Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Gestionale
A.a. 2025/2026
Sessione di Laurea novembre/dicembre 2025

Cybersecurity: gestione del rischio aziendale e il ruolo dell'intelligenza artificiale nell'era digitale

Relatrice:
Prof.ssa Laura Abrardi

Candidato:
Federico Arduini

Indice

1. Introduzione

In un'epoca segnata da una trasformazione digitale pervasiva, la cybersecurity rappresenta ormai uno dei pilastri fondamentali su cui poggia la tenuta economica, sociale e istituzionale delle moderne società. La rapida evoluzione tecnologica, l'espansione esponenziale delle reti di comunicazione, la moltiplicazione dei dispositivi connessi e l'aumento costante dei dati scambiati e conservati generano quotidianamente nuove opportunità di sviluppo, innovazione e crescita competitiva. Tuttavia, queste stesse dinamiche aprono scenari di rischio sempre più complessi, nei quali minacce informatiche di natura eterogenea possono compromettere la riservatezza, l'integrità e la disponibilità di asset critici per organizzazioni pubbliche e private, cittadini e intere infrastrutture strategiche. La consapevolezza dell'importanza di proteggere lo spazio cibernetico non è mai stata così diffusa, né così imprescindibile per garantire la resilienza di sistemi economici globalizzati e interconnessi. La crescente frequenza di attacchi informatici di vasta portata ha dimostrato come la cybersicurezza non possa più essere considerata una mera questione tecnica, confinata nei dipartimenti IT, ma richieda una governance integrata, politiche pubbliche coerenti e una cultura diffusa della gestione del rischio. In questo contesto, la presente tesi si propone di offrire una trattazione organica e multidisciplinare del fenomeno, partendo dai fondamenti teorici fino ad arrivare alle declinazioni più attuali delle strategie di difesa. Nella prima parte viene fornita una panoramica concettuale dei principi fondamentali della cybersecurity, evidenziandone gli obiettivi cardine e ripercorrendo le tappe evolutive che, dal secondo dopoguerra all'odierna società dell'informazione, hanno contribuito a trasformare il cybercrime in una minaccia globale. Particolare attenzione è dedicata all'analisi delle principali tipologie di attacco informatico, delle tecniche più diffuse e delle statistiche relative all'andamento dei crimini digitali, con un focus specifico sul contesto italiano, ancora troppo spesso trascurato in letteratura. Un capitolo centrale è riservato all'analisi dell'ecosistema normativo che disciplina la cybersicurezza a livello europeo e nazionale. Le recenti iniziative legislative, come la Direttiva NIS2, il Cyber Resilience Act, la revisione del Cybersecurity Act e il Cyber Solidarity Act, delineano un quadro di regole sempre più stringente per le organizzazioni considerate essenziali o di interesse vitale. Tali strumenti non solo fissano standard minimi di sicurezza, ma promuovono la cooperazione transfrontaliera, la condivisione delle informazioni e la costruzione di capacità comuni per fronteggiare incidenti su larga scala. A livello italiano, il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) e l'implementazione del Perimetro di Sicurezza Nazionale Cibernetica evidenziano come la dimensione strategica della difesa informatica sia diventata un tema di interesse prioritario per la sicurezza nazionale. Successivamente, la tesi approfondisce le logiche del cyber risk management, delineandone i modelli teorici e i processi pratici, con riferimento alle metodologie di Enterprise

Risk Management (ERM) e all'approccio circolare PDCA (Plan-Do-Check-Act). Viene analizzata l'importanza di sviluppare capability interne, di istituire procedure di monitoraggio proattivo e di definire piani di risposta e recovery capaci di limitare l'impatto economico, reputazionale e operativo degli incidenti informatici. L'analisi si estende poi alle problematiche legate alla supply chain e alla gestione dei rischi connessi ai fornitori terzi, oggi considerati uno dei principali vettori di compromissione. Un'attenzione particolare è rivolta all'economia della cybersecurity e alle scelte di investimento in sicurezza informatica, tema di crescente interesse anche in ambito accademico. Gli studi economici hanno infatti messo in luce come la razionalità delle decisioni di spesa in cybersecurity non sia scontata: l'esistenza di fenomeni di interdipendenza, esternalità di spillover tecnico o di mercato e le dinamiche di free riding richiedono politiche pubbliche di incentivo e interventi correttivi per garantire un livello di protezione adeguato dal punto di vista collettivo. L'inquadramento teorico di questi modelli, dai pionieristici contributi di Gordon e Loeb fino alle più recenti applicazioni di teoria dei giochi, fornisce un quadro di riferimento per comprendere come la cooperazione e la standardizzazione possano ridurre inefficienze e vulnerabilità sistemiche. Per evidenziare come tali modelli si traducano in pratica, la tesi propone un caso di studio: l'attacco ransomware al Colonial Pipeline. Analizzando le dinamiche dell'incidente, i costi economici diretti e indiretti, la gestione operativa e le implicazioni strategiche, si mostra come vulnerabilità apparentemente marginali possano avere ripercussioni a livello nazionale ed evidenziano l'importanza di investimenti continui in prevenzione, detection e resilienza. Infine, uno sguardo è dedicato alle nuove frontiere tecnologiche e alle prospettive future della difesa informatica. L'intelligenza artificiale, in particolare, si configura come un pilastro fondamentale per l'evoluzione dei sistemi di cybersecurity. Le tecniche di machine learning, l'analisi comportamentale e le architetture di difesa adattive consentono di passare da un approccio puramente reattivo a un paradigma predittivo e proattivo. Tuttavia, questa evoluzione porta con sé nuove sfide, legate ai costi di implementazione, al deficit di competenze, ai rischi di attacchi avversari e alle delicate questioni etiche e normative. La cybersecurity, dunque, non è più un ambito ristretto alla dimensione tecnica, ma si afferma come fattore critico di competitività, resilienza e fiducia collettiva. La presente ricerca si propone di mettere in evidenza come strategie integrate, investimenti mirati, governance consapevole e una cultura diffusa della sicurezza siano condizioni imprescindibili per affrontare un futuro sempre più interconnesso, complesso e vulnerabile. Solo attraverso un approccio multidimensionale sarà possibile conciliare innovazione e protezione, progresso tecnologico e responsabilità, sicurezza individuale e stabilità sistemica.

2. Fondamenti di Cybersecurity

2.1 Concetti di base: definizioni, obiettivi e principi fondamentali della cybersecurity

Negli ultimi anni, il concetto di cybersecurity ha acquisito crescente rilevanza nei dibattiti accademici, politici e industriali, senza che si sia consolidata una definizione univoca in grado di rappresentarne pienamente la complessità. La difficoltà di definizione è dovuta alla natura intrinsecamente trasversale della materia, che coinvolge aspetti tecnologici, sociali, economici e normativi. Frederick Chang [1], ex direttore della ricerca della National Security Agency statunitense, sottolinea la natura interdisciplinare della cybersecurity, affermando:

"Una scienza della cybersecurity offre molte opportunità di progresso grazie a un approccio multidisciplinare, perché, in fondo, la cybersecurity è fondamentalmente un continuo scontro tra attacco e difesa. Gli esseri umani devono difendere macchine che vengono attaccate da altri esseri umani attraverso le macchine. Pertanto, oltre ai campi tradizionali e fondamentali come l'informatica, l'ingegneria elettronica e la matematica, sono necessarie prospettive provenienti da altre discipline."

L'analisi della letteratura passata evidenzia come le varie definizioni di cybersecurity risultino fortemente influenzate dal contesto disciplinare in cui sono elaborate. Spesso si tratta di interpretazioni soggettive e non sempre esaustive dal punto di vista operativo. Il concetto di cybersecurity, infatti, è stato affrontato da una vasta gamma di ambiti accademici: oltre ai settori più tradizionali come l'ingegneria, la tecnologia, l'informatica, la sicurezza e la difesa, vi è un crescente interesse anche da parte delle scienze politiche, della psicologia, dell'educazione, della sociologia e del diritto. Come osserva Cavelty [2], il campo della cybersicurezza è attraversato da molteplici discorsi interconnessi e comprendere il significato del termine implica la necessità di scomporlo nei suoi due elementi costitutivi: cyber e security. Il prefisso cyber si riferisce a concetti come il cyberspazio e la realtà virtuale, in particolare alle reti di comunicazione elettronica. Il termine deriva da cybernetics, coniato da Wiener [3] nel 1948 per indicare la teoria del controllo e della comunicazione, sia nei sistemi meccanici sia negli esseri viventi. Per quanto riguarda il termine security, la letteratura mostra una persistente difficoltà nel giungere a una definizione universalmente condivisa. Secondo Buzan, Wæver e Wilde [4], parlare di sicurezza significa analizzare chi produce sicurezza (securitizing actor), rispetto a quali minacce, per chi (referent object), con quali scopi, conseguenze e in quale struttura. Sebbene esistano definizioni più concrete, legate a proprietà fisiche, sistemi informatici o modelli matematici, la sicurezza resta un concetto contestato, il cui significato dipende dal punto di vista e dai valori dell'osservatore. Nonostante ciò,

l'idea centrale di security rimane quella di uno stato privo di pericoli o minacce. Di seguito sono riportate le definizioni principali che possono fornire un quadro generale delle diverse prospettive:

1. *"La cybersecurity consiste principalmente in metodi difensivi utilizzati per rilevare e contrastare potenziali intrusi" [5].*
2. *"La cybersecurity implica la protezione delle reti informatiche e delle informazioni in esse contenute da accessi non autorizzati, danni o interruzioni" [6].*
3. *"La cybersecurity riguarda la riduzione del rischio di attacchi dannosi a software, computer e reti, comprendendo strumenti per il rilevamento di intrusioni, il blocco di accessi malevoli, la cifratura e l'autenticazione" [7].*
4. *"La cybersecurity è l'insieme di strumenti, politiche, concetti, salvaguardie, linee guida, approcci alla gestione del rischio, buone pratiche e tecnologie impiegati per proteggere l'ambiente cibernetico e le risorse di utenti e organizzazioni" [8].*
5. *"Capacità di proteggere o difendere l'uso del cyberspazio da attacchi informatici" [9].*
6. *"Insieme di tecnologie, processi e misure di risposta progettati per proteggere reti, dati e sistemi da accessi non autorizzati, danni o attacchi, garantendone riservatezza, integrità e disponibilità" [10].*
7. *"L'arte di garantire l'esistenza e la continuità della società dell'informazione, proteggendo nel cyberspazio i suoi dati, beni e infrastrutture critiche" [11].*
8. *"Lo stato di protezione contro l'uso criminale o non autorizzato dei dati elettronici o le misure adottate per raggiungerlo" [12].*
9. *"Attività, capacità o condizione attraverso cui i sistemi di informazione e comunicazione vengono protetti da danni, manipolazioni o utilizzi non autorizzati" [13].*

Sebbene alcune di queste definizioni riconoscano esplicitamente il ruolo delle interazioni umane e delle dinamiche non tecniche, emerge con chiarezza il predominio di un approccio tecnico. Come osserva Cavelty [14], le definizioni tendono ad adattarsi ai contesti e alle condizioni in cui i principali attori definiscono soggettivamente cosa sia una minaccia alla sicurezza e come vi si debba rispondere. Ciò significa che, pur essendo utili nel proprio ambito, tali definizioni non sempre riescono a restituire una visione complessiva e interdisciplinare del fenomeno. Nonostante l'ampia varietà di definizioni presenti nella letteratura, è stato adottato un approccio pragmatico di tipo qualitativo, che combina elementi di analisi oggettiva con componenti soggettive, come indicato da Cooper [15]. Questo metodo ha reso possibile l'elaborazione di una definizione teorica

capace di bilanciare aspetti concreti e misurabili, come i sistemi di rilevamento delle intrusioni, con dimensioni più interpretative, legate ad esempio alle intenzioni degli attaccanti.
Da tale impostazione emerge una definizione operativa di cybersecurity intesa come:

"L'organizzazione e l'insieme di risorse, processi e strutture finalizzati alla protezione del cyberspazio e dei sistemi digitali connessi da eventi che generano disallineamento tra i diritti di proprietà formali (de Jure) e quelli effettivi (de facto)."

Questa formulazione mira a sintetizzare in modo inclusivo le principali dimensioni concettuali emerse dalla letteratura che di seguito viene scomposta nei suoi elementi essenziali:

- *"L'organizzazione e l'insieme di risorse, processi e strutture":* questa espressione mette in evidenza la complessità intrinseca della cybersecurity, che implica interazioni tra soggetti umani, tra sistemi tecnologici, e tra esseri umani e sistemi digitali. L'assenza di una specificazione puntuale su quali siano tali risorse o strutture rende la definizione intenzionalmente aperta e flessibile, in grado di adattarsi al carattere dinamico e in continua evoluzione del dominio cibernetico.
- *"Finalizzati alla protezione del cyberspazio e dei sistemi digitali connessi"*: si fa riferimento a una concezione ampia di cyberspazio, che comprende non solo le reti e gli ambienti digitali tradizionali, ma anche sistemi ibridi come le infrastrutture di controllo industriale e i sistemi cibernetico-fisici (cyber-physical systems). La nozione di protezione è intesa in senso esteso, includendo minacce intenzionali, eventi accidentali dovuti ad errori umani e persino rischi derivanti da fenomeni naturali.
- *"Da eventi che generano disallineamento tra i diritti di proprietà de Jure e de facto":* questo passaggio si fonda sul quadro teorico dei diritti di proprietà elaborato da Ostrom e Hess [16] nel 2007, che distingue tra i de Jure, diritti legalmente riconosciuti, e de facto, diritti effettivamente esercitati. Nel contesto della cybersicurezza, ogni evento, sia esso volontario o involontario, che altera questo equilibrio costituisce un incidente rilevante. Le dimensioni implicate possono riguardare l'accesso, l'uso, la gestione, l'esclusione o l'alienazione di dati, risorse digitali e infrastrutture.

La definizione proposta di cybersecurity mira a superare l'approccio tecnico tradizionale, offrendo una visione interdisciplinare, inclusiva e coerente con l'evoluzione digitale. Questa prospettiva favorisce un dialogo integrato tra discipline, fondamentale per affrontare in modo efficace le sfide cibernetiche contemporanee. Nel contesto della protezione dei dati e dei sistemi, i concetti di Information Security e Cybersecurity sono spesso utilizzati in modo intercambiabile, ma presentano

differenze sostanziali sia in termini di ambito applicativo che di obiettivi. La sicurezza delle informazioni (Information Security) si focalizza sulla protezione delle informazioni in tutte le loro forme, digitali, cartacee, audiovisive o verbali, con l'obiettivo di garantire tre principi fondamentali: riservatezza, integrità e disponibilità. Questo significa, ad esempio, prevenire accessi non autorizzati, modifiche arbitrarie, perdite o distruzioni, attraverso misure tecniche e organizzative come controlli logici e fisici, protocolli di accesso e sistemi di backup. La cybersecurity, invece, rappresenta un sottoinsieme più specifico, orientato alla protezione delle informazioni e dei sistemi nel solo ambiente digitale, ovvero il cyberspazio. Si tratta quindi di prevenire e contrastare attacchi informatici, violazioni di sicurezza, incidenti digitali e minacce che possono compromettere dati, servizi e infrastrutture connesse a Internet [17]. Un aspetto distintivo della cybersecurity è il suo legame con la dimensione cibernetica delle tecnologie dell'informazione e della comunicazione (ICT): essa include la protezione di strumenti, applicazioni, reti, infrastrutture critiche e sistemi cloud da accessi non autorizzati, perdita di dati e interruzioni dei servizi. Come definito dall'International Telecommunication Union (ITU), la cybersecurity comprende un insieme articolato di strumenti, politiche, metodologie, pratiche e tecnologie mirate a tutelare l'ambiente cibernetico e le risorse digitali di utenti e organizzazioni [8]. Un ulteriore elemento di distinzione riguarda l'ambito delle minacce: mentre la sicurezza delle informazioni affronta ogni tipo di rischio che possa compromettere i dati, indipendentemente dalla sua natura fisica o digitale, la cybersecurity si occupa esclusivamente delle minacce che si originano o si manifestano nel cyberspazio, come attacchi malware, phishing, furti di credenziali, sabotaggi digitali e violazioni sistemiche. Entrambi i concetti condividono la finalità di proteggere l'informazione, ma differiscono per scopo, contesto e strumenti applicati. L'information security si propone di ridurre il rischio operativo, ottimizzare le attività aziendali e garantire continuità e conformità normativa. La cybersecurity, invece, si concentra su minacce mirate a sistemi interconnessi, con un'attenzione crescente alle vulnerabilità di rete, ai dispositivi e ai comportamenti digitali. La cybersecurity e la sicurezza delle informazioni sono discipline complementari: la prima agisce in ambito digitale, proteggendo gli ecosistemi connessi; la seconda fornisce un quadro più ampio, volto a salvaguardare l'informazione in qualsiasi forma e contesto. Una comprensione chiara di entrambi i concetti è essenziale per sviluppare strategie di protezione efficaci e integrate in un panorama digitale sempre più complesso e interconnesso. Una rappresentazione grafica della loro relazione è riportata nella Figura 1.

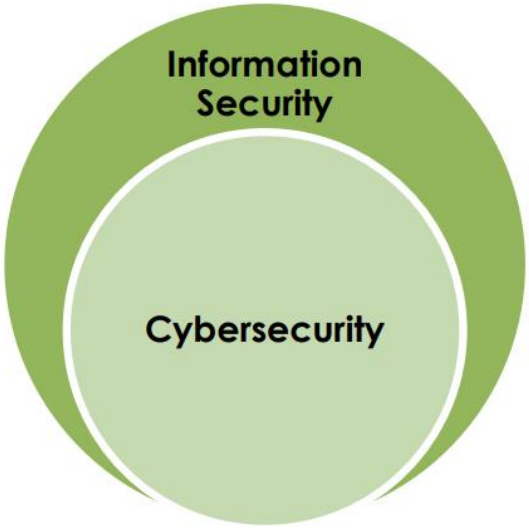

Figura 1 - Relazione tra Information Security e Cybersecurity

2.2 Storia

Il progresso tecnologico ha segnato profondamente lo sviluppo della società contemporanea, trasformando il modo in cui comunichiamo, lavoriamo, gestiamo l'informazione e affrontiamo le sfide globali. In questo contesto in continua evoluzione, la cybersecurity ha assunto un ruolo sempre più centrale, diventando un elemento imprescindibile per garantire l'affidabilità e la resilienza dei sistemi digitali. Pur trattandosi di una disciplina relativamente recente, emersa nella seconda metà del XX secolo, la cybersecurity ha conosciuto un'evoluzione rapida e complessa, rispondendo a minacce in costante mutamento e adattandosi alle trasformazioni del cyberspazio. Negli anni '60, la cybersecurity iniziò a emergere con lo sviluppo delle prime reti informatiche. Fino a quel momento, i computer erano dispositivi isolati e l'unico modo per comprometterli era ottenere accesso fisico alla macchina. Tuttavia, con la creazione di Arpanet da parte dell'Advanced Research Project Agency (ARPA) del Pentagono, i computer iniziarono a connettersi tra loro, ponendo le basi per Internet. Nel 1969, Arpanet trasmise il primo messaggio host-to-host tra Stanford Research Institute (SRI), dedicato all' "Augmentazione dell'Intelletto Umano" e il laboratorio di Kleinrock a UCLA e tra due computer situati uno in University of California, Santa Barbara (UCSB), e uno presso la University of Utah. segnando la nascita del cyberspazio. Alla fine del 1969, quattro computer host erano interconnessi nella prima versione dell'Arpanet, e l'embrione di Internet era ormai nato [18]. Questo nuovo ambiente digitale creava nuove possibilità, ma anche nuove vulnerabilità, rendendo necessario lo sviluppo delle prime misure di sicurezza informatica. Nel decennio successivo, con la

diffusione delle reti informatiche, emersero le prime minacce alla sicurezza dei sistemi. Il primo worm, malware in grado di autoreplicarsi, della storia vide la luce nel 1971 presso BBN Technologies, una compagnia situata a Cambridge, che giocò un ruolo cruciale nello sviluppo delle reti informatiche, in particolare Arpanet. Bob Thomas, uno degli ingegneri della società, volle dimostrare la possibilità di creare un programma capace di spostarsi autonomamente tra i computer connessi. Il programma Creeper non era pensato per causare danni. Non cancellava dati né prendeva il controllo del sistema: si limitava a replicarsi, a passare da un computer all'altro e a restituire come output un messaggio che recitava: «I'M THE CREEPER. CATCH ME IF YOU CAN!» [19]. Questo messaggio, che invitava simpaticamente a “prendere” Creeper, era tutto ciò che l'utente vedeva sul proprio terminale prima che il worm si trasferisse su un altro sistema. Anche se Creeper non era dannoso, dimostrò che i sistemi informatici potevano essere compromessi. In risposta, Ray Samuel Tomlinson sviluppò nel 1972 Reaper [19], il primo software di sicurezza in grado di individuare ed eliminare il malware dai sistemi infettati da quest’ultimo, segnando l’inizio della lotta tra virus e programmi di protezione, una dinamica che continua ancora oggi. Parallelamente, emersero attacchi informatici basati sul social engineering. Nel 1979, un liceale statunitense di nome Kevin Mitnick, un giovane hacker, riuscì ad hackerare The Ark accedendo illegalmente ai sistemi di Digital Equipment Corporation (DEC) semplicemente ingannando un dipendente al telefono per ottenere le credenziali di accesso. Questo episodio dimostrò che non solo la tecnologia, ma anche il fattore umano, rappresentava un punto debole nella sicurezza informatica. Utilizzando una tecnica che oggi chiamiamo “social engineering” [20], il giovane Mitnick chiamò un funzionario della DEC e si spacciò per uno degli sviluppatori principali, dicendo di essere stato estromesso da uno dei suoi account. Riuscì a convincere la persona contattata a dargli le credenziali di accesso e quindi fu in grado di accedere senza autorizzazione a grandi quantità di dati aziendali. Un altro grande passo avanti nell’ambito della sicurezza è stato fatto con lo sviluppo del Data Encryption Standard (DES) [21]. All’inizio degli anni ’70, il governo degli Stati Uniti stava cominciando a capire che era necessario proteggere i dati che venivano archiviati e inviati tramite reti. Per questo alcuni ricercatori di IBM, con la collaborazione della NASA, crearono il DES. Nel 1977 questo standard fu ufficialmente pubblicato con il nome di Federal Information Processing Standard, e se ne incoraggiò l’adozione su larga scala. Il DES non era un protocollo di crittografia particolarmente valido, ma abbastanza funzionale da essere adottato dall’NSA e da tutta la community dedicata alla sicurezza informatica. È rimasto uno dei protocolli più usati fino al 2001, quando venne soppiantato. Negli anni ’80, con la diffusione dei computer e delle reti, gli attacchi informatici divennero più frequenti e complessi. I criminali informatici iniziarono a prendere di mira istituzioni finanziarie, aziende e governi, portando alla necessità di sviluppare soluzioni di sicurezza più

avanzate. Gli attacchi iniziarono ad attirare l'attenzione del pubblico, anche grazie al cinema. Il film "WarGames – Giochi di guerra" (1983) mostrò al mondo il rischio di accessi non autorizzati ai sistemi governativi, contribuendo a diffondere la consapevolezza sulla cybersecurity. Il primo virus venne scritto un decennio dopo, nel 1982, e attaccava l'Apple II. Si chiamava Elk Cloner [22] e il suo autore, Richard "Rich" Skrenta, aveva 15 anni. L'Elk Cloner infettava il settore di boot dei dischi dell'Apple Dos e veniva caricato all'avvio del computer. Il suo scopo era creare confusione: uno scherzo vandalico di un ragazzino molto intelligente, che utilizzava i floppy disk come metodo per spargersi e contagiare altri computer, dato che praticamente non esistevano le reti per gli home computer come l'attuale internet, e l'unica altra alternativa possibile sarebbero state le Bbs (Bulletin Board System), che oltre alla messaggistica favorivano la condivisione di file. Un malware che attirò l'attenzione fu il virus Vienna [23], un programma in grado di autoreplicarsi che poteva corrompere i file di un dispositivo infetto. A quel tempo erano in circolazione molte minacce simili, ma Vienna si guadagnò un posto nella storia non tanto per quello che riuscì a fare, ma per come fu fermato. A metà anni '80, l'esperto di sicurezza informatica tedesco Bernd Fix si rese conto che il suo dispositivo era stato infettato dal virus Vienna. Sviluppò quindi un antivirus in grado di individuare e rimuovere Vienna. Questo fu uno dei primi esempi di antivirus moderno, per come lo conosciamo oggi. Di conseguenza, il mercato della sicurezza informatica iniziò a svilupparsi rapidamente: nel corso degli anni Ottanta, con la proliferazione dei floppy disk, si ebbe una notevole diffusione dei virus, essendo lo scambio di floppy una pratica assai comune in ogni ambito della società. Bastavano pochi floppy infetti per far partire un attacco su vasta scala. Nel 1988 nacquero i primi antivirus commerciali, tra cui McAfee VirusScan, che portarono la cybersecurity nel settore aziendale e privato. Le aziende iniziarono a investire in software di protezione e misure di sicurezza più sofisticate, dando il via all'industria della cybersecurity per come la conosciamo oggi. Negli anni '90 con la diffusione di internet, i virus e i cosiddetti malware iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni. Con Windows 95 venne lanciato Internet Explorer, che per anni rimase il browser più popolare. La crescente accessibilità dei computer e il loro costo sempre più contenuto permisero a milioni di persone di connettersi a Internet, inviare e-mail e giocare online. Tuttavia, con la diffusione della rete emersero anche nuove minacce. L'e-mail divenne uno strumento fondamentale per la comunicazione, ma anche un vettore per attacchi informatici. Un esempio eclatante fu il virus Melissa del 1999 [24]. Il malware veniva inviato tramite e-mail in messaggi che avevano come oggetto "Messaggio importante". In allegato si trovava il file "list.doc", che conteneva appunto il virus Melissa. Non appena il file veniva aperto, il malware si installava sul dispositivo e cominciava a creare problemi. Prima di tutto, provocava l'apertura di diversi siti pornografici e mentre gli utenti

cercavano di chiuderli, il malware disattivava i sistemi di sicurezza di Outlook. In un secondo momento, con Outlook ormai vulnerabile, il virus generava nuovi messaggi e-mail con lo stesso oggetto e lo stesso allegato, e li inviava a 50 persone della lista contatti della vittima. Melissa si diffuse così molto rapidamente e si stima che i danni provocati ammontassero a circa 80 milioni di dollari. Questo incidente dimostrò due cose. Primo, la nuova rete globale permetteva al malware di diffondersi a velocità impensabili prima di allora; secondo, i protocolli di sicurezza erano ancora tremendamente inadeguati, soprattutto se si considera la loro inefficacia contro il social engineering. Un buon software di sicurezza non può nulla contro la curiosità umana che porta ad aprire i "messaggi importanti". Negli anni 2000, il cyberspazio si evolse ulteriormente. Gli hacker svilupparono nuove strategie per diffondere malware, come l'inganno tramite e-mail di phishing che spingevano gli utenti a visitare siti dannosi. In risposta all'aumento delle minacce, il Department of Homeland Security degli Stati Uniti creò una sezione dedicata alla sicurezza informatica, la National Cyber Security Division. Per la prima volta, il governo americano e il resto del mondo avevano riconosciuto ufficialmente che la sicurezza informatica era un importante problema globale. Difendere il cyberspazio dai criminali era diventata una questione di sicurezza personale e nazionale. Parallelamente, le aziende iniziarono a sviluppare strumenti di sicurezza più avanzati, tra cui le VPN e i primi software basati su cloud, che permisero una protezione più efficace senza impattare sulle risorse dei dispositivi. Durante il 2010, la cybersecurity divenne un campo di battaglia per governi e aziende. Il malware Stuxnet, utilizzato contro il programma nucleare iraniano, segnò l'inizio della guerra cibernetica su scala internazionale. Alcuni computer utilizzati dall'Iran per lo sviluppo del loro programma nucleare vennero infettati da malware, provocando così dei disservizi su tutte le loro reti. Questo incidente diede inizio a un nuovo periodo di spionaggio e conflitti internazionali e divenne chiaro che gli attacchi informatici potevano essere usati come armi per colpire obiettivi governativi. Nel frattempo, il dibattito sulla privacy online si intensificò a causa della raccolta massiccia di dati da parte di aziende come Google e Facebook. I furti di dati divennero sempre più frequenti, con casi clamorosi come il furto di informazioni di Yahoo nel 2013, che coinvolse tre miliardi di utenti [25]. Con l'arrivo del 2020, nuovi scenari hanno caratterizzato la cybersecurity, in particolare la pandemia da Covid-19 ha accelerato l'adozione del lavoro da remoto, aumentando le vulnerabilità informatiche. Il passaggio al lavoro da remoto ha obbligato milioni di persone a collegarsi alle reti e ai database aziendali direttamente da casa propria, spesso utilizzando dispositivi personali. Questa è stata un'ottima opportunità per gli hacker, che potevano attaccare computer personali e smartphone con più facilità, in quanto generalmente privi di soluzioni di sicurezza avanzate. Secondo il Sophos Group [26], un'azienda di sicurezza software britannica, solo nel 2020 più della metà delle aziende è stata colpita da attacchi

ransomware. Gli attacchi ransomware si sono moltiplicati e i tentativi di phishing legati alla pandemia hanno ingannato milioni di persone. Inoltre, attacchi alle infrastrutture critiche, come quello alla Colonial Pipeline nel 2021, hanno dimostrato l'impatto devastante della criminalità informatica sull'economia e sulla sicurezza nazionale. Il Covid ci ha ricordato che, 40 anni dopo la truffa di Kevin Mitnick ai danni dei sistemi di The Ark, il social engineering è ancora un metodo molto efficace per bypassare i protocolli di sicurezza. Nel 2022, la guerra tra Russia e Ucraina ha segnato un ulteriore passo nella guerra cibernetica, con attacchi informatici che hanno preceduto e accompagnato il conflitto armato. Per contrastare queste minacce, l'Unione Europea ha istituito il Cyber Rapid Response Team [27], dimostrando come la cybersecurity sia ormai una componente fondamentale della difesa nazionale e internazionale. In particolare, la missione delle Cyber Rapid Response Teams (CRRT) è supportare gli Stati Membri (MS) del progetto e le altre parti coinvolte nel rispondere agli incidenti informatici e garantire un più alto livello di resilienza cibernetica. Questi eventi hanno decisamente confermato la possibilità che la guerra cibernetica possa avere un ruolo fondamentale nei prossimi conflitti. Negli ultimi decenni, la cybersecurity è passata dall'essere una questione marginale a diventare una delle sfide più importanti della nostra epoca, con implicazioni che coinvolgono governi, aziende e cittadini di tutto il mondo. L'evoluzione delle minacce informatiche ha dimostrato che non si tratta più solo di proteggere dati personali o aziendali, ma di garantire la sicurezza nazionale e la stabilità economica globale. Gli attacchi informatici non sono più confinati a singoli hacker o piccoli gruppi criminali, ma vengono ormai utilizzati come strumenti di guerra geopolitica e spionaggio dagli stati più potenti al mondo.

2.3 Cybercrime: principali minacce e attacchi informatici

Il cybercrime, o crimine informatico, rappresenta oggi una delle forme di criminalità più pervasive, insidiose e in costante evoluzione. Esso si configura come l'insieme delle condotte illecite realizzate attraverso l'utilizzo improprio di tecnologie informatiche, sia hardware che software, con l'obiettivo di commettere uno o più reati [28]. Si tratta di un fenomeno complesso, che comprende una vasta gamma di comportamenti criminosi: dall'accesso abusivo a sistemi informatici alla sottrazione, manipolazione o cancellazione di dati sensibili, fino ad attività ancora più sofisticate come la distribuzione di malware e l'estorsione digitale mediante ransomware. Un aspetto distintivo del crimine informatico risiede proprio nella sua capacità di adattarsi rapidamente al progresso tecnologico e la costante trasformazione delle tecnologie digitali apre infatti nuove possibilità di attacco, rendendo obsolete molte contromisure in tempi relativamente brevi. Ciò che un tempo poteva apparire come un fenomeno criminale di nicchia si è progressivamente evoluto in una minaccia globale, con conseguenze di rilievo non solo economico, ma anche sociale e geopolitico.

Le vittime del cybercrime sono molteplici e possono includere singoli individui, istituzioni pubbliche e imprese private. Se per i privati cittadini le conseguenze si manifestano spesso sotto forma di frodi o furti di identità, per le organizzazioni gli effetti possono rivelarsi ancora più devastanti. In particolare, le imprese, indipendentemente dalle loro dimensioni, si trovano esposte a minacce che compromettono l'integrità finanziaria, la continuità operativa e la reputazione aziendale. La crescente digitalizzazione dei processi produttivi e dei servizi ha infatti reso le aziende vulnerabili a un'ampia gamma di attacchi. Tra le principali minacce figurano il phishing, il ransomware e altre forme di social engineering, che colpiscono non solo le grandi realtà, ma anche le piccole e medie imprese (PMI), spesso meno attrezzate in termini di risorse tecnologiche e cultura della cybersicurezza [29]. Le violazioni dei dati aziendali, come il furto di informazioni finanziarie o personali, costituiscono un ulteriore fattore di rischio, esponendo le imprese a pesanti danni reputazionali e a sanzioni derivanti dalla mancata conformità alla normativa vigente in materia di protezione dei dati personali, come il GDPR. L'evoluzione del cybercrime è tale che la gamma degli attacchi informatici è estremamente ampia e mutevole: già nella Raccomandazione del 13 settembre 1989 successivamente integrata dal XV Congresso dell'Associazione Internazionale di Diritto Penale nel 1994 [30] il Consiglio dell'Unione Europea evidenziava l'esigenza di definire e classificare in maniera puntuale le diverse fattispecie di reati informatici, individuandone inizialmente quattordici tipologie. Tali condotte possono essere ricondotte a due macrocategorie principali: da un lato, l'abuso della tecnologia informatica; dall'altro, l'abuso dei contenuti informativi.

2.3.1. Abuso della tecnologia informatica

Questa prima categoria comprende tutti quei comportamenti illeciti che sfruttano in modo diretto strumenti e infrastrutture informatiche con l'obiettivo di arrecare un danno o trarre un indebito profitto. Si tratta di attacchi di natura prevalentemente tecnica, spesso resi possibili da vulnerabilità nei sistemi o da configurazioni inadeguate. Tra gli esempi più rilevanti si possono individuare le seguenti sottocategorie:

- Attacchi basati su malware: rientrano in questa tipologia tutte le minacce informatiche che utilizzano software malevoli come virus, worm, trojan horse, ransomware, spyware o rootkit, con finalità diversificate che spaziano dal sabotaggio dei sistemi informatici all'estorsione economica, fino al furto o alla compromissione di dati riservati. L'impatto di questi attacchi può variare notevolmente in base al livello di sofisticazione del malware e alla capacità delle difese implementate dall'organizzazione bersaglio.

- Attacchi alle applicazioni web: in un contesto di crescente dipendenza da piattaforme online, le applicazioni web rappresentano uno dei bersagli più comuni. Tecniche come la SQL Injection, il Cross-Site Scripting (XSS), il Cross-Site Request Forgery (CSRF) o la file inclusion mirano a compromettere l'integrità dei dati, ad accedere in modo illecito a sistemi o a manipolare informazioni sensibili. Tali vulnerabilità sono spesso il risultato di errori di programmazione o di controlli di sicurezza insufficienti.

- Attacchi alla rete e ai protocolli:una forma di abuso che riguarda l'intercettazione o l'interruzione del traffico di rete. Tecniche come gli attacchi Distributed Denial of Service (DDoS), l'ARP spoofing, il DNS poisoning o il TCP/IP hijacking possono compromettere la disponibilità dei servizi, alterare le comunicazioni o deviare i dati verso canali controllati dall'attaccante. La finalità di questi attacchi può spaziare dall'intercettazione di informazioni riservate al blocco delle attività di intere organizzazioni.

2.3.1.1 Attacchi basati su malware

Il termine malware, abbreviazione di malicious software, identifica qualsiasi programma informatico progettato con intenti malevoli, al fine di compromettere l'integrità, la riservatezza o la disponibilità di un sistema, senza il consenso o la consapevolezza dell'utente. I malware possono infettare computer, dispositivi mobili, server o reti, e operano attraverso una vasta gamma di tecniche per spiare, danneggiare o manipolare il sistema bersaglio. Essi rappresentano una delle minacce più diffuse e persistenti nel panorama della cybersicurezza, contribuendo significativamente al numero complessivo di incidenti informatici rilevati a livello globale [30]. Gli attacchi basati su malware non sono finalizzati esclusivamente alla distruzione dei sistemi, ma mirano spesso a obiettivi economici, strategici o politici. I criminali informatici, infatti, utilizzano questi strumenti per sottrarre dati sensibili, come credenziali di accesso, informazioni bancarie o documenti riservati, al fine di rivenderli nel dark web oppure sfruttarli per attività di estorsione, ricatto o profilazione indebita degli utenti [31]. In altri casi, il malware può essere impiegato come strumento di cyber espionage, al servizio di governi o organizzazioni che intendono raccogliere informazioni da entità pubbliche, aziende o individui specifici. [32] Il malware si diffonde attraverso numerosi vettori, spesso basati sull'ingegneria sociale. Tra i metodi più comuni rientrano l'invio di e-mail di phishing contenenti link o allegati infetti, il download da siti web compromessi (drive-by download), l'uso di dispositivi USB contaminati, lo sfruttamento di vulnerabilità nei sistemi operativi o nei software non aggiornati e l'installazione di applicazioni malevole da store

non ufficiali. In alcuni casi, persino software apparentemente legittimi distribuiti attraverso canali ufficiali possono contenere codice dannoso**.** Una volta infettato un sistema, il malware può operare in modi differenti, a seconda della tipologia. Esistono infatti numerose varianti di malware, ciascuna con caratteristiche specifiche:

- I *virus informatici* sono una forma di malware progettata per infettare file e programmi, replicandosi e diffondendosi all'interno del sistema. Si attivano quando l'utente esegue un file infetto, eseguendo azioni dannose come la cancellazione o modifica di dati, la disattivazione dell'antivirus o l'installazione di altri malware. Tra le varianti principali si trovano i *boot sector virus*, che colpiscono il settore di avvio del disco, i *macro-virus*, che infettano documenti con macro come Word o Excel, e i *file infector virus*, che si legano ai file eseguibili. I virus sono stati tra i primi malware sviluppati, tanto che i software di sicurezza sono tuttora chiamati "antivirus", pur avendo ormai funzioni molto più ampie. [33]

- I *worms* sono malware simili ai virus, ma con la capacità di autoreplicarsi e diffondersi autonomamente, senza bisogno dell'interazione dell'utente né di legarsi a file o programmi esistenti. Possono propagarsi rapidamente tramite reti, e-mail o condivisione file, causando spesso il blocco di intere infrastrutture. Oltre a danneggiare i sistemi, i worm possono installare backdoor, ossia accessi nascosti che permettono ai cybercriminali di aggirare le misure di sicurezza e controllare il sistema infetto. Tra le principali varianti si trovano i *LAN worms* che si diffondono tramite reti locali, gli *e-mail worms* via posta elettronica e i *file sharing worms* tramite reti peer-to-peer.

- I *trojan* sono malware che si camuffano da software legittimi per ingannare l'utente e farsi eseguire. Diversamente da virus e worm, non si replicano autonomamente, ma si basano sull'inganno per penetrare nei sistemi. Una volta attivati, possono rubare dati sensibili (*trojan spy*, *trojan banker*), concedere accesso remoto agli attaccanti (*trojan backdoor*), o avviare attacchi DDoS organizzando botnet di dispositivi compromessi (*trojan DDoS*, *trojan botnet*). Si diffondono attraverso allegati e-mail, download da siti non sicuri, reti P2P o altri malware.

- Lo *spyware* è un malware progettato per spiare gli utenti e raccogliere informazioni personali o sensibili senza il loro consenso. Può sottrarre dati finanziari, credenziali, cronologia di navigazione e altri dati comportamentali, rappresentando una seria minaccia per la privacy e la sicurezza informatica. Ci sono vari tipi di spyware, tra cui adware, che spesso raccolgono dati per scopi di marketing; trojans, che possono nascondere spyware; system monitors come i keylogger, che possono registrare attività come i tasti premuti sulla tastiera e tracking cookies, che tracciano la navigazione web. Lo spyware può essere installato tramite software gratuiti, phishing, social engineering o da altri malware.

- Il *keylogger* è un tipo di software o dispositivo hardware che registra tutto ciò che viene digitato su una tastiera. Sebbene possa avere usi legittimi come il monitoraggio aziendale o la risoluzione di problemi, viene spesso impiegato in modo illecito per rubare credenziali, dati bancari, messaggi e informazioni sensibili. I keylogger software sono programmi che vengono istallati sul computer di un utente, mentre i keylogger hardware sono dispositivi fisici che vengono inseriti tra la tastiera e il computer che verrà controllato. A differenza dei primi i keylogger hardware richiedono un accesso fisico ai computer dell'utente.

- Un *ransomware* è un tipo di malware che crittografa i dati dell'utente, rendendoli inaccessibili, e poi richiede un riscatto "ransom" generalmente in criptovaluta per mantenere l'anonimato dell'attaccante, per ottenere la chiave di decrittografia. La crittografia utilizzata è molto forte, il che significa che senza la chiave di decrittografia è quasi impossibile recuperare un file. Una volta che i file sono crittografati, il malware visualizza un messaggio in cui richiede un pagamento in cambio della chiave di decrittografia. Il costo del riscatto può variare notevolmente, a seconda del tipo di ransomware, dell'hacker e dell'attaccato. Questi attacchi sono particolarmente dannosi per le piccole e medie imprese (PMI), che spesso non dispongono di risorse sufficienti per proteggere adeguatamente i propri sistemi e dati.

- I *bot* permettono il controllo remoto del dispositivo infetto per compiere azioni coordinate, spesso all'interno di botnet usate per attacchi DDoS.

Riconoscere un'infezione da malware non è sempre immediato. Alcuni sintomi comuni includono il rallentamento delle prestazioni del sistema, la comparsa di pubblicità invasive tramite pop-up, blocchi frequenti, schermate di errore (BSOD), utilizzo anomalo delle risorse, cambiamenti nella configurazione del browser o disattivazione degli strumenti antivirus. Tuttavia, alcune forme particolarmente sofisticate di malware, come i *fileless malware* o malware senza file, operano esclusivamente in memoria RAM, evitando di scrivere file su disco e rendendosi così estremamente difficili da individuare [34]. È un tipo di software maligno che sfrutta tutti i processi di funzionamento di un sistema operativo per infettare un sistema e propagarsi. A differenza del malware tradizionale, il fileless malware non si appoggia sul file system di un computer per operare, rendendolo così più difficile da identificare e da rimuovere. Poiché il fileless malware non lascia file eseguibili sul disco rigido del computer, è difficile da rilevare con i metodi di sicurezza tradizionali, come gli scanner antimalware, che abitualmente cercano proprio file malevoli nel sistema controllato. Come altri tipi di malware può essere utilizzato per una serie di attività dannose, tra cui la raccolta di dati sensibili, l'installazione di altri tipi di malware o l'esecuzione di attacchi DDoS. Si può diffondere attraverso vari canali, tra cui e-mail di phishing, attacchi drive-by-

download, dove il malware si installa quando un utente visita un sito web infetto, o attraverso dispositivi usb infetti. La rilevazione e la rimozione del fileless malware può essere complessa a causa del suo approccio stealth invisibile. La prevenzione è quindi la miglior difesa. Questo tipo di minacce rappresenta una delle nuove frontiere del malware. Contrastare efficacemente tutti le tipologie di malware elencate richiede un approccio difensivo multilivello. Le contromisure devono includere l'adozione di software antivirus e anti-malware aggiornati, il costante aggiornamento dei sistemi operativi e delle applicazioni, la segmentazione delle reti aziendali, l'implementazione di firewall e sistemi di rilevamento delle intrusioni (IDS), nonché l'educazione e la formazione degli utenti, che restano il principale bersaglio delle tecniche di ingegneria sociale [35]. In ambito aziendale, la sicurezza informatica dovrebbe essere trattata come un processo continuo, che combina prevenzione, rilevamento e risposta agli incidenti, in linea con i principi della resilienza digitale. La costante evoluzione delle tecniche di attacco e delle varianti di malware rende necessaria un'attività di ricerca continua e il rafforzamento della collaborazione tra enti pubblici, aziende, ricercatori e fornitori di soluzioni di sicurezza. Solo attraverso un ecosistema di sicurezza proattivo è possibile far fronte a una minaccia in continua trasformazione, che rappresenta una delle principali sfide dell'era digitale.

