Audito	Sintesi degli interventi	Punti Trasversali
Audizione del Sottosegretario di Stato, Segretario del Consiglio dei Ministri e Autorità delegata per la sicurezza della Repubblica, **Alfredo Mantovano** n. 1 del 31/1/2024	In un paese come l'Italia, molto colpito da attacchi cyber e da ransomware (estorsioni cyber), la legislazione cyber è troppo risalente: le sanzioni sono inadeguate e non vi sono norme di coordinamento fra i vari dipartimenti coinvolti (es. autorità giudiziaria interessata al fatto che la scena del crimine rimanga inalterata; ACN interessata a ripristinare al più presto la funzionalità dell'ente colpito). Bene perciò l'inasprimento delle sanzioni, l'obbligo di notifica all'ACN dell'attacco cyber e il coordinamento previsto dalla l. 90/2024. L'intelligence svolge una costante azione di supporto, insieme all'ACN, per prevenire e neutralizzare gli attacchi e, rispetto alla Polizia, ha la possibilità strutturale di operare ex ante e sotto copertura rispetto alle condotte illecite → anche per questo vi è una constante e proficua interlocuzione con il COPASIR. Competenze in teoria ben distinte fra cyberdefence e cyberintelligence, venendo la prima in gioco quando l'attacco cyber integra un vero e proprio attacco di guerra; in pratica la distinzione è molto difficile da tracciare sul piano operativo (guerra "ibrida). Necessario perciò avvalersi della collaborazione della Difesa, ma sotto l'egida dell'Intelligence, indispensabile per evitare che le attività di cybersecurity poste in essere a tutela della sicurezza nazionale non siano riconducibili al Paese che le compie (approccio "ibrido"). La possibilità dei Servizi di operare sotto copertura e di avvalersi di omologhi servizi esteri scongiura infatti il rischio di un'attribuzione formale all'Italia di ingerenza nella sovranità altrui.	• Legislazione cyber troppo risalente; • ruolo di guida dell'Intelligence nella collaborazione con Polizia e Difesa; • necessario coordinamento e cooperazione fra le amministrazioni coinvolte; • grande difficoltà nel trovare professionisti esperti cyber.

	Ad ogni modo, è importante agire in modo coordinato: molto utile è in questa prospettiva CIC (Comitato Interministeriale per la Cybersicurezza), che ha un ruolo di raccordo fra le varie amministrazioni coinvolte per poter procedere d'intesa. Molto difficile trovare professionisti esperti della materia: sarebbe in proposito utile una parziale rimodulazione dell'offerta formativa delle università.	
Audizione del Direttore della Direzione informatica, telematica e tecnologie avanzate (TELEDIFE) del Ministero della Difesa, **Ten. Gen. E.I. Angelo Gervasio** n. 2 del 29/2/2024	TELEDIFE: Direzione del Ministero della difesa a composizione interforze, competente per le esigenze degli Stati maggiori che riguardano le tecnologie avanzate, elettroniche di telecomunicazioni e informatico-digitali, purché si tratti di tecnologie che non fanno parte di un sistema d'arma; è inoltre un importante punto di riferimento per le aziende private, curando l'individuazione dei partner commerciali (opportunamente certificati, se necessario) e la corretta esecuzione dei contratti d'appalto stipulati. La cybersecurity è sia una competenza trasversale a tutte le tecnologie sia un dominio a sé, caratterizzato da sistemi dedicati alla sua implementazione. Fondamentale curare aggiornamento dei dipendenti sulle proposte di mercato in materia cyber: la Direzione ha così organizzato moltissimi seminari di presentazione delle aziende nazionali e internazionali con cui la Direzione entri in rapporto; iniziativa utile ovviamente anche per garantire la continua formazione dei dipendenti.	• Cooperazione pubblico-privato; • cybersecurity: dominio a sé e dominio trasversale → necessario adottare un approccio coordinato e integrato, sia a livello nazionale (PCM; DIS/NSC; Agenzia di cybersicurezza) sia internazionale (UE, NATO, ONU)§; • aggiornamento sulle proposte di mercato e formazione dipendenti → seminari di presentazione di aziende con cui l'ente pubblico entri in rapporto; • necessario intervento normativo/direttiva nazionale per:

	La Direzione, nel migliore interesse della sicurezza nazionale, ha coinvolto realtà parte dell'alleanza NATO, affidabili e necessarie per l'impiego di sistemi e tecnologie altrimenti non reperibili sul territorio nazionale. Perciò, come affermato nelle risposte fornite per iscritto alla Commissione, è essenziale operare nell'ambito di un approccio strategico coordinato ricondotto all'interno di dispositivi nazionali (PCM; DIS/NSC; Agenzia di cybersicurezza) e/o multinazionali (UE, NATO, ONU). Necessario prevedere norme e direttive nazionali che: – definiscano le misure di cybersecurity minime da implementare per considerare sicura una infrastruttura informatica; – riconoscano la natura degli attacchi cyber e ci indichino i marcatori per identificarle come vere e proprie azioni ostili. È necessario disporre di procedure e mezzi che, per la loro applicazione in ambito cyber e per i possibili effetti che possono produrre (blocco e/o avarie di centri di produzione, di centrali energetiche, nodi telefonici e così via), sono certamente assimilabili a veri e propri sistemi d'arma → è quindi necessario intervenire sulla l.142/22 per modificare il regime normativo dell'autorizzazione al contrattacco, intervento reso necessario anche dal fatto che il dominio cibernetico è caratterizzato da elementi quali l'anonimia, l'ubiquità e l'assenza di confini geografici e politici, sicché l'attaccante beneficia dell'impunità e non è possibile con certezza attribuire la responsabilità di un determinato attacco cibernetico ad uno specifico Stato.	– definire misure di cybersecurity minime da implementare per considerare sicura una infrastruttura informatica; – riconoscere la natura degli attacchi cyber, indicando i marcatori per identificarle.; • intervenire normativamente sul regime di autorizzazione al contrattacco in ambito cyber, attesa l'assimilabilità a sistemi d'arma di determinati attacchi cyber e l'anonimia che caratterizza tale dominio; • adeguati investimenti pluriennali necessari, tenuto conto della velocità di sviluppo di tale materia.

	Stare al passo con i Paesi Europei implica una strategia nazionale complessiva che preveda adeguati interventi pluriennali d'investimento tesi ad allineare, continuamente, il livello di sicurezza delle piattaforme digitali e dei correlati servizi allo stato dell'arte tecnologico, in relazione al continuo evolversi della minaccia cibernetica; le risorse disponibili in ambito cyber-sicurezza crescono con minore velocità rispetto alla crescita esponenziale delle possibili minacce → possibile impiego intelligenza artificiale.	
Audizione del Direttore dell'Agenzia per la cybersicurezza nazionale, **Bruno Frattasi** n. 3 del 21/3/2024	La strategia nazionale di cybersecurity si fonda su 4 pilastri: 1. Il primo, il principale, fa capo all'ACN, responsabile della resilienza del Paese nel processo di transizione tecnologica; 2. Il secondo è costituito dallo strumento miliare, ossia la cyberdefence, intesa come controffensiva, che prefigura un vero e proprio stato di guerra; 3. il terzo è costituito dal cybercrime, assicurato dall'apparato di polizia, in particolare la Polizia postale; 4. il quarto è quello della raccolta informativa, la cyberintelligence, appannaggio dei Servizi di informazione. La distinzione, chiara in teoria, fra cyberdefence e cybercrime sfuma in concreto. Il rischio cyber è sensibilmente cresciuto, anche in conseguenza di determinati eventi storici: la crisi pandemica e la remotizzazione dei rapporti di lavoro ed economici, con lo scoppio del conflitto Russia-Ucraina e, infine, il conflitto Israele-Hamas.	• Campagne di sensibilizzazione; • maggiori investimenti nella cyber; • più stretto coordinamento fra ACN e PA; • approccio olistico e visione sistemica del rischio cyber impongono: – una maggiore integrazione delle competenze; – un innalzamento trasversale del grado e del livello della formazione in tale materia.

	Il rischio cyber coinvolge la PA, le piccole e medie imprese, i grandi player nazionali e cittadini professionisti. L'Italia è in ritardo nella risposta cibernetica. È quindi necessario: – promuovere la consapevolezza della comunità nazionale rispetto al rischio cyber → campagne di sensibilizzazione. – promuovere investimenti; – rafforzare il coordinamento delle PA con l'ACN sottoscrivendo intese e protocolli di attività (bene l'obbligo di notifica all'ACN dell'attacco cyber sancito dalla l. 90/2024); – maggior coesione dell'ACN con l'apparato militare e la Difesa, sia in termini di condivisione di competenze per specifiche aree sia di apporto di personale (con il "doppio cappello", affiancando alla dipendenza gerarchica militare quella funzionale rispetto all'ACN) → è infatti fondamentale privilegiare l'integrazione delle competenze, mantenendo un approccio olistico e una visione sistemica che tiene conto dell'interdipendenza e della multifattorialità che caratterizzano la cybersecurity.	
Audizione del Comandante del Comando per le Operazioni in Rete (COR), Gen. Sq. AAran, **Sergio Antonio Scalese** n. 4 del 4/4/2024	Seduta segreta	

Audizione dell'Amministratore delegato di CY4GATE S.p.A. **Emanuele Galtieri** n. 5 del 7/5/2024	Elementi di contesto: – in Italia stanno aumentando sia il numero degli incidenti dovuti alle minacce cyber che il loro livello di gravità; – il livello di insicurezza digitale percepito è particolarmente rilevante; – la digitalizzazione nelle istituzioni e nelle aziende si va a sovrapporre a una serie di sistemi e architetture informatiche *legacy,* ovvero vecchie, che non erano state create con l'attenzione a garantire un'adeguata sicurezza cibernetica; – democratizzazione del crimine digitale (creare virus o generare attacchi sono ormai azioni a basso costo). L'Italia si è mossa creando un'infrastruttura di governance che vede la ACN a capo della *cyber resilience* del Paese e con il ddl Atto Camera 1717 (Commissioni riunite Affari costituzionali e Giustizia) su rafforzamento delle misure cibernetiche e contrasto ai crimini informatici. Quattro sono i punti essenziali dal punto di vista di un'azienda che produce tecnologie per alzare barriere contro gli attacchi cibernetici: 1) le risorse umane (sono troppo pochi i professionisti operativi della *cyber security* e le aziende si contendono i "*cyber* talenti") e la protezione cibernetica del cittadino e la formazione finalizzata ad essere cittadini in grado di proteggersi dagli attacchi digitali; 2) l'incentivazione delle *partnership* pubblico-privato; 3) la necessità di proteggere le filiere di approvvigionamento (*supply chain).* Le PMI non godono degli stessi livelli di protezione delle aziende di importanti dimensioni, ma sono queste stesse *supply chain* che mettono a rischio le aziende e le istituzioni a cui esse forniscono i propri beni e servizi. Il rischio è che gli hacker passino attraverso le	• Occorre incrementare il bacino di reclutamento per le università nelle discipline STEM, che sono maggiormente impiegate nel segmento della *cyber security.* • Servono laboratori *cyber* nelle scuole per insegnare a vivere il mondo digitale, a lavoro o nella ▪ vita privata, in maniera più consapevole. • Nell'A.C. 1717, articolo 7, estendere l'incentivazione delle *partnership* pubblico-privato anche al campo della *cyber security.* • Bisogna avviare un percorso di "impermeabilizzazione" delle PMI, valutando delle formule incentivanti sulla tematica della cybersecurity (anche rivedendo la clausola di invarianza finanziaria prevista dall'articolo 18 del ddl A.C. 1717). • Valutare se inserire nell'articolo 10 del ddl A.C. 1717 un riferimento all'obbligo di acquisire tecnologia italiana ed europea nell'ambito dei

