte che la Commissione, nella seduta odierna, prosegue l'esame in sede referente del disegno di legge C. 2171, approvato dal Senato, recante disposizioni per l'esercizio della libertà sindacale del personale delle Forze armate e delle Forze di polizia a ordinamento militare, nonché di proroga della delega di cui all'articolo 9, comma 15, della legge 28 aprile 2022, n. 46.

Ricorda come nella seduta del 26 marzo scorso, non essendo stati presentati emendamenti, il testo sia stato trasmesso alle Commissioni competenti in sede consultiva, nonché al Comitato per la Legislazione, per l'espressione dei prescritti pareri.

Avverte che sono pervenuti, oltre al parere del Comitato per la Legislazione, i pareri favorevoli delle Commissioni I, V e XI.

Nessuno chiedendo d'intervenire, la Commissione delibera di conferire al relatore il mandato a riferire favorevolmente all'Assemblea sul provvedimento in esame. Delibera, altresì, di chiedere l'autorizzazione a riferire oralmente.

Antonino MINARDO, *presidente*, avverte che la Presidenza si riserva di designare i componenti del Comitato dei nove sulla base delle indicazioni dei gruppi.

La seduta termina alle 8.35.

INDAGINE CONOSCITIVA

Mercoledì 2 aprile 2025. — Presidenza del presidente Antonino MINARDO.

La seduta comincia alle 8.35.

Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità.

(Esame e approvazione del documento conclusivo).

La Commissione inizia l'esame del documento conclusivo.

Antonino MINARDO, *presidente*, avverte che la pubblicità dei lavori della seduta odierna sarà assicurata anche mediante la resocontazione stenografica.

Fa presente che con la presentazione da parte della Presidenza della proposta di documento conclusivo in esame, già trasmesso ai singoli rappresentanti dei gruppi per le vie brevi *(vedi allegato)*, si avvia a conclusione l'indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità, avviata l'8 novembre 2023.

Auspica che la proposta di documento conclusivo possa incontrare un ampio consenso.

Stefano GRAZIANO (PD-IDP), giudicando positivamente il lavoro svolto dalla Commissione nell'ambito dell'indagine conoscitiva, auspica che l'approvazione della proposta di documento conclusivo in esame possa rappresentare un cambio di paradigma nell'approccio alla difesa cibernetica. Evidenzia, in particolare, la necessità di adottare le misure atte a permettere che la sicurezza cibernetica divenga materia di studio nelle accademie e scuole militari. Ritiene, da ultimo, che il testo in esame avrà il merito di portare all'attenzione del Governo temi di primario interesse per la difesa del Paese.

Antonino MINARDO, *presidente*, auspica che, a valle dell'approvazione della proposta di documento conclusivo, la Commissione valuti tutti i possibili contributi di carattere normativo che definiscano una cornice legislativa coerente con il ruolo della Difesa, al fine di rafforzare la resilienza del Paese di fronte a potenziali attacchi informatici.

La Commissione approva il documento conclusivo dell'indagine conoscitiva *(vedi allegato)*.

La seduta termina alle 8.40.

N.B.: Il resoconto stenografico della seduta è pubblicato in un fascicolo a parte.

INDAGINE CONOSCITIVA

Mercoledì 2 aprile 2025. — Presidenza del presidente Antonino MINARDO.

La seduta comincia alle 8.40.

Indagine conoscitiva sulla sicurezza nazionale e nuove sfide per la difesa.

(Deliberazione di una proroga del termine).

Antonino MINARDO, *presidente*, propone, sulla base di quanto stabilito dall'Ufficio di presidenza, integrato dai rappresentanti dei gruppi del 25 marzo scorso, ed essendo stata acquisita l'intesa con il Presidente della Camera dei deputati, ai sensi dell'articolo 144, comma 1, del Regolamento della Camera, la proroga del termine per la conclusione dell'indagine

conoscitiva sulla sicurezza nazionale e nuove sfide per la difesa al 2 ottobre 2025.

Nessuno chiedendo di intervenire, la Commissione delibera la proroga del termine dell'indagine conoscitiva proposta dal presidente.

La seduta termina alle 8.45.

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI

Mercoledì 2 aprile 2025.

L'ufficio di presidenza si è riunito dalle 8.45 alle 8.55.

ALLEGATO

Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità.

DOCUMENTO CONCLUSIVO APPROVATO

PREMESSA

L'esigenza di avviare un'indagine conoscitiva sulla difesa cibernetica, deliberata dalla Commissione Difesa della Camera dei deputati, ai sensi dell'articolo 144 del Regolamento, nella seduta dell'8 novembre 2023, nasce dalla constatazione che il tema della *cyberdefence* ha assunto crescente rilevanza in Italia (come nel resto del mondo) a causa dei numerosi attacchi informatici rivolti a soggetti sia privati che pubblici. La difesa cibernetica si sostanzia, infatti, in uno spettro di competenze dello Stato di natura prettamente militare, da inquadrare in una più ampia strategia nazionale per la sicurezza cibernetica, la cui architettura si è andata componendo grazie a una serie di interventi normativi, di seguito analiticamente ricostruiti.

Lo svolgimento dell'indagine conoscitiva da parte della Commissione Difesa sul tema delle nuove tecnologie della difesa applicate al dominio cibernetico ha dunque consentito, mediante l'apporto degli autorevoli esponenti del mondo accademico e delle istituzioni auditi, di meglio comprendere le diverse sfaccettature di questa nuova minaccia ibrida e trasversale e, di conseguenza, di costruire un patrimonio informativo incentrato sugli elementi indispensabili per assicurare forme di difesa cibernetica più moderne ed efficaci.

Il termine per la conclusione dell'indagine, inizialmente fissato al 30 giugno 2024, in seguito ad apposite proroghe, è stato fissato al 31 marzo 2025, al fine di consentire alla Commissione di concludere le audizioni programmate e di predisporre il documento conclusivo.

Nell'ambito dell'indagine conoscitiva, tra il 31 gennaio 2024 e il 23 gennaio 2025, sono state svolte le seguenti **28 audizioni**:

1) audizione del Sottosegretario di Stato, Segretario del Consiglio dei Ministri e Autorità delegata per la sicurezza della Repubblica, **Alfredo Mantovano** (*mercoledì 31 gennaio 2024*);
2) audizione del Direttore della Direzione informatica, telematica e tecnologie avanzate (TELEDIFE) del Ministero della Difesa, Ten. Gen. E.I. **Angelo Gervasio** (*giovedì 29 febbraio 2024*);
3) audizione di **Bruno Frattasi**, Direttore dell'Agenzia per la cybersicurezza nazionale (*giovedì 21 marzo 2024*);

4) audizione del Comandante del Comando per le Operazioni in Rete (COR), Gen. Sq. AAran **Sergio Antonio Scalese** (*giovedì 04 aprile 2024*);

5) audizione di **Emanuele Galtieri**, Amministratore delegato di CY4GATE S.p.A. (*martedì 07 maggio 2024*);

6) audizione di **Alessia Di Nucci**, Senior Public affairs manager di Fastweb S.p.A., e di **Francesco Aragano**, Head of Homeland Security & Infrastructures Sales di Fastweb S.p.A. (*mercoledì 15 maggio 2024*);

7) audizione di **Lorenzo Mariani**, Condirettore generale di Leonardo S.p.A., e di **Andrea Campora**, Capo divisione cyber sicurezza di Leonardo S.p.A. (*mercoledì 22 maggio 2024*);

8) audizione di **Gianmatteo Manghi**, Amministratore Delegato di Cisco Systems Italy S.r.l., di **Giuseppe Massa**, Responsabile Sicurezza Cibernetica di Cisco Systems Italy S.r.l., e di **Lorenzo Ghioni**, Direttore Cisco Photonics di Cisco Systems Italy S.r.l. (*giovedì 23 maggio 2024*);

9) audizione del Gen. di D. CC **Paolo Aceto**, Capo del III Reparto del Comando Generale dell'Arma dei Carabinieri, e di **Giovanni Bottazzi**, Capo Centro Sicurezza Telematica del Comando Generale dell'Arma dei Carabinieri (*mercoledì 29 maggio 2024*);

10) audizione del Gen. C.A. **Luciano Portolano**, Segretario Generale della Difesa e Direttore Nazionale degli Armamenti (*giovedì 30 maggio 2024*);

11) audizione di **Pierroberto Folgiero**, Amministratore delegato di Fincantieri S.p.A., e di **Daniele Alì**, Vice Presidente Cybersecurity di Fincantieri S.p.A. (*mercoledì 12 giugno 2024*);

12) audizione di **Benjamin Jolivet**, Country Manager di Nutanix Italy S.r.l., **Pasquale Potenza**, Senior Sales Director Italy S.r.l. e **Pierluigi Valentini**, Sales Manager S.r.l. (*mercoledì 03 luglio 2024*);

13) audizione di **Gianvittorio Abate**, Chief Executive Officer di Innovery S.p.A., **Guido Moscarella**, Direttore divisione cyber di Innovery S.p.A., **Pasquale Patricelli**, Sales director di Innovery S.p.A., e **Pietro Parente**, Corporate affairs&business development di Innovery S.p.A. (*mercoledì 10 luglio 2024*);

14) audizione del Presidente dell'Associazione nazionale giovani innovatori (ANGI), **Gabriele Ferrieri** (*giovedì 19 settembre 2024*);

15) audizione di rappresentanti di **Marco Valentini**, Group Director Public Affairs di Engineering S.p.A. e **Vito Morreale**, Responsabile Laboratorio Ricerca e Innovazione Data e Analytics di Engineering S.p.A. (*mercoledì 25 settembre 2024*);

16) audizione di **Antonio Amati**, Direttore Generale Divisione IT di Almaviva S.p.A., **Roberto Rossi**, Responsabile Mercato Difesa e Sicurezza di Almaviva S.p.A., e **Giovanni Giovanetti**, Responsabile Area Cyber Security di Almaviva S.p.A. (*mercoledì 09 ottobre 2024*);

17) audizione di **Alessandro Manfredini**, presidente dell'Associazione italiana professioni security aziendale (AIPSA) (*mercoledì 16 ottobre 2024*);

18) audizione di **Alessandro Rivara**, Direttore relazioni istituzionali di Akamai Italia e **Nicola Ferioli**, Head of Engineering di Akamai Italia (*giovedì 17 ottobre 2024*);

19) audizione di **Roberto Setola**, Professore ordinario di Automatica presso l'Università Campus Bio-Medico di Roma (*mercoledì 23 ottobre 2024*);

20) audizione di **Alessandro La Volpe**, Amministratore delegato di IBM Italia, e **Federico Mattei**, IBM Quantum Business Developer for Europe (*mercoledì 06 novembre 2024*);

21) audizione di **Ludovico Diaz**, CEO di NTT DATA Italia S.p.A., e di **Dolman Aradori**, Vice President, Head of Cyber Security Italia - NTT DATA Italia Spa (*mercoledì 13 novembre 2024*);

22) audizione di **Alessandro Moretti**, Presidente di MERIDIAN Group, Andrea Purificato, Vicedirettore generale di MERIDIAN Group, e **Aldo Carabellese**, Direttore dei servizi e delle operazioni internazionali di MERIDIAN Group (*martedì 19 novembre 2024*);

23) audizione di **Nicolò Bellorini**, Vicepresident Head of Business della divisione Mobile eXperience Samsung Electronics Italia S.p.A. (*giovedì 21 novembre 2024*);

24) audizione di **Domitilla Benigni**, Amministratore delegato di Elettronica S.p.A. (*giovedì 28 novembre 2024*);

25) audizione di **Paolo Boccardelli**, Rettore dell'Università LUISS Guido Carli - Libera Università Internazionale degli Studi Sociali, **Giuseppe Francesco Italiano**, Prorettore per l'intelligenza artificiale e le Digital

Skills nonché Professore Ordinario di Computer Science presso il Dipartimento di Impresa e Management della LUISS, e **Paolo Spagnoletti**, Professore associato, titolare della cattedra Vodafone in Cybersecurity and Digital Transformation presso il Dipartimento di Impresa e Management della LUISS (*martedì 03 dicembre 2024*);

26) audizione di **Nicola Sotira**, Responsabile CERT in ambito Tutela Aziendale di Poste italiane S.p.A. (*mercoledì 04 dicembre 2024*);

27) audizione di **Dario Lo Bosco**, Presidente di RFI Rete Ferroviaria italiana S.p.A. e **Riccardo Barrile**, Responsabile della Cyber Security di RFI Rete Ferroviaria italiana S.p.A. (*mercoledì 11 dicembre 2024*);

28) audizione del Ministro della difesa, **Guido Crosetto** (*giovedì 23 gennaio 2025*).