2.3.1.2 Attacchi alle applicazioni web

L'SQL Injection rappresenta una delle minacce più insidiose e diffuse nel contesto della sicurezza delle applicazioni web, ed è ampiamente riconosciuta tra le principali vulnerabilità secondo l'OWASP (Open Web Application Security Project) [36]. Questo tipo di attacco si basa sull'inserimento, da parte dell'utente, di comandi SQL malevoli nei campi di input di un'applicazione, con l'obiettivo di manipolare le interrogazioni che quest'ultima esegue sul database sottostante. Il successo dell'attacco dipende dall'assenza o dall'inadeguatezza delle misure di controllo sull'input utente, che consentono di eseguire comandi arbitrari all'interno del sistema di gestione dei dati. Il principio su cui si fonda l'SQL Injection è semplice ma estremamente potente: l'attaccante approfitta del fatto che l'applicazione concatena direttamente l'input dell'utente all'interno di una query SQL, senza verificarne la validità o neutralizzare eventuali caratteri speciali. In questo modo, è possibile alterare la logica della query originale, forzando l'esecuzione di istruzioni non previste dal programmatore. Un esempio classico si verifica nei moduli di login, dove l'inserimento di una stringa come ' OR '1'='1 nel campo di autenticazione può trasformare una query legittima in una condizione sempre vera, consentendo l'accesso non autorizzato al sistema [37]. Le conseguenze di un attacco SQL Injection possono essere molto gravi. L'attaccante può accedere a dati riservati, modificarli o cancellarli, compromettere l'integrità del database o, nei casi più estremi, ottenere il controllo completo del sistema. In ambito aziendale, ciò può comportare la

violazione della riservatezza di dati sensibili, danni economici e reputazionali, nonché conseguenze legali legate alla mancata protezione delle informazioni, soprattutto in presenza di normative come il GDPR [38]. Esistono diverse varianti di SQL Injection, alcune delle quali estremamente sofisticate. L'iniezione classica prevede l'inserimento diretto del codice SQL all'interno della query. Tuttavia, in situazioni in cui il sistema non restituisce messaggi di errore visibili, l'attaccante può ricorrere a tecniche di tipo blind, ovvero "alla cieca", basandosi sul comportamento dell'applicazione per dedurre informazioni. Un'altra variante è l'error-based injection, che sfrutta i messaggi di errore del database per ottenere dettagli utili sulla struttura delle tabelle. Infine, l'attacco può avvenire anche attraverso un meccanismo temporale, noto come time-based blind, dove la risposta dell'applicazione è ritardata artificialmente per verificare l'esecuzione di comandi specifici. Prevenire l'SQL Injection richiede l'adozione di buone pratiche di programmazione e architetture sicure. La misura più efficace consiste nell'utilizzo di query parametrizzate, anche dette prepared statements, che separano il codice SQL dai dati dell'utente, impedendo che questi ultimi vengano interpretati come parte della logica della query [39]. L'impiego di stored procedures ben progettate può offrire un ulteriore livello di protezione. È inoltre fondamentale validare e sanificare correttamente tutti gli input, limitare i privilegi degli account del database usati dalle applicazioni e monitorare costantemente il traffico e il comportamento delle query, al fine di individuare eventuali anomalie. Un ulteriore strumento di difesa è rappresentato dai Web Application Firewall (WAF), che consentono di filtrare preventivamente le richieste HTTP potenzialmente pericolose prima che raggiungano l'applicazione. Tuttavia, la sicurezza efficace non può basarsi su una singola soluzione, ma deve derivare da un approccio integrato, che coinvolga lo sviluppo sicuro del software, l'amministrazione del sistema e la formazione degli operatori. L'SQL Injection continua a rappresentare una minaccia concreta per le applicazioni web moderne, nonostante la disponibilità di strumenti e metodologie per contrastarla. La sua pericolosità risiede nella facilità di esecuzione, nella difficoltà di rilevamento e nei potenziali danni che può arrecare. Per questo motivo, ogni sistema che interagisce con un database relazionale deve essere progettato con criteri di sicurezza robusti e aggiornato costantemente per fronteggiare una tipologia di attacco che, ancora oggi, miete numerose vittime tra le applicazioni vulnerabili.

2.3.1.3 Attacchi alla rete e ai protocolli

Gli attacchi Distributed Denial of Service (DDoS) rappresentano una delle minacce più gravi e pervasive nel campo della sicurezza delle reti e delle infrastrutture informatiche. A differenza degli attacchi DoS tradizionali, che provengono da una singola sorgente, gli attacchi DDoS coinvolgono un numero elevato di dispositivi compromessi, noti come zombie o bot, controllati da un'entità centrale che coordina l'attacco in modo distribuito. Lo scopo principale è quello di saturare le

risorse di un sistema bersaglio, rendendolo indisponibile per gli utenti legittimi [40]. Il successo di questi attacchi risiede nella loro capacità di sfruttare la natura aperta e scalabile di Internet. Un attaccante può, ad esempio, distribuire malware tramite Trojan horse o backdoor su centinaia o migliaia di dispositivi vulnerabili, spesso senza che i proprietari se ne rendano conto. Una volta ottenuto il controllo dei dispositivi infetti, l'attaccante può coordinare l'invio simultaneo di un'enorme quantità di traffico verso un server o un'infrastruttura bersaglio, fino a causarne l'arresto o il crash del servizio [41]. I DDoS si classificano come attacchi attivi, poiché non si limitano ad intercettare dati o risorse, ma puntano a rendere inservibili determinati servizi, provocando un'interruzione del funzionamento delle reti, dei siti web o delle applicazioni colpite. Le risorse colpite possono essere sia computazionali, come per esempio CPU, RAM, spazio disco, sia di rete come la larghezza di banda, il numero massimo di connessioni simultanee, e il sovraccarico può condurre a rallentamenti gravi o a un'interruzione totale del servizio [42]. Tra le tecniche più comuni utilizzate nei DDoS figurano gli attacchi di tipo UDP Flood, che prevedono l'invio massiccio di pacchetti UDP verso porte casuali del sistema vittima, forzandolo a controllare continuamente la disponibilità di applicazioni a tali porte. Un'altra tipologia frequente è l'ICMP Flood, che sfrutta pacchetti echo request (ping) per sovraccaricare la rete. Particolarmente noto è anche il SYN Flood, che si basa sull'invio di richieste di connessione TCP senza completare il processo di handshake, lasciando le connessioni aperte e saturando la capacità del server di accettare nuove connessioni [43]. Ulteriori varianti includono il Smurf Attack, in cui l'attaccante invia pacchetti ICMP a un indirizzo di broadcast di rete con l'indirizzo IP della vittima come mittente, generando una tempesta di risposte che ricade sul sistema bersaglio. Vi è poi il Teardrop Attack, che sfrutta errori nella gestione della frammentazione IP da parte del sistema operativo per causarne il blocco. Anche attacchi meno noti, come il Ping of Death, il Land Attack e le tecniche di esaurimento delle tabelle di processo, contribuiscono a rendere variegato e pericoloso il panorama delle minacce DDoS. Nel corso degli anni, questi attacchi sono diventati sempre più frequenti e sofisticati. Un esempio emblematico si è verificato nel 2013, quando l'exchange di criptovalute giapponese Mt. Gox fu colpito da un attacco DDoS di larga scala, che manipolò il prezzo del Bitcoin e creò gravi instabilità nei mercati virtuali [44]. Un altro caso rilevante è quello dell'attacco contro Spamhaus, nel quale furono generati picchi di traffico superiori a 300 Gbps, rendendolo uno degli attacchi DDoS più massicci della storia [45]. Le conseguenze di un attacco DDoS possono essere disastrose: interruzione dei servizi essenziali, danni economici ingenti, perdita di fiducia da parte degli utenti e reputazione compromessa. In contesti bancari e finanziari, attacchi di questo tipo hanno causato perdite per miliardi di dollari, come nel caso delle istituzioni statunitensi Webster Bank e Zions Bancorp, colpite da attacchi nel 2012 [46]. Contrastare i DDoS richiede un approccio

multilivello che combini misure preventive, strumenti di rilevamento e meccanismi di risposta. Tra le tecniche di prevenzione più efficaci si annoverano il filtraggio dei pacchetti in entrata e in uscita tramite ingress ed egress filtering, la disattivazione dei servizi inutilizzati, l'applicazione costante di patch di sicurezza, l'adozione di sistemi di IP hopping e la disattivazione del broadcast IP [47]. Tuttavia, la sola prevenzione non è sufficiente. È necessario integrare sistemi di rilevamento basati su firme, anomalie o approcci ibridi, e predisporre piani di risposta rapidi e automatizzati. Inoltre, l'uso di firewall di nuova generazione, sistemi di mitigazione cloud e CDN (Content Delivery Network) può ridurre l'impatto degli attacchi in tempo reale. In un contesto in cui la superficie d'attacco cresce proporzionalmente alla digitalizzazione, i DDoS continueranno a rappresentare una minaccia prioritaria. La resilienza delle infrastrutture digitali passa attraverso la capacità delle organizzazioni di anticipare, rilevare e contrastare tali attacchi in modo coordinato, sfruttando al meglio le risorse tecnologiche e le competenze umane disponibili.

2.3.2. Abuso dei contenuti informativi

Questa seconda macrocategoria comprende tutte le condotte in cui la tecnologia digitale non rappresenta tanto l'obiettivo dell'attacco, quanto piuttosto lo strumento attraverso il quale vengono perpetrati reati di natura tradizionale in una forma nuova, resa più insidiosa dalla rapidità di diffusione e dall'apparente anonimato che il cyberspazio garantisce agli autori. Si tratta di comportamenti che, pur essendo spesso configurabili anche come reati già previsti dal diritto penale classico, assumono nel contesto informatico una portata amplificata, con rilevanti ricadute di tipo psicologico, sociale ed economico.

2.3.2.1 Attacchi di tipo Social Engineering

Il Social Engineering, o ingegneria sociale, si basa sulla manipolazione psicologica delle vittime, sfruttando la fiducia o la disattenzione per ottenere informazioni riservate o accesso non autorizzato a sistemi e risorse. Rientrano in questa tipologia vari attacchi come: phishing, spear phishing, vishing, baiting, pretexting. La finalità di tali attacchi è principalmente l'inganno dell'utente per ottenere credenziali di accesso, trasferimenti di denaro o altre risorse di valore, sfruttando la vulnerabilità umana come punto d'ingresso. In particolare, il phishing è una delle tecniche di attacco informatico più diffuse e longeve, in quanto sfrutta principalmente l'ingegneria sociale piuttosto che vulnerabilità tecniche, inducendo l'utente a fornire volontariamente informazioni riservate. Il termine deriva dalla parola fishing*,* in italiano pescare, a indicare proprio la "pesca" di dati personali con l'uso di esche digitali. L'attaccante, detto phisher*,* si finge un'entità affidabile, come una banca, un corriere o un ente governativo, per indurre la vittima a cliccare su un link,

scaricare un allegato o compilare un modulo con credenziali, numeri di carte di credito o altri dati sensibili [48]. Il phishing rappresenta una minaccia particolarmente insidiosa perché sfrutta la fiducia e la disattenzione dell'utente, inducendolo ad agire in modo dannoso per sé stesso senza rendersene conto. A differenza degli attacchi puramente tecnici, in questo caso il punto debole risiede nel fattore umano, considerato uno degli elementi più vulnerabili nei sistemi di sicurezza. Le campagne di phishing sfruttano una varietà di canali di comunicazione per ingannare le vittime. Oltre alle tradizionali e-mail contraffatte, i cybercriminali utilizzano anche altre forme di attacco mirato, come lo smishing, che avviene tramite SMS fraudolenti, e il vishing, che si basa su chiamate telefoniche ingannevoli. Inoltre, queste campagne possono diffondersi attraverso messaggi diretti sui social network o tramite finte pagine web progettate per imitare siti legittimi, aumentando le possibilità di successo delle truffe. Le e-mail di phishing sono spesso caratterizzate da messaggi urgenti, minacce o promesse allettanti, elementi progettati per spingere l'utente ad agire impulsivamente, aggirando ogni valutazione razionale [49]. Nel corso degli anni, le tecniche di phishing si sono evolute notevolmente. Se in passato i messaggi erano spesso riconoscibili per errori grammaticali o layout approssimativi, oggi grazie a strumenti avanzati, inclusi algoritmi di intelligenza artificiale, gli attacchi sono sempre più sofisticati e difficili da individuare. Inoltre, si è assistito a una crescente personalizzazione degli attacchi: nel cosiddetto spear phishing, l'attaccante prende di mira un individuo specifico, utilizzando informazioni raccolte in precedenza per rendere il messaggio più credibile. Quando la vittima è una figura apicale all'interno di un'organizzazione, si parla invece di whaling. Le conseguenze di un attacco di phishing possono essere gravi e durature. Oltre al furto di identità e alla perdita di dati sensibili, le vittime possono subire danni economici diretti, come l'esaurimento dei fondi bancari o l'attivazione di pagamenti non autorizzati. A livello aziendale, un singolo clic su un link dannoso può aprire la porta a malware, ransomware o attacchi più ampi ai sistemi informativi interni. Per fronteggiare efficacemente il phishing, è fondamentale adottare un approccio multilivello che combini misure tecniche e formative. Tra le contromisure tecniche si annoverano l'uso di filtri antispam, software antivirus aggiornati, autenticazione a più fattori (MFA), e soluzioni di sicurezza per la posta elettronica basate su machine learning. Tuttavia, nessuna tecnologia può sostituire l'importanza della formazione degli utenti: insegnare a riconoscere i segnali di un messaggio fraudolento e promuovere buone pratiche digitali è essenziale per ridurre il rischio [50]. L'importanza di sensibilizzare gli utenti è stata evidenziata anche da numerosi studi recenti. Ad esempio, ricerche condotte su campioni di utenti aziendali hanno dimostrato che la probabilità di cadere in un attacco di phishing diminuisce significativamente dopo attività formative specifiche. Inoltre, è stato osservato che fattori come la stanchezza, il multitasking e il sovraccarico informativo aumentano la vulnerabilità individuale agli attacchi basati su inganno

psicologico [51]. Alla luce di ciò, il phishing non può più essere considerato un problema meramente tecnico, ma va interpretato come un fenomeno multidimensionale che coinvolge tecnologia, psicologia e cultura della sicurezza. Combatterlo richiede non solo strumenti informatici avanzati, ma anche una strategia organizzativa fondata sulla consapevolezza e sull'educazione degli utenti, che rimangono il primo e più importante baluardo contro questo tipo di minaccia.

2.4 Cybercrime in Italia: andamento, settori e tecniche di attacco

Dopo aver delineato la natura, le modalità operative e le principali categorie di crimini informatici, risulta essenziale tradurre questa cornice teorica in una lettura concreta della realtà nazionale. Analizzare i dati relativi agli attacchi informatici in Italia consente infatti di misurare l'effettiva portata del fenomeno, individuare i settori maggiormente esposti e comprendere come la crescente digitalizzazione nel nostro paese stia trasformando la superficie di rischio per imprese, istituzioni e cittadini. L'analisi dell'andamento degli attacchi informatici gravi che hanno colpito soggetti italiani tra il 2020 e il 2024, rappresentato nella figura 2, evidenzia una tendenza di crescente esposizione e vulnerabilità, con dati che confermano la rilevanza strategica del nostro Paese come obiettivo di campagne di attacco sempre più frequenti e mirate, alimentate dalla progressiva digitalizzazione dei servizi essenziali e dall'interconnessione di infrastrutture critiche. In particolare, il fenomeno può essere letto attraverso tre dimensioni chiave: il volume complessivo degli incidenti rilevati, la dinamica temporale della loro crescita e il peso relativo dell'Italia rispetto al contesto globale. Nel quinquennio 2020–2024 sono stati registrati 973 attacchi informatici di particolare gravità ai danni di organizzazioni italiane. Il solo 2024, infatti, ha fatto registrare 357 attacchi, pari al 36,7% del totale quinquennale, a testimonianza di un'intensificazione preoccupante e costante. [52] Questo incremento suggerisce come le organizzazioni italiane, comprese le piccole e medie imprese e le amministrazioni pubbliche, stiano progressivamente diventando obiettivi privilegiati per gruppi criminali organizzati, cyber-attivisti o attori statuali, attratti anche dalle lacune ancora presenti nei livelli di resilienza informatica. Fattori come la diffusione del lavoro da remoto, l'adozione accelerata di tecnologie cloud e la modernizzazione talvolta non accompagnata da adeguate misure di sicurezza contribuiscono ad ampliare la superficie di attacco.

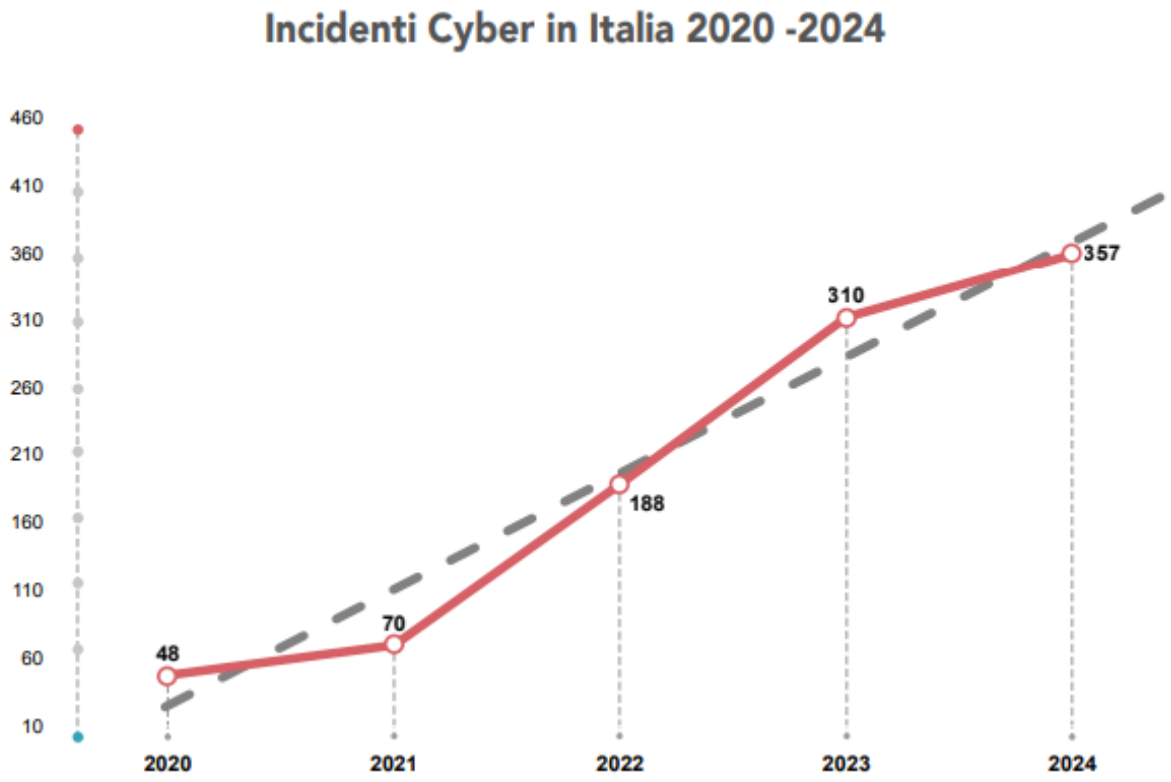

Figura 2 - Andamento del numero di incidenti informatici registrati in Italia nel periodo 2020–2024

Pur confermando la crescita numerica degli attacchi, il 2024 evidenzia una lieve attenuazione nel tasso di crescita rispetto alle dinamiche osservate negli anni precedenti. In particolare, rispetto al 2023, l'aumento degli incidenti gravi in Italia si attesta al +15,2%, un valore significativamente inferiore al +65% osservato tra il 2022 e il 2023. Questa inversione di tendenza appare ancora più evidente se confrontata con l'andamento su scala globale (figura 3): a livello internazionale, infatti, nel 2024 è stato rilevato un incremento medio degli attacchi del +27,4%, superiore quindi a quello italiano. Tale dinamica rappresenta un'inversione rispetto al quadro del 2023, quando la crescita degli incidenti in Italia superava di gran lunga quella rilevata a livello mondiale Nel complesso, questi dati suggeriscono che, pur permanendo un livello di rischio elevato, l'Italia stia attraversando una fase di relativo assestamento, verosimilmente riconducibile a un progressivo innalzamento del livello di consapevolezza in materia di sicurezza informatica, nonché a interventi mirati di potenziamento delle difese cyber da parte di imprese e istituzioni. Resta tuttavia fondamentale monitorare con attenzione l'evoluzione di questa tendenza, considerando la capacità di adattamento degli attori malevoli e la rapidità con cui emergono nuove vulnerabilità tecnologiche.

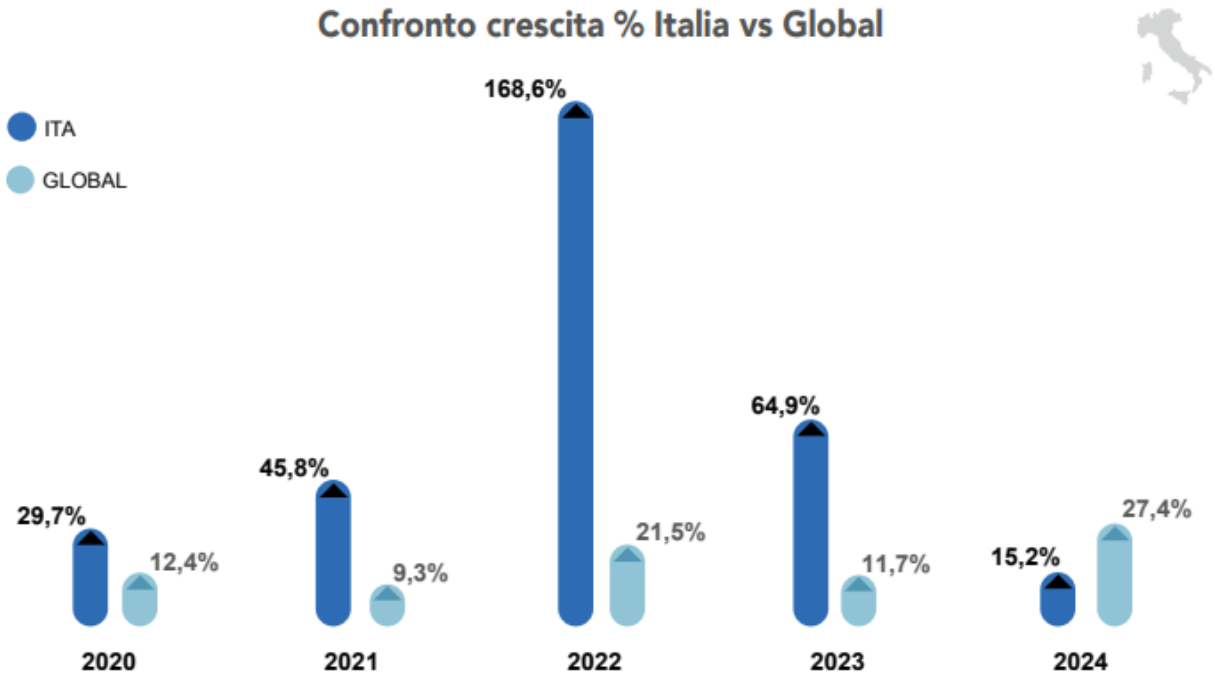

Figura 3 - Confronto percentuale della crescita degli incidenti cyber: Italia vs Global (2020–2024)

Nel 2024 (figura 4), l'incidenza degli attacchi subiti da organizzazioni italiane sul totale degli incidenti rilevati a livello mondiale si attesta al 10,1%. Sebbene si tratti di una leggera riduzione rispetto al 2023 (11,2%), questo valore rimane comunque elevato e vicino al massimo storico registrato negli ultimi anni. Tale dato conferma che l'Italia rappresenta uno degli obiettivi primari a livello europeo, per via della rilevanza economica dei suoi settori industriali, della frammentazione del tessuto produttivo, e della persistenza di vulnerabilità strutturali, soprattutto nelle piccole e medie imprese, spesso sprovviste di adeguate risorse e competenze per implementare strategie di cybersicurezza efficaci.

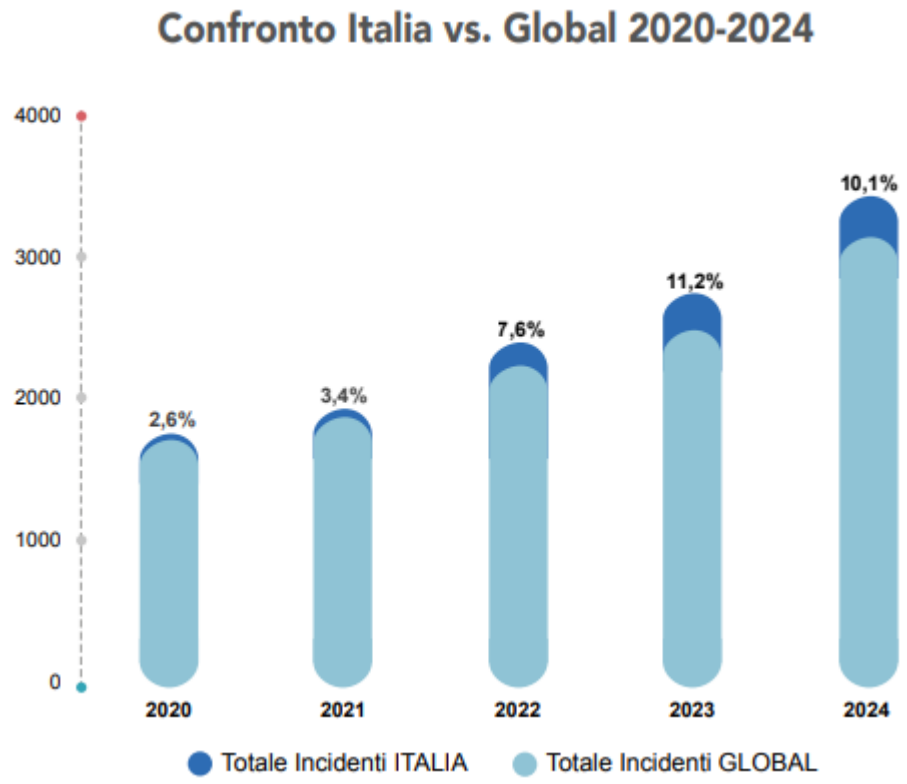

Figura 4 - Confronto tra il totale degli incidenti cyber in Italia e nel mondo (2020–2024)

Tra gli elementi di rilievo emersi dall'analisi degli attacchi informatici subiti da organizzazioni italiane nel 2024, particolare attenzione merita la distribuzione settoriale delle vittime. Quest'anno, come mostrato nella figura 5, si registra una significativa anomalia rispetto alle tendenze consolidate: il settore News / Multimedia si colloca per la prima volta al primo posto per numero di attacchi rilevati, con una quota pari al 18% del totale. Questo dato rappresenta una possibile discontinuità, che potrebbe indicare un caso eccezionale piuttosto che l'inizio di un mutamento strutturale. Lo scenario italiano presenta quindi delle peculiarità, non solo derivanti dall'elevata incidenza degli incidenti rispetto al dato globale, anche in termini di distribuzione delle vittime. Nel campione mondiale, infatti, News / Multimedia è solo all'ottavo posto, subito dopo Manufacturing. I comparti tradizionalmente più colpiti seguono nelle posizioni immediatamente successive. Il settore Manufacturing si conferma tra i più esposti, con il 16% degli attacchi, mantenendo una presenza costante tra i principali obiettivi a livello nazionale. Subito dopo si colloca il comparto Government, con il 10% degli incidenti, in discesa rispetto al 2023, anno in cui aveva occupato il primo posto. Un altro elemento di rilievo riguarda gli attacchi definiti Multiple Target, ovvero incidenti che colpiscono simultaneamente più settori o categorie. Storicamente predominanti sia in Italia che a livello globale, nel 2024 rappresentano meno di un quinto degli attacchi totali, condividendo la seconda posizione in classifica con il settore manifatturiero. Completano la

distribuzione i comparti Transportation / Storage (7%), Professional / Scientific / Technical (6%) e Organizations (5%), che confermano la diffusione trasversale della minaccia cibernetica in settori eterogenei per struttura e funzione, ma accomunati da una crescente esposizione alla digitalizzazione e, spesso, da vulnerabilità persistenti nei sistemi di difesa.

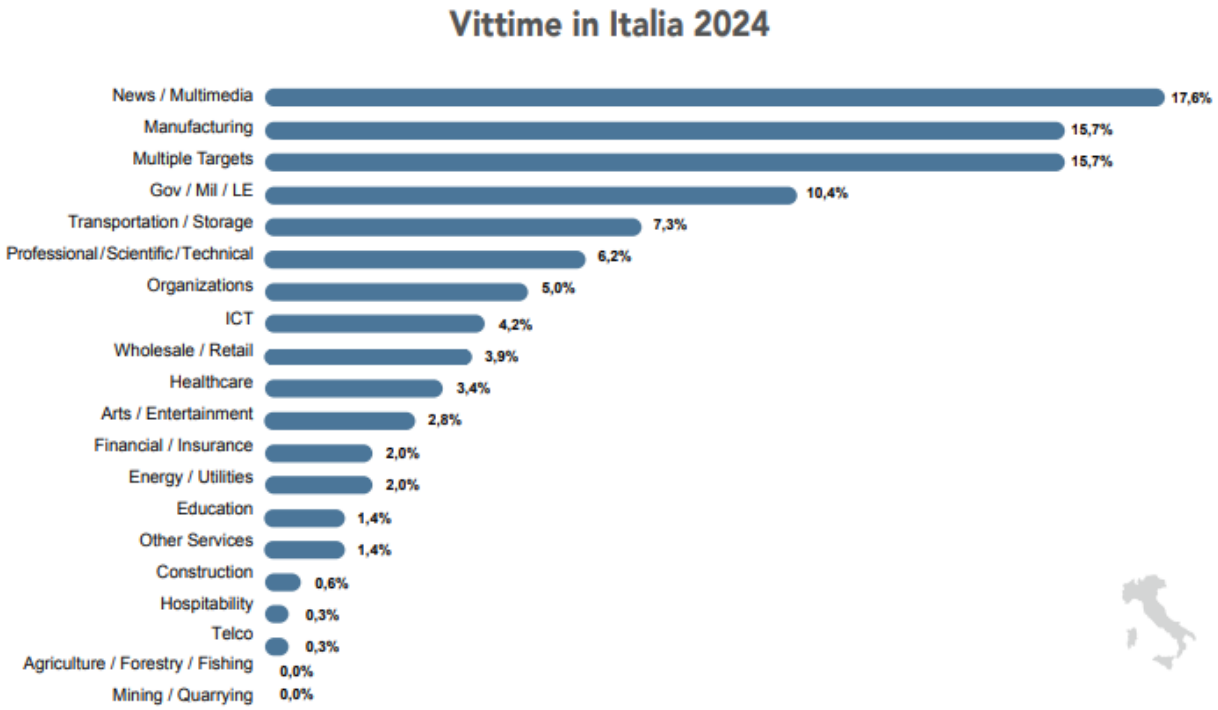

Figura 5 - Distribuzione percentuale delle vittime di attacchi informatici in Italia nel 2024 per settore di attività

Il confronto tra i dati del 2023 e quelli del 2024, presente nella figura 6, evidenzia alcune variazioni significative nella distribuzione degli attacchi informatici per settore, che suggeriscono l'emergere di nuovi obiettivi prioritari e, al contempo, un ridimensionamento di alcuni bersagli tradizionali. Il cambiamento più marcato riguarda il settore News / Multimedia, che nel 2024 registra un incremento improvviso e rilevante nel numero di incidenti, balzando in testa alla classifica settoriale. Questo "salto" rappresenta l'anomalia più evidente rispetto all'anno precedente, con una variazione che, per entità e rapidità, potrebbe essere attribuibile a eventi eccezionali piuttosto che a una trasformazione strutturale della minaccia. Anche il settore Multiple Target registra un aumento significativo: con 21 attacchi in più rispetto al 2023, la sua quota nella ripartizione complessiva cresce di 5 punti percentuali, segnando una ripresa rispetto al calo osservato negli ultimi anni. Parallelamente, il comparto Manufacturing evidenzia una crescita netta, passando da 35 a 56 incidenti, con un incremento di 3 punti percentuali, a conferma della persistente vulnerabilità di un settore strategico e fortemente digitalizzato. Il comparto Professional / Scientific / Technical mostra anch'esso un incremento, sebbene meno marcato in termini assoluti, indicando una crescente

attenzione da parte degli attori malevoli anche verso ambiti ad alta intensità intellettuale e tecnologica. Diversamente, il settore Healthcare presenta un andamento pressoché stabile, con un numero di attacchi simile a quello dell'anno precedente, suggerendo una permanenza del rischio ma senza variazioni sostanziali. Decisamente in controtendenza è invece il settore Government, che nel 2024 subisce 37 attacchi, registrando una diminuzione significativa rispetto al 2023. Il calo, pari a 8 punti percentuali nella distribuzione complessiva, sembra in parte riconducibile a una riduzione degli attacchi di matrice hacktivista, che avevano invece caratterizzato fortemente il panorama dell'anno precedente. L'analisi congiunta di questi dati suggerisce una dinamica fluida nella scelta dei bersagli da parte degli attori della minaccia, influenzata non solo da fattori strutturali, ma anche da contingenze geopolitiche, mediatiche o simboliche. Un ulteriore elemento degno di nota nell'analisi 2024 riguarda l'evoluzione del rischio informatico nel settore Financial / Insurance, che lo scorso anno aveva fatto registrare un picco anomalo nel numero di attacchi. Nel 2023, infatti, le istituzioni finanziarie e assicurative erano comparse tra i settori più colpiti, in quella che appariva come una deviazione rispetto al trend storico. Nel 2024, tuttavia, si osserva un netto ridimensionamento: il numero di attacchi rilevati torna ai livelli del 2022, con 7 incidenti, pari ad appena il 2% del totale, segnando un calo di 7 punti percentuali rispetto all'anno precedente e facendo uscire il comparto dalla Top 10 dei settori più colpiti. Questa significativa riduzione può essere interpretata come il risultato di una serie di fattori strutturali, in primo luogo la forte pressione normativa che insiste da anni sul settore finanziario. L'obbligo di conformarsi a standard stringenti di sicurezza e resilienza operativa, imposti sia a livello europeo che nazionale, ha spinto gli operatori del comparto a rafforzare in modo significativo le proprie difese cibernetiche. In particolare, l'adozione di sistemi avanzati di rilevamento, risposta agli incidenti e protezione dei dati, unita a investimenti costanti in tecnologie di sicurezza e nella formazione del personale, sembra aver prodotto effetti tangibili in termini di riduzione dell'esposizione. Questa dinamica suggerisce che, almeno in contesti altamente regolamentati, l'efficacia delle politiche di compliance e governance della sicurezza possa costituire un valido fattore di mitigazione del rischio informatico, contribuendo a rafforzare la resilienza complessiva del sistema.

Figura 6 - Evoluzione delle prime 10 categorie di vittime di attacchi informatici in Italia (2020–2024)

L'analisi delle tecniche di attacco più utilizzate nel 2024, rappresentata nella figura 7, consente di approfondire le cause alla base dell'elevato numero di incidenti che hanno colpito organizzazioni pubbliche e private in Italia. Queste informazioni sono fondamentali per comprendere le dinamiche dell'offensiva cibernetica e per indirizzare con maggiore efficacia strategie difensive mirate. Nel 2024, il Malware torna a essere la tecnica d'attacco prevalente, risultando responsabile del 38% degli incidenti rilevati. Dopo un periodo in cui era stato temporaneamente superato da altre modalità, il ritorno del malware in cima alla classifica conferma la sua versatilità e capacità di adattamento ai diversi contesti tecnologici e settoriali. Le famiglie di malware impiegate risultano spesso raffinate e progettate per eludere i controlli tradizionali, colpendo infrastrutture critiche e sistemi scarsamente aggiornati. Al secondo posto si collocano gli attacchi DDoS (Distributed Denial of Service), che rappresentano il 21% del totale. Sebbene in calo rispetto al 2023, quando avevano raggiunto il 36%, rimangono una tecnica ampiamente sfruttata per interrompere la disponibilità dei servizi e generare impatti reputazionali o economici sulle vittime, in particolare nel settore pubblico e nei servizi essenziali. Una novità rilevante riguarda la crescita degli attacchi che sfruttano vulnerabilità note o non ancora corrette, i quali si attestano al 19% degli incidenti, una quota senza precedenti nel contesto italiano. Questo aumento è in parte correlato all'impennata di attacchi nel settore News / Multimedia, dove sono state sfruttate falle nei sistemi di pubblicazione o nei CMS. L'incremento degli attacchi basati su vulnerabilità suggerisce la crescente importanza dell'aggiornamento tempestivo dei sistemi, della gestione delle patch e dell'adozione di strumenti avanzati di vulnerability assessment. Il Phishing e Social Engineering, con l'11%, si confermano

come tecniche costanti nel panorama delle minacce. La loro efficacia continua a poggiare sull'elemento umano, che rimane il punto d'ingresso più facilmente manipolabile, soprattutto in assenza di un'adeguata cultura della sicurezza informatica all'interno delle organizzazioni. Le tecniche non classificate (categoria Undisclosed) scendono al 7%, segnando un calo rispetto agli anni precedenti. Questa riduzione è attribuibile, da un lato, a una maggiore trasparenza nella comunicazione degli incidenti da parte delle vittime; dall'altro, alla crescente tendenza dei gruppi cybercriminali a rivendicare pubblicamente le proprie azioni, spesso fornendo dettagli tecnici sugli attacchi condotti. Infine, si rilevano due categorie minori ma significative: le Multiple Techniques (2%), che indicano attacchi complessi condotti attraverso la combinazione di più vettori e fasi, e i Web Attacks (2%), che mantengono una presenza costante, in particolare nei confronti di portali pubblici e servizi online. Questi dati evidenziano un panorama in continua evoluzione, in cui alla varietà delle tecniche corrisponde una crescente difficoltà nella previsione e nella prevenzione degli attacchi. L'adattamento delle contromisure, la formazione del personale e l'automazione della difesa diventano elementi centrali per ridurre l'impatto di minacce sempre più sofisticate.

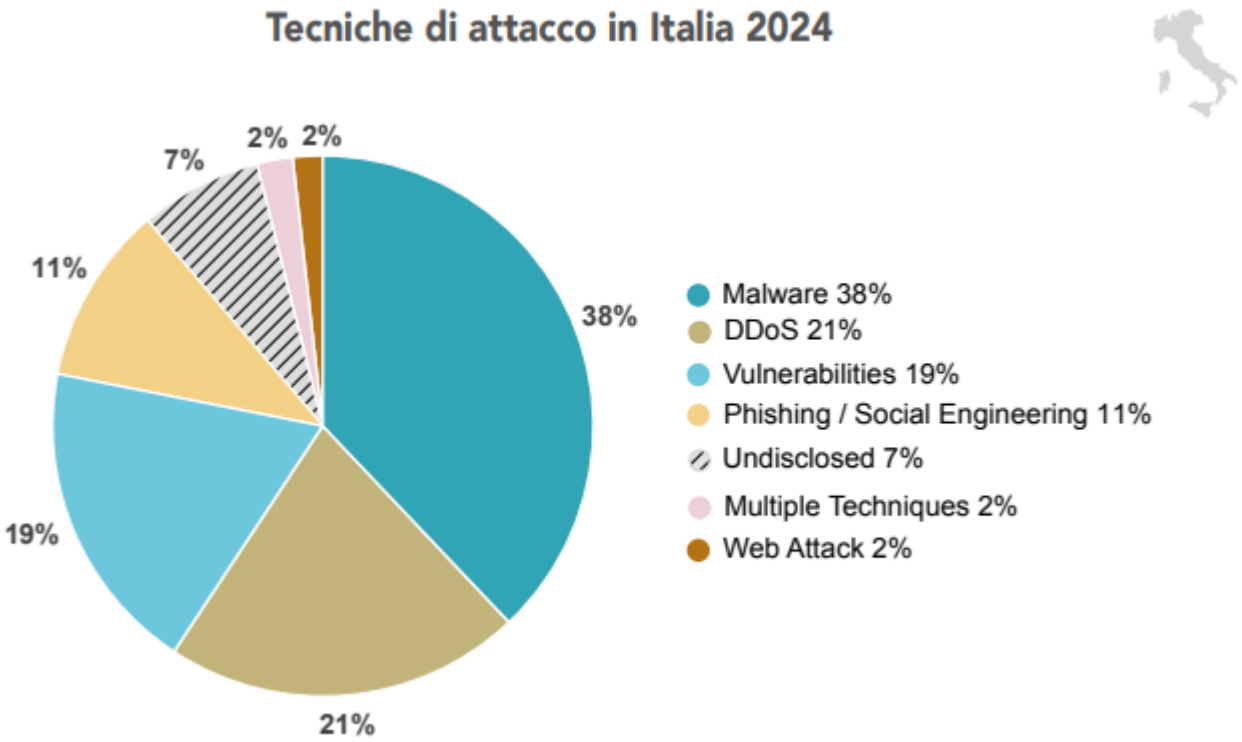

Figura 7 - Principali tecniche di attacco informatico in Italia nel 2024

L'analisi delle tecniche di attacco più impiegate contro soggetti italiani nel 2024, presente nella figura 8, offre una chiave di lettura fondamentale per comprendere la natura e l'evoluzione della minaccia informatica. L'andamento delle diverse modalità offensive, confrontato con quello degli

anni precedenti e con i dati internazionali, evidenzia cambiamenti significativi tanto sul piano quantitativo quanto su quello qualitativo. Nel 2024, il Malware riconquista la prima posizione nella classifica delle tecniche di attacco, con 135 incidenti rilevati, pari al 38% del totale, segnando un incremento di oltre il 30% rispetto al 2023 (103 casi). Questo aumento è in linea con la tendenza globale e conferma la perdurante efficacia e versatilità di questo strumento, in continua evoluzione per sfuggire alle misure di rilevamento tradizionali. In calo invece gli attacchi DDoS (Distributed Denial of Service), che si attestano al 21%, con 76 incidenti contro i 111 registrati nel 2023, segnando una riduzione del 36%. Si tratta di un'inversione rispetto alla crescita costante osservata negli anni precedenti, e che risulta in controtendenza rispetto al dato globale, dove gli attacchi DDoS risultano in aumento. Questo declino può essere attribuito a due fattori principali: da un lato, un possibile spostamento dell'attenzione degli attivisti verso Paesi più direttamente coinvolti nei conflitti internazionali in corso; dall'altro, una migliorata postura difensiva da parte delle organizzazioni italiane, che oggi sembrano più capaci di assorbire o neutralizzare attacchi dimostrativi di tipo hacktivista. La correlazione con il calo generale dell'hacktivism registrato nel 2024 rafforza questa interpretazione, considerando che i DDoS rappresentano una delle principali forme di protesta digitale associate a questo fenomeno. Altre dinamiche degne di nota emergono dall'aumento degli attacchi basati su vulnerabilità note o zero-day, che passano da 7 casi nel 2023 a 67 nel 2024, con una crescita di quasi il +900%. Questa impennata, senza precedenti in Italia, è fortemente influenzata dagli attacchi al settore News / Multimedia, dove sono stati sfruttati exploit su piattaforme di pubblicazione e gestione dei contenuti. A livello globale, invece, tali attacchi risultano stabili, a conferma della natura contingente e settoriale del fenomeno nel contesto italiano. Anche il Phishing e il Social Engineering registrano un incremento, passando da 28 a 38 incidenti (+35%). Tali tecniche, basate sull'inganno e sull'errore umano, restano tra le più diffuse ed efficaci, soprattutto nei confronti di utenti poco formati o in ambienti lavorativi con scarsa consapevolezza della sicurezza informatica. I Web Attacks rimangono pressoché stabili in Italia, mentre a livello globale si osserva un aumento del 50%, a conferma di una differente esposizione o di un possibile gap nella digitalizzazione dei servizi pubblici e privati. Più preoccupante, invece, è l'aumento degli attacchi condotti tramite Multiple Techniques, che crescono del 90% passando da 1 a 8 incidenti, segnalando una maggiore sofisticazione delle operazioni offensive, spesso costruite in più fasi e con vettori combinati. Infine, la quota di incidenti legati al furto di identità resta trascurabile nei dati ufficiali. Tuttavia, è importante sottolineare che in Italia le cosiddette truffe informatiche, rivolte a individui o piccole imprese, risultano in costante crescita. Pur non rientrando nei criteri di gravità per essere incluse nella presente analisi statistica, esse rappresentano una componente rilevante del panorama delle minacce digitali, soprattutto per il tessuto economico frammentato del Paese. Nel

complesso, i dati 2024 confermano che l'evoluzione delle tecniche di attacco in Italia segue in parte i trend globali, ma è anche fortemente influenzata da dinamiche locali e settoriali, che impongono una continua adattabilità delle misure di prevenzione, risposta e resilienza.