	filiere per arrivare alle aziende o alle istituzioni, che, invece, hanno modo di proteggersi; 4) l'autonomia digitale italiana ed europea (creazione di tecnologie nazionali ed europee).	contratti pubblici di beni e servizi
Audizione dei rappresentanti di Fastweb S.p.A., **Alessia Di Nucci, Francesco Argano** n. 6 del 15/5/2024	Fastweb, titolare di tutte le principali convenzioni in ambito della *cybersecurity* legate alla pubblica amministrazione, evidenzia che l'Italia è sempre più nel mirino degli attacchi informatici e gli attacchi sono sempre più frequenti e gravi, con oggetti privilegiati la pubblica amministrazione e il settore *finance*. In particolare, sono aumentati sia le modalità di attacco, sia il volume degli attacchi generati tramite l'intelligenza artificiale (AI). Dall'altro lato, l'AI è uno strumento in grado di potenziare fortemente la resilienza della postura cibernetica di un Paese, ad esempio attraverso processi di crittoanalisi, di simulazione di attacco e difesa, o come strumento decisionale. Tuttavia in Italia c'è il problema che l'AI generativa non dispone di modelli linguistici basati sulla conoscenza e sul linguaggio italiano. Pertanto, Fastweb sta creando il primo *Large Language Model* (LLM) italiano attraverso un investimento mirato alla creazione di un supercomputer che possa fornire quella capacità computazionale necessaria per poter elaborare questo algoritmo dalle fondamenta. Un punto chiave, quindi, è il corretto addestramento del modello attraverso fonti di buona qualità.	• L'AI rappresenta la nuova frontiera del perimetro di difesa cibernetica. • Occorre investire sia nella formazione di professionalità nel campo della *cybersecurity* sia nella formazione diffusa di tutti quelli che utilizzano gli strumenti digitali (ad esempio i dipendenti di un'azienda o di una pubblica amministrazione). • Aumentare l'autonomia tecnologica del Paese, ridurre le dipendenze dall'estero e creare un ecosistema italiano per la difesa cibernetica e l'AI.
Audizione dei rappresentanti di Leonardo S.p.A., **Lorenzo Mariani, Andrea Campora**	Il contesto di riferimento della sicurezza è segnato da: – i conflitti Russo-Ucraino, quello in Medio Oriente e numerosi altri conflitti e tensioni nel mondo; – la minaccia ibrida e asimmetrica	• Garantire un approccio *Risk-Based* trasversale ai decisori che assicuri la resilienza cibernetica delle organizzazioni e degli asset nazionali.

n. 7 del 22/5/2024	– la digitalizzazione pervasiva, che ha portato benefici ma anche una maggiore vulnerabilità nei confronti della minaccia *cyber*. Le infrastrutture critiche digitali sono divenute «target non convenzionali». La superiorità tecnologica, e non solo militare, è un nuovo elemento di deterrenza. La difesa convenzionale si sta evolvendo in un concetto più ampio di Sicurezza Nazionale e Globale, che include anche produzione e uso di dati, cyber security, controllo dello spazio, sicurezza delle infrastrutture, sicurezza energetica, capacità di previsione avanzate, intelligenza artificiale, cooperazione internazionale. A supporto di questa nuova visione di sicurezza globale, Leonardo si pone come motore tecnologico e industriale, per la crescita dell'ecosistema nazionale. All'interno di Leonardo, la Divisione Cyber & Security Solutions di Leonardo ha in carico tutti gli aspetti di *cybersecurity*, con tre mercati di riferimento: - quello della difesa (il mercato principale), - la space economy, - le organizzazioni strategiche nazionali (*government* e infrastrutture critiche) e tre tecnologie: la *cybersecurity*, l'intelligenza artificiale e tutto il mondo dei dati (data plafond, controllo, gestione e sviluppo dei dati). Vengono illustrati anche i progetti chiave della Divisione in ambito di *cybersecurity*. Il buon funzionamento di questo sistema è legato fortemente alla presenza di grandi realtà che siano, però, in grado di valorizzare e farsi giustamente supportare da una filiera produttiva di PMI, che vede nell'innovazione uno dei suoi punti di forza. Anche ai fini dell'export di	• Supportare l'evoluzione della Difesa verso la Sicurezza Globale, garantendo la protezione delle infrastrutture critiche civili e militari. • Assicurare il coinvolgimento dei soggetti privati da parte del Pubblico (ad esempio PPP). • Stanziare risorse per lo sviluppo di tecnologie sovrane e capacità autonome nei settori cyber strategici per la resilienza delle difese nazionali. • Tutti i sistemi della difesa devono essere *cyber secure by design* in futuro.

	sistemi di difesa, sicurezza e alta tecnologia, è importante il ruolo di un federatore dei componenti della *supply chain*.	
Audizione dei rappresentanti di CISCO Systems Italy S.r.l. **Gianmatteo Manghi, Giuseppe Massa, Lorenzo Ghioni** n. 8 del 23/5/2024	Tre argomenti principali: – il ruolo che può avere l'intelligenza artificiale come strumento di difesa. Nell'ambito di *Cyber Security* Cisco sta lavorando in alcune direzioni prioritarie, fra cui controllo del traffico cifrato, supporto attivo alle configurazioni, rilevamento e reazione alle minacce, controllo degli accessi. – suggerimenti sull'aspetto normativo: ▪ sicurezza delle reti dei fornitori (*supply chain*). Occorre implementare la «sicurezza pervasiva», prevedendo sistemi di sicurezza sull'originalità e l'autenticità delle componenti (ad esempio, *chip* anti-manomissione, che dovrebbero essere obbligatori almeno per le infrastrutture critiche); ▪ un'incentivazione a favore di interventi di *cybersecurity* posti in essere dagli operatori di telecomunicazione, a fini di protezione delle dorsali strategiche, le più grandi linee di comunicazione che portano il traffico internet, che sono controllate e di proprietà degli operatori di telecomunicazione; ▪ a livello di strategia europea, il partenariato tra l'Unione europea e la NATO è la soluzione colmato il gap tecnologico esistente rispetto ad alcuni Paesi (Cina, Stati Uniti, India, …). – il ruolo che giocano le tecnologie quantistiche e fotoniche sviluppate nel centro di ricerca Cisco di Vimercate. In questo centro, fra l'altro,	• sicurezza della *supply chain*. • protezione delle dorsali strategiche di comunicazione internet

	si stanno sviluppando algoritmi che siano robusti ai computer quantistici, al fine di evitare, ad esempio, che i computer quantistici possano, con quello che viene definito « *brute force attack* », provare miliardi di *password* fino a quando non trovano quella giusta. Inoltre, in questo centro si svolgono ricerca riguardanti la protezione dei cavi di telecomunicazione, anche nell'ottica di salvaguardare le infrastrutture critiche dell'infrastruttura sia nazionale sia europea.	
Audizione del Capo del III Reparto del Comando Generale dell'Arma dei Carabinieri, **Gen. di D. CC Paolo Aceto,** e del Capo Centro Sicurezza Telematica del Comando Generale dell'Arma dei Carabinieri, **Bottazzi Giovanni** n. 9 del 29/5/2024	C'è stata un'evoluzione della minaccia criminale nella dimensione *cyber*: Il processo di globalizzazione rappresenta un'occasione anche per la criminalità. Per la difesa da questa minaccia occorre: – un'ampia e strutturata collaborazione internazionale; – valorizzare le capacità *cyber;* – un adeguato e condiviso flusso informativo, filtrato ed elaborato, mediante un'efficace capacità di – analisi e valutazione strategica; – incremento delle risorse umane in possesso di competenze tecniche; – garantire la flessibilità dello strumento operativo, anche con riferimento alle procedure di approvvigionamento e finanziarie. Sotto il profilo normativo, il quadro legislativo e regolamentare nazionale si è evoluto nel tempo per garantire al Paese uno spazio cibernetico sicuro, al fine di raggiungere adeguati livelli di resilienza delle reti e dei sistemi, ma anche di elevare la capacità di risposta e la reattività alle attività ostili. Tali obiettivi possono essere raggiunti pianificando apposite misure tecniche a seguito di un'attenta valutazione del rischio: – i software dei sistemi e degli apparati devono essere adeguatamente supportati, aggiornati, sottoposti a verifiche di sicurezza periodiche,	Prevedere significativi investimenti: • in tecnologie di tipo *cloud*, ipotizzando la progressiva riduzione dei *data center* fisici, in un'ottica di consolidamento e riduzione della superficie di attacco e, di conseguenza, maggiore sicurezza fisica e logica, nonché sostenibilità economica e ambientale; • nella formazione di tecnici e di personale specializzato, ma anche per tutto il personale in materia di cyber-sicurezza.

	privi di vulnerabilità posturale o debolezze progettuali e, soprattutto, debolezze comportamentali; – è necessario dotarsi di strutture altamente specializzate che, in caso di incidente informatico, dispongano, da un lato, di una mappatura dei sistemi di proprio interesse e, dall'altro, siano in grado di individuare e interrompere i servizi compromessi o in corso di compromissione; – occorre considerare anche le variabili da connesse con i profili organizzativi, con i processi, con le attività di vigilanza e, nella consapevolezza che il fattore umano costituisce spesso un importante elemento di vulnerabilità, con l'aspetto formativo. Queste variabili risultano ancora più significative per l'Arma dei Carabinieri, la cui struttura organizzativa è particolarmente complessa perché articolata su migliaia di presìdi, ove agiscono oltre 100 mila operatori, che utilizzano terminali fissi e mobili, fortemente interconnessi con sistemi informativi interni ed esterni all'istituzione. Alcune funzioni, inoltre, vengono svolte anche in territorio estero, nell'ambito di missioni o altre attività diversamente strutturate. Tale impianto organizzativo, dunque, necessita di una solida architettura informatica.	
Audizione del Segretario Generale della Difesa e Direttore Nazionale degli Armamenti, **Gen. C.A. Luciano Portolano** n. 10 del 30/5/24	Occorre privilegiare, in ambito militare, un approccio multisettoriale e integrato, capace di operare in ogni dominio, compreso quello cyber, che si sovrappone in modo trasversale ai domini tradizionali (terrestre, aereo, marittimo e spaziale) e allarga il confine delle operazioni militari, fondendo la sfera militare con quella civile, sia pubblica che privata. L'Italia è in ritardo nella risposta cibernetica. La cyberdefence non è un prodotto, ma un processo in continua evoluzione; questo richiede: – formazione continua; – agilità organizzativa;	• Approccio multisettoriale e integrato; • formazione continua; • agilità organizzativa; • implementazione di standard di sicurezza; • ricerca e innovazione; • approccio secure by design;