In aggiunta, la Commissione ha svolto le seguenti **missioni**:

- in data 28 maggio, presso gli uffici di **Engineering S.p.A**.;
- in data 10 luglio 2024, presso gli uffici di Roma di **Elettronica S.p.A**.

Proposte di lavoro della IV Commissione all'esito dello svolgimento dell'indagine conoscitiva sulla difesa cibernetica

1. Lo spazio cibernetico rappresenta un nuovo fondamentale dominio operativo accanto a quelli tradizionali di terra, aria, mare e spazio; un dominio operativo di importanza strategica per lo sviluppo economico, sociale e culturale delle nazioni ma anche un nuovo campo di battaglia e di competizione economica e geopolitica nel quale possono essere perpetrati attacchi dalla quale ci si deve difendere.

L'indagine conoscitiva svolta dalla Commissione Difesa ha infatti evidenziato come la sicurezza informatica rappresenti oggi una delle sfide più rilevanti per la sicurezza nazionale e globale, con un impatto che si estende trasversalmente sia sul settore pubblico sia su quello privato.

L'ultima Relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza ha ribadito la centralità del dominio cibernetico quale strumento preferenziale nel quale gli attori ostili fanno ricorso per il raggiungimento di obiettivi strategici. Le azioni malevoli più incisive che negli ultimi anni hanno investito il nostro Paese sono state condotte prevalentemente da gruppi altamente specializzati (Minacce Avanzate e Persistenti – APT), contigui ad apparati governativi dai quali ricevono linee di indirizzo strategico e supporto finanziario. Per questo sono ritenute le più insidiose per il Sistema Paese in termini di informazioni esfiltrate (di natura sia geo-politica, sia economico-industriale), di perdita di operatività e competitività, nonché di dispendio delle risorse economiche necessarie per la loro mitigazione.

2. L'interconnessione tra infrastrutture critiche, reti di telecomunicazione e sistemi digitali ha aumentato esponenzialmente la vulnerabilità degli Stati, rendendo la difesa cibernetica una necessità imperativa per la salvaguardia degli interessi nazionali.

La trasformazione digitale in corso ha, in particolare, moltiplicato i punti di accesso alle reti, aumentando al contempo la superficie di attacco disponibile per gli aggressori. Gli attacchi *ransomware*, le campagne di disinformazione e le violazioni dei dati sono diventati strumenti di guerra ibrida, con conseguenze non solo economiche ma anche geopolitiche.

L’ampia e autorevole platea dei soggetti auditi dalla Commissione è concorde nel sostenere che la sicurezza cibernetica non può più essere relegata a un ambito esclusivamente settoriale di competenza di pochi tecnici, ma deve essere affrontata come una priorità nazionale e internazionale, richiedendo investimenti strutturali e una *governance* della difesa cibernetica coordinata, flessibile e dinamica.

L'evoluzione della *cybersecurity* è peraltro sempre più legata allo sviluppo di tecnologie emergenti come **l'intelligenza artificiale e la computazione quantistica**. Queste innovazioni offrono opportunità significative per migliorare la protezione delle infrastrutture digitali, ma pongono anche nuove sfide che devono essere affrontate con un approccio strategico e integrato.

L'intelligenza artificiale, in particolare, sta rivoluzionando la *cybersecurity* grazie alla sua capacità di analizzare enormi quantità di dati in tempo reale, identificare schemi anomali e prevedere potenziali minacce con un livello di precisione prima sconosciuto. In questo quadro, nel corso dell’indagine, gli esperti hanno sottolineato come tale tecnologia dovrebbe essere utilizzata per automatizzare i processi di rilevamento degli attacchi, migliorare le risposte agli incidenti e rafforzare i sistemi di autenticazione basati su comportamenti anomali. Tuttavia, allo stesso tempo, la stessa intelligenza artificiale può essere sfruttata da attori malevoli per sviluppare attacchi più sofisticati, come *malware* adattativi o *deepfake* destinati alla manipolazione dell’informazione.

Del pari, anche le tecnologie quantistiche rappresentano, ad un tempo, un’opportunità e una minaccia per la sicurezza informatica: i computer quantistici, infatti, una volta sviluppati, potrebbero infrangere gli attuali algoritmi crittografici, rendendo obsolete le tradizionali tecniche di protezione dei dati. Per questo motivo, la ricerca sulla crittografia post-quantistica è diventata una priorità per le istituzioni e le aziende che operano nella sicurezza informatica.

Come più volte evocato dagli auditi, i nuovi sistemi di crittografia dovranno essere in grado di resistere alla potenza di calcolo dei computer quantistici, garantendo la protezione delle informazioni sensibili nel lungo termine.

L'integrazione di *cybersecurity*, intelligenza artificiale e tecnologie quantistiche richiede un quadro normativo aggiornato e un forte

investimento nella ricerca e sviluppo. È fondamentale, in questo contesto, promuovere la collaborazione tra settore pubblico e privato, garantire la formazione di esperti specializzati e sviluppare strategie di sicurezza che anticipino le minacce emergenti. L'ampia e autorevole platea dei soggetti auditi dalla Commissione è concorde nel sostenere che solo attraverso un approccio sinergico e multidisciplinare è possibile proteggere il cyberspazio in un'epoca di trasformazioni tecnologiche senza precedenti.

3. In questa prospettiva, la maggior parte degli auditi ha evidenziato come un elemento chiave per rafforzare la *cybersecurity* sia rappresentato dalla **formazione**, sia in ambito specifico sia in maniera trasversale nei diversi settori economici e istituzionali. Dall'indagine è emerso con chiarezza come investire sulla formazione di personale altamente qualificato nel settore *cyber* costituisca una priorità strategica per il Paese. In quest'ottica, più volte è emersa nel corso dell'indagine conoscitiva l'opportunità di rendere **la sicurezza informatica parte integrante dell'educazione scolastica**, promuovendo una maggiore consapevolezza tra i cittadini e garantendo la crescita di una generazione più preparata a fronteggiare le sfide digitali. In questo è stata più volte sottolineata l'importanza del ruolo svolto da campagne di sensibilizzazione, da realizzare a tutti i livelli della società, al fine di accrescere la consapevolezza del valore dei dati informatici e promuovere la formazione di una cultura diffusa sulla sicurezza informatica.

Un aspetto fondamentale della formazione riguarda indubbiamente il mondo accademico, rappresentato da autorevoli esponenti auditi nel corso dell'indagine. Dai loro contributi è emerso come le università e i centri di ricerca debbano **intensificare gli sforzi per sviluppare programmi di studio mirati**, con corsi specializzati in *cybersecurity*, crittografia avanzata, intelligenza artificiale applicata alla sicurezza informatica e gestione delle crisi *cyber*. Inoltre, da molte audizioni è emersa la necessità inderogabile di incentivare il trasferimento tecnologico tra accademia e industria, facilitando l'adozione di nuove tecnologie nei processi di difesa *cyber* delle aziende e delle istituzioni.

Nella medesima prospettiva si pone l'opportunità di realizzare una più stretta **cooperazione tra enti pubblici e imprese private**, cooperazione cruciale per sviluppare capacità di difesa più efficaci e garantire

un'integrazione delle competenze. Iniziative di partenariato pubblico-privato che coinvolgano istituzioni, università e imprese, se sostenute da un coerente e massiccio programma di investimenti, potrebbero invero contribuire significativamente alla creazione di programmi di formazione avanzata e dottorati industriali finalizzati alla formazione di figure apicali nella gestione delle minacce *cyber*.

Nel corso dell'indagine è emerso con chiarezza come anche l'industria privata svolga un ruolo fondamentale nella protezione delle infrastrutture critiche, molte delle quali sono gestite da aziende private.

La collaborazione tra aziende private e istituzioni pubbliche è essenziale per ottenere una difesa robusta e per condividere informazioni vitali sui rischi emergenti e sulle minacce in corso.

In tale direzione è emersa una proposta volta a sottolineare la necessità di promuovere l'integrazione della sicurezza fin dalla progettazione dei sistemi informatici, riducendo i rischi associati a interventi post-sviluppo, in una logica di "*cybersecurity by design*" La creazione di standard condivisi e l'adozione di *framework* di sicurezza costituiscono perciò elementi essenziali per ridurre la vulnerabilità delle reti. La sicurezza informatica non può e non deve più essere concepita come un semplice insieme di misure difensive, ma deve diventare un processo dinamico e adattivo che prevede la collaborazione continua tra pubblico e privato. In questa direzione, **la Commissione auspica un incremento delle risorse e degli investimenti pubblici e privati** con la finalità di garantire un rafforzamento dei **programmi di formazione** – trasversalmente e a tutti i livelli della società – sviluppati sinergicamente da attori pubblici e privati e capaci di rafforzare la consapevolezza e le capacità del Paese nel contrasto della minaccia *cyber*.

In tal senso, è stata spesso manifestata la necessità di stanziare investimenti strutturali volti ad assicurare adeguata protezione non solo e non tanto alle singole imprese ma, più incisivamente, a vantaggio dell'intero sistema produttivo, che è fortemente interconnesso e interdipendente, soprattutto in un contesto di *supply chain* globale, dove un attacco informatico a un anello della catena rischia di avere ripercussioni a cascata su tutti gli altri.

4. Quanto al tema della *governance,* nel corso dell'indagine è emerso come l'architettura strategica nazionale in materia di sicurezza e difesa cibernetica (più approfonditamente trattata nell'allegato approfondimento dedicato alla disciplina della sicurezza cibernetica in Italia) si fondi essenzialmente sui seguenti pilastri:

1) resilienza cibernetica, affidata all'Agenzia per la Cybersicurezza Nazionale (ACN), che ha il compito di rafforzare la capacità del Paese di resistere agli attacchi *cyber*, migliorando la protezione delle infrastrutture critiche e assicurando una rapida capacità di risposta in caso di attacchi.