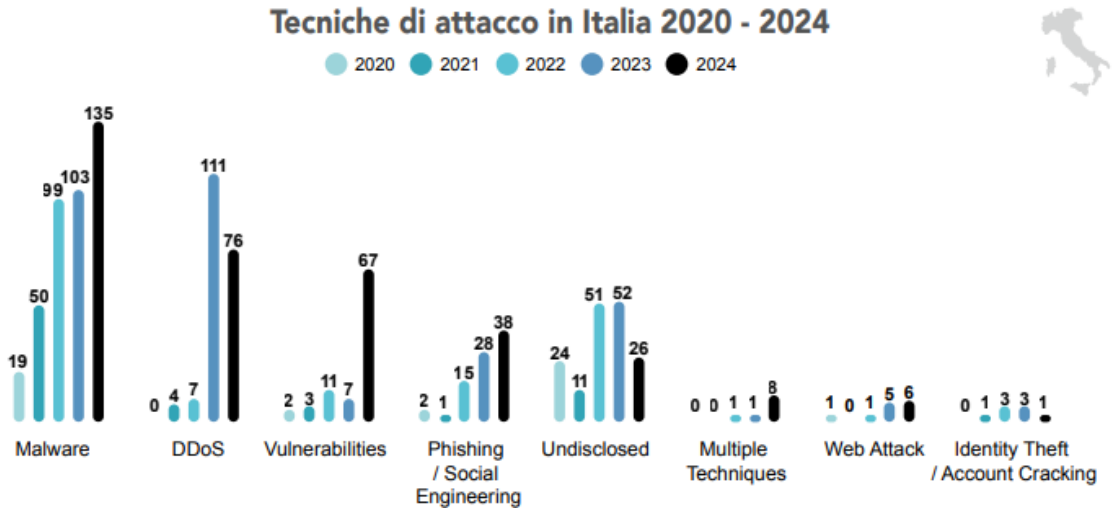

Figura 8 - Evoluzione delle principali tecniche di attacco informatico in Italia (2020–2024)

[52] Clusit – Associazione Italiana per la Sicurezza Informatica. (2025). *Rapporto Clusit 2025 sulla sicurezza ICT in Italia*.

3. L'ecosistema normativo sulla cybersecurity

3.1 L'evoluzione del framework europeo

3.1.1 Il Cybersecurity Package: la direttiva NIS 2 e il nuovo scenario normativo

L'evoluzione del quadro normativo europeo in materia di cybersicurezza ha conosciuto un'importante accelerazione a partire dal 2020, anno in cui la commissione europea ha presentato il cosiddetto *Cybersecurity Package*, un insieme di iniziative strategiche e legislative mirate a rafforzare la sicurezza informatica dell'Unione Europea nel contesto del decennio digitale [53]. Tale pacchetto comprende la nuova strategia dell'UE per la cybersicurezza composto da una proposta di revisione della direttiva NIS (Network and Information Security) e da una direttiva sulla resilienza delle entità critiche, nota come Direttiva CER. Insieme definiscono un quadro integrato per la sicurezza delle infrastrutture critiche e dei servizi essenziali, promuovendo un modello di protezione resiliente e coordinato a livello europeo. La Direttiva NIS (Network and Information Security) del 2016, è stato il primo strumento normativo europeo in materia di sicurezza delle reti e dei sistemi informativi, recepito in Italia con il d.lgs. n. 65/2018 [54]. La NIS ha introdotto obblighi per gli operatori di servizi essenziali (OSE) e per i fornitori di servizi digitali (FSD), imponendo

l'adozione di misure di sicurezza e la notifica degli incidenti significativi. Tuttavia, l'applicazione dello strumento ha rivelato alcune criticità, tra cui la limitata copertura dei settori coinvolti, l'eterogeneità delle prassi di implementazione negli Stati membri e l'insufficiente condivisione delle informazioni tra le autorità competenti. Per rispondere a tali sfide è stata adottata la Direttiva NIS2, che amplia l'ambito di applicazione, includendo non solo gli OSE e i FSD, ma anche altre categorie di soggetti, come le piccole e medie imprese attive in settori critici, i fornitori di reti di comunicazione elettronica e i servizi cloud [55]. La NIS2 introduce un approccio basato sulla gestione del rischio, prevedendo che i soggetti essenziali e importanti adottino misure di sicurezza tecniche, organizzative e operative adeguate e proporzionate. Inoltre, viene potenziato il ruolo delle autorità nazionali competenti, con l'istituzione di un sistema di vigilanza e controllo più rigoroso e l'introduzione di sanzioni in caso di inadempienza. Di particolare rilievo è l'attenzione riservata alla sicurezza della supply chain, con l'obbligo per i soggetti interessati di valutare le vulnerabilità dei fornitori e di garantire la sicurezza dei prodotti e servizi utilizzati. La direttiva NIS2 introduce anche una nuova classificazione degli incidenti, suddivisi in base alla gravità, prevedendo tre finestre temporali per la loro segnalazione: preallarme entro 24 ore, notifica entro 72 ore e report finale. Viene inoltre rafforzata la cooperazione tra i CSIRT nazionali (Computer Security Incident Response Teams) e potenziata la gestione delle crisi informatiche a livello europeo, con l'istituzione di EU-CyCLONe, una piattaforma per il coordinamento delle crisi informatiche tra gli Stati membri. Gli Stati membri sono tenuti a designare o istituire una o più autorità competenti per la gestione della direttiva, che devono garantire la supervisione e l'applicazione degli obblighi previsti, nonché fornire assistenza ai soggetti obbligati. A livello nazionale, la governance si articola attorno a un punto di contatto unico e alla collaborazione tra le autorità competenti. In Italia, tale ruolo è stato affidato all'Agenzia per la Cybersicurezza Nazionale (ACN), che agisce quale autorità nazionale competente per la NIS2. La principale differenza tra la NIS e la NIS2 risiede nell'ampliamento del perimetro di applicazione, nella maggiore centralizzazione della governance e nella previsione di obblighi più stringenti in termini di gestione dei rischi e segnalazione degli incidenti. La NIS2 riflette l'evoluzione delle minacce informatiche e la crescente interconnessione delle infrastrutture digitali, promuovendo un approccio più armonizzato e resiliente a livello europeo. La direttiva CER (Critical Entities Resilience) [56], invece, pubblicata il 27 dicembre 2022, ha un obiettivo complementare rispetto alla NIS2, concentrandosi sulla resilienza fisica delle infrastrutture critiche in settori come energia, trasporti, finanza, sanità e infrastrutture digitali. Gli Stati membri sono chiamati a individuare i soggetti critici entro il 17 luglio 2026 e a garantire che questi adottino misure tecniche e organizzative per la gestione dei rischi, comprese le minacce naturali, umane o tecnologiche. La direttiva impone obblighi specifici per i soggetti critici, tra cui la

valutazione dei rischi, la predisposizione di misure di protezione e la notifica degli incidenti significativi alle autorità competenti. Inoltre, istituisce un gruppo europeo per la resilienza dei soggetti critici, con il compito di promuovere la cooperazione e lo scambio di buone prassi tra gli Stati membri. Un elemento chiave di differenziazione tra NIS2 e CER è dato dalla loro area di applicazione: mentre la NIS2 si concentra sulla sicurezza delle reti e dei sistemi informativi, la CER si focalizza sulla resilienza fisica e operativa delle infrastrutture critiche, garantendo un approccio integrato alla protezione dei servizi essenziali. In pratica, la NIS2 tutela la sicurezza informatica dei sistemi, mentre la CER garantisce la continuità fisica e operativa delle infrastrutture che forniscono tali servizi.

3.1.2 La revisione del Cybersecurity Act (CSA)

L'evoluzione del quadro normativo europeo in materia di cybersicurezza ha visto, accanto al rafforzamento della Direttiva NIS, recentemente aggiornata con la NIS2, un importante sviluppo anche sul versante regolamentare con l'adozione del Regolamento UE 2019/881, noto come Cybersecurity Act. Tale regolamento, entrato in vigore il 17 aprile 2019, persegue l'obiettivo di garantire un elevato livello di cybersicurezza, resilienza digitale e fiducia nel mercato interno dell'Unione europea, intervenendo su due direttrici principali: da un lato, il rafforzamento delle competenze e del ruolo dell'Agenzia dell'Unione Europea per la cybersicurezza (ENISA); dall'altro, l'istituzione di un quadro europeo armonizzato di certificazione della cybersicurezza per prodotti, servizi e processi ICT [57]. Nello specifico, i primi articoli del Regolamento disciplinano l'organizzazione, le funzioni e i compiti dell'ENISA. In particolare, quest'ultima, con mandato permanente, è incaricata di supportare gli Stati membri nella prevenzione e gestione delle minacce informatiche, coordinare le risposte a incidenti di ampia portata e promuovere la cooperazione internazionale. A partire dall'art. 46, il regolamento introduce il sistema europeo di certificazione della cybersicurezza, che uniforma le prassi di certificazione per i prodotti, servizi e processi TIC (Tecnologie dell'Informazione e della Comunicazione), riducendo la frammentazione del mercato e favorendo il riconoscimento reciproco delle certificazioni tra gli Stati membri. Sulla base di tale programma, la Commissione può incaricare l'ENISA di elaborare nuovi schemi di certificazione o revisionare quelli esistenti. L'ENISA è stata già investita dell'elaborazione dei primi tre schemi relativi a common criteria, servizi cloud e reti 5G[58]. Sebbene la certificazione resti formalmente volontaria, la commissione può decidere di renderla obbligatoria in casi specifici, per garantire un livello minimo di sicurezza nel mercato interno. Un aspetto di particolare rilievo è il divieto per gli stati membri di introdurre sistemi nazionali di certificazione per prodotti, servizi e processi TIC già coperti da un sistema europeo in vigore, garantendo così l'unità del mercato interno. Tuttavia, ogni

Stato è tenuto a designare una o più autorità nazionali di certificazione della cybersicurezza, responsabili della sorveglianza e dell'attuazione dei sistemi europei nel proprio territorio. I sistemi di certificazione sono articolati su tre livelli di affidabilità in funzione del rischio e dell'impatto dell'incidente: base, sostanziale, elevato. La certificazione "elevata" mira a garantire la protezione da minacce avanzate. Nel 2023, la Commissione europea ha avviato una revisione del Cybersecurity Act, con l'obiettivo di estendere il sistema di certificazione anche ai Managed Security Services (MSS), ovvero i servizi di sicurezza gestiti come la risposta agli incidenti, il penetration testing e l'audit di sicurezza, ritenuti cruciali per la protezione delle infrastrutture critiche e dei soggetti essenziali definiti dalla NIS2. Questa evoluzione risponde alla crescente importanza dei servizi di sicurezza gestiti nel garantire la resilienza operativa delle organizzazioni in Europa. La Commissione è chiamata inoltre a valutare ogni due anni l'efficacia dei sistemi adottati e, se necessario, a renderli obbligatori. Parallelamente, si prevedono forme rafforzate di cooperazione tra autorità nazionali e Commissione per assicurare trasparenza e tempestività nell'adozione degli schemi. Infine, la Commissione per l'industria, la ricerca e l'energia ha adottato una relazione nella quale il Parlamento viene sollecitato ad inserire una serie di modifiche al testo proposto nella logica di valutare i percorsi formativi esistenti, individuare l'attuale divario di competenze, formulare un elenco di proposte per affrontare le necessità dei lavoratori qualificati e prevedere specifiche forme di sostegno per le microimprese e le PMI [59].

3.1.3 La sicurezza dei prodotti con elementi digitali: il Cyber Resilience Act

Il Cyber Resilience Act (Regolamento (UE) 2024/2847 [60], entrato in vigore il 10 dicembre 2024, rappresenta un altro tassello fondamentale nel processo di consolidamento del quadro normativo europeo in materia di cybersicurezza. Esso si inserisce nell'ambito della Strategia dell'UE per la cibersicurezza avviata nel 2020, perseguendo l'obiettivo di assicurare che tutti i prodotti con elementi digitali immessi nel mercato dell'Unione soddisfino requisiti di sicurezza adeguati, contribuendo così a creare un ecosistema digitale europeo resiliente e sicuro per cittadini, imprese e pubbliche amministrazioni. Il regolamento si propone di tutelare gli utilizzatori finali, siano essi consumatori o imprese, attraverso norme armonizzate che disciplinano l'immissione sul mercato di prodotti hardware e software con componenti digitali, imponendo requisiti di cybersicurezza per tutte le fasi del ciclo di vita del prodotto: dalla progettazione alla produzione, dalla manutenzione all'eventuale dismissione. Esso introduce inoltre un obbligo generale di diligenza a carico di tutti gli attori economici coinvolti nella catena del valore. L'ambito di applicazione del regolamento comprende i prodotti il cui utilizzo prevede, o può ragionevolmente prevedere, una connessione diretta o indiretta a reti o dispositivi, classificandoli in categorie sulla base della loro criticità. Il

regolamento stabilisce una serie articolata di obblighi a carico dei produttori, tra cui la conduzione di valutazione dei rischi, la previsione di periodi minimi di assistenza, la notifica tempestiva delle vulnerabilità a ENISA (entro 24 ore) e la redazione della dichiarazione UE di conformità. Gli obblighi si estendono anche a importatori e distributori, in particolare quando modificano o reimmettono i prodotti sul mercato con il proprio marchio. Il regolamento introduce un sistema di sorveglianza e controllo, delegando agli stati membri la designazione delle autorità di notifica e di vigilanza del mercato. Gli organismi di valutazione della conformità devono soddisfare rigorosi requisiti di indipendenza, competenza e riservatezza, e la loro remunerazione non può essere collegata al numero o all'esito delle valutazioni. In caso di violazioni gravi degli obblighi previsti, il CRA stabilisce un regime sanzionatorio significativo, con multe fino a 15 milioni di euro o al 2,5% del fatturato globale annuo dell'impresa, a seconda del valore più elevato. A supporto dell'implementazione, è stato istituito il Cyber Resilience Act Expert Group, con funzioni consultive e di supporto tecnico nella redazione di linee guida operative e nella promozione del dialogo tra Commissione, autorità nazionali ed esperti [61]. Il Cyber Resilience Act introduce, quindi, un quadro normativo innovativo e complesso, che attribuisce rilevanza primaria alla sicurezza dei prodotti digitali nell'ottica di una cybersicurezza strutturale e preventiva, promuovendo un approccio integrato tra operatori economici, autorità nazionali e istituzioni europee, a beneficio del mercato interno e della sicurezza collettiva dell'Unione europea.

3.1.4 Uno scudo per l'Europa: il Cyber Solidarity Act (CSoA)

Il Cyber Solidarity Act [62], pubblicato il 15 gennaio 2025, rappresenta una delle più recenti e significative iniziative legislative dell'Unione Europea nel campo della cybersicurezza. Tale regolamento nasce con l'intento di rafforzare le capacità dell'Unione europea in materia di rilevamento, preparazione e risposta alle minacce e agli incidenti informatici, delineando un vero e proprio "scudo digitale" a tutela del mercato interno, delle istituzioni e dei cittadini europei. Il Cyber Solidarity Act persegue questo obiettivo attraverso l'introduzione di tre strumenti fondamentali: la rete paneuropea di poli informatici; il meccanismo di emergenza per la cybersicurezza e il meccanismo di riesame degli incidenti informatici. Tali strumenti sono concepiti per supportare gli stati membri nello sviluppo di capacità coordinate e condivise di rilevamento delle minacce, nonché nella gestione e mitigazione degli effetti degli incidenti significativi e su vasta scala, favorendo anche la ripresa post-evento. L'intento è altresì quello di sostenere soggetti terzi, pubblici o privati, colpiti da incidenti equivalenti per portata o impatto a quelli su larga scala. In tale contesto, il regolamento istituisce il "Sistema europeo di allerta per la cybersicurezza", una

rete paneuropea di infrastrutture composta da poli informatici nazionali e, su base volontaria, da poli transfrontalieri. I poli nazionali sono istituiti dagli Stati membri, mentre i poli transfrontalieri possono essere creati su iniziativa congiunta di almeno tre stati, mediante apposito accordo. I compiti affidati a tali poli includono la raccolta e condivisione di informazioni su minacce e incidenti informatici, con particolare attenzione alla cooperazione interna ed esterna tra i poli stessi, allo scopo di migliorare la capacità collettiva di rilevamento e risposta e di rafforzare la resilienza della rete europea dei CSIRT (Computer Security Incident Response Teams). Un ulteriore elemento centrale del regolamento è la creazione di una riserva europea per la cybersicurezza, composta da fornitori fidati di servizi di sicurezza gestiti, selezionati per offrire servizi di risposta rapida in caso di incidenti significativi. L'accesso a tali servizi è riservato a soggetti specificamente individuati, previa richiesta formale secondo le modalità stabilite dal regolamento. L'attuazione di tale riserva è affidata alla Commissione europea, mentre l'ENISA ha il compito di aggiornare, con cadenza biennale, la mappatura dei servizi necessari agli utenti beneficiari. Il meccanismo di riesame degli incidenti di cybersicurezza rappresenta un ulteriore strumento strategico previsto dal Cyber Solidarity Act. In particolare, l'ENISA, su richiesta della Commissione o di EU-CyCLONe (European Cyber Crises Liaison Organisation Network), con il supporto della rete CSIRT e previo consenso degli Stati membri interessati, è incaricata di condurre un riesame dettagliato degli incidenti informatici di particolare rilievo. Tale riesame comprende l'analisi delle minacce coinvolte, delle vulnerabilità sfruttate e delle misure di attenuazione adottate con l'obiettivo di trarre insegnamenti operativi e strategici, utili per prevenire o mitigare eventi simili in futuro. Al termine della procedura, ENISA redige una relazione ufficiale, che viene trasmessa a EU-CyCLONe, alla rete dei CSIRT, agli Stati membri coinvolti e alla Commissione europea, contribuendo così al miglioramento continuo del sistema europeo di cybersicurezza. Il Cyber Solidarity Act si configura come un'iniziativa ambiziosa e lungimirante, volta a dotare l'Unione Europea di strumenti operativi concreti per fronteggiare le minacce informatiche più gravi in modo tempestivo, coordinato ed efficace, rafforzando la solidarietà tra gli Stati membri e garantendo un approccio comune e integrato alla sicurezza cibernetica a livello europeo.

3.1.5 Il futuro della Cibersecurity in UE tra Digital Networks Act e rapporto Draghi

Il futuro della cybersicurezza in Unione Europea si intreccia in maniera sempre più evidente con le dinamiche evolutive delle infrastrutture digitali e delle reti di telecomunicazione, come dimostrato dai più recenti sviluppi normativi e strategici. In tale contesto, il Digital Connectivity Package, pubblicato dalla Commissione europea il 21 febbraio 2024, rappresenta una tappa significativa. Il pacchetto comprende il libro bianco "How to master Europe's digital infrastructure needs?" [63] e

una raccomandazione per la sicurezza e resilienza delle infrastrutture sottomarine, documenti orientati a rafforzare la capacità dell'Unione di rispondere alle sfide digitali, infrastrutturali e geopolitiche del prossimo decennio. Il White Paper, in particolare, evidenzia la correlazione tra lo sviluppo delle infrastrutture di telecomunicazioni e la competitività dell'UE, sottolineando il ritardo rispetto ad altre economie avanzate come USA, Cina e Corea del Sud, sia in termini di copertura in fibra ottica che nello sviluppo delle reti 5G standalone. Il documento descrive una serie di azioni strategiche volte a colmare tali lacune, promuovendo la transizione dalle reti in rame alle reti in fibra ottica, lo sviluppo delle reti 5G e delle soluzioni cloud, nonché la promozione delle tecnologie emergenti come edge computing e intelligenza artificiale. Tra le proposte avanzate, si segnalano tre direttrici di intervento strategico:la creazione di un "NextGen Network Hub", Il completamento del Mercato Unico Digitale, la realizzazione di infrastrutture digitali sicure e resilienti. Parallelamente, il rapporto "The future of European competitiveness", redatto da Mario Draghi su incarico della Commissione europea e presentato il 9 settembre 2024 [64], offre un'analisi di ampio respiro sulla competitività dell'UE nel contesto globale. Tra i temi centrali figurano: la riduzione del divario di innovazione con USA e Cina, la promozione di un piano comune per la decarbonizzazione e l'aumento della sicurezza e dell'autonomia strategica europea. Il documento evidenzia il ritardo dell'Europa in settori chiave come il cloud e l'intelligenza artificiale, e propone un piano d'azione per rafforzare la competitività europea, promuovere la digitalizzazione e ridurre la dipendenza tecnologica da Paesi terzi. Grande attenzione è dedicata al tema della cybersicurezza, considerata una dimensione imprescindibile della competitività. Il rapporto sollecita un rafforzamento della sovranità tecnologica dell'UE, attraverso il sostegno a fornitori europei di apparati e software, l'introduzione di criteri di sicurezza nell'assegnazione dello spettro, e l'inclusione di fornitori europei nelle negoziazioni commerciali internazionali. In ultima analisi, sia il libro bianco che il rapporto Draghi convergono su una visione condivisa: l'Europa necessita di un nuovo modello di governance digitale, capace di integrare sicurezza, innovazione, investimenti e semplificazione normativa, al fine di colmare i ritardi accumulati, rilanciare la competitività e costruire un'autentica sovranità digitale europea.

3.2 L'ecosistema normativo nazionale

3.2.1 L'ACN e la strategia italiana di cybersicurezza

Nel quadro del rafforzamento delle politiche nazionali in materia di cybersicurezza, l'Italia ha avviato un processo di profonda riorganizzazione istituzionale e normativa, sostenuto anche dal Piano Nazionale di Ripresa e Resilienza (PNRR), che ha previsto investimenti specifici volti alla

creazione e al potenziamento delle infrastrutture cibernetiche. Tra le iniziative più significative, si colloca l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), avvenuta con il D.L. n. 82/2021, convertito con legge n. 109/2021 [65], che ha segnato l'avvio di una nuova fase nella governance italiana del dominio cibernetico. L'ACN è l'autorità nazionale competente per la cybersicurezza, responsabile della protezione delle infrastrutture critiche, della resilienza dei servizi essenziali e della tutela degli interessi nazionali da minacce cibernetiche. Rappresenta oggi il fulcro della strategia nazionale di cybersicurezza, con funzioni di coordinamento, supervisione, vigilanza e attuazione ed è investita del compito di predisporre e attuare la strategia nazionale di cybersicurezza, di promuovere azioni comuni tra soggetti pubblici e privati, di fungere da punto di contatto unico per le reti e i sistemi informativi, nonché di esercitare competenze in materia di certificazione, ispezione, conformità e sanzione. Contestualmente, viene definitivamente superato il precedente modello frammentato, con l'accentramento in capo all'Agenzia di competenze precedentemente attribuite a diversi ministeri e autorità. A livello operativo, l'ACN è affiancata da strutture chiave come il Comitato interministeriale per la cybersicurezza (CIC), con funzioni consultive, propositive e di alta vigilanza sulle politiche nazionali, e del Nucleo per la cybersicurezza, operativo presso la Presidenza del Consiglio, con il compito di supportare la gestione delle crisi cibernetiche, promuovere esercitazioni interministeriali e coordinare la risposta in caso di minacce sistemiche. Oltre all'attività operativa e regolatoria, l'ACN è incaricata anche della promozione della cultura della cybersicurezza, della formazione e della ricerca. A tal fine, si avvale del Comitato tecnico-scientifico (CTS) che fornisce indirizzi strategici e garantisce il coordinamento delle politiche nazionali di cybersicurezza. Ulteriori supporti provengono dal CSIRT Italia, incaricato di monitorare e rispondere agli incidenti informatici, dal Centro di Valutazione e Certificazione Nazionale (CVCN), responsabile della sicurezza dei prodotti e servizi TIC. Nel maggio 2022 è stata presentata la Strategia nazionale di cybersicurezza 2022–2026, accompagnata da un articolato Piano di implementazione [66], che si fonda su una visione integrata che riconosce la centralità della cybersicurezza nella transizione digitale del Paese e mira a conseguire l'autonomia strategica nazionale attraverso il rafforzamento della resilienza, la protezione dei diritti fondamentali e la promozione della fiducia dei cittadini. La strategia definisce 82 misure specifiche, accompagnate da indicatori di performance (KPI) per monitorare l'attuazione e l'efficacia delle azioni previste. Il piano identifica tre macro-obiettivi:

- Protezione delle infrastrutture critiche: rafforzamento delle capacità di difesa cibernetica, messa in sicurezza delle infrastrutture critiche, promozione della crittografia e della sicurezza delle supply chain ICT, contrasto alla disinformazione;

- Risposta alle minacce cibernetiche: sviluppo di un sistema nazionale di gestione delle crisi cibernetiche, potenziamento dei servizi cyber, promozione di esercitazioni e miglioramento della cooperazione transnazionale, nonché contrasto al cybercrime e rafforzamento della capacità di deterrenza;
- Sviluppo delle capacità nazionali: promozione dell'industria e della ricerca in ambito cyber, creazione del Parco nazionale della cybersicurezza, internazionalizzazione delle imprese, impulso all'innovazione e sostegno alle tecnologie emergenti (cloud, edge, blockchain, spazio, quantum computing).

Trasversali a tali obiettivi, figurano i fattori abilitanti, in particolare: la formazione che comprende percorsi di istruzione specialistica, ITS, alternanza scuola-lavoro, certificazioni delle competenze, programmi per il personale pubblico e privato; e cooperazione, ossia il rafforzamento della presenza nei consessi internazionali, tavoli operativi con i soggetti del perimetro di sicurezza, capacity building per Paesi terzi. A completamento del modello, la strategia si basa su un approccio 'whole of society' prevede l'attivazione di una Partnership Pubblico-Privata (PPP) come elemento trasversale e abilitante per coinvolgere attivamente imprese, accademia, enti di ricerca e società civile, con l'obiettivo di realizzare un ecosistema nazionale pienamente resiliente e competitivo a livello europeo.

3.2.2 La direttiva del NIS2 in Italia

Il quadro normativo nazionale in materia di cybersicurezza si è notevolmente ampliato negli ultimi anni, anche per impulso del legislatore eurounitario. In tale contesto si colloca il decreto legislativo 4 settembre 2024, n. 138, con cui l'Italia ha recepito la direttiva (UE) 2022/2555, nota come NIS2, risultando tra i primi Stati membri ad aver adottato formalmente il nuovo quadro regolatorio [67]. Il decreto, entrato in vigore il 16 ottobre 2024, ha introdotto un'articolata disciplina volta a rafforzare la resilienza dei soggetti pubblici e privati che operano in settori considerati critici per il funzionamento e la sicurezza dello Stato e del mercato interno. Il Decreto Legislativo NIS2 si applica a una vasta gamma di soggetti pubblici e privati che operano nei settori critici indicati negli allegati della direttiva, tra cui energia, trasporti, telecomunicazioni, finanza, sanità e infrastrutture digitali. Questi soggetti, definiti come "essenziali" o "importanti" a seconda della loro rilevanza, sono tenuti a garantire la sicurezza dei propri sistemi informativi e a rispettare specifiche misure di protezione e resilienza. È previsto un sistema di esenzioni per determinate categorie di organizzazioni, in particolare quelle di dimensioni ridotte, per le quali l'impatto di un eventuale incidente sarebbe limitato. La governance nazionale della NIS2 conferma il ruolo centrale

dell'Agenzia per la Cybersicurezza Nazionale (ACN), che agisce quale autorità nazionale competente e punto di contatto unico, con la responsabilità di coordinare le attività di cybersicurezza a livello nazionale, supportare i soggetti obbligati e monitorare l'attuazione delle misure previste dalla direttiva. A supporto dell'ACN, il decreto identifica una serie di Autorità settoriali (Ministeri) per i vari ambiti di applicazione, tra cui la Presidenza del Consiglio dei ministri per i settori delle tecnologie dell'informazione e della comunicazione (TIC), spazio e pubblica amministrazione. È inoltre istituito il tavolo per l'attuazione della disciplina NIS, una piattaforma permanente di confronto tra le istituzioni, il mondo accademico, enti di ricerca e operatori privati, con l'obiettivo di formulare proposte, pareri e linee guida per una corretta applicazione della normativa. Sul piano operativo, il decreto prevede che i soggetti essenziali e importanti debbano registrarsi sulla piattaforma digitale dell'ACN dal 1° gennaio al 28° febbraio di ogni anno, fornendo informazioni aggiornate sui propri sistemi informativi e sulle misure di sicurezza adottate. Questi soggetti devono inoltre adottare misure tecniche e organizzative adeguate a proteggere le proprie reti e sistemi informativi, garantire la gestione delle vulnerabilità, prevenire gli incidenti e, in caso di violazione, procedere a una tempestiva notifica degli incidenti significativi all'ACN. L'ACN è incaricata di definire i termini, le modalità e i criteri di segnalazione, con la possibilità di emettere linee guida e raccomandazioni vincolanti per supportare i soggetti obbligati. Una novità di rilievo è rappresentata dalla possibilità per l'ACN di imporre l'uso di prodotti, servizi e processi TIC certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza previsti dal Cybersecurity Act (Regolamento UE 2019/881) [68]. Qualora tali sistemi non siano ancora disponibili, l'ACN può richiedere l'adozione di schemi di certificazione riconosciuti a livello nazionale o europeo, rafforzando così la fiducia e la sicurezza dei prodotti digitali utilizzati nel Paese. Il decreto stabilisce anche un sistema di vigilanza e sanzioni, affidato all'ACN, che ha il compito di monitorare il rispetto degli obblighi da parte dei soggetti essenziali e importanti, supportata dalle Autorità settoriali competenti. In caso di violazione, sono previste sanzioni amministrative proporzionate alla gravità dell'infrazione e, nei casi più gravi, la possibilità di sospendere o limitare l'attività del soggetto interessato. In tale direzione si inserisce anche la legge 28 giugno 2024, n. 90 [69], recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici". che introduce l'obbligo, per i soggetti pubblici e privati interessati, di adottare tempestivamente le misure correttive indicate da ACN in relazione a vulnerabilità specifiche. In caso di inadempimento reiterato, è prevista l'applicazione di sanzioni pecuniarie, salvo la dimostrazione di oggettive motivazioni tecnico-organizzative. Quanto al percorso di implementazione della NIS2, l'ACN ha avviato un piano triennale strutturato in tre fasi:

- Prima Fase (dicembre 2024 - aprile 2025): registrazione dei soggetti obbligati sulla piattaforma ACN, avvio dei tavoli settoriali, censimento dei soggetti e notifica degli obblighi di base.
- Seconda Fase (aprile 2025 - aprile 2026): notifica degli incidenti, definizione degli obblighi di sicurezza a lungo termine, categorizzazione delle attività e dei servizi.
- Terza Fase (da aprile 2026): piena attuazione delle misure di sicurezza e monitoraggio continuo da parte dell'ACN.

Infine, il decreto prevede specifiche norme di coordinamento con la legge sulla cybersicurezza nazionale (legge 28 giugno 2024, n. 90), che introduce ulteriori obblighi di gestione delle vulnerabilità e sanzioni per la mancata adozione di misure correttive. Questo rafforzamento normativo mira a garantire un livello elevato di sicurezza delle reti e dei sistemi informativi italiani, in linea con gli standard europei.

3.2.3 Il Perimetro di Sicurezza Nazionale Cybernetica (PSNC)

Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è uno strumento normativo fondamentale per la protezione delle infrastrutture critiche e dei servizi essenziali in Italia. Istituito con il Decreto-Legge 21 settembre 2019, n. 105, convertito con la Legge 133/2019 [70], il PSNC mira a garantire un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche e degli operatori privati che forniscono servizi essenziali per la società e l'economia del Paese. Tali servizi sono considerati fondamentali per la sicurezza nazionale e il loro malfunzionamento o utilizzo improprio potrebbe compromettere la sicurezza dello Stato. La disciplina del PSNC prevede una serie di obblighi per i soggetti pubblici e privati inclusi nel perimetro, definiti sulla base di criteri tecnici e strategici. Tra questi obblighi, il più rilevante è la necessità di predisporre un elenco dei beni ICT (Information and Communication Technology), che identifica le reti, i sistemi e i servizi informatici ritenuti essenziali per il funzionamento dell'organizzazione e che devono essere protetti da misure di sicurezza specifiche. I soggetti inclusi nel PSNC sono tenuti ad aggiornare questo elenco su base periodica, segnalando eventuali modifiche all'Agenzia per la Cybersicurezza Nazionale (ACN). Il Centro di Valutazione e Certificazione Nazionale (CVCN) svolge un ruolo cruciale nel PSNC, poiché è responsabile della valutazione dei beni e dei servizi ICT utilizzati dai soggetti inclusi nel perimetro. Le procedure di valutazione prevedono tre fasi: la verifica preliminare dei beni ICT, la preparazione dei test e l'esecuzione delle prove tecniche sui beni ICT, che devono soddisfare requisiti di sicurezza stabiliti. L'obiettivo è garantire che i prodotti e i servizi ICT utilizzati nelle infrastrutture critiche siano sicuri

e privi di vulnerabilità note. Il PSNC prevede anche un sistema di notifiche degli incidenti di sicurezza informatica, che devono essere segnalati al CSIRT Italia entro un termine stabilito. Gli incidenti sono classificati in base alla loro gravità e impatto, e le informazioni fornite nella notifica devono essere sufficienti a consentire una rapida valutazione e gestione della crisi. Questa procedura consente di monitorare e gestire in modo coordinato gli incidenti di sicurezza a livello nazionale, garantendo una risposta tempestiva ed efficace. I soggetti inclusi nel PSNC devono adottare misure di sicurezza per garantire l'integrità, la disponibilità e la riservatezza dei loro sistemi informativi, nonché segnalare tempestivamente eventuali incidenti al CSIRT Italia. Questi obblighi si sovrappongono a quelli previsti dalla Direttiva NIS2, garantendo una protezione multilivello per i servizi essenziali. Il PSNC prevede anche la possibilità di imporre controlli di sicurezza sui fornitori di prodotti e servizi ICT utilizzati dai soggetti inclusi nel perimetro. Questa attenzione alla supply chain è fondamentale per prevenire l'introduzione di vulnerabilità attraverso software o hardware non sicuri. In particolare, i fornitori possono essere soggetti a valutazioni di sicurezza condotte dal CVCN e dai laboratori accreditati, e i prodotti che non superano queste verifiche non possono essere utilizzati. Dal punto di vista operativo, l'ACN svolge un ruolo centrale nel coordinare le attività di attuazione del PSNC, fornendo supporto tecnico e normativo ai soggetti inclusi nel perimetro e monitorando il rispetto degli obblighi di sicurezza. Questo approccio garantisce un controllo centralizzato e una gestione coordinata delle minacce cibernetiche, migliorando la resilienza complessiva del Paese alle minacce informatiche. Quindi, il PSNC rappresenta una componente essenziale della strategia italiana per la cybersicurezza, garantendo la protezione delle infrastrutture critiche e dei servizi essenziali. Attraverso un sistema articolato di obblighi, controlli e sanzioni, il PSNC contribuisce a rafforzare la sicurezza delle reti e dei sistemi informativi italiani, promuovendo un approccio basato sulla prevenzione, la gestione del rischio e la resilienza.

3.2.4 La legge nazionale sulla cybersicurezza

La legge 28 giugno 2024, n. 90, conosciuta come "legge sulla cybersicurezza", ha introdotto nuove e più stringenti disposizioni per rafforzare la sicurezza informatica nel contesto nazionale [71]. Essa si applica a soggetti pubblici e privati già sottoposti alla disciplina NIS2 e al Perimetro di Sicurezza Nazionale Cibernetica (PSNC), imponendo obblighi specifici per la gestione delle vulnerabilità e delle minacce cyber. La legge introduce una serie di adempimenti cogenti, principalmente rivolti ai soggetti già ricompresi nel perimetro applicativo della NIS2, prevedendo:

- L'istituzione di una struttura interna per la cybersicurezza, anche coincidente con l'ufficio del responsabile per la transizione digitale, incaricata di sviluppare politiche di sicurezza,

definire ruoli e responsabilità, adottare misure tecniche, e monitorare costantemente minacce e vulnerabilità.

- La nomina di un referente per la cybersicurezza, con specifiche competenze, incaricato di fungere da punto di contatto unico con l'ACN e di coordinare l'attuazione degli obblighi anche previsti da altre normative (NIS2, PSNC). Tale referente può anche essere individuato tra figure esistenti nell'organico dell'ente o proveniente da un'altra PA.
- L'obbligo di notifica degli incidenti cyber entro 24 ore dalla conoscenza dell'evento, seguito da una segnalazione completa entro 72 ore. Le tempistiche di attuazione variano tra PA centrali e altri soggetti pubblici.
- L'obbligo di adottare interventi correttivi indicati dall'ACN per la risoluzione di specifiche vulnerabilità entro 15 giorni dalla ricezione della comunicazione. Il mancato adempimento può comportare sanzioni fino a 125.000 euro, oltre a responsabilità disciplinari e contabili per i funzionari coinvolti.

Nonostante l'obiettivo condivisibile di consolidare la postura cibernetica nazionale, la legge presenta alcune criticità applicative, in particolare legate alla clausola di invarianza finanziaria, che rischia di ostacolare l'effettiva implementazione nelle amministrazioni pubbliche. Analogamente, il termine ristretto per l'adozione di misure correttive può risultare problematico soprattutto per il settore privato e in presenza di vulnerabilità complesse, come le cosiddette 0-day, che richiedono interventi tecnici complessi e tempestivi. Nel complesso, la L. 90/2024 si configura come un elemento di rafforzamento e razionalizzazione normativa, che mira a garantire una maggiore omogeneità tra discipline esistenti, e a migliorare la resilienza cibernetica dell'ecosistema nazionale, anche attraverso un approccio preventivo e coordinato tra soggetti pubblici, privati e ACN. L'evoluzione del quadro normativo europeo e nazionale in materia di cybersicurezza riflette la crescente consapevolezza dell'importanza della sicurezza digitale in un contesto sempre più interconnesso. Dalla direttiva NIS2 al Cybersecurity Act, dal Perimetro di Sicurezza Nazionale Cibernetica alla legge nazionale sulla cybersicurezza, l'Italia ha progressivamente costruito un sistema di protezione articolato, volto a garantire la resilienza delle infrastrutture critiche, la tutela dei dati e la gestione delle minacce cibernetiche. Questo complesso ecosistema normativo impone ai soggetti pubblici e privati obblighi stringenti in termini di sicurezza dei sistemi informativi, gestione delle vulnerabilità e segnalazione degli incidenti. Tali disposizioni mirano a promuovere un approccio proattivo alla sicurezza, che non si limiti alla reazione agli attacchi, ma si estenda alla prevenzione e alla gestione del rischio. L'obbligo di conformità normativa si traduce così in un'opportunità per le aziende di rafforzare la propria resilienza cibernetica e migliorare la gestione

del rischio. La presenza di un quadro normativo chiaro e armonizzato offre una guida per l'implementazione di misure di sicurezza efficaci, mentre il supporto dell'Agenzia per la Cybersicurezza Nazionale (ACN) e degli altri organismi competenti consente alle organizzazioni di ricevere assistenza e orientamento. Per le imprese, l'integrazione del Cyber Risk Management nei processi aziendali rappresenta non solo un requisito di compliance, ma un vero e proprio fattore competitivo. Un'efficace gestione del rischio cyber permette infatti di proteggere il patrimonio informativo, garantire la continuità operativa, preservare la fiducia dei clienti e degli stakeholder e minimizzare l'impatto economico e reputazionale di eventuali incidenti. Nel capitolo successivo, l'analisi si concentrerà proprio su come le aziende possono strutturare un sistema di Cyber Risk Management, partendo dalla definizione delle strategie di sicurezza fino all'implementazione delle contromisure operative, con particolare attenzione agli strumenti di monitoraggio, alla gestione delle vulnerabilità e alla risposta agli incidenti.

4. Modello di Cyber Risk Management: Strategie, Processi e Capability

4.1 Modello di Cyber Risk Management (ERM)

In un contesto caratterizzato da minacce informatiche sempre più sofisticate e pervasive, la capacità di un'organizzazione di individuare, valutare e mitigare in modo sistematico i rischi cibernetici rappresenta un requisito essenziale per garantire la continuità operativa, la protezione delle informazioni e la resilienza complessiva. Il Cyber Risk Management si inserisce proprio in questa prospettiva, configurandosi come una disciplina strategica che integra la gestione del rischio nella governance aziendale, favorendo un approccio proattivo e consapevole alla sicurezza informatica. Il cyber Risk Management consiste nell'insieme di attività, politiche e processi finalizzate alla gestione del rischio cyber dell'organizzazione ad un livello per essa accettabile [72]. Il dominio comprende tutte le attività di definizione, gestione e mantenimento di un programma di cyber risk management, che sono volte a identificare, analizzare e gestire i rischi informatici a cui l'organizzazione è soggetta. In particolare, nell'ambito di queste attività si fa riferimento al concetto di rischio cyber, che secondo il framework *Cybersecurity Capability Maturity Model (C2M2)* può essere definito come la possibilità che si verifichino danni o perdite derivanti da accessi non autorizzati, utilizzo improprio, divulgazione, interruzione, modifica o distruzione di risorse IT, OT o di informazioni sensibili [73]. Tale definizione sottolinea come il rischio cyber non riguardi esclusivamente la componente tecnologica, ma coinvolga anche aspetti organizzativi, procedurali e umani. Va evidenziato che, per sua natura, il rischio cibernetico non può essere completamente eliminato: può tuttavia essere ridotto e gestito attraverso l'adozione di adeguate misure di sicurezza,

capaci di agire su due variabili fondamentali che sono la probabilità di accadimento e l'impatto potenziale di un evento dannoso. La capacità di un'organizzazione di mitigare efficacemente questi fattori rappresenta un indicatore cruciale di maturità nel campo della cybersecurity e costituisce un presupposto essenziale per la resilienza complessiva di sistemi e processi aziendali. L'impossibilità di azzerare completamente il rischio cyber rappresenta una delle più grandi sfide per ogni organizzazione ed è legata a tre motivazioni principali, tra loro strettamente interconnesse:

- *necessità operative*: le attività operative di un'organizzazione comportano inevitabilmente dei rischi, poiché alcune funzionalità essenziali, come la gestione delle utenze o la condivisione di informazioni, rappresentano potenziali vulnerabilità. Per questa ragione, la gestione del rischio si traduce nell'adozione di misure come l'impiego del numero minimo di utenze necessarie, l'applicazione del principio del minimo privilegio, assegnando a ciascun utente solo i permessi indispensabili, e l'implementazione di sistemi di autenticazione sicuri. Queste misure riducono la superficie d'attacco e mantengono il rischio entro livelli accettabili senza compromettere l'operatività.
- *Mutevolezza del contesto*: le tecniche di attacco informatico evolvono continuamente, emergono nuove vulnerabilità e gli attori malevoli adattano in modo rapido le proprie strategie. Di conseguenza, anche i sistemi di difesa più avanzati non possono garantire una protezione assoluta. Tale dinamicità implica che il rischio cyber, per quanto gestito e mitigato, non possa mai essere completamente eliminato, ma soltanto contenuto entro soglie di rischio accettabili.
- *Limitatezza delle risorse***:** le attività di cybersicurezza richiedono investimenti significativi in termini di risorse economiche, competenze specialistiche e infrastrutture tecnologiche. Tuttavia, tali risorse sono per definizione limitate, specialmente nel caso di organizzazioni di piccole e medie dimensioni. Ne deriva la necessità di stabilire priorità strategiche, orientando gli interventi verso le aree di maggiore criticità e valutando attentamente il rapporto costi-benefici di ogni misura adottata. Non sempre, infatti, l'investimento in una nuova tecnologia o in un livello di protezione più elevato risulta economicamente sostenibile in relazione alla riduzione del rischio effettivamente conseguibile**.**

Il dominio di Cyber Risk Management riveste un ruolo centrale sotto due differenti prospettive. In primo luogo, rappresenta un elemento chiave per la definizione degli obiettivi di lungo periodo all'interno della strategia di cybersicurezza. La determinazione degli obiettivi dipende in larga misura dal livello di rischio che l'organizzazione è disposta a tollerare, ossia dalla sua propensione al rischio. In base a questa propensione, vengono stabiliti valori soglia o obiettivi specifici per

ciascuna tipologia di rischio identificata; la strategia di cybersicurezza deve quindi essere orientata al raggiungimento di tali valori o, preferibilmente, al mantenimento dei livelli di rischio al di sotto di essi [74]. In secondo luogo, esso rappresenta la base informativa e metodologica per orientare le scelte di sviluppo delle capability afferenti agli altri domini della sicurezza informatica. La scelta delle capability da sviluppare, così come il livello di maturità da perseguire per ciascuna di esse, dipende dalla natura e dall'entità del rischio cyber cui l'organizzazione risulta esposta. Ad esempio, un'organizzazione che gestisce un elevato numero di utenze e credenziali di accesso sarà naturalmente portata a rafforzare le capability legate all'Identity and Access Management (IAM), così da ridurre la probabilità di compromissione attraverso account non adeguatamente protetti. Il dominio del Cyber Risk Management si configura, quindi, come un presupposto essenziale sia per definire obiettivi realistici e misurabili di cybersicurezza, sia per individuare e implementare gli strumenti più idonei al loro conseguimento. Lo sviluppo efficace delle attività in questo ambito è frequentemente supportato dall'adozione di framework strutturati, in grado di guidare l'organizzazione lungo tutte le fasi del processo di gestione del rischio. Tra i riferimenti di maggiore rilievo si possono menzionare lo standard internazionale ISO/IEC 27005 [75], specificamente dedicato alla gestione del rischio in ambito sicurezza delle informazioni, oppure il Risk Management Framework (RMF) elaborato dal National Institute of Standards and Technology (NIST) [76] ampiamente adottato come best practice in contesti internazionali.