	– implementazione di standard di sicurezza; – soprattutto, propensione alla ricerca e all'innovazione, anche ai fini dell'elaborazione di prodotti "dual use" (ossia utili non solo per le Forze armate, ma anche per la società civile). La cooperazione internazionale (es. il fondo europeo per la difesa), anche a carattere industriale, è particolarmente essere utile per: – sviluppare nuove tecnologie e capacità; – creare un approccio sistemico e integrato di collaborazione con paesi alleati. L'eccessiva frammentazione è infatti un ostacolo allo sviluppo delle tecnologie made in Ue. Necessario adottare approccio "secure by design". Il crescente ricorso a tecnologie digitalizzate nel rendere i nuovi sistemi d'arma più efficaci ne ha anche innalzato il livello di vulnerabilità ad azioni cibernetiche; si rende dunque necessario supportare la politica industriale in tale settore, anche al fine di perseguire l'obiettivo di autonomia strategica nazionale ed europea nel settore digitale.	• maggiore cooperazione in ambito Ue e con paesi alleati per autonomia strategica e sicurezza; • supporto alle politiche industriali in tema di cybersecurity.
Audizione dei rappresentanti di FINCANTIERI S.p.A., **Pierroberto Folgiero, Daniele Alì** n. 11 del 12/6/2024	La cyber, in Fincantieri, è di fondamentale importanza sia nel processo produttivo che nel prodotto. L'azienda ribadisce l'importanza di proteggere tutto quello che riguarda la propria catena del valore, quindi la progettazione, l'ingegneria, la qualità, il sistema produttivo e l'export. Anche il *top management* assume un ruolo in tal senso, in particolare attraverso tutte le operazioni di *awareness,* ovvero attraverso la conoscenza	• La cybersicurezza come elemento centrale nella creazione del valore per le imprese; • l'impiego di meccanismi di intelligenza artificiale in maniera sempre più convinta all'interno dei processi operativi;

	della disciplina, dell'impianto regolatorio, in modo da farli venire alla luce e renderli parte della cultura aziendale. Con riferimento agli investimenti, Fincantieri investe molto sulla *cybersecurity*, e ne ribadisce l'importanza. Il primo piano di investimenti in cybersecurity ha previsto diversi filoni di investimento, tra cui il più importante è certamente l'*insourcing* strategico delle competenze. In sintesi i tre filoni sono i seguenti: - fare in modo che le competenze di cybersecurity diventino parte integrante del DNA dell'azienda; - il miglioramento tecnologico, perché bisogna essere sempre al passo con i tempi; - lo sviluppo di funzionalità e servizi che ci aiutino a essere sempre più competitivi e resilienti. Per quanto riguarda il futuro, il piano di evoluzione prevede: • l'impiego di meccanismi di intelligenza artificiale in maniera sempre più convinta all'interno dei processi operativi; • un'attenzione sempre maggiore alla catena di fornitura e ai requisiti di conformità, che stanno diventando sempre più attenti alla *cybersecurity;* • un rafforzamento delle nostre strutture preventive per far sì che l'attacco sia gestito in fase di prevenzione, piuttosto che in fase di blocco. Questo implica cambiare operativamente alcuni processi, cercare di fare in modo che l'analisi delle anomalie venga il più possibile automatizzata. Considerazioni e riflessioni per la Commissione: • innanzitutto quando si parla di investimenti in *cybersecurity*, nel momento in cui un'azienda investe in *cybersecurity* e questo	• attenzione sempre maggiore alla catena di fornitura e ai requisiti di conformità, che stanno diventando sempre più attenti alla *cybersecurity;* • un rafforzamento delle nostre strutture preventive per far sì che l'attacco sia gestito in fase di prevenzione, piuttosto che in fase di blocco; • il problema della mancanza di risorse professionali sul mercato; • utilità della creazione di percorsi formativi attraverso un confronto diretto tra accademie e istituti tecnici e privato; • necessità di supportare, attraverso un cofinanziamento dello Stato, gli investimenti in *cybersecurity* nel momento in cui un'azienda investe in *cybersecurity* e questo investimento va a proteggere parte di un segmento aziendale che è parte integrante del sistema di sicurezza dello Stato; • necessità di supportare in generale la piccola e media

	investimento va a proteggere parte di un segmento aziendale che è parte integrante del sistema di sicurezza dello Stato, un cofinanziamento di quegli investimenti potrebbe essere di grande aiuto; • siamo consapevoli che la piccola e media impresa ha problemi sia a garantire finanziariamente gli sviluppi tecnologici relativi alla creazione di un programma di *cybersecurity*, sia a trovare competenze di rilievo che possano supportarla nell'attuazione di un programma. Pertanto, sarebbe importante incentivare il sistema delle piccole e medie imprese a essere sempre più resilienti; • il problema della mancanza di risorse professionali sul mercato è un problema che credo sia trasversale a ogni segmento. Quindi, la creazione di percorsi formativi attraverso un confronto diretto tra accademie e istituti tecnici e privato sicuramente gioverebbe. Fare *cybersecurity* non vuol dire solo recepire laureati, ma selezionare persone che abbiano un *mindset* orientato al *problem solving* e siano in grado di supportare le aziende a superare problemi complessi; • sarebbe importante favorire in ambiti critici tecnologie italiane, possibilmente a «codice aperto», in modo che ne sia permessa l'ispezione e diventi patrimonio nazionale per tutte quelle applicazioni tecnologiche che sono critiche per il nostro sistema-Paese; • da ultimo, bisognerebbe supportare le *start-up* nazionali nella creazione di iniziative congiunte tra pubblico e privato in cui aziende del calibro di Fincantieri, che hanno sia la capacità sia che la palestra tecnologica in cui sperimentare queste tecnologie, possano incubare un	impresa che presenta difficoltà sia a garantire finanziariamente gli sviluppi tecnologici relativi alla creazione di un programma di *cybersecurity*, sia a trovare competenze di rilievo che possano supportarla nell'attuazione di un programma; • supportare le *start-up* nazionali nella creazione di iniziative congiunte tra pubblico e privato.

	sistema di *start-up* nazionali e aiutarle anche nel travaso tecnologico tra settore difesa e settore civile, nonché spalancare loro le porte della propria rete commerciale.	
Audizione dei rappresentanti di Nutanix Italy S.r.l., **Benjamin Jolivet, Pasquale Potenza, Pierluigi Valentini** n. 12 del 3/7/2024	Nutanix è una società nuova nel settore difesa. È stata fondata nel 2009 e si presenta come *leader* mondiale di piattaforme *software* che organizzano l'infrastruttura digitale. L'obiettivo dell'impresa è dunque quello di organizzare e collegare queste piattaforme a livello software orientando questa infrastruttura a poter ospitare l'intelligenza artificiale. Viene sottolineata l'importanza di avere un'infrastruttura software resiliente, forte, scalabile, che sia quasi impenetrabile. Viene poi sostenuta la necessità di ridurre le emissioni di CO2 di queste infrastrutture. Relativamente alla sicurezza viene riportato che: - attualmente si registra un aumento esponenziale degli attacchi cibernetici. Sicuramente i conflitti che stiamo vivendo negli ultimi anni non ci stanno aiutando (soltanto a metà 2023 si è osservato un 40 per cento in più di attacchi rispetto al 2022). - tra questi attacchi possiamo, mettere al primo posto il *cyber-spionaggio* condotto da gruppi di *cybercriminali*, tipicamente di origine russa o asiatica, che quotidianamente cercano di attaccare obiettivi strategici di enti governativi o internazionali. Sebbene vi siano anche *cyber-criminali* che cercano di estorcere denaro trafugando dati o cercando di rivenderli. Ancora, certamente vi è, tra le ragioni degli attacchi *cyber*, anche la notorietà, in quanto c'è una grande attenzione mediatica su questo fenomeno. Si pensi che l'NCA (*National Crime Agency*) del Regno Unito ha fatto un'indagine dalla quale è emerso che l'età media degli hacker arrestati recentemente è di diciassette anni;	• Importanza della piattaforma *software* rispetto all'*hardware*; • Diffusione di struttura cd. Ibrida, ovvero a *cloud* ibrido. In questa struttura, un attacco si può manifestare dappertutto, rendendo necessario proteggersi dal movimento laterale in ambito *cybersecurity*. Con un attacco ad un'impresa è possibile comprometterne anche altre ad essa collegata; • si registra un aumento esponenziale degli attacchi cibernetici; • al primo posto, tra questi attacchi, troviamo il *cyber-spionaggio* condotto da gruppi di *cybercriminali*, tipicamente di origine russa o asiatica; • abbiamo sempre meno risorse competenti nella cybersicurezza; • importanza della formazione come misura di contrasto agli attacchi cyber;

	- abbiamo sempre meno risorse competenti in questo settore, anche perché c'è un movimento forte nella direzione di abbandonare la gestione del *data center* per affidarsi alle potenze digitali; Soluzioni: - predisporre una resiliente infrastruttura tecnologica e un sistema di sicurezza fatto di tecnologia, tipicamente *software*, quali *firewall*, *antimalware*, *antivirus*, *intrusion detection system* e simili; - aggiornare costantemente la propria infrastruttura tecnologica con il *backup* dei sistemi (le famose *patch*, in gergo); - la formazione, perché se in azienda ci sono i cosiddetti «cliccatori seriali» che aprono tutti gli allegati delle *e-mail* va da sé che qualunque protezione non ha alcun effetto; - è necessario innalzare la formazione dei giovani, per far sì che le organizzazioni non soffrano di un *gap* conoscitivo importante. Per prevenire questo e organizzare la competenza, dunque, occorre un innalzamento del livello digitale in tutte le organizzazioni. Viene evidenziato che oltre il 70 per cento delle aziende, quando vengono attaccate da un *ransomware* o da qualsiasi altro *malware*, per ripristinare la funzionalità ci impiegano settimane, poiché le infrastrutture che sono sotto le applicazioni, erano deboli, o in altri casi sono state compromesse, o non hanno ricevuto le adeguate azioni di *governance* quali il *backup* e il *disaster recovery*. Questo rende necessario dunque il fermo delle istituzioni o delle imprese interessate. La resilienza informatica e delle infrastrutture, dunque, è importante, anche per le nostre forze armate, in quanto oggi le minacce sono tantissime e persistenti. Ci troviamo, infatti, in un contesto geopolitico nel quale basta attaccare un'impresa per comprometterne altre o,	• importanza di gestire gli attacchi informatici con adeguate azioni di *governance* quali il *backup* e il *disaster recovery*.

	addirittura, compromettere le pubbliche amministrazioni che eventualmente collaborano con l'impresa. In considerazione del *cloud* ibrido, peraltro, questo attacco si può manifestare dappertutto, rendendo necessario proteggersi dal movimento laterale in ambito *cybersecurity*. Vi è quindi la necessità di organizzare l'interoperabilità delle piattaforme che state costruendo, che il Governo sta costruendo con le amministrazioni centrali e con le imprese. È necessaria una particolare attenzione alla piattaforma *software* che si sta costruendo. L'IT di oggi non è guidato dall'*hardware*. Il *software* guida tutto.	
Audizione dei rappresentanti di Innovery S.p.A. **Gianvittorio Abate, Guido Moscarella, Pasquale Patricelli, Pietro Parente** n. 13 del 10/7/2024	Innovery SpA è una società di servizi, nata nel 2001, che lavora nell'ambito della sicurezza informatica. Essa è fondamentalmente un system integrator, quindi integra soluzioni di terze parti per proteggere sia le applicazioni, sia il perimetro aziendale e i dati, di aziende e di enti governativi. Stiamo passando da una realtà tecno-centrica, in cui la tecnologia è sempre stata al centro delle «securizzazioni» dei perimetri delle aziende, ad una realtà in cui invece si pone molta attenzione a quello che è il comportamento umano, ovvero l'aspetto che, ad oggi, rappresenta la maggiore vulnerabilità di un'azienda. Il fattore chiave del successo viene riconosciuto nel personale. In tal senso: - occorre riconoscere e favorire il continuo aggiornamento del personale; - la formazione non può essere vista come la semplice *awareness* che viene fatta in un momento successivo, quando il dipendente entra nell'azienda. È importante che la formazione avvenga anche	- personale quale elemento chiave di successo nella cybersicurezza, ma al contempo una delle principali criticità; - ruolo centrale della formazione e della istruzione, in tutti i suoi livelli, nello sviluppo delle competenze del personale; - pubblica amministrazione (ed in particolare quello dell'*healtcare*) quale settore che ha ricevuto più attacchi nel 2023; - le nuove frontiere e i nuovi scenari a cui dobbiamo prepararci a rispondere nel medio e nel lungo termine, sono il *quantum computing* e l'intelligenza artificiale;