2) difesa cibernetica, che rientra nell'ambito della difesa militare e implica misure di contrasto alle minacce cibernetiche, ponendo la sicurezza del Paese in una prospettiva prioritaria nel dominio cyber. In particolare, il Dicastero definisce e coordina la politica militare, la *governance* e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero (per una più articolata disamina si rinvia al successivo approfondimento);

3) criminalità cibernetica, affidata alle forze di polizia, in particolare alla Polizia Postale, per prevenire e contrastare le attività criminali in rete, dall'*hacking* alla diffusione di *malware* e alla protezione delle transazioni finanziarie *online*. Nell'ambito del Servizio di Polizia Postale e delle Comunicazioni, opera il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), quale unità specializzata nella protezione delle infrastrutture critiche informatizzate dai reati informatici e punto di contatto nazionale per le emergenze in materia di criminalità informatica transnazionale. Nell'ambito del Dipartimento di Pubblica Sicurezza, inoltre, è stata creata la Direzione Centrale per la polizia scientifica e la sicurezza cibernetica, nella quale confluiscono le attribuzioni di organo centrale del Ministero dell'Interno per la sicurezza e la regolarità delle comunicazioni e quelle di contrasto ai reati di sfruttamento sessuale per via informatica e di prevenzione del terrorismo, in precedenza assicurate dal Servizio polizia postale e delle comunicazioni. Presso la Direzione Centrale per la Sicurezza Cibernetica opera il *Computer Emergency Response Team* (CERT) del Ministero dell'Interno, istituito per garantire la sicurezza delle reti e dei sistemi informativi del Dicastero, attraverso la prevenzione e la

gestione degli eventi critici. Per quanto riguarda l'Arma dei Carabinieri, il Reparto Indagini Telematiche del Raggruppamento Operativo Speciale (ROS) costituisce l'articolazione specializzata dell'Arma nel contrasto alla criminalità informatica, nello studio e sperimentazione delle tecnologie per l'esplorazione del *web* e l'intercettazione dei flussi telematici, mentre per la Guardia di Finanza è il *Nucleo Speciale Tutela Privacy e Frodi Tecnologiche* (NSTPFT) quale reparto Speciale deputato al contrasto delle frodi telematiche ed informatiche, nonché alla tutela della *privacy*.

4) *cyberintelligence*, sotto la competenza dei servizi di informazione e sicurezza, per la raccolta e l'analisi di dati utili alla prevenzione degli attacchi e alla difesa proattiva nei confronti di minacce emergenti.

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

In relazione ai richiamati pilastri, nel corso dell'indagine è emerso come **l'attuale** l'architettura strategica nazionale in materia di sicurezza e difesa cibernetica **risulti priva di un comando unificato** durante le fasi critiche degli attacchi cibernetici con conseguenti ritardi nei meccanismi di risposta.

In particolare, il carattere ibrido e trasversale che caratterizza le minacce cibernetiche e la difficoltà di identificare con precisione la provenienza delle minacce rende poco agevole identificare la natura degli attacchi informatici, per cui la distinzione fra *cyberdefenc*e e *cybercrime*, chiara in teoria, sfuma in concreto.

Inoltre, il cyberspazio, come visto, è un ambiente interconnesso, privo di confini tangibili, in cui attacchi a settori civili possono avere ripercussioni diretti anche sulle infrastrutture militari e viceversa**.**

In questa direzione, il Ministro della Difesa, nel corso della sua audizione dello scorso 23 gennaio, nell'osservare che l'attuale assetto normativo assegna sostanzialmente alla Difesa il compito di proteggere le sole reti

militari, ha osservato che la distinzione tra reti militari e reti civili appare poco funzionale nel contrasto della minaccia cibernetica.

Viceversa, occorrerebbe che lo strumento militare**, nell'ambito delle proprie competenze istituzionali,** si occupasse della difesa del dominio cibernetico nella sua interezza, analogamente a quanto attualmente avviene nei domini tradizionali, come quello terrestre, marittimo, aereo e spaziale, nei quali la Difesa ha il compito di proteggere l'intero territorio e le infrastrutture strategiche della nazione.

5. In conclusione, i contributi acquisiti nel corso delle audizioni hanno messo in luce numerose tematiche chiave che attraversano diversi ambiti del settore della sicurezza e della difesa cibernetica. Tra queste, la formazione e la sensibilizzazione sulla sicurezza informatica, la collaborazione tra il settore pubblico e quello privato, l'importanza di un coordinamento istituzionale centrale, e la necessità di innovare e adottare tecnologie all'avanguardia. I soggetti auditi hanno fornito contributi significativi su questi temi, offrendo soluzioni concrete e una visione chiara delle sfide da affrontare. Le loro audizioni hanno non solo messo in luce le problematiche relative alla protezione delle infrastrutture critiche, ma anche proposto modelli operativi per l'implementazione di misure di difesa efficaci.

Ogni intervento ha contribuito a delineare un quadro assai complesso, nel quale la sicurezza cibernetica deve essere vista come un bene pubblico, una responsabilità collettiva e un elemento fondamentale per la sicurezza nazionale.

In particolare, è emerso un comune consenso in merito all'opportunità di avviare un percorso, anche di carattere normativo, che favorisca un approccio complessivo e integrato nei confronti della minaccia cibernetica, basato sulla collaborazione tra i diversi attori che definiscono il perimetro della sicurezza cibernetica.

La resilienza dei sistemi informatici, delle infrastrutture critiche e delle PMI, che costituiscono la spina dorsale dell'economia italiana, dipende dalla capacità di costruire una difesa a più livelli, che vada dalla protezione delle reti e dei dispositivi alla formazione dei professionisti, fino al coordinamento delle politiche a livello nazionale e internazionale.

Solo con una strategia globale che preveda il coinvolgimento di tutte le istituzioni pubbliche e private, le agenzie governative e le forze dell'ordine, ciascuno nell'ambito delle proprie competenze istituzionali, sarà possibile rispondere efficacemente alle sfide cibernetiche, che sono in costante evoluzione.

Con specifico riferimento ai profili di competenza della Difesa, l'indagine si è soffermata sulla nuova formulazione dell'articolo 88 del Codice dell'ordinamento militare (decreto legislativo n. 66 del 2010), che include ora il dominio cibernetico tra gli ambiti tutelati dalla difesa nazionale, quale funzione propria e principale dello strumento militare.

Partendo da tale presupposto, è emersa la necessità di assegnare allo strumento militare un ruolo più ampio nella protezione dell'intero cyberspazio nazionale e delle sue infrastrutture critiche, in sinergia con le autorità civili e con il settore privato.

Al contempo, è stato altresì sottolineato come un approccio multisettoriale, integrato e coordinato nel contrasto della minaccia cibernetica richieda l'adozione di procedure trasparenti e regolate che rendano chiaro l'apporto di tutti i soggetti inclusi nel perimetro di sicurezza cibernetica ed evitino contrasti o sovrapposizioni di competenze.

A tal riguardo, è stata auspicata, in ambito militare, una maggiore integrazione, in particolare, con l'Agenzia per la Cybersicurezza Nazionale volta a garantire sia una condivisione di competenze per specifiche aree, sia un apporto di personale nella protezione dell'intero cyberspazio nazionale e delle sue infrastrutture critiche.

Nel solco di questo orientamento è quindi emersa la possibilità di configurare, una capacità *cyber* integrata, specificatamente dedicata alla gestione delle minacce ibride, composta da personale civile e militare abilitato ad operare nello spazio cibernetico sulla base di precise regole d'ingaggio da sottoporre **al controllo del Parlamento**.

In tale ambito, nel pieno rispetto delle competenze di tutte le altre amministrazioni coinvolte nello specifico settore: *cyber resilience*, in capo all'Agenzia per la Cybersicurezza Nazionale, *cyber intelligence*, di competenza del Dipartimento Informazioni per la Sicurezza e le collegate Agenzie, *cyber crime & investigation*, attestata al Ministero degli Interni, appare opportuno considerare la possibilità di abilitare la Difesa a utilizzare

strumenti cibernetici anche in operazioni congiunte con le autorità civili, sia nel complesso delle attività di identificazione, sia nel contrasto alla minaccia cibernetica.

L'adozione di un approccio integrato, dove la Difesa collabori attivamente con altri attori istituzionali, consentirebbe di implementare strategie più efficaci e di rispondere in modo più rapido alle emergenze digitali, migliorando la resilienza complessiva del sistema Paese.

La Commissione Difesa della Camera dei Deputati valuterà i possibili contributi al fine di costruire una coerente cornice legislativa aderente agli esiti dell'indagine conoscitiva sulla difesa cibernetica.

Per un'analisi più approfondita dei temi trattati nel corso dell'indagine si rimanda alla parte successiva

FOCUS

1. La disciplina della sicurezza cibernetica in Italia

1.1. L'evoluzione normativa italiana dal 2013 al 2020

Sulla spinta di iniziative sia a livello dell'Unione europea (Ue) che nell'ambito dell'Alleanza atlantica, con il decreto del Presidente del Consiglio dei Ministri (Dpcm) del 24 gennaio 2013 (Decreto Monti) l'Italia si dota per la prima volta di una struttura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche.

Il Decreto Monti individua nel Dipartimento delle Informazioni per la Sicurezza (Dis) l'organo responsabile per la tutela della sicurezza cibernetica del Paese.

Il Decreto istituisce, inoltre, il Nucleo per la Sicurezza Cibernetica (Nsc) per il supporto operativo in caso di crisi cibernetiche di rilevanza per la sicurezza nazionale, e un tavolo interministeriale per la prevenzione e gestione di tali crisi. Il Decreto conferisce inoltre al Comitato Interministeriale per la Sicurezza della Repubblica (Cisr) il compito di proporre al Presidente del Consiglio dei Ministri il quadro strategico nazionale per la sicurezza dello spazio cibernetico e gli indirizzi strategici in materia di cybersecurity tramite il Piano nazionale per la sicurezza dello spazio cibernetico.

Tra le ulteriori attribuzioni del Cisr definite dal Decreto Monti, vi sono l'elaborazione di linee di indirizzo per eventuali collaborazioni tra enti pubblici e privati e la diffusione di buone prassi per la protezione dello spazio cibernetico, nonché la promozione di adozione di iniziative atte ad assicurare la partecipazione italiana a quadri di cooperazione a geometria variabile, compresi quelli Nato e Ue. In tutte le sue funzioni, il Cisr era affiancato da un Cisr tecnico, ovvero da un organismo collegiale di coordinamento.

L'impianto normativo e istituzionale italiano per la sicurezza cibernetica è stato poi modificato dal Dpcm del 17 febbraio 2017 (Decreto Gentiloni), seguito dal Piano nazionale per la protezione cibernetica e la sicurezza informatica.

Una certa spinta all'evoluzione dell'architettura nazionale è stata fornita dalla necessità di razionalizzare e semplificare un panorama istituzionale complesso, con il tentativo di creare sinergie ed economie di scala nel contrasto coordinato alla minaccia cyber.

Con il Decreto Gentiloni il Dis viene investito di ulteriori compiti e diventa sia l'apparato operativo della struttura di sicurezza cibernetica, sia l'organo deputato a definire le linee d'azione per la sicurezza in questo dominio e della risposta in caso di crisi. Tra le modifiche che vanno verso un rafforzamento dei ruoli del Dipartimento, vi è lo spostamento del Nsc: precedentemente presso l'Ufficio del Consigliere militare della Presidenza del Consiglio, il Nucleo viene inserito nella struttura del Dis, che lo presiede con un proprio vice direttore generale. Tra i vari compiti dell'organo vi è quello di raccordo tra gli attori coinvolti a vario titolo nell'architettura di sicurezza cibernetica nazionale, nonché di gestione delle crisi nello spazio cibernetico.