4.2 Il processo circolare di gestione del rischio cyber: un approccio volto al miglioramento continuo

L'approccio alla gestione del rischio cyber si fonda, generalmente, su un modello di natura ciclica, in cui le diverse attività sono strettamente interconnesse in un processo di miglioramento continuo. In questo schema, gli output di ciascuna fase costituiscono gli input per la fase successiva, consentendo un adattamento costante delle strategie di mitigazione alle evoluzioni del contesto operativo e delle minacce. Il modello di riferimento è quello noto come ciclo di Deming o Plan-Do-Check-Act (PDCA), che costituisce la base logica di diversi standard e framework riconosciuti a livello internazionale per la gestione del rischio, tra cui la ISO/IEC 27005 e il Risk Management Framework for Information Systems and Organizations [77] pubblicato dal NIST. Questo approccio metodologico garantisce coerenza, sistematicità e una continua verifica dell'efficacia delle misure adottate. Le quattro fasi del ciclo di Deming si articolano come segue:

- *Plan*: in questa fase preliminare, l'organizzazione identifica i rischi cyber potenziali che potrebbero influire sulle proprie attività, valutandone la probabilità di accadimento e

l'impatto potenziale. Sulla base di tale analisi vengono definiti obiettivi chiari in termini di livello di rischio accettabile e pianificate le strategie di mitigazione più adeguate a contenerlo entro soglie sostenibili.

- *Do*: la seconda fase riguarda l'implementazione concreta delle strategie di risposta al rischio definite nella fase di pianificazione. In questo momento si mettono in atto misure tecniche, organizzative e procedurali volte a ridurre il rischio cyber, garantendo la corretta allocazione delle risorse e il coinvolgimento delle funzioni aziendali competenti.
- *Check*: una volta implementate le azioni di mitigazione, è essenziale procedere con il monitoraggio continuo dell'efficacia delle misure adottate. In questa fase si raccolgono e si analizzano dati significativi, confrontando i risultati ottenuti con gli obiettivi prefissati. Tale verifica permette di identificare eventuali scostamenti o aree di miglioramento.
- *Act*: l'ultima fase prevede l'adozione di azioni correttive e di miglioramento, basate sui risultati della fase di controllo. Le strategie di gestione del rischio vengono aggiornate e adattate per rispondere ai cambiamenti del contesto organizzativo, alle nuove minacce emergenti o alle carenze riscontrate, alimentando così un ciclo virtuoso di apprendimento e rafforzamento continuo.

L'applicazione del modello PDCA al Cyber Risk Management consente di trasformare la gestione del rischio in un processo dinamico e proattivo, in grado di evolvere insieme alle esigenze dell'organizzazione e alle sfide poste dal contesto digitale contemporaneo.

4.2.1 Sviluppo di capability: costruzione delle capacità operative

Sviluppare capability di cybersicurezza all'interno del dominio del Cyber Risk Management significa mettere in atto un insieme articolato di attività finalizzate a garantire un approccio strutturato, continuo ed efficace alla gestione del rischio cibernetico. Queste attività costituiscono la base su cui si fonda la capacità di un'organizzazione di individuare, valutare e mitigare in modo adeguato le minacce informatiche, assicurando al contempo una comunicazione trasparente e una gestione coerente delle vulnerabilità interne ed esterne. In particolare, tra le attività principali riconducibili a questo dominio è possibile identificare quattro aree fondamentali di intervento:

- identificazione e analisi del rischio cyber;
- gestione del rischio cyber;
- comunicazione del rischio cyber;
- gestione del rischio cyber di terze parti.

Nel loro complesso, queste attività contribuiscono a consolidare la maturità del Cyber Risk Management, rafforzando la resilienza dell'organizzazione di fronte a scenari di rischio in continua evoluzione.

4.2.2 Identificazione e analisi del rischio cyber

Il processo inizia con una fase preliminare di analisi del contesto, attraverso un pre-assessment mirato a individuare i domini interni ed esterni rilevanti per l'organizzazione. Tale analisi contestuale permette di comprendere l'ambiente operativo in cui l'organizzazione si colloca, identificando fattori interni, come risorse, processi e asset critici, ed esterni, quali fornitori, stakeholder e normative di riferimento, che possono influire sul livello di esposizione al rischio [78]. Successivamente, si procede con la valutazione degli impatti sui principi di Riservatezza, Integrità e Disponibilità delle informazioni gestite da ciascun servizio, tramite una Business Impact Analysis (BIA) [79]. Questa attività consente di stimare in modo oggettivo le conseguenze di un eventuale incidente di sicurezza, fornendo una base solida per stabilire le priorità di intervento e pianificare le misure di mitigazione più adeguate. La valutazione del rischio (Risk Assessment) si articola in tre fasi principali: identificazione del rischio (Risk Identification), analisi del rischio (Risk Analysis) e valutazione finale (Risk Evaluation) che di seguito verranno approfondite:

- Identificazione del rischio**:** rappresenta la fase in cui il rischio viene identificato, riconosciuto e descritto. L'output di tale attività è una lista strutturata di rischi relativi a diversi eventi di cybersicurezza che possono verificarsi. In tale fase è possibile utilizzare due tipologie di approcci:
  - *Approccio basato sulle minacce*: si fonda sull'analisi di scenari potenzialmente dannosi, considerando le minacce rilevanti in relazione al contesto organizzativo, le vulnerabilità sfruttabili e le motivazioni e capacità degli attori malevoli. Questo approccio, di tipo scenario-based, consente di modellare situazioni realistiche, evidenziando le possibili catene di eventi che possono portare a un incidente.

  - *Approccio basato sugli asset*: **s**i concentra sull'identificazione degli asset informativi (hardware, software, dati, persone) e sulla loro classificazione in base alla criticità e al valore per l'organizzazione. Questo metodo prevede l'analisi congiunta di asset, vulnerabilità e minacce, al fine di individuare specifiche misure di protezione. L'approccio asset-based è ampiamente riconosciuto come modello concettuale di riferimento in numerosi standard internazionali.

In questa fase risulta di cruciale importanza l'utilizzo di processi e strumenti come gli asset inventory e i threat inventory. L'utilizzo di questi strumenti è particolarmente utile poiché il rischio cyber nasce dall'interazione tra asset, vulnerabilità e minacce. In particolare, il rischio si manifesta quando una minaccia informatica sfrutta una vulnerabilità su un asset dell'organizzazione e, per questo motivo, l'identificazione del rischio può avvenire partendo sia dall'analisi delle vulnerabilità sugli asset, sia dall'esame delle minacce potenziali.

- Analisi del rischio**:** tale fase ha lo scopo di determinare il livello di rischio associato a ciascun evento individuato. Per fare ciò occorre definire le due variabili fondamentali: impatto e probabilità. Dalla loro interazione un valore complessivo che guida l'organizzazione nella definizione delle priorità di intervento e delle misure di mitigazione più adeguate. L'impatto rappresenta l'entità del danno che può essere calcolato attraverso una stima di variabili quantitative e qualitative, tra cui:
  - *Costo di ripristino*: comprende l'insieme dei costi che devono essere sostenuti per riportare i sistemi alla situazione esistente prima del verificarsi dell'evento negativo associato al rischio.
  - *Perdite finanziarie ed economiche*: una stima dell'ammontare di risorse finanziarie ed economiche che possono essere associate al verificarsi dell'evento di rischio, come interruzioni delle attività o perdita di opportunità di business.
  - *Costo operativo*: inteso come l'impatto negativo sull'operatività in termini di tempi di fermo dei sistemi e ammontare di dati compromessi e/o persi. [80]

La probabilità di accadimento di un evento rappresenta la stima di quanto è realistico che una specifica minaccia si concretizzi sfruttando una vulnerabilità. Tale stima rimane inevitabilmente soggettiva, in quanto non esiste una metodologia di calcolo universalmente accettata; essa dipende dai fattori considerati e dal contesto organizzativo di riferimento.

Tra i principali fattori che possono incidere sulla probabilità si possono annoverare:

- livello di efficacia dei controlli esistenti: un buon sistema di presidi di sicurezza interni può ridurre la probabilità che si verifichi l'evento sfavorevole del quale si sta valutando il rischio;

- vantaggio potenziale dell'attaccante: la probabilità di un attacco dipende dal tipo di organizzazione e dai dati da proteggere. Dati sensibili, come credenziali bancarie, attirano gli attaccanti, rendendo probabili attacchi mirati, ad esempio tramite phishing verso utenti con accesso privilegiato.
- numero e tipologia di vulnerabilità**: l**a probabilità di un evento cyber aumenta con il numero e la gravità delle vulnerabilità nei sistemi, come falle o configurazioni errate.

La stima di impatto e probabilità può essere realizzata attraverso diverse metodologie, che le organizzazioni scelgono e personalizzano in base al contesto e al livello di maturità del proprio sistema di gestione del rischio. L'Analisi qualitativa si basa prevalentemente sul giudizio soggettivo degli esperti che mediante interviste, questionari, scenari o checklist, assegnano punteggi a ciascun rischio utilizzando scale qualitative come "basso", "medio", "alto" o "critico". L'analisi quantitativa, invece, fa ricorso a funzioni matematiche e modelli statistici per stimare in termini numerici sia la probabilità sia l'impatto, fornendo risultati più oggettivi e facilmente interpretabili. Infine, è possibile adottare una metodologia mista, che combina principi e strumenti delle due tipologie precedenti, utilizzando variabili qualitative e quantitative in modo integrato per ottenere una caratterizzazione più articolata e completa dei rischi da monitorare. In questa fase, attraverso le metodologie sopra descritte, vengono definiti il "Risk Appetite" e la "Risk Tolerance" [81] e raffigurati nella tabella 9. Il primo rappresenta la quantità di rischio che un'organizzazione è disposta ad accettare per raggiungere i propri obiettivi strategici, mentre il secondo rappresenta il livello accettabile di variazione relativo al raggiungimento di specifici obiettivi ovvero la deviazione massima dal Risk Appetite consentita. La chiarezza e la condivisione di questi parametri guidano tutte le decisioni successive di gestione e trattamento del rischio.

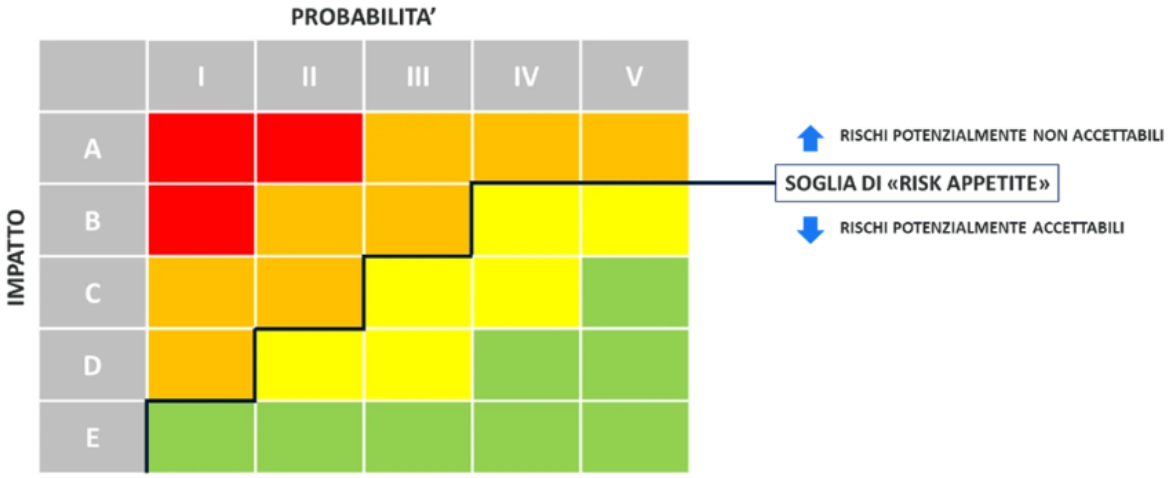

Figura 9 Rappresentazione della soglia di Risk Appetite

Questi valori rappresentano, per l'organizzazione, rispettivamente l'obiettivo da perseguire e il massimo livello di rischio a cui può essere esposta. La loro determinazione deve tenere in considerazione fattori come ad esempio, requisiti normativi, vincoli finanziari, opportunità organizzative, obiettivi organizzativi, rapporti con i fornitori.

- Attività di valutazione del rischio:

L'attività rappresenta la fase conclusiva del processo di analisi, attraverso la quale l'organizzazione determina il livello di rischio inerente, ossia il rischio a cui risulta esposta prima dell'adozione di qualsiasi misura di mitigazione [82]. Questo valore esprime la perdita massima potenziale qualora l'evento si verificasse senza l'attuazione di interventi preventivi o correttivi. Il livello di rischio inerente deve essere confrontato con il risk appetite dell'organizzazione, ovvero con il livello di rischio che la stessa ritiene accettabile in funzione dei propri obiettivi strategici. Qualora il rischio stimato superi tale soglia di tolleranza, si rende necessario pianificare e attuare interventi di gestione appropriati. In questo contesto, la definizione delle priorità di intervento tiene conto di diversi fattori, quali il grado di scostamento rispetto alla soglia di rischio accettabile, gli obiettivi organizzativi, eventuali requisiti normativi o legali e vincoli contrattuali specifici. Questo processo consente di orientare in modo efficace risorse, investimenti e attività di mitigazione, massimizzando l'efficacia delle azioni intraprese. Per supportare le organizzazioni nello svolgimento del cyber risk assessment sono disponibili diversi strumenti e framework di riferimento. Tra questi si possono citare, ad esempio, il Tool di valutazione e trattamento del rischio cyber reso disponibile dall'Agenzia per la Cybersicurezza Nazionale (ACN) per le Pubbliche Amministrazioni, oppure il Framework Nazionale per la Cybersecurity e la Data Protection, sviluppato dal CINI [83], e la Guida per la conduzione del Risk Assessment pubblicata dal NIST, ampiamente utilizzata anche nel settore privato Il processo di valutazione del rischio viene generalmente coordinato dal Cybersecurity Risk Manager, figura professionale che possiede le conoscenze e le competenze necessarie per condurre l'identificazione, l'analisi e la valutazione dei rischi in modo sistematico. Tale ruolo richiede la capacità di interfacciarsi efficacemente con i diversi Risk Owner coinvolti, i quali hanno la responsabilità di gestire i rischi relativi alle rispettive aree di competenza. In questo ambito, assume un ruolo cruciale anche il Chief Information Security Officer (CISO), che, in qualità di responsabile della Cybersecurity Governance, contribuisce alla definizione del risk appetite dell'organizzazione e guida le decisioni strategiche in materia di prioritizzazione dei rischi. A supporto delle attività di valutazione, le organizzazioni possono fare ricorso a diverse tecnologie per la cybersicurezza: piattaforme automatizzate per l'individuazione di vulnerabilità, strumenti basati su Artificial Intelligence per l'analisi dei dati e il rilevamento di anomalie, nonché software di simulazione per

valutare scenari di rischio e potenziali impatti. Per garantire la coerenza e la conformità alle policy di sicurezza, è inoltre essenziale definire controlli specifici a presidio dell'intero processo di risk assessment [84]. Nella Tabella 10 sono riportati alcuni esempi di controlli predisposti in relazione ai principali requisiti di sicurezza, a dimostrazione dell'importanza di integrare aspetti tecnologici, procedurali e organizzativi nel governo del rischio cibernetico.

Requisiti di sicurezza	**Controlli**
Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio devono essere definiti e utilizzati per supportare le decisioni sul rischio operazionale.	• Verificare che il rischio tollerato dall'organizzazione sia identificato ed espresso chiaramente. • Verificare che il rischio tollerato sia determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore di appartenenza.
I rischi cyber attuali dell'organizzazione, compresi quelli legati all'operatività, devono essere compresi.	• Verificare che i rischi legati all'operatività dell'organizzazione vengano analizzati e compresi. • Verificare che le vulnerabilità degli asset siano identificate, convalidate e registrate. • Verificare che gli impatti potenziali e le probabilità di minacce che sfruttano le vulnerabilità vengano identificati e registrati.
La strategia, le aspettative e la politica di gestione del rischio di cybersicurezza dell'organizzazione devono essere stabilite, comunicate e monitorate.	• Verificare che i livelli di propensione al rischio e la tolleranza al rischio siano stabiliti, comunicati e aggiornati. • Verificare che venga stabilito e comunicato un metodo standardizzato per il calcolo, la documentazione, la categorizzazione e la prioritizzazione dei rischi di cybersicurezza.

Tabella 10 - Esempi di requisiti di sicurezza e controlli relativi all'attività di valutazione del rischio

4.2.3 Monitoraggio e rilevamento delle minacce

Una volta ottenuta la lista dei rischi individuati e valutati, l'organizzazione deve definire in modo consapevole come trattare ciascun rischio, scegliendo la modalità di gestione più adeguata in relazione al proprio risk appetite e alle risorse disponibili. Generalmente, le opzioni di trattamento

possono essere ricondotte a quattro categorie principali. La prima opzione è quella di mitigare il rischio, intervenendo attraverso l'introduzione di controlli e misure di sicurezza mirate a ridurre il rischio entro un livello ritenuto accettabile. A questo scopo possono essere adottati diversi framework di controlli, come lo standard internazionale ISO/IEC 27001 [85], il NIST Cybersecurity Framework (CSF) 2.0, l'"Italian Cybersecurity Report – Controlli Essenziali di Cybersecurity", i CIS Critical Security Controls o il NIST SP 800-53. Alcuni meccanismi di mitigazione agiscono direttamente sulle vulnerabilità dei sistemi, mentre altri puntano a contenere o dissuadere la minaccia stessa, scoraggiando l'aggressore dal portare a termine l'attacco. Ciò può avvenire, ad esempio, tramite attività di monitoraggio costante delle reti e dei log, attraverso la collaborazione con le autorità competenti o mediante azioni legali nei confronti degli attori malevoli. In alternativa, l'organizzazione può decidere di trasferire il rischio, affidando a soggetti terzi la copertura dei potenziali danni derivanti dal verificarsi di un evento avverso. Rientrano in questa categoria strumenti come le polizze assicurative cyber, che consentono di assorbire gli impatti finanziari di un incidente, oppure l'esternalizzazione (outsourcing) di specifiche attività a fornitori specializzati in grado di garantire livelli di sicurezza più elevati. Un'altra opzione è quella di evitare il rischio, intervenendo sulle cause alla radice e modificando le condizioni che generano l'esposizione. Questo può avvenire, ad esempio, ripensando la collocazione fisica di infrastrutture critiche: se un rischio elevato fosse legato alla presenza di server in un'area geografica particolarmente esposta a minacce informatiche, l'organizzazione potrebbe decidere di spostarli in una zona considerata più sicura sotto il profilo cyber. Infine, l'organizzazione può scegliere di accettare il rischio. Questa opzione si configura nei casi in cui i costi di implementazione delle misure di mitigazione risultino sproporzionati rispetto alle potenziali perdite derivanti dall'evento di rischio. In tali situazioni, si preferisce accettare consapevolmente il rischio residuo, monitorandolo costantemente e prevedendo eventuali piani di risposta per contenerne gli effetti. In queste casistiche, quindi, l'organizzazione deve stabilire quali controlli e presidi associare a ciascun rischio individuato, valutando attentamente diversi criteri di selezione. In primo luogo, il costo di ciascun controllo dovrebbe essere commisurato al valore dell'asset che intende proteggere e al beneficio che tale misura può apportare all'organizzazione. Inoltre, il beneficio associato al controllo deve poter essere testato e verificato in modo oggettivo, così da garantirne l'efficacia e l'effettivo contributo alla riduzione del rischio. Altro criterio fondamentale riguarda la connessione tangibile tra il controllo implementato e un rischio chiaramente identificabile; questo principio mira a evitare l'introduzione di misure di sicurezza superflue o ridondanti, scelte unicamente perché disponibili o promosse sul mercato, ma non realmente necessarie in relazione al contesto operativo. Come già accennato, l'organizzazione può scegliere di adottare controlli "standard", facendo riferimento a quelli previsti dai principali

framework, oppure personalizzarli in base a esigenze specifiche. In quest'ultimo caso, è fondamentale che i controlli vengano formalizzati in modo chiaro e dettagliato, specificando il loro funzionamento, i soggetti responsabili della loro applicazione e tutte le informazioni necessarie a garantirne un'interpretazione univoca e una facile implementazione. Generalmente, i controlli possono appartenere a tre categorie distinte:

- funzionali alla prevenzione che sono progettati per impedire il verificarsi dell'evento associato al rischio, attraverso misure come l'installazione di firewall, l'adozione di sistemi di autenticazione avanzati o la realizzazione di programmi formativi per aumentare la consapevolezza in ambito cyber.
- funzionali alla rilevazione che sono finalizzati a rilevare gli eventi legati al rischio e intervengono dopo che tali eventi si sono verificati. Per questo motivo, è essenziale che agiscano con tempestività. Tra questi controlli rientrano, ad esempio, i sistemi di Intrusion Detection System (IDS) e l'analisi dei log attraverso soluzioni di Security Information and Event Management (SIEM).
- funzionali alla correzione che mirano a ripristinare i sistemi al loro stato originario, precedente all'evento dannoso. Appartengono a questa categoria i software antimalware, in grado di rimuovere o isolare minacce, le procedure di backup e recovery per il recupero di dati persi o compromessi, e le procedure di incident management, fondamentali per la gestione e il contenimento dell'incidente.

Le organizzazioni adottano diverse tipologie di controlli di sicurezza, combinandole in modo strategico per applicare il principio della "Defense in Depth" [86], ovvero la difesa su più livelli. Questo approccio prevede l'implementazione di strati multipli di protezione, così che, qualora uno di essi fallisse, gli altri possano comunque contrastare la minaccia, rendendo più complesso per un attaccante compromettere i sistemi.
A titolo esemplificativo, si può considerare il caso di un attacco di phishing in cui un dipendente clicchi su un link dannoso e installi involontariamente un malware. In questo scenario, la formazione sulla sicurezza informatica (controllo di tipo preventivo) avrebbe dovuto fornire al dipendente le competenze necessarie per riconoscere e bloccare tali minacce.
Qualora questa prima barriera fallisse, un Intrusion Detection System (IDS) [87], controllo di tipo rilevativo, potrebbe individuare l'attività sospetta e contrastare l'infezione in tempo utile. Se entrambi i controlli non risultassero sufficienti e il malware riuscisse comunque a infettare il sistema, interverrebbe un controllo di tipo correttivo, come un software antimalware, in grado di rilevare, isolare e neutralizzare la minaccia, limitando i danni potenziali. Inoltre, un sistema di

backup costituirebbe un ulteriore strato di protezione, consentendo di ripristinare i dati eventualmente compromessi e riducendo al minimo l'impatto sull'operatività. È importante sottolineare che, anche in presenza di un sistema di difesa ben strutturato e articolato su più livelli, il rischio non può essere completamente eliminato. Rimarrà sempre una quota di rischio, detta rischio residuo, che deve essere costantemente monitorata, gestita e, se necessario, ulteriormente mitigata nel tempo attraverso azioni di revisione e aggiornamento continuo delle misure di sicurezza. Le decisioni relative al trattamento del rischio vengono formalizzate all'interno del Piano di trattamento del rischio, un documento strategico che descrive in modo chiaro come l'organizzazione intende gestire i rischi identificati, al fine di riportarli entro i livelli di accettabilità definiti dal risk appetite. Per ciascun rischio individuato, il piano deve contenere informazioni dettagliate sulle modalità di gestione da adottare. n particolare, devono essere specificati: le modalità di risposta al rischio, con un'eventuale descrizione puntuale dei controlli previsti; i diversi responsabili del rischio e delle azioni di risposta correlate; le motivazioni che giustificano la scelta delle soluzioni individuate; le risorse necessarie per attuare le misure pianificate; i risultati attesi in termini di riduzione del livello di rischio; eventuali limiti o vincoli di natura organizzativa o normativa che possono incidere sulle modalità di trattamento; le tempistiche previste per raggiungere i livelli di rischio desiderati; la modalità di reporting e monitoraggio del rischio con gli indicatori di riferimento; nonché lo stato di implementazione delle azioni di risposta programmate. Così come avviene per le attività di analisi, anche le attività di gestione del rischio vengono generalmente coordinate dal Cyber Risk Manager, figura professionale dotata delle competenze necessarie per assumere decisioni coerenti con gli obiettivi strategici dell'organizzazione. Il Cyber Risk Manager collabora strettamente con il Risk Owner, ovvero il responsabile operativo dell'area interessata dal rischio, per valutare la soluzione più adeguata da adottare in relazione a ciascun scenario. Dal punto di vista operativo, diverse tecnologie possono supportare l'organizzazione nella definizione e nell'attuazione del piano di trattamento del rischio. Tra gli strumenti più diffusi vi sono i fogli di calcolo e i software di collaborazione, utili per la redazione, l'aggiornamento e il monitoraggio del piano stesso; i software di gestione del rischio, che consentono di centralizzare la catalogazione, il tracciamento e la valutazione dei rischi; e gli strumenti di simulazione ed esercitazione, che permettono di ricreare scenari di attacco realistici, con l'obiettivo di stimare i livelli di rischio potenziali associati a ciascun evento cyber e di testare l'efficacia delle contromisure pianificate. Infine, per garantire il rispetto dei requisiti di sicurezza legati all'attività di risposta al rischio, è possibile definire e implementare specifici controlli di verifica. Questi controlli hanno la funzione di monitorare la coerenza tra quanto pianificato e quanto effettivamente realizzato, assicurando la tracciabilità delle decisioni e la misurabilità dei risultati ottenuti in un'ottica di

miglioramento continuo. Nella tabella 11 vengono mostrati esempi di requisiti di sicurezza e controlli relativi all'attività di risposta al rischio.

Requisito di sicurezza	Controlli
Devono essere identificate e prioritizzate le azioni relative alla gestione del rischio.	• Verificare che vengano identificate le azioni relative alla gestione del rischio e che siano classificate per priorità, pianificate, monitorate e comunicate.
La strategia, le aspettative e le politiche di gestione del rischio di cybersicurezza dell'organizzazione sono stabilite, comunicate e monitorate.	• Verificare che le politiche per la gestione dei rischi di cybersicurezza siano stabilite in base al contesto organizzativo, alla strategia di cybersicurezza e alle priorità e verificare che siano comunicate ed applicate. • Verificare che le attività e i risultati della gestione del rischio di cybersicurezza siano inclusi nei processi di gestione del rischio organizzativo.
Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) devono essere compresi e utilizzati nella gestione del rischio di cybersicurezza.	• Verificare che le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) siano compresi e utilizzati nella gestione del rischio di cybersicurezza.

Tabella 11 - Esempio di requisiti di sicurezza e controlli relativi all'attività di risposta al rischio

4.2.4 Comunicazione e circolazione delle informazioni sul rischio cyber

Le attività di comunicazione del rischio cyber costituiscono processi trasversali di fondamentale importanza, da attuare in modo sistematico sia durante le fasi di valutazione del rischio sia nel corso delle attività di trattamento. Una comunicazione chiara, strutturata e costante riveste infatti un ruolo cruciale per diverse ragioni. In primo luogo, la comunicazione permette di informare i Risk Owner in merito ai risultati del risk assessment, consentendo loro di comprendere in modo puntuale quali minacce interessano l'organizzazione, quali vulnerabilità sono state individuate e quale potrebbe essere l'impatto di un potenziale incidente sulla cybersicurezza complessiva. Questa condivisione di informazioni è indispensabile per favorire decisioni consapevoli e coerenti con il livello di rischio

identificato. Allo stesso modo, è fondamentale informare i Risk Owner riguardo alle modalità di trattamento del rischio, illustrando come i rischi individuati verranno gestiti e mitigati. Il coinvolgimento diretto dei responsabili di area è essenziale, poiché essi partecipano attivamente, a vario titolo, ai processi di valutazione e gestione dei rischi. Un altro obiettivo strategico della comunicazione riguarda la raccolta di informazioni dai diversi stakeholder, interni ed esterni. Coinvolgere queste figure consente di raccogliere contributi e feedback preziosi, utili a migliorare continuamente l'accuratezza dei processi di valutazione e la qualità delle soluzioni di mitigazione, promuovendo una visione condivisa e integrata del rischio cyber. La comunicazione contribuisce inoltre ad aumentare il grado di consapevolezza e di responsabilità all'interno dell'organizzazione, sensibilizzando i dipendenti e tutti gli stakeholder sul valore della cybersicurezza e sui rischi correlati. Un livello di consapevolezza più elevato favorisce comportamenti più sicuri, riduce la probabilità di errori umani e può incidere significativamente sulla prevenzione degli incidenti. Infine, la comunicazione efficace permette di identificare le interrelazioni tra i diversi rischi e le relative modalità di risposta. Comprendere come i rischi cyber possano interagire tra loro e come le azioni di mitigazione possano influenzarsi reciprocamente è fondamentale per sviluppare una strategia di risposta integrata e coerente, in grado di massimizzare l'efficacia complessiva delle misure di sicurezza. È prioritario per ogni organizzazione sviluppare piani di comunicazione del rischio cyber, efficaci sia in situazioni ordinarie che di emergenza, coinvolgendo i responsabili interni e, se necessario, fornitori e autorità esterne. Le attività di comunicazione del rischio, all'interno dell'organizzazione vengono svolte su tre diversi livelli [88]:

- *livello strategico* che affronta il rischio dal punto di vista organizzativo, a questo livello viene definita la strategia di cyber risk management identificando obiettivi di lungo periodo in termini di "Risk Appetite" e "Risk Tolerance" e comunicandoli al livello tattico per assicurarsi che la strategia e gli obiettivi siano sempre allineati;
- *livello tattico* che affronta il rischio dal punto di vista dei processi organizzativi che devono supportare il raggiungimento degli obiettivi in termini di rischio definiti dal livello strategico;
- *livello operativo* che affronta il rischio dal punto di vista delle attività operative di cybersicurezza e si occupa della definizione dei controlli di sicurezza, della loro gestione e del loro monitoraggio nel rispetto dei processi e delle procedure definite dal livello tattico.

Come si può osservare, il processo di comunicazione del rischio cyber investe trasversalmente l'intera organizzazione, richiedendo il coinvolgimento di tutti i ruoli e le funzioni responsabili della gestione del rischio informatico. È importante sottolineare che i soggetti coinvolti all'interno di

ciascun flusso comunicativo possono variare a seconda della tipologia di rischio a cui ci si riferisce, del contesto operativo e dei livelli di responsabilità interessati. Dal punto di vista operativo, esistono numerose tecnologie che possono supportare l'attivazione e la gestione efficace dei flussi comunicativi legati al rischio cyber. Tra queste rientrano innanzitutto i software di gestione del rischio, che facilitano la comunicazione fornendo reportistica dettagliata, dashboard intuitive e strumenti di monitoraggio in tempo reale dello stato di ciascun rischio. Questi strumenti consentono di condividere informazioni aggiornate con i Risk Owner, i responsabili di funzione e i vertici aziendali, favorendo decisioni informate e tempestive. A supporto della diffusione della conoscenza interna, i software di gestione della conoscenza permettono di archiviare e condividere documenti, procedure operative, politiche di sicurezza e lesson learned utili a migliorare la comprensione del rischio cyber e a promuovere pratiche coerenti in tutta l'organizzazione. Un ruolo importante è svolto anche dalle applicazioni per la creazione di contenuti, che consentono di produrre presentazioni, report e materiali informativi utili a comunicare, soprattutto dal livello tattico a quello strategico, lo stato di avanzamento delle azioni intraprese per la gestione e la mitigazione dei rischi. Questi strumenti sono particolarmente rilevanti per sensibilizzare il management e garantire un allineamento con gli obiettivi di sicurezza dell'organizzazione [89]. La intranet organizzativa costituisce un ulteriore strumento funzionale, in quanto può essere utilizzata per l'archiviazione e la condivisione di informazioni, procedure e aggiornamenti sul rischio, assicurando un accesso centralizzato e strutturato alla documentazione rilevante. Infine, tra gli strumenti di comunicazione intraorganizzativa si collocano anche le piattaforme di messaggistica istantanea e collaborazione, che agevolano la comunicazione tra gruppi di lavoro, consentendo di condividere rapidamente informazioni, segnalazioni e aggiornamenti sui rischi in tempo reale. Al fine di verificare e garantire il rispetto dei requisiti di cybersicurezza legati alla comunicazione del rischio di cybersicurezza possono essere definiti diversi controlli. Si riportano nella Tabella 12 alcuni esempi di controlli individuati in relazione ai requisiti di sicurezza:

Requisito di sicurezza	**Controlli**
La strategia, le aspettative e la politica di gestione del rischio di cybersicurezza dell'organizzazione devono essere stabilite, comunicate e monitorate.	• Verificare che la direzione strategica che descrive le modalità di risposta al rischio sia stata comunicata. • Verificare che siano stabilite linee di comunicazione all'interno dell'organizzazione per i rischi di cybersicurezza, compresi i rischi dei fornitori e di altre terze parti.

Requisito di sicurezza	Controlli
I rischi cyber attuali dell'organizzazione devono essere compresi.	• Verificare che le risposte al rischio vengano scelte, classificate per priorità, pianificate, monitorate e comunicate.

Tabella 11 - Esempi di requisiti di sicurezza e controlli relativi all'attività di comunicazione del rischio

4.2.5 Gestione dei rischi informatici legati a soggetti terzi

Il rischio cyber di terze parti riguarda le minacce alla cybersicurezza che possono derivare da entità esterne lungo la catena di fornitura [90]. Non si tratta solo di fornitori diretti, ma anche di partner, consorzi, subappaltatori, investitori o altre realtà esterne che, a vario titolo, possono influenzare la postura di sicurezza dell'organizzazione. Secondo il NIST, è fondamentale che ogni organizzazione definisca un processo strutturato per monitorare, valutare e mitigare questo rischio, garantendo che tutte le terze parti rispettino i controlli di sicurezza stabiliti. In termini operativi, la gestione del rischio cyber di terze parti può articolarsi in diverse fasi [91]. La prima fase riguarda la definizione dei requisiti di cybersicurezza, durante la quale l'organizzazione deve identificare in modo chiaro i requisiti minimi che i fornitori devono soddisfare per garantire livelli di protezione adeguati. A supporto di questa attività, uno degli strumenti più utilizzati è rappresentato dai cosiddetti Minimum Security Requirements (MSR), che definiscono i livelli minimi di cybersicurezza accettabili e vincolano formalmente il fornitore a garantirli lungo l'intera durata contrattuale. Successivamente, si procede con l'identificazione dei potenziali fornitori, selezionando sul mercato quegli operatori che presentano i requisiti di cybersicurezza in linea con le esigenze individuate. Tale fase può essere supportata da strumenti come le Request For Information (RFI), sondaggi esplorativi o analisi di mercato, utili per raccogliere informazioni preliminari sulle offerte disponibili. La fase di acquisizione del fornitore si concentra sulla scelta effettiva del partner e sulla formalizzazione del contratto di fornitura. Essa comprende attività specifiche come lo sviluppo di uno Statement Of Work (SOW) o di uno Statement Of Objective (SOO), documenti che definiscono con chiarezza obiettivi, caratteristiche della fornitura, responsabilità di gestione dei rischi, requisiti di conformità e criteri di cybersicurezza esternalizzati. Successivamente, l'organizzazione può procedere con il rilascio di una Request For Proposal (RFP) o di una Request For Quote (RFQ), ossia rispettivamente una richiesta di offerta o di preventivo basata sui contenuti del SOW o del SOO, per raccogliere proposte formali dai fornitori interessati. Un passaggio cruciale consiste nello sviluppo di criteri di valutazione specifici per la gestione del rischio cyber lungo la catena di fornitura. Tali criteri devono essere chiari, misurabili e strettamente correlati ai requisiti di sicurezza, così da

consentire una valutazione coerente delle risposte ricevute alle RFP o RFQ. La selezione finale dei fornitori avviene quindi applicando questi criteri per individuare le soluzioni che meglio soddisfano gli standard di sicurezza e le esigenze di continuità operativa dell'organizzazione. Una volta individuato il fornitore più idoneo, è necessario procedere alla definizione puntuale delle condizioni contrattuali, includendo clausole specifiche di cybersicurezza, termini di servizio, penali per eventuali violazioni e requisiti di conformità e audit [92]. Ciò consente di ridurre i margini di ambiguità e di responsabilizzare la terza parte rispetto agli obblighi di sicurezza. Infine, la fase di esecuzione del contratto richiede controlli periodici per monitorare l'effettivo rispetto dei requisiti di cybersicurezza da parte del fornitore. Eventuali cambiamenti nel contesto operativo o nel livello di conformità del partner possono rendere necessario aggiornare politiche, procedure o clausole contrattuali. A tal fine, possono essere previsti audit regolari, controlli documentali o verifiche di terze parti, così da garantire un presidio costante del rischio cyber lungo tutta la catena di fornitura. Relativamente ai diversi ruoli coinvolti all'interno del processo di gestione del rischio cyber di terze parti, il Chief Information Security Officer (CISO) riveste un ruolo fondamentale. Il CISO è infatti responsabile della definizione e della promulgazione delle politiche interne relative alla gestione del rischio lungo la catena di fornitura e svolge un ruolo di primo piano nell'introduzione di una metodologia strutturata per identificare, valutare e mitigare le minacce legate alle terze parti [93]. In particolare, il CISO mette a disposizione le competenze e le conoscenze necessarie per sviluppare procedure di esecuzione, analisi e utilizzo delle valutazioni sui fornitori, oltre a delineare strategie di mitigazione tecnica coerenti con i risultati delle verifiche effettuate. All'interno di tale processo, assumono una funzione di rilievo anche i Cyber Risk Manager, figure professionali che dispongono delle competenze e delle conoscenze specifiche per tradurre la strategia definita dal CISO e dalla funzione di Cybersecurity Governance in processi operativi concreti. I Cyber Risk Manager definiscono e implementano procedure, controlli e attività di monitoraggio, assicurandosi che la gestione del rischio cyber di terze parti sia coerente con gli obiettivi di sicurezza complessivi dell'organizzazione. A completare la filiera dei ruoli coinvolti vi è il contributo del Risk Owner, che, in qualità di responsabile dell'area operativa direttamente interessata dal rischio, collabora strettamente con i Risk Manager. Questa collaborazione risulta essenziale per l'identificazione puntuale dei rischi, la definizione di azioni di risposta adeguate e la corretta implementazione delle procedure di mitigazione previste. Per garantire che le misure di gestione del rischio di terze parti siano effettivamente efficaci e coerenti con i requisiti di cybersicurezza definiti, è inoltre opportuno prevedere e implementare controlli specifici di verifica. Tali controlli consentono di monitorare in modo costante la conformità dei fornitori alle politiche di sicurezza, individuando eventuali scostamenti o aree di miglioramento. A titolo esemplificativo, nella Tabella 13 sono riportati alcuni

esempi di controlli predisposti in relazione ai principali requisiti di sicurezza applicabili alla gestione del rischio lungo la catena di fornitura.

Requisito di sicurezza	**Controllo**
I processi di gestione del rischio legato alla “supply chain” devono essere identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder organizzativi.	• Verificare che la gestione del rischio della catena di approvvigionamento per la cybersicurezza sia integrata nei processi di cybersicurezza e di gestione del rischio organizzativo. • Verificare che i fornitori siano censiti e prioritizzati per livello di criticità. • Verificare che sia stabilito e approvato con i fornitori un programma, una strategia, degli obiettivi, delle politiche e dei processi di gestione del rischio della catena di approvvigionamento.
Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione devono essere stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione deve definire e implementare processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	• Verificare che i contratti con i fornitori e i partner terzi siano utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersicurezza dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber. • Verificare che i fornitori e partner terzi siano regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali.

Tabella 13 – Esempio di requisiti e controlli relativi all’attività di gestione del rischio delle terze parti

5. L’economia della cybersecurity: modelli di investimento e interdipendenza

L’evoluzione delle minacce informatiche ha reso sempre più evidente che la cybersecurity non è solo un problema tecnico, ma anche e soprattutto, un problema economico. Ogni decisione di investimento in misure di sicurezza implica un trade-off: da un lato, i costi, spesso elevati e in parte non perfettamente prevedibili, delle tecnologie, delle competenze e dei processi; dall’altro, i benefici attesi in termini di riduzione del rischio, di continuità operativa e di tutela del valore informativo.

In questo quadro, la teoria economica ha cercato di formalizzare le scelte delle imprese, costruendo modelli che permettono di:

- capire quanto convenga investire, in particolare il livello ottimale di spesa;
- valutare come l’interdipendenza tra imprese, tecnica e/o di mercato, alteri tali scelte rispetto all’ottimo sociale;
- individuare quali strumenti di policy possano correggere sottoinvestimento o sovrainvestimento in sicurezza.

Nei paragrafi che seguono si presentano i principali filoni della letteratura, con l’obiettivo non solo di descrivere i modelli, ma anche di evidenziarne i limiti, le implicazioni pratiche e le possibili connessioni con la realtà dei mercati digitali contemporanei.