	prima, perché ormai tutti i processi digitali che accompagnano la nostra quotidianità hanno necessità di essere protetti; - è necessario il rafforzamento della formazione e dell'istruzione a tutti i livelli quale elemento fondamentale nella ricerca del personale. Essere presenti in maniera diffusa sul territorio e di investire sull'università e sulla formazione è un elemento qualificante. - sarebbe opportuno valorizzare le competenze in possesso delle aziende, ad esempio, nelle procedure di gara, potrebbe essere utile, in alcuni perimetri specifici di altissima professionalità, provare anche ad ingaggiare le società con delle *challenge*, con delle prove sul campo, al fine di testare effettivamente le abilità, al di là di quella che è una mera descrizione che si può avere durante una fase di risposta di gara. Il riconoscimento del ruolo chiave giocato dal personale deriva proprio dal fatto che l'azienda riconosce che, nell'ambito della nell'ambito dei servizi legati alla cyber-sicurezza, una delle principali criticità è proprio il personale che viene impiegato. Inoltre viene riportato che, con riferimento alle principali minacce presenti nel mercato, i settori maggiormente colpiti sono quelli della pubblica amministrazione, in particolare quelli dell'healthcare (come evidenziato anche dal report del Threat Landscape, il panorama delle minacce redatto dall'ENISA). le tipologie di attacco, le principali sono quelle del ransomware e degli attacchi di disponibilità dei servizi. Questi attacchi stanno aumentando. Le nuove frontiere e i nuovi scenari a cui dobbiamo prepararci a rispondere nel medio e nel lungo termine, sono il *quantum computing* e l'intelligenza artificiale.	- emerge una proposta particolare in tema di valutazione delle competenze delle imprese nelle procedure di gara, proponendo una *challenge* per testare effettivamente le abilità delle imprese.

	Questo poiché con il *quantum computing*, con l'aumento enorme delle capacità computazionali di questi computer, possono essere facilmente compromessi gli algoritmi di crittografia che sono attualmente utilizzati. Si rende necessario, dunque, predisporre soluzioni *quantum-proof* poiché in un'eventuale esfiltrazione di dati, questi, anche se non possono essere letti al momento della sottrazione, potrebbero essere letti in futuro quando questi computer quantistici saranno pronti. Quindi, è importante già da ora iniziare a pensare a soluzioni di tipo *quantum-proof*, alcune delle quali sono state già identificate proprio quest'anno e poi dovranno essere certificate per essere adottate sul perimetro nazionale. L'intelligenza artificiale è, invece, una minaccia che si è ormai palesata nel nostro scenario. È qualcosa che esisteva già da tempo, ma quello che è cambiato con l'AI (Artificial Intelligence) generativa dipende dal fatto che essa è diventata accessibile a tutti, quindi anche agli attaccanti, che possono fare attacchi più sofisticati. Il più banale è un attacco di phishing; laddove prima ci si accorgeva immediatamente, in modo abbastanza semplice, che una mail poteva essere di phishing, già dalla grammatica, oggi errori grammaticali non se ne fanno più, perché l'attaccante si fa correggere il testo tramite ChatGPT rendendone più complessa l'identificazione. Aumentano anche le superfici di attacco. Con i SOC, Security operations center, occorre utilizzare l'intelligenza artificiale per supportare gli analisti nell'identificazione di questo nuovo tipo di minacce e per efficientare il loro lavoro.	
Audizione del Presidente dell'Associazione nazionale giovani innovatori (ANGI), **Gabriele Ferrieri**	ANGI è un'organizzazione no profit dedicata all'innovazione. Rappresenta più di 5.000 imprese, con l'obiettivo di promuovere il tema del trasferimento tecnologico e digitale e di creare un ecosistema digitale stabile e sicuro.	• Aumento degli attacchi cyber; • importanza dell'attività di formazione e sensibilizzazione sul tema della cybersicurezza per la diffusione di una cultura della

n. 14 del 19/9/2024	La cyber security viene identificata come una priorità globale, in considerazione dell'aumento esponenziale delle minacce informatiche e della crescente dipendenza dalle tecnologie digitali. Dopo una illustrazione delle normative disciplinanti la tematica della cybersicurezza, anche a livello europeo, viene segnalata una crescita delle minacce cyber. In particolare, abbiamo: - un incremento degli attacchi ransomware e phishing, che colpisce soprattutto PMI e infrastrutture critiche. - una esposizione crescente al dark web e al furto di identità. Viene evidenziato come l'Europa abbia adottato misure per favorire l'attività, per salvaguardare istituzioni, organi e organismi, con l'obiettivo di avere una cabina di regia unica per la gestione, la governance e il controllo dei rischi. Vengono quindi formulate le seguenti proposte: - la creazione di una Cabina di regia unica sulla sicurezza delle infrastrutture critiche. Con questo strumento si auspica che la cooperazione possa essere ulteriormente allargata anche ad altri organi coinvolti nella cybersicurezza, tra cui ad esempio l'Agenzia per l'Italia Digitale. - il rafforzamento di un Comitato interistituzionale, che possa aiutare e favorire il monitoraggio, ma soprattutto sostenere l'attuazione di misure sia in ambito europeo che nazionale; - la necessità di un'armonizzazione della normativa, soprattutto su settori critici (difesa, telecomunicazioni, energia); - un maggior avvicendamento, anche di risorse, cui non soltanto deve far fronte l'Italia, ma soprattutto l'Europa, fondamentale per adottare misure di cyber security specifiche che possano aiutare a proteggere le infrastrutture critiche, lavorando maggiormente in	sicurezza digitale tra cittadini e imprese; • armonizzazione normativa; • creazione di una Cabina di regia unica sulla sicurezza delle infrastrutture critiche che garantisca un maggior coordinamento tra i diversi soggetti coinvolti in materia di cybersicurezza; • maggiori investimenti in cybersicurezza e maggiore collaborazione tra pubblico e privato; • necessità di garantire un dialogo trasversale tra tutti gli attori che fanno parte dell'ecosistema, individuando soprattutto il tema della tecnologia a disposizione.

	dipartimenti intercomunitari tra i vari soggetti ed esponenti dello Stato maggiore della difesa; - una collaborazione rafforzata tra pubblico e privato ed un rafforzamento degli investimenti in ricerca e sviluppo, al fine di sviluppare nuove tecnologie per la sicurezza; - la cooperazione internazionale per le sfide globali sulla cyber defence, in quanto anche il trasferimento tecnologico con Paesi membri della NATO può essere utile per far fronte a minacce comuni; - la sensibilizzazione e la formazione sul tema della cybersicurezza per diffondere una cultura della sicurezza digitale tra cittadini e imprese; - rafforzare le sanzioni per crimini informatici. Viene infine ribadita la mancanza di dialogo e la conseguente necessità di creare una sicurezza che possa essere trasversale tra tutti gli attori che fanno parte dell'ecosistema, individuando soprattutto il tema della tecnologia a disposizione. Si ritiene che su questo tutti gli strumenti siano in mano alle Forze armate. Si individua quale punto fondamentale quello di una maggiore inclusione e di un maggiore dialogo tra diversi esperti delle infrastrutture critiche dello Stato.	
Audizione dei rappresentanti di Engineering S.p.A., **Marco Valentini Vito Morreale** n. 15 del 25/09/2024	Engineering Spa è una società italiana nata a Padova nel 1980. La società opera in diversi settori strategici come la difesa, *l'energy*, la salute, la pubblica amministrazione e l'agricoltura. Per quanto la sicurezza cybernetica, evidenziamo che l'anno scorso, rispetto al 2022, a livello mondiale c'è stato un incremento degli attacchi di circa l'11%, mentre in Italia del 65%. Sulle tipologie di attacco siamo invece allineati con il resto del mondo.	• Incremento attacchi cyber nel nostro Paese; • Necessaria la focalizzazione, come Paese, su alcuni elementi distintivi del mercato globale della cybersecurity, senza sovrapporsi a quello che stanno facendo altri Paesi;

	Negli ultimi anni ci sono stati più attacchi efficaci alle infrastrutture critiche nazionali. Il concetto di infrastruttura critica si è esteso. Viene evidenziata la tendenza di una convergenza tra la sicurezza fisica e la sicurezza cibernetica. Molto importante, dunque è l'«integrazione», cioè guardare a tutti gli aspetti (l'analisi del rischio, quindi, non è solo l'analisi del rischio cyber, ma è l'analisi del rischio cyber-fisico, guardo l'intera infrastruttura), ma anche a tutti gli altri aspetti della governance. Viene poi ricordato che i potenziali target di attacchi, se contaminati diventano a loro volta attaccanti. Bisogna per questi lavorare sull'anello debole della catena e soprattutto sull'elemento umano: è fondamentale rafforzare la consapevolezza. Per il futuro occorrerà lavorare su: - intelligenza artificiale (che può essere utilizzata anche in maniera malevola per attacchi di tipo informatico); - tecnologie quantistiche (gli attuali sistemi di crittografia saranno «bucati» attraverso i computer quantistici); - asset critici da proteggere (rete 5G). Viene sottolineato che molte PMI le quali non posseggono l'infrastruttura per potere gestire soluzioni di cyber security, oltre al ruolo fondamentale rivestito dalla ricerca e dell'innovazione. Il mercato della *cyber security* è in crescita (attualmente ammonta a 22 miliardi di dollari). Per l'Italia, l'idea dovrebbe essere quella di focalizzarsi su alcuni elementi distintivi, quali ad esempio: il rilevamento degli attacchi, l'analisi forense, lo sviluppo di « codice sicuro » (cioè di «software sicuro», utilizzando, anche in questo caso, l'intelligenza artificiale), la focalizzazione sul tema della disinformazione e misinformazione (utilizzare l'intelligenza artificiale quale supporto per discernere se un'informazione può essere vera o falsa), o ancora sul tema della threat	• Affrontare il tema della sicurezza con un approccio olistico; • Importanza di avere piani di gestione delle crisi a livello nazionale, nonché settoriale; • Importanza della consapevolezza e dell'educazione delle persone sul tema della sicurezza.