Un'altra importante novità introdotta dal decreto attiene alla creazione, in capo al Ministero dello Sviluppo economico, di un Centro di valutazione e certificazione nazionale (Cvcn) per la verifica degli standard di sicurezza dei prodotti tecnologici destinati a essere impiegati nelle infrastrutture critiche del Paese.

1.2. Il perimetro della sicurezza nazionale cibernetica

Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica (PNSC) e la previsione di misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi, è stato successivamente adottato il DL n. 105 del 21 settembre 2019. Tra i vari obblighi degli operatori individuati vi è anche la necessità di certificazione dei prodotti e servizi da loro utilizzati, che dovrà essere effettuata dal Cvcn secondo le modalità recentemente definite.

Al centro del PSNC vi è la sicurezza delle reti, dei sistemi informativi e dei servizi informatici (cosiddetti "beni ICT"), dal cui funzionamento dipende l'esercizio di funzioni e servizi essenziali dello Stato. Per preservare questa sicurezza, la legge impone determinati obblighi in capo ad amministrazioni pubbliche, enti, e operatori pubblici e privati con sede nel territorio nazionale, che esercitino funzioni o servizi essenziali dello Stato che dipendono dall'utilizzo di reti, sistemi informativi e servizi informatici il cui malfunzionamento, utilizzo improprio, o interruzione, anche parziale, possa causare un pregiudizio alla sicurezza nazionale.

Tutte azioni che vanno nella direzione di un rafforzamento della sicurezza dell'apparato nazionale e di una maggiore resilienza degli operatori e fornitori di funzioni essenziali dello stato, grazie all'adozione di beni, prodotti e servizi di *Information and Communications Technology* (Ict) che dovrebbero essere concepiti a monte come più sicuri e resistenti rispetto alle minacce cyber.

1.3. L'attuale quadro legislativo-istituzionale: la governance del sistema di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale

Con il decreto legge n. 82 del 2021, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale, in attuazione di precisi obiettivi del Piano nazionale di ripresa e resilienza (PNRR): la sicurezza cibernetica costituisce, infatti, uno dei principali interventi previsti dal PNRR nell'ambito della trasformazione digitale della p.a. e della digitalizzazione del Paese (vedi oltre).

La *governance* del sistema di sicurezza cibernetica ha al suo vertice il Presidente del Consiglio dei ministri, al quale è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza nonché l'adozione della relativa strategia nazionale e - previa deliberazione del Consiglio dei ministri - la nomina e la revoca dei vertici dell'Agenzia per la cybersicurezza nazionale; di tali nomine sono preventivamente informati il COPASIR e le competenti Commissioni parlamentari.

Il Presidente del Consiglio dei ministri può delegare all'Autorità delegata per il sistema di informazione per la sicurezza della Repubblica, ove istituita, le funzioni in materia di sicurezza cibernetica che non sono a lui attribuite in via esclusiva.

Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

Il CIC è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata per la sicurezza della Repubblica, 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 delle imprese e del made in Italy, dal Ministro

dell'ambiente e della sicurezza energetica, dal Ministro dell'università e della ricerca e dal Ministro delle infrastrutture e dei trasporti. Le funzioni di segretario del CIC sono svolte dal Direttore Generale dell'Agenzia.

L'Agenzia per la cybersicurezza nazionale (ACN) è istituita a tutela degli interessi nazionali nel campo della cibersicurezza.

L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

L'Agenzia è l'Autorità nazionale per la cybersicurezza e in quanto tale ha:

a) assicura il coordinamento tra i soggetti pubblici coinvolti nella cibersicurezza a livello nazionale;

b) promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore;

c) predispone la strategia nazionale di cibersicurezza;

d) ai sensi del nuovo Codice europeo delle comunicazioni elettroniche, svolge anche i compiti relativi alla sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza (D.Lgs. 8 novembre 2021, n. 207, art. 6, comma 3 e artt. 40 e 41).

I vertici dell'Agenzia sono il Direttore Generale e il Vice Direttore Generale e la stessa si articola in servizi generali e divisioni.

I Servizi operano sulla base degli indirizzi del Direttore Generale e presidiano ambiti ampi e complessi, correlati alle funzioni e alle politiche generali dell'Agenzia. Le Divisioni sono istituite per la gestione di un insieme omogeneo di tematiche e macro-processi e operano all'interno dei Servizi. L'organizzazione di ACN è regolamentata dal decreto del Presidente del Consiglio dei ministri n. 223 del 9 dicembre 2021.

Il 9 marzo 2023 è stato nominato l'attuale Direttore Generale dell'Agenzia per la cybersicurezza nazionale su proposta del Presidente del Consiglio dei ministri.

Le funzioni attribuite all'Agenzia esprimono un approccio olistico alla gestione della cybersicurezza, nel quale acquistano rilevanza non solo gli interventi di natura prevalentemente tecnica, volti a garantire la sicurezza e la resilienza delle reti, dei sistemi informativi e dei servizi informatici, ma anche le progettualità finalizzate allo sviluppo di nuovi prodotti e tecnologie, della ricerca e della competitività industriale, nonché alla creazione di una forza lavoro nazionale di settore in grado di rispondere alle esigenze del mercato.

In particolare, l'Agenzia, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni:

- opera quale ente regolatore, certificatore, nonché di vigilanza del settore della cybersicurezza, che definisce, ad esempio, i livelli minimi delle misure di sicurezza nei diversi ambiti (tra cui energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, comunicazioni elettroniche, cloud nazionale, pubblica amministrazione), potendo anche effettuare ispezioni e irrogare sanzioni;
- cura e promuove la definizione ed il mantenimento di un quadro normativo aggiornato e coerente nel settore della cybersicurezza;
- contribuisce a ridurre il rischio derivante dall'approvvigionamento tecnologico, incrementando i livelli di sicurezza della supply chain, con particolare riguardo a soluzioni e prodotti destinati ad essere utilizzati su infrastrutture e sistemi ICT rilevanti per la sicurezza nazionale;
- sviluppa le capacità di monitoraggio, rilevamento, prevenzione, analisi e risposta agli incidenti cibernetici;
- coordina, in raccordo con il MAECI, la cooperazione internazionale nella materia della cybersicurezza;
- supporta lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e promuove la formazione, la crescita tecnico-

professionale e la qualificazione delle risorse umane nel campo della cybersicurezza;

- svolge attività di comunicazione e di promozione della consapevolezza riguardo al tema della cybersicurezza, contribuendo così allo sviluppo di una cultura nazionale in materia;
- è designata quale Centro Nazionale di Coordinamento (NCC), ai sensi dell'articolo 6 del Regolamento (UE) 2021/887 del Parlamento e del Consiglio europeo, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

Ai fini dello svolgimento delle funzioni sopra illustrate, operano presso l'Agenzia:

- il Computer Security Incident Response Team (CSIRT) Italia, la cui azione è volta alla prevenzione, al monitoraggio, al rilevamento, all'analisi e alla risposta ad incidenti cibernetici;
- il Centro di Valutazione e Certificazione Nazionale (CVCN), che si occuperà di verificare la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT in uso nelle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese;
- il Centro Nazionale di Coordinamento in materia di cybersicurezza nell'ambito industriale, tecnologico e della ricerca.

Il Piano di implementazione della Strategia Nazionale di cybersicurezza riporta il disegno complessivo dell'architettura istituzionale della sicurezza cibernetica che rende imprescindibile, per il raggiungimento di elevati livelli di sicurezza nel dominio cibernetico e la protezione degli asset strategici, il concorso in stretta sinergia con altre Amministrazioni, cui la normativa vigente assegna prerogative esclusive in aderenza ai rispettivi mandati istituzionali.

Tra queste, in particolare:

- il Comparto intelligence, competente per la cyber-intelligence, conduce attività di ricerca e raccolta informativa finalizzata alla tutela degli interessi politici, militari, economici, scientifici e industriali dell'Italia, e provvede alla formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica, al fine di preservare la sicurezza

nazionale, anche attraverso la conduzione di operazioni cyber. In particolare, secondo le modalità e le procedure stabilite dalla legge n. 124/2007, il Direttore Generale del DIS, avvalendosi degli uffici del Dipartimento, cura il coordinamento delle attività di ricerca informativa e le Agenzie, ciascuna nell'ambito delle rispettive attribuzioni, svolgono, secondo gli indirizzi definiti dalle direttive che il Presidente del Consiglio dei ministri impartisce, sentito il CISR, e le linee di coordinamento delle attività di ricerca informativa stabilite dal Direttore Generale del DIS, le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali.

- il Ministero dell'interno, quale autorità nazionale di pubblica sicurezza, tutela l'ordine e la sicurezza pubblica, il soccorso pubblico e la difesa civile. In particolare, il Dipartimento di pubblica sicurezza assicura le attività di prevenzione e contrasto ai crimini informatici attraverso la Polizia Postale e delle Comunicazioni, ferme restando le competenze negli ambiti definiti dal legislatore degli uffici e comandi della Polizia di Stato, dell'Arma dei carabinieri e della Guardia di finanza. Per la protezione delle infrastrutture critiche informatizzate dai reati informatici opera il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) della Polizia di Stato che svolge un costante monitoraggio della rete internet, oltre alle funzioni di punto di contatto nazionale per le emergenze in materia di criminalità informatica transnazionale.
- il Ministero della difesa, competente per la difesa e la sicurezza militare dello Stato.

In particolare, il Dicastero definisce e coordina la politica militare, la governance e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero. La Difesa, attraverso il Comando per le Operazioni in Rete (COR) e col contributo specialistico del Reparto Informazioni e Sicurezza (RIS) dello Stato Maggiore della Difesa (SMD), è deputato alla pianificazione e conduzione di operazioni militari cibernetiche offensive e difensive nei casi previsti.

Tale Dicastero, pertanto, assicura, anche in situazioni di crisi di natura cibernetica (sia nazionale sia internazionale), tutti i servizi e le attività

necessari, da un lato, a garantire la protezione, la resilienza e l'efficienza delle reti e infrastrutture militari e, dall'altro, a sviluppare le proprie peculiari capacità necessarie all'implementazione di attività di supporto, difesa, reazione e stabilizzazione.

In ambito NATO, la Difesa assicura la partecipazione dell'Italia alle attività di natura militare conseguenti all'elezione dello spazio cibernetico a dominio di operazioni. La Difesa contribuisce, altresì, nel rispetto delle competenze attribuite dalla normativa vigente ad altre Amministrazioni, ad assicurare la definizione delle policy cyber, al rafforzamento e allo sviluppo delle capacità cyber dell'Alleanza.

Analogamente al Ministero dell'interno, la Difesa verifica le condizioni di sicurezza e l'assenza di vulnerabilità note per le forniture ICT da impiegare su reti, sistemi informativi e servizi informatici di propria pertinenza inclusi nel Perimetro di sicurezza nazionale cibernetica, attraverso il proprio Centro di Valutazione che opera in stretto raccordo con il CVCN.

Parallelamente, nell'ambito del coordinamento operato dall'ACN, ciascun Ministero e autorità con competenze e interessi trasversali in materia cyber svolge un ruolo nel raggiungimento dei suddetti obiettivi. Tale ruolo assume rilievo sia attraverso la messa in sicurezza delle proprie reti e infrastrutture digitali, sia attraverso la partecipazione agli organismi inter-istituzionali e alle iniziative promosse dall'ACN, volte ad accrescere la cybersicurezza.

Presso l'Agenzia per la cybersicurezza nazionale è prevista la costituzione, in via permanente, di un Nucleo per la cybersicurezza, per profili attinenti a eventuali situazioni di crisi.

