LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze Politiche

Cattedra di Relazioni Internazionali

LA QUINTA DIMENSIONE DELLA CONFLITTUALITA': EVOLUZIONE DEL CONCETTO DI SICUREZZA E IL *CYBER SPACE*

RELATORE:
Raffaele Marchetti

CANDIDATO:
Francesca Romana Ajale
Matricola 097692

ASSISTENTE RELATORE:
Carolina Polito

Anno academico: 2022- 2023

INDICE

It is our choices that show what we really are, much more than our abilities.

J.K Rowling

INTRODUZIONE

Nella nostra società sempre più interconnessa, la sicurezza informatica rappresenta una delle principali sfide per la sicurezza nazionale e internazionale. Il cyber spazio, ovvero l'ambiente digitale in cui si svolgono le attività online, è diventato una nuova frontiera di conflitto tra le nazioni e i gruppi di attori non statali, e la protezione delle infrastrutture critiche è diventata una priorità assoluta per governi, organizzazioni pubbliche e private e individui. Il presente lavoro di tesi si concentra sulla *cyber sicurezza* e sul *cyber spazio*, analizzando le principali questioni relative alla protezione delle infrastrutture critiche, alla prevenzione degli attacchi cyber e alla tutela della privacy dei dati personali. Questo tema è di grande attualità e importanza, in quanto gli attacchi informatici possono causare danni significativi alla sicurezza nazionale, alla stabilità economica e alla privacy dei cittadini. Inoltre è fondamentale per comprendere i rischi e le opportunità associate alla sicurezza informatica, al fine di sviluppare politiche e strategie efficaci per la prevenzione degli attacchi cyber e la protezione delle infrastrutture critiche

La cyber sicurezza e il cyber spazio rappresentano un tema di crescente importanza nella società odierna. La diffusione delle tecnologie digitali e l'interconnessione globale hanno creato nuove opportunità, ma anche nuove minacce per la sicurezza nazionale e internazionale. La protezione delle infrastrutture critiche, la prevenzione degli attacchi cyber e la tutela della privacy dei dati personali sono diventati obiettivi prioritari per governi, organizzazioni pubbliche e private e individui. Il presente lavoro di tesi ha come obiettivo quello di analizzare come si è evoluta la sicurezza informatica negli ultimi anni e quali sono stati i principali fattori che hanno guidato questo cambiamento

Le variabili indipendenti che hanno influenzato l'evoluzione del concetto di sicurezza cibernetica includono l’'evoluzione delle tecnologie digitali ossia l'avanzamento delle tecnologie digitali e l'espansione delle reti di comunicazione che hanno portato ad un aumento delle minacce cibernetiche rendendo necessaria una maggiore attenzione alla sicurezza informatica; la crescente dipendenza dalle tecnologie digitali e quindi la dipendenza delle organizzazioni e dei cittadini dalle tecnologie digitali che ha reso la sicurezza informatica una priorità per la tutela dei dati personali e delle infrastrutture critiche; l’'adozione di normative a livello Europeo e a livello nazionale, come nel caso dell’Italia; la collaborazione internazionale: che ha contribuito a promuovere la sicurezza informatica a livello globale ed infine la

consapevolezza pubblica sui rischi legati alla sicurezza informatica che ha portato una maggiore attenzione e impegno nella promozione della sicurezza cibernetica.

In sintesi, l'evoluzione del concetto di sicurezza cibernetica è stata influenzata dalle seguenti variabili indipendenti: l'evoluzione delle tecnologie digitali, la crescente dipendenza dalle tecnologie digitali, l'adozione di normative, la collaborazione internazionale e la consapevolezza pubblica. Tenendo conto di quanto sia migliorata la sicurezza informatica dagli anni ’90 ad oggi i tre capitoli della tesi si concentreranno su diverse questioni relative alla cyber sicurezza e al cyber spazio, legando tra di loro i temi trattati. Il primo capitolo offrirà una panoramica sul cyber spazio, introducendo il concetto di nuova frontiera di conflitto e analizzando le ragioni per cui le grandi potenze cominciano ad interessarsi al cyber spazio. In questo capitolo verranno anche descritti gli attori principali del cyber warfare, le armi del cyber warfare e le diverse tipologie di cyber-activities. In aggiunta è proprio in questo capitolo che vanno a delinearsi le principali variabili, come l’aumento delle minacce, che hanno portato ad una evoluzione del concetto di sicurezza.

Una volta analizzate le variabili più generali si approfondirà il concetto di cyber sicurezza che aiuta a comprendere le variabili più specifiche, ad esempio l’aumento della dipendenza dalle tecnologie digitali. Il secondo capitolo del lavoro si concentra sul concetto generale di sicurezza nazionale e analizza l'importanza dell'analisi del rischio e dell'intelligenza artificiale nella protezione delle infrastrutture critiche. Inoltre, verrà discussa la resilienza nella sicurezza cibernetica e l'importanza di una risposta rapida ed efficace in caso di attacco. Con questo capitolo cercherò di approfondire come si sia evoluto il concetto di sicurezza cibernetica e quali le variabili da tenere in considerazione.

Infine, nel terzo capitolo si analizzerà un paese specifico per comprendere al meglio le variabili prese in considerazione nei primi due capitoli. Ho deciso di analizzare il caso italiano, fornendo un'analisi dell'impatto degli attacchi cyber in Italia e la relazione tra sicurezza nazionale e minaccia cibernetica. Inoltre, verrà descritto il piano nazionale per la protezione cibernetica e la sicurezza informatica, il ruolo dell'azienda Generali Italia Spa nella copertura di "eventi cyber", il quadro strategico nazionale per la sicurezza dello spazio e la direttiva N.I.S.

In definitiva, come vedremo in sede di conclusione, le ipotesi riguardanti l'evoluzione del concetto di sicurezza cibernetica comprendono l'idea che la crescente diffusione delle tecnologie digitali e l'espansione delle reti di comunicazione abbiano portato ad un aumento delle minacce cibernetiche e della necessità di protezione delle infrastrutture critiche e dei dati personali. Le minacce informatiche sono aumentate in numero, sofisticazione e impatto, spingendo le organizzazioni a rafforzare le proprie difese e investire maggiormente in sicurezza

informatica. La tecnologia e le soluzioni di sicurezza sono migliorate significativamente, passando da semplici firewall e antivirus a strategie multi-livello che includono analisi avanzate, prevenzione delle intrusioni, crittografia, rilevamento e risposta agli incidenti. Vi è stata una crescente standardizzazione ed armonizzazione delle regole e normative sulla cybersecurity a livello nazionale, regionale e internazionale, come nel caso italiano, contribuendo a migliorare le pratiche di sicurezza. La dipendenza da Internet e dalle tecnologie digitali è aumentata esponenzialmente per aziende e privati, rendendo la protezione di dati e sistemi informatici sempre più critica. Le conoscenze e competenze nel campo della cybersecurity sono cresciute tra i professionisti IT e di sicurezza, ma anche a livello manageriale e dirigenziale all'interno delle organizzazioni. La consapevolezza sui rischi legati alla sicurezza informatica è aumentata sia tra le imprese che tra i privati, spingendo ad adottare comportamenti più sicuri e investire nella protezione dei sistemi. Infine, la sicurezza cibernetica è diventata sempre più centrale per la sicurezza nazionale, dato il ruolo critico delle infrastrutture digitali nell'economia e nella società contemporanee.

CAPITOLO 1

1. IL CYBER SPAZIO: UNA NUOVA FRONTIERA

1.1 Il Cyber Spazio

Il termine *Cyber Spazio* appare per la prima volta nel 1982, in lingua inglese come *cyberspace,* in un racconto di fantascienza dal titolo *Burning Chrome*[1], pubblicato da William Gibson, scrittore canadese, sulla rivista Omni[2] e riutilizzato nel suo romanzo *Neuromancer (1984)*[3]. Egli descrisse *il Cyber Spazio* come:

> un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici [...] Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...].[4]

Il lavoro svolto da Gibson ha contribuito alla diffusione del termine, che deriva dalla fusione di cibernetica e spazio. Per Gibson il termine *Cyber spazio* identificava un luogo immaginario di fantasticherie e allucinazioni tecnologiche. In realtà l'origine etimologica del termine è più antica e richiama la tradizione filosofica dell'Atene classica. *Kibernetes* deriva dal greco e significa "colui che governa" o "colui che si governa".[5] Il mito della caverna incluso nella *Repubblica* di Platone è un chiaro riferimento. Con la nascita di internet, negli anni Novanta, il termine assume un significato più vicino a ciò che gli attribuiamo oggi. Esso fu impiegato per indicare un luogo virtuale in cui avviene la comunicazione grazie alle reti informatiche. Lo scrittore e giornalista Bruce Sterling, con cui divenne popolare questo termine, accreditò John Perry Barlow per essere stato il primo ad usare questo termine per riferirsi al "nesso attuale tra

[1] Treccani enciclopedia: Cyber Spazio - Lessico del XXI secolo
[2] Rivista di fantascienza e scienza pubblicata negli Stati Uniti e in Gran Bretagna, che conteneva articoli riguardanti fatti scientifici e piccoli racconti fantascientifici.
[3] Treccani enciclopedia: Cyber Spazio – Lessico del XXI secolo
[4] Gibson W. (1984) Neuromancer, Ace Pub., New York
[5] Treccani enciclopedia: cibernetica

il computer e i network delle telecomunicazioni"[6]. Barlow lo descrive così per annunciare la formazione dell'EFF[7] nel giugno del 1990:

> «In questo mondo silenzioso, tutta la comunicazione è digitata. Per entrare in esso, ci si deve liberare sia del corpo che dell'ambiente circostante e si diviene solo una cosa fatta di parole. Si può vedere quello che i nostri interlocutori stanno dicendo (o che hanno detto di recente), ma non come sono loro fisicamente, né il luogo dove si trovano. Gli incontri in questa città virtuale sono continui e le discussioni variano dagli ambiti sessuali ai programmi di deprezzamento.»[8]

Questo ci fa meglio comprendere come la cibernetica e tutto il mondo tecnologico non si fermi solo ed esclusivamente ad un oggetto o un elemento fisico ma che esso sia effettivamente anche qualcosa di impercettibile all'occhio umano. Nascono così incontri virtuali, di lavoro e intimi, che portano a discussioni di vario tipo e su vari argomenti.
Esiste anche una più recente definizione di Cyber Spazio, fornita dal pentagono, che nel 2008 decide di riunire una serie di esperti del settore affinché venisse creata una definizione univoca e condivisa di tale termine.9 Il Cyber Spazio viene identificato come:

> il dominio globale all'interno dell'ambiente dell'informazione costituito dalla rete interdipendente delle infrastrutture della tecnologia dell'informazione, tra cui Internet, reti di telecomunicazioni, sistemi informatici e processori e controllori incorporate.[10]

In parole più semplici il Cyber Spazio è il regno delle reti informatiche e degli utenti dietro queste nel quali le informazioni vengono immagazzinate, memorizzate, condivise e diffuse. Quali sono le caratteristiche del Cyber Spazio e perché è considerata una nuova frontiera sono domande a cui rispondere per capire al meglio questo argomento.
La primissima caratteristica che mi sento di analizzare è l'uso dell'elettronica e dello spettro elettromagnetico. È importante sottolineare che parliamo di una realtà astratta che riesce a connettere ad un'unica rete i computer consentendo così di far interagire gli utenti di tutto il mondo. Tuttavia, nonostante questa sua caratteristica immateriale, bisogna tenere in considerazione che per potersi connettere è necessaria la presenza finisca di un oggetto (di

[6] Barlow's, J. P. (1996). Declaration of independence for cyberspace.
[7] Electronic Frontier Foundation
[8] Il lavoro nell'era digitale, l'anima al lavoro: saggio di Franco Berardi Bifo, 2017
[9] Giovanni Campanale (2020). Dal concetto di cyber attack al cyberwarfare: l'uso della forza in ambito cyber. Articolo pubblicato su "Cybersecurity360"
[10] Singer, Friedman (2014: 12), tradotto

dispositivi elettronici come computer, telefonini o *tablet*).[11] Dietro a questi ultimi gli utenti svolgono un ruolo fondamentale nel plasmare questo mondo, in continua evoluzione, in cui non solo condividono e trasmettono informazioni, ma sono anche in grado di crearne di nuove. Il *Know-How* dell'uomo consente di produrre nuove tecnologie che risultano essere sempre più avanzate, nuovi dispostivi e, nel complesso, la creazione di un mondo che è sempre più interconnesso e interdipendente.