	intelligence (l'identificazione di minacce e di informazioni utili per potersi proteggere). Non bisogna sovrapporsi, come Italia, a quello che stanno facendo in altri Paesi. Considerazioni finali: - il tema è la sicurezza va affrontato da un punto di vista «olistico». Quello che apprendiamo dall'esperienza europea è che la cooperazione internazionale, gli standard globali e la condivisione di informazioni e anche di *intelligence* sono fondamentali; - sarebbe auspicabile avere piani di gestione delle crisi a livello nazionale, nonché a livello settoriale, anche se un attacco può coinvolgere più settori e sostituire o, se vogliamo, evolvere il tema della protezione nel tema della resilienza, quindi la capacità di assorbire il colpo. - la capacità di vagliare l'interno di *internet* e scovare tutte le informazioni è un elemento critico e in Italia ci sono decisamente competenze e *asset* per farlo; - un ruolo fondamentale è svolto dalla consapevolezza e dall'educazione educazione, sul tema della sicurezza, delle persone fin dalle giovani generazioni (bisognerebbe insegnare loro a usare ChatGPT e a capire quali sono le debolezze e le vulnerabilità).	
Audizione dei rappresentanti di Almaviva S.p.A., **Antonio Amati**, **Giovanni Giovannetti**, **Roberto Rossi**	Almaviva è una multinazionale italiana attiva in Europa, Medio Oriente, Stati Uniti e Brasile, con un fatturato di 1,2 miliardi di euro e 45.000 dipendenti. Opera principalmente in tre ambiti: *information technology*; intelligenza artificiale (attraverso Almawave che sviluppa soluzioni proprietarie); sicurezza e difesa (*partner* della Guardia di Finanza e della Guardia Costiera, per le quali ha sviluppato reti radar, sistemi di comando	• importanza di una collaborazione pubblico-privata e di un approccio proattivo per affrontare le sfide della sicurezza digitale;

n. 16 del 9/10/2024	e controllo (C4I), e tecnologie per il monitoraggio del traffico marittimo; nonché partner tecnologico per la digitalizzazione dei processi del Ministero, inclusa la gestione delle infrastrutture cibernetiche). Almaviva, nell'ambito delle piattaforme proprietarie, propone soluzioni per la compliance NIS2 e la rilevazione in tempo reale delle minacce; sistemi di ***info sharing*** che permettono la condivisione di informazioni sugli attacchi tra diverse organizzazioni, migliorando la prevenzione; servizi e sistemi di controllo del ciclo di vita delle identità digitali per evitare utilizzi impropri. Tra gli ambiti di ricerca, attualmente in corso, Almaviva sta sviluppando algoritmi di cifratura per il *quantum computing* e predisponendo laboratori dedicati all'intelligenza artificiale (AI) per rafforzare la sicurezza cibernetica. Tra gli aspetti problematici, si sono evidenziati i rischi della crescente digitalizzazione. Infatti, la pandemia ha accelerato la digitalizzazione, aumentando la vulnerabilità di settori critici come sanità, idrico e *smart working*. Peraltro, si è evidenziato l'importanza della ricerca costante. In particolare, mediante laboratori In cui si affrontano le minacce emergenti come gli attacchi "*zero-day*" e simulazioni di difesa dagli attacchi dell'AI. Categorizzano le anomalie riscontrate sui sistemi informatici in tre ambiti: quello dei dati, quello delle applicazioni e quello degli utenti, degli *humans*.	• Almaviva dispone di un SOC (*Security Operations Center*), situato a Roma e composto da persone italiane, attivo 24 ore su 24, che si occupa del monitoraggio e analisi; • partecipazione a progetti europei per migliorare la condivisione di informazioni e implementare standard avanzati.
Audizione del presidente dell'Associazione italiana professioni security	L'Associazione italiana professionisti security aziendale (AIPSA) rappresenta oltre 800 professionisti della sicurezza aziendale, attivi in più di 200 società italiane, comprese infrastrutture critiche, grandi gruppi industriali e medie imprese. Da oltre trent'anni, l'associazione promuove	• collaborazione pubblico-privato all'interno dei tavoli tecnici (composti esclusivamente da autorità istituzionali che

aziendale (AIPSA), **Alessandro Manfredini** n. 17 del 16/10/2024	una cultura della sicurezza integrata, orientata alla prevenzione e alla gestione delle minacce. Il Presidente Manfredini, nel corso dell'audizione, ha sottolineato come il panorama delle minacce sia in costante evoluzione, includendo: – minacce ibride, che combinano rischi fisici e cibernetici; – instabilità geopolitica, con conseguenze sui sistemi critici. – eventi climatici estremi e crisi sanitarie, che ampliano la vulnerabilità delle infrastrutture; – *cyber-crime* come servizio (*crime-as-a-service*), che sfrutta tecnologie emergenti quali l'intelligenza artificiale e il *quantum computing;* – la progressiva interdipendenza dei mercati e il carattere sempre più transfrontaliero dei servizi essenziali rendono le crisi, anche laddove principiate localmente, sempre più globali; e – l'integrazione dei sistemi dell'IoT (*internet of things*) e dell'IIoT (*industrial IoT*) a livello di città sempre più intelligenti, che espande la superficie del rischio, esponendo le infrastrutture critiche e i servizi essenziali e importanti a minacce ibride sempre più sofisticate. AIPSA ha accolto positivamente la normativa europea di recente emanazione (Direttive CER e NIS2, legge 90/2024), evidenziando tuttavia la necessità di includere una rappresentanza stabile di soggetti privati nei tavoli istituzionali per migliorare la gestione proattiva delle minacce. Infatti, ad avviso dell'Associazione, sono principalmente le imprese a rilevare, spesso per prime, le minacce emergenti, potendo contribuire con competenze specifiche e innovazioni tecnologiche.	avrebbero la facoltà di convocare, audire e coinvolgere i soggetti privati titolari della gestione di infrastrutture critiche o servizi essenziali importanti); • centralità della formazione e dell'aggiornamento professionale come "strumento" per la prevenzione e risoluzione dei rischi *cyber*.

	Il Presidente Manfredini, non ha mancato di sottolineare la centralità e il ruolo del *security manager* che meriterebbe un riconoscimento formale mediante una normativa dedicata. Si renderebbe necessario, infatti, assicurare che tale figura professionale possieda specifiche qualifiche, una formazione professionale *ad hoc* e competenze manageriali (*corporate security manager*). In sintesi, il *security manager* è una figura chiave per la resilienza aziendale, incaricato di proteggere persone, *asset* e dati aziendali. Nella prospettiva proposta da AIPSA, la formazione assume un carattere centrale per affrontare le sfide provenienti dalla *cybersecurity*. In questa prospettiva, infatti, appare fondamentale investire nella formazione continua attraverso corsi, esercitazioni e aggiornamenti costanti. Peraltro, AIPSA propone incentivi finanziari, sgravi fiscali e programmi di decontribuzione per promuovere la formazione e trattenere i giovani talenti in Italia, riducendo il rischio di "fuga di cervelli". Da ultimo, con riferimento al rilievo che assume la collaborazione pubblico-privato, il Presidente Manfredini ha ribadito che la condivisione di informazioni sugli incidenti, anonimizzate e protette, potrebbe rafforzare la resilienza complessiva del sistema, ove messa a sistema da privati e attori istituzionali. Tra gli esempi di successo di tale collaborazione, si è citato: – il dialogo avviato dall'Agenzia per la Cybersicurezza Nazionale e della Segreteria infrastrutture critiche, istituita presso l'Ufficio del consigliere militare della Presidenza del Consiglio dei ministri, per favorire una collaborazione tra autorità costituite e operatori (nonché la stessa AIPSA); nonché	

	– i tavoli tecnici realizzati in ambito di perimetro di sicurezza nazionale cibernetica e l'altro in esecuzione di *stress test* nel settore energetico per testare appunto il grado di resilienza delle infrastrutture critiche energetiche italiane.	
Audizione dei rappresentanti di Akamai Italia, **Nicola Ferioli, Alessandro Rivara** n. 18 del 17/10/2024	Akamai è un'azienda che nasce negli Stati Uniti, quotata sul *New York Stock Exchange* e nasce all'interno della principale Università di ingegneria informatica degli Stati Uniti, il MIT. Akamai garantisce a molte infrastrutture pubbliche nazionali una tecnologia in grado di rispondere, gestire e ridurre la superficie d'attacco minimizzando gli impatti. Frontiere da monitorare legate al rischio cibernetico: – settore degli attacchi applicativi rivolti alle API (*Application Programming Interface*), ovvero dei micro servizi che tutti i portali utilizzano per recuperare informazioni da terze parti (questo rappresenta circa il 50 per cento di tutto il traffico *internet* e gli attacchi su questa superficie si incrementano del 50 per cento di anno in anno); – settori delle istituzioni finanziarie e delle infrastrutture critiche (qui l'incremento è addirittura del 250 per cento anno su anno). Gli attacchi DDoS (*Distributed Denial of Service*) sono quelli che puntano a mettere fuori uso un'infrastruttura. Questi tipi di attacchi si sono semplificati per l'attaccante, grazie anche a sistemi di tipo *as-a-service*. È possibile acquistare degli attacchi da piattaforme che hanno come *business model* il lanciare attacchi verso infrastrutture terze, coprendo vari ambiti. Nell'ambito della difesa di infrastrutture è difficile fare pubblicamente dei riferimenti, perché chi acquista una soluzione di difesa molto spesso non vuole annunciare quali tecnologie utilizza per difendersi, in quanto si	• In relazione alla scala globale degli attacchi, serve una forma di reazione che sia coordinata a livello globale, e una particolare attenzione al controllo degli accessi e dei movimenti all'interno di un'infrastruttura informatica.

	tratta di un'informazione che può essere utilizzata anche a scopo di attacco o di identificazione. Ad ogni modo, è importante rimarcare la necessità di sovrapposizione tra l'ambiente strettamente legato alla difesa (che però risulta molto meno robusto e sicuro quando si passa a infrastrutture alle quali devono avere accesso persone terze) e molti dei problemi che si riscontrano in clienti commerciali di livello meno critico. Anche le istituzioni finanziarie hanno rilevanti interessi economici, ma non hanno lo stesso livello di criticità. In particolare, occorre pensare alla scala globale degli attacchi delle organizzazioni, e cioè al fatto che le tecnologie sono in qualche modo condivise a livello mondiale e le sorgenti di attacco possono essere distribuite a tale livello, per cui serve una forma di reazione che sia coordinata a livello globale, e una particolare attenzione al controllo degli accessi, che devono diventare sempre più sicuri e controllati, e dei movimenti all'interno di un'infrastruttura informatica.	
Audizione del professore ordinario di Automatica presso l'Università Campus Bio-Medico di Roma, **Roberto Setola** n. 19 del 23/10/2024	Gli attacchi cyber ai sistemi OT (Operational Technologies), ovvero a quei sistemi informatici che hanno la funzione di controllare dei processi fisici, chimici, biologici, possono avere esiti particolarmente gravi. La principale differenza fra un attacco *cyber* contro un normale sistema IT e contro un sistema OT risiede nel fatto che un'azione cyber contro un sistema OT può generare un evento cinetico, cioè può trasformare un attacco cyber in qualcosa che impatta direttamente sull'ambiente, sulla salute delle persone, come paralizzare un impianto, una fabbrica, i treni. Nell'audizione vengono portati diversi esempi. Occorre una capacità dello Stato di difendersi da questi attacchi, e dunque la Difesa deve costruire questa competenza, partendo dalla realizzazione di sistemi di *test range*, cioè di sistemi in cui è possibile analizzare tecnologie, comprendere le vulnerabilità, comprendere come queste	• Oltre alla cyber security IT, esiste cyber security OT (*operational technologies*), su cui vi è ancora poca consapevolezza e sono poche le figure professionali con le competenze adatte (che spaziano fra informatica, automatica e altre competenze). • Occorre aumentare la formazione e la capacità delle Forze armate di attrarre e formare quei talenti quei talenti

	tecnologie si interfacciano con l'architettura OT e, al di sotto, con il progetto sottostante. Per fare ciò la Difesa deve: – interfacciarsi con gli operatori delle infrastrutture critiche nazionali per definire assieme le strategie di difesa, favorendo la nascita all'interno di ognuna di queste infrastrutture critiche di una figura che abbia specifiche responsabilità e competenze nel campo della *security* a figure tipo il *security manager*. Attualmente le norme italiane, da questo punto di vista, non hanno una formulazione esatta. Abbiamo il responsabile della *safety*, adesso con la NIS2 della *cybersecurity*, ma non abbiamo, per legge, un responsabile della sicurezza *tout court;* – promuovere una collaborazione con il mondo della ricerca, che in un dominio così dinamico, come quello cyber, è fondamentale; – confronto e cooperazione con i nostri alleati, per dare ai nostri militari la possibilità di testare tecnologie diverse, operare in ambienti diversi; – fare formazione, richiedendo che tutti gli ufficiali superiori abbiano una formazione in ambito *cybersecurity* e formando degli specialisti. Qui, però, abbiamo un grosso problema: il mondo della *cyber security* soffre di un *gap skill* enorme. In questo scenario non è difficile immaginare che la capacità attrattiva del pubblico in generale e delle Forze armate in particolare non è così forte, sia per un problema economico (il mondo privato offre remunerazioni decisamente diverse), sia perché l'aspetto cyber è relegato nei ruoli tecnici, carriera che viene vista come subalterna ai ruoli regolari. Il suggerimento è provare a inserire la formazione cyber già a livello di accademia, quindi ai ruoli regolari.	che servono per gestire questo complesso scenario.