Esso è previsto in via permanente, quale supporto del Presidente del Consiglio riguardo alle tematiche 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 è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale.

La relativa composizione, sulla base delle modifiche apportate dalla Camera dei deputati, è così definita:

- ✓ un rappresentante del Dipartimento dell'informazione per la sicurezza (DIS);
- ✓ il Consigliere militare del Presidente del Consiglio;
- ✓ un rappresentante dell'Agenzia informazioni e sicurezza esterna (AISE) di cui all'articolo 6 della legge n. 124 del 2007;
- ✓ un rappresentante dell'Agenzia informazioni e sicurezza interna (AISI) di cui all'articolo 7 della legge n. 124 del 2007;
- ✓ un rappresentante di ciascuno dei Ministeri rappresentati[1] nel Comitato interministeriale per la cybersicurezza – CIC;
- ✓ un rappresentante del Dipartimento della protezione civile della Presidenza del Consiglio;
- ✓ limitatamente alla trattazione di informazioni classificate, un rappresentante dell'Ufficio centrale per la segretezza (istituito presso il DIS, ai sensi dell'articolo 9 della legge n. 124 del 2007).

A fronte di questa composizione "allargata", è prevista una possibile composizione "ristretta", con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi (sulla quale interviene l'articolo 10 del decreto-legge, dettando altresì disposizione circa la composizione - in quel caso, integrata con altri esponenti - del Nucleo in situazioni di crisi di natura cibernetica).

È utile sottolineare che, nel delineare i compiti dell'Agenzia e del Nucleo, il DL 82, nel testo originario, non riconosceva ruoli particolari al Ministero della Difesa. Mentre in materia di cooperazione internazionale sulla cybersecurity si prevedeva già nel testo del DL un raccordo con il Ministero degli Affari esteri e della Cooperazione internazionale (art. 7, comma 3(q)), nel caso delle Forze Armate e della partecipazione italiana a quadri di cooperazione e organizzazioni di sicurezza le specificità della Difesa non sembravano essere messe adeguatamente in luce. Al Ministero della Difesa veniva solamente riconosciuta la competenza specifica di ente abilitato al

[1] I ministri rappresentati nel CIC sono : il Ministro degli affari esteri e della cooperazione internazionale; il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro delle imprese e del made in Italy; il Ministro dell'ambiente e della sicurezza energetica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e dei trasporti.

rilascio del certificato europeo di sicurezza cibernetica, ossia della certificazione di prodotti Ict a livello di affidabilità, come da regolamento (Ue) 2019/881 (art. 7).

Grazie all'introduzione di emendamenti nella fase di conversione in legge, le specificità di settore sembrano essere prese maggiormente in considerazione. La legge di conversione esplicita la necessità di un raccordo con il Ministero della Difesa in diversi ambiti d'azione, a partire proprio dalla partecipazione italiana a progetti e iniziative in collaborazione con la Nato e l'Agenzia Europea per la Difesa, per includere gli aspetti collegati alla ricerca militare e la contribuzione alla formazione settoriale grazie alle competenze altamente specializzate delle Forze Armate.

Con il D.L. 82/2021 è stata definita l'attuale architettura nazionale di sicurezza cibernetica, definendo un ulteriore pilastro, con la creazione dell'ACN, a completamento di quelli esistenti.

Si individua dunque un'architettura a 4 pilastri:

1) cyber-resilience, assicurata dall'ACN;

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

costituisce l'articolazione specializzata dell'Arma nel contrasto alla criminalità informatica, nello studio e sperimentazione delle tecnologie per l'esplorazione del web e l'intercettazione dei flussi telematici, mentre per la Guardia di Finanza è il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT) quale reparto Speciale deputato al contrasto delle frodi telematiche ed informatiche, nonché alla tutela della privacy;

3) difesa e sicurezza militare dello Stato nello spazio cibernetico, di spettanza del Ministero della Difesa. In particolare, il Dicastero definisce e coordina la politica militare, la *governance* e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero. La Difesa, attraverso il Comando per le Operazioni in Rete (COR) e col contributo specialistico del Reparto Informazioni e Sicurezza (RIS) dello Stato Maggiore della Difesa (SMD), è deputato alla pianificazione e conduzione di operazioni militari cibernetiche offensive e difensive nei casi previsti. Tale Dicastero, pertanto, assicura, anche in situazioni di crisi di natura cibernetica (sia nazionale sia internazionale), tutti i servizi e le attività necessari, da un lato, a garantire la protezione, la resilienza e l'efficienza delle reti e infrastrutture militari e, dall'altro, a sviluppare le proprie peculiari capacità necessarie all'implementazione di attività di supporto, difesa, reazione e stabilizzazione. In ambito NATO, la Difesa assicura la partecipazione dell'Italia alle attività di natura militare conseguenti all'elezione dello spazio cibernetico a dominio di operazioni. La Difesa contribuisce, altresì, nel rispetto delle competenze attribuite dalla normativa vigente ad altre Amministrazioni, ad assicurare la definizione delle policy cyber, al rafforzamento e allo sviluppo delle capacità cyber dell'Alleanza. Analogamente al Ministero dell'interno, la Difesa verifica le condizioni di sicurezza e l'assenza di vulnerabilità note per le forniture ICT da impiegare su reti, sistemi informativi e servizi informatici di propria pertinenza inclusi nel Perimetro di sicurezza nazionale cibernetica, attraverso il proprio Centro di Valutazione che opera in stretto raccordo con il CVCN;

4) ricerca ed elaborazione informativa, finalizzata alla tutela degli interessi politici, militari, economici, scientifici e industriali dell'Italia, è affidata al Comparto intelligence, che a tali fini provvede anche alle attività volte

alla rilevazione e alla sistematica azione di monitoraggio, prevenzione e contrasto delle minacce cibernetiche più insidiose, perpetrate nel o attraverso l'ambiente digitale, anche attraverso la conduzione di operazioni cyber.

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

Il Presidente del Consiglio dei ministri trasmette al Parlamento (entro il 30 aprile di ogni anno) una relazione sull'attività svolta dall'Agenzia nell'anno precedente. Così come trasmette al COPASIR (entro il 30 giugno di ogni anno) una relazione sulle attività svolte nell'anno precedente dall'Agenzia concernenti la tutela della sicurezza nazionale nello spazio cibernetico per i profili di competenza del Comitato.

Da ultimo, con il decreto legislativo 4 settembre 2024, n. 138, è stata recepita nell'ordinamento interno la direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. direttiva NIS 2) che ha aggiornato la direttiva NIS 1 (n. 2016/1148) al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza.

La direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. direttiva NIS 2) che ha aggiornato la direttiva NIS 1 (n. 2016/1148) al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza. L'aggiornamento della direttiva mira inoltre ad eliminare le ampie divergenze tra gli Stati membri che hanno attuato gli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione, stabiliti dalla direttiva NIS in modi significativamente diversi a livello nazionale, con un effetto potenzialmente pregiudizievole sul funzionamento del mercato interno.

Il decreto legislativo 138/2024:

- introduce la Strategia nazionale di cybersicurezza quale strumento per individuare gli obiettivi strategici e le risorse necessarie per conseguirli, nonché le misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza;
- individua nell'Autorità per la cybersicurezza nazionale l'autorità nazionale competente NIS responsabile per l'attuazione della direttiva e autorità nazionale, assieme al Ministero della difesa, di gestione delle crisi informatiche;
- individua il Computer Security Incident Response Team – CSIRT Italia, l'organo tecnico preposto alla gestione delle crisi informatiche;
- individua le misure tecniche di gestione dei rischi per la sicurezza informatica e gli obblighi di notifica di incidente;
- prevede la possibilità di imporre obblighi di certificazione di cybersicurezza.

Si ricorda inoltre che il 2 luglio 2024 è stata pubblicata nella *Gazzetta Ufficiale* la legge 28 giugno 2024, n. 90, originata da un disegno di legge di iniziativa governativa, in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Il provvedimento si articola in due parti.

Il Capo I del disegno di legge, reca disposizioni concernenti la cybersicurezza nazionale finalizzate a conseguire una più elevata capacità di protezione e risposta di fronte a emergenze cibernetiche.

Il Capo II del provvedimento reca disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari.

Si segnala che la legge di bilancio 2023 (L. 29 dicembre 2022, n. 197, articolo 1, comma 899, lettera b)) ha istituito nello stato di previsione del Ministero dell'economia e delle finanze (cap. 3081) il Fondo per la gestione della cybersicurezza, con una dotazione finanziaria di 10 milioni di euro per l'anno 2023, 50 milioni di euro per l'anno 2024 e 70 milioni di euro annui a decorrere dall'anno 2025. Tale fondo è destinato al finanziamento delle attività di gestione operativa dei progetti finalizzati al conseguimento dell'autonomia tecnologica in ambito digitale, nonché all'innalzamento dei

livelli di cybersicurezza dei sistemi informativi nazionali in attuazione della Strategia nazionale di cybersicurezza, adottata con decreto del Presidente del Consiglio dei ministri 17 maggio 2022.

Infine, appare utile segnalare che tale Fondo è stato da ultimo rifinanziato dalla legge di bilancio per il triennio 2025-2027 (articolo 1, comma 630, della l. 30 dicembre 2024, n. 207) per 0,2 milioni di euro per anno 2025 e di 1 milione di euro per ciascuno degli anni 2026 e 2027.

1.4. Le risorse del PNRR per la cibersicurezza

Nell'ambito del PNRR la Cybersecurity è uno dei 7 investimenti afferenti alla Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo".

L'investimento (investimento 1.5) è volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica; ad esso sono destinati 622 milioni di euro di cui:

- 241 per la creazione di una infrastruttura per la cybersicurezza (attuata con la creazione della ACN);
- 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC;
- 150 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, ministero della Difesa, Guardia di Finanza, ministero della Giustizia e Consiglio di Stato.

L'intervento si articola in 4 aree principali:

1. rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio verso la PA e le imprese di interesse nazionale;
2. consolidamento delle capacità tecniche di valutazione e *audit* della sicurezza dell'*hardware* e del *software*;
3. potenziamento del personale delle Forze di polizia dedicate alla prevenzione e investigazione del crimine informatico;

4. implementazione degli *asset* e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

L'investimento è finalizzato a garantire il funzionamento dell'intero sistema di digitalizzazione della p.a. che prevede in primo luogo la creazione di infrastrutture digitali per la p.a. anche attraverso la realizzazione del Polo strategico nazionale (investimento 1.1). Si tratta di un ambiente *cloud* destinato ad ospitare la Piattaforma digitale nazionale dati ove confluiranno le informazioni provenienti da tutte le amministrazioni, consentendo l'interoperabilità dei dati (investimento 1.3). L'obiettivo finale è di sviluppare, attraverso la piattaforma, un'offerta integrata e armonizzata di servizi digitali per i cittadini (investimento 1.4). In tutte queste fasi è necessario garantire la sicurezza cibernetica delle infrastrutture e dei dati.

1.5. La difesa cibernetica

La difesa cibernetica si sostanzia in uno spettro di competenze dello Stato di natura prettamente militare, da inquadrare in una più ampia strategia nazionale per la sicurezza cibernetica, la cui architettura si è andata componendo grazie a una serie di interventi normativi.

Il tema della difesa cibernetica ha assunto rilevanza crescente in Italia, a fronte dell'elevato numero di gravi attacchi informatici, sia verso soggetti privati, sia contro le Forze armate e la pubblica amministrazione.