Per Evan Shumel, nel Cyber Spazio, coesistono tre diversi elementi[12]:

- *the human layer,* vale a dire le risorse umane dedite all'utilizzo dei sistemi di informatizzazione e comunicazione;
- *the logical layer,* ossia i programmi/software, i sistemi operativi e le varie applicazioni e, infine, i bit che viaggiano nell'etere;
- *the physical layer*, ovvero le infrastrutture e le apparecchiature fisiche mobili o fisse, che rendono possibile la trasmissione di dati.[13]

1.2 Perché le grandi potenze cominciano ad interessarsi al Cyber Spazio?

L'avvento di questo mondo ha provocato cambiamenti sulla vita di chiunque conferendo un certo quantitativo di potere sia a singoli individui ma soprattutto a organizzazioni e stati. Il potere più grande è quello di poter ottenere e fornire informazione in pochissimo tempo e da qualsiasi posto.[14] La forza, anche distruttiva, dell'informazione non risiede tanto nell'informazione stessa bensì nella sua velocità di circolazione tra un individuo e l'altro o tra uno stato e l'altro.[15] L'eliminazione di un mondo incentrato sulla carta e sull'inchiostro e la nascita di un mondo incentrato sulla tecnologia e su nuove forme di interazione, in un periodo in cui gli Stati Uniti erano interessati a primeggiare sul resto del mondo, ha spinto le super potenze prima e successivamente gli stati più piccoli ad interessarsi a questa nuova frontiera. Il mondo e soprattutto chi detiene il potere capisce che esistono orizzonti più ampi e modalità diverse di ottenere ciò che si vuole. Una forza che può essere usata non solo per il progresso sociale ma soprattutto col fine di ottenere vantaggi maggiori. La capacità di rompere barriere e confini territoriali ha portato gli stati ad attuare nuovi comportamenti e soprattutto nuove strategie sia di difesa che di attacco. Un modello di connessione non solo istituzionale ma anche

[11] Farina, G. (2017). Il cyber space: una nuova dimensione per la conflittualità e la tutela dei diritti umani.
[12] *Ibidem*
[13] Even, Siman-Tov (2012: 10)
[14] Chiaruzzi, M. Geopolitica e geostrategia.
[15] Messa, P. (2018). L'era dello sharp power: la guerra (cyber) al potere. EGEA spa.

privato innesca una serie di problemi che, come vedremo più avanti, dovranno essere affrontati. Bisogna anche aggiungere che all'interno di questo mondo, che secondo molte teorie può essere considerato privo di delimitazioni fisiche o di confini territoriali, le attività che possono essere svolte assumono una particolare rilevanza.[16] Queste attività possono essere svolte sia da *state-actors* sia dai *non-state actors* e se un tempo gli attori ricercavano lo sviluppo tecnologico come strumento per ampliare e migliorare la loro condizione di vita, oggi è molto elevata la possibilità di utilizzare gli strumenti cibernetici e in generale il *cyber world* come arma e con l'intento di colpire altri stati o attori non-statali.[17] E' in questo contesto che si può parlare di un'evoluzione del concetto di guerra e di conseguenza del concetto di sicurezza.

1.3 La Guerra cibernetica: i concetti di Cyber War e Cyber warfare

> Cyberwar: "Cyberwar si riferisce alla conduzione e alla preparazione a condurre operazioni militari secondo principi relativi all'informazione. Significa interrompere se non distruggere i sistemi di informazione e comunicazione, definiti in senso lato per includere anche la cultura militare, su cui un avversario fa affidamento per conoscere se stesso: chi è, dove si trova, cosa può fare quando, perché sta combattendo, quali minacce contrastare per prime, ecc. Significa cercare di sapere tutto su un avversario impedendogli di sapere molto su se stessi. Significa ribaltare l'equilibrio delle informazioni e delle conoscenze a proprio favore, soprattutto se l'equilibrio delle forze non lo è. Significa usare la conoscenza in modo da dover spendere meno capitale e lavoro".[18]

> Cyber Warfare : "La guerra fondata su determinati usi delle TIC all'interno di una strategia militare offensiva o difensiva approvata da uno stato e mirante all'interruzione immediata o al controllo delle risorse del nemico, e che è condotta all'interno dell'ambiente informativo, con agenti e obiettivi che vanno sia nel dominio fisico che in quello non fisico e il cui livello di violenza può variare a seconda delle circostanze".[19]

Gli scontri tra le super potenze non si sono evoluti solo sotto il profilo delle armi ma anche e soprattutto sul piano metodologico. Dalla classica battaglia sul campo di guerra, condotta da eserciti fisicamente schierati, l'evoluzione, la tecnologia e la diplomazia hanno comportato cambiamenti radicali grazie alla creazione di armi di distruzione di massa come quelle nucleari.

[16] Xiangsui, Q. L. W. (2001). Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione.
[17] *Ibidem*
[18] Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Santa Monica, CA: RAND Corporation. Tradotto
[19] Taddeo, M. (2012). An analysis for a just cyber warfare. 2012 4th International Conference on Cyber Conflict (CYCON 2012), Tradotto

Il concetto di conflitto si è così modificato e con esso anche il concetto di attacco e di armi. Ad oggi, essendosi ridotti di molto gli scontri su un campo di battaglia fisico e materiale, l'attenzione si è spostata sul campo dell'informatica e su nuovi strumenti utilizzati per attaccare individui o stati digitalmente. In questo contesto si è ampliato il concetto di *War* includendo tre elementi distinti: *Cyber Attack*, *Cyber War e Cyber Warfare*. Il concetto di *Cyber Attack* riprende il concetto di operazione cibernetica, offensiva o difensiva, in grado di causare danni e distruzione.[20] È importante qui capire un concetto fondamentale: il danno che si prende in considerazione può avere una dimensione molto ampia, sia di tipo economico, strutturale sia di tipo psicologico e psicofisico. Un altro elemento da prendere in considerazione è l'intenzione. Con il termine *Cyber War* possiamo indicare quella situazione che si verifica in seguito alla realizzazione di due presupposti: la dichiarazione di guerra di uno stato-nazione o lo svolgimento, esclusivamente in maniera cibernetica, di detta guerra.[21] Questo concetto è ricollegabile ad uno stato d'essere continuo a differenza del Cyber Warfare che rimane un'attività.
Infine, per *Cyber Warfare* si intende l'utilizzo di attacchi cibernetici con intento ostile col fine di ottenere, distruggere o alterare le informazioni della controparte[22].

Tra le varie operazioni figurano:

- cyber attacchi (*cyber attack*), cioè attacchi mirati con lo scopo di paralizzare, disabilitare o danneggiare i sistemi informatici della controparte, realizzando così gli obiettivi principali di una *cyberwar*;
- attività di raccolta informazioni (Intelligence) e cyber spionaggio;
- cyber defense, ovvero il complesso di operazioni volte a difendere il cyber spazio da cyber attacchi relativi ad una *cyberwar*;
- propaganda e diffusione di messaggi volti a disinformare i cittadini e a fiaccare il morale del nemico, seguendo le modalità tipiche della guerra psicologica.[23]

In un mondo interconnesso come il nostro è difficile riuscire a dare una definizione di *Cyber Warfare* rilegata alla sola dimensione tradizionale di guerra tra stati. Infatti, nella maggior parte

[20] Schmitt, M. N. (Cur.). (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf. (Vedi p. 106).
[21] Clarke, R. A., & Knake, R. K. (2014). Cyber war. Old Saybrook: Tantor Media, Incorporated.
[22] Lisi, S., & Gori, U. (2015). Cyber Warfare 2014: armi cibernetiche, sicurezza nazionale e difesa del business. Cyber Warfare 2014, 1-287.
[23] Gori, U., & Lisi, S. (2015). Cyber Warfare, Armi cibernetiche, sicurezza nazionale e difesa del business.

dei casi le attività di *Cyber Warfare* avvengono in modo segreto, imprevedibile e gli effetti non sono sempre evidenti subito. Esso non riconosce i confini geografici di uno stato, non esistono. Questo rende difficile riconoscere un attacco ad uno stato o ad una organizzazione.

> "Nel momento in cui ci rendiamo conto che tutte queste azioni di non guerra possono essere i nuovi fattori costitutivi dello scenario di guerra del futuro, dobbiamo inevitabilmente trovare un nuovo nome per questa nuova forma di guerra, uno scenario che trascende qualsiasi confine e limite. In poche parole una guerra senza limiti."[24].

Queste le parole di due generali cinesi, nella seconda metà degli anni Novanta, sostenendo l'inesistenza di confini di quello che oggi chiamiamo *Cyber Warfare.* Loro sostengono proprio che non esiste effettivamente un confine o un limite che ci aiuti a definire effettivamente questa nuova forma di guerra. Per questo motivo il dilemma nella letteratura odierna è proprio comprendere se effettivamente tutti i mezzi che conosciamo si possono impiegare in questa guerra senza limiti.

Il *Cyber Warfare* non riconosce nemmeno confini di impiego, *Tabella 1*[25], dove si evidenziano le tipologie di conflitti[26] che si possono attuare con operazioni e strumenti tipici del *Cyber Warfare.*

Militari	***Trans-militari***	***Non militari***
Guerra atomica	Guerra diplomatica	Guerra finanziaria
Guerra convenzionale	Guerra di network	Guerra commerciale
Guerra biochimica	Guerra di intelligence	Guerra di risorse
Guerra ecologica	Guerra psicologica	Guerra di aiuto economico
Guerra spaziale	Guerra tattica	Guerra normativa
Guerra elettronica	Guerra di contrabbando	Guerra di sanzioni
Guerra di guerriglia	Guerra di droga	Guerra mediatica
Guerra terroristica	Guerra virtuale	Guerra ideologica

Tabella 1 – Tipologie di guerra

[24] Xiangsui, Q. L. W. (2001). Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione. p.50
[25] Rapaccini, (2017). Cyberwarfare: definizioni, casi di studio e analisi
[26] Xiangsui, Q. L. W. (2001). Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione. p.50

In questo modo accade che "in larghissima parte, la guerra non è nemmeno più guerra, quanto piuttosto uno scontrarsi in internet, fronteggiare i mass media, attaccare e difendersi in transazioni di cambio a termine, insieme a tutta una serie di realtà che non abbiamo mai considerato come 'guerra', e che potrebbero coglierci di sorpresa"[27]

1.4 Gli attori principali del cyber warfare

Bisogna distinguere tra diversi tipi di attori principali che operano nel campo del *cyberwarfare*:

- stati sovrani;
- mercenari;
- hacktivisti[28];
- terroristi;
- cyber crimine organizzato;
- aziende e gruppi finanziari.

E' evidente come molti più ambiti possono essere coinvolti rispetto agli attori principali che ritroviamo in un tradizionale scontro. Inoltre, è interessante notare la presenza di aziende e gruppi finanziari in questa lista. Quest'ultime sono spesso responsabile di una qualsiasi azione non violenta di *cyberwarfare* come lo spionaggio industriale o la diffusione di pubblicità negativa.

Il concetto generale di cyberwarfare, a seconda degli obiettivi degli attori e delle modalità di perseguimento, può essere quindi esteso ad altri campi, identificandosi in nuovi aspetti come il cyber terrorismo o cyber crimine.[29] Non è sufficiente, al fine della comprensione, fermarci a questa distinzione. Come detto in precedenza vengono distinti gli *attori statali* da quelli *non-statali*[30]. Quando parliamo di *attori statali* facciamo riferimento ad entità statali come governi, ministeri della difesa e aziende pubbliche che dispongono di un personale qualificato o che ricorrono ad attori non statali per conseguire i propri obiettivi politici, militari e amministrativi.[31] Gli attori non statali invece sono liberi professionisti, aziende private, attivisti

[27] *Ivi. P.125*
[28] Il termine "hacktivista" deriva dall'inglese "hacktivism", che "[...] indica la pratica di utilizzare in maniera diretta ed a volte sovversiva un computer e una rete, con una precisa finalità politica". Si veda: E. Florindi,"Deep Web e Bitcoin", Imprimatur, 2016, p. 164.
[29] Rapaccini, (2017). Cyberwarfare: definizioni, casi di studio e analisi
[30] S. Mele, "Cyberwarfare e danni ai cittadini", p. 13.
[31] Rapaccini, (2017). Cyberwarfare: definizioni, casi di studio e analisi

e militanti che effettuano cyber operations per motivi ideologici o economici, agendo in modo arbitrario o per conto di terzi. [32] Gli attori statali si dedicano a due attività distinte[33]:

- *Cyberespionage:* Spionaggio esercitato mediante la rete telematica con il fine di raccogliere informazioni civili e governativi[34]. Un esempio è il caso *Datagate*[35] dove l'ex dipendente dell'*NSA*[36] *Edward Snowden*[37] ha rivelato pubblicamente l'esistenza del programma di sorveglianza di massa *PRISM*[38];
- progettazione e utilizzo di *cyber armi*: gli enti statali finanziano la progettazione di armi cibernetiche, mentre lo sviluppo delle varie componenti viene affidato ad aziende private o cyber criminali.[39] E' possibile notare una collaborazione tra stati e gruppi privati come hacker, criminali e specialisti "[...] necessari per la parte economica e di finanziamento della ricerca, per l'intelligence sull'obiettivo e l'eventuale iniezione della cyber-arma in caso di sistemi non direttamente connessi alla rete Internet (come è avvenuto per Stuxnet[40]) o di difficile accesso"[41], mentre i secondi sono "[...] utili per ottimizzare la risorsa tempo e l'impiego di forza-lavoro specializzata. [...] non è un caso che la realizzazione di Stuxnet pare essere stata delegata a più soggetti non- governativi,