Audizione dei rappresentanti di IBM Italia, **Alessandro La Volpe**, **Federico Mattei** n. 20 del 6/11/2024	I rappresentati di IBM hanno, in primo luogo, evidenziato che tre forze principali influenzano la *cybersecurity*: scenari geopolitici, tecnologia (cloud, AI generativa, *quantum computing*), e le *cyber* minacce. L'IBM osserva globalmente gli attacchi informatici attraverso un'apposita struttura: il team X-Force, che analizza 150 miliardi di eventi giornalieri e produce *report* annuali sulle minacce. IBM investe principalmente in tecnologia in tre domini della sicurezza: la sicurezza dei dati, la sicurezza delle identità e la sicurezza in termini di gestione delle minacce (c.d. *threat management*). Quanto alle tecnologie e alle innovazioni, si è sottolineato che il *quantum computing* si presenta come una tecnologia *distruptive*, potendo infatti rivoluzionare vari settori. Allo stesso modo, essa pone alcuni rischi, principalmente, crittografici. Infatti, i computer quantistici saranno in grado di decriptare la crittografia attuale entro il 2030, rendendo urgenti le misure di sicurezza post-quantum. Le minacce includono il furto di dati oggi per decriptarli in futuro ("*harvest now, decrypt later*"). IBM ritiene, pertanto, necessario che le istituzioni, nell'ambito di strategie di transizione tecnologica, censiscano e mappino i propri sistemi crittografici, prioritizzando gli aggiornamenti. L'intelligenza artificiale è una risorsa per migliorare i sistemi di difesa dei sistemi informatici, ma anche un rischio per gli stessi in considerazione dei fini malevoli per i quali può essere utilizzata. Occorre, dunque, bilanciare *AI for Security* e *Security for AI*. Infatti, i principali rischi, in ambito di intelligenza artificiale, sono legati alla trasparenza nella *governance* dell'IA (e, dunque, anche evitare i possibili *bias*), alla potenziale violazione dei diritti proprietari di terzi sui dati immessi nell'IA (*intellectual property*); nonché la spiegabilità delle decisioni assunte e delle modalità di lavoro di un algoritmo di IA.	• formazione: IBM ha inaugurato una "Cyber Academy" (con patrocinio dell'ACN) a Roma per simulare attacchi e formare aziende e istituzioni. Un approccio pratico per affrontare la sicurezza a livello di governance e operatività. • sinergia tra pubblico e privato, formazione e innovazione è cruciale per affrontare le sfide della sicurezza informatica.

	Da ultimo, si è sottolineato l'urgenza di rafforzare le competenze tecniche e adottare metodologie di sicurezza innovative. L'Italia può assumere un ruolo guida in Europa nel campo del *quantum safe*, ma deve agire rapidamente per evitare *gap* competitivi assicurandosi, in sostanza, che le tecnologie *hardware* e *software* siano *compliant,* rispondenti cioè a logiche di *quantum safe* e dunque pronte per poter adottare i nuovi algoritmi di crittografia in fase di sviluppo.	
Audizione dei rappresentanti di NTT DATA Italia S.p.A., **Ludovico Diaz, Dolman Aradori** n. 21 del 13/11/2024	NTT DATA è parte del gruppo giapponese NTT, uno dei maggiori operatori di telecomunicazioni al mondo, con una forte presenza globale e un *focus* sull'innovazione tecnologica. In Italia, l'azienda conta oltre 6.000 dipendenti e un fatturato di circa 600 milioni di euro. L'Italia è un centro chiave per la ricerca e sviluppo, con contributi significativi in settori come il 5G, l'IoT e l'intelligenza artificiale. La *cybersecurity* è uno dei pilastri strategici per NTT DATA. L'azienda ha sviluppato una rete globale di Security Operations Center (SOC), con uno specifico in Italia, operativo dal 2016, integrato in una rete globale di 14 centri capaci di monitorare e gestire minacce in tempo reale, sfruttando informazioni provenienti dal 40% del traffico internet mondiale. Il SOC italiano offre servizi di sicurezza gestita, analisi delle minacce e supporto alle crisi, con un'attenzione particolare alla gestione degli attacchi *ransomware*. La società prevede investimenti in *data center* di nuova generazione in Italia, progettati per gestire in modo sicuro i dati sensibili e ottimizzare la sostenibilità energetica. L'azienda collabora con leader globali (e.g., Microsoft) per affrontare minacce avanzate (e.g., il *malware* TrickBot), utilizzando capacità analitiche e di *intelligence*. Si è evidenziato come le piccole e medie imprese (PMI) italiane siano particolarmente vulnerabili agli attacchi *cyber* a causa della limitata	• formazione come punto fondamentale nello sviluppo di una coscienza verso i temi della *cybersecurity* (anche attraverso la collaborazione con le università). Creazione di una *Cyber Security Academy*, a livello italiano e mondiale, per rendere i professionisti di NTT consapevoli dell'importanza della *cybersecurity*; • iniziative di formazione, inclusi programmi per scuole primarie e secondarie, per sensibilizzare sui rischi informatici (185 classi tra scuole primarie e secondarie, 460 ore di lezione erogate, 25 città); • collaborazione con enti, amministrazioni e altri attori del modo *cyber* al fine di incrementare gli sviluppi dei

	consapevolezza e delle risorse insufficienti, sottolineandosi che la *cybersecurity* debba essere vista come un investimento strategico, necessario per proteggere i dati aziendali, sempre più considerati il vero valore di un'organizzazione. Con particolare riferimento ai rischi attuali per la *cybersecurity*, infatti, NTT ha rilevato che: (i) i *ransomware* rappresentano una sfida globale, con impatti significativi sulla continuità operativa delle aziende; (ii) la crescente digitalizzazione e l'interconnessione espongono le infrastrutture critiche a rischi maggiori, incluse intrusioni nei sistemi IT e OT (tecnologie operative); la carenza di professionisti qualificati in *cybersecurity* è un problema rilevante sia a livello nazionale che globale. In definitiva, con riferimento alle proposte che possono evincersi, NTT ha sottolineato l'importanza: (i) della predisposizione di piani specifichi per le PMI che le permettano di accedere a soluzioni di sicurezza avanzate senza dover investire direttamente in costose infrastrutture; (ii) di promuove 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*"; (iii) della collaborazione pubblico-privata e l'importanza di *framework* condivisi per affrontare le minacce, citando la partecipazione di NTT DATA nella Cyber Threat Alliance e nei progetti di sicurezza globale (e.g., GCAP).	sistemi mediante *sharing* di dati ed esperienze; • rilevanza della quantità di dati raccolti e processati.
Audizione dei rappresentanti di Meridian Group, **Alessandro Moretti**, **Andrea Purificato**, **Aldo Carabellese**,	Meridian Group è una piccola azienda italiana specializzata in ***cyber intelligence*** e *cybersecurity*, che sviluppa interamente tecnologie e soluzioni proprie. L'azienda sottolinea l'importanza della difesa cibernetica come elemento cruciale per la sicurezza nazionale, paragonandola ad altre infrastrutture critiche come energia e trasporti.	• importanza di programmi di formazione professionale e di campagne educative per accrescere la consapevolezza sulla sicurezza informatica, sia nel settore pubblico che privato;

n. 22 del 19/11/2024	L'Italia, pur rappresentando solo lo 0,7% della popolazione mondiale e il 2% del PIL, subisce il 10% degli attacchi cibernetici globali. Questo dato sottolinea l'urgenza di rafforzare il perimetro di difesa nazionale. Le PMI e le pubbliche amministrazioni spesso non dispongono di strumenti adeguati per garantire la sicurezza informatica. Meridian propone un sostegno economico e normativo per migliorare l'accesso a soluzioni avanzate. Secondo Meridian, in aggiunta, si rendono necessari protocolli chiari per rispondere agli incidenti di sicurezza, così come l'importanza di evitare conflitti normativi che possono complicare le azioni difensive. È stata proposta l'introduzione di programmi nazionali di ***bug bounty***, permettendo a esperti esterni di identificare vulnerabilità in infrastrutture pubbliche e private senza incorrere in rischi legali. Andrea Purificato, in particolare, ha suggerito un approccio interdisciplinare alla formazione, proponendo di definire meglio i potenziali profili di formazione per il personale dedicato a intervenire negli ambiti della *cyber security*, coinvolgendo tutti gli aspetti giuridici. Ritiene utile, infatti, lo sviluppo di piattaforme per la partecipazione attiva di soggetti privati, istituzioni pubbliche, professionisti per poter arricchire ambiti non strettamente affini alla normale operatività del professionista o del soggetto che partecipa, quindi creando un ambiente – su scala nazionale – dedicato al rafforzamento della sicurezza informatica, in cui poter scambiare informazioni che possano circolare liberamente e far sì che sia possibile adottare le migliori pratiche, tenendo conto di tanti aspetti, perché spesso il professionista conosce bene l'ambito tecnico di propria competenza, ma non conosce il contesto in cui quella competenza deve essere applicata**.** In definitiva, è stata enfatizzata la necessità di un approccio sistemico alla *cybersecurity*, incentrato su prevenzione, formazione e innovazione	• impegno di Meridian nell'erogazione, anche a titolo gratuita, di corsi di formazione in contesti universitari (e.g., EDHEC *Business School*); • suggeriti incentivi fiscali e finanziamenti per promuovere corsi di formazione e programmi educativi.

	tecnologica, con particolare attenzione alla collaborazione tra pubblico e privato.	
Audizione del Vicepresident Head of Business della divisione Mobile eXperience Samsung Electronics Italia S.p.A., **Nicolò Bellorini** n. 23 del 21/11/2024	Samsung ha evidenziato come il controllo totale della *supply chain* sia un elemento chiave per garantire la sicurezza informatica. Samsung, infatti, gestisce internamente l'intera *supply chain*, dalla produzione dei semiconduttori all'assemblaggio dei dispositivi. Questo garantisce un controllo rigoroso per evitare vulnerabilità informatiche nei prodotti distribuiti a livello globale e in Italia. La piattaforma Knox (certificata in Italia secondo protocolli dell'ACN), integrata nei dispositivi Samsung, è stata descritta come un pilastro fondamentale della strategia di sicurezza. In primo luogo, essa assicura la protezione *hardware* e *software* garantendo aree di memoria cifrate e sicurezza dall'*hardware* fino alle applicazioni. In secondo luogo, con riferimento alla gestione dei dispositivi, essa consente alle organizzazioni di avere controllo e sovranità sui dati condivisi attraverso un'interfaccia utente semplice e trasparente. Samsung ha collaborato con governi e istituzioni per personalizzare i dispositivi secondo esigenze specifiche. In particolare, ha realizzato: *device* tattici per l'Esercito statunitense; *tablet rugged* per le forze dell'ordine italiane, progettati per resistere a condizioni estreme; nonché soluzioni per il trasferimento sicuro di dati nelle auto dei Carabinieri e della Polizia. Si è evidenziato l'importanza di considerare il "costo totale di proprietà" (*total cost of ownership*) dei dispositivi, anziché il semplice prezzo di acquisto, sottolineando i rischi di approvvigionamento da fornitori non affidabili. Samsung ha suggerito: (i) di identificare criteri di approvvigionamento che privilegino sicurezza e affidabilità; (ii) stabilire criteri oggettivi di certificazione delle tecnologie di *cyber*-sicurezza; (iii) predisporre soluzioni	• realizzazione di piattaforme secondo l'approccio "*secured by design*"; • necessità di educare cittadini e amministrazioni a gestire dispositivi e dati in modo sicuro.