Il Ministero della Difesa e le Forze Armate sono dunque coinvolte sia per fronteggiare il rischio che corrono le proprie infrastrutture digitali sia per assolvere, contestualmente, il compito di "difesa dello Stato" che già si estrinseca nei domini tradizionali e, ora, anche nel *cyber space*. A tal proposito, si ricorda che il decreto-legge n. 50 del 2022 (all'articolo 51, comma 8, lettera e)) ha riconosciuto il *cyberspace* come dominio militare, aggiungendo nell'articolo 88 del Codice dell'ordinamento militare (decreto legislativo n. 66 del 2010), oltre ai domini tradizionali (terrestre, marittimo e aereo), anche i domini cibernetico e aero-spaziale tra gli ambiti tutelati dalla difesa nazionale, quale funzione propria e principale dello strumento militare. Sono state al contempo adeguate (alla lettera f) le funzioni di concorso delle Forze armate includendo quelle previste, sempre in ambito di cybersicurezza, dall'articolo 5, comma 5, del decreto-legge 14 giugno 2021, n. 82.

Come precisato dal Governo (cfr relazione illustrativa allegata al D.L. n. 50 del 2022 che ha novellato l'articolo 88 del COM) la disposizione relativa alla difesa dello spazio cibernetico opera nel pieno rispetto delle competenze di tutte le altre amministrazioni coinvolte nello specifico settore: *cyber resilience*, in capo all'Agenzia per la Cybersicurezza Nazionale, *cyber intelligence*, di competenza del Dipartimento Informazioni per la Sicurezza e le collegate Agenzie*, cyber crime & investigation*, attestata al Ministero degli Interni. Allo stesso modo, afferendo esclusivamente ai profili di tutela militare delle infrastrutture spaziali (antenne satelliti strutture per la comunicazione satellitare, ecc.) strettamente connessi alla funzione di difesa nazionale, anche l'inclusione del dominio aero-spaziale non implica contrasti o sovrapposizioni di competenze, ma solo l'adeguamento dell'ambito di interesse della difesa nazionale.

Si ricorda anche che, a seguito del Summit dei paesi NATO a Varsavia del 2016, il cyberspazio è divenuto un nuovo dominio di operazione al pari dei domini "tradizionali" quali, terra, mare e aria e, più recentemente, lo spazio. Il Summit di Bruxelles dell'11 luglio 2018 ha segnato poi un ulteriore, importante rafforzamento delle capacità cibernetiche della Nato. Il Summit ha infatti stabilito la nascita di un *Cyber Operations Center* con l'obiettivo coordinare le operazioni degli alleati nel dominio cibernetico.

L'Italia ha affrontato il tema della difesa cibernetica anche con l'istituzione, nell'ambito della Difesa, del Comando per le Operazioni in Rete (COR) e, su un piano più generale, con una più ampia riforma della *governance* del settore che, nella scorsa Legislatura, ha portato alla definizione del perimetro di sicurezza cibernetica nazionale e alla creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN).

In estrema sintesi, si ricorda che nel 2018 il Capo di Stato Maggiore della Difesa ha dato mandato a un Gruppo di Progetto C5ISR, denominato "Riorganizzazione e razionalizzazione del settore Cyber", di individuare possibili soluzioni per rendere più efficace ed efficiente il settore C4/ICT-Cyber (Dominio Cibernetico).

Dalle risultanze del lavoro svolto dal Gruppo di Progetto è emersa la necessità di costituire un comando capace di riunire le competenze di diversi attori operanti in ambito Difesa.

La soluzione ordinativo-organica rispondente a tale esigenza è stata individuata aggregando due comandi preesistenti: il Comando C4 Difesa (C4D) e il Comando Interforze per le Operazioni Cibernetiche (CIOC).

In data 9 marzo 2020, è stato costituito il Comando per le Operazioni in Rete della Difesa (CORDIFESA), soluzione rispondente a criteri di efficienza ed efficacia, che si pone quale ente attraverso il quale la Difesa ha inteso razionalizzare il citato settore per eliminare le preesistenti criticità.

Il CORDIFESA ha assunto il ruolo di responsabile della Rete, dei Sistemi, dei Servizi, degli Applicativi e dei Portali Web della Difesa, consentendo pertanto l'accentramento, a connotazione Interforze, di quelle funzioni comuni tra le Forze Armate e l'Area Interforze.

Dal 26 luglio 2021, il Comando per le Operazioni in Rete (COR), unitamente al Comando interforze per le Operazioni delle Forze Speciali (COFS) e al Comando delle Operazioni Spaziali (COS) è posto alle dipendenze del Comando Operativo di Vertice Interforze (COVI).

Nel contesto normativo e istituzionale delineato, il COR rientra dunque tra i soggetti più rilevanti per la difesa cibernetica del Paese, con l'incarico di coordinare le attività di sicurezza e difesa cibernetica delle Forze Armate e del Ministero della Difesa.

Si tratta di un organismo:

- che riunisce in un unico comando le competenze necessarie a operare nello spazio cibernetico, incluse le Ict, le capacità di comando, controllo, telecomunicazioni e informatica (*Command, control, communication, and computers*, C4) e di *intelligence*, sorveglianza e ricognizione. Tali competenze e responsabilità erano in precedenza frammentate, soprattutto per le unità che si occupano delle componenti Ict e C4 della Difesa, e per quelle incaricate di condurre operazioni nel dominio cibernetico;
- posto sotto la diretta catena di comando dello Stato Maggiore della Difesa (SMD) e lavora in sinergia con le unità di Esercito, Marina e Aeronautica che si occupano di difesa e sicurezza cibernetica;
- di natura interforze, anche nell'ottica di una collaborazione tra le diverse Forze Armate sempre più sinergica e consolidata, al fine di

raggiungere un più alto livello di efficienza e razionalizzazione della struttura tecnico-operativa della Difesa.

Il COR è composto di tre reparti:

1. il Reparto C4, che ha assunto le competenze prima garantite dal Comando interforze C4 Difesa (C4D), assicurando la direzione della Rete della difesa (Difenet) oltre che la gestione delle capacità Ict di tutti gli Stati maggiori. Presso il Reparto C4 è inoltre collocato l'Ufficio Reti e Data Center, che svolge le funzioni necessarie per garantire la continuità di attività della Difesa e di ripresa in caso di grave incidente. Il Reparto comprende anche l'Ufficio Infrastrutture di Sicurezza, incaricato di sviluppare sistemi di sicurezza che siano ideati, progettati e realizzati tenendo in considerazione fin dall'inizio le esigenze di sicurezza e difesa cibernetica, secondo il principio di *security by design*;

2. il Reparto Sicurezza e *Cyber Defence*, deputato allo sviluppo di un'architettura nazionale di difesa cibernetica e di sistemi preposti alla protezione dell'infrastruttura Ict. Nel Reparto Sicurezza e Cyber Defence continua a operare l'Ufficio *Computer Emergency Response Team* (Cert), che svolge anche attività preventive quali lo sviluppo di competenze di *threat intelligence* per le Forze Armate;

3. il Reparto *Cyber Operations*, che rappresenta infine l'integrazione nel COR dell'ex-Comando Interforze per le Operazioni Cibernetiche (Cioc). Ad esso spetta l'intero ventaglio di attività militari che si svolgono nello spazio cibernetico, mirate alla protezione di sistemi e servizi della Difesa da minacce cibernetiche, in relazione non solo al territorio nazionale, ma anche ai vari teatri operativi. È in questo contesto che lavorano le Cellule Operative Cibernetiche (COC), inizialmente istituite all'interno del Cioc e poi confluite nel Reparto Operazioni Cibernetiche del COR, che consistono in team di specialisti interforze in grado di condurre operazioni difensive e offensive, lavorando per ridurre il livello di vulnerabilità cui sono soggette sia le infrastrutture cibernetiche in Italia sia i contingenti dispiegati all'estero nell'ambito delle missioni internazionali. Il Reparto si occupa di formazione e reclutamento di personale, oltre che di attività per l'analisi delle minacce e la protezione delle infrastrutture informatiche, l'innovazione della Difesa in ambito cibernetico e il *procurement* tecnologico.

A livello normativo, si ricorda inoltre che sono state adottate alcune misure volte a potenziare la capacità di contrasto in ambito cibernetico in situazioni di crisi o emergenza a fronte di minacce che coinvolgano aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale. A questo fine si segnala in particolare l'articolo 37 del decreto-legge n. 115 del 2022 (c.d. decreto «Aiuti bis», come modificato in sede di conversione), che ha attribuito al Presidente del Consiglio il potere di autorizzare l'adozione di particolari misure di intelligence di contrasto in ambito cibernetico.

L'emanazione di tali disposizioni deve avvenire previo parere del Comitato interministeriale per la sicurezza della Repubblica (Cisr) e sentito il Comitato parlamentare per la sicurezza della Repubblica (Copasir).

Nell'adottare le misure di *intelligence* si prevede:

- la cooperazione del Ministero della difesa;
- il ricorso alle garanzie funzionali, di cui all'articolo 17 della legge 124/2007; si tratta di una speciale causa di giustificazione che prevede la non punibilità del personale dei servizi che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizi, nel rispetto di limiti tassativi previsti dal medesimo articolo.

L'attuazione delle misure autorizzate di contrasto in ambito cibernetico spetta agli organismi operativi dei servici di *intelligence*, ossia l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI), con il coordinamento del Dipartimento delle informazioni per la sicurezza (DIS).

Si ricorda che, in via ordinaria, al DIS spetta il coordinamento dell'intera attività di informazione per la sicurezza svolte dall'AISE e dall'AISI, (art. 4, comma 3, lett. *a)*, L. 124/2007) comprese le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali (art. 4, comma 3, lett. *d-bis)*, L. 124/2007.

Restano ferme le competenze del Ministero della difesa ai sensi dell'articolo 88 del Codice dell'ordinamento militare (D.Lgs. 15 marzo 2010, n.66).

Il Presidente del Consiglio deve informare delle misure *intelligence* autorizzate il Comitato parlamentare per la sicurezza della Repubblica (Copasir).

2. La disciplina della sicurezza cibernetica negli altri Paesi del G7

2.1. Canada

La sicurezza cibernetica in Canada è assicurata da una pluralità di soggetti che nel loro insieme costituiscono la "cybersecurity community" del Governo del Canada, tra questi il Communications Security Establishment (CSE), il Department of National Defence (DND) e le Canadian Armed Forces (CAF).

Il Communications Security Establishment (CSE) è l'agenzia nazionale del Canada per l'*intelligence* estera e l'autorità tecnica per la cybersicurezza e la protezione delle informazioni. Il CSE, disciplinato dal Communications Security Establishment Act del 2019, raccoglie informazioni sulle minacce ai sistemi e alle reti governative, gestisce una rete difensiva di sensori che identifica e blocca tali minacce e fornisce indicazioni e consigli alle organizzazioni governative e del settore privato per rafforzare la propria sicurezza informatica. È posto sotto il controllo del Ministro della difesa nazionale.

Il CSE gestisce il Canadian Centre for Cyber Security (Cyber Centre). Il Cyber Centre fornisce consulenza, guida, servizi e supporto di esperti sulla sicurezza informatica per i dipartimenti e agenzie federali, province e territori (province e territori costituiscono gli stati federali), municipalità, proprietari di infrastrutture critiche, settore privato, mondo accademico e cittadini.

Il CSE inoltra gli incidenti informatici di rilevanza nazionale al Government Operations Centre (GOC), che poi contribuisce al coordinamento della risposta nazionale.