[32] *Ibidem*
[33] *Ibidem*
[34] Treccani enciclopedia: Cyber spionaggio
[35] "Datagate": scandalo scoppiato nel 2013 in seguito alla diffusione di documenti riservati sulle attività di spionaggio di massa condotte dall'NSA. Per approfondire: http://www.internazionale.it/notizie/2015/06/25/datagate-snowden- spionaggio (31/05/2018).
[36] L'NSA (National Security Agency) è l'agenzia governativa statunitense che si occupa di garantire la sicurezza nazionale. Mentre la CIA si occupa dello spionaggio all'estero, l'NSA è responsabile delle operazioni di intelligence in territorio americano. Sito ufficiale: https://www.nsa.gov/ (31/05/2018).
[37] Edward Joseph Snowden, ex tecnico della CIA e collaboratore della Booz Allen Hamilton, azienda consulente dell'NSA, è un informatico statunitense che ha dato origine allo scandalo Datagate, grazie alla pubblicazione di documenti top secret sulla piattaforma WikiLeaks. Accusato di spionaggio e di furto di proprietà governativa, Snowden attualmente risiede in Russia dove ha richiesto asilo. Profilo Twitter ufficiale di Snowden: https://twitter.com/snowden (31/05/2018).
[38] PRISM è uno strumento software utilizzato dall'NSA per raccogliere dati sugli utenti di Gmail, Facebook, Outlook e altri fornitori di servizi online. Per approfondire: http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism- surveillance-cheat-sheet (31/05/2018).
[39] Rapaccini, (2017). Cyberwarfare: definizioni, casi di studio e analisi
[40] Stuxnet è uno dei virus informatici passati alla storia per essere tra i più distruttivi mai realizzati. La particolarità di Stuxnet era la sua capacità di danneggiare direttamente le strutture fisiche tramite dei drive USB infetti.
[41] S. Mele, "Cyber-Weapons: aspetti giuridici e strategici", versione 2.0, Istituto Italiano di Studi Strategici "Niccolò Machiavelli", 2013, paper consultabile all'indirizzo: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and- Strategic-Aspects-V2.0.pdf (31/05/2018), p. 15.

ognuno dei quali deputato a sviluppare solo una parte del malware restando all'oscuro del progetto complessivo".[42]

Gli *Hacktivisti* sono invece personaggi che agiscono prevalentemente per scopi politici, ideologici o personal e possono decidere di operare singolarmente o in gruppi, come Anonymous[43], per condurre attacchi più ampi e contro bersagli ambiziosi (come un sito web militare o i sistemi informatici di una multinazionale), sfruttando reti protette e chat sicure tipiche del Dark Web[44].

Quando nominiamo le aziende parliamo di *PMI* e *multinazionali.* Esse operano nel campo informatico e tecnologico e spesso sono incaricate dagli stati o governi di sviluppare *componenti software* per *cyber armi*. Altre aziende potrebbero essere collegate con organizzazioni criminali o statali col fine di utilizzare una *cyber weapon* in operazioni di *cyberwarfare* con scopi diversi dalla *progettazione di software.*

I gruppi finanziari, attori non-statali, possono distinguersi per operazioni di *terrorismo finanziario*[45]. Un esempio chiaro che mi aiuta a spiegare questo tipo di operazione è il caso di George Soros, imprenditore ungherese, che durante la crisi finanziaria asiatica del 1997 ha usato gli strumenti finanziari derivati per incentivare l'instabilità e causare una bolla finanziaria[46].

1.5 Le armi del cyber warfare: Cyber weapons

È importante capire la differenza tra una *Cyber weapons* e un comune attacco *hacker*. Abbiamo nominato spesso il concetto di Cyber arma ma non ne abbiamo ancora dato una definizione chiara.

> "Inquadrare dal punto di vista giuridico il concetto di cyber arma, infatti, risulta ormai uno sforzo di primaria importanza per avere la possibilità di valutare correttamente sia il livello

[42] *Ibidem*
[43] "Anonymous" è il nome di un'organizzazione internazionale di attivisti che agiscono in modo anonimo, coordinato o individuale, contro ogni sorta di censura e di mistificazione, in nome della libertà di parola e dei diritti umani
[44] Con il termine dark web si identifica la parte più profonda del deep web, costituita dalle cosiddette DarkNet: si tratta di contenuti intenzionalmente nascosti ai comuni navigatori e accessibili soltanto attraverso appositi strumenti [...] di anonimato.
[45] Rapaccini, (2017). Cyberwarfare: definizioni, casi di studio e analisi
[46] Andrea Giuntini, A. (2011). La crisi economica fra interpretazione, narrazione e retorica. Storici a confronto. Memoria e Ricerca, (2010/35).

> di minaccia proveniente da un attacco informatico, che le eventuali responsabilità politiche e giuridiche ascrivibili a chi ha agito"[47]

Una *Cyber arma* è, in sintesi, un'avanzata e sofisticata porzione di codice che può essere impiegata a scopi militari o di intelligence[48]. Essa viene usata sia per condurre una *Cyberwar* sia per delle operazioni di *Cyberwarfare.*

La definizione che abbiamo appena dato non ci aiuta a identificare il concetto di *Cyber weapon.* Dobbiamo quindi andare più nel dettaglio per comprendere cosa contraddistingue una *cyber arma.* Le *Cyber weapon* sono caratterizzata da tre elementi fondamentali[49]:

1. *Contesto:* ci deve essere una situazione tipica di un atto di Cyberwarfare o un qualsiasi tipo di conflitto tra attori statali e non;
2. *Scopo:* l'obiettivo deve essere quello di "procurare anche indirettamente un danno fisico a cose o persone ovvero di danneggiare in maniera diretta i sistemi informativi di un obiettivo critico nazionale del soggetto attaccato"[50];
3. *Mezzo/strumento:* cioè attraverso quale canale; dispositivo o software viene compiuto l'attacco

Dati questi elementi possiamo dare una definizione univoca di *Cyber arma:*

> "un'apparecchiatura, un dispositivo ovvero un qualsiasi insieme di istruzioni informatiche utilizzato all'interno di un conflitto tra attori, statali e non, al fine di procurare anche indirettamente un danno fisico a cose o persone, ovvero di danneggiare in maniera diretta i sistemi informativi di un obiettivo critico nazionale del soggetto attaccato"[51]

In aggiunta le Cyber weapons possono essere suddivise in due tipologie[52]:

1. *Proprie:* armi create appositamente per colpire un obiettivo ben preciso, come ad esempio Stuxnet. Paragonabile ad una cyber arma propria è la pistola;
2. *Improprie:* possono essere strumenti hardware o software "passivi" o difensivi pensati per la sicurezza dei sistemi informatici, che all'occorrenza possono essere usati anche per attacchi. Paragonabile ad un'arma impropria

[47] S, Mele "Cyber-Weapons: aspetti giuridici e strategici", op. cit., p. 8.
[48] Definizione di "cyber weapon" secondo la compagnia di sicurezza informatica Heimdal Security.
[49] S. MELE, "Cyber-Weapons: aspetti giuridici e strategici", op. cit., p. 10
[50] *Ibidem*
[51] *Ibidem.*
[52] *Cfr. Ivi, pp. 10-11*

> sono ad esempio le mura difensive di una città: dal momento in cui si ha il controllo delle mura, si ha anche il controlla della difesa, ma dopo che il nemico ha conquistato le mura, i difensori all'interno delle mura si trovano in una posizione di svantaggio rispetto al nemico.

La rivoluzione tecnologica ha favorito lo stravolgimento del concetto stesso di "potere" nelle dinamiche della politica internazionale trascinando il sistema verso un processo di spoliticizzazione della violenza.[53] Infatti, l'aumento della diffusione delle tecnologie ICTs[54] nel settore bellico, così come la relativa assenza di soglia di accesso a tali strumenti, hanno provocato un superamento del concetto classico di arma, dal momento che oggetti apparentemente pacifici, pensati e prodotti per l'ambito civile, si sono trasformati in mezzi offensivi di portata globale.[55]

A tal proposito Alessandro Colombo sottolinea che:

> Se l'abbassamento della soglia d'accesso alle armi leggere aumentava la vulnerabilità delle società e degli stati deboli, la propensione delle tecnologie civili a essere trasformate in strumenti offensivi aumenta prima di tutto quella delle società complesse. [...] A mano a mano che crescono l'interconnessione e la concentrazione di ricchezza, capitale umano, conoscenza e comunicazione in un insieme di nodi strategici e simbolici – le 'città globali' come New York o, al suo interno, il World Trade Center – aumentano anche gli spazi (compreso quello virtuale) di un possibile attacco effettuato con mezzi 'non convenzionali' (non più nel senso di 'estremi', bensì di 'apparentemente pacifici')[56]

1.6 Diverse tipologie di cyber-activities: cyber exploitation, cyber espionage e cyber attack

Le cyber- activities che si possono attuare possono essere di varie tipologie. La *Cyber exploitation* è una di queste. Sulla base di questa visione comparatistica, è possibile asserire che l'attività di *Cyber exploitation* viene generalmente considerata come un comportamento ostile realizzato contro una rete di computers[57]. La differenza con un *Cyber attack* è che questa

[53] Rapaccini, (2017). Cyberwarfare: definizioni, casi di studio e analisi
[54] ICT: (*Information and Communication Technologies*) Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni.
[55] Xiangsui, Q. L. W. (2001). Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione.
[56] Colombo, A. (2006). La guerra ineguale: pace e violenza nel tramonto della società internazionale. Il mulino.
[57] Wortham, A. (2012). Should cyber exploitation ever constitute demonstration of hostile intent that may violate un charter provisions prohibiting the threat or use of force. Federal Communications Law Journal, 64(3), 643-660.

è un attacco diretto contro una rete di computers, con l'obiettivo di causare danni ad oggetti, lesione o morte mentre *Cyber exploitation* si caratterizza per il tentativo di ottenere informazioni attraverso sistemi o reti di computer avversari[58]. L'elemento principale di questa attività è la raccolta di informazioni che non va a colpire il corretto funzionamento dell'attività di rete. Il punto in comune tra i due, *cyber attack* e *cyber exploitation*, è che esiste una vulnerabilità del sistema delle reti. Il carattere che invece li differenzia è la segretezza. Nel caso del *Cyber attack*, la segretezza è inferiore rispetto al *Cyber exploitation* che invece è l'elemento fondamentale[59]. Ultimo concetto da spiegare è il concetto di *Cyber-espionage*: la caratteristica principale è quella di riunire un gran numero di informazioni, che non sono reperibile dai normali motori di ricerca, per porre lo stato in questione in una posizione di vantaggio rispetto ad un gruppo, un altro stato o un singolo soggetto. Si può quindi evincere che, negli ultimi anni, la tecnologia ha aumentato i metodi di attacco e di armi utilizzate. Per questo motivo è importante capire come la difesa dei vari attori si sia modificata, con l'avvento della *cyberwar* e soprattutto quale sia il miglior mezzo per difendere le proprie informazioni e i propri territori. È per questo che la sicurezza è il tema centrale del prossimo capitolo. Ritengo infatti che dopo la trattazione del *cyber war* è indispensabile capire come essa sia nata, come si sia modificata e perché è avvenuto questo cambiamento. Fatta questa premessa cercherò di rispondere alla domanda che mi sono posta analizzando questo tema, ossia come, con l'introduzione dell'era cibernetica, il concetto di sicurezza si è evoluto. Si è passati da un tradizionale concetto di sicurezza, ad oggi non più del tutto efficiente, ad un concetto ancora in evoluzione di Cyber Security. Questo passaggio ha portato con sé non solo gli aspetti positivi della scoperta e della tecnologia ma anche quelli negativi di un nuovo modo di fare guerra, di attaccare e di conseguenza di difendere (Cyber Security). In generale, l'evoluzione del concetto di sicurezza cibernetica è stata influenzata dalla crescente dipendenza delle società moderne dai sistemi informatici e dalla diffusione di nuove tecnologie. Le ipotesi al riguardo includono l'adozione di strategie di cyber security sempre più avanzate, l'utilizzo di tecnologie emergenti come l'intelligenza artificiale per la prevenzione e la gestione degli attacchi informatici, e la collaborazione tra le nazioni per affrontare le minacce a livello globale.

[58] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace
[59] Denning, P. J., & Denning, D. E. (2010). Discussing cyber attack. Communications of the ACM, 53(9), 29-31.

CAPITOLO 2

2. CYBER SECURITY

2.1 Il concetto generale di sicurezza nazionale

Il secondo capitolo del testo è dedicato alla cybersecurity e alla sua evoluzione nel contesto delle minacce informatiche descritte nel primo capitolo. La domanda di ricerca riguarda l'evoluzione del concetto di sicurezza cibernetica e le ipotesi al riguardo, e questo capitolo sarà l'occasione per esplorare le variabili e le opportunità di miglioramento in questo campo.
Nel primo capitolo, abbiamo visto come le minacce informatiche siano aumentate in numero e sofisticazione, spingendo le organizzazioni a rafforzare le proprie difese e investire maggiormente in sicurezza informatica. Nel secondo capitolo, esamineremo in dettaglio le strategie e le tecniche utilizzate per proteggere i sistemi informatici dalle minacce informatiche, partendo dal concetto generale di sicurezza nazionale.
Inoltre, esploreremo le opportunità offerte dall'utilizzo dell'intelligenza artificiale e della resilienza nella sicurezza cibernetica, verificando se le ipotesi formulate siano state verificate nella pratica. Infine, discuteremo il ruolo della collaborazione tra i settori pubblico e privato per affrontare le minacce informatiche in modo più efficace.
In sintesi, questo capitolo rappresenta un'occasione per esplorare l'evoluzione del concetto di sicurezza cibernetica, le variabili e le opportunità di miglioramento della sicurezza informatica, approfondendo le ipotesi formulate nella domanda di ricerca e fornendo una visione più completa del contesto della cybersecurity.
In generale la sicurezza nazionale viene concepita in termini militare e viene definita come l'abilità del paese di difendersi dalle incursioni armate[60]. Ad oggi, con l'avvento dell'era cibernetica e di guerre sempre più asimmetriche, è necessario ridefinire il concetto di sicurezza. Il mondo, la società e i territori sono spesso minacciati in modi che trascendono i calcoli della sicurezza tradizionale. La sicurezza in generale è contraddistinta da quattro distinte ma interconnesse dimensioni che hanno caratteristiche e variabili diverse: la sicurezza esterna, la sicurezza interna, la sicurezza ambientale e la sicurezza virtuale (*cyber security*)[61]. È possibile

[60] La Rocca, (2015). La Cyberpolitica nelle Relazioni Internazionali.
[61] *Ibidem*

dedurre che uno stato è considerato sicuro se tutte e quattro le dimensioni della sicurezza sono solide.