5.1 L’analisi economica delle decisioni di sicurezza informatica

In un ecosistema digitale sempre più esposto a minacce complesse e in rapida evoluzione, gli investimenti nella sicurezza informatica sono diventati una componente imprescindibile per le imprese, al fine di garantire l’integrità, la riservatezza e la disponibilità del proprio patrimonio informativo e, in ultima istanza, la sopravvivenza stessa dell’organizzazione. Questo spiega perché la spesa in cybersecurity sia ormai entrata stabilmente tra le variabili strategiche di gestione e di pianificazione che ogni azienda dovrebbe considerare all’interno delle proprie scelte di governance. Tuttavia, l’efficacia reale di tali investimenti rimane ancora oggi oggetto di dibattito. Non esistono, infatti, evidenze empiriche definitive che colleghino in modo diretto l’aumento dei costi generati dagli attacchi informatici all’entità degli investimenti effettuati o, viceversa, alla loro eventuale carenza. Ciò nonostante, esperti e professionisti del settore concordano sul fatto che livelli inadeguati di protezione espongano inevitabilmente le imprese a rischi maggiori e a conseguenze

potenzialmente devastanti [94]. In tale contesto, l'analisi economica delle scelte di sicurezza è divenuta negli anni un campo di studio di crescente rilevanza, favorendo la nascita di una letteratura teorica ampia e multidisciplinare. La consapevolezza sull'importanza della sicurezza informatica e, più in generale, sulla protezione dei dati, ha ricevuto un impulso decisivo nei primi anni 2000, anche a seguito di eventi di portata globale come gli attentati terroristici dell'11 settembre. È in questo periodo che emergono due principali filoni di ricerca che hanno contribuito a definire le basi dell'analisi economica degli investimenti in sicurezza. Il primo filone, inaugurato da Gordon e Loeb [95], si concentra sugli incentivi delle singole imprese a investire nella protezione dei propri sistemi informativi, sviluppando un modello di analisi che considera l'azienda come unità isolata. Questo approccio, tuttavia, non tiene conto delle forme di interdipendenza che possono emergere tra più organizzazioni, le quali, nella realtà, operano spesso su reti comuni o condividono infrastrutture critiche, anche in assenza di una diretta relazione di concorrenza. Di conseguenza, le conclusioni derivanti da questa letteratura risultano talvolta di applicabilità limitata in contesti operativi complessi. Su queste basi si sviluppa un secondo filone di ricerca, promosso da Kunreuther e Heal [96], che introduce il concetto di sicurezza interdipendente (interdependent security). Questo approccio allarga l'analisi oltre il perimetro aziendale, considerando come le decisioni di investimento in sicurezza di un'organizzazione possano influenzare (positivamente o negativamente) la postura di sicurezza di altre realtà collegate. Sebbene tale approccio sia nato in ambiti diversi, come la sicurezza aeroportuale, la prevenzione incendi o le campagne di vaccinazione, esso trova applicazione diretta anche nel contesto della cybersecurity, dove le imprese operano sempre più spesso su infrastrutture di rete comuni. Questo quadro interdipendente evidenzia come una strategia di investimento isolata rischi di essere inefficace se non inserita in una più ampia logica di cooperazione, coordinamento e standardizzazione dei livelli di protezione.
Un terzo filone di letteratura, sviluppato successivamente da Garcia e Horowitz [97], ha spostato l'attenzione sulle decisioni di investimento in sicurezza informatica da parte di aziende concorrenti che operano su sistemi informatici distinti. Un esempio emblematico è rappresentato da realtà come Amazon ed eBay, che competono direttamente nel settore dell'e-commerce ma utilizzano infrastrutture digitali separate e indipendenti. Più di recente, alcuni studi hanno ulteriormente ampliato il campo di indagine, esplorando le scelte di investimento in sicurezza informatica di aziende che, oltre a competere sul mercato, condividono infrastrutture o reti comuni. Un caso particolarmente rilevante è rappresentato dal settore bancario, dove le banche, pur essendo concorrenti dirette, sono interconnesse attraverso reti essenziali come SWIFT, utilizzata per gestire transazioni finanziarie internazionali. In questo contesto, la sicurezza interdipendente si manifesta in modo particolarmente evidente: una violazione in un nodo della rete può generare effetti a catena,

incidendo sulla resilienza dell'intero sistema. A livello metodologico, la letteratura di riferimento evidenzia come l'analisi delle scelte di investimento in cybersecurity abbia spesso fatto ricorso a sondaggi e studi di revisione, in particolare nel campo delle reti informatiche e di comunicazione. Numerosi contributi si sono concentrati sull'esame di aziende operanti su reti comuni, anche in assenza di una relazione di concorrenza diretta sul mercato. In questi studi, approcci basati sulla teoria dei giochi sono stati spesso impiegati per affrontare problematiche come l'assicurazione informatica, la tutela della privacy e dell'anonimato, la sicurezza delle reti veicolari, i sistemi di rilevamento delle intrusioni o la protezione delle reti intelligenti. Tra questi contributi, i lavori di Cavusoglu et al. [98] risultano particolarmente significativi per l'analisi, in quanto focalizzati sulle decisioni strategiche delle imprese riguardanti la pianificazione e l'allocazione degli investimenti in sicurezza informatica.

Per garantire una panoramica chiara e accessibile di questa ampia letteratura, viene adottato un approccio sistematico in due fasi. In una prima fase, vengono individuati cinque dimensioni fondamentali che consentono di caratterizzare i diversi modelli proposti, organizzando così la letteratura in modo strutturato:

1. Investimento: distingue tra modelli che considerano un investimento continuo, qualunque valore positivo e quelli che adottano un'impostazione binaria, in cui l'impresa decide se investire o meno in sicurezza.
2. Interdipendenza: differenzia i modelli basati sull'analisi di una singola impresa da quelli che, utilizzando strumenti di teoria dei giochi, esaminano contesti multi-impresa, in cui le decisioni di un attore influenzano la postura di sicurezza degli altri.
3. Benessere (Welfare): dimensione rilevante per i modelli interdipendenti, indica se viene calcolato il livello di investimento socialmente ottimale e confrontato con l'equilibrio di mercato, evidenziando potenziali inefficienze.
4. Spillover: per i contesti multi-impresa, definisce la natura delle esternalità derivanti dalle scelte di investimento. Tali spillover possono essere di tipo tecnico (effetti diretti su tutte le imprese connesse), di mercato (effetti legati alla concorrenza tra imprese) o misti, laddove siano presenti entrambi gli elementi.
5. Rete: per gli studi che considerano spillover tecnici, specifica se la topologia della rete è assunta come esogena, ossia definita esternamente, oppure endogena, cioè derivante da un processo di ottimizzazione.

Nella seconda fase, viene utilizzato un modello teorico di riferimento per l'analisi degli investimenti in sicurezza informatica, che integra le principali caratteristiche emerse dai contributi esaminati.

Partendo da un contesto di riferimento privo di interdipendenza tra imprese, il modello viene progressivamente arricchito per includere scenari in cui emergono esternalità di tipo tecnico, di mercato o misto, offrendo così un quadro interpretativo coerente e unificato per comprendere le dinamiche di investimento.
Questo approccio consente non solo di sintetizzare le diverse prospettive teoriche, ma anche di confrontare l'investimento effettivo delle imprese, descritto attraverso l'equilibrio di Nash, con il livello di investimento socialmente ottimale. A tale scopo, viene adottato il concetto di "Prezzo dell'Anarchia" [99], che misura la perdita di efficienza collettiva derivante dall'adozione di comportamenti individualistici non coordinati. In questo modo, il modello contribuisce a evidenziare le principali distorsioni e i potenziali margini di miglioramento in termini di cooperazione, regolamentazione o incentivi economici nel campo della cybersecurity.

5.2 Modelli di investimento senza interdipendenza

Il framework più semplice per analizzare i trade-off economici legati agli investimenti in cybersecurity si basa su un modello a periodo unico con un solo decisore. In questa impostazione di base, si assume esplicitamente che non vi sia alcuna interdipendenza tra imprese: ciò significa che le scelte di investimento di un'organizzazione non influenzano, né sono influenzate, dalle decisioni di altri attori. Di conseguenza, il processo decisionale è circoscritto alle sole variabili interne dell'impresa, semplificando l'analisi ma anche escludendo le esternalità di rete.

All'interno di questo modello, si considera un'impresa neutrale al rischio, che deve decidere l'ammontare da destinare alle contromisure di sicurezza necessarie a proteggere un determinato insieme di informazioni.

A tal fine, vengono introdotte alcune variabili e parametri fondamentali per descrivere la struttura del problema:

- X indica il valore dell'insieme di informazioni dell'impresa, indicato come reddito dell'impresa;
- $t \in [0,1]$ rappresenta la probabilità che si verifichi un attacco informatico;
- $v \in [0,1]$ denota la vulnerabilità dell'insieme di informazioni dell'impresa, ossia la probabilità ex ante di una violazione della sicurezza dell'insieme di informazioni, prima che venga effettuato qualsiasi investimento nella sicurezza informatica, subordinata al verificarsi di un attacco informatico;
- aX, con $a \in [0,1]$, è la perdita monetaria attesa derivante da una violazione della sicurezza, espressa come quota del valore complessivo delle informazioni.

Per semplificare l'analisi, ma senza perdita di generalità, si assume che la probabilità che si verifichi un attacco informatico sia pari a uno (t = 1). In questo modo, l'intero rischio dipende esclusivamente dal livello di vulnerabilità iniziale e dall'efficacia dell'investimento in sicurezza. L'impresa può decidere di investire un importo monetario continuo I ≥ 0, destinato a ridurre la vulnerabilità v.

La probabilità *ex post* di una violazione della sicurezza, una volta effettuato l'investimento, è rappresentata dalla funzione π(I,v), la quale soddisfa tre ipotesi di base:

- Se la vulnerabilità iniziale è nulla, cioè v = 0, la probabilità ex post resta sempre zero, indipendentemente dal livello di investimento: π(I,0) = 0.
- Se l'impresa non investe nulla in sicurezza (I = 0), la probabilità ex post coincide esattamente con la vulnerabilità iniziale: π(0,v) = v.
- La funzione π è continuamente doppiamente differenziabile rispetto a I, e mostra rendimenti marginali decrescenti per 0 < v < 1; in altre parole, all'aumentare dell'investimento, la riduzione della probabilità di violazione avviene a un tasso marginale decrescente.

In base a queste ipotesi, il processo decisionale dell'impresa può essere formalizzato come segue: l'obiettivo è scegliere il livello di investimento I per massimizzare il payoff netto, dato dal ricavo complessivo al netto sia della perdita attesa a seguito di un attacco sia del costo dell'investimento. Formalmente, il problema è espresso come:

$$\max_{I\geq 0} R(I) - I = \{X - [\pi(I,v)]aX - I\} \qquad (1)$$

La condizione del primo ordine per risolvere il problema di ottimizzazione (1) è:

$$-\frac{\partial\pi(I,v)}{\partial I}aX = 1 \quad (2)$$

Risolvendo questa equazione per I, si determina il livello di investimento ottimale I*, ossia il punto in cui il beneficio marginale derivante dalla riduzione della perdita attesa è esattamente pari al costo marginale dell'investimento in sicurezza.

Per rendere il modello più concreto, Gordon e Loab illustrano una soluzione in forma chiusa, una forma esplicita per la funzione di probabilità *ex post* coerente con la prima e la terza ipotesi:

$$\pi_0(I,v) = \frac{v}{I+1} \qquad (3)$$

Inserendo questa equazione nella condizione di primo ordine e risolvendo per I, si ottiene:

$$I^* = \sqrt{vaX} - 1 \quad (4)$$

Da questa soluzione emergono due risultati di particolare interesse. In primo luogo, il livello ottimale di investimento I* aumenta al crescere sia della vulnerabilità iniziale (v) sia del valore monetario dell'insieme di informazioni da proteggere (aX). In secondo luogo, se si divide I* per la perdita attesa senza protezione (vaX), si ottiene un massimo teorico pari a 0,25, e nelle estensioni successive arriva a circa il 36,8%: ciò implica che, anche nel peggiore dei casi, l'impresa non investirà mai più di un quarto della perdita attesa per proteggersi. Questo risultato, noto come paradosso di Gordon e Loeb, suggerisce che, oltre una certa soglia, ulteriori investimenti in sicurezza non siano economicamente giustificabili, perché il costo della protezione supera il danno atteso.

Questo risultato ha implicazioni pratiche non banali:

- da un lato, smentisce l'idea, a volte diffusa nel dibattito pubblico, che "più sicurezza è sempre meglio";
- dall'altro, suggerisce che una strategia efficace debba combinare misure tecniche e altri strumenti (assicurazioni, trasferimento del rischio, misure organizzative), piuttosto che inseguire la sicurezza "assoluta", che il modello considera di fatto irraggiungibile.

Una parte consistente della letteratura successiva si è concentrata sulla forma della funzione di probabilità $\pi(I, v)$:

- Tanaka et al. [100] confermano, su dati di e-government giapponese, che un'ipotesi di rendimenti marginali decrescenti è spesso realistica e coerente con molte realtà operative;
- Hausken [101] ed altri esplorano casi con rendimenti crescenti, crescenti–decrescenti o costanti, mostrando che il livello ottimale di investimento può variare molto al variare delle ipotesi tecniche;
- Willemson [102] e Wang [103] evidenziano come, modificando queste ipotesi, ad esempio abbandonando la decrescenza dei rendimenti o assumendo una probabilità di violazione pari al 100% in assenza di protezione, l'investimento ottimale possa superare i limiti inizialmente individuati.

Dal punto di vista riflessivo, questo segnala un punto chiave: la "risposta ottimale" dell'impresa dipende in modo critico da come si modella l'efficacia della sicurezza. Se nella realtà le difese

hanno rendimenti molto diversi tra contesti, applicare meccanicamente il limite del 25–36,8% rischia di essere fuorviante.

La letteratura ha poi esteso il modello in tre direzioni fondamentali:

- dimensione temporale (Gordon et al. [104]; Krutilla et al. [105]): l'investimento in cybersecurity è spesso irreversibile e gli asset di sicurezza sono soggetti a deperimento (software da aggiornare, competenze da mantenere). Ne deriva che il timing degli investimenti e i tassi di sconto possono portare a sottostime importanti se si resta in un modello monoperiodale;
- avversione al rischio (Huang et al. [106]): imprese più avverse al rischio potrebbero investire molto di più, ma devono allo stesso tempo bilanciare il rischio "di sicurezza" e il rischio "di investimento", ovvero il timore che le misure adottate non funzionino o diventino rapidamente obsolete;
- interdipendenza implicita (Wang [107]): l'idea che un'impresa che non investe sia "completamente vulnerabile" anticipa il passaggio ai modelli con interdipendenza esplicita, in cui la vulnerabilità di un attore influenza la sicurezza dell'intero sistema.

Il modello così descritto rappresenta uno schema di base per comprendere la letteratura teorica che analizza le scelte di investimento in sicurezza informatica in assenza di interdipendenza tra imprese. Nel complesso, i modelli senza interdipendenza hanno il merito di chiarire la logica di base delle scelte di investimento, ma, presi isolatamente, descrivono solo una parte della realtà: quella in cui le imprese sono "isole". Nella pratica, però, le imprese agiscono quasi sempre in ecosistemi di rete e in mercati interconnessi.

Da un punto di vista riflessivo, l'insegnamento principale è che il modello base è un utile punto di partenza, ma per applicazioni concrete è necessario essere a conoscenza che:

1. l'investimento ottimale in sicurezza non è "infinito", ma ha un limite economicamente ragionevole;
2. questo limite dipende fortemente da ipotesi tecniche (forma di $\pi(I, v)$), temporali (orizzonte, deperimento) e comportamentali (atteggiamento verso il rischio) che, nella pratica, devono essere calibrate con dati reali e non assunte in modo meccanico

Tuttavia, questo modello presenta alcuni limiti rilevanti quando lo si confronta con la realtà operativa delle imprese. In primo luogo, l'ipotesi di neutralità al rischio e di orizzonte monoperiodale tende a semplificare eccessivamente il processo decisionale: nella pratica, le imprese devono gestire investimenti irreversibili, con orizzonti pluriennali, in un contesto di forte incertezza

sull'evoluzione delle minacce. In secondo luogo, parametri teorici come il valore economico dell'asset informativo (X) o la vulnerabilità iniziale (v) sono difficili da misurare con precisione, soprattutto per le PMI che non dispongono di strumenti avanzati di risk assessment. Dal mio punto di vista, questi elementi suggeriscono che i risultati del modello vadano interpretati come indicazioni qualitative sulla logica dell'investimento, più che come regole quantitative da applicare in modo meccanico.

5.3 Modelli con interdipendenza: effetti di spillover tecnico

In questa sezione si analizza l'interdipendenza tra aziende sotto forma di spillover tecnico, un aspetto cruciale per comprendere le dinamiche della sicurezza informatica in un contesto di rete in cui più organizzazioni condividono la medesima infrastruttura tecnologica. Questo fenomeno riflette il fatto che gli investimenti in cybersicurezza effettuati da una singola impresa possono generare benefici indiretti anche per le altre imprese connesse alla stessa rete. Nella realtà, infatti, le imprese non vivono in ambienti informatici isolati: usano gli stessi fornitori cloud, condividono reti, piattaforme applicative, standard di comunicazione e, spesso, anche dati o servizi.

Per studiare in modo formale questo meccanismo si considera un insieme di $N \geq 2$ imprese simmetriche e avverse al rischio, che operano sulla stessa rete informatica pur non essendo concorrenti dirette sul mercato del prodotto. Per semplicità, si assume che ciascuna impresa affronti la stessa probabilità iniziale di essere attaccata (ad esempio t=1) e decida in modo simultaneo il proprio livello di investimento in misure di cybersicurezza. Gli spillover tecnici emergono quando l'investimento di un'impresa non solo riduce la probabilità di violazione per sé, ma contribuisce anche a ridurre la probabilità di violazione per tutte le altre imprese connesse alla stessa infrastruttura.

Per chiarire l'intuizione, si parte dal caso più semplice con N=2 imprese simmetriche, collegate operativamente tramite la rete. In questa configurazione, ciascuna impresa i=1,2 risolve simultaneamente il seguente problema di ottimizzazione:

$$\max_{I_i \geq 0} R_T(I_i, I_j) - I_i = \left(X - \frac{1}{I_i + eI_j + 1} aX - I_i \right) \quad (5)$$

dove $R^T(I_i, I_j) - I_i$, è il payoff dell'impresa i, e l'apice 'T' richiama la presenza di spillover tecnici. Il ricavo lordo è X, assunto costante per entrambe le imprese, mentre la perdita attesa per un attacco è data da

$1 / (I_i + eI_j + 1)\, aX$.

Il parametro ‘e’cattura l’entità dello spillover tecnico: quanto è più elevato, tanto maggiore è il beneficio che un’impresa trae dall’investimento di sicurezza dell’altra. La probabilità ex post di violazione della sicurezza è quindi

$1 / (I_i + eI_j + 1)$,

che estende la formulazione del caso di impresa isolata includendo esplicitamente l’effetto delle esternalità tecniche. In questo contesto, il parametro $e \in [0,1]$ misura l’intensità dello spillover positivo generato dall’investimento di sicurezza dell’impresa $j \neq i$ sul livello di protezione dell’impresa i. I due estremi sono particolarmente istruttivi:

- quando e=0, non si verificano spillover tecnici: l’investimento dell’impresa j non ha alcun effetto sulla probabilità che iii subisca una violazione; siamo nel caso tradizionale senza interdipendenza;
- quando e=1, gli spillover tecnici raggiungono la loro massima intensità: la riduzione della probabilità di violazione di cui beneficia i grazie all’investimento di j è pari a quella goduta dalla stessa impresa j.

La condizione del primo ordine per il problema di massimizzazione (5) è:

$$I_i^*(I_j) = \sqrt{aX} - 1 - eI_j \quad (6)$$

Data la natura simmetrica del modello, le due aziende presentano caratteristiche identiche e gestiscono informazioni di pari valore, si può semplificare l’analisi considerando che in equilibrio entrambe sceglieranno lo stesso livello di investimento. Tale ipotesi consente di ottenere una soluzione compatta e facilmente generalizzabile anche per scenari più complessi. L’equilibrio simmetrico nel caso di due imprese può quindi essere espresso come:

$$I_T^*(2) = \frac{\sqrt{aX} - 1}{1 + e} \quad (7)$$

L’equilibrio di Nash che emerge da questo modello mostra come il livello ottimale di investimento in sicurezza di ciascuna azienda sia direttamente influenzato dall’intensità degli spillover tecnici (e). Più in dettaglio:

- Quando e=0, non ci sono spillover tecnici. L'investimento ottimale di ciascuna azienda è pari allo stesso risultato che si otterrebbe per una singola azienda isolata.
- Quando e>0, gli spillover tecnici riducono l'incentivo di ciascuna azienda a investire in sicurezza. Più alto è e, minore sarà l'investimento di ciascuna azienda.

- Quando e=1, ciascuna azienda è fortemente incentivata a ridurre il proprio investimento, confidando che l'altra azienda investa abbastanza per garantire la sicurezza complessiva.

Questo fenomeno riflette un meccanismo noto come free riding, per cui le imprese tendono a sfruttare gli investimenti in sicurezza delle altre, traendo vantaggio dagli spillover tecnici senza contribuire in modo proporzionato alla protezione collettiva.

Il modello può essere facilmente esteso da una configurazione a due imprese a un contesto con $N \geq 2$ imprese simmetriche, tutte collegate attraverso la stessa infrastruttura informatica. In questa rete più ampia, ciascuna azienda può beneficiare delle misure di sicurezza implementate dalle altre, ma anche scegliere di sfruttare tali esternalità riducendo i propri investimenti individuali. Si considera quindi un insieme di N imprese, neutrali al rischio e interconnesse operativamente, che risolvono simultaneamente il seguente problema di ottimizzazione:

$$\max_{I_i \geq 0} R_T(I_1, \ldots, I_N) - I_i = X - \frac{1}{I_i + e\sum_{j \neq i}^{N-1} I_j + 1} aX - I_i \quad (8)$$

La differenza rispetto al caso a due imprese sta nell'espressione della probabilità ex post di violazione per l'impresa i, che ora dipende dal proprio investimento e da quello di tutte le altre $N-1$ imprese, ponderati da e:

$$\frac{1}{I_i + e\sum_{j \neq i}^{N-1} I_j + 1}$$

Questa formulazione evidenzia come ogni azienda tragga beneficio non solo dal proprio sforzo di investimento, ma anche da quello degli altri attori operanti sulla stessa rete. Il calcolo della condizione di primo ordine per la massimizzazione del payoff (8) e la risoluzione per l'equilibrio di Nash simmetrico portano al seguente risultato:

$$I_T^*(N) = \frac{\sqrt{aX} - 1}{1 + (N-1)e} \quad (9)$$

Da un punto di vista economico, questo risultato è molto espressivo. Se non vi sono spillover (e=0), il livello di investimento di equilibrio coincide con quello dell'impresa isolata, indipendentemente dal numero di imprese N: il fatto di essere "in rete" non cambia nulla se l'interdipendenza non genera benefici condivisi. Quando invece e>0, l'investimento di equilibrio si riduce progressivamente sia all'aumentare di e sia all'aumentare di N. La logica è che, in una rete più ampia, ogni impresa sa che ci sono molti altri soggetti che possono contribuire alla sicurezza complessiva, e quindi il proprio incentivo a investire si attenua. Nel limite, quando $N \to \infty$,

l'investimento ottimale di ciascuna impresa tende a zero: la cybersicurezza finisce per essere trattata come un bene pubblico puro, che tutti desiderano ma che nessuno ha convenienza privata a finanziare adeguatamente. Il modello può essere utilizzato per fornire un'analisi del benessere collettivo. Per un dato N, si confronta quindi il livello di investimento in equilibrio $I^{T*}(N)$, espresso nell'equazione (9), con il livello di investimento ottimale $I^{TE}(N)$, definito come quello che verrebbe scelto da un pianificatore sociale intenzionato a massimizzare la somma dei payoff di tutte le imprese connesse.

Il pianificatore sociale massimizza:

$$\max_{I \geq 0} N \times [R_T(I) - I] = N\left(X - \frac{1}{I + e(N-1)I + 1}aX - I\right)$$

dove $N \times [R^T(I) - I]$ rappresenta la somma dei payoff delle imprese.

Il livello di investimento socialmente efficiente risulta quindi dato dalla condizione di primo ordine calcolata su questa funzione collettiva, includendo gli effetti positivi degli spillover tecnici su tutti gli attori della rete.

$$I_T^E(N) = \frac{\sqrt{[1 + (N-1)e]aX} - 1}{1 + (N-1)e}$$

Il confronto tra $I^{T*}(N)$ e $I^{TE}(N)$ mette in evidenza un risultato cruciale: quando $e > 0$, ossia in presenza di esternalità positive, il livello di investimento in equilibrio è sempre inferiore a quello socialmente efficiente, indipendentemente dal numero di imprese ($N \geq 2$). In altri termini, le imprese, lasciate libere di decidere autonomamente, tendono a investire troppo poco in cybersicurezza rispetto a quanto sarebbe ottimale per il benessere collettivo. Questo fenomeno di sottoinvestimento è una conseguenza diretta delle esternalità positive generate dagli spillover tecnici. Il motivo è che il beneficio marginale privato dell'investimento (miglioramento del payoff dell'impresa i) è inferiore al beneficio marginale sociale, che include anche la riduzione della probabilità di violazione per le altre $N-1$ imprese.

Questa intuizione emerge in modo ancora più netto nel modello pionieristico di Kunreuther e Heal [108], che considerano un contesto con due imprese (N=2) che devono decidere se investire o meno in sicurezza informatica. In questo modello, l'investimento è una variabile dicotomica:

- $I_i=0$: non investire in sicurezza.
- $I_i=I$: investire un importo positivo e fisso I.

Sostituendo queste due opzioni nella funzione obiettivo del problema di ciascuna impresa i = 1, 2, cioè $R^T(I_i, I_j) - I_i$, si ottiene la seguente struttura di gioco strategico:

Firm 1; Firm 2	I	0
I	$R_T(I,I)-I; R_T(I,I)-I$	$R_T(I,0)-I; R_T(0,I)$
0	$R_T(0,I); R_T(I,0)-I$	$R_T(0,0); R_T(0,0)$

where

$$R_T(I,I) = X - \frac{1}{I+eI+1}aX \geq R_T(I,0) = X - \frac{1}{I+1}aX \geq$$
$$R_T(0,I) = X - \frac{1}{eI+1}aX \geq R_T(0,0) = X - aX \geq 0 \quad \text{(10) (11)}$$

Kunreuther e Heal osservano che l'equilibrio di Nash di questo gioco prevede che entrambe le imprese investano in cybersecurity se la seguente condizione è soddisfatta:

$R^T(I,I) - R^T(0,I) \geq 1$ (12)

In altre parole, ciascuna impresa è disposta a sostenere il costo normalizzato pari a 1 solo se il payoff netto derivante dall'investimento, assumendo che anche l'altra investa, è almeno pari al payoff che otterrebbe non investendo e godendo comunque della protezione derivante dall'investimento altrui. Se questa condizione non è soddisfatta, nessuna delle due imprese sarà disposta a investire, nonostante l'esistenza di un beneficio collettivo.

Per mettere in prospettiva questo risultato, gli autori confrontano il caso interconnesso con il caso di impresa isolata. Un'impresa che utilizza un sistema informatico isolato, senza interdipendenze, ottiene un payoff pari a: (X−1/I+1*aX−I) se investe, mentre il payoff dell'impresa che non investe è semplicemente: (X−aX).

Questi due valori si ottengono sostituendo I e 0 nella funzione obiettivo R(I) del problema di ottimizzazione iniziale (1), utilizzando la funzione di probabilità $\pi_0(I) = 1/(I + 1)$. Sono, di fatto, equivalenti ai termini $R^T(I, 0)$ e $R^T(0, 0)$ dell'equazione (11). Ciò evidenzia come l'introduzione degli spillover tecnici modifichi in modo sostanziale gli incentivi individuali rispetto al caso di un'impresa isolata: in presenza di interdipendenze, le imprese devono tenere conto non solo del proprio livello di protezione, ma anche di quello garantito dagli altri attori connessi alla stessa rete. Pertanto, un'impresa isolata è disposta a investire solo se il beneficio netto dell'investimento è maggiore o uguale al costo sostenuto. Formalmente, questa condizione può essere espressa come:

$R^T(I,0) - R^T(0,0) \geq 1$ (13)

Si può facilmente verificare che, in presenza di spillover tecnici (e > 0), il lato sinistro della condizione (12) risulta inferiore a quello della condizione (13). In termini formali:

$R^T(I,I) - R^T(0,I) < R^T(I,0) - R^T(0,0)$ (14)

Questo risultato mette in evidenza un punto centrale: l'investimento in sicurezza informatica è meno efficace per un'azienda interconnessa rispetto a un'azienda isolata. La ragione di questa

differenza risiede nel fatto che, in un contesto di rete, le imprese si influenzano reciprocamente attraverso gli spillover tecnici: ogni azienda può beneficiare della protezione generata dagli investimenti altrui, riducendo così il proprio incentivo a investire. Kunreuther e Heal concludono che nel seguente intervallo parametrico:

$$R^T(I,I) - R^T(0,I) \leq I < R^T(I,0) - R^T(0,0) \quad (15)$$

si verifica una situazione paradossale: la condizione (13) è soddisfatta e quindi un'impresa isolata investirebbe, ma la condizione (12) no. In altre parole, la semplice presenza di una seconda impresa interconnessa riduce l'incentivo individuale a investire in cybersicurezza, evidenziando come l'interdipendenza, se non regolata, possa generare un sottoinvestimento collettivo. Il risultato più rilevante del modello di Kunreuther e Heal è proprio questo: l'interdipendenza tra aziende, attraverso gli spillover tecnici, può portare a un livello di investimento in sicurezza inferiore a quello socialmente desiderabile.

Questo fenomeno diventa ancora più marcato con l'aumentare del numero di imprese connesse (N). All'aumentare di N, la condizione per cui tutte le imprese scelgono di investire diventa progressivamente più restrittiva; nel limite, quando $N \to \infty$, nessuna impresa è disposta a sostenere il costo dell'investimento, confidando esclusivamente nella protezione derivante dagli altri. Si tratta di una chiara manifestazione del problema del free riding, dove ciascun attore spera di beneficiare degli sforzi altrui senza contribuire attivamente. Una corrente di lavori successivi estende il quadro di Kunreuther e Heal sostituendo la scelta dicotomica "investo / non investo" con un livello di investimento continuo e approfondendo l'analisi del benessere collettivo. Böhme [109] considera un modello con due imprese interconnesse e distingue tra un rischio diretto di attacco e un rischio indiretto di contagio proveniente dall'altra impresa; anche in questo caso l'equilibrio di Nash presenta un sottoinvestimento sistematico, perché le esternalità positive della protezione condivisa restano solo parzialmente internalizzate. Varian [110] si concentra invece sul caso di spillover massimi (e=1e = 1e=1), mostrando che un'elevata interdipendenza induce le imprese a ridurre drasticamente il proprio sforzo, aggravando il problema del free riding. Grossklags et al. [111] introducono poi una distinzione tra autoprotezione, che riduce la probabilità di violazione e genera spillover positivi, e autoassicurazione (backup, polizze, ecc.), che limita l'entità della perdita ma non produce esternalità: ne risulta che l'autoprotezione tende a essere sotto–fornita rispetto all'ottimo sociale, mentre l'autoassicurazione si colloca su livelli più vicini a quello efficiente. Altri contributi, come Riordan [112] e Lelarge e Bolot, nonché Lelarge [113], approfondiscono il rapporto tra rischi diretti e rischi di contagio, mostrando che una maggiore efficacia delle misure contro il contagio può attenuare il problema del sottoinvestimento, ma che questo può riemergere

quando l'aumento della protezione nella rete riduce il rischio percepito e quindi l'incentivo individuale a investire. Infine, Anderson e Moore [114] richiamano l'attenzione sul fatto che, nella pratica, le interdipendenze sono spesso asimmetriche, e che la presenza di nodi più critici di altri può generare schemi di incentivo eterogenei, rafforzando l'esigenza di interventi di coordinamento e regolazione mirati.

Rispetto ai modelli senza interdipendenza, i modelli con spillover tecnici ribaltano in parte l'intuizione di base: la decisione di investire non riguarda più solo il bilanciamento tra costo della protezione e riduzione della perdita attesa per il singolo, ma anche i benefici che interessano le altre imprese connesse alla stessa rete. Dal punto di vista della mia analisi, questo passaggio è cruciale, perché spiega il motivo per cui in contesti come le infrastrutture critiche, i servizi cloud o le supply chain digitali la razionalità privata tenda sistematicamente a produrre un sottoinvestimento rispetto all'ottimo sociale.

Un altro limite importante è rappresentato dall'ipotesi, spesso implicita, di imprese simmetriche. Nella realtà delle reti digitali, invece, esistono nodi altamente eterogenei per dimensione, ruolo e criticità sistemica, come per esempio i grandi provider cloud o i principali operatori di infrastrutture essenziali. In questi casi, una stessa unità di investimento in cybersecurity da parte di un soggetto centrale può avere un impatto molto maggiore sulla sicurezza complessiva della rete rispetto a quella di un attore periferico. Questo aspetto non è pienamente catturato dai modelli più semplici, ma è rilevante dal punto di vista regolatorio, perché suggerisce la necessità di requisiti di sicurezza differenziati in base al rischio sistemico. In questa prospettiva, i risultati dei modelli con spillover tecnici offrono una base teorica per interpretare gli interventi regolatori europei richiamati nei capitoli precedenti, ad esempio la Direttiva NIS2 o il Cyber Resilience Act, che impongono obblighi minimi di sicurezza e responsabilità rafforzate per operatori essenziali e fornitori di servizi digitali. Dal mio punto di vista, tali interventi possono essere letti come tentativi di correggere proprio il sottoinvestimento generato dalle esternalità positive di rete.

5.4 Modelli di interdipendenza: spillover di mercato

L'analisi degli investimenti in cybersecurity cambia prospettiva quando le imprese non possono solo essere interconnesse a livello tecnico, ma possono anche essere concorrenti dirette sul mercato dei prodotti. In questo caso emerge una particolare forma di interdipendenza, definita spillover di mercato, in cui la sicurezza informatica di un'impresa non si limita a proteggere i propri sistemi digitali, ma incide direttamente sulle sue performance competitive.

In un simile contesto, un attacco informatico che colpisce un'azienda può tradursi in un vantaggio competitivo per i suoi rivali, che possono conquistare nuove quote di mercato approfittando della temporanea debolezza dell'impresa attaccata. Il modello degli spillover di mercato considera $N \geq 2$ imprese simmetriche e neutrali al rischio, che operano sullo stesso mercato dei prodotti ma utilizzano infrastrutture informatiche separate, prive di connessioni tecniche reciproche. In altri termini, non si generano spillover tecnici: l'investimento in sicurezza di una singola impresa non accresce direttamente il livello di protezione delle altre. L'interdipendenza nasce invece sul piano dei ricavi: un attacco che compromette una delle aziende riduce la sua capacità competitiva e trasferisce valore ai concorrenti.

Il modello si basa su due ipotesi centrali:

1. Ricavi di Mercato Condivisi: il parametro X rappresenta i ricavi totali del mercato, che vengono equamente suddivisi tra tutte le imprese concorrenti. Ciascuna azienda riceve quindi una quota pari a X/N
2. Perdita di Ricavi in Caso di Attacco: le aziende che subiscono una violazione perdono la loro quota di ricavi, la quale viene acquisita in toto dai concorrenti non colpiti. Per semplicità, si assume che la perdita sia totale (a = 1).

Per comprendere meglio le dinamiche di questo modello, iniziamo analizzando il caso di duopolio, in cui due aziende simmetriche competono sullo stesso mercato. Ogni azienda decide quanto investire in sicurezza informatica per proteggere i propri ricavi e massimizzare il proprio profitto. La funzione di payoff di ciascuna azienda i=1,2 definita come:

$$\max_{I_i \geq 0} R_M(I_i, I_j) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + 1}\left(-\frac{X}{2}\right) + \left(1 - \frac{1}{I_i + 1}\right)\frac{1}{I_j + 1}\frac{X}{2} - I_i\right] \quad (16)$$

dove:

- $R^M(I_i, I_j)$ indica il payoff lordo dell'impresa i, e il pedice M funge da mnemotecnico per "spillover di mercato".
- Il primo termine, X/2, rappresenta i ricavi di mercato, equamente distribuiti tra i due concorrenti.
- Il secondo termine riflette la probabilità che l'impresa iii subisca una violazione di sicurezza (1/Ii+1) e perda la propria quota di ricavi −X/2.

- Il terzo termine rappresenta la probabilità che l'impresa iii non subisca una violazione, mentre il concorrente j≠i viene colpito. In questo caso, l'impresa i acquisisce l'intera quota di ricavi del concorrente (X/2).

Per determinare l'equilibrio di Nash simmetrico, si risolve il problema di massimizzazione del payoff per ciascuna impresa, tenendo conto della strategia dell'altra. In equilibrio, entrambe le imprese scelgono lo stesso livello di investimento, indicato con $I^{M*}(2)$, che soddisfa la seguente condizione di primo ordine:

$$I_M^*(2) = \frac{X + 6H^2}{6H} - 1 \quad (17)$$

Analizziamo ora queste dinamiche dal punto di vista del benessere sociale, confrontando il livello di investimento in equilibrio competitivo, indicato come $I^{M*}(2)$, con l'investimento socialmente efficiente, definito come $I^{ME}(2)$. Quest'ultimo rappresenta il livello di investimento che un pianificatore sociale sceglierebbe per massimizzare la somma dei payoff delle due imprese interdipendenti. Formalmente, il problema di ottimizzazione collettiva si esprime come:

$$\max_{I \geq 0} 2 \times [R_M(I) - I] = \left\{ 2\left[\frac{X}{2} + \frac{1}{I+1}\left(-\frac{X}{2}\right) + \left(1 - \frac{1}{I+1}\right)\frac{1}{I+1}\frac{X}{2} - I\right]\right\} \quad (18)$$

Questa analisi consente di determinare se l'investimento privato in cybersecurity è sufficiente per massimizzare il benessere collettivo o se, al contrario, vi è sottoinvestimento o sovrainvestimento.

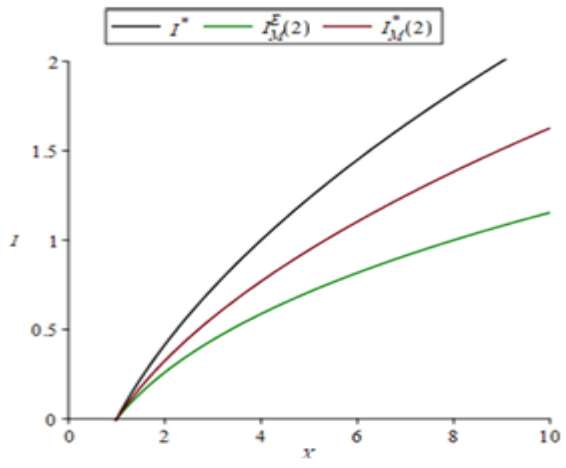

Figura 14 - Confronto tra livello di investimento in cybersecurity per impresa singola I, investimento socialmente efficiente con spillover di mercato $I^E_M(2)$ e investimento di equilibrio di Nash con spillover di mercato $I^*_M(2)$*

Dalla soluzione del problema di massimizzazione del welfare collettivo si ottiene il livello di investimento socialmente efficiente nel caso di duopolio. Come evidenziato in Figura 14 dalla curva verde, tale livello è sempre inferiore all'investimento di equilibrio $I^M*(2)$ (curva rossa) per qualsiasi valore di $X > 1$. Ciò implica che le imprese tendono a investire in cybersecurity più di quanto sarebbe ottimale dal punto di vista sociale. Questo risultato normativo di sovrainvestimento è riconducibile a un'esternalità negativa generata dagli spillover di mercato. In particolare, quando un'impresa i aumenta il proprio investimento I_i per ridurre il rischio di subire un attacco, il beneficio marginale che ne ricava è superiore al beneficio marginale per la collettività. Ciò accade perché il rendimento privato non considera la perdita di opportunità per l'impresa concorrente j, la quale, in caso di attacco andato a segno contro i, acquisirebbe la sua quota di ricavi. Un livello di protezione più elevato riduce dunque la probabilità che i concorrenti ottengano questi benefici di mercato, generando un incentivo a investire oltre il livello efficiente dal punto di vista collettivo. Per valutare meglio la portata di questo risultato, l'analisi viene estesa al caso generale con $N \geq 2$ imprese simmetriche, neutrali al rischio, che competono sullo stesso mercato del prodotto. Anche in questo contesto le imprese utilizzano sistemi informatici separati, per cui non si generano spillover tecnici; l'interdipendenza tra di esse deriva esclusivamente dalla condivisione dei ricavi di mercato.

Il problema di massimizzazione del payoff di ciascuna impresa i = 1, …, N può quindi essere definito come:

$$\max_{I_i \geq 0} R_M(I_1 \dots, I_N) - I_i = \left[\frac{X}{N} + \frac{1}{I_i + 1}\left(-\frac{X}{N}\right) + \left(1 - \frac{1}{I_i + 1}\right)K - I_i\right] \quad (19)$$

Nel modello presentato, i primi due termini all'interno delle parentesi quadre nell'equazione (19) corrispondono a quelli già introdotti nel problema (16), con la differenza che ora si considera un numero generico di imprese $N \geq 2$, invece di due. Il terzo termine, invece, rappresenta il guadagno atteso per l'impresa iii nel caso in cui essa non subisca una violazione della sicurezza: questo è calcolato come la probabilità che l'impresa non venga colpita ($1 - 1/(Ii+1)$), moltiplicata per un'espressione indicata con K. Tale espressione descrive il valore atteso del guadagno che l'impresa ottiene acquisendo le quote di ricavi delle imprese concorrenti che risultano colpite da attacchi informatici. Sebbene non sia possibile derivare una soluzione in forma chiusa per il problema (19), la soluzione implicita risulta monotonicamente decrescente rispetto a N. In altre parole, all'aumentare del numero di concorrenti, ciascuna impresa tende a ridurre progressivamente il proprio investimento in cybersecurity. Questa evidenza dimostra che, mentre nel caso di duopolio si osserva un sovrainvestimento in misure di sicurezza informatica, nel contesto dell'oligopolio con

più imprese si verifica un fenomeno di sottoinvestimento progressivo. Questa dinamica è una conseguenza diretta delle esternalità negative generate dagli spillover di mercato:

- Ogni azienda tende a ridurre i propri costi di investimento, confidando nella possibilità che siano i concorrenti a subire violazioni e a perdere quote di mercato.
- Maggiore è il numero di concorrenti presenti sul mercato, minore è l'incentivo di ciascuna impresa a investire, poiché il potenziale guadagno atteso derivante da attacchi informatici ai danni altrui si frammenta tra un numero crescente di imprese.

Questo risultato conferma che l'impatto negativo degli spillover di mercato sull'investimento per impresa, già osservato nel caso di duopolio, si estende senza difficoltà al caso di oligopolio con $N \geq 2$ imprese. Utilizzando questo quadro, possiamo discutere la letteratura che analizza gli investimenti aziendali in cybersecurity quando l'interdipendenza tra imprese assume la forma di spillover di mercato.

Una parte della letteratura successiva il contributo di Garcia e Horowitz [115] considera l'investimento in cybersecurity come una scelta binaria (investire o non investire) e mostra che, in un mercato concorrenziale, il passaggio dal monopolio al duopolio riduce l'incentivo individuale a investire: un'impresa che in regime di monopolio sarebbe disposta a sostenere il costo della sicurezza può non esserlo più quando si trova a competere con un'altra, perché la possibilità di acquisire quote di mercato da un concorrente colpito rende meno "costoso" restare vulnerabili. Estendendo l'analisi a $N \geq 2$ imprese, gli autori dimostrano che la condizione affinché tutte investano si fa via via più restrittiva, e che può emergere un fenomeno di sovrainvestimento rispetto al livello socialmente efficiente, in quanto il beneficio privato dell'investimento supera il beneficio per la collettività. Su questa base si sviluppa un filone che introduce esplicitamente il comportamento della domanda. Gao e Zhong [116] analizzano il ruolo dei costi di cambio fornitore: quando i consumatori possono cambiare facilmente in seguito a una violazione, la pressione competitiva spinge le imprese a investire maggiormente in sicurezza; al contrario, costi di switching elevati attenuano tali incentivi. Qian et al. [117] distinguono tra consumatori "mobili", sensibili alla sicurezza, e consumatori "fedeli": una quota ampia di questi ultimi riduce ulteriormente la pressione competitiva e, di conseguenza, l'incentivo a investire.

Un altro filone applica la logica degli spillover di mercato al contesto delle piattaforme digitali. In mercati a due lati, dove una piattaforma collega, ad esempio, fornitori e utenti finali, la cybersecurity diventa un fattore competitivo decisivo. Geer et al. [118] introducono il concetto di "piattaforme magnete", ovvero piattaforme molto grandi che, proprio per la loro scala, attraggono l'attenzione dei cybercriminali e diventano bersagli privilegiati, con la conseguenza di dover

sostenere investimenti crescenti in sicurezza per mantenere la fiducia degli utenti. Arce [119] mostra come una piattaforma che investe di più in sicurezza possa guadagnare quota di mercato grazie alla maggiore fiducia degli utenti, ma diventi al tempo stesso un obiettivo più appetibile e, quindi, costretta a mantenere nel tempo livelli elevati di investimento. Questi contributi evidenziano che la sicurezza informatica può diventare una leva competitiva sia per le imprese già dominanti sia per quelle che cercano di differenziarsi.

Nel complesso, i modelli di spillover di mercato mettono in luce un punto cruciale per la governance della cybersecurity: qui l'esternalità non nasce dalla condivisione tecnica dell'infrastruttura, ma dal modo in cui gli attacchi ridistribuiscono quote di mercato. In alcuni casi questo genera sovrainvestimento (per difendersi da perdite di ricavi che, dal punto di vista del sistema, sono solo trasferimenti tra imprese); in altri, soprattutto con molti concorrenti o con consumatori poco mobili, si osserva di nuovo sottoinvestimento. Dal punto di vista delle politiche pubbliche, ciò suggerisce l'importanza di:

- aumentare la trasparenza sui livelli di sicurezza (ad esempio tramite obblighi di disclosure e schemi di certificazione);
- ridurre i costi di switching e facilitare la portabilità dei dati;
- promuovere una concorrenza basata anche sulla sicurezza, e non solo sul prezzo.