	post-installazione per rafforzare la sicurezza delle infrastrutture esistenti, particolarmente nei piccoli comuni e nelle aree sensibili. In definitiva, si è ribadita la necessità di investire continuamente in tecnologie innovative per affrontare le evoluzioni delle minacce informatiche.	
Audizione dell'Amministratore delegato di Elettronica S.p.A., **Domitilla Benigni** n. 24 del 28/11/2024	Domitilla Benigni, Amministratore Delegato di Elettronica S.p.A., nel corso dell'audizione ha ricordato che: – le minacce *cyber* sono sempre più pervasive, colpendo infrastrutture critiche come reti satellitari e cavi sottomarini. Queste infrastrutture trasportano dati strategici, rendendole obiettivi primari per attacchi e sabotaggi (con effetti che si riverberano globalmente); nonché – i nuovi modelli di *business* criminale, come il *crime-as-a-service*, consentono attacchi a basso costo ma con impatti devastanti. Il che, invece, contrasta con i vincoli (economici e legislativi) che gravano su "chi si difende". Nel corso dell'audizione si è posta particolare attenzione al fatto che le piccole e medie imprese, fondamentali per la filiera produttiva (*supply chain*), sono spesso le più esposte. La direttiva NIS2 ha introdotto requisiti per migliorare la resilienza *cyber*, ma molte PMI necessitano di supporto per adeguarsi. Domitilla Benigni, peraltro, ha sottolineato l'urgenza di ridurre la dipendenza da tecnologie non europee, sviluppando capacità autonome per la sicurezza nazionale ed europea. Proposte per il sistema Paese:	• formazione: il settore della *cybersecurity* soffre di una grave carenza di competenze, risulterebbe dunque necessario investire in programmi formativi e attrarre nuovi talenti; • università italiane, leggermente indietro nell'intercettare l'evoluzione del settore e le esigenze formative richieste dal mercato del lavoro; • importanza di creare una rete di supporto per le PMI non autonomamente in grado di difendersi dagli attacchi *cyber*.

	– essenzialità di approccio sistemico, con il coinvolgimento di istituzioni, aziende e società civile; – ridurre l'affidamento su tecnologie e servizi informatici *extra*-UE; e – incrementare il novero delle competenze professionali in ambito *cyber*. Da ultimo, si è evidenziata l'importanza di aumentare la rappresentanza femminile nell'ambito della *cybersecurity*. Ad avviso dell'audita, infatti, le donne potrebbero avere un impatto molto significativo nel settore, grazie alle loro competenze tecniche e *soft skill*.	
Audizione del Rettore dell'Università LUISS Guido Carli - Libera Università Internazionale degli Studi Sociali, **Paolo Boccardelli**, del Prorettore per l'intelligenza artificiale e le Digital Skills nonché Professore Ordinario di Computer Science presso il Dipartimento di Impresa e Management della LUISS **Giuseppe Francesco Italiano**, e del Professore associato, titolare della cattedra	Il Professor Paolo Boccardelli, Rettore dell'Università LUISS, ha evidenziato la necessità di porre particolare attenzione a quattro aspetti: • tecnologie della difesa applicata al dominio cibernetico; • tema della formazione del personale di eccellenza nel campo della difesa cibernetica; • diffusione della cultura *cyber* in generale e, in particolare, nelle nuove generazioni; • profili di rilievo internazionale connessi in particolare agli accordi in ambito NATO. Con riferimento al primo aspetto, ha sottolineato l'emergere di nuove tecnologie quantistiche. In particolare, si impone l'importanza di sviluppare la **crittografia post-quantistica** per proteggere i dati da futuri attacchi di computer quantistici, capaci di superare gli attuali sistemi crittografici. Ha inoltre evidenziato la necessità di proteggere	• formazione di personale di eccellenza nel campo della *cybersecurity* sia una priorità strategica per il Paese. Logica di *partnership* pubblico-privato nella formazione di figure apicali; • necessità di trattenere i talenti in Italia mediante una nuova politica contrattuale e salariale;

Vodafone in Cybersecurity and Digital Transformation presso il Dipartimento di Impresa e Management della LUISS **Paolo Spagnoletti** n. 25 del 3/12/2024	infrastrutture fisiche critiche, come cavi sottomarini e satelliti, utilizzando tecnologie IoT (*Internet of Things*) e UAV (*Unmanned Aerial Vehicle*) per monitoraggio e protezione. Un elemento chiave è rappresentato dalla **Zero Trust Architecture (ZTA),** un modello che richiede verifiche costanti delle identità e dei permessi di accesso, riducendo i rischi di compromissione. Infatti, Le ZTA (*Zero Trust Architecture*) offrono una protezione robusta e granulare rispetto ai modelli di sicurezza tradizionale, perché implementano una serie di controlli rigorosi, tra cui l'autenticazione multi-fattore, l'autorizzazione basata sui ruoli e la micro-segmentazione della rete. Ogni connessione, sia essa tra dispositivi, applicazioni o utenti, è soggetta a verifica e autorizzazione in tempo reale che minimizza l'impatto di una potenziale violazione, perché, nel caso, più che compromettere un intero sistema, compromette un segmento locale. Con riferimento al secondo aspetto, quello della formazione, il Rettore Boccardelli ha rimarcato come la formazione di personale di eccellenza nel campo della *cybersecurity* sia una priorità strategica per il Paese. Ha, peraltro, sottolineato l'importanza di integrare competenze tecniche avanzate con capacità giuridiche e una visione strategica delle dinamiche cibernetiche. In particolare, ha proposto – oltre alla preparazione tradizionale in aula – l'uso di **cyber range** (ambienti virtuali progettati per simulare scenari complessi di attacco e difesa) e simulatori avanzati per formare operatori in scenari realistici di attacco e difesa, migliorando la capacità di risposta a minacce sofisticate. Ha sottolineato che la formazione in *cybersecurity* deve essere inclusiva, coinvolgendo sia grandi organizzazioni che PMI, e deve promuovere una preparazione interdisciplinare per affrontare le complessità tecnologiche, organizzative e normative. In particolare, ha proposto un'iniziativa di partenariato	

	pubblico-privato, quindi istituzioni, università, imprese, partecipate dallo Stato ma non solo, per costruire dei progetti di formazione avanzata – anche mediante un programma di dottorato industriale – per formare delle figure apicali nella gestione del tema *cybercrime*. Quanto al terzo aspetto, si è evidenziata la necessità di diffondere la consapevolezza della sicurezza cibernetica tra i giovani, integrando questa tematica nei programmi scolastici fin dalla scuola primaria. Si sono suggeriti metodi educativi immersivi e ludici, come ad esempio le competizioni di "**capture the flag"**, per rendere la *cybersecurity* accessibile e coinvolgente. Inoltre, ha sottolineato l'importanza di promuovere opportunità professionali nel settore per attirare i giovani verso carriere cibernetiche. Su quest'ultimo aspetto, peraltro, il Prof. Italiano ha sottolineato come molti studenti formatisi in campo *cyber* abbiano lasciato l'Italia per l'estero, con stipendi e traiettorie professionali evidentemente più competitivi rispetto a quelli italiani. In aggiunta, ha fatto presente come, tra gli studenti rimasti italiani, solo pochissimi lavorino nella pubblica amministrazione, concludendo con la considerazione della necessità di un maggior sforzo – anche di natura saliare – per incentivare e trattenere i talenti in Italia. In merito alla formazione, il Prof. Spagnoletti ha rilevato come le competenze specifiche del mondo della difesa siano necessari per lo sviluppo della resilienza *cyber* in ambito civile. Infatti, ha evidenziato come le competenze della difesa possano essere trasferite alla società civile per aumentare la consapevolezza dei rischi e migliorare i comportamenti tecnologici. Peraltro, ha proposto di considerare la *cybersecurity* non come un ostacolo, ma come un'opportunità educativa e di crescita, da integrare nelle scuole e nei percorsi formativi	

	Da ultimo, con riferimento al quarto aspetto, il Rettore Boccardelli ha posto l'accento sulla collaborazione tra istituzioni nazionali e internazionali, citando il ***Cooperative Cyber Defence Centre of Excellence di Tallinn*** come esempio di partenariato efficace. Ha proposto un modello analogo per il dominio *cyber*, che coinvolga attori militari, civili e accademici, al fine di costruire una sicurezza più resiliente e inclusiva.	
Audizione dei rappresentanti di Poste Italiane, **Nicola Sotira**, Responsabile CERT in ambito Tutela Aziendale di Poste italiane S.p.A. n. 26 del 4/12/2024	Poste Italiane adotta un approccio integrato alla *cybersecurity*, con una *governance* strutturata in diverse unità, il cui centro è rappresentato dal CERT (Computer Emergency Response Team), il quale gestisce le operazioni di risposta agli incidenti, i *penetration test*, le valutazioni delle vulnerabilità e il monitoraggio continuo 24/7 del perimetro cibernetico. Poste Italiane gestisce milioni di eventi giornalieri, grazie a sistemi di automazione e *machine learning*, riducendo significativamente i tempi di risposta e migliorando la resilienza della struttura aziendale. Nel 2023 sono stati gestiti circa 1,3 milioni di tentativi di attacco, molti dei quali bloccati prima di causare danni. L'azienda, tramite il CERT, adotta un approccio di condivisione delle informazioni, scambiandole con le Forze dell'ordine, altri istituti finanziari, e con l'Agenzia per la Cybersicurezza Nazionale (ACN). Poste Italiane dedica grande attenzione alla *brand protection* e alla lotta alle frodi, ad esempio:	• formazione pratica ai rischi della *cyber* mediante esercitazioni sottoposte ai propri dipendenti; • campagne di sensibilizzazione in favore della cittadinanza in relazione ai rischi *cyber* connessi ai servizi offerti dall'azienda; • collaborazione con altre istituzioni (*e.g.*, ACN).

	– sono state rimosse 319 *app* fraudolente dai *marketplace*, che imitavano quelle ufficiali dell'azienda; – implementazione di esercitazioni trimestrali al fine di formare i dipendenti a reagire alle campagne di *phishing* (con una riduzione degli incidenti del 38% dal 2017); e – utilizzo di sistemi di intelligenza artificiale per monitorare il comportamento delle transazioni finanziarie degli utenti al fine di riscontrare eventuali frodi da essi subiti a seguito di attacco *cyber*. Per aumentare la consapevolezza delle problematiche legate al dominio *cyber*, Poste Italiane S.p.A. ha avviato programmi di sensibilizzazione per dipendenti e clienti. In particolare, sono state poste in essere: simulazioni di incidenti per testare le capacità di risposta dei dipendenti (anche al fine di riscontrare l'applicazione delle *policy* interne); campagne educative in favore della cittadinanza e degli utenti dei servizi offerti, tramite il sito aziendale, collaborazioni con università, scuole e associazioni dei consumatori, nonché attraverso strumenti di comunicazione (*e.g.*, TGPoste). Peraltro, Poste Italiane S.p.A. ha adottato sistemi avanzati di automazione per gestire un volume crescente di eventi. L'intelligenza artificiale viene utilizzata per prioritizzare le vulnerabilità e fornire una visione in tempo reale della postura di sicurezza tramite dashboard accessibili ai vertici aziendali.	
Audizione del Presidente di RFI Rete Ferroviaria italiana S.p.A., **Dario Lo Bosco**, e del	Dario Lo Bosco, Presidente di RFI, ha sottolineato l'importanza della rete ferroviaria per la sicurezza nazionale, considerandola un'infrastruttura critica. Ha evidenziato il rischio crescente di attacchi cibernetici che	• RFI ha manifestato l'intenzione di divenire un *driver* per la formazione, l'alta formazione e la valorizzazione dei talenti.