La sicurezza esterna ci concentra sulla capacità di difendere i confini territoriale contro minacce militari[62]. È considerata centrale nella visione della sicurezza tradizionale e trattata con particolare attenzione nella teoria realista delle relazioni internazionali. La sicurezza interna è visibile grazie alla stabilità e la legittimazione delle istituzioni governative e al loro potere all'interno dei possibili conflitti interni ai confini nazionali[63]. La sicurezza interna si concentra non solo sulle questioni militari ma e soprattutto su quelle politiche. La sicurezza ambientale è caratterizzata dagli elementi naturali e dalla loro resilienza nei confronti della pressione che è generata dalla popolazione, dall'accesso alle risorse e dalla tecnologia[64]. Questa sicurezza si caratterizza dalla capacità di assecondare le richieste della popolazione. La sicurezza virtuale, *cyber security*, è l'ultima dimensione della sicurezza statale. È definita come la capacità di uno stato di proteggere sé stesso e le sue istituzioni da minacce, spionaggio, sabotaggio, crimine, frode e altre transizioni virtuali.[65] Avendo fatto questa premessa bisogna tenere conto che ogni dimensione spesso interagisce con l'altra. Proprio per questo, quando tutte e quattro funzionano, uno stato può essere considerato solido.

Una volta chiarito che cos'è la sicurezza nazionale e le varie dimensioni che la compongono è importante analizzare le minacce che potrebbero mettere in pericolo lo stato-nazione. Quali sono le minacce che mettono in pericolo l'indipendenza politica, l'integrità territoriale e la coesione sociopolitica dello stato? In questo contesto è possibile dividere gli interessi di un paese in tre sottosettori: politico-militare, economica e energetica.[66] È importante specificare che queste sono semplicemente sfere concettuali che ci aiutano nell'analisi, ogni valutazione deve essere fatta caso per caso a seconda delle circostanze peculiari di un paese. Ogni setto settore racchiude in sé delle minacce specifiche che sono spesso interconnesse creando così delle sovrapposizioni di interessi. Questa dinamica crea la cosiddetta "catena della sicurezza", Tabella *2* [67],dove si ritrovano i tre settori critici dove lo stato-nazione deve intervenire per proteggere i propri interessi [68]. La catena è uno strumento analitico che serva a valutare le minacce secondo gli interessi di uno stato. Si divide in livello settoriale (minacce specifiche al settore), livello intersettoriale (la sovrapposizione di due settori) e infine il livello di sicurezza

[62] *Ibidem*
[63] *Ibidem*
[64] *Ibidem*
[65] *Ibidem*
[66] Camilli, E. (2014). Sicurezza nazionale: tra concetto e strategia.
[67] *Ibidem*
[68] *Ibidem*

nazionale dove si sovrappongono i settori[69]. La *cyber security*, sicurezza cibernetica, appartiene all'ultimo livello perché i vari attacchi possono gravare sugli interessi nazionali.

Tabella 2 – La catena della sicurezza

2.2 I concetti di Cyber Security e Cyber Defense

È stato necessario discutere del concetto generale di sicurezza nazionale per poter introdurre un concetto nuovo, la sicurezza cibernetica o Cyber Security. Con un rapido sviluppo di internet e soprattutto grazie alla globalizzazione il cyberspace è diventata una delle piattaforme più grandi e importanti mai esistite sia per lo scambio delle informazioni sia per l'economia globale. Bisogna tener conto che questa evoluzione ha portato con sé non solo l'aspetto innovativo e positivo della tecnologia ma, come tutto, anche un aspetto negativo, come ad esempio i crimini informatici. Molti sono gli studi che negli anni sono stati effettuati intorno al termine di *Cyber Security* e *Cyber Defense* ed è per questo che non è facile dare una definizione unitaria di *Cyber security*. La *Cyber Security* è il campo dell'informatica che si occupa di proteggere i sistemi informatici, le reti, i dati e le infrastrutture connesse dalle minacce informatiche, come attacchi informatici, virus informatici, accessi non autorizzati, furti di dati e altre attività malevole[70]. La cybersecurity mira a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni e dei sistemi informatici, al fine di prevenire danni o perdite

[69] *Ibidem*
[70] Pili, G. Cyber security e cyber guerra.

che potrebbero compromettere la sicurezza, la privacy o la continuità delle attività di un'organizzazione. Essa si basa su una serie di tecniche e strumenti di sicurezza informatica, come firewall, software antivirus, sistemi di rilevamento delle intrusioni, crittografia, autenticazione degli utenti, e così via[71]. Tuttavia, la cybersecurity non riguarda solo l'aspetto tecnologico, ma anche la gestione dei rischi e delle politiche di sicurezza[72]. Come detto precedentemente la sicurezza nazionale è una questione prettamente statale mentre non è possibile riuscire a contenere la cyber security in questa dimensione. Per questo motivo è necessario rifarsi ad una seri di documenti per fornire una visione, e quindi una definizione, generale del tema. Secondo l'Agenzia Europea per la sicurezza delle reti e dell'informazione (ENISA)[73], è necessario che ciascun stato si doti di una "*National cyber security strategy (NCISS)*" per affrontare tutti i pericoli derivanti da attacchi cibernetici sulla base della definizione fornita da *Tallinn Manual* alla *Rule 30.* Il Tallinn Manual è un documento che fornisce linee guida e raccomandazioni per l'applicazione delle leggi internazionali alle operazioni cibernetiche. La Rule 30 è una semplice regola matematica che produce schemi di comportamento complessi. Il lavoro svolto da ENISA è fondamentale perché pone le linee guida per quelli che sono i caratteri comuni dei vari piani strategici relativi alla cyber security per tutti gli stati[74]. Adottare strategie per la sicurezza informatica si è rivelato uno strumento utile per migliorare non solo la sicurezza nazionale ma anche la resilienza delle infrastrutture e dei servizi nazionale[75]. Queste strategie portano gli stati a stabilire una serie di obiettivi e di priorità che saranno successivamente raggiunti e che garantiscono al singolo stato di attivare un'attività di *Cyber Defense* in presenza di vari attacchi[76].

Successivamente alla caduta delle torri gemelle gli Stati Uniti adottano un piano di *Cyber* sicurezza nazionale[77]. Questo perché il paese si è reso contro che le minacce possono provenire da diversi fonti e l'adozione di un piano di cybersecurity nazionale è stato necessario per proteggere le infrastrutture critiche del paese, come le infrastrutture di trasporto. Con questa azione si stabiliscono i settori di interesse del paese e il cyberspace diventa una zona di controllo degli Stati Uniti[78]. In aggiunta a ciò, introducono la "*International strategy for cyber-*

[71] Pili, G. Cyber security e cyber guerra.
[72] *Ibidem*
[73] ENISA. (2012, 8 maggio). National Cyber Security Strategies: setting the course for national efforts to strengthen security in cyberspace.
[74] *Ibidem*
[75] *Ibidem*
[76] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace
[77] United Nations CISA. (2003). National Strategy to Secure Cyberspace. Consultato da https://www.cisa.gov/national-strategy-secure-cyberspace
[78] *Ibidem*

space" nel maggio del 2011[79], aggiornato con "*National cyber strategy of United States Of America*" approvato dall'ex presidente Donald Trump nel settembre del 2018[80]. Tra gli obiettivi di questo piano rientrano: la difesa della patria tramite la protezione delle reti, la promozione della prosperità americana tramite l'alimentazione di un'economia digitale più sicura e fiorente ma soprattutto il mantenimento della pace e della sicurezza rafforzando, in concerto con alleati e partner internazionali, la capacità statale di scoraggiare e, in determinati casi, punire coloro che utilizzano strumenti informatici per scopi illeciti[81]. Gli Stati Uniti hanno dato il via ad una serie di azioni, concernenti la *Cyber* sicurezza nazionale, adottati da molti paesi europei. Come la Germania che, nel 2016, adotta il piano "Cyber security strategy for Germany[82]" che si fonda su quattro libelli distinti: mantenimento della sicurezza e dell'autonomia tedesca all'interno del mondo digitale; implementazione della collaborazione tra il governo tedesco e il settore privato; creazione di un'architettura forte e sostenibile per la sicurezza informatica; amplificazione del ruolo attivo della Germania nella politica europea ed internazionale in tema di sicurezza informatica[83]. Da un punto di vista Italiano viene adottato nel 2013 il "*National strategic framework for cyberspace security*"[84]. Le azioni che vengono svolte con questo documento sono il rafforzamento di infrastrutture critiche nazionali e della loro capacità di difesa, il miglioramento della capacità di controazione. Nei confronti di attività criminali ed infine l'implementazione di una migliore cooperazione internazionale in materia di sicurezza informatica[85]. Mancando quindi una definizione chiara di *Cyber Security* è possibile comprenderne la dimensione solo analizzando le azioni adottate da stato a stato andando a delineare una serie di elementi comuni a tutte le strategie fino ad ora discusse[86]. Introducendo il concetto di *Cyber Defense* è importante analizzare subito la differenza con la *Cyber Security*. La prima si concentra sulla prevenzione degli attacchi informatici e sulla

[79] National Security Council (U.S.), & United States. Executive Office of the President. (2011). International strategy for cyberspace: Prosperity, security, and openness in a networked world. [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspac e.pdf
[80] National Security Council (U.S.), & United States. Executive Office of the President. (2018). National Cyber Strategy of the United States of America. [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council. Consultato da https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[81] *Ibidem*
[82] ENISA. (2016). German National Cyber Security Strategy. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany
[83] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace
[84] Presidency of the Council of Ministers. (2013). National Strategic Framework for Cyberspace Security. Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian- national-strategic-framework-for-cyberspace-security.pdf
[85] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace
[86] ENISA, op. cit., p. 41.

protezione delle risorse digitali, mentre la seconda riguarda la risposta agli attacchi informatici e la gestione degli incidenti di sicurezza informatica[87]. La cyber defense si occupa quindi di identificare le minacce informatiche in atto, di valutare gli impatti degli attacchi informatici, di mettere in atto misure per contenere e mitigare gli effetti degli attacchi informatici, di ripristinare le funzionalità dei sistemi informatici colpiti e di ricostruire le informazioni e i dati perduti o compromessi.[88] E' possibile dividere l'attività di difesa in due tipologie*: active cyber defense* e *passive cyber defense*[89]. Il primo è una strategia di difesa informatica che prevede l'adozione di misure proattive per proteggere i sistemi informatici e prevenire gli attacchi informatici, implica l'utilizzo di tecniche di intelligence e di analisi dei dati per identificare le minacce informatiche in atto e prevenire gli attacchi prima che possano causare danni.[90] Tra i benefici dell'Active Defense vi è la capacità di rilevare gli attacchi in modo più tempestivo, impedendo ai criminali informatici di portare a termine il loro intento. Inoltre, l'Active Defense può anche consentire di identificare gli attaccanti e monitorare le loro attività, fornendo informazioni preziose per le indagini di sicurezza. Tuttavia, come accennato, l'Active Defense può comportare rischi legali e di privacy. Il secondo è una strategia di difesa informatica che si basa principalmente sulla protezione dei sistemi informatici da attacchi esterni. In pratica, la *passive cyber defense* implica l'adozione di misure di sicurezza per proteggere i sistemi informatici, come l'utilizzo di firewall, antivirus e altre soluzioni di sicurezza. Tra i benefici del Passive Defense vi è la maggiore facilità di implementazione, la riduzione dei rischi legali e di privacy e la maggiore flessibilità nella gestione dei sistemi. Tuttavia, il Passive Defense può risultare meno efficace nel rilevare gli attacchi informatici, in quanto si limita a difendersi piuttosto che a prevenire gli attacchi. In generale, la scelta tra Active Defense e Passive Defense dipende dalle esigenze specifiche dell'organizzazione e dalle sue capacità di gestione della sicurezza informatica. Entrambe le strategie presentano benefici e criticità, e la scelta migliore dipenderà dalle esigenze e dalle risorse dell'organizzazione. In ogni caso, è importante che l'organizzazione adotti una strategia di sicurezza informatica efficace e che mantenga costantemente aggiornati i propri sistemi e le proprie politiche di sicurezza. In sintesi, la *Cyber Security* e la *Cyber Defense* sono due aspetti complementari della sicurezza informatica, in cui la prima si concentra sulla prevenzione e la protezione delle risorse digitali, mentre la seconda si occupa della gestione degli incidenti e della risposta agli attacchi informatici.