In questa prospettiva, la cybersecurity non è solo un costo da contenere, ma diventa un elemento strategico di posizionamento competitivo e, al tempo stesso, un ambito in cui l'intervento regolatorio può aiutare a riallineare incentivi privati e benessere collettivo.

5.5 Modelli di interdipendenza: spillover tecnici e di mercato

In questa sezione si assume che l'interdipendenza tra imprese assuma contemporaneamente la forma di spillover tecnici e spillover di mercato. In altre parole, si considerano imprese che gestiscono la propria attività attraverso una rete informatica comune, ma che allo stesso tempo sono anche concorrenti dirette sul mercato dei prodotti. Per semplicità, si restringe l'attenzione al caso di N = 2 imprese, assunte simmetriche e neutrali al rischio, che affrontano la stessa probabilità t=1 di subire un attacco informatico. In questo scenario, ciascuna impresa i=1,2 risolve simultaneamente il seguente problema di ottimizzazione: massimizzare il proprio payoff netto, bilanciando i benefici derivanti dall'investimento in cybersecurity con i costi sostenuti per la protezione.

$$\max_{I_i \geq 0} R_{TM}(I_i, I_j) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + eI_j + 1}\left(-\frac{X}{2}\right) + \left(1 - \frac{1}{I_i + eI_j + 1}\right)\frac{1}{I_j + eI_i + 1}\frac{X}{2} - I_i \right] \quad (20)$$

Il payoff lordo, indicato come R_{TM}(Ii, Ij), si ottiene combinando R_T(Ii, Ij), che cattura il solo effetto degli spillover tecnici, con R_M(Ii, Ij), che invece tiene conto esclusivamente degli spillover di mercato. In questo modo si costruisce una rappresentazione integrata che tiene conto di entrambe le forme di interdipendenza tra le imprese. Si risolve il problema (20) per ottenere il livello di investimento di equilibrio di Nash simmetrico, indicato come $I^*_{TM}(2)$. Poiché l'espressione in forma chiusa è piuttosto complessa, si ricorre a una rappresentazione grafica per diversi valori del parametro degli spillover tecnici e. La Figura 14 mostra $I^*_{TM}(2)$ per e = {0.1, 0.3, 0.5, 0.7, 0.9} (curve colorate) e I* definito nell'equazione (7) con a = 1 (curva nera), in funzione di X. Tutte le curve colorate che rappresentano $I^*_{TM}(2)$ risultano inferiori a I* per ogni valore X > 1. Questo significa che l'investimento di equilibrio in cybersecurity si riduce quando si passa da un'impresa singola a due imprese, indipendentemente dal valore di e. Questo risultato non sorprende poiché abbiamo già dimostrato che l'incentivo al free riding generato dagli spillover tecnici riduce l'investimento di equilibrio di ciascuna impresa quando entra una seconda impresa nella rete informatica comune e che anche gli spillover di mercato hanno un effetto negativo, perché la probabilità che un'impresa ottenga l'intero ricavo di mercato X diminuisce passando da monopolio a duopolio. Quando entrambi i tipi di spillover sono presenti, questi due effetti negativi si sommano e spiegano il risultato riportato in Figura 15. L'analisi grafica conferma, inoltre, che un valore più alto del parametro e, indicativo di spillover tecnici più intensi, riduce ulteriormente $I^*_{TM}(2)$ a causa di un incentivo al free riding sempre più marcato.

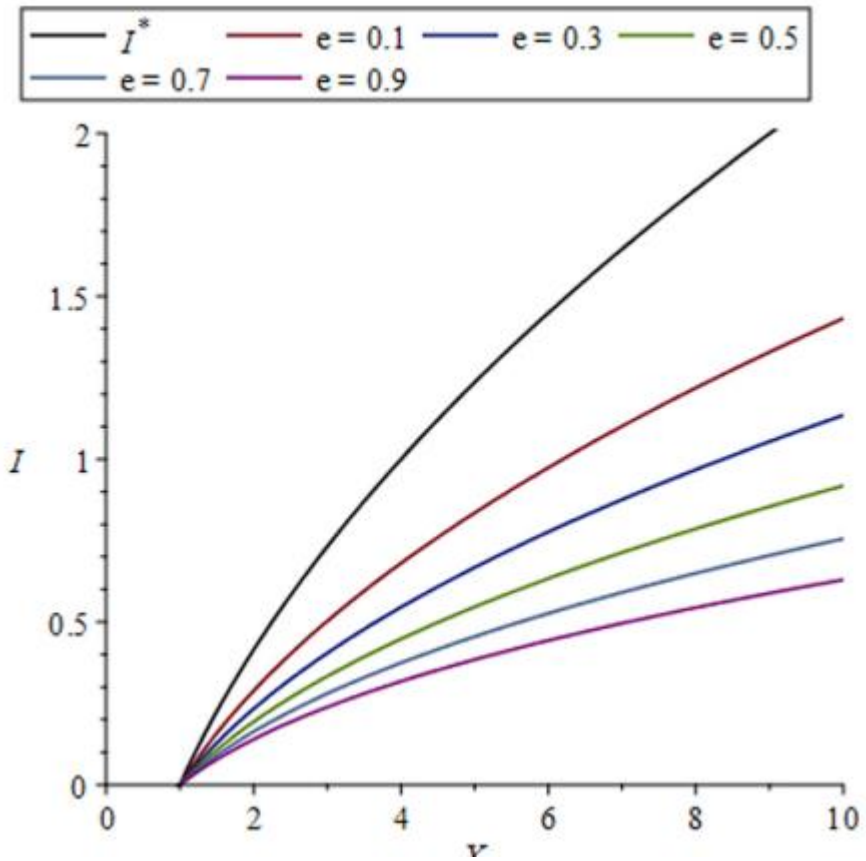

Figura 15 - Livello di investimento di equilibrio in cybersecurity (I e $I^*_{TM}2$)) con spillover tecnici e di mercato, per diversi valori del parametro degli spillover tecnici (e)*

Quando i due diversi spillover sono considerati simultaneamente, emergono spunti interessanti dal punto di vista del benessere collettivo, poiché gli spillover tecnici da soli determinano un sottoinvestimento, mentre gli spillover di mercato da soli portano al risultato opposto di sovrainvestimento. È quindi opportuno verificare in quali condizioni prevalga l'una o l'altra dinamica. A questo scopo, si calcola innanzitutto l'investimento socialmente efficiente nel modo consueto, cioè come il valore scelto da un pianificatore sociale per massimizzare la somma dei payoff delle due imprese.

$$\max_{I\geq 0} 2\times[R_{TM}(I)-I] = \left\{2\left[\frac{X}{2}+\frac{1}{I+eI+1}\left(-\frac{X}{2}\right)+\left(1-\frac{1}{I+eI+1}\right)\frac{1}{I+eI+1}\frac{X}{2}-I\right]\right\}$$

Successivamente, confrontiamo questo livello socialmente efficiente, indicato con $I^E_{TM}(2)$, con quello di equilibrio, $I^*_{TM}(2)$, per ciascun valore di e = {0.1, 0.3, 0.5, 0.7, 0.9}. A tal fine, ricorriamo a una rappresentazione grafica, riportata nella figura 16. Il sovrainvestimento ($I^*_{TM}(2) > I^E_{TM}(2)$) tende a manifestarsi per valori relativamente bassi di e. Al contrario, valori più elevati di e portano all'esito opposto, ossia al sottoinvestimento ($I^*_{TM}(2) < I^E_{TM}(2)$). Quindi quando e è basso, prevalgono gli spillover di mercato e questo genera l'esternalità negativa descritta precedentemente,

la quale fa sì che il beneficio sociale dell'investimento risulti inferiore al beneficio privato, determinando così un sovrainvestimento. All'aumentare di e, l'esternalità positiva legata agli spillover tecnici diventa sempre più rilevante e alla fine prevale su quella negativa prodotta dagli spillover di mercato. Di conseguenza, il beneficio sociale diventa maggiore del beneficio privato e si verifica un sottoinvestimento.

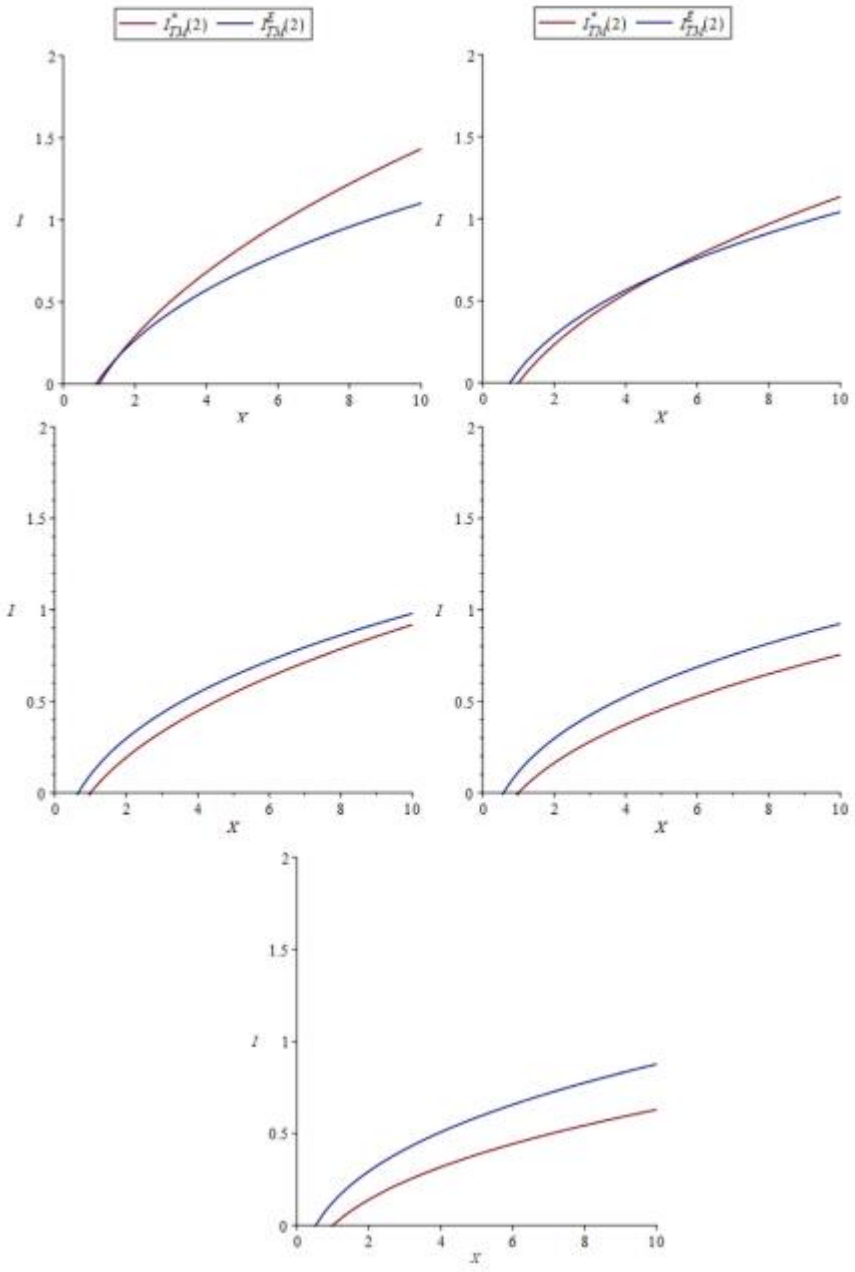

Figura 6 - Confronto tra investimento di equilibrio $I^*_{TM}(2)$ e investimento socialmente efficiente $I^E_{TM}(2)$ per diversi valori di spillover tecnico (e)

Dal punto di vista interpretativo, i modelli misti con spillover tecnici e di mercato mostrano che la realtà può collocarsi lungo un continuum in cui, a seconda dell'intensità relativa delle due forme di interdipendenza, si osservano risultati molto diversi: dal sovrainvestimento spinto dalla

competizione sul mercato alla ricomparsa del sottoinvestimento tipico dei beni pubblici. Questo aiuta a spiegare perché, empiricamente, si osservino comportamenti eterogenei fra settori e fra imprese: alcune organizzazioni tendono a spendere 'troppo' in sicurezza per difendere la propria reputazione e le proprie quote di mercato, mentre altre restano strutturalmente sottoprotette, confidando negli investimenti altrui o nella scarsa visibilità degli incidenti.

Le prospettive di ricerca delineate evidenziano, infatti, come lo studio degli investimenti in cybersecurity sia ancora un campo in piena evoluzione. Da un lato, la teoria necessita di modelli sempre più realistici, capaci di tenere conto delle interdipendenze complesse tra le aziende, degli spillover tecnici e di mercato, e delle dinamiche di competizione nei mercati digitali. Dall'altro, la ricerca empirica deve migliorare la qualità e l'affidabilità dei dati, offrendo evidenze concrete sull'efficacia delle diverse misure di sicurezza adottate dalle imprese. In un contesto sempre più digitale, in cui le minacce informatiche continuano a crescere e le conseguenze di una violazione possono rivelarsi devastanti, comprendere come e perché le imprese decidono di investire in sicurezza non è soltanto una questione teorica, ma rappresenta una necessità pratica. Si tratta di un presupposto fondamentale per garantire la resilienza organizzativa e la protezione dei dati degli utenti, elementi essenziali per la competitività e la fiducia nel mercato. Investire nella ricerca sulla cybersecurity non significa soltanto sviluppare tecnologie di protezione sempre più sofisticate, ma anche comprendere le motivazioni economiche, strategiche e comportamentali che determinano l'efficacia o l'inefficacia delle strategie di difesa. Un'analisi integrata, capace di coniugare rigore teorico ed evidenza empirica, può costituire la base per politiche pubbliche più efficaci e per una maggiore consapevolezza da parte di imprese e consumatori, rafforzando l'intero ecosistema digitale di fronte alle sfide future.

5.6 Implicazioni per le imprese: lettura manageriale dei modelli

Dal punto di vista aziendale, i modelli economici della cybersecurity non vanno interpretati come istruzioni operative, ma come lenti di analisi per orientare scelte e priorità. Aiutano a capire dove hanno senso ulteriori investimenti, quando si rischia di sovraspendere e come bilanciare gli strumenti a disposizione.

Tre implicazioni appaiono particolarmente rilevanti:

1. L'illusione della decisione puramente tecnica.
   I modelli mostrano che la scelta di quanto investire in cybersecurity è una scelta di allocazione di risorse sotto incertezza, influenzata da:

- valore degli asset informativi,
- struttura dei costi,
- atteggiamento verso il rischio,
- posizione nella rete,
- dinamiche concorrenziali.

In questo senso, trattare la cybersecurity come una questione esclusivamente "IT" rischia di sottovalutare la dimensione strategica della decisione. Inoltre l'avversione al rischio sposta l'ottimo, ma va bilanciata con il rischio di investimento dove più spesa non è sinonimo di più sicurezza utile.

2. L'importanza di riconoscere le interdipendenze.
   Una stessa impresa può essere contemporaneamente:

   - "fornitore di sicurezza" per altri, per esempio lungo la supply chain,
   - "beneficiaria" degli investimenti altrui,
   - concorrente sul mercato di prodotti o servizi digitali.

I modelli di interdipendenza chiariscono che la posizione nella rete plasma gli incentivi a investire. Un'impresa centrale in un'infrastruttura critica che sottostima questo ruolo può generare esternalità e rischi sistemici. Al contrario, in contesti altamente competitivi, la minaccia di perdita di quote di mercato in caso di incidente può spingere a sovrainvestire rispetto all'ottimo sociale. In entrambi i casi, riconoscere esplicitamente le interdipendenze consente di evitare decisioni miopi.

3. La necessità di una visione di portfolio degli strumenti di gestione del rischio
   I modelli distinguono fra autoprotezione (riduzione della probabilità di incidente) e autoassicurazione (limitazione dell'impatto). Nella pratica, una strategia efficace combina:

   - controlli tecnici,
   - misure organizzative,
   - strumenti contrattuali e assicurativi,
   - accordi di cooperazione con altri attori della rete.

La domanda manageriale non è più solo "quanto investire", ma "in che cosa investire" e "con chi coordinarsi". Una gestione a portafoglio riduce il rischio di sotto- o sovrainvestimento e allinea la sicurezza agli obiettivi di business.

5.7 Politiche Pubbliche ed interventi correttivi

L'analisi presentata evidenzia le condizioni in cui possono emergere fenomeni di sottoinvestimento o di sovrainvestimento in cybersecurity, fornendo così indicazioni utili per delineare strumenti di intervento che i regolatori e i decisori pubblici possono adottare per promuovere livelli adeguati di investimento nella sicurezza informatica.

- Sussidi o tassazione sugli investimenti in cybersecurity

- Spillover tecnici prevalenti: Quando le esternalità positive di tipo tecnico sono dominanti (ad esempio, nel caso di imprese che condividono una rete informatica comune ma non sono concorrenti dirette), il rischio di sottoinvestimento può essere affrontato attraverso sussidi mirati a coprire una parte dei costi di investimento. Secondo il modello illustrato nella sezione degli spillover tecnici, una sovvenzione pari a:

$$\frac{(N-1)e}{1+(N-1)e}$$

per ogni unità di investimento I indurrebbe le imprese a selezionare il livello di investimento socialmente efficiente $I^{E}_{T}(N)$. Tuttavia, questo strumento richiede che l'autorità fiscale abbia una conoscenza perfetta della struttura di mercato (N) e del grado di interdipendenza tecnica (e).

- Spillover di Mercato Prevalenti**:** quando gli spillover di mercato sono prevalenti, come per esempio le imprese che competono sul mercato dei prodotti ma che non condividono una rete informatica comune, il rischio di sovrainvestimento potrebbe essere mitigato imponendo una tassa per unità di investimento I. Anche in questo caso, l'autorità fiscale dovrebbe conoscere l'impatto preciso dell'investimento di ciascuna impresa sulla probabilità di una violazione della sicurezza.

- Condivisione delle Informazioni

Un problema ricorrente è che le imprese tendono a sottostimare le perdite potenziali derivanti da una violazione o l'efficacia dell'investimento, a causa della mancanza di dati accurati su minacce e vulnerabilità. Una possibile soluzione consiste nell'introdurre incentivi che favoriscano la condivisione di informazioni tra imprese che operano all'interno di una stessa rete o in mercati simili. Tuttavia, la letteratura dimostra che le imprese sono spesso restie a condividere dati sensibili.

Gal-Or e Ghose [120] evidenziano che la condivisione può diventare più probabile se è percepita come un valore aggiunto dai clienti finali. In questo caso, l'utilità reputazionale derivante dalla trasparenza può ridurre la necessità di incentivi esterni.

- Regolamentazione Diretta
  Un ulteriore strumento di intervento è l'introduzione di regolamenti che fissino standard minimi di qualità per le pratiche di cybersecurity. Tali standard possono riguardare sia i processi interni sia i requisiti di sicurezza dei prodotti destinati al mercato. Tuttavia, definire e aggiornare standard tecnici di cybersecurity è una sfida complessa. Come evidenziato da Garcia e Horowitz non è affatto scontato che le buone pratiche possano essere interamente codificate in norme rigide, né che queste riescano da sole a garantire livelli di protezione sufficientemente elevati in un contesto caratterizzato da minacce in continua evoluzione.

6. Caso di studio: l'attacco al Colonial Pipeline

L'efficacia di qualsiasi strategia di gestione del rischio informatico non si misura soltanto attraverso policy, strumenti o investimenti tecnologici, ma soprattutto nella capacità di prevenire, rilevare e rispondere ad attacchi concreti che possono avere conseguenze di vasta portata. Dopo aver analizzato nel Capitolo 4 le principali pratiche di cyber risk management e le scelte di investimento per la protezione delle infrastrutture critiche, questo capitolo si propone di tradurre questi concetti teorici in un contesto reale e tangibile. A tal fine, viene esaminato l'attacco ransomware che nel maggio 2021 ha colpito Colonial Pipeline, una delle infrastrutture energetiche più strategiche degli Stati Uniti. Questo caso di studio evidenzia come vulnerabilità apparentemente banali, come l'assenza di controlli di accesso multifattoriali, possano compromettere intere catene di fornitura di rilevanza nazionale. Analizzando il contesto, le dinamiche e le conseguenze dell'attacco, si mettono in luce lezioni fondamentali per le organizzazioni, in termini di prevenzione, risposta agli incidenti e rafforzamento della resilienza cyber.

6.1 Contesto e dettagli dell'attacco

L'oleodotto coloniale è un'infrastruttura cruciale e strategica nella catena di approvvigionamento del carburante degli Stati Uniti. Estendendosi per oltre 8.800 chilometri dal Texas a New York, rappresenta il 45% dell'approvvigionamento di carburante della costa orientale. L'azienda consegna oltre 100 milioni di galloni di carburante al giorno a clienti in 14 stati e serve circa 28 raffinerie. Come sottolinea Kimberly Wood [121], senza il contributo del Colonial Pipeline non sarebbe possibile garantire carburante per trasporto, aerei, riscaldamento domestico e rifornimento di importanti aeroporti e basi militari. L'attacco subito da questa infrastruttura nel maggio 2021 ha dunque messo in evidenza in modo drammatico quanto la sicurezza digitale sia cruciale non solo a

fini economici, ma anche per la sicurezza nazionale. L'attacco fu orchestrato dal gruppo criminale DarkSide, che riuscì a infiltrarsi nella rete aziendale IT di Colonial tramite l'utilizzo di credenziali compromesse per l'accesso remoto. Queste credenziali, verosimilmente ottenute tramite tecniche di ingegneria sociale o pratiche come il credential stuffing, che sfruttano password già esposte in precedenti data breach, non erano protette da autenticazione a due fattori (MFA), una misura semplice e ormai considerata standard nella maggior parte dei contesti organizzativi. Una volta ottenuto l'accesso, gli attaccanti hanno installato un ransomware che ha cifrato file e server, impedendo all'azienda di accedere a dati e funzioni vitali. Inoltre, hanno minacciato di divulgare informazioni sensibili come ulteriore forma di ricatto [122]. Secondo la Cybersecurity and Infrastructure Security Agency (CISA) [123], DarkSide ha utilizzato tecniche avanzate, come il phishing, lo sfruttamento di applicazioni esposte pubblicamente, l'accesso remoto tramite Virtual Desktop Infrastructure (VDI) e Remote Desktop Protocol (RDP), garantendosi una presenza continua nella rete. La scelta di un modello RaaS ha permesso a DarkSide di operare in modo scalabile, collaborando con altri gruppi criminali per distribuire il ransomware e dividere i profitti. Un aspetto fondamentale per comprendere la portata dell'attacco subito dal Colonial Pipeline riguarda l'analisi delle vulnerabilità presenti all'interno dell'infrastruttura informatica al momento dell'incidente. La valutazione effettuata dopo l'attacco ha infatti evidenziato come diversi componenti critici fossero caratterizzati da un livello di esposizione elevato, tale da facilitare l'infiltrazione da parte del gruppo criminale DarkSide [124]. In particolare, come sintetizzato nella Tabella 17, i meccanismi di controllo degli accessi presentavano una vulnerabilità del 100%, a testimonianza di procedure di autenticazione e gestione delle credenziali evidentemente insufficienti a prevenire accessi non autorizzati. Allo stesso modo, i sistemi di rilevamento delle intrusioni e le funzionalità di monitoraggio del traffico di rete mostravano percentuali di vulnerabilità superiori all'80%, con un livello di rischio classificato come "Critico". Ciò significa che eventuali tentativi di intrusione potevano passare inosservati o essere rilevati con ritardo, compromettendo la capacità di reazione dell'organizzazione. Non meno significativi risultano i dati relativi agli endpoint di accesso remoto e alle sessioni VPN: l'attacco è avvenuto proprio sfruttando credenziali compromesse e l'assenza di adeguate misure di autenticazione multifattoriale. Queste lacune hanno permesso agli aggressori di superare senza ostacoli i controlli di sicurezza di base, garantendosi un accesso persistente alla rete aziendale e la possibilità di distribuire il ransomware in modo capillare. L'analisi delle vulnerabilità mette in luce, in definitiva, come l'attacco non sia stato un semplice evento isolato, ma piuttosto il risultato di una serie di debolezze strutturali e di pratiche di gestione del rischio non adeguatamente implementate. Questa consapevolezza è essenziale per evidenziare quanto la protezione di infrastrutture critiche non possa prescindere da una valutazione continua dei

punti deboli e da investimenti mirati in strumenti, formazione e governance di sicurezza. In assenza di tali presidi, anche una singola falla può trasformarsi rapidamente in una crisi di ampia portata, con conseguenze economiche e sociali potenzialmente devastanti.

Componente di Sicurezza	% Sistemi Vulnerabili	Numero di Sistemi Coinvolti	Livello di Rischio
Endpoint di Accesso Remoto	76%	189	Alto
Monitoraggio del Traffico di Rete	84%	142	Critico
Sessioni VPN	47%	324	Medio
Sistemi di Rilevamento delle Intrusioni	84%	2.846	Critico
Meccanismi di Controllo degli Accessi	100%	17	Critico

Tabella 17 - Valutazione delle vulnerabilità di sicurezza rilevate durante l'attacco informatico al Colonial Pipeline

6.2 Impatto Economico e Sociale dell'Attacco

Questa sezione si propone di analizzare in modo approfondito gli impatti economici e sociali derivanti dall'attacco informatico subito da Colonial Pipeline, con l'obiettivo di evidenziare come una singola vulnerabilità tecnologica possa evolvere rapidamente in una crisi di vasta portata. Gli effetti prodotti dall'attacco sono stati molteplici e si sono manifestati sia sul piano economico, con conseguenze dirette e indirette per l'azienda e i suoi stakeholder, sia sul piano sociale, incidendo sul tessuto economico locale e sulla quotidianità dei consumatori. Per quanto riguarda l'impatto economico diretto, l'azienda si è trovata a dover sostenere costi immediati e rilevanti per far fronte all'emergenza. In primo luogo, Colonial Pipeline ha deciso di pagare un riscatto di circa 4,4 milioni di dollari in Bitcoin al gruppo criminale, al fine di ottenere la chiave di decrittazione necessaria a ripristinare l'accesso ai propri sistemi [125]. Si è trattato di una scelta controversa, ma motivata dall'urgenza di ridurre al minimo i tempi di fermo dell'infrastruttura, considerata strategica per l'approvvigionamento energetico di una vasta area del Paese. A questi costi si sono aggiunte le ingenti spese sostenute per le attività di recupero e ripristino, che hanno incluso l'ingaggio di consulenti esperti di cybersecurity, il rafforzamento delle misure di protezione informatica, la gestione tecnica dell'incidente e le comunicazioni di crisi verso i diversi interlocutori, oltre all'assistenza legale necessaria per affrontare le implicazioni normative e contrattuali. Infine, la

sospensione delle operazioni per circa sei giorni ha comportato una significativa perdita di ricavi per l'azienda, che ha dovuto interrompere la fornitura di carburante lungo una tratta che garantisce quasi la metà dell'approvvigionamento della costa orientale degli Stati Uniti. La combinazione tra mancati introiti e costi operativi fissi ha aggravato ulteriormente l'impatto economico immediato dell'incidente. Ma gli effetti dell'attacco non si sono limitati alle perdite subite direttamente dall'azienda. Gli impatti economici indiretti si sono infatti propagati rapidamente a livello nazionale, coinvolgendo diversi settori e milioni di consumatori. Uno degli effetti più evidenti è stato l'aumento dei prezzi del carburante: il prezzo medio della benzina negli Stati Uniti è salito fino a 3,04 dollari per gallone, raggiungendo il livello più alto degli ultimi sei anni [126]. Questa impennata ha inciso in modo significativo sui bilanci delle famiglie lungo la costa orientale e ha generato un effetto domino sui costi di trasporto e, di conseguenza, sui prezzi di numerosi beni di consumo. Le conseguenze si sono fatte sentire anche nel settore dei trasporti. Compagnie aeree e aziende di logistica hanno dovuto affrontare costi operativi maggiori a causa della carenza di carburante, con ricadute sui prezzi dei biglietti aerei e sulle tariffe di spedizione delle merci. A ciò si è aggiunta una situazione di incertezza che ha messo in difficoltà la pianificazione delle operazioni di trasporto, aggravando ulteriormente le perdite per gli operatori del settore. Anche l'industria energetica, a monte e a valle della catena di distribuzione, ha subito contraccolpi significativi. Raffinerie e distributori hanno dovuto far fronte a ritardi e interruzioni nella consegna dei prodotti petroliferi, con conseguente gestione inefficiente delle scorte, accumulo di costi imprevisti e inevitabili perdite economiche. L'attacco ha generato anche impatti di rilievo sul piano sociale, facendo emergere come le conseguenze di un incidente informatico possano ricadere direttamente sui cittadini, incidendo sulla quotidianità e sulle spese delle famiglie. I consumatori, infatti, sono stati tra i soggetti più esposti agli effetti immediati dell'interruzione dell'oleodotto. L'aumento dei prezzi del carburante ha rappresentato uno degli aspetti più tangibili di questa crisi: milioni di automobilisti si sono trovati a dover fronteggiare un rincaro significativo, con un impatto diretto sui bilanci familiari. Tale incremento ha colpito in modo particolare le fasce di popolazione a basso reddito, per le quali la spesa per il carburante rappresenta una voce di costo particolarmente rilevante. Inoltre, la paura di una carenza prolungata di carburante ha alimentato comportamenti di "panic buying", ovvero l'acquisto compulsivo dettato dall'ansia di rimanere senza risorse essenziali. Questo fenomeno ha provocato lunghe code ai distributori, episodi di esaurimento delle scorte e una percezione diffusa di insicurezza nell'approvvigionamento. Non meno rilevante è stato l'impatto sul costo dei trasporti, poiché compagnie aeree e corrieri hanno trasferito l'aumento dei costi operativi sui consumatori finali. Ciò si è tradotto in biglietti aerei più costosi e in un incremento delle tariffe di spedizione, generando ulteriori ripercussioni sui prezzi di beni e servizi

di uso quotidiano. Gli attacchi informatici non generano soltanto costi diretti per le aziende colpite, ma producono una serie di effetti a cascata in grado di colpire l'intera economia e la società nel suo complesso. Secondo il Cost of a Data Breach Report pubblicato da IBM [127] nel 2023, l'impatto medio di una violazione dei dati si attesta intorno ai 4,45 milioni di dollari, ma questo valore rappresenta solo la parte più visibile di un fenomeno molto più ampio e complesso. Oltre al riscatto eventualmente pagato agli attaccanti, le aziende devono affrontare numerosi costi "nascosti", spesso di lungo termine. Tra questi rientrano le spese per le operazioni di ripristino e bonifica dei sistemi, la consulenza di esperti di cybersecurity, la gestione delle comunicazioni di crisi verso stakeholder interni ed esterni, così come la perdita di fiducia da parte dei clienti e i conseguenti danni reputazionali. In casi come quello del Colonial Pipeline, l'azienda è stata percepita non solo come vittima di un attacco sofisticato, ma anche come un'organizzazione impreparata a proteggere infrastrutture di importanza critica per l'intero Paese. Gli effetti a catena di un attacco di tale portata sono stati evidenti anche sui prezzi di beni e servizi essenziali. L'aumento dei costi del carburante e dei trasporti si è riflesso sui prezzi al consumo, incidendo direttamente sui bilanci delle famiglie e sulla competitività delle imprese. La diffusione mediatica della notizia ha contribuito ad alimentare un clima di incertezza e sfiducia: la paura di rimanere senza carburante ha spinto molti cittadini a comportamenti di acquisto compulsivo e ad accumulare scorte di benzina, aggravando ulteriormente la situazione. Non meno rilevanti sono stati gli impatti di natura psicosociale. Gli attacchi informatici di grande risonanza possono infatti generare ansia diffusa, alimentare la sfiducia nelle infrastrutture digitali e nelle istituzioni preposte alla loro protezione, e innescare un senso di vulnerabilità collettiva. Nel caso specifico, la copertura mediatica ha spesso enfatizzato la gravità dell'incidente, trasformando la preoccupazione pubblica in un vero e proprio panico generalizzato. Questo tipo di comunicazione non solo aumenta la pressione sociale, ma contribuisce a mettere in evidenza le criticità di sistemi considerati strategici, amplificando la percezione di insicurezza tra i cittadini. Secondo le stime di Cybersecurity Ventures [128], il costo globale degli attacchi informatici è destinato a raggiungere i 10,5 trilioni di dollari entro la fine del 2025. Tali cifre confermano in modo inequivocabile che la cybersecurity non può più essere considerata un ambito esclusivamente tecnico, ma costituisce ormai una componente imprescindibile della stabilità economica e sociale. L'attacco al Colonial Pipeline dimostra chiaramente che le crisi informatiche non producono solo danni economici immediati, ma hanno anche un impatto profondo sul comportamento collettivo, sulla fiducia del pubblico e sulla percezione generale di sicurezza. Per questa ragione, la gestione delle crisi informatiche dovrebbe prevedere non soltanto misure tecniche di prevenzione e protezione, ma anche strategie di comunicazione efficaci e trasparenti, capaci di

contenere la disinformazione, rassicurare la popolazione e preservare la fiducia nelle infrastrutture e nelle istituzioni.

6.3 Gestione dell'incidente e risposta operativa

Secondo Sean Kerner (2022), Colonial Pipeline ha attivato il proprio protocollo di risposta alle emergenze eseguendo un arresto operativo completo che ha interessato 5500 miglia di struttura pipeline, nel tentativo di impedire al ransomware DarkSide di diffondersi ulteriormente e di minimizzare i danni. Questa decisione drastica ha bloccato l'intera rete dell'oleodotto, ma è stata considerata necessaria per evitare che l'attacco si propagasse ai sistemi operativi, compromettendo potenzialmente la distribuzione fisica del carburante. Successivamente, l'azienda ha avviato una collaborazione con esperti di cybersecurity e con l'FBI, cercando di comprendere come DarkSide fosse riuscito a ottenere l'accesso ai sistemi, come contenere la diffusione del ransomware e come avviare il processo di recupero dei dati. La fase di contenimento della rete ha previsto l'applicazione di procedure di isolamento in 31 località geografiche, portando alla disconnessione strategica di 1.285 endpoint potenzialmente compromessi. I team di sicurezza hanno riconfigurato 89 switch di rete per applicare protocolli di segmentazione avanzata, creando di fatto 23 zone di sicurezza isolate all'interno dell'infrastruttura operativa. L'analisi dettagliata di *Industrial Cybersecurity Pulse* rivela che la fase di ripristino ha seguito un approccio meticolosamente pianificato, distribuito su un arco di 72 ore. La valutazione iniziale della rete ha riguardato 4.827 endpoint distribuiti su 89 segmenti di rete distinti. I team forensi hanno elaborato e analizzato 7,2 terabyte di log di sistema e 3,1 terabyte di dati di configurazione, individuando 147 sistemi che necessitavano di interventi di bonifica immediata e 283 endpoint che richiedevano aggiornamenti di sicurezza critici [129]. Durante le prime 24 ore del ripristino, i team tecnici di Colonial hanno implementato un'infrastruttura di monitoraggio potenziata, integrando 342 sensori di sicurezza di nuova generazione e 17 sistemi avanzati di rilevamento delle intrusioni. Questa espansione ha aumentato la copertura dell'analisi del traffico di rete dal 76,3% al 98,7% delle comunicazioni delle infrastrutture critiche, offrendo una visibilità senza precedenti sulle reti di tecnologia operativa. Il dispiegamento ha incluso capacità di monitoraggio specializzate per i sistemi di controllo industriale (ICS), coprendo l'89% dei sistemi SCADA precedentemente non monitorati. Il secondo e terzo giorno sono stati dedicati al ripristino delle operazioni aziendali critiche, dando priorità ai sistemi di fatturazione e alle piattaforme di interfaccia con i clienti. I team di recupero hanno riportato in funzione l'89% delle applicazioni aziendali principali entro 48 ore, implementando solidi controlli di sicurezza, tra cui l'autenticazione a più fattori per 1.874 account utente e protezioni avanzate degli endpoint su 3.127 dispositivi. L'architettura di sicurezza potenziata ha

incorporato i principi dello *zero-trust*, richiedendo un'autenticazione continua per tutti gli accessi alle tecnologie operative. La sequenza di riavvio dell'oleodotto ha rappresentato la fase più critica delle operazioni di ripristino. A partire dal quarto giorno, i team tecnici hanno validato 247 punti di controllo e testato in modo completo 89 sistemi automatizzati. I flussi iniziali sono stati mantenuti attentamente al 42% della capacità normale, consentendo un monitoraggio dettagliato dell'integrità del sistema e delle metriche di sicurezza. Entro il quinto giorno, la capacità di trasporto è salita al 75% di quella operativa standard, con un monitoraggio continuo di 1.285 sensori che fornivano telemetria di sicurezza in tempo reale. La piena capacità operativa è stata raggiunta al sesto giorno, dopo la validazione completa di tutti i controlli di sicurezza e dei sistemi di monitoraggio.
Nonostante l'imponente risposta tecnica e organizzativa messa in atto per mitigare i danni e prevenire ulteriori compromissioni, Colonial Pipeline decise di pagare un riscatto di 4,4 milioni di dollari in Bitcoin, corrispondenti a circa 75 Bitcoin al momento del pagamento. Purtroppo, le misure di sicurezza messe in atto non furono considerate sufficienti da sole a garantire un ripristino tempestivo dell'intera struttura pipeline. Questa scelta riflette una dinamica paradossale ma ricorrente negli attacchi ransomware: anche quando un'organizzazione dispone di risorse, piani di risposta, tecnologie di monitoraggio e capacità di ripristino indipendenti, la pressione derivante da un'interruzione critica dei servizi essenziali può indurre a cedere alle richieste degli attaccanti. Nel caso di Colonial Pipeline, il decryptor ricevuto dopo il pagamento si rivelò inefficiente e lento, tanto che i gruppi tecnici proseguirono con il ripristino tramite backup sicuri e operazioni manuali. Per mitigare i danni causati dall'interruzione improvvisa dell'oleodotto, furono adottate diverse misure a livello federale. Il Dipartimento dei Trasporti (DoT) emanò direttive specifiche per facilitare il trasporto alternativo di carburante verso le aree più colpite. Fu inoltre decisa la sospensione temporanea delle restrizioni sugli orari di guida per i conducenti di autocisterne, così da accelerare le consegne e garantire la continuità dell'approvvigionamento. Parallelamente, venne avviato un coordinamento con i governi statali per monitorare la distribuzione, ottimizzare le risorse disponibili e ridurre il rischio di panico tra i consumatori. Come riportano Renee Dudley e Daniel Golden [130], in seguito all'incidente, il presidente Joe Biden ha firmato un ordine esecutivo per migliorare la sicurezza informatica delle infrastrutture critiche e creare un modello di risposta federale agli attacchi informatici. Pochi giorni dopo, DarkSide ha annunciato la propria chiusura "sotto la pressione degli Stati Uniti". Tuttavia, come spesso accade in questi casi, il gruppo probabilmente si è semplicemente riorganizzato sotto un nuovo nome, per continuare le proprie attività criminali.
La risposta all'attacco, pur mostrando un buon livello di coordinamento tra azienda e autorità federali, ha rivelato anche la difficoltà di bilanciare la necessità di ripristinare rapidamente le

operazioni e quella di non incentivare ulteriori attacchi pagando il riscatto. L'episodio ha quindi evidenziato la necessità di protocolli di risposta più efficaci e di una maggiore preparazione delle infrastrutture critiche per fronteggiare le minacce informatiche.

6.4 Implicazioni strategiche e considerazioni conclusive

L'attacco a Colonial Pipeline ha messo in luce la necessità critica di potenziare le misure di sicurezza informatica in tutte le infrastrutture critiche. Tra le principali lezioni apprese si evidenziano:

1. Importanza di una risposta tempestiva agli incidenti: La capacità di rilevare e rispondere rapidamente a un attacco è fondamentale per contenere i danni. Secondo John Shier [131], gli investigatori hanno confermato che il punto di ingresso iniziale nella rete di Colonial Pipeline era una singola password rubata, che gli attaccanti sono riusciti a utilizzare senza incontrare ostacoli perché l'account non disponeva dell'autenticazione a più fattori (MFA). Questo dimostra quanto una misura di sicurezza semplice ma efficace come l'MFA possa fare la differenza.
2. Vulnerabilità derivanti da violazioni di dati passate: La password compromessa potrebbe essere stata ottenuta tramite una precedente violazione dei dati non adeguatamente gestita. Questo evidenzia l'importanza di un monitoraggio continuo e di un audit regolare delle credenziali, per identificare e neutralizzare eventuali esposizioni. Come afferma Shier, "le violazioni di dati passate possono avere effetti duraturi se non vengono considerate nel processo di recupero post-attacco".
3. Necessità di sistemi di rilevamento migliorati: I rapporti hanno rivelato che i criminali informatici sono stati presenti nella rete di Colonial Pipeline per almeno otto giorni prima che l'attacco ransomware venisse rilevato. Se il malware fosse stato individuato e isolato tempestivamente, l'interruzione delle operazioni sarebbe stata evitata. Questo sottolinea l'importanza di soluzioni di monitoraggio continuo e di sistemi di rilevamento delle anomalie in tempo reale.
4. Adozione di tecniche di mitigazione avanzate: Come raccomandato dalla Cybersecurity and Infrastructure Security Agency (CISA) [132], Colonial Pipeline e altre organizzazioni critiche dovrebbero implementare:
    - Filtraggio del traffico di rete: per bloccare connessioni sospette.
    - Limitazione dell'accesso alle risorse di rete: per ridurre la superficie di attacco.

- Distribuzione di firme per bloccare connessioni da nodi di uscita Tor e altri servizi anonimi.
- Creazione di zone demilitarizzate (DMZ): per isolare comunicazioni irregolari.
- Allowlisting delle applicazioni: per garantire che solo software autorizzato possa essere eseguito.

5. Miglioramento della collaborazione con le agenzie di sicurezza: A seguito dell'attacco, Colonial Pipeline ha incrementato la collaborazione con le autorità federali e con esperti di cybersecurity, unendo le competenze per rafforzare le proprie difese. L'intervento della CISA e dell'FBI è stato fondamentale per contenere l'impatto e fornire linee guida aggiornate a tutte le organizzazioni a rischio.
6. Consapevolezza del rischio umano e tecnologico: L'incidente ha dimostrato come una singola vulnerabilità, spesso legata a una gestione inadeguata delle credenziali, possa essere sfruttata per compromettere un'intera infrastruttura. Questo richiama l'importanza di una formazione continua del personale in materia di sicurezza informatica, per riconoscere e prevenire i comportamenti a rischio.

L'attacco a Colonial Pipeline è un esempio emblematico che ha messo in luce la fragilità delle infrastrutture critiche di fronte alle minacce informatiche. Non si è trattato solo di un problema tecnico, ma di un fallimento organizzativo che ha evidenziato l'assenza di una strategia di resilienza adeguata. Le vulnerabilità sfruttate dagli aggressori erano note e prevenibili, ma l'azienda si è trovata impreparata a fronteggiarle, priva di piani strutturati di continuità operativa e di strumenti efficaci di risposta e contenimento. Questo incidente ha dimostrato che la cybersecurity non è solo una questione tecnologica, ma un elemento strategico che richiede un approccio integrato. Investire in sicurezza informatica non significa semplicemente adottare tecnologie avanzate, ma sviluppare una cultura della sicurezza diffusa, mantenere un monitoraggio continuo delle vulnerabilità e garantire una capacità di risposta immediata. In assenza di questi elementi, anche una singola vulnerabilità può paralizzare un'intera infrastruttura.
La scelta di non adottare misure di sicurezza di base, come l'autenticazione a più fattori (MFA), evidenzia una visione miope della sicurezza, spesso percepita come un costo e non come un investimento strategico. Questa mentalità ha esposto Colonial Pipeline a un rischio prevedibile, amplificando l'impatto dell'attacco e dimostrando quanto la resilienza non possa essere improvvisata. Il valore di questo caso, soprattutto per un'analisi europea, è ancora più significativo alla luce delle recenti evoluzioni normative. La Direttiva NIS2, il Digital Operational Resilience Act (DORA) e il Cyber Resilience Act stabiliscono oggi obblighi chiari per le organizzazioni critiche,

imponendo controlli minimi di sicurezza, piani di continuità operativa e comunicazione tempestiva con le autorità competenti. Un incidente simile in Europa comporterebbe oggi responsabilità ben più gravi. Questo caso rappresenta quindi un monito attuale: le organizzazioni devono superare l'approccio reattivo e costruire una cultura della sicurezza che sia parte integrante della loro strategia. Resilienza significa essere in grado di prevenire, rilevare, rispondere e recuperare da un attacco informatico, proteggendo non solo la continuità operativa, ma anche la fiducia del pubblico. L'investimento in cybersecurity non è solo una spesa, ma una garanzia di stabilità economica, sociale e istituzionale.