Responsabile della Cyber Security di RFI Rete Ferroviaria italiana S.p.A **Riccardo Barrile**. n. 27 del 11/12/2024	potrebbero compromettere la circolazione di persone e merci, incluse quelle di tipo classificato. Tra gli approcci innovativi di RFI alla tematica della *cyber*-sicurezza, nel corso dell'audizione, è emerso l'inserimento della componente *cyber* nel recente Modello 231 di RFI. Il Modello, peraltro, si caratterizza per una *advisory* esterna, per la presenza di presìdi di controllo per la prevenzione dei rischi di commissione dei cosiddetti «reati presupposto», ma anche per valorizzare i piani anticorruzione. Peraltro, il Presidente Lo Bosco ha sottolineato il valore della sinergia tra ricerca scientifica e applicazioni pratiche, favorendo lo sviluppo di brevetti e soluzioni tecnologiche innovative. Nel corso dell'audizione, Riccardo Barrile, Responsabile della Cyber Security di RFI, ha spiegato che l'unità di Cyber Security di RFI si occupa sia della protezione dei sistemi IT sia di quelli OT (*Operational Technology*), fondamentali per il controllo e il segnalamento ferroviario. Un malfunzionamento in queste aree, infatti, potrebbe avere conseguenze critiche. Ha chiarito, inoltre, che RFI applica il principio della security by design, integrando la sicurezza già nella fase di progettazione degli impianti e promuovendo questa filosofia anche tra i partner industriali. L'organizzazione aziendale, nelle sue strutture dedicate alla sicurezza cibernetica, include un SOC (*Security Operations Center*) e un CSIRT (*Computer Security Incident Response Team*), che operano 24/7 per monitorare, rilevare e rispondere agli incidenti. Infine, l'approccio di RFI combina infrastrutture on-premise con soluzioni multi-cloud per garantire la sicurezza e la resilienza dei dati.	Infatti, ha attivato, con alcune università italiane, dei programmi di master in *cyber security;* • approccio alla difesa cibernetica secondo una logica di *security by design*. Peraltro, RFI opera anche nel senso della sensibilizzazione dei propri *partner* più importanti nel tentativo di cambiare il paradigma nell'approccio a questa tematica, propriamente secondo le logiche di *security by design*.

	Da ultimo, come sottolineato dal Presidente Lo Bosco, l'azienda collabora con *partner* come Leonardo e con atenei internazionali, tra cui l'Università di Salonicco, per sviluppare nuove soluzioni di protezione rispetto alle minacce cibernetiche.	
Audizione del Ministro della Difesa, **Guido Crosetto** n.28 del 15/01/2025	Il Ministro della Difesa ha anzitutto sottolineato come il cyberspazio sia ormai un dominio strategico al pari di quelli terrestre, marittimo, aereo e spaziale, come riconosciuto anche dalla NATO. L'accelerazione dello sviluppo tecnologico, in particolare di intelligenza artificiale e tecnologie quantistiche, sta ridefinendo le modalità con cui si manifestano, in modo trasversale e dirompente, le minacce nel dominio cyber. In questo quadro, l'IA facilita la diffusione di contenuti manipolati, rendendo difficile distinguere tra informazioni autentiche e artefatte. La crescente digitalizzazione espone lo Stato a continui attacchi cibernetici, spesso condotti da attori statali e non statali, colpendo infrastrutture critiche, enti governativi e il settore privato. La sicurezza informatica deve diventare parte di una cultura condivisa anche con le aziende e cittadini, investendo sulla formazione. In questa prospettiva sottolinea l'importanza della costante e proficua cooperazione degli attori istituzionali con il mondo accademico e con gli esperti del settore cyber, cooperazione tuttavia molto complessa da assicurare in ragione delle rigide regole che governano il funzionamento del pubblico impiego. Ad ogni modo evidenzia come il dominio cyber rappresenta un campo di battaglia permanente; in questo contesto fa presente come i *cyber command* in seno alle forze armate straniere rappresentano punti di riferimento nazionale per la protezione delle infrastrutture critiche e il contrasto dell'attività di manipolazione cognitiva, svolgendo un ruolo di primaria	• Promuovere una cultura della sicurezza informatica, condivisa con aziende e cittadini, investendo sulla formazione e collaborando con il mondo accademico; • rafforzare la deterrenza contro le minacce cyber rendendo la risposta più rapida ed efficace → l'attuale governance è troppo frammentata e inefficace: la Difesa deve essere messa nelle condizioni di poter operare in maniera persistente nell'intero spazio cibernetico, analogamente agli altri domini; • necessità di avviare un percorso normativo volto a: - abilitare la Difesa all'identificazione, mitigazione e contrasto delle minacce *cyber*, dirette e indirette, alla sicurezza nazionale;

	responsabilità nella protezione del cyber spazio nazionale, analogamente a quanto accade nei domini fisici. Si impone quindi l'urgente necessità di rafforzare la deterrenza contro le minacce cyber, intesa come la capacità di agire rapidamente ed efficacemente in caso di attacco contro il Paese o i suoi alleati. Per migliorare la sicurezza nel dominio cibernetico, il Ministero della Difesa promuove: • condivisione strutturata delle informazioni sulle minacce; • definizione di procedure comuni tra attori istituzionali per prevenire e contrastare incidenti cyber; • piani di resilienza per le infrastrutture critiche nazionali; • formazione e ricerca per consolidare le capacità operative; • cooperazione internazionale, con programmi di "cyber capacity building". Il Ministro ha poi ripercorso le principali normative adottate in Italia negli ultimi anni per rafforzare la sicurezza cibernetica: I. **D.L. n. 82/2021**: istituisce l'Agenzia per la Cybersicurezza Nazionale e il Comitato interministeriale per la cybersecurty, ripartendo competenze in materia cyber in 4 pilastri: 1. la resilienza cibernetica all'Agenzia per la cybersecurity nazionale; 2. la prevenzione e il contrasto cyber al Ministero degli interni; 3. la difesa e la sicurezza militare al Ministero della difesa;	- legittimare le forze armate all'utilizzo di strumenti cibernetici; - allineare il ruolo del Ministero della Difesa a quello del comparto *intelligence*; - svolgere attività di *intelligence* preparatorie; - estendere le garanzie funzionali, di cui all'articolo 17 della legge 3 agosto 2007, n. 124, al personale delle forze armate impiegato nella conduzione di operazioni militari nel dominio cibernetico; - assicurare la compartecipazione alla Strategia nazionale per l'intelligenza artificiale per gli aspetti relativi ai sistemi impiegabili in chiave duale; • quattro priorità essenziali: 1) identificare lo spazio *cyber* di interesse nazionale per la difesa e la sicurezza dello Stato, così da consentire alla Difesa di poter operare senza soluzione di continuità;

	4. la ricerca e l'elaborazione informativa al comparto informazioni e sicurezza. II. **D.L. n. 115/2022**: misure di intelligence per contrastare minacce cibernetiche. III. **Legge n. 90/2024**: rafforzamento delle sanzioni contro i crimini informatici. IV. **Direttiva NIS2**: implementazione di un approccio europeo alla cybersecurity. Pur prendendo atto con favore degli interventi normativi adottati volti a rafforzare la sicurezza cibernetica, l'audito ha evidenziato come l'attuale governance, immaginata molto prima degli sviluppi *cyber*, sia ancora troppo frammentata e inefficace, con la Difesa incaricata solo della protezione delle proprie reti e non dell'intero cyberspazio nazionale. Tale architettura vede infatti al momento il pilastro della difesa cibernetica rivolto sostanzialmente alla protezione delle sole reti militari: la difesa è dunque il pilastro incaricato della difesa cibernetica, ma di fatto solo di se stessa, in evidente difformità da quanto avviene in tutti gli altri quattro domini, in cui la difesa è naturalmente assicurata all'intero territorio nazionale. Sottolinea come, invece, in linea con un approccio maggiormente flessibile, inclusivo e innovativo, eventualmente anche attraverso il coinvolgimento delle risorse private, i quattro pilastri dovrebbero essere in grado di coordinarsi e consultarsi efficacemente così da addivenire in modo rapido e tempestivo ad un'ipotesi strutturata di azione. A questo proposito, ribadisce con forza la necessità di mettere la difesa nelle condizioni di poter operare in maniera persistente nell'intero spazio cibernetico di interesse nazionale.	2) disporre di un'arma *cyber* civile e militare; 3) realizzare un centro per il contrasto alla guerra ibrida; 4) condividere le *best practices* per lo scambio informativo e il contrasto alla propaganda.

	Il rafforzamento della deterrenza in ambito cibernetico si fonda su 4 fattori: 1. *due diligence*, obbligo dello Stato di prevenire attacchi dal proprio cyberspazio; 2. *denial*, sviluppo di misure per contrastare attacchi cibernetici; 3. *attribution*, capacità tecnica di identificare gli autori degli attacchi; 4. *punishment*, applicazione di misure concrete contro i responsabili degli attacchi. Il Ministro ha quindi auspicato che all'esito dell'indagine possa avviarsi un percorso normativo al fine di : • abilitare le azioni e le capacità della difesa all'identificazione, mitigazione e contrasto delle minacce *cyber*, dirette e indirette, alla sicurezza nazionale; • legittimare le forze armate all'utilizzo di strumenti cibernetici, sia nelle ipotesi di risposta alle crisi, di cui la *leadership* della gestione e il suo coordinamento sono in capo alla difesa, sia nelle operazioni promosse in concorso con le autorità civili; • allineare il ruolo del Ministero della difesa a quello del comparto *intelligence* nel caso di adozione e attuazione delle misure di *intelligence* di contrasto in ambito cibernetico in situazioni di crisi e di emergenza; • svolgere attività di *intelligence* preparatorie nell'imminenza di un attacco *cyber*, a prescindere dall'esistenza di una situazione di crisi e di emergenza e della possibilità di fronteggiare tale crisi con azioni di resilienza;	

- estendere le garanzie funzionali, di cui all'articolo 17 della legge 3 agosto 2007, n. 124, al personale delle forze armate impiegato nella conduzione di operazioni militari nel dominio cibernetico, in territorio nazionale e all'estero, anche quando non opera congiuntamente con il personale addetto ai servizi di informazione e sicurezza;
- compartecipare alla predisposizione della Strategia nazionale per l'intelligenza artificiale per gli aspetti relativi ai sistemi impiegabili in chiave duale (disegno di legge di iniziativa governativa in termini di intelligenza artificiale, collegato alla Nota di aggiornamento del Documento di economia e finanza 2023, attualmente all'esame delle Commissioni parlamentari competenti presso il Senato della Repubblica).

Allo stesso modo, infine, il Ministro ha ritenuto essenziali quattro priorità di fondo:

1) identificare lo spazio *cyber* di interesse nazionale per la difesa e la sicurezza dello Stato, un campo di operazioni all'interno del quale il Ministero della difesa operi senza soluzione di continuità per adempiere ai propri compiti istituzionali;
2) disporre di un'arma *cyber* civile e militare numericamente adeguata a livello di minaccia osservata, che sia operativa e continuamente capace di intervenire, arma *cyber* che abbia tutte le adeguate tutele funzionali per il personale incaricato;
3) realizzare un centro per il contrasto alla guerra ibrida, che esprima la capacità di comando e controllo, condiviso con le agenzie e con gli attori non militari;

	4) condivisione delle *best practices* per lo scambio informativo e il contrasto alla propaganda che sviluppi sinergie tra istituzioni e mondo accademico per creare gli anticorpi di base contro i fenomeni di propaganda e disinformazione.	