[87] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace
[88] *Ibidem*
[89] Denning, D. E. (2013). Framework and Principles for Active Cyber Defense. Computers & security, 40. DOI: 10.1016/j.cose.2013.11.004. (Vedi pp. 109-110).
[90] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace

2.3 Evoluzione del concetto di Sicurezza: Industria 4.0

Bisogna fare un passo indietro nel tempo per comprendere a pieno come si è entrati in un'era di guerre asimmetriche e di attacchi cibernetiche. Nell'arco di 200 anni di storia la società ha subito tali e tanti cambiamenti che hanno inciso profondamente su molti aspetti della vita[91]. In particolar modo, lo sviluppo della tecnologia ha determinato una serie di cambiamenti nelle attività umane, nelle istituzioni e nei rapporti tra attori statali e non che sono sempre più sofisticati[92]. Si pensi ad esempio a tutte le attività agricole e di produzioni che oggi vengono svolte in larga scala grazie all'uso sempre più frequente di tecnologie che si adattano ad una grande domanda e ad esigenze personali, professionali, di lavoro e di svago. Le scoperte tecnologiche degli ultimi anni hanno scatenato un effetto sorprendente e trainante dell'evoluzione umana: dalla prima rivoluzione industriale (1750) con le macchine a vapore, alla seconda (1870) con il motore a scoppio e dell'elettricità, alla terza rivoluzione industriale (1950) con l'elettronica e l'informatica[93]. Ad oggi è possibile parlare di "Industria 4.0" che, dal 2011 in poi, ha portato con sé uno sviluppo delle più sofisticate tecnologie in campo sociale, militare e politico. Una rivoluzione innescata dalla nascita dei computer, dei robot, dei satelliti, dell'esplorazione planetaria. Questa quarta rivoluzione ha creato dei modelli, delle strategie e dei paradigmi nuovi di gestione delle attività economiche e scambi commerciali. I principali componenti che hanno determinato questo cambiamento sono[94]:

1. *I big data,* che sono una raccolta molto estesa di dati connessi a diversi tipi di ambienti. Possono provenire da qualsiasi fonte e possono essere di qualsiasi tipo. Un esempio sono le carte di credito collegate a dei conti. Ad oggi, grazie alla velocità di trasmissione, se ne fa un utilizzo sempre maggiore;
2. *Gli analytics*, ossia il complesso di tecniche e degli algoritmi che sono necessari per estrarre dei dati dalle informazioni utili e ricavarne un valore.[95] Un esempio sono lo sviluppo di tecniche di intelligenza artificiale;
3. *L'interazione tra essere umani e macchine* che è possibile vedere con l'introduzione del touch screen o dei comandi vocali;

[91] Pili, G. Cyber security e cyber guerra.
[92] *Ibidem*
[93] Zanfini (2021). Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace
[94] *Ibidem*
[95] *Ibidem*

4. *L'additive manufactuting* anche chiamata tecnologia tridimensionale che permette di poter creare un oggetto dal computer all'oggetto fisico con l'ausilio di un macchinario.

Con l'aumentare di queste interconnessioni, soprattutto nel mondo digitale e con l'uso di internet, il termine *Cyber Security* diventa sempre più importante al fine di prevenire e limitare dei danni che queste muove tecnologie possono causare.[96] Non è un caso che lo sviluppo di tecnologie avanzare e telematiche (ICT), sempre più sofisticate e quindi più pericolose, ha favorito l'insorgere di forme di attività illecite anche definite *Cyber Crime*[97]. È per questo che con l'introduzione dell'era cibernetica, il concetto di sicurezza è cambiato radicalmente. La cyber security, ovvero la protezione delle infrastrutture informatiche e dei dati digitali, è diventata una delle priorità per le organizzazioni di tutto il mondo. I cyber criminali hanno sviluppato tecniche sempre più sofisticate per violare la sicurezza dei sistemi informatici e ottenere accesso a dati sensibili. In questo contesto, la sicurezza informatica non può più essere considerata un'attività marginale o secondaria, ma deve diventare un elemento fondamentale dell'organizzazione. La protezione dei dati, la prevenzione degli attacchi informatici e la gestione delle crisi sono diventate attività cruciali per garantire la continuità del business e la tutela degli interessi dell'organizzazione. Inoltre, la sicurezza informatica non riguarda più solo le organizzazioni private, ma è diventata una preoccupazione anche per le istituzioni pubbliche e governative. La protezione dei dati personali dei cittadini e la difesa dalle minacce informatiche sono diventati temi di grande rilevanza sociale e politica. In sintesi, con l'introduzione dell'era cibernetica, la sicurezza informatica è diventata una sfida fondamentale per le organizzazioni di ogni settore.

2.4 Analisi del Rischio

Con l'evoluzione del concetto di sicurezza è nata l'esigenza di creare delle valutazioni dei rischi associati all'utilizzo dei sistemi informatici e la protezione dei dati sensibili[98]. L'analisi del rischio sulla cybersecurity è un'attività fondamentale per garantire la sicurezza dei sistemi informatici e la protezione dei dati sensibili. Gli investimenti sulla Cyber Security dei privati, delle aziende e delle microimprese sono sempre maggiori.[99]

[96] Pili, G. Cyber security e cyber guerra.
[97] *Ibidem*
[98] *Ibidem*
[99] Stizza, M. (2020). Cybersecurity: La Gestione Del Rischio Aziendale Nell'era Digitale.

Bisogna tenere presente che non è possibile garantire una sicurezza totale soprattutto perché in un contesto di scarsità di risorse è necessario utilizzare una logica di analisi del rischio[100]. In ogni azienda o organizzazione che ha raggiunto un alto livello di gestione della sicurezza è presente un documento di analisi del rischio che viene applicato a processi, applicazioni e altri asset[101].

In primo luogo, l'analisi del rischio sulla cybersecurity parte dall'identificazione del *risk appetite*, ossia quanto l'organizzazione è disposta a esporsi in una situazione in cui una minaccia si realizzi, successivamente ad ogni minaccia viene attribuito un grado dei potenziali rischi, delle vulnerabilità dei sistemi informatici e dell'impatto che avrebbe sull'organizzazione[102]. Si tratta di individuare le minacce esterne e interne che possono compromettere la sicurezza dei sistemi informatici, come gli attacchi informatici, le violazioni dei dati, le perdite dei dati e le interruzioni del servizio. In aggiunta, l'analisi del rischio sulla cybersecurity prevede la definizione di strategie per mitigare i rischi identificati.[103] Si tratta di individuare le contromisure appropriate per ridurre la probabilità che i rischi si verifichino e mitigare l'impatto in caso di eventi indesiderati. In questo contesto, le tecnologie di sicurezza informatica sono fondamentali per garantire la protezione dei sistemi informatici e dei dati sensibili. Tra queste, si possono citare le tecnologie di autenticazione, di crittografia, di firewall e di controllo degli accessi[104]. Tuttavia, le tecnologie di sicurezza informatica da sole non sono sufficienti per garantire la protezione dei sistemi informatici. È necessario adottare una serie di politiche di sicurezza e di *best practice*[105] informatica per minimizzare i rischi associati all'utilizzo dei sistemi informatici[106]. Tra le best practice, si possono citare la definizione di policy di sicurezza informatica, la formazione dei dipendenti sulla sicurezza informatica, la gestione degli accessi e delle autorizzazioni e la gestione delle patch di sicurezza[107].

Inoltre, è importante sottolineare che l'analisi del rischio sulla cybersecurity è un'attività continuativa e dinamica. È necessario monitorare costantemente i sistemi informatici e gli ambienti di lavoro per individuare eventuali nuove minacce e vulnerabilità. In sintesi, l'analisi del rischio sulla cybersecurity è un'attività fondamentale per garantire la protezione dei sistemi informatici e dei dati sensibili. Tale analisi parte dall'identificazione dei potenziali rischi e delle

[100] *Ibidem*
[101] *Ibidem*
[102] *Ibidem*
[103] Pili, G. Cyber security e cyber guerra.
[104] *Ibidem*
[105] Si intendono le esperienze, le procedure o le azioni più significative, o comunque quelle che hanno permesso di ottenere i migliori risultati, relativamente a svariati contesti e obiettivi preposti.
[106] *Ibidem*
[107] Stizza, M. (2020). Cybersecurity: La Gestione Del Rischio Aziendale Nell'era Digitale.

vulnerabilità dei sistemi informatici, passa per la valutazione della probabilità e dell'impatto di tali rischi e si conclude con la definizione di strategie per mitigare i rischi identificati.
In questo contesto è importante fare una piccola digressione sull'analisi del rischio nei confronti delle democrazie odierne che risulta essere un argomento di grande attualità e importanza[108]. In un mondo sempre più interconnesso e digitale, le minacce informatiche rappresentano una minaccia per la sicurezza delle democrazie moderne. In primo luogo, le democrazie odierne sono sempre più dipendenti dai sistemi informatici e dalle tecnologie digitali. L'utilizzo di tali sistemi e tecnologie rappresenta un vantaggio per l'efficienza e la trasparenza dei processi democratici, ma allo stesso tempo rappresenta anche una minaccia per la sicurezza dei sistemi informatici e dei dati sensibili[109]. In secondo luogo, le minacce informatiche contro le democrazie odierne sono sempre più sofisticate e complesse. Tra le minacce più diffuse si possono citare gli attacchi informatici, le violazioni dei dati, le campagne di disinformazione e le attività di spionaggio informatico. In questo contesto, l'analisi del rischio sulla cybersecurity diventa fondamentale per garantire la protezione dei sistemi informatici e dei dati sensibili delle democrazie odierne[110]. Tale analisi consiste nell'identificazione dei potenziali rischi e delle vulnerabilità dei sistemi informatici, nella valutazione della probabilità e dell'impatto di tali rischi e nella definizione di strategie per mitigare i rischi identificati. Per garantire la sicurezza delle democrazie odierne, è importante adottare politiche di sicurezza informatica adeguate, che prevedano la definizione di policy di sicurezza informatica, la formazione dei dipendenti sulla sicurezza informatica, la gestione degli accessi e delle autorizzazioni e la gestione delle patch di sicurezza[111].
Inoltre, è necessario monitorare costantemente i sistemi informatici e gli ambienti di lavoro per individuare eventuali nuove minacce e vulnerabilità. In questo contesto, le tecnologie di sicurezza informatica sono fondamentali per garantire la protezione dei sistemi informatici e dei dati sensibili delle democrazie odierne.

2.5 L'intelligenza artificiale

L'intelligenza artificiale è una delle tematiche più approfondite degli ultimi tempi. Essa può essere usata in molti modi, sicuramente quella più interessante è l'adozione dell'intelligenza

[108] De Luca, S. (2022). Democrazia e rivoluzione digitale. Storia del pensiero politico
[109] *Ibidem*
[110] *Ibidem*
[111] Marrani, D. (2021). Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia

artificiale a difesa di uno stato, di un'organizzazione o di un'azienda. L'IA, posto al servizio della cyber security, permette di potenziare le capacità predittive dei sistemi di difesa di organizzazioni o di aziende, che esse siano private o pubbliche[112]. È per questo motivo che si utilizzano sempre di più le *machine learning* per rilevare le minacce: una branca dell'intelligenza artificiale che consente ai computer di imparare e migliorare le loro prestazioni in base all'esperienza. Il machine learning si basa sull'analisi di grandi quantità di dati, che vengono utilizzati per creare modelli predittivi e algoritmi che consentono ai computer di imparare automaticamente dai dati senza essere esplicitamente programmato. Il vero potenziale e anche la vera scoperta dell'intelligenza artificiale è la capacità di effettuare previsioni realistiche di attacchi quando queste non si sono ancora avverate[113]. Il tradizionale sistema di sicurezza basato su file che venivano usati come vettori di infezione non sono più sufficienti per fermare gli attacchi nel cyberspazio[114]. Ad oggi è sempre più diffuso l'utilizzo di *malware fileless*: è una categoria di malware che non viene memorizzato sul disco rigido come un file, ma piuttosto sfrutta le funzionalità di un sistema operativo per eseguire il suo codice direttamente in memoria. Questo significa che non c'è un file eseguibile da cercare e rimuovere come con il malware tradizionale, rendendo la sua rilevazione più difficile. Inoltre, con l'utilizzo di questo malware si cerca di colpire più obiettivi diversi. L'utilizzo di metodi persistenti è un'altra tipologia di attacco informatico che gli hacker possono utilizzare per infiltrarsi e mantenere il controllo sui sistemi compromessi. Questo tipo di attacco è particolarmente insidioso perché, una volta che il malware è stato installato, può essere difficile da individuare e rimuovere. L'utilizzo di *payload*[115] caricati in memoria rappresenta un modo per l'attaccante di garantire la persistenza del malware sui sistemi compromessi anche dopo il riavvio del sistema. In questo caso, l'attaccante carica il payload in una zona di memoria in cui il sistema operativo non lo rimuoverà e lo utilizza per avviare il malware ogni volta che il sistema viene avviato.