7. Nuove tendenze e tecnologie emergenti in cybersecurity: l'Intelligenza Artificiale

7.1 L'evoluzione delle minacce informatiche e il ruolo strategico dell'IA

Il panorama delle minacce informatiche è oggi caratterizzato da una costante evoluzione e da una crescente complessità. Negli ultimi anni, la criminalità informatica, come visto nei grafici precedenti, non è solo aumentata in frequenza, ma è anche diventata più sofisticata, trasformandosi in un'industria significativa che sfida anche le difese più fortificate. Attacchi di alto profilo, come "Colonial Pipeline" analizzato nel capitolo precedente, rappresentano esempi emblematici della portata e della complessità delle minacce contemporanee. Tali episodi costituiscono casi di studio fondamentali per l'analisi delle tecniche impiegate dagli attori malevoli e per l'individuazione delle principali vulnerabilità presenti nei sistemi di cybersicurezza attuali [133]. Questi eventi, di natura e impatto differenti, evidenziano la varietà e la pervasività delle minacce informatiche moderne, offrendo preziosi spunti per comprendere meglio le dinamiche delle violazioni e le loro conseguenze a livello sistemico. A fronte di uno scenario così complesso e in continua mutazione, le strategie di difesa tradizionali, basate su regole statiche o su interventi esclusivamente reattivi, si sono dimostrate inadeguate a garantire una protezione efficace e sostenibile. Di conseguenza, l'attenzione si è progressivamente spostata sull'impiego dell'Intelligenza Artificiale (IA) come strumento strategico per potenziare le capacità di rilevamento e risposta agli incidenti di sicurezza. Grazie all'uso di algoritmi di machine learning (ML) e di tecniche di analisi predittiva, l'IA consente infatti di superare i limiti degli approcci convenzionali, rendendo possibile un monitoraggio continuo e una risposta adattiva alle minacce in costante evoluzione. Tali tecnologie consentono di affrontare in modo più tempestivo ed efficace minacce complesse, come i malware di nuova generazione e gli exploit *zero-day* [134], ossia quei cyberattacchi che sfruttano vulnerabilità ancora sconosciute per le quali non esistono contromisure predefinite. L'apprendimento automatico consente di correlare milioni di

eventi in tempo reale, estraendo pattern significativi da enormi quantità di dati, senza richiedere un incremento proporzionale delle risorse umane o infrastrutturali. In tal modo, le organizzazioni possono scalare i propri processi di sicurezza, mantenendo elevati standard di resilienza e capacità di risposta. Con l'espansione delle infrastrutture digitali e l'aumento esponenziale dei dati da monitorare, l'adozione di IA consente di scalare i processi di sicurezza senza richiedere un corrispondente aumento delle risorse umane o materiali. In questo contesto si assiste a un cambiamento significativo: da un approccio prevalentemente reattivo a uno sempre più proattivo, in cui le capacità predittive dell'IA vengono impiegate per analizzare incidenti pregressi e comportamenti di sistema in tempo reale, al fine di anticipare e prevenire potenziali attacchi futuri. Diversi contributi accademici hanno esaminato in modo sistematico l'impiego dell'Intelligenza Artificiale nella sicurezza informatica, offrendo una panoramica che abbraccia l'evoluzione storica della criminalità digitale, l'analisi delle tecnologie emergenti e lo sviluppo di modelli predittivi per la gestione delle minacce. La forza distintiva dell'IA risiede proprio nella sua capacità di dar vita a modelli adattivi, in grado di reagire dinamicamente ai cambiamenti del contesto operativo. [135] Questo meccanismo di apprendimento continuo costituisce un valore aggiunto per le strategie di protezione, poiché consente di colmare progressivamente le vulnerabilità identificate e di rafforzare l'intero ecosistema difensivo. Non a caso, l'IA è oggi considerata non solo un'innovazione tecnologica, ma un pilastro strutturale delle architetture digitali di ultima generazione e come sottolinea Mengidis et al. [136], le organizzazioni che integrano soluzioni intelligenti nelle proprie infrastrutture IT registrano miglioramenti significativi sia in termini di efficienza operativa sia nella qualità e tempestività dei servizi offerti, trasformando i processi aziendali e produttivi e modificando profondamente le modalità decisionali e strategiche delle organizzazioni. Dal punto di vista metodologico, emergono tre approcci principali che alimentano la ricerca e l'applicazione concreta dell'IA nella cybersicurezza. Il primo è l'analisi storica, impiegata per tracciare l'evoluzione dei modelli di attacco e comprendere come le minacce si siano sviluppate nel tempo. Attraverso un monitoraggio sistematico e una valutazione critica dell'efficacia delle contromisure adottate, i ricercatori possono derivare indicazioni preziose per definire strategie di difesa più efficaci. Tuttavia, l'affidabilità di questo approccio dipende dalla disponibilità di un archivio di dati storico accurato e aggiornato, che garantisca una base empirica solida per le elaborazioni successive. Il secondo approccio è la valutazione tecnologica, che si concentra sull'esame critico delle soluzioni di IA già esistenti, verificandone i punti di forza e le criticità nella rilevazione e gestione delle minacce. Tale metodologia si avvale di ambienti di prova controllati, dove i sistemi vengono messi alla prova contro minacce simulate: queste simulazioni sono indispensabili per misurare la capacità di rilevamento e i tempi di risposta, ma richiedono un aggiornamento continuo per restare efficaci di fronte a minacce

sempre più sofisticate. Il terzo approccio è rappresentato dalla modellazione predittiva, che si distingue per il suo orientamento proattivo. Essa sfrutta l'ampio patrimonio di dati storici per anticipare potenziali minacce future, grazie all'impiego di algoritmi avanzati di IA e machine learning. Questa metodologia consente di individuare vulnerabilità latenti e di predisporre misure preventive mirate. Tuttavia, l'adozione di modelli predittivi solleva questioni delicate, in particolare riguardo alla gestione di dati sensibili e alla tutela della privacy: diventa dunque essenziale trovare un equilibrio tra l'uso dei dati per finalità di sicurezza e il rispetto delle responsabilità etiche e normative. Negli ultimi anni si sta affermando una tendenza integrativa, che mira a unificare questi approcci in un quadro metodologico più ampio e coerente. L'obiettivo è combinare i risultati delle analisi storiche con le evidenze derivanti dalla valutazione tecnologica, potenziando così la precisione e la rilevanza dei modelli predittivi. Questo approccio sinergico richiede una stretta cooperazione tra diversi gruppi di ricerca e l'integrazione di fonti di dati eterogenee. La principale sfida, in questo caso, è riuscire a sincronizzare informazioni e intuizioni provenienti da ambiti differenti, così da definire una strategia di cybersicurezza che sia al tempo stesso solida, dinamica e realmente applicabile. Un framework integrato non solo massimizza i punti di forza dei singoli approcci, ma produce anche un effetto di rafforzamento reciproco che incrementa la resilienza complessiva delle infrastrutture digitali. In questa prospettiva, l'IA si configura come il motore di un ecosistema difensivo capace di evolversi in modo autonomo, adattandosi alle trasformazioni di un contesto operativo sempre più complesso e interconnesso. L'IA si distingue per la sua versatilità in ambito cybersecurity, adattandosi a contesti applicativi differenti e rispondendo a esigenze settoriali specifiche. In ambito finanziario, ad esempio, la gestione di grandi quantità di dati sensibili e l'elevato rischio di attività fraudolente impongono l'adozione di soluzioni di sicurezza avanzate. In questo contesto, i sistemi antifrode basati su IA si sono dimostrati particolarmente efficaci nel rilevare transazioni sospette e nel prevenire frodi in tempo reale [137]. Anche nel settore sanitario, l'intelligenza artificiale ha trovato applicazioni sempre più ampie, in particolare nella protezione delle cartelle cliniche elettroniche (*Electronic Health Records* – EHR), alla luce delle crescenti preoccupazioni legate alla fuga di dati personali [138]. L'espansione della telemedicina e delle soluzioni digitali per la salute ha infatti amplificato il rischio di accessi non autorizzati, rendendo l'IA uno strumento cruciale per garantire la riservatezza e l'integrità delle informazioni sanitarie. Nel settore pubblico le tecnologie basate su IA sono state adottate per rafforzare i framework di protezione delle infrastrutture critiche e migliorare la sicurezza nazionale. Come osservano Ahmad et al. [139], l'IA viene impiegata per contrastare le minacce informatiche rivolte a settori strategici come le reti elettriche, i sistemi di trasporto e le comunicazioni. Un esempio emblematico è rappresentato dal Dipartimento della Sicurezza Interna degli Stati Uniti (*Department of Homeland Security*), che ha

implementato soluzioni basate su intelligenza artificiale non solo per difendersi da attacchi informatici, ma anche per condurre operazioni proattive di contrasto alle minacce emergenti. L'adozione dell'intelligenza artificiale ha contribuito, in determinati contesti, a una generale riduzione della criminalità informatica. Il monitoraggio continuo del traffico di rete e la capacità di individuare comportamenti sospetti in tempo reale rappresentano strumenti efficaci per intervenire prima che l'attacco comprometta l'integrità dei dati o la funzionalità dei sistemi. In particolare, questa prontezza di reazione si rivela cruciale nei settori più sensibili, dove la protezione delle informazioni è strettamente connessa alla sicurezza nazionale, alla salute pubblica o alla stabilità finanziaria. Come affermano Kumar e Singla [140], tale caratteristica la rende un pilastro fondamentale delle moderne infrastrutture di sicurezza digitale. L'efficacia dell'intelligenza artificiale nella protezione dei sistemi informativi si riflette anche nella varietà di minacce che essa è in grado di contrastare. Le applicazioni più diffuse riguardano il rilevamento e la mitigazione di attacchi di phishing, ransomware e DDoS, che rappresentano le tipologie di incidenti informatici più frequenti e dannose per le organizzazioni. I sistemi basati su IA, grazie alla loro capacità di analisi comportamentale in tempo reale, offrono un supporto determinante nella risposta a queste minacce. Come evidenzia la figura seguente, il phishing costituisce la categoria più rilevante tra quelle intercettate dai sistemi intelligenti, seguito da ransomware e attacchi distribuiti di tipo denial-of-service. Questo dato conferma la capacità dell'IA di intervenire su vettori di attacco eterogenei, offrendo una protezione trasversale e adattiva.

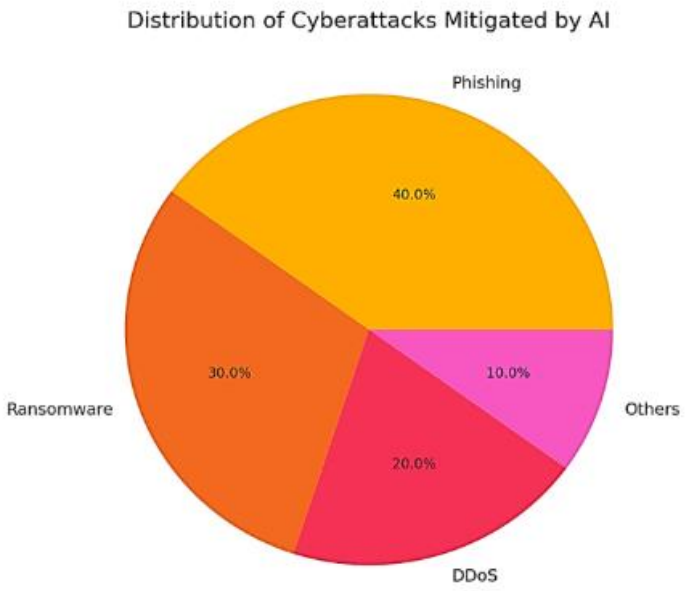

Figura 18 - Distribuzione percentuale degli attacchi informatici mitigati dall'Intelligenza Artificiale

Un ulteriore contributo importante dell'intelligenza artificiale riguarda la valutazione predittiva del rischio. Attraverso l'analisi storica di incidenti informatici e la mappatura delle vulnerabilità note,

gli algoritmi intelligenti sono in grado di individuare punti deboli potenziali e suggerire interventi correttivi prima che il danno si verifichi [141]. Questo approccio proattivo ha introdotto un vero e proprio cambio di paradigma nella cybersicurezza: si è infatti passati da un modello puramente reattivo, incentrato sulla gestione dell'emergenza, a uno preventivo e predittivo, basato sull'analisi del rischio e sull'intervento automatizzato. Tale trasformazione ha permesso alle organizzazioni non solo di individuare con maggiore rapidità le minacce informatiche, ma anche di affrontarle in modo più strutturato, rafforzando la resilienza dell'intero sistema informativo. L'integrazione delle tecniche di machine learning nei processi di cybersecurity ha quindi prodotto un impatto profondo, delineando un nuovo assetto difensivo che si fonda sull'autonomia decisionale dei sistemi e sulla capacità di adattamento alle condizioni operative in continua evoluzione. Nonostante questi progressi, è importante considerare anche le implicazioni e le sfide associate all'adozione di tecnologie intelligenti. La crescente centralità dell'IA nei sistemi aziendali ha sollevato questioni rilevanti legate alla protezione dei dati personali e alla gestione sicura delle informazioni sensibili. Come osservano Perols e Murthy [142], l'implementazione di soluzioni basate su IA ha determinato una trasformazione profonda dei processi organizzativi, costringendo le imprese a ripensare le proprie strategie di sicurezza per rispondere all'ampliamento della superficie d'attacco e alla maggiore complessità dei sistemi. In questo contesto, si rende necessario non solo sfruttare l'IA come strumento di difesa, ma anche affrontare con attenzione le implicazioni etiche e normative derivanti dal suo utilizzo. Tra i principali aspetti critici vi sono la trasparenza e l'interpretabilità degli algoritmi, la sicurezza dei dati impiegati per l'addestramento dei modelli e il rispetto delle normative vigenti in materia di protezione dei dati, come il Regolamento generale sulla protezione dei dati (GDPR). L'intelligenza artificiale, quindi, pur rappresentando una risorsa di straordinario valore strategico, impone anche nuove responsabilità a chi la implementa, soprattutto nei contesti in cui essa è chiamata a trattare informazioni sensibili in maniera automatizzata. Con l'evoluzione costante delle minacce digitali e la crescita esponenziale della complessità dei sistemi informativi, le tecnologie basate su IA sono destinate ad assumere ruoli sempre più diversificati e centrali nella protezione dei dati e delle infrastrutture. In un panorama in cui le organizzazioni gestiscono quotidianamente enormi volumi di informazioni sensibili, l'adozione di soluzioni intelligenti non è più un'opzione, ma una necessità strategica per garantire adeguati livelli di sicurezza e resilienza. Guardando al futuro, è ragionevole prevedere che l'intelligenza artificiale sarà integrata in misura sempre maggiore nelle architetture di cybersicurezza, dando origine a sistemi capaci di apprendere autonomamente, adattarsi a nuovi scenari e rispondere con tempestività e precisione alle minacce più complesse. Questo sviluppo apre la strada a una nuova generazione di difese digitali, basate su

modelli predittivi, capacità adattive e autonomia operativa, che costituiranno la base della cybersicurezza del prossimo decennio.

7.2 Tecniche e applicazioni operative dell'IA nella cybersicurezza

L'integrazione dell'intelligenza artificiale (IA) nei sistemi di cybersicurezza non si limita all'adozione di strumenti automatizzati, ma coinvolge un insieme articolato di tecniche avanzate e applicazioni operative capaci di trasformare profondamente le modalità con cui vengono rilevate, analizzate e contrastate le minacce informatiche. In questo contesto, l'IA non è solo una tecnologia di supporto, ma un elemento strategico e adattivo, in grado di apprendere dai dati, anticipare comportamenti anomali e rispondere in modo proattivo agli attacchi. In questo contesto, le tecniche basate sull'IA si intrecciano sempre più strettamente con le applicazioni pratiche, dando vita a soluzioni avanzate in grado di rispondere con efficacia alla crescente complessità delle minacce informatiche. Il presente paragrafo intende analizzare in maniera sistematica queste tecnologie e il loro impatto sul piano operativo, mettendo in evidenza i benefici che ne derivano in termini di tempestività, adattabilità e resilienza delle infrastrutture digitali.

7.2.1 Signature-based detection

Uno degli effetti più rilevanti dell'intelligenza artificiale sulla cybersicurezza si riscontra nell'uso delle tecniche basate su firma (signature-based techniques). La capacità dell'IA di analizzare e riconoscere codici di firma si configura come una delle sue competenze chiave in questo settore. Attraverso questi metodi, l'IA è in grado di individuare malware e attacchi informatici rilevando i codici specifici presenti nelle minacce. Questi codici vengono identificati mediante algoritmi di intelligenza artificiale sviluppati appositamente [143]. Il processo prevede il confronto tra la firma individuata e quelle già archiviate in precedenza in database dedicati, consentendo al team di cybersicurezza di reagire con maggiore rapidità ed efficacia. Comprendere fin da subito la natura dell'attacco aiuta infatti a definire in tempi brevi le risorse e le strategie necessarie per contenerlo. Prima che l'IA fosse applicata alla cybersicurezza, simili operazioni richiedevano tempi molto più lunghi, aumentando il rischio di errori e provocando spesso gravi danni. Il database dove vengono raccolte le firme di malware noti è comunemente chiamato "blacklist". Qui il sistema confronta ogni nuova firma rilevata con quelle già catalogate, così da identificare e bloccare tempestivamente eventuali minacce. Le firme, che rappresentano schemi comportamentali tipici degli attacchi, sono alla base di un tipo di apprendimento automatico fondato sul riconoscimento di pattern. Nonostante l'efficacia dimostrata negli anni, questo approccio presenta delle limitazioni: se l'attacco è completamente nuovo, privo cioè di una firma già registrata nel database, il sistema può non

riuscire a rilevarlo. Tuttavia, le tecniche basate su firma si sono rivelate determinanti nel contrastare un'ampia gamma di minacce informatiche conosciute. Tuttavia, i criminali informatici particolarmente esperti sono riusciti, in alcuni casi, ad aggirare questi sistemi modificando deliberatamente i pattern delle minacce per eludere il rilevamento. Alterando le firme, riescono ad accedere ai dati prima che il sistema possa identificarli. Nonostante queste criticità, le tecniche basate su firma hanno avuto un impatto significativo sulla sicurezza informatica, consentendo di individuare e neutralizzare la maggior parte degli attacchi conosciuti.

7.2.2 Rilevamento delle Intrusioni di Rete (Network Intrusion Detection)

Gli attacchi alle reti rappresentano una delle modalità più comuni con cui vengono perpetrate aggressioni informatiche. Poiché le reti sono alla base del funzionamento di organizzazioni e aziende, la capacità di rilevare tempestivamente eventuali intrusioni è diventata fondamentale per garantire la sicurezza dei dati. È proprio in questo ambito che l'intelligenza artificiale ha mostrato tutto il suo potenziale, rendendo il rilevamento delle intrusioni di rete più semplice, rapido ed efficace. L'integrazione dell'IA nei firewall di rete ha aumentato in modo significativo la capacità di impedire accessi non autorizzati, rendendo le reti aziendali molto più resistenti agli attacchi. Prevenire le intrusioni a livello di rete rappresenta infatti il primo e più importante passo per proteggere le informazioni sensibili. Grazie all'uso dell'intelligenza artificiale, è oggi possibile intercettare molte minacce in fase iniziale e prevenire potenziali attacchi futuri, poiché le linee guida di sicurezza vengono incorporate direttamente nei sistemi di rete. Nei sistemi di rilevamento delle intrusioni di rete, *Network Intrusion Detection Systems* (NIDS) [144], basati su IA, si individuano cinque componenti chiave che contribuiscono alla protezione complessiva delle reti. Il primo e più rilevante è la capacità dei sistemi intelligenti di raccogliere ed elaborare grandi volumi di dati provenienti dal traffico di rete. Questo permette di identificare con precisione anomalie, tentativi di intrusione e comportamenti sospetti, spesso in tempo reale. Bloccare un attacco direttamente a livello di rete è cruciale: intervenire sul punto di accesso al sistema riduce drasticamente il rischio che le informazioni vengano compromesse. L'intelligenza artificiale, grazie alle sue tecniche avanzate, consente di individuare e neutralizzare tutti i possibili vettori di compromissione. Le analisi disponibili dimostrano come l'adozione dell'IA abbia trasformato profondamente la cybersicurezza, soprattutto per quanto riguarda la protezione delle reti. I sistemi intelligenti vengono continuamente addestrati a riconoscere nuove forme di attacco e a intervenire preventivamente, garantendo così l'integrità della rete. Questo processo di apprendimento continuo è uno degli elementi che ha reso l'IA una risorsa fondamentale per il rafforzamento delle infrastrutture informatiche. In conclusione, la protezione delle reti aziendali attraverso l'impiego

dell’intelligenza artificiale rappresenta oggi uno dei settori più avanzati e promettenti della cybersicurezza moderna.

7.2.3 Gestione delle Vulnerabilità (Vulnerability Management)

Un altro ambito in cui l’intelligenza artificiale sta apportando benefici significativi alla cybersicurezza è quello della gestione delle vulnerabilità. In questo contesto, l'IA viene utilizzata per individuare, monitorare e gestire in modo efficiente le potenziali debolezze presenti nei sistemi informatici delle organizzazioni. Secondo alcuni studi, solo nel 2019 sono state segnalate circa 20.362 vulnerabilità, con un incremento del 18% rispetto all'anno precedente [145]. Un dato che mette in evidenza come la crescita delle minacce sia continua, rendendo sempre più complessa e gravosa la loro gestione per il personale umano. Di fronte a questa evoluzione del rischio, è diventato indispensabile affidarsi a soluzioni basate sull'intelligenza artificiale. I sistemi IA permettono infatti di automatizzare il rilevamento e la classificazione delle vulnerabilità conosciute, riducendo in modo significativo i tempi di reazione e minimizzando il rischio di errore umano. Questa capacità di intervento rapido e preciso ha reso più difficile per gli hacker sfruttare le debolezze presenti nei sistemi, migliorando così il livello complessivo di sicurezza delle organizzazioni. La gestione automatizzata delle vulnerabilità si configura quindi come uno dei principali vantaggi introdotti dall’intelligenza artificiale nel campo della cybersicurezza. Secondo una ricerca di IBM sul mercato dell’IA applicata alla sicurezza informatica, che ha analizzato l’andamento delle vulnerabilità divulgate a livello globale, la spesa per la protezione nel cyberspazio continua a crescere, nonostante le difficoltà legate alla pandemia di COVID-19. Attraverso l’impiego di sistemi intelligenti, le organizzazioni sono ora in grado di monitorare costantemente la propria infrastruttura IT, di attribuire priorità alle vulnerabilità più critiche e di implementare rapidamente le misure correttive necessarie. Questo approccio proattivo, reso possibile dall'IA, contribuisce in modo determinante alla prevenzione degli attacchi e al rafforzamento della sicurezza complessiva.

In passato, molti attacchi riuscivano a compromettere i sistemi proprio approfittando della lentezza dei processi di gestione delle vulnerabilità. Oggi, invece, i sistemi IA dedicati a questa funzione sono capaci di rilevare e segnalare i tentativi di attacco in tempo reale, migliorando sensibilmente la protezione dei dati e dei sistemi. Un ulteriore punto di forza dell'approccio basato sull'IA è rappresentato dalla capacità degli algoritmi di machine learning di riconoscere comportamenti anomali negli account utente. Questo consente di individuare rapidamente eventuali minacce interne, come account compromessi o comportamenti sospetti da parte di utenti legittimi. Grazie alla gestione intelligente delle vulnerabilità, i server aziendali risultano oggi molto più protetti e le informazioni archiviate sono tutelate con maggiore efficacia. In sintesi, l'introduzione

dell'intelligenza artificiale ha trasformato la gestione delle vulnerabilità da un processo tradizionalmente reattivo e manuale a un approccio proattivo, continuo e automatizzato, rafforzando in modo significativo la resilienza delle infrastrutture informatiche.

7.2.4 Sicurezza dei Data Center (Data Centers Security)

La cybersicurezza comprende tutte le attività volte a proteggere i dati da attacchi informatici e altre minacce, e, come già emerso nei paragrafi precedenti, l'intelligenza artificiale ha reso questi processi decisamente più rapidi ed efficaci. In particolare, i data center rappresentano una delle infrastrutture più critiche da tutelare nell'ambito della cybersicurezza [146]. Con l'introduzione dell'IA, molti dei processi fondamentali all'interno dei data center sono stati automatizzati, con significativi miglioramenti sia in termini di efficienza sia di sicurezza operativa. Tra i parametri più importanti gestiti oggi con il supporto dell'intelligenza artificiale troviamo il consumo energetico, l'uso della banda di rete e il controllo delle temperature. Poiché gli operatori umani sono suscettibili di errori, l'impiego dell'IA assicura una gestione più precisa, continua e affidabile di questi aspetti cruciali. Un altro elemento da considerare riguarda i costi di manutenzione dell'hardware, che possono essere notevolmente ridotti grazie all'utilizzo di sistemi intelligenti. I data center, infatti, devono essere protetti non soltanto da minacce informatiche, ma anche da rischi ambientali, considerando che custodiscono informazioni sensibili appartenenti a clienti e organizzazioni. Per questo motivo, l'intelligenza artificiale viene impiegata anche nel monitoraggio e nella gestione della sicurezza fisica delle infrastrutture, oltre che nel controllo delle operazioni digitali. Negli ultimi anni, sempre più aziende hanno scelto di integrare soluzioni basate su IA all'interno dei propri data center, puntando a garantire livelli più elevati di sicurezza e di efficienza. Questo trend sottolinea ulteriormente come l'intelligenza artificiale abbia avuto un impatto positivo non solo nella protezione contro i cyber attacchi, ma anche nella gestione ottimizzata delle risorse tecnologiche e fisiche. È importante, tuttavia, ricordare che, sebbene i benefici derivanti dall'adozione dell'IA siano numerosi, l'uso di queste tecnologie non è esente da criticità e limiti, che verranno analizzati nelle sezioni successive.

7.2.5 Rilevamento e Risposta in Tempo Reale

I sistemi di rilevamento e risposta in tempo reale (RTDR, *Real-Time Detection and Response*) rappresentano una componente fondamentale nei moderni framework di sicurezza, in quanto consentono alle organizzazioni di individuare e contrastare rapidamente le minacce nel momento stesso in cui si manifestano. Tali sistemi si avvalgono di tecniche avanzate di analisi automatizzata, come l'intelligenza artificiale (IA) e il machine learning (ML), che permettono di processare grandi

volumi di dati provenienti da reti, endpoint e log di sistema, allo scopo di rilevare in tempo reale comportamenti anomali o segnali di compromissione. L'efficacia della risposta in tempo reale è cruciale per la mitigazione degli attacchi informatici, poiché un intervento ritardato espone l'organizzazione a elevati rischi di perdita di dati, danni economici e compromissione della reputazione [147]. Come mostra la Figura 19, l'introduzione di sistemi RTDR nelle organizzazioni ha comportato un abbattimento drastico dei tempi di risposta e dei costi legati agli incidenti informatici. Prima dell'adozione del sistema, il tempo medio di rilevamento era di circa 30 giorni, mentre quello di risposta si aggirava intorno ai 20 giorni. Dopo l'integrazione di RTDR, tali valori si sono ridotti rispettivamente a 1 giorno per la rilevazione e 1 giorno per la risposta, dimostrando un miglioramento radicale nei processi di gestione degli incidenti. Ancora più significativo è il dato relativo ai costi degli incidenti: secondo un'analisi condotta dal Ponemon Institute [148], le spese medie per attacco sono diminuite da 350.000 dollari a 50.000 dollari, grazie alla rapidità di intervento garantita dai sistemi intelligenti. Questo calo, pari a una riduzione dell'85% circa, evidenzia non solo l'efficacia tecnica delle soluzioni RTDR, ma anche il loro impatto strategico in termini di ottimizzazione delle risorse e protezione degli asset aziendali. L'adozione di questi sistemi è inoltre potenziata dall'integrazione con feed di threat intelligence, che forniscono informazioni aggiornate su nuovi vettori di attacco, comportamenti sospetti e indicatori di compromissione. Tali dati, una volta integrati nei motori di analisi automatica, contribuiscono a rendere le risposte ancora più contestualizzate ed efficaci [149]. Alla luce di queste evidenze, i sistemi RTDR non sono più un'opzione avanzata riservata a grandi aziende, ma uno strumento imprescindibile per ogni organizzazione che voglia difendere efficacemente i propri sistemi in un contesto digitale sempre più esposto a minacce complesse e persistenti.

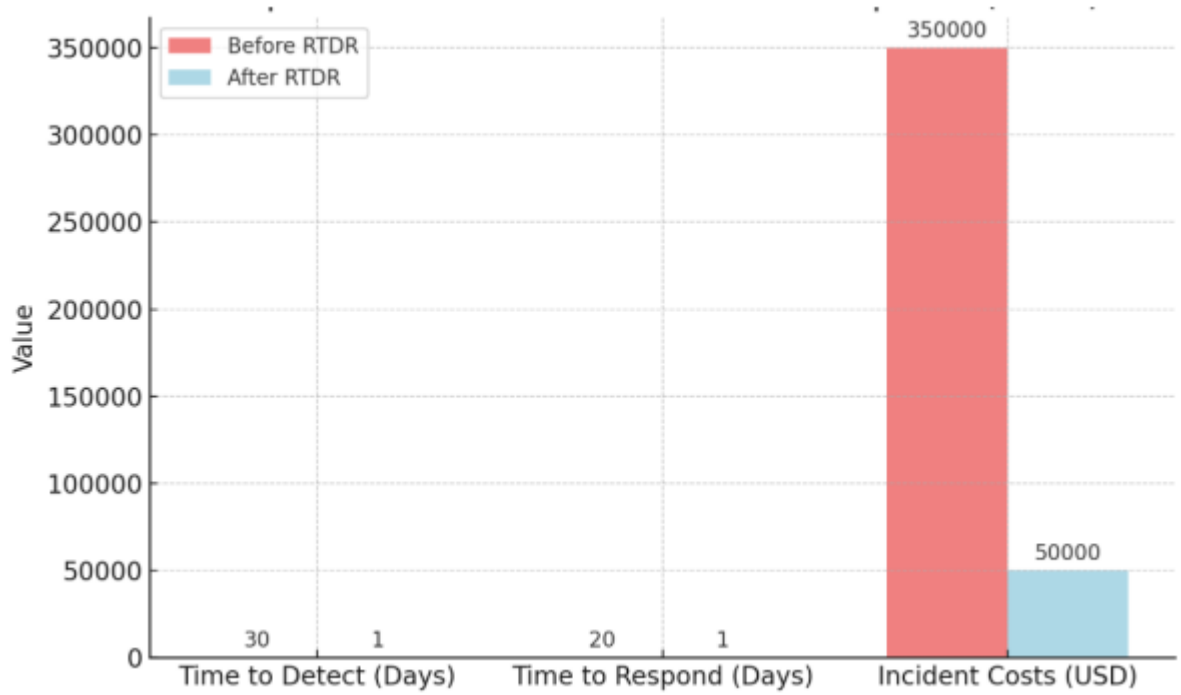

Figura 19 - Confronto dell'efficacia operativa prima e dopo l'adozione di sistemi di Real-Time Detection and Response (RTDR)

7.2.6 L'approccio basato su Machine Learning

Nel panorama delle tecniche di intelligenza artificiale applicate alla cybersicurezza, l'approccio basato su machine learning (ML) rappresenta una delle soluzioni più efficaci, versatili e strategiche per il contrasto alle minacce informatiche. Il ML si fonda sulla capacità dei sistemi di apprendere automaticamente dai dati, riconoscere schemi e migliorare le proprie prestazioni nel tempo senza una programmazione esplicita. L'integrazione di queste tecnologie nei framework di sicurezza informatica consente di potenziare le capacità di rilevamento, analisi e risposta in maniera radicale. Questo paradigma ha radicalmente trasformato le modalità con cui si gestisce la sicurezza digitale, superando le limitazioni dei metodi tradizionali basati su regole fisse, e aprendo la strada a forme di difesa intelligenti, adattive e in grado di evolvere insieme al panorama delle minacce.
L'integrazione del machine learning nei sistemi di cybersecurity ha avuto un impatto profondo dovuto alla sua capacità di elaborare grandi quantità di dati in tempo reale, il machine learning è oggi in grado di rilevare anomalie comportamentali, attacchi zero-day e minacce avanzate APT (Advanced Persistent Threats) che sfuggirebbero facilmente ai controlli tradizionali. I sistemi intelligenti analizzano continuamente flussi informativi eterogenei, come traffico di rete, log di sistema e accessi utente e dati da endpoint, per individuare eventi sospetti. Rispetto all'analisi manuale, che è soggetta a errori, limiti cognitivi e vincoli temporali, gli algoritmi di apprendimento automatico garantiscono una maggiore affidabilità e tempestività [150]. Due tra le tecniche di

machine learning, la classificazione e il clustering, si sono dimostrate estremamente efficaci nell'individuare minacce. La classificazione consente al sistema di distinguere in modo automatico tra traffico lecito e malevolo, assegnando etichette predittive agli eventi osservati. Il clustering permette di individuare comportamenti sospetti attraverso il raggruppamento di dati simili che, pur non etichettati, mostrano pattern potenzialmente anomali. Questi strumenti si rivelano particolarmente efficaci perché permettono di rilevare attacchi in tempo reale, anche su dataset complessi e voluminosi, superando di gran lunga le capacità di analisi manuale. L'efficacia del ML non si limita alla fase di rilevamento: i modelli intelligenti si dimostrano fondamentali anche nell'analisi contestuale e nella risposta automatizzata agli incidenti, ma grazie alla capacità di correlare eventi provenienti da fonti disparate, i sistemi di machine learning riescono a costruire una comprensione approfondita degli attacchi in corso, facilitando interventi mirati e tempestivi. Ad esempio, una volta rilevata un'anomalia, il sistema può avviare automaticamente contromisure preconfigurate, come l'isolamento di host compromessi, il blocco di indirizzi IP sospetti o l'interruzione di sessioni dannose. Questo tipo di intervento si rivela essenziale in presenza di minacce ad alta velocità di propagazione, come i ransomware. Una delle qualità più significative del machine learning è la sua capacità di apprendere dai dati passati [151]. Analizzando archivi storici, i modelli predittivi sono in grado di identificare pattern ricorrenti e anticipare comportamenti potenzialmente dannosi. In particolare, questi sistemi permettono di intercettare le cosiddette TTP, Tactics, Techniques and Procedures, comunemente utilizzate dagli attaccanti, suggerendo miglioramenti continui alle policy di sicurezza. Tale apprendimento progressivo rende il machine learning uno strumento flessibile e resiliente, capace di aggiornarsi in risposta all'evoluzione delle minacce. Non meno importante è l'aspetto della scalabilità operativa: in un contesto in cui le infrastrutture digitali sono sempre più estese e interconnesse, i sistemi possono essere implementati su larga scala senza richiedere un incremento proporzionale delle risorse umane impiegate e questo consente di mantenere elevati standard di sicurezza anche in ambienti complessi e distribuiti. L'adozione di modelli predittivi basati su ML è oggi considerata un elemento centrale della strategia di difesa informatica. Queste tecnologie si sono dimostrate efficaci nel rilevare e contrastare le minacce informatiche, risultando particolarmente preziose nei contesti caratterizzati da grandi volumi di dati e da scenari in rapido cambiamento. Le ricerche più recenti evidenziano come queste tecnologie siano sempre più utilizzate per anticipare attacchi informatici sulla base dell'analisi del traffico di rete e del rilevamento di anomalie indicative di comportamenti malevoli. In settori come la sanità, la finanza e l'industria, tali modelli sono già impiegati per prevedere eventi critici, supportando decisioni preventive. Sul piano più ampio, i benefici dell'integrazione ML nella cybersicurezza possono essere sintetizzati lungo quattro direttrici principali:

1. Rilevamento avanzato: individuazione in tempo reale di comportamenti anomali e minacce emergenti attraverso l'analisi continua di flussi informativi complessi.
2. Capacità predittive: anticipazione degli attacchi futuri mediante l'identificazione di pattern ricorrenti e l'incrocio di informazioni da fonti eterogenee, incluse dark web e intelligence esterna.
3. Risposta automatizzata: attivazione tempestiva di contromisure per contenere gli incidenti e limitarne o neutralizzarne l'impatto.
4. Apprendimento continuo: aggiornamento dinamico dei modelli in base ai dati più recenti, con miglioramenti progressivi nelle prestazioni di rilevamento e prevenzione.

Questi elementi dimostrano come l'adozione di IA nella cybersicurezza non rappresenti solo un'evoluzione tecnologica, ma anche un cambio di paradigma nella gestione delle minacce digitali. Nonostante l'impatto trasformativo del ML nella cybersecurity, permangono alcune criticità. In particolare, l'affidabilità e la generalizzabilità dei modelli rimangono oggetto di dibattito. In scenari complessi, infatti, i modelli potrebbero non riuscire a interpretare correttamente nuove minacce se non addestrati su dati adeguati. Per ovviare a tale limite, si stanno sviluppando approcci ibridi che combinano ML con modellazione tradizionale e simulazioni, con l'obiettivo di ottenere risultati più stabili e affidabili. Un'altra sfida riguarda l'uso malevolo delle stesse tecnologie da parte degli attaccanti, che sfruttano l'IA per creare malware intelligenti o per ingannare i sistemi tramite input avversariali [152]. In risposta, diventa sempre più urgente implementare misure etiche e normative che disciplinino l'uso dell'IA nella cybersicurezza. Come sottolineato da numerosi studi, è fondamentale adottare pratiche di sviluppo responsabile che includano trasparenza, rendicontabilità e protezione della privacy. Il potenziale di crescita del settore è notevole: il mercato globale delle soluzioni IA e ML per la cybersicurezza è stimato in forte espansione, con previsioni di crescita da 8,6 miliardi di dollari nel 2019 a oltre 100 miliardi entro il 2030. Questo dato riflette l'interesse crescente delle imprese verso strumenti in grado di affrontare le sfide digitali con maggiore flessibilità, rapidità e precisione. Inoltre, i modelli di ML sfruttano ampi archivi di dati storici per eccellere nel riconoscimento avanzato dei modelli. Ciò consente loro di rilevare schemi complessi associati a diversi tipi di minacce informatiche, inclusi sofisticati schemi di phishing e potenziali minacce interne che i metodi tradizionali potrebbero non identificare facilmente. Integrando IA e ML nei sistemi di cybersicurezza, le organizzazioni possono migliorare significativamente le proprie capacità di rilevamento e i tempi di risposta, rafforzando così le proprie difese in un panorama di minacce in continua evoluzione. L'integrazione del Machine Learning nella cybersicurezza rappresenta un passo avanti significativo nella lotta contro minacce informatiche

sempre più sofisticate. L'approccio basato su machine learning non rappresenta soltanto una novità tecnica, ma un vero e proprio cambio di paradigma nella difesa cibernetica. Esso consente alle organizzazioni di passare da una postura reattiva a una strategia predittiva e proattiva, migliorando la capacità di rilevare, analizzare, contenere e prevenire le minacce in un ambiente digitale sempre più complesso e interconnesso. L'efficacia di questo cambio di paradigma è dimostrata anche da numerosi indicatori quantitativi. Come riportato nella Tabella 20, l'integrazione di modelli di intelligenza artificiale e machine learning nei sistemi di cybersicurezza ha prodotto miglioramenti sostanziali nei tempi di rilevamento e risposta, nella riduzione dei falsi positivi e nel numero di attacchi non identificati. Questi risultati evidenziano il contributo reale e misurabile di tali tecnologie all'ottimizzazione delle operazioni di difesa digitale.

Metriche	Prima dell'integrazione AI/ML	Dopo l'integrazione AI/ML	Miglioramento %
Tempo medio di rilevamento	48 h	3 h	93.75
Tasso di falsi positivi	20%	5%	75
Tempo di risposta alla minaccia	24 h	1 h	95.83
Numero di attacchi non rilevati	50 per anno	15 per anno	70

Tabella 20 - Confronto delle metriche di cybersicurezza prima e dopo l'integrazione di AI/ML

7.3 Criticità e limiti dell'IA nella cybersicurezza

Nonostante i numerosi vantaggi offerti dall'intelligenza artificiale (IA) nell'ambito della cybersicurezza, è fondamentale evidenziarne anche le criticità, che possono limitarne l'efficacia e ostacolarne l'adozione su larga scala. Una delle principali problematiche riguarda il divario di competenze: molte organizzazioni faticano a reperire personale qualificato in grado di sviluppare, integrare e gestire efficacemente soluzioni basate su IA. Secondo un rapporto dell'ISC² [153], il deficit globale di professionisti nel settore della sicurezza informatica ammontava a circa 3,1 milioni di unità, una carenza che incide negativamente sulla capacità delle imprese di adottare strumenti avanzati di difesa. Inoltre, alcune mansioni tradizionali, precedentemente svolte da

operatori umani, sono state progressivamente ridimensionate a favore di sistemi automatizzati, più rapidi ed efficienti. Parallelamente, l'introduzione massiva dell'automazione ha trasformato profondamente l'organizzazione del lavoro nel campo della cybersicurezza e alcune mansioni tradizionali, precedentemente svolte da operatori umani, sono state progressivamente ridimensionate a favore di sistemi intelligenti, in grado di operare con maggiore rapidità ed efficienza. Questa evoluzione ha ridotto la necessità di interventi manuali nelle fasi di monitoraggio e manutenzione, determinando una ridefinizione del ruolo degli specialisti della sicurezza, che oggi sono sempre più orientati verso attività di supervisione, auditing, validazione dei risultati e gestione strategica delle infrastrutture automatizzate. Un altro ostacolo significativo è rappresentato dai costi elevati di implementazione e manutenzione dei sistemi intelligenti. Le piccole e medie imprese, in particolare, incontrano notevoli difficoltà nell'accedere a queste tecnologie, a causa della necessità di infrastrutture hardware e software specialistiche, come evidenziato da Dilmegani [154]. A questi fattori si aggiungono sfide tecniche complesse, tra cui la vulnerabilità degli algoritmi di machine learning ad attacchi mirati. Tecniche come gli *adversarial examples* permettono di introdurre dati manipolati nei modelli di IA, inducendo classificazioni errate o eludendo i meccanismi di rilevamento. Papernot et al. [155] hanno dimostrato, attraverso studi sperimentali, che tali tecniche possono compromettere seriamente l'affidabilità dei sistemi di sicurezza basati su IA, creando nuove superfici di vulnerabilità. Dal punto di vista operativo, la complessità di integrazione dell'IA nei processi aziendali rappresenta un'ulteriore criticità. Se da un lato l'IA offre enormi potenzialità in termini di automazione, analisi predittiva e risposta in tempo reale, dall'altro la sua implementazione effettiva richiede una serie di condizioni infrastrutturali, organizzative e culturali non sempre presenti all'interno delle imprese. L'inserimento di tecnologie intelligenti nei flussi operativi esistenti comporta non solo l'adeguamento di piattaforme tecniche e architetture digitali, ma anche un cambiamento nei modelli di governance dei dati e nei processi decisionali. L'efficacia degli algoritmi intelligenti dipende dalla loro trasparenza e interpretabilità, due requisiti ancora difficili da garantire nei modelli più avanzati. Errori come falsi positivi o falsi negativi possono avere impatti significativi, compromettendo la tempestività e l'efficacia delle risposte. Inoltre, pur essendo progettati per seguire rigidi protocolli di sicurezza, i sistemi di IA non sono infallibili e restano suscettibili ad attacchi sofisticati, manipolazioni o tentativi di reverse engineering da parte di cybercriminali esperti. Come evidenziato nella Figura 21, la difficoltà principale riscontrata dalle organizzazioni riguarda proprio la capacità di integrare le soluzioni basate su IA all'interno di applicazioni e processi aziendali (47%), un dato che sottolinea come la sfida non sia meramente tecnologica, ma sistemica. A ciò si aggiungono resistenze interne e dinamiche politiche (36%) che possono ostacolare l'introduzione di innovazioni percepite come dirompenti, soprattutto in contesti

ad alta burocratizzazione o con scarsa cultura digitale. Un'altra barriera significativa è la carenza di competenze manageriali (31%), che limita la capacità delle imprese di progettare e gestire in modo efficace progetti di IA in ambito sicurezza. Altri ostacoli degni di nota includono l'incapacità di garantire la qualità e l'integrità dei dati utilizzati per l'addestramento degli algoritmi (18%), l'insufficienza di finanziamenti o strumenti adeguati (20%) e l'utilizzo di tecnologie open source non ancora mature per ambienti produttivi (16%). Ancora più emblematico è il fatto che il 13% delle organizzazioni non riesce a dimostrare il ritorno sull'investimento (ROI) dei progetti basati su IA, un limite che mina la sostenibilità economica dell'adozione e alimenta un clima di incertezza strategica. È evidente, quindi, che l'adozione dell'IA in ambito cybersecurity non può essere affrontata solo come un aggiornamento tecnologico, ma richiede una pianificazione multidimensionale che consideri le implicazioni organizzative, culturali ed economiche. Alla luce di questi dati, emerge con chiarezza che la diffusione delle tecnologie intelligenti incontra ostacoli che vanno ben oltre la disponibilità tecnica delle soluzioni. Le barriere individuate pongono l'attenzione sulla necessità di politiche di formazione, investimento e governance dei dati, affinché l'adozione dell'IA non rimanga confinata a pochi contesti d'avanguardia, ma possa diventare uno strumento accessibile, affidabile e sostenibile anche per le realtà più piccole e meno strutturate.