Mentre il CSE ha una competenza generale, il Department of National Defence (DND) e le Canadian Armed Forces (CAF) sono principalmente responsabili della protezione dei propri sistemi informativi e reti dalle minacce informatiche, e non della protezione di quelli di altri dipartimenti e agenzie federali o del settore privato.

Nel giugno 2023 la Commissione difesa della Camera dei Comuni ha presentato una relazione sulla Difesa cybernetica in Canada.

La relazione conclude l'indagine conoscitiva deliberata dalla Commissione sulla sicurezza informatica e la guerra informatica. In particolare, la mozione istitutiva dell'indagine richiedeva alla Commissione di studiare "l'evoluzione della sofisticatezza delle minacce associate alla

sicurezza informatica e alle capacità degli attori stranieri di *hackerare*, interrompere e smantellare mezzi di comunicazione, reti elettriche, *database* e altre infrastrutture critiche". Inoltre, incaricava la Commissione di esaminare "le piene capacità dei paesi avanzati di condurre una guerra informatica", nonché "la minaccia degli attori non statali alla nostra sicurezza informatica", le azioni intraprese per "difendere il Canada dalle" minacce informatiche straniere e "il ruolo degli individui e del settore privato nella sicurezza informatica".

La prima sezione del rapporto analizza l'ambiente delle minacce informatiche. La seconda sezione delinea i membri della "cybersecurity community" del Governo del Canada, ed esamina i ruoli e le responsabilità di tre membri della cybersecurity community: il Canadian Security Establishment (CSE); il Department of National Defence (DND); e le Canadian Armed Forces (CAF). La terza sezione descrive alcune sfide che le organizzazioni federali canadesi devono attualmente affrontare in materia di cybersecurity, e identifica possibili aree di miglioramento. La quarta sezione affronta gli sforzi per la cybersecurity dell'intera società e considera i modi per migliorare la cyber resilienza del Canada, con un'attenzione particolare alle infrastrutture critiche, alla cooperazione tra i settori pubblico e privato, alla ricerca e sviluppo, all'istruzione, alla sensibilizzazione e alla formazione fornite al pubblico, nonché alla privacy individuale e alle libertà civili. Il rapporto si conclude con alcune raccomandazioni della Commissione al Governo.

2.2. Francia

Nell'ottobre 2015 è stata annunciata la Strategia nazionale per la sicurezza digitale (*Stratégie nationale pour la sécurité du numérique*), volta a sostenere la transizione digitale della società francese.

Alla realizzazione della strategia partecipano diversi soggetti.

Un ruolo fondamentale è svolto dall'Agenzia nazionale della sicurezza dei sistemi di informazione (*Agence Nationale de la Sécurité des Systèmes d'Information,* ANSSI), che è il soggetto primario incaricato di misurare e valutare i rischi e gli effetti degli attacchi informatici, rivolti sia ai soggetti pubblici sia ai privati. Il ruolo dell'ANSSI è quello di promuovere una

risposta coordinata ed efficiente ai problemi di della sicurezza digitale in Francia.

L'Agenzia, istituita con il *Décret n. 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information»*, fa riferimento al Segretario della difesa e della sicurezza nazionale, che assiste il Primo ministro nell'esercizio delle sue responsabilità in materia di difesa e sicurezza. La Direzione dell'Agenzia è affidata a un Direttore generale, nominato dal Primo ministro.

All'interno dell' Agenzia opera il Centro governativo di vigilanza, allerta e risposta agli attacchi informatici (*Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*, CERT-FR), che fornisce supporto nella gestione degli incidenti a ministeri, istituzioni, giurisdizioni, autorità indipendenti, collettività territoriali e OIV (operatori di importanza vitale). È responsabile dell'assistenza agli organi dell'amministrazione nell'attivare i mezzi di protezione necessari. Esso svolge funzioni di CERT (*computer emergency response team*) nazionale.

Ai sensi dell'art. L. 2321-1 del Codice della difesa (inserito dalla *Loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*), nel quadro della strategia di sicurezza nazionale e della politica di difesa, il Primo ministro definisce la politica e coordina l'azione del Governo in materia di sicurezza e di difesa dei sistemi di informazione. Egli a tal fine ha a sua disposizione l'autorità nazionale di sicurezza dei sistemi di informazione.

La *Loi n. 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense* prevede in materia di cybersicurezza che, ai fini della sicurezza e della difesa dei sistemi di informazione, gli operatori, di cui all'art. L. 1332-1 del Codice della difesa, così designati in virtù della loro attività di gestori di una rete di comunicazione elettronica aperta al pubblico, utilizzino, sulle reti di comunicazione elettronica da essi gestite, dispositivi che implementano marcatori tecnici forniti dall'Autorità nazionale per la sicurezza dei sistemi di informazione al solo scopo di rilevare eventi che possono compromettere la sicurezza dei sistemi di informazione dei loro abbonati. Tali sistemi sono implementati per rispondere alle richieste dell'ANSSI. Quando viene a conoscenza di una minaccia che può

compromettere la sicurezza dei sistemi di informazione, infatti, l'Autorità chiede agli operatori di utilizzare i marcatori tecnici da essa forniti (art. L. 33-14 del Codice delle poste e delle comunicazioni elettroniche, inserito dalla legge n. 2018-607, così come modificato da ultimo dalla *loi 2023-703* del 1° agosto 2023*)*.

L'ANSSI coordina i Centri per la valutazione della sicurezza dell'informazione (*Centres d'Évaluation de la Sécurité des Technologies de l'Information*, CESTI), che sono fornitori di servizi volti a certificare la sicurezza dei prodotti. Per essere certificato, un prodotto deve rispettare le regole del regime di certificazione, che consente due tipi di valutazione:

– la conformità al livello di garanzia della valutazione;

– la certificazione della sicurezza di primo livello (*Certification de Sécurité de Premier Niveau*, CSPN) dei prodotti informatici, istituita dall'ANSSI nel 2008.

L'ANSSI dispone anche di un proprio centro di formazione, il Centro di formazione sulla sicurezza dei sistemi di informazione (*Centre de formation à la sécurité des systèmes d'information*, CFSSI), che rilascia un Diploma di esperto in sicurezza dei sistemi di informazione (ESSI) riconosciuto come titolo di livello 1 e registrato nel Repertorio nazionale delle certificazioni professionali.

È stato inoltre previsto, agli inizi del 2021, un Piano per rafforzare la cybersecurity. Finanziata attraverso il piano adottato dal Governo francese per uscire dalle difficoltà economiche legate al Covid-19 (*Plan de Relance*) e attraverso il *Programme d'investissement d'avenir, la Stratégie nationale pour la cybersécurité* mira a raddoppiare la forza lavoro nel settore entro il 2025. Per far fronte alla minaccia di attacchi informatici, il Governo ha annunciato l'intenzione di mobilitare 1 miliardo di euro, di cui 720 milioni di sussidi pubblici.

Tra i principali obiettivi fissati per il 2025 si segnalano i seguenti:

- triplicare il fatturato del settore (da 7,3 miliardi a 25 miliardi di euro);
- posizionare la Francia rispetto alla concorrenza internazionale, in particolare raddoppiando i posti di lavoro nel settore (da 37.000 a 75.000);
- strutturare il settore e riposizionare la Francia rispetto alla concorrenza internazionale in termini di numero di imprese;

- far emergere le eccellenze francesi della *cybersecurity* affidandosi alle maggiori *start-up* del settore;
- diffondere una vera cultura della *cybersecurity* nelle aziende;
- stimolare la ricerca francese nell'innovazione informatica e industriale (aumento del 20% dei brevetti).

Nell'ambito della nuova Strategia il Governo ha inteso rafforzare la *cybersecurity* anche per le strutture sanitarie e medico-sociali e in tal senso il *Ségur de la Santé* ha deciso lo stanziamento di 350 milioni di euro specificamente dedicati al rafforzamento della sicurezza informatica in questi settori.

2.3. Germania

Elemento centrale della Strategia di cybersicurezza è stata l'istituzione del Centro nazionale di difesa cibernetica (*Nationale Cyber-Abwehrzentrum - Cyber-AZ*), una struttura di cooperazione di autorità e organismi di sicurezza che operano a livello federale per la difesa da attacchi informatici. Il *Cyber-Az*, istituito in base a una decisione del Governo federale del 23 febbraio 2011, ha sede a Bonn presso l'Ufficio federale per la sicurezza informatica. I principali compiti del Centro sono la prevenzione, l'informazione e l'allerta precoce contro i c.d. attacchi informatici (*Cyber-Angriffe*) diretti contro uno o più sistemi informatici allo scopo di comprometterne la sicurezza.

Per quanto riguarda più specificamente il settore della difesa, tutte le funzioni relative alla cybersicurezza sono state accentrate in una struttura interforze con quartier generale a Bonn, l'Unità di cyberdifesa nazionale (*Kommando Cyber- und Informationsraum - KdoCIR*) inaugurata alla presenza dell'allora Ministro federale della difesa Ursula von der Leyen ed entrata in funzione il 5 aprile 2017 per sovrintendere alle operazioni cibernetiche e coordinare l'infrastruttura IT, le comunicazioni militari, operative e i servizi di geolocalizzazione. Il *KdoCIR* rappresenta quindi l'equivalente del *Cyber-AZ* – creato solo per scopi civili – sul piano militare. L'Unità ha raggiunto la piena operatività nel 2021.

Successivamente, il 14 settembre 2017, è stata inaugurata a Monaco di Baviera una nuova Agenzia per la cybersicurezza, l'Ufficio centrale per l'informatica nel settore della sicurezza, *Zentrale Stelle für*

Informationstechnik im Sicherheitsbereich - ZITiS*)* per affrontare la criminalità informatica e lo spionaggio digitale mediante la sorveglianza delle telecomunicazioni di massa, la crittografia dei dati e la raccolta delle informazioni. Dal punto di vista giuridico, lo ZIYiS è stato istituito come ente federale senza capacità giuridica nella sfera di competenza del Ministero federale dell'interno con un decreto ministeriale (*Erlass*), emanato il 6 aprile 2017 dall'allora Ministro federale dell'interno De Maizière.

Il 6 settembre 2018 il Governo federale ha approvato la creazione di un'Agenzia per l'innovazione nella cybersicurezza (*Agentur für Innovation in der Cybersicherheit*) investendo 200 milioni di euro in un programma di durata quadriennale. La nuova agenzia governativa, creata nel 2020, è guidata congiuntamente dal Ministero federale della difesa e dal Ministero federale dell'interno con l'obiettivo di proteggere e difendere lo Stato dalle minacce del futuro, *in primis* dai *cyber* attacchi. Il modello per la creazione di questa nuova organizzazione governativa è stata la *Darpa* del Pentagono USA (*Defense Advanced Research Projects Agency*). Lo scopo dei funzionari del Ministero federale della difesa che lavorano al progetto è quello di rafforzare la rete di sicurezza informatica del Paese con l'acquisizione di tecnologie adeguate, garantendo la sicurezza dei dati sensibili e lo sviluppo di contromisure per difendere la Germania e i paesi alleati della Nato dai sofisticati attacchi di *hacker* che si sono moltiplicati negli ultimi anni.

2.4. Giappone

Nel 2014 il Giappone ha approvato una legge in materia di sicurezza cibernetica, la legge 12 novembre 2014, n. 104, The Basic Act on Cybersecurity.