L'utilizzo di "*dual use tools*[116]" è un altro metodo che gli hacker possono utilizzare per infiltrarsi nei sistemi informatici. Questo tipo di attacco consiste nell'utilizzare applicazioni legittime del sistema operativo o strumenti utilizzati comunemente dagli amministratori di

[112] Stizza, M. (2020). Cybersecurity: La Gestione Del Rischio Aziendale Nell'era Digitale
[113] J. S. Nye, The Future of Power, PublicAffairs, New York, 2011.
[114] Pili, G. Cyber security e cyber guerra.
[115] Un payload è un termine utilizzato in informatica per indicare un software malevolo, un virus o un worm che viene inserito all'interno di un altro programma o file legittimo.
[116] Chiamati anche strumenti a doppio uso, sono programmi o applicazioni software che possono essere utilizzati per scopi legittimi o da un attaccante per scopi malevoli

sistema, come PowerShell, per eseguire comandi malevoli[117]. Questo rende difficile per i programmi di sicurezza individuare l'attività del malware, poiché le applicazioni utilizzate sono legittime e non sollevano sospetti.

Per prevenire questi tipi di attacchi, è importante adottare misure di sicurezza a più livelli, come l'utilizzo di software antivirus aggiornati, il monitoraggio costante delle attività di rete, la formazione del personale sulle pratiche di sicurezza e l'implementazione di procedure per la gestione degli accessi e dei permessi utente[118]. Inoltre, è importante mantenere costantemente aggiornati i software e i sistemi operativi per proteggere da eventuali vulnerabilità note che potrebbero essere sfruttate dagli hacker per infiltrarsi nei sistemi. La difesa attiva è una tendenza emergente nell'ambito della sicurezza informatica che si concentra sulla protezione e sulla resilienza degli asset digitali e dei sistemi informatici attraverso un approccio proattivo[119]. Questo approccio mira a prevenire gli attacchi prima che possano causare danni significativi, piuttosto che limitarsi a reagire a un attacco in corso. La difesa attiva si basa su tecniche avanzate come l'intelligenza artificiale (AI) e il machine learning per rilevare e prevenire gli attacchi informatici.[120] L'IA è utilizzata per analizzare grandi quantità di dati e identificare schemi di comportamento anomalo che potrebbero indicare un attacco imminente. Inoltre, la difesa attiva può essere implementata attraverso l'adozione di politiche di sicurezza avanzate, come l'implementazione di logiche di "*security-by-design*[121]", ovvero la progettazione di sistemi informatici tenendo in considerazione i requisiti di sicurezza.[122]

In definitiva, la difesa attiva rappresenta un approccio innovativo alla sicurezza informatica, che si concentra sulla prevenzione piuttosto che sulla reazione. L'adozione di tecniche avanzate come l'intelligenza artificiale e il machine learning, unitamente alla promozione della sicurezza-by-design, può contribuire significativamente a proteggere i sistemi informatici dalle minacce sempre più sofisticate.

2.6 La resilienza nella Sicurezza Cibernetica

Come abbiamo analizzato esistono diverse modalità di minacce che possono provenire dal cyber-spazio e che costringono gli Stati ad adottare misure efficaci per evitare di subire gravi

[117] Teti, A. (2018). Cyber espionage e cyber counterintelligence: spionaggio e controspionaggio cibernetico
[118] *Ibidem*
[119] Rassega, V. (2017). Cyber security risk management nei servizi pubblici strategici.
[120] *Ibidem*
[121] E' un approccio alla sicurezza informatica che mira a integrare la sicurezza nei prodotti e nei sistemi informatici fin dalla fase di progettazione, piuttosto che aggiungere la sicurezza successivamente.
[122] Boot, A. W., & Thakor, A. V. (1993). Security design. The Journal of Finance

danni ai propri sistemi di comunicazione, di comando e controllo[123]. L'obbiettivo da raggiungere non è per niente semplice. La continua evoluzione tecnologia e la velocità con cui essa si propaga fa sì che costantemente vengano pensate nuove strategie di difesa[124]. Conseguentemente il concetto di sicurezza nazionale che viene applicato alla sicurezza cyber assume connotazioni particolari[125]. Il modo convenzionale di pensare alla difesa nazionale è in termini militare e di protezione del territorio, secondo Choucri Nazli. Ovviamente la natura del cyber spazio cambia radicalmente questo paradigma. Secondo Shreier:

> "La sicurezza informatica non può essere raggiunta solo a livello di Stato nazione. Richiede risposte pienamente integrate che includano partenariati pubblico-privato e un coordinamento e una cooperazione internazionali di natura senza precedenti [126]"

Egli ci indica le linee guida per raggiungere una piena ed effettiva Cyber Security. Bisogna considerare la difesa cibernetica come un'entità isolata e indipendente della difesa, anche se spesso è interconnessa e risponde alle stesse esigenze della sicurezza nazionale[127]. È possibile dire che un sistema di sicurezza cibernetica può essere considerato efficace se è in grado di fronteggiare una quantità elevatissima di minacce differenti e un sempre più crescente numero di attori. Se per la sicurezza tradizionale è impossibile pensare ad un territorio totalmente sicuro, in ogni istante, lo stesso vale per la cyber security. Il livello di permeabilità in questo contesto è molto alto ed è per questo che, nonostante le tecnologie si siano evoluti con sistemi di rilevazioni, di isolamento dei malware e di riconoscimento, esse non sono in grado di garantire una sicurezza soddisfacente[128]. Per questo, nello sviluppo delle tecniche di difesa, ci si è basati su un modello difensivo basato sulla *resilienza* che si riferisce alla capacità dei paesi o delle organizzazioni internazionali di adattarsi e resistere a situazioni di crisi o di instabilità politica, economica o sociale[129]. Ciò può includere la capacità di riprendersi da conflitti armati, disastri naturali, crisi finanziarie o epidemie. La resilienza delle relazioni internazionali richiede un forte sistema di cooperazione e coordinamento tra i paesi e le organizzazioni internazionali, nonché un'adeguata capacità di prevenzione e risposta alle situazioni di crisi[130]. Inoltre, richiede anche la capacità di adattarsi ai cambiamenti globali, come le sfide ambientali

[123] Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture.
[124] *Ibidem*
[125] *Ibidem*
[126] Shreier, F. (2010) On Cyber Warfare, DCAF Publication, Geneva, Tradotto
[127] Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture.
[128] *Ibidem*
[129] *Ibidem*
[130] *Ibidem*

o tecnologiche, e di promuovere la pace e la stabilità attraverso la diplomazia e la cooperazione internazionale. Bologna afferma che:

> "Il concetto di resilienza (...) nasce da un modo di porsi che rende capaci di convivere con i fallimenti e le sconfitte, mentre spinge a trovare e valorizzare tutte le risorse e potenzialità: tecnologiche, organizzative, economiche e sociali. Il concetto del "non è mai successo" è sostituito dalla visione del "se dovesse succedere", che non significa necessariamente il sovradimensionamento delle soluzioni, ma la predisposizione e la preparazione all'accadimento dell'evento"[131]

Queste parole si riferiscono principalmente al contesto della sicurezza informatica e alla necessità di essere resilienti contro le minacce informatiche. La consapevolezza delle vulnerabilità e la capacità di reagire rapidamente alle minacce (la *readiness*) sono due elementi fondamentali della resilienza in questo contesto. La *readiness* è la capacità di essere pronti e preparati a fronteggiare una situazione specifica o una minaccia imminente[132]. Il concetto di readiness si riferisce a una serie di misure preventive e di preparazione che vengono messe in atto per minimizzare il rischio di eventuali danni o perdite[133]. Robert Lentz ha elaborato un modello[134] dove mostra come la readiness si sviluppa attraverso un processo graduale di crescita delle competenze individuali e collettive[135]. In particolare, il modello identifica la necessità di creare un ecosistema difensivo efficace e snello, capace di intercettare le minacce in modo tempestivo e di coinvolgere tutti gli utenti nella gestione dei rischi. Questo modello può essere applicato anche a livello internazionale, dove gli stati possono collaborare per creare un sistema di sicurezza informatica condiviso e per sviluppare competenze collettive nella gestione dei rischi[136]. La collaborazione internazionale e la condivisione di informazioni possono aumentare la capacità di risposta degli stati alle minacce informatiche, rendendo il sistema internazionale più resiliente e sicuro. Il passaggio dalla resilienza tradizionale alla resilienza nella cyber security rappresenta una sfida importante per molte organizzazioni e Stati, in quanto richiede un cambiamento di mentalità e di approccio alla sicurezza. La resilienza tradizionale nelle relazioni internazionali è un concetto relativamente nuovo e in

[131] Juvara, R. (2013) Infrastrutture critiche, il centro dell'attenzione. Sandro Bologna, ex Presidente dell'Associazione Italiana Infrastrutture Critiche
[132] Treccan enciclopediai: definizione di readiness
[133] *Ibidem*
[134] GRAUMAN B. (2012) Cyber-security: the vexed question of global rules, Security and Defense Agenda publications, Bruxelles.
[135] Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture.
[136] *Ibidem*

evoluzione che si riferisce alla capacità di adattarsi e di resistere a eventi imprevisti o alle sfide che si presentano nelle relazioni tra stati e tra attori internazionali[137]. La letteratura sulla resilienza nelle relazioni internazionali è ancora in fase di sviluppo, ma ci sono alcuni studi e contributi che hanno iniziato ad approfondire il tema. Uno dei contributi più importanti sulla resilienza nelle relazioni internazionali è stato fornito da Martha Finnemore e Judith Goldstein nel loro libro del 2013 "Back to Basics: State Power in a Contemporary World". In questo lavoro, le autrici sostengono che la resilienza è un elemento cruciale del potere statale e che gli stati più resilienti sono quelli in grado di adattarsi e di reagire rapidamente alle sfide che si presentano nell'arena internazionale[138]. Nella sicurezza tradizionale, la resilienza si concentra spesso sulla capacità di resistere e riprendersi da eventi traumatici come attacchi terroristici, calamità naturali o conflitti militari. Questi eventi possono causare danni fisici alle infrastrutture, alle persone e ai beni, e pertanto si concentra sulla preparazione pre-evento, sulla capacità di risposta durante l'evento e sulla ripresa post-evento. Inoltre, spesso richiede la collaborazione di varie agenzie governative, organizzazioni non governative e cittadini per garantire una risposta efficace e tempestiva. Questo approccio si basa sull'idea che la sicurezza può essere raggiunta attraverso una serie di contromisure tecniche e organizzative volte a ridurre il rischio di attacco e a mitigare le conseguenze in caso di successo dell'attacco. Nella cyber security, invece, la resilienza si concentra sulla capacità di prevenire, rilevare e rispondere agli attacchi informatici, come malware, ransomware, attacchi DDoS e phishing[139]. Gli attacchi informatici possono causare danni a infrastrutture informatiche, dati sensibili, privacy e reputazione. Pertanto, la resilienza nella cyber security si concentra sulla preparazione pre-attacco, sulla capacità di rispondere in modo tempestivo e coordinato all'attacco e sulla capacità di ripristinare rapidamente la situazione precedente all'attacco. Inoltre, la resilienza nella cyber security richiede spesso la collaborazione tra organizzazioni pubbliche e private, fornitori di servizi di sicurezza informatica e utenti finali per garantire una risposta efficace e tempestiva agli attacchi informatici. Questo approccio si basa sulla comprensione che gli attacchi informatici sono inevitabili e che la prevenzione da sola non è sufficiente per garantire la sicurezza. Pertanto, la resilienza nella cyber security prevede una serie di misure volte a garantire la disponibilità delle infrastrutture e dei servizi anche in caso

[137] Tramontana, E. (2017). Il soft law e la resilienza del diritto internazionale.
[138] *Ibidem*
[139] Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture.

di attacco, come la pianificazione di contingenza, la replica di dati, la separazione delle reti e l'uso di sistemi di rilevamento e risposta automatica agli attacchi[140].

2.6 La Sicurezza Cibernetica in Italia

Nel prossimo capitolo ho deciso di concentrarmi su un determinato paese per approfondire meglio come la sicurezza cibernetica si sia evoluta e se le variabili e le ipotesi descritte nei precedenti due capitoli possano essere verificate. L'Italia è un paese che, come molti altri, è stato oggetto di attacchi informatici sempre più frequenti e sofisticati negli ultimi anni. Questi attacchi possono avere gravi conseguenze sulla sicurezza nazionale, sull'economia e sulla privacy dei cittadini. Pertanto, la cyber sicurezza è diventata una priorità per il governo Italiano e per le organizzazioni pubbliche e private che operano nel paese. In aggiunta, l'Italia è un paese membro della UE e ha recepito le principali direttive europee in materia di sicurezza informatica e cybersecurity. Analizzerò in che modo l'Italia ha implementato queste direttive, quali specificità ha introdotto nella propria legislazione e di conseguenza quale sia stata l'evoluzione. Inoltre, l'Italia è uno dei paesi fondatori dell'UE e ha avuto un ruolo significativo nella definizione delle politiche europee di cybersecurity. Comprendere questo aspetto aiuta a inquadrare meglio le strategie cyber adottate a livello europeo e l'evoluzione che il concetto di sicurezza cibernetica ha subito negli anni. Infine, l'Italia è impegnata in diverse iniziative internazionali sulla cybersicurezza, tra cui la Partnership per la Sicurezza e la Stabilità in Europa (OSCE), il Consiglio d'Europa e la NATO. Analizzare il ruolo dell'Italia in queste organizzazioni può fornire una panoramica delle sfide e delle opportunità che si presentano a livello internazionale nella gestione della cybersicurezza. È evidente come in Italia, il concetto di sicurezza cibernetica sia diventato sempre più rilevante con l'aumento della dipendenza dei settori pubblico e privato dai sistemi informatici. Nel 2013 è stato creato il Centro Nazionale per la Protezione delle Infrastrutture Critiche (CNPIC), con l'obiettivo di garantire la sicurezza dei sistemi informatici di importanza strategica per il Paese. Negli ultimi anni, l'Italia ha adottato diverse iniziative per migliorare la sicurezza cibernetica. Tuttavia, ci sono ancora diverse sfide da affrontare per garantire una sicurezza cibernetica adeguata in Italia.