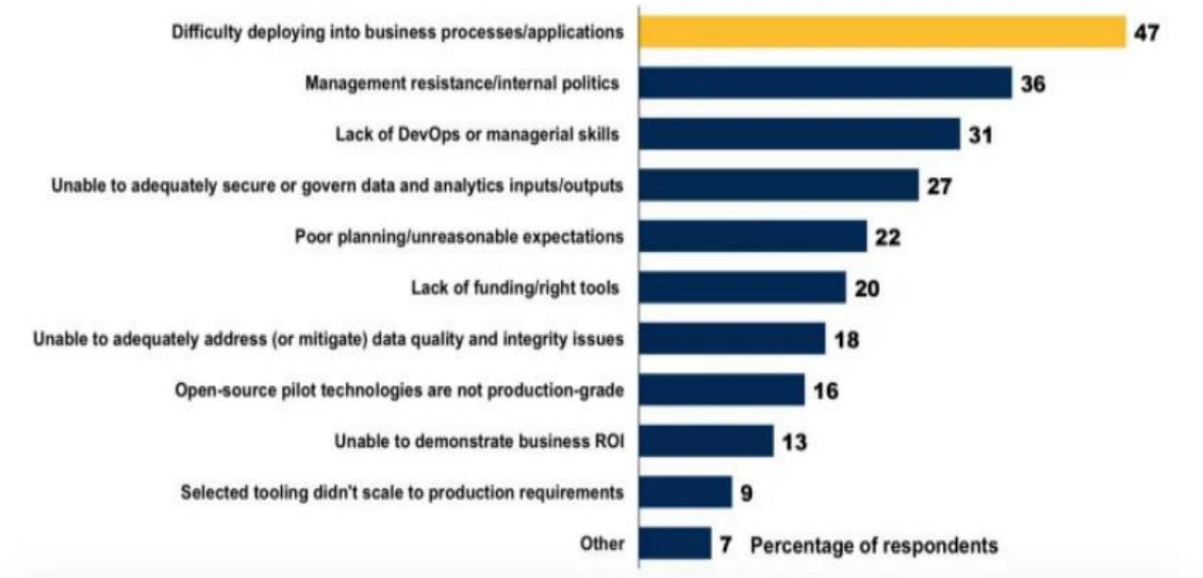

Figura 21 - Principali ostacoli all'implementazione dell'Intelligenza Artificiale nelle organizzazioni

Un aspetto particolarmente delicato riguarda la programmabilità dei sistemi intelligenti: modifiche mirate al codice sorgente possono trasformare strumenti di difesa in potenziali armi digitali, come sottolineato anche dalla letteratura più recente. Sebbene l'IA venga spesso integrata nei protocolli di crittografia per rafforzare la protezione dei dati, essa può essere utilizzata anche in senso inverso, ad esempio per generare codice malevolo in grado di aggirare i sistemi di rilevamento o compromettere database sensibili. Questo paradosso evidenzia come l'IA possa costituire sia una

risorsa difensiva sia una minaccia, qualora venga impiegata in modo scorretto o malevolo. Inoltre, l'efficacia degli algoritmi dipende in larga parte dalla qualità e dall'aggiornamento costante dei dataset di addestramento. Attacchi molto sofisticati, progettati per camuffarsi da attività legittime, possono ancora sfuggire al rilevamento automatizzato. In assenza di supervisione umana e aggiornamenti continui, anche i sistemi più evoluti rischiano di diventare rapidamente obsoleti. Infine, come già evidenziato, i costi e la carenza di competenze specifiche restano barriere significative all'adozione diffusa di soluzioni basate su IA, in particolare nei contesti aziendali meno strutturati. Oltre agli ostacoli di natura organizzativa e alla carenza di competenze, l'adozione dell'intelligenza artificiale nella cybersicurezza comporta anche una serie di vulnerabilità tecniche specifiche che meritano particolare attenzione. Tra queste, un ruolo crescente è assunto dagli attacchi adversariali (Adversarial AI), che si basano sulla manipolazione intenzionale degli input forniti ai modelli di IA al fine di ingannarli. Gli aggressori, in questi casi, progettano input apparentemente legittimi agli occhi dell'utente umano, ma strutturati in modo da essere erroneamente interpretati dai sistemi intelligenti, riuscendo così ad aggirare i meccanismi di rilevamento automatico e a compromettere la sicurezza del sistema. Un'ulteriore minaccia tecnica è rappresentata dal fenomeno noto come data poisoning, ovvero l'avvelenamento dei dati di addestramento. Questo tipo di attacco si verifica quando l'aggressore riesce a inserire, in modo diretto o indiretto, dati falsati all'interno dei dataset utilizzati per l'apprendimento automatico, alterando così la capacità del modello di riconoscere minacce reali o creando bias sistemici che ne compromettono l'affidabilità. In entrambi i casi, la sicurezza stessa del sistema IA è presa di mira, rendendo necessario un controllo accurato delle fonti di dati e dei processi di validazione. A queste problematiche si aggiunge il rischio di eccessiva dipendenza dai sistemi automatizzati. Un affidamento esclusivo sull'intelligenza artificiale nella gestione della sicurezza può generare una pericolosa riduzione della supervisione umana, con conseguenze rilevanti soprattutto in presenza di minacce nuove, complesse o non contemplate nei dati utilizzati per l'addestramento. In scenari di questo tipo, l'IA può trovarsi impreparata ad agire in modo adeguato, aprendo la strada a potenziali falle nei sistemi difensivi.

Per mitigare efficacemente questi rischi, è indispensabile adottare un approccio fondato su monitoraggio continuo, aggiornamento costante dei modelli e, soprattutto, integrazione sinergica tra uomo e macchina. L'utilizzo di soluzioni ibride, in cui l'analisi automatizzata è affiancata dall'intervento umano, consente di aumentare l'affidabilità e la resilienza dei sistemi di cybersicurezza. Tale combinazione permette infatti di gestire con maggiore efficacia situazioni anomale o non previste, mantenendo un elevato livello di controllo e garantendo una risposta tempestiva anche in condizioni critiche. Nonostante queste limitazioni, l'impatto complessivo

dell'intelligenza artificiale sulla cybersicurezza rimane positivo. Con una gestione consapevole, una supervisione umana competente e aggiornamenti regolari, l'IA può continuare a rappresentare una risorsa strategica per la protezione digitale, bilanciando efficacemente innovazione tecnologica e sicurezza operativa.

7.4 Prospettive future e sfide di governance

L'intelligenza artificiale è destinata a trasformare in modo sempre più radicale le strategie e le pratiche legate alla cybersicurezza, ridefinendo l'intero paradigma della protezione digitale. Le evoluzioni tecnologiche in atto indicano che, negli anni a venire, l'IA sarà protagonista di uno sviluppo orientato non solo al miglioramento delle capacità di rilevamento, ma anche all'automazione avanzata della risposta agli attacchi, alla gestione adattiva del rischio e alla costruzione di ecosistemi di difesa più resilienti e collaborativi. Uno degli ambiti di maggiore evoluzione sarà la capacità dei sistemi di IA di operare in modo sempre più autonomo. I futuri strumenti di cybersicurezza saranno in grado non solo di individuare tempestivamente minacce e anomalie, ma anche di attuare risposte automatizzate e coordinate in tempo reale, riducendo drasticamente la necessità dell'intervento umano. In questa direzione si colloca lo sviluppo delle cosiddette architetture di sicurezza adattive (adaptive security architecture), in cui i sistemi si modificano dinamicamente in risposta all'evolversi delle minacce. Ad esse si affiancheranno funzionalità di self-healing, ossia la capacità dei sistemi di auto-ripararsi in seguito a un attacco, garantendo continuità operativa anche in contesti di crisi. Un altro fronte innovativo sarà l'impiego di tecniche avanzate di analisi comportamentale, come la User and Entity Behavior Analytics (UEBA), che consentono di identificare deviazioni dai comportamenti attesi di utenti e dispositivi, migliorando la precisione nella rilevazione delle minacce e riducendo il numero di falsi positivi. L'integrazione tra analisi predittiva e intelligenza contestuale renderà le difese sempre più proattive, in grado di anticipare le mosse degli attaccanti. Il ruolo dell'IA sarà inoltre potenziato dall'espansione dell'Internet of Things (IoT), che moltiplicherà i punti di accesso e le superfici di attacco all'interno delle reti digitali. In questo scenario complesso e frammentato, sarà fondamentale disporre di sistemi intelligenti in grado di proteggere i dispositivi connessi e garantire una gestione centralizzata ed efficiente delle misure di sicurezza. L'IA potrà contribuire anche al rafforzamento delle attività di formazione nel settore della cybersecurity, attraverso la creazione di ambienti di apprendimento continuo e simulativo, personalizzati sulla base dei comportamenti degli utenti. A fianco dell'innovazione tecnologica, sarà altrettanto cruciale affrontare le sfide critiche che l'integrazione dell'intelligenza artificiale nella cybersicurezza comporta. Tra queste, emerge in

primo piano la questione della protezione della privacy. Poiché i modelli di IA necessitano di grandi quantità di dati per essere addestrati e aggiornati, diventa essenziale adottare tecnologie che garantiscano il rispetto della riservatezza, come il federated learning o la privacy differenziale, che permettono di migliorare le prestazioni dei modelli senza accedere direttamente ai dati sensibili. Ulteriori sfide riguardano la necessità di un addestramento continuo e accurato dei modelli, affinché restino efficaci contro minacce in costante mutamento. Questo richiede un processo costante di aggiornamento, monitoraggio e verifica della qualità dei dati, al fine di evitare che gli algoritmi diventino obsoleti o sviluppino bias. Al contempo, sarà necessario rafforzare la robustezza dei modelli contro tentativi di manipolazione, come il data poisoning o gli attacchi avversari [156], che mirano a compromettere il funzionamento dei sistemi di difesa automatizzati. Un capitolo a parte merita l'uso potenziale dell'intelligenza artificiale da parte degli stessi attaccanti. Le tecniche di IA avversaria (adversarial AI) stanno emergendo come minacce concrete, in cui attori malevoli sfruttano l'IA per generare attacchi sofisticati, eludere le difese o manipolare i modelli di sicurezza. La ricerca futura dovrà concentrarsi sullo sviluppo di metodi efficaci per contrastare tali minacce, assicurando che l'IA impiegata nella difesa non diventi essa stessa un punto di vulnerabilità. L'evoluzione dei sistemi di sicurezza intelligenti non potrà prescindere da una maggiore trasparenza dei processi decisionali. In quest'ottica, lo sviluppo di approcci Explainable AI (XAI) rappresenta un requisito sempre più urgente, affinché le decisioni automatizzate siano comprensibili, verificabili e conformi a principi di responsabilità [157]. Questo aspetto è cruciale non solo per la fiducia degli operatori e degli utenti, ma anche per soddisfare i requisiti imposti da normative come il Regolamento europeo sull'intelligenza artificiale (AI Act), che introduce obblighi stringenti per l'utilizzo di IA in settori ad alto rischio, tra cui rientra a pieno titolo la cybersicurezza. La gestione di queste sfide richiederà meccanismi solidi di supervisione e governance. Sarà necessario implementare framework capaci di garantire responsabilità, trasparenza e tracciabilità nelle decisioni automatizzate. Tra le pratiche fondamentali si annoverano fasi rigorose di test, il monitoraggio continuo del comportamento dei sistemi e l'adozione di standard che assicurino un uso etico e controllato dell'IA in ambito critico. In questo contesto, la collaborazione tra settore accademico, industria e istituzioni pubbliche sarà determinante per promuovere un ecosistema condiviso, basato sulla condivisione delle informazioni, sull'elaborazione di standard internazionali e sull'adozione di pratiche comuni. L'intelligenza artificiale potrà così sostenere una sicurezza cibernetica collettiva, più reattiva e distribuita. Le prospettive future dell'IA nella cybersicurezza ruotano attorno a tre assi principali: l'evoluzione tecnologica con sistemi sempre più intelligenti, autonomi e resilienti, la protezione della privacy e dell'etica, e l'affermazione di una governance responsabile e condivisa [158]. Solo attraverso un approccio integrato, che coniughi innovazione,

sicurezza e responsabilità, sarà possibile sfruttare pienamente il potenziale dell'IA per costruire un futuro digitale più sicuro, efficiente e sostenibile.

8. Conclusione

L'analisi condotta in questa tesi ha inteso offrire una panoramica organica e multidimensionale sul fenomeno della cybersecurity, evidenziandone la crescente centralità per la resilienza economica, sociale e istituzionale delle moderne società digitali. A partire dalla ricostruzione dei concetti fondamentali, della storia evolutiva del cybercrime e delle principali tipologie di minaccia, è emersa con chiarezza la natura complessa e dinamica di un rischio che, lungi dall'essere confinato a una dimensione puramente tecnica, si manifesta oggi come una sfida strategica che richiede approcci integrati, capacità operative avanzate e una governance condivisa a livello nazionale e internazionale.

Lo studio dell'evoluzione del quadro normativo, tanto europeo quanto nazionale, ha permesso di comprendere come le istituzioni stiano progressivamente rafforzando la cornice regolatoria e cooperativa per far fronte a minacce sempre più sofisticate e interconnesse. Iniziative come la Direttiva NIS2, il Cyber Resilience Act, il Cyber Solidarity Act e il Perimetro di Sicurezza Nazionale Cibernetica rappresentano passi significativi verso una cultura della prevenzione, della responsabilità condivisa e della standardizzazione dei livelli minimi di protezione, indispensabili in un contesto di interdipendenza tra attori pubblici e privati. Tuttavia, il vero banco di prova di queste iniziative non sarà tanto l'ampiezza del quadro regolatorio, quanto la capacità di tradurlo in pratiche effettive, sostenibili e comprensibili per le organizzazioni di ogni dimensione, incluse quelle che dispongono di risorse limitate.

La trattazione del cyber risk management ha evidenziato come la sicurezza informatica non possa limitarsi a interventi episodici o a investimenti una tantum, ma debba tradursi in processi circolari di pianificazione, monitoraggio, rilevamento, risposta e apprendimento continuo. La capacità di sviluppare capability interne, di coinvolgere i fornitori terzi in una gestione integrata del rischio e di rafforzare la cultura organizzativa si confermano fattori determinanti per ridurre le vulnerabilità strutturali e migliorare la resilienza complessiva. In questo senso, una delle principali lezioni che emerge dal lavoro è la necessità di affiancare agli strumenti tecnici e regolatori un vero cambiamento di mentalità: passare da una logica di mera "compliance", spesso vissuta come adempimento burocratico, a un approccio genuinamente risk-based, in cui la cybersecurity è percepita come parte integrante delle decisioni strategiche e non come un vincolo esterno.

L'approfondimento dell'economia della cybersecurity ha offerto ulteriori spunti di riflessione. Se da un lato la letteratura ha chiarito i meccanismi di incentivo individuale all'investimento in sicurezza,

dall'altro è emerso come le esternalità di interdipendenza, di tipo tecnico o di mercato, generino inefficienze che solo politiche pubbliche mirate e strumenti di cooperazione possono colmare. In quest'ottica, le scelte di spesa in cybersecurity non devono più essere viste come un costo isolato, ma come una variabile strategica in grado di influenzare la competitività, la fiducia degli stakeholder e la continuità operativa. Uno dei rischi più concreti è che il divario tra organizzazioni "mature" e realtà meno strutturate si ampli ulteriormente: da qui l'esigenza di politiche che favoriscano la diffusione di competenze, servizi e strumenti anche presso PMI e soggetti meno attrezzati, affinché la sicurezza non diventi un ulteriore fattore di disuguaglianza.

Il caso di studio sull'attacco al Colonial Pipeline ha tradotto in termini concreti questi principi teorici, dimostrando come anche vulnerabilità apparentemente elementari possano generare crisi di portata nazionale, con impatti significativi sul piano economico, sociale e reputazionale. L'evento ha messo in luce l'importanza di un approccio olistico alla protezione delle infrastrutture critiche, di una gestione efficace delle vulnerabilità e di un coordinamento tempestivo tra attori pubblici e privati nella risposta agli incidenti. A livello personale, l'analisi di questo caso ha reso particolarmente evidente come, in assenza di preparazione e pianificazione, la linea di confine tra incidente "tecnico" e crisi sistemica possa essere oltrepassata in tempi estremamente rapidi.

L'approfondimento dedicato all'intelligenza artificiale ha permesso di gettare uno sguardo sulle tendenze emergenti. Le tecnologie basate su machine learning e analisi comportamentale rappresentano oggi uno dei principali vettori di innovazione nella cybersecurity, consentendo di passare da una difesa reattiva a un paradigma predittivo e adattivo. Tuttavia, le stesse potenzialità tecnologiche pongono sfide complesse: dai rischi legati all'utilizzo malevolo dell'IA alle questioni etiche, passando per la trasparenza, l'accountability e la sostenibilità economica delle soluzioni avanzate.

A questo proposito, il grafico "Le sfide principali affrontate per garantire la sicurezza dei dati (2023, 2024)" restituisce un messaggio tanto semplice quanto cruciale: la cybersicurezza rimane, prima di tutto, una questione di fattore umano. La percentuale più alta riguarda infatti errori o negligenza degli utenti aziendali, seguita dalla carenza di risorse economiche, dalla mancanza di competenze specialistiche e da processi disallineati in ambienti IT sempre più complessi. Questi dati dimostrano come, nonostante gli investimenti tecnologici, le organizzazioni continuino a scontrarsi con problemi strutturali e culturali che rendono vulnerabili anche i sistemi più avanzati.

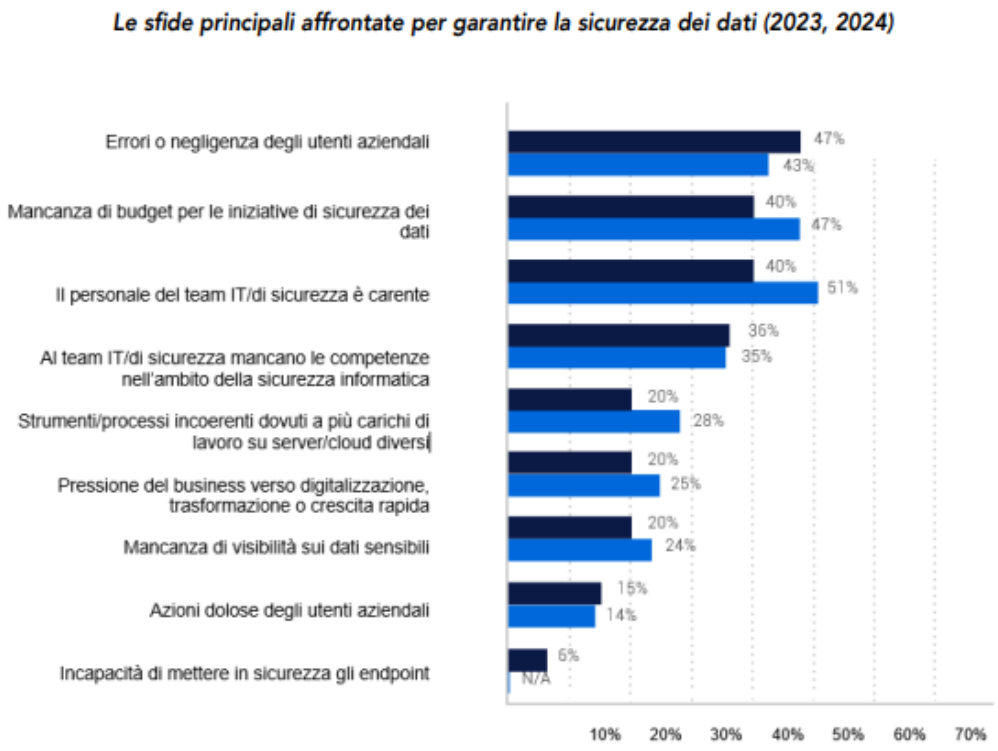

Figura 22 - Le sfide principali affrontate per garantire la sicurezza dei dati (2023, 2024)

In questo contesto, l'intelligenza artificiale non si propone come sostituto dell'intelligenza umana, ma come potenziamento indispensabile. L'IA, infatti, può intervenire là dove l'errore umano è più frequente e dove la mole di dati rende impossibile un monitoraggio esclusivamente manuale: automatizza il rilevamento delle vulnerabilità, velocizza l'analisi degli incidenti, segnala in tempo reale attività anomale e offre alle organizzazioni strumenti predittivi per agire prima che le minacce si concretizzino. Grazie a queste capacità, l'intelligenza artificiale trasforma la gestione della sicurezza da reattiva a proattiva, da puntuale a continua e adattiva. Eppure, questi stessi dati ci ricordano che la tecnologia da sola non basta. Se mancano investimenti adeguati, se le competenze non vengono aggiornate, se la consapevolezza degli utenti resta bassa, l'efficacia dell'IA è destinata a ridursi drasticamente.

Per questo motivo, una strategia di sicurezza realmente resiliente deve integrare l'IA in un ecosistema di processi, governance e cultura organizzativa, capace di responsabilizzare ogni attore coinvolto. La convinzione maturata nel corso di questo lavoro è che la sfida non consista soltanto nell'adottare strumenti più sofisticati, ma nel progettare organizzazioni "apprendenti", in grado di utilizzare i dati generati dall'IA per rivedere procedure, formare il personale, ridefinire le priorità di investimento. In altri termini, il valore dell'IA dipende meno dall'algoritmo in sé e più dalla capacità delle strutture di farne un motore di cambiamento continuo.

In definitiva, questa tesi ha evidenziato come la convergenza tra intelligenza artificiale e cybersicurezza rappresenti non solo una risposta tecnica all'aumento delle minacce, ma anche una sfida culturale: imparare a convivere con strumenti sempre più autonomi, governarne le decisioni, comprenderne i limiti e, soprattutto, formare persone in grado di collaborare con essi in modo consapevole. Solo così sarà possibile ridurre quell'ampio margine di vulnerabilità che ancora oggi dipende, come mostrano questi dati, più dagli esseri umani che dalle macchine.

Guardando al futuro, è chiaro che la resilienza digitale non potrà prescindere da un investimento costante in competenze, automazione intelligente e collaborazione tra uomo e tecnologia. In prospettiva, sarebbe interessante estendere le riflessioni sviluppate in questo lavoro ad altri ambiti – come l'Internet of Things, i servizi finanziari decentralizzati o i contesti di amministrazione pubblica – per comprendere come le dinamiche analizzate si declinino in ecosistemi ancora più eterogenei. In questo equilibrio tra innovazione tecnologica e responsabilità umana risiede la vera forza della cybersicurezza del domani: un sistema in cui l'intelligenza artificiale non sostituisce l'uomo, ma lo libera dai suoi errori più prevedibili, restituendogli il compito di guidare l'innovazione verso un cyberspazio più sicuro, etico e sostenibile.

In conclusione, il percorso di ricerca e scrittura di questa tesi mi ha confermato che la cybersicurezza non è soltanto un settore tecnico in rapida evoluzione, ma uno snodo critico per il futuro delle nostre società. Lavorando su questi temi ho maturato la convinzione che la vera sfida non consista tanto nell'inseguire le minacce, quanto nel costruire contesti in cui tecnologia, regole e competenze crescano insieme.

BIBLIOGRAFIA

[1] Chang, F. R. (2011). *The Science of Cybersecurity*. Center for Strategic and International Studies (CSIS).

[2] Dunn Cavelty, M. (2010). *Cyber-security and resilience in the European Union*. Security Dialogue, 41(5), 523–539.

[3] Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*. MIT Press.

[4] Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

[5] Kemmerer, R. A. 2003. Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715.

[6] Lewis, J. A. (2006). *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies.

[7] Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

[8] International Telecommunication Union. (2009). *Overview of Cybersecurity*. Recommendation ITU-T X.1205.

[9] Committee on National Security Systems (CNSS). (2010). *National Information Assurance Glossary*.

[10] Public Safety Canada. (2014). *Terminology Bulletin 281: Emergency Management Vocabulary*.

[11] Canongia, C., & Mandarino, R. (2014). Cybersecurity: The new challenge of the information society.

[12] Oxford University Press. (2014). *Oxford Online Dictionary*. Oxford: Oxford University Press.

[13] U.S. Department of Homeland Security. (2014). *A Glossary of Common Cybersecurity Terminology*. National Initiative for Cybersecurity Careers and Studies.

[14] Dunn Cavelty, M. (2010). Cyber-Security. In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies* (pp. 154–162).

[15] Cooper, S. (2013). Pragmatic qualitative research. In M. Savin-Baden & C. H. Major (Eds.), *Qualitative Research: The Essential Guide to Theory and Practice* (pp. 170–181).

[16] Ostrom, E., & Hess, C. (2007). Private and common property rights. In B. Bouckaert (Ed.), *Encyclopedia of Law & Economics*. Northampton, MA: Edward Elgar.

[17] Taherdoost, H., Jalaliyoon, N., & Yousefi, A. (2022). Cybersecurity vs. information security: A short comparison. *International Journal of Computer Applications*.

[18] Internet Society. (n.d.). *A Brief History of the Internet*. Retrieved from https://www.internetsociety.org/internet/history-internet/

[19] Hafner, K., & Markoff, J. (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.C

[20] Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley.

[21] National Institute of Standards and Technology (NIST). (1977). *FIPS PUB 46: Data Encryption Standard (DES)*. Washington, DC: U.S. Department of Commerce.

[22] Skoudis, E., & Zeltser, L. (2003). *Malware: Fighting Malicious Code*. Prentice Hall.

[23] Skrenta, R. (1982). *Elk Cloner* [Malware sperimentale per Apple II]. Documentazione storica raccolta presso il Computer History Museum.

[24] CERT Coordination Center. (1999). *Melissa Macro Virus*. Carnegie Mellon University.

[25] Perlroth, N. (2017). *Yahoo says 3 billion accounts were hacked in 2013 breach*. The New York Times.

[26] Sophos Group. (2021). *The State of Ransomware 2021*. Retrieved from https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

[27] Council of the European Union. (2022). *Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security*. Retrieved from https://www.consilium.europa.eu

[28] Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. The Hague: European Union Agency for Law Enforcement Cooperation.

[29] European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023: Cybercrime and Threat Actors*.
[30] Consiglio d'Europa. (1989). *Raccomandazione No. R(89)9 del Comitato dei Ministri agli Stati membri sulla criminalità informatica*. Strasburgo: Consiglio d'Europa. Integrata da Associazione Internazionale di Diritto Penale (1994). *XV Congresso Internazionale di Diritto Penale*, Rio de Janeiro.[9] Symantec, *Internet Security Threat Report*, Vol. 24, 2019.
[31] ENISA, *Threat Landscape Report 2022: Malware*, European Union Agency for Cybersecurity.
[32] Zetter, K., *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown Publishing Group, 2014.

[33] Castroreale, Renato. *Cybersecurity per tutti*. Milano: Apogeo Editore, 2021.
[34] Feuerstein, M. (2021). Fileless malware: Attack and defense. *Cybersecurity Journal, 5*, 43–57.
[35] Howard, M., & LeBlanc, D. (2002). *Writing Secure Code* (2nd ed.). Microsoft Press.

[36] OWASP Foundation. (2023). *OWASP Top Ten Web Application Security Risks*.
[37] Halfond, W. G., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. In *Proceedings of the IEEE International Symposium on Secure Software Engineering*.

[38] Anley, C. (2002). Advanced SQL injection in SQL Server applications. *NGSSoftware Whitepaper*.

[39] Howard, M., & LeBlanc, D. (2002). *Writing Secure Code* (2nd ed.). Microsoft Press.

[40] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53.
[41] Moore, D., Shannon, C., & Brown, J. (2002). Code-Red: A case study on the spread and victims of an Internet worm. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement* (pp. 273–284).

[42] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks, 44*(5), 643–666
[43] Cisco Systems. (2021). *Understanding Denial-of-Service Attacks*. Retrieved from https://www.cisco.com
[44] M. Gox Incident Analysis (2013). "Bitcoin DDoS attack and market manipulation."

[45] Cloudflare. (2013). *The DDoS attack that almost broke the Internet*. Retrieved from https://www.cloudflare.com
[46] Krebs, B. (2012). "Bank Hackers Steal Millions via DDoS," *Krebs on Security*. Retrieved from https://krebsonsecurity.com
[47] Beitollahi, H., & Deconinck, G. (2012). "Analyzing well-known countermeasures against Distributed Denial of Service attacks," *Computer Communications*, 35(11), pp. 1312–1332.

[48] Jakobsson, M., & Myers, S. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Interscience.

[49] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Wiley.
[50] European Union Agency for Cybersecurity (ENISA). (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*.
[51] Pethers, B., et al. (2023). Design and deception in phishing: How message structure influences susceptibility to cyber-sextortion. *Cyberpsychology, Behavior, and Social Networking*.

[52] Clusit – Associazione Italiana per la Sicurezza Informatica. (2025). *Rapporto Clusit 2025 sulla sicurezza ICT in Italia*.

[53] European Commission. (2020). *EU Cybersecurity Strategy for the Digital Decade*. Retrieved from https://digital-strategy.ec.europa.eu/

[54] European Parliament & Council. (2016). Directive (EU) 2016/1148 on security of network and information systems (NIS Directive). *Official Journal of the European Union*.

[55] European Parliament & Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*.

[56] European Parliament & Council. (2022). Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*, L 333, 27.12.2022, p. 164.

[57] European Parliament & Council. (2019). Regulation (EU) 2019/881 on ENISA and on ICT cybersecurity certification (Cybersecurity Act). *Official Journal of the European Union*.
[58] European Commission. (2024). Proposal for amending Regulation (EU) 2019/881 to include Managed Security Services (MSS).

[59] European Parliament, ITRE Committee. (2024). Report on the revision of the Cybersecurity Act. *European Parliament Working Document*.

[60] European Parliament & Council. (2024). Regulation (EU) 2024/2847 on cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union*, L 231, 10.12.2024.

[61] European Commission. (2025). *Cyber Resilience Act Expert Group – Terms of Reference*.

[62] European Parliament & Council. (2025). Regulation (EU) 2025/38 on the Cyber Solidarity Act. *Official Journal of the European Union*, L 15, 15.01.2025.

[63] European Commission. (2024). *Digital Connectivity Package, White Paper: How to Master Europe's Digital Infrastructure Needs?* and Recommendation on Submarine Cable Security, 21 February 2024.

[64] Draghi, M. (2024). *The Future of European Competitiveness: Report for the European Commission*. Brussels: European Commission.

[65] Governo Italiano. (2021). *Decreto-Legge 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*. Gazzetta Ufficiale della Repubblica Italiana.

[66] Agenzia per la Cybersicurezza Nazionale. (2022, maggio). *Strategia Nazionale di Cybersicurezza 2022–2026*. Roma: Presidenza del Consiglio dei Ministri.

[67] Governo Italiano. (2024, 4 settembre). *Decreto Legislativo 4 settembre 2024, n. 138: Recepimento della Direttiva (UE) 2022/2555 (NIS2)*. Gazzetta Ufficiale della Repubblica Italiana.

[68] Unione Europea. (2019). *Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'Agenzia dell'Unione europea per la cybersicurezza (ENISA) e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (Cybersecurity Act)*, Articolo 49. Gazzetta Ufficiale dell'Unione Europea.

[69] Parlamento Italiano. (2024, 28 giugno). *Legge 28 giugno 2024, n. 90: Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*. Gazzetta Ufficiale della Repubblica Italiana.

[70] Governo Italiano. (2019, 21 settembre). *Decreto-Legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133: Perimetro di Sicurezza Nazionale Cibernetica*. Gazzetta Ufficiale della Repubblica Italiana, Serie Generale n. 222.

[71] Parlamento Italiano. (2024, 28 giugno). *Legge 28 giugno 2024, n. 90: Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*. Gazzetta Ufficiale della Repubblica Italiana.

[72] Chapple, M., Stewart, J. M., & Gibson, D. (2021). *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide* (9th ed.). Indianapolis, IN: John Wiley & Sons.

[73] U.S. Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response. (2022, June). *Cybersecurity Capability Maturity Model (C2M2)*. Washington, DC.

[74] Computer Security Resource Center – NIST. (n.d.). *Risk Appetite – Glossary*. Retrieved from https://csrc.nist.gov/glossary

[75] International Organization for Standardization (ISO)/IEC. (2014). *ISO/IEC 25001:2014 – Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Planning and management*. Geneva: ISO.

[76] National Institute of Standards and Technology (NIST). (n.d.). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (SP 800-37). Gaithersburg, MD: NIST.

[77] Joint Task Force Transformation Initiative. (2018, December). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST SP 800-37r2)*. Gaithersburg, MD: National Institute of Standards and Technology.

[78] International Organization for Standardization (ISO)/IEC. (2022). *ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Geneva: ISO.

[79] National Institute of Standards and Technology (NIST). (2012). *Guide for Conducting Risk Assessments (SP 800-30 Rev. 1)*. Gaithersburg, MD: NIST.

[80] Deane, A., & Kraus, A. (2021). *The Official (ISC)² CISSP CBK Reference* (6th ed.). Indianapolis, IN: John Wiley & Sons.

[81] Carmichael, M. (n.d.). *Risk Appetite vs. Risk Tolerance: What is the Difference?* Retrieved from [aggiungi link se disponibile]

[82] Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments (NIST SP 800-30r1)*. Gaithersburg, MD: National Institute of Standards and Technology.

[83] Angelini, M., Ciccottelli, C., Franchina, L., Marchetti Spaccamela, A., & Querzoni, L. (2019, February). *Framework Nazionale per la Cybersecurity e la Data Protection*. Cyber Intelligence and Information Security (CIS) Sapienza – Cybersecurity National Lab (CINI).

[84] Joint Task Force Interagency Working Group. (2020, September). *Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology.

[85] International Organization for Standardization (ISO)/IEC. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: ISO.

[86] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W.W. Norton & Company.

[87] Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94)*. Gaithersburg, MD: National Institute of Standards and Technology.

[88] Joint Task Force Transformation Initiative. (2011). *Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39)*. Gaithersburg, MD: National Institute of Standards and Technology.

[89] Sbriz, L. (n.d.). *Comunicare il rischio di sicurezza delle informazioni in modo semplice ed efficace, parte 1*. Retrieved from [aggiungi link se disponibile]

[90] Computer Security Resource Center – NIST. (n.d.). *Third-party Providers – Glossary*. Retrieved from https://csrc.nist.gov/glossary

[91] Boyens, J., Paulsen, C., Bartol, N., Shankles, S. A., & Moorthy, R. (2012, October). *Notional Supply Chain Risk Management Practices for Federal Information Systems (NIST IR 7622)*. Gaithersburg, MD: National Institute of Standards and Technology.

[92] International Organization for Standardization (ISO)/IEC. (2018). *ISO 31000:2018 – Risk management – Guidelines*. Geneva: ISO.

[93] Quinn, S., Ivy, N., Barret, M., Witte, G., & Gardner, R. K. (2022, February). *Prioritizing Cybersecurity Risk for Enterprise Risk Management (NIST IR 8286B)*. Gaithersburg, MD: National Institute of Standards and Technology.

[94] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613.

[95] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. https://doi.org/10.1145/581271.581274

[96] Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, 26(2–3), 231–249. https://doi.org/10.1023/A:1024119208155

[97] Garcia, A., & Horowitz, B. M. (2007). The potential for security investments leads to socially suboptimal outcomes. *Decision Analysis*, 4(3), 127–134.

[98] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2008). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 69–104.

[99] Koutsoupias, E., & Papadimitriou, C. H. (2009). Worst-case equilibria. *Computer Science Review*, 3(2), 65–69.

[100] Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-Government in Japan. In *Proceedings of the Workshop on the Economics of Information Security (WEIS 2005)*.

[101] Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy*, 25(6), 629–665. https://doi.org/10.1016/j.jaccpubpol.2006.09.003

[102] Willemson, J. (2006). On the Gordon & Loeb Model for Information Security Investment. In *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*.

[103] Wang, T. (2017). On Gordon-Loeb's 1/e rule for information security investment. *Information and Computer Security*, 25(4), 444–452.

[104] Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A real options approach to information security investment. *Journal of Information Security*, 5(1), 5–12.

[105] Krutilla, K., Graham, J. D., & Krause, R. M. (2021). A dynamic model of optimal cybersecurity investment. *Risk Analysis*, 41(5), 792–807.

[106] Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, 114(2), 793–804. https://doi.org/10.1016/j.ijpe.2008.04.001

[107] Wang, T. (2017). On Gordon-Loeb's 1/e rule for information security investment. *Information and Computer Security*, 25(4), 444–452.

[108] Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, 26(2–3), 231–249.

[109] Böhme, R. (2012). Security metrics and externalities: Exploring the economics of security information sharing. In *Proceedings of the 11th Workshop on the Economics of Information Security (WEIS 2012)*.

[110] Varian, H. R. (2004). System reliability and free riding. In L. J. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 1–15). Springer.

[111] Grossklags, J., Christin, N., & Chuang, J. (2008). Secure or insure? A game-theoretic analysis of information security games. In *Proceedings of the 17th International Conference on World Wide Web* (pp. 209–218). https://doi.org/10.1145/1367497.1367528

[112] Riordan, M. H. (2014). Cybersecurity and interdependent risk. In M. E. Johnson, B. J. Koops, & A. P. M. Stuurman (Eds.), *Economics of Information Security and Privacy III* (pp. 15–35). Springer.

[113] Lelarge, M. (2009). Coordination in network security games: A monotone comparative statics approach. In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing* (pp. 221–229). https://doi.org/10.1109/ALLERTON.2009.5380552

[114] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613.

[115] Garcia, A., & Horowitz, B. M. (2007). *The potential for security investments to lead to socially suboptimal outcomes*. *Decision Analysis*, 4(3), 127–134

[116] Gao, L., & Zhong, Z. (2016). *Cybersecurity investment and competition in the presence of switching costs*. *Information Economics and Policy*, 36, 34–44.

[117] Qian, L., Ma, J., & Wang, T. (2019). *Consumer loyalty, switching costs, and security investments in competitive markets*. *Decision Support Systems*, 121, 95–106.

[118] Geer, D., Pfleeger, S. L., & Schneier, B. (2020). *Magnet platforms and the cyber security investment dilemma*. *IEEE Security & Privacy*, 18(2), 54–61.

[119] Arce, I. (2018). *Security investment and market share in platform competition*. *Journal of Cybersecurity*.

[120] Gal-Or, E., & Ghose, A. (2005). *The economic incentives for sharing security information*. *Information Systems Research*, 16(2), 186–208.

[121] Wood, K. (2023). *Colonial Pipeline and the security of critical fuel infrastructure*. *Journal of Energy Security*, 15(1), 22–29.

[122] Kerner, S. M. (2022). How the Colonial Pipeline ransomware attack unfolded. *CSO Online*. Retrieved from https://www.csoonline.com/article/3614639/how-the-colonial-pipeline-ransomware-attack-unfolded.html

[123] Cybersecurity and Infrastructure Security Agency (CISA). (2021). *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*.

[124] Congressional Research Service. (2021, May 11). *Colonial Pipeline: The DarkSide Strikes.*

[125] CNN Business. (2021). Colonial Pipeline paid $4.4 million to hackers. Retrieved from https://edition.cnn.com/2021/05/19/business/colonial-pipeline-ransom-payment/index.html

[126] U.S. Energy Information Administration (EIA). (2021). Gasoline prices hit highest level since 2014. Retrieved from https://www.eia.gov/todayinenergy/detail.php?id=48116

[127] IBM Security. (2023). *Cost of a Data Breach Report 2023*. Retrieved from https://www.ibm.com/reports/data-breach

[128] Cybersecurity Ventures. (2023). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[129] Ron Brash, "Lessons learned from the Colonial Pipeline attack," Industrial Cybersecurity Pulse, May 11, 2021.

[130] Dudley, R., & Golden, D. (2021). *The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime*. New York: Farrar, Straus and Giroux.

[131] Shier, J. (2021). *Colonial Pipeline attack highlights importance of MFA and detection*. Sophos News.

[132] Cybersecurity and Infrastructure Security Agency (CISA). (2021). *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*.

[133] Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing.
[134] Symantec. (2020). *Internet Security Threat Report*. Version 25.
[135] Ahmad, I., Basheri, M., Iqbal, M. J., & Raheem, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. *IEEE Access*, 6, 33789–33795.
[136] Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities. *IEEE Access*, 7, 146546–146561.
[137] Sahu, S., & Kumar, N. (2019). Fraud Detection in E-commerce Using Machine Learning. *International Journal of Computer Sciences and Engineering*, 7(6), 732–737.
[138] Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2017). Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. *IEEE Systems Journal*, 11(1), 88–95.
[139] Ahmad, M., & Chen, H. (2020). Threat Intelligence Sharing for Cybersecurity: A Review. *Computers & Security*, 92, 101752.
[140] Kumar, R., & Singla, J. (2022). AI-Powered Cybersecurity: The Future of Protection. *International Journal of Computer Applications*, 184(43), 8–15.
[141] Xue, J., Wang, X., & Zhang, C. (2020). Predictive Analytics for Cybersecurity: A Review. *IEEE Access*, 8, 180314–180330.
[142] Perols, J., & Murthy, S. (2011). Information Security Risk Assessment Using a Bayesian Belief Network. *Decision Support Systems*, 51(3), 396–405.

[143] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*.
[144] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *NIST Special Publication 800-94*. National Institute of Standards and Technology.
[145] IBM Security. (2020). *Cost of a Data Breach Report 2020*. Ponemon Institute.

[146] Heldah, C. (2021). *How Artificial Intelligence (AI) is Transforming Cybersecurity*. Plug and Play Tech Center. Retrieved September 1, 2021

[147] Chandramouli, R., Iorga, M., & Franklin, J. (2021). *Security Considerations for Open Banking APIs*. National Institute of Standards and Technology.

[148] Ponemon Institute. (2020). *Cost of a Data Breach Report 2020*. IBM Security.

[149] Verizon. (2023). *Data Breach Investigations Report 2023*. Verizon Enterprise.

[150] Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). Blockchain and AI for the next generation energy grids: Cybersecurity challenges and opportunities.

[151] Chen, Z., & Liu, B. (2018). *Lifelong Machine Learning* (2nd ed.). Synthesis Lectures on Artificial Intelligence and Machine Learning, 12(3), 1–207.

[152] Vorobeychik, Y., & Kantarcioglu, M. (2018). *Adversarial Machine Learning*. Synthesis Lectures on Artificial Intelligence and Machine Learning, 12(3), 1–169.

[153] ISC². (2021). *Cybersecurity Workforce Study 2021*. ISC².

[154] Dilmegani, C. (2022, September 12). *AI platforms: Guide to ML Life Cycle Support Tools*. AIMultiple. Retrieved September 26, 2022

[155] Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2018). Practical black-box attacks against machine learning. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 506–519).

[156] Puthal, D., & Mohanty, S. (2021). Cybersecurity issues in AI. *IEEE Consumer Electronics Magazine*, 10(2), 18–27.

[157] Dubber, M. D., Pasquale, F., & Das, S. (Eds.). (2020). *The Oxford Handbook of Ethics of AI*. Oxford University Press.

[158] Johnson, R. (2022, July 18). Artificial intelligence in cybersecurity market size to reach USD 133.8 billion by 2030 driven by growing number of cyber-attacks. *Market Research Future*.