La legge individua nel Governo nazionale l'organo responsabile della formulazione e dell'attuazione delle politiche in materia di sicurezza informatica. In particolare, il Governo adotta le misure legislative, finanziarie, fiscali e qualsiasi altra misura necessaria per attuare la politica di sicurezza informatica e stabilisce un piano di base per la sicurezza informatica, denominato "Strategia per la sicurezza informatica" con l'obiettivo di una promozione globale ed efficace della politica in materia di sicurezza informatica.

Specifici compiti spettano ai governi locali, ai fornitori di infrastrutture critiche, alle imprese collegate al cyberspazio e alle organizzazioni educative e di ricerca.

Le misure di promozione della difesa cibernetica sono adottate dal Quartier generale strategico per la sicurezza informatica, un comitato interministeriale composto da:

- il Ministro degli Affari Interni e delle Comunicazioni;
- il Ministro degli Affari Esteri;
- il Ministro dell'Economia, del Commercio e dell'Industria;
- il Ministro della Difesa.

Vi fanno parte anche esperti in materia di sicurezza informatica designati dal Primo Ministro.

Il Quartier generale è coadiuvato dal Consiglio per la sicurezza informatica, con compiti consultivi.

Il Quartier generale si avvale del National Center of Incident Readiness and Strategy for Cybersecurity – NISC, organo operativo e di coordinamento. Il NISC definisce gli standard comuni per le misure di sicurezza informatiche per le pubbliche amministrazione e gli altri soggetti che rientrano nel campo di applicazione della legge.

Il NISC svolge, inoltre, il ruolo di CERT governativo (Computer Emergency Response Team) ossia di responsabile del coordinamento in caso di un grave attacco informatico, consentendo una serie di azioni, dalla raccolta e analisi delle informazioni all'indagine, valutazione, emissione di allarmi, risposta all'attacco e successiva pianificazione di misure politiche per prevenire il ripetersi dell'evento.

Il Governo giapponese ha approvato nel settembre 2021 la Strategia di Cybersecurity, che sottolinea la necessità di perseguire iniziative per garantire la sicurezza informatica "senza lasciare indietro nessuno." Nella Strategia sono identificate le seguenti tre direzioni fondamentali:

- progredire simultaneamente nella trasformazione digitale e nella sicurezza informatica;
- garantire la sicurezza complessiva del cyberspazio;

- rafforzare le iniziative dal punto di vista della sicurezza nazionale.

Il Giappone ha anche formulato un Piano d'Azione per la Cybersecurity delle Infrastrutture Critiche un insieme comune di linee guida operative per il Governo e gli operatori delle infrastrutture critiche. Basandosi su questo Piano d'Azione, si stanno facendo progressi nella promozione della condivisione delle informazioni e nell'implementazione di esercitazioni intersettoriali.

2.5. Regno Unito

La disciplina legislativa di riferimento è costituita principalmente dal *Computer Misuse Act 1990* e dal *National Security Act 2023*.

Ad integrare la disciplina applicabile concorrono le *Network and Information Systems Regulations 2018* (cosiddette *NIS Regulations*, di attuazione del diritto eurounitario e più volte modificate), che con prescrizioni di dettaglio regolano la sicurezza delle reti e dei sistemi informatici rilevanti per l'operatività dei servizi digitali (motori di ricerca, piattaforme commerciali, servizi di *cloud computing*) e per la prestazione di servizi essenziali (trasporti, energia, servizi sanitari, infrastrutture digitali).

La materia della *cybersecurity* è altresì oggetto di documenti strategici la cui redazione da parte del Governo si colloca nel quadro più generale delle linee programmatiche per la sicurezza nazionale individuate dalla *National Security Strategy* (NSS). A seguito della mutata impostazione assunta dal Regno Unito dopo il recesso dall'Unione Europea, la NSS è stata successivamente inclusa nella *Integrated Review 2021* (aggiornata nel 2023), ispirata alla visione della cosiddetta "*Global Britain*" e protesa a delineare in un unico schema le politiche nazionali in materia di sicurezza, difesa, sviluppo economico e politica estera.

Al primo piano strategico per la cibersicurezza (del 2011) e a quello successivo (del 2016) è seguita da ultimo la *Cyber Security Strategy* pubblicata nel 2021, riferita al periodo 2022-2030. Nelle linee fondamentali, il più recente piano strategico risente di un mutamento di prospettiva, in quanto non si limita a perseguire la *cybersecurity* ma pone come obiettivo nazionale il conseguimento del "*cyber power*", definito come "la capacità di proteggere e di promuovere gli interessi nazionali nel - e attraverso il - ciberspazio". Questa finalità aveva avuto la sua prima enunciazione nella

Integrated Review già richiamata, in cui veniva riconosciuta l'importanza per il Regno Unito di una posizione preminente da conseguire nello "spazio conteso" rappresentato dal ciberspazio; il piano strategico sulla cibersicurezza fa seguito a tale impostazione, nel presupposto che il ciberspazio sia destinato ad essere sempre più utilizzato dagli Stati per esercitare la loro influenza e proiettare all'estero il proprio potere nonché – nel caso dei "competitori sistemici" rappresentati dalla Russia e dalla Cina – il loro modello autoritario.

Nel 2016 è stato istituito il *National Cyber Security Centre* (NCSC), individuato come punto unitario di interlocuzione per le amministrazioni pubbliche, per le imprese e per la società civile relativamente ai temi della sicurezza cibernetica. Il NCSC esercita i propri compiti di protezione delle infrastrutture digitali principalmente mediante l'analisi degli incidenti oggetto di notifica nei suoi confronti. L'organismo svolge inoltre attività di ricerca e di assistenza in dialogo con l'industria di settore e con i centri di ricerca, utilizzandone i risultati anche ai fini della pubblicazione di guide operative dedicate ai molteplici aspetti della *cybersecurity*.

Nel 2023, il precedente *Centre for Protection of National Infrastructure* (CPNI) è stato trasformato nella *National Protective Security Authority* (NPSA), qualificata come autorità tecnica nazionale preposta alla sicurezza nazionale e alla difesa rispetto ad attività ostili provenienti dall'esterno. Essa opera come organismo ausiliario del Governo e degli apparati di sicurezza, tra cui il già noto NCSC e l'agenzia tecnica preposta alla segretezza delle comunicazioni (*UK National Authority for Counter Eavesdropping* - UKNACE).

Il concetto di *protective security* che guida l'attività della NPSA è destinato a trovare applicazione in una pluralità di settori, accomunati dalla loro rilevanza per la tutela della sicurezza nazionale da interferenze ostili od operazioni di sabotaggi poste in essere da entità straniere, e si declina nella scansione procedimentale di misure precauzionali di cui è imposta, o talora raccomandata, l'adozione a soggetti pubblici e privati.

Tali misure consistono essenzialmente nella previa identificazione dei rischi (*security risk assessment*) e nell'aggiornamento delle strategie di sicurezza; nel reclutamento, da parte delle organizzazioni interessate, di personale qualificato e appositamente selezionato; nella revisione dei *recovery plans* da applicare in caso di sabotaggio; nella notifica alle autorità

competenti di ogni attività insolita o sospetta. In relazione al profilo della *cybersecurity*, l'attività della NPSA si segnala anche per la definizione dei requisiti di sicurezza delle componenti elettroniche di sistemi fisici, allo scopo di ridurne la vulnerabilità rispetto ad attacchi esterni in grado di disattivare tali sistemi o di alterare le informazioni alla base del loro funzionamento (*Cyber Assurance of Physical Security Systems* – CAPPS).

Ad integrare il quadro delle autorità pubbliche titolari di competenze rilevanti in materia, sono inoltre la *National Cyber Force*, organismo costituito dalla collaborazione tra il Ministero della Difesa e il GCHQ e responsabile per l'esecuzione di operazioni sotto copertura dirette ad ostacolare o minimizzare attacchi cibernetici posti in essere da entità criminali o terroristiche oppure da Stati stranieri; la *National Crime Agency* (NCA) preposta alla lotta contro la criminalità organizzata e alla repressione di gravi reati, tra cui il *cybercrime*; ed infine, lo *UK Cyber Security Council*, organismo indipendente finanziato dal *Department for Science, Innovation and Technology* (DSIT) per la formazione professionale nel settore.

2.6. Stati Uniti d'America

La disciplina della sicurezza cibernetica negli USA è recata principalmente nel Federal Information Security Management Act (FISMA) del 2002. La legge è stata emendata da ultimo dal Strengthening American Cybersecurity Act of 2022.

Quest'ultima legge si compone di tre parti: la prima modifica il FISMA, la seconda disciplina la segnalazione di incidenti informatici, in particolare delle infrastrutture critiche, la terza riguarda la sicurezza del *cloud*.

Il principale organismo in materia di sicurezza cibernetica degli Stati Uniti è la Cybersecurity and Infrastructure Security Agency (CISA), che opera nell'ambito Dipartimento della Sicurezza Interna degli Stati Uniti. La CISA è il responsabile operativo per la sicurezza informatica federale e il coordinatore nazionale per la sicurezza e la resilienza delle infrastrutture critiche. CISA fornisce servizi e risorse incentrati sulla resilienza operativa, sulle pratiche di sicurezza informatica, sulla gestione organizzativa delle dipendenze esterne. CISA supporta cittadini e organizzazioni a comunicare gli attacchi informatici, gestire i rischi informatici, rafforzare le difese e adottare misure preventive.

Nel 2021 è stato istituito l'Office of the National Cyber Director (ONCD), organismo di consulenza al Presidente degli Stati Uniti in materia di politica e strategia di sicurezza informatica. L'ONCD è un componente dell'Executive Office del Presidente alla Casa Bianca.

Nel 2023 è stata pubblicata la National Cybersecurity Strategy con due obiettivi:

a) riequilibrare la responsabilità di difendere il cyberspazio, spostando l'onere della sicurezza informatica dai singoli individui, dalle piccole imprese, dagli enti locali e dai gestori delle infrastrutture alle organizzazioni più capaci e meglio posizionate per ridurre i rischi;

b) riallineare gli incentivi per favorire gli investimenti a lungo termine, cercando di bilanciare la difesa dalle minacce contingenti e la pianificazione strategica e gli investimenti del futuro.

Sulla base di tale documento sono stati elaborati due piani di attuazione, l'ultimo dei quali, National Cybersecurity Strategy Implementation Plan, risale al maggio 2024. Il piano delinea le azioni concrete intraprese dal Governo federale per migliorare la posizione di sicurezza informatica nazionale degli Stati Uniti.

Nel maggio 2024, the National Cyber Director ha trasmesso al Presidente degli Stati Uniti, all'Assistente del Presidente per gli Affari di Sicurezza Nazionale e al Congresso il Cybersecurity Posture of the United States 2024.

Si tratta di un documento che valuta la posizione della sicurezza informatica degli Stati Uniti, l'efficacia della politica e della strategia informatica nazionale e lo stato di attuazione della politica e della strategia informatica nazionale da parte dei dipartimenti e delle agenzie federali. Per "posizione di sicurezza informatica" si intende la capacità di identificare, proteggere, rilevare, rispondere e riprendersi da un'intrusione in un sistema informativo la cui compromissione potrebbe costituire un attacco informatico o una campagna informatica di conseguenze significative. Inoltre, questo documento riferisce al Congresso sulle minacce e sui problemi di sicurezza informatica che gli Stati Uniti devono affrontare, comprese quelle correlate alle nuove tecnologie che possono influire sulla sicurezza nazionale, sulla prosperità economica o sull'applicazione dello stato di diritto.