[140] *Ibidem*

CAPITOLO 3

3. IL CASO ITALIANO

3.1 L'impatto degli attacchi cyber in Italia

Gli attacchi cyber rappresentano una minaccia concreta per l'Italia. I recenti episodi di aggressioni informatiche hanno colpito sia aziende strategiche sia istituzioni pubbliche, provocando danni economici e minando la fiducia dei cittadini nei sistemi digitali[141].

Le aziende sono il bersaglio privilegiato degli hacker, che cercano di rubare dati sensibili, sabotare le infrastrutture o chiedere riscatti. Gli attacchi ransomware hanno paralizzato le operations di grandi imprese italiane, costringendole a sospendere la produzione e i servizi con gravi perdite economiche[142]. Questi sono una tipologia di attacco informatico in cui un malintenzionato infetta un sistema informatico con un software malevolo che crittografa i dati presenti sul dispositivo o sulla rete dell'organizzazione colpita, rendendoli inaccessibili[143]. Il malintenzionato richiede quindi un riscatto (ransom) in cambio della decrittografia dei dati, spesso in forma di criptovaluta per difficoltare il tracciamento delle transazioni[144].

In pratica, gli attacchi ransomware sono un'estorsione digitale in cui i dati dell'organizzazione colpita vengono presi in ostaggio, e il riscatto viene richiesto come condizione per la liberazione dei dati. Gli attacchi ransomware possono essere effettuati attraverso diversi vettori di attacco, come e-mail di phishing, exploit di vulnerabilità di software, o attraverso il compromesso di credenziali di accesso[145]. Anche il settore bancario e finanziario deve fare i conti con continui tentativi di furto di credenziali e informazioni riservate dei correntisti.

Le istituzioni pubbliche subiscono attacchi per finalità di spionaggio, destabilizzazione e propaganda. Record contabili, liste elettorali, documenti sensibili sono stati oggetto di attacchi hacker promossi da nazioni ostili per minare la stabilità politica del Paese.

Negli ultimi anni sono stati numerosi gli attacchi cibernetici che ha subito l'Italia. Nel 2021, il Gruppo FS Italiane, il principale operatore del trasporto ferroviario italiano, è stato colpito da un attacco ransomware che ha causato interruzioni dei servizi e rallentamenti dei treni in alcune

[141] Baldoni R., Montanari L., "Italian Security Report. Un framework nazionale per la Cyber Security", Cyber Intelligence and Information Security Center, Sapienza Università di Roma, Febbraio 2018
[142] *Ibidem*
[143] *Ibidem*
[144] Baldoni, R., & De Nicola, R. (2015). Il futuro della Cybersecurity in Italia. CINI-Consorzio Interuniversitario Nazionale Informatica.
[145] *Ibidem*

regioni del paese[146]. Gli hacker hanno criptato i database e i file del Gruppo FS, prendendoli in ostaggio e chiedendo un riscatto. Per evitare il pagamento del riscatto e ripristinare i sistemi, gli esperti della Polizia Postale hanno lavorato per settimane per neutralizzare il ransomware, riuscendo a recuperare parte dei dati criptati[147].

L'attacco ha messo in luce la grave esposizione di un'infrastruttura critica come il trasporto ferroviario alle minacce cyber, evidenziando il livello di maturità ancora insufficiente nella cultura della sicurezza digitale. Per essere protetti da attacchi sempre più sofisticati, complessi e dannosi, i gestori di servizi essenziali devono investire nella formazione continua degli addetti, nell'aggiornamento tecnologico e nella stretta collaborazione con le autorità preposte alla sicurezza nazionale. L'attacco al Gruppo FS ha dimostrato che la cybersicurezza deve diventare una priorità anche per il settore dei trasporti. Nel 2020, l'azienda italiana Campari è stata colpita da un attacco ransomware che ha causato il blocco dei sistemi informatici dell'azienda[148]. I criminali informatici hanno richiesto un riscatto in bitcoin per sbloccare i dati. Questo episodio dimostra ancora una volta l'importanza della prevenzione degli attacchi ransomware attraverso la sicurezza informatica e il backup dei dati. Inoltre, è importante che le organizzazioni siano pronte a gestire eventuali attacchi informatici attraverso piani di risposta agli incidenti e la formazione del personale. Nel 2019, il gruppo bancario Unicredit ha subito un attacco informatico che ha compromesso i dati personali e finanziari di circa 3 milioni di clienti italiani[149]. L'attacco ha coinvolto principalmente i dati relativi ai mutui ipotecari, ma anche informazioni personali come nomi, indirizzi e numeri di telefono sono state compromesse. L'attacco informatico contro UniCredit è stato uno dei più gravi nella storia delle banche italiane, e ha dimostrato l'importanza della sicurezza informatica per le organizzazioni finanziarie, che gestiscono grandi quantità di dati sensibili[150]. L'azienda ha dovuto affrontare una vasta operazione di risposta all'incidente, che ha incluso la notifica dei clienti e l'implementazione di misure di sicurezza aggiuntive per prevenire futuri attacchi. L'attacco informatico contro UniCredit ha sottolineato la necessità per le organizzazioni di adottare misure di sicurezza informatica adeguate, come la crittografia dei dati, l'autenticazione forte e il monitoraggio costante dei sistemi informatici[151]. Inoltre, è importante che le organizzazioni pianifichino e testino regolarmente la loro capacità di risposta agli incidenti, al fine di limitare

[146] Romoli, A. L. (2023). Analisi del settore economico della cybersecurity.
[147] *Ibidem*
[148] *Ibidem*
[149] *Ibidem*
[150] Razzante, R. (2023). L'attribuzione degli attacchi informatici.
[151] *Ibidem*

al minimo i danni in caso di attacco informatico. Sempre nel 2019 l'attacco DDoS contro il sito del Ministero dell'Interno durante le elezioni europee del 2019[152]. DDoS sta per "*Distributed Denial-of-Service*" ed è un tipo di attacco informatico che mira a rendere inaccessibili i servizi online di un'organizzazione, come siti web o applicazioni, saturando la loro capacità di elaborazione con un flusso massiccio di traffico internet[153]. L'attacco viene eseguito da una rete di computer infetti, chiamata "botnet", che agisce in modo coordinato per inviare richieste di connessione simultaneamente ai server dell'organizzazione, sovraccaricandoli e impedendo l'accesso ai servizi online.

Gli attacchi DDoS sono particolarmente dannosi per le organizzazioni che dipendono fortemente dai loro servizi online, come e-commerce, banche online, servizi di streaming video, e altre piattaforme web. Possono causare interruzioni del servizio per ore o addirittura giorni, causando gravi danni economici e reputazionali. Il cyberattacco ha messo ko per alcune ore i servizi online del Viminale[154]. Nel 2016, il gruppo energetico italiano Enel è stato colpito da un attacco informatico che ha causato interruzioni dei servizi elettrici in alcune parti del paese[155]. L'attacco è stato eseguito attraverso un malware che ha colpito il sistema di gestione delle energie rinnovabili dell'azienda, causando interruzioni nella produzione di energia solare ed eolica[156]. L'attacco informatico contro Enel è stato uno dei primi ad aver causato interruzioni dei servizi elettrici in Italia e ha dimostrato l'importanza della sicurezza informatica per le società energetiche, che gestiscono infrastrutture critiche per il funzionamento del paese. In conclusione, gli attacchi cyber rappresentano ormai una grave minaccia per l'Italia. Essi causano ingenti danni economici, minano la fiducia nelle infrastrutture digitali, mettono a rischio la sicurezza delle informazioni sensibili e possono essere utilizzati per interferire nel processo democratico. Per rafforzare la cybersicurezza nazionale è necessario investire in prevenzione, formazione, tecnologie innovative e cooperazione internazionale per respingere questa nuova forma di aggressione silenziosa e subdola.

3.2 Sicurezza nazionale e minaccia cibernetica

Le aziende, le istituzioni pubbliche e le organizzazioni italiane stanno progressivamente rafforzando gli sforzi per fronteggiare le minacce cyber, ma la mentalità di sicurezza è ancora

[152] Razzante, R. (2023). L'attribuzione degli attacchi informatici.
[153] Enciclopedia Treccani: Definizione di DDoS
[154] Razzante, R. (2023). L'attribuzione degli attacchi informatici
[155] Romoli, A. L. (2023). Analisi del settore economico della cybersecurity.
[156] *Ibidem*

lontana dall'essere diffusa e pervasiva. Una delle sfide principali è quella di creare una cultura della sicurezza cibernetica all'interno delle organizzazioni. Molte aziende e organizzazioni in Italia considerano la sicurezza cibernetica come un costo inutile piuttosto che come un investimento necessario per proteggere il proprio business. Tuttavia, le conseguenze di un attacco cyber possono essere molto costose, sia in termini finanziari che reputazionali. Pertanto, è importante che le organizzazioni comprendano la necessità di investire nella sicurezza cibernetica e di adottare le misure necessarie per proteggere i propri dati e le infrastrutture critiche. Soltanto dopo gravi incidenti come attacchi ransomware o furti di dati, le organizzazioni finalmente si impegnano nell'adozione di difese più robuste e nella formazione del personale. Ma si tratta di interventi tardivi, dettati dall'urgenza piuttosto che da una strategia di prevenzione efficace.

La sicurezza nazionale è affidata in parte al governo e ai servizi segreti, ma aziende e individui debbono fare ciascuno la propria parte[157]. Se ogni organizzazione si comportasse in maniera più responsabile, proteggendo le proprie infrastrutture e promuovendo una cultura della sicurezza a tutti i livelli, il rischio cyber per il paese si ridurrebbe notevolmente. Il governo italiano è impegnato nella promozione della sicurezza cibernetica attraverso la creazione di una serie di iniziative, tra cui *l'istituzione dell'Agenzia per la Sicurezza cibernetica* (CNCN)[158] e l'adozione di misure legislative volte a proteggere le infrastrutture critiche. Tuttavia, la sicurezza cibernetica è un problema che richiede un approccio collaborativo, in cui le aziende e le organizzazioni lavorano insieme per proteggere l'ecosistema cibernetico del paese. Per affrontare una minaccia che non conosce confini, le singole entità devono collaborare in maniera più stretta e coordinata. Il dialogo tra pubblico e privato deve intensificarsi, così come la condivisione tempestiva di informazioni sugli attacchi e sulle migliori prassi da adottare. La digitalizzazione produce benefici, ma li mette anche a repentaglio se non è supportata da una strategia di sicurezza condivisa. La creazione del *Laboratorio Nazionale di Intelligenza Artificiale* e *Sistemi Intelligenti* (IA&SI) all'interno del *Consorzio Interuniversitario Nazionale per l'Informatica* (CINI) rappresenta un importante passo avanti nella promozione dell'adozione dell'AI per la sicurezza informatica in Italia.[159] L'IA può essere utilizzata per analizzare grandi quantità di dati in tempo reale, identificare comportamenti anomali e fornire una risposta immediata agli attacchi informatici[160] Il Laboratorio Nazionale di IA&SI ha

[157] Borriello, G., & Fristachi, G. (2022). Stato (d'assedio) digitale e strategia italiana di cybersicurezza.
[158] *Ibidem*
[159] Italian Cybersecurity Report : Controlli Essenziali di Cybersecurity
[160] Rassega, V. (2017). Cyber security risk management nei servizi pubblici strategici.

l'obiettivo di promuovere la ricerca, lo sviluppo e la formazione nell'ambito dell'IA e dei sistemi intelligenti, con particolare attenzione alla sicurezza informatica. Il laboratorio è composto da un gruppo di ricercatori, docenti e studenti universitari che lavorano insieme per sviluppare soluzioni avanzate di sicurezza informatica basate sull'IA. L'IA può essere utilizzata per migliorare la sicurezza informatica in molte aree. Ad esempio, l'IA può essere utilizzata per l'analisi dei dati di log per identificare comportamenti anomali che potrebbero essere indicativi di un attacco informatico in corso. Può anche essere utilizzata per analizzare i flussi di traffico di rete per individuare attività sospette e potenzialmente dannose. Inoltre, è utile per migliorare la sicurezza degli endpoint, ovvero dei dispositivi utilizzati dagli utenti finali per accedere alla rete e ai dati. L'IA può essere utilizzata per identificare comportamenti anomali sui dispositivi, come ad esempio la presenza di malware o l'accesso non autorizzato a dati sensibili. In Italia, finora sono stati fatti passi avanti, ma non sufficienti. Vincere la sfida della cybersicurezza sarà una responsabilità collettiva, e richiederà un cambio di mentalità per fare della protezione dei sistemi e dei dati una priorità non più rinviabile. Il percorso è lungo, ma le energie da mettere in campo sono tante. La cybersecurity è una corsa che non si può perdere.

3.3 Il piano nazionale per la protezione cibernetica e la sicurezza informatica

La legislazione italiana sulle questioni di sicurezza cibernetica e sicurezza nazionale si è sviluppata negli ultimi anni, pur rimanendo ancora parziale e frammentaria. Alcuni provvedimenti hanno gettato le basi per una strategia di difesa cyber del paese, ma molto resta da fare perché le minacce in continua evoluzione trovino una risposta normativa adeguata. È opportuno, per comprendere l'evoluzione della sicurezza cibernetica in Italia, citare la Legge 3 agosto 2007, n. 124, che va a sostituire dopo trent'anni la Legge 801/1977[161], recante disposizioni urgenti in materia di sicurezza che ha introdotto importanti misure a tutela della cybersecurity nazionale. Si tratta di uno dei primi provvedimenti organici sul tema, seppur ancora parziali, dal quale ha poi preso l'avvio una progressiva legislazione di settore. In particolare, la riforma ha creato il *Dipartimento delle Informazioni per la Sicurezza* (DIS), un organismo di coordinamento e controllo dell'intelligence nazionale, che ha assunto la responsabilità di coordinare gli sforzi di cyber difesa tra i vari attori del sistema di sicurezza nazionale, inclusi le forze armate, le forze dell'ordine e le agenzie di intelligence. Inoltre, la

[161] La legge 801/1977 è una legge italiana che riguarda la sicurezza informatica e la protezione dei dati personali. In particolare, la legge ha introdotto il concetto di "secreto informatico", ovvero la protezione dei dati contenuti in sistemi informatici e la punizione di coloro che li violano.

riforma ha introdotto una serie di misure per migliorare la capacità del paese di prevenire e contrastare le minacce informatiche. Ad esempio, sono stati istituiti *i Centri di Protezione delle Infrastrutture Critiche* (CPIC), che hanno il compito di identificare e proteggere le infrastrutture critiche del paese, ad esempio, le reti di telecomunicazioni, le centrali elettriche, le banche e le reti di trasporto), da eventuali attacchi informatici, attraverso l'implementazione di misure di sicurezza informatica adeguate. Inoltre, l'Italia ha sviluppato una serie di strumenti di cyber difesa, tra cui il *Sistema di Allerta Nazionale* (SAN), che ha il compito di individuare e prevenire gli attacchi informatici contro le infrastrutture critiche del paese, e il *Computer Emergency Response Team for Italy* (CERT-IT), che fornisce supporto tecnico alle organizzazioni pubbliche e private per la gestione degli incidenti di sicurezza informatica. In sintesi, la riforma dell'intelligence del 2007 ha rappresentato un importante passo avanti nella modernizzazione dell'apparato di sicurezza nazionale dell'Italia, compresa la cyber difesa. Dal 2009 l'Italia si rende conto che le minacce cibernetiche possono colpire una pluralità di settori interconnessi. Gli attori coinvolti cominciano ad aumentare ed è proprio per questo che lo stato italiano sottolinea la necessità di una pianificazione strategica a livello nazionale e di un impianto organizzativo che assicuri il coordinamento tra gli attori interessati, anche attraverso la ridefinizione delle attività delle strutture esistenti ed una rimodulazione delle attuali competenze e responsabilità[162]. La legge n. 133/2012 è una legge Italiana che ha introdotto importanti innovazioni nel settore della sicurezza informatica, in particolare per quanto riguarda la protezione dei dati personali e che è andata a modificare lievemente la normativa del 2007[163]. La legge ha infatti recepito la normativa europea in materia di protezione dei dati personali (GDPR)[164], introducendo nuove regole e sanzioni per le organizzazioni che gestiscono dati personali. In particolare, la legge ha introdotto l'obbligo per le organizzazioni di notificare le violazioni dei dati personali all'Autorità Garante per la Protezione dei Dati Personali e agli interessati, non appena possibile e in ogni caso entro 72 ore dalla scoperta della violazione. Inoltre, la legge ha introdotto anche sanzioni molto severe per le organizzazioni che violano le norme sulla protezione dei dati personali, tra cui multe fino a 10 milioni di euro o il 2% del fatturato annuo globale dell'organizzazione, a seconda di quale importo sia più

[162] "Relazione sulla politica dell'informazione per la sicurezza -2010", febbraio 2011, Sistema di informazione per la sicurezza della Repubblica.
[163] Sito: Sistema di informazione per la sicurezza della Repubblica a protezione degli interessi politici, militari, economici, scientifici e industriali del paese.
[164] Il GDPR (General Data Protection Regulation) è il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea, entrato in vigore il 25 maggio 2018, che stabilisce le norme per la protezione dei dati personali degli individui all'interno dell'UE.

elevato[165]. La legge n. 133/2012 ha rappresentato un importante passo avanti per la protezione dei dati personali in Italia, introducendo nuove regole e sanzioni per le organizzazioni che gestiscono dati personali e garantendo un maggior livello di tutela per gli interessati. Inoltre, la legge ha contribuito a migliorare la conformità delle organizzazioni alle norme europee sulla protezione dei dati personali, aumentando la sicurezza informatica a livello nazionale. Nel 2013 l'Italia pubblica in gazzetta il *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico* (QSN)[166]: una strategia nazionale italiana per la sicurezza informatica, adottata dal governo italiano nel 2013. Il QSN ha come obiettivo principale quello di migliorare la sicurezza informatica del paese, contrastando le minacce informatiche e proteggendo le infrastrutture critiche del paese[167]. La strategia prevede un approccio integrato alla sicurezza informatica, che coinvolge tutti gli attori del sistema di sicurezza nazionale, tra cui le forze armate, le forze dell'ordine, le agenzie di intelligence e le organizzazioni pubbliche e private. Il QSN prevede anche l'istituzione di un *Centro di Competenza Nazionale per la Cybersecurity* (CCNC)[168], che ha il compito di coordinare gli sforzi di cyber difesa del paese, promuovere la ricerca e lo sviluppo nel campo della sicurezza informatica e fornire supporto tecnico alle organizzazioni pubbliche e private.

Inoltre, il QSN prevede anche l'adozione di misure per migliorare la sicurezza informatica delle infrastrutture critiche del paese, tra cui la definizione di standard di sicurezza, l'implementazione di misure di sicurezza adeguate e la formazione del personale[169].

Il QSN rappresenta un importante strumento per migliorare la sicurezza informatica in Italia, fornendo una strategia integrata per la cyber difesa e una serie di misure per proteggere le infrastrutture critiche del paese. La strategia ha contribuito a migliorare la capacità del paese di prevenire e contrastare le minacce informatiche e a proteggere la sicurezza nazionale. Successivamente, nel 2014, l'Italia sigla l'accordo di collaborazione tra il Dipartimento delle Informazioni per la Sicurezza (DIS) e il Consorzio Interuniversitario Nazionale per l'Informatica (CINI) che ha portato alla creazione del Cybersecurity National Lab, un laboratorio nazionale dedicato alla sicurezza informatica[170]. Il Cybersecurity National Lab ha come obiettivo quello di promuovere la ricerca e lo sviluppo nel campo della sicurezza informatica, creando un ambiente di collaborazione tra il mondo accademico, la ricerca e il

[165] Sito: Sistema di informazione per la sicurezza della Repubblica a protezione degli interessi politici, militari, economici, scientifici e industriali del paese.
[166] dei Ministri, P. D. C. (2013). Quadro strategico nazionale per la sicurezza dello spazio cibernetico.
[167] *Ibidem*
[168] *Ibidem*
[169] *Ibidem*
[170] Sapienza, C. I. S. (2017). Cybersecurity National Lab.

settore pubblico e privato[171]. Il laboratorio si concentra sulla ricerca e lo sviluppo di tecnologie avanzate per la cyber difesa, la formazione di esperti in sicurezza informatica e la creazione di soluzioni innovative per proteggere le infrastrutture critiche del paese.

Il Cybersecurity National Lab è stato istituito nel 2016 e rappresenta un importante passo avanti per la sicurezza informatica in Italia, fornendo un ambiente di collaborazione tra i principali attori del settore e promuovendo la ricerca e lo sviluppo di tecnologie avanzate per la cyber difesa. Inoltre, il laboratorio contribuisce a formare una nuova generazione di esperti in sicurezza informatica, aumentando la capacità del paese di prevenire e contrastare le minacce informatiche e proteggere la sicurezza nazionale. Sempre nel 2014 viene introdotta la legge italiana sulla sicurezza nazionale (legge 124/2014)[172] che definisce le misure di sicurezza da adottare per proteggere le infrastrutture critiche, come le reti energetiche, le infrastrutture di trasporto e le reti di telecomunicazione, da possibili attacchi informatici. La legge prevede la creazione di un Comitato Interministeriale per la Sicurezza della Repubblica (CISR)[173], che ha il compito di coordinare le attività di sicurezza nazionale e di elaborare le linee guida per proteggere le infrastrutture critiche. Essa prevede anche la creazione di un Centro di Controllo della Sicurezza delle Reti (CCSR)[174], che ha il compito di monitorare costantemente le reti di telecomunicazione e di coordinare la risposta agli attacchi informatici. Il CCSR è in grado di rilevare eventuali attacchi informatici e di coordinare la risposta delle autorità competenti per garantire la sicurezza delle reti di telecomunicazione. Il governo italiano ha adottato anche una serie di direttive e linee guida per proteggere le infrastrutture critiche da possibili attacchi informatici. Successivamente viene scritto il Libro Bianco per la sicurezza internazionale e la difesa: un documento ufficiale pubblicato dal governo italiano nel luglio 2015, che rappresenta una guida strategica per la politica di sicurezza e difesa del paese[175]. Il libro bianco individua le principali sfide per la sicurezza internazionale e la difesa e definisce gli obiettivi strategici per affrontare queste sfide. Tra le principali sfide identificate vi sono il terrorismo internazionale, la proliferazione delle armi di distruzione di massa, il cambiamento climatico, la crisi migratoria e la cyber security.

Il libro bianco si concentra in particolare sulle questioni della sicurezza informatica, riconoscendo la crescente importanza della protezione delle infrastrutture critiche del paese e

[171] *Ibidem*
[172] Di Mascio, F., & Natalini, A. (2021). L'agenda di riforma del lavoro pubblico nell'era digitale.
[173] *Ibidem*
[174] *Ibidem*
[175] Italia, I. M. D. D. (2014). Libro Bianco, per La Sicurezza Internazionale e la Difesa.

la necessità di sviluppare una capacità di cyber difesa adeguate[176]. Il libro bianco per la sicurezza internazionale e la difesa rappresenta un importante strumento per la politica di sicurezza e difesa del paese, fornendo una guida strategica per affrontare le principali sfide alla sicurezza internazionale. In particolare, il libro bianco ha contribuito a riconoscere l'importanza della sicurezza informatica per la sicurezza nazionale e ha fornito una base per lo sviluppo di politiche e strategie di cyber difesa adeguate. Nel 2018, Il Decreto Legislativo n. 182 prevede la creazione di un registro delle infrastrutture critiche, che comprende le infrastrutture di trasporto, le reti energetiche, le reti di telecomunicazione e le infrastrutture finanziarie[177]. Il registro è gestito dal Ministero dell'Interno e contiene le informazioni necessarie per identificare le infrastrutture critiche del paese. Inoltre, il Ministero dello Sviluppo Economico ha adottato una serie di linee guida per la sicurezza informatica delle infrastrutture critiche. Le linee guida prevedono l'adozione di misure di sicurezza informatica adeguate, come la crittografia dei dati, l'autenticazione forte e il monitoraggio costante dei sistemi informatici. Il governo italiano ha anche creato il Centro Nazionale per la Protezione
delle Infrastrutture Critiche (CNPIC)[178], che ha il compito di coordinare le attività di protezione delle infrastrutture critiche e di garantire la sicurezza nazionale. Il CNPIC è responsabile della gestione del registro delle infrastrutture critiche e si occupa di coordinare la risposta agli attacchi informatici[179]. Inoltre, il governo italiano ha adottato una serie di misure per contrastare le minacce informatiche provenienti dall'estero. Viene così delineata la nuova architettura nazionale cyber[180], riassumibile in Figura 2.

[176] Italia, I. M. D. D. (2014). Libro Bianco, per La Sicurezza Internazionale e la Difesa. Linee Guida.
[177] Rapporto Clusit 2018 sulla sicurezza ICT in Italia
[178] Vulpiani, D. (2007). La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto. Rivista di Criminologia, Vittimologia e Sicurezza, 1, 46-54.
[179] *Ibidem*
[180] "Documento di sicurezza nazionale", allegato alla "Relazione sulla politica dell'informazione per la sicurezza - 2017", febbraio 2018, Sistema di informazione per la sicurezza della Repubblica, documento consultabile all'indirizzo: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf (25/06/2018), p. 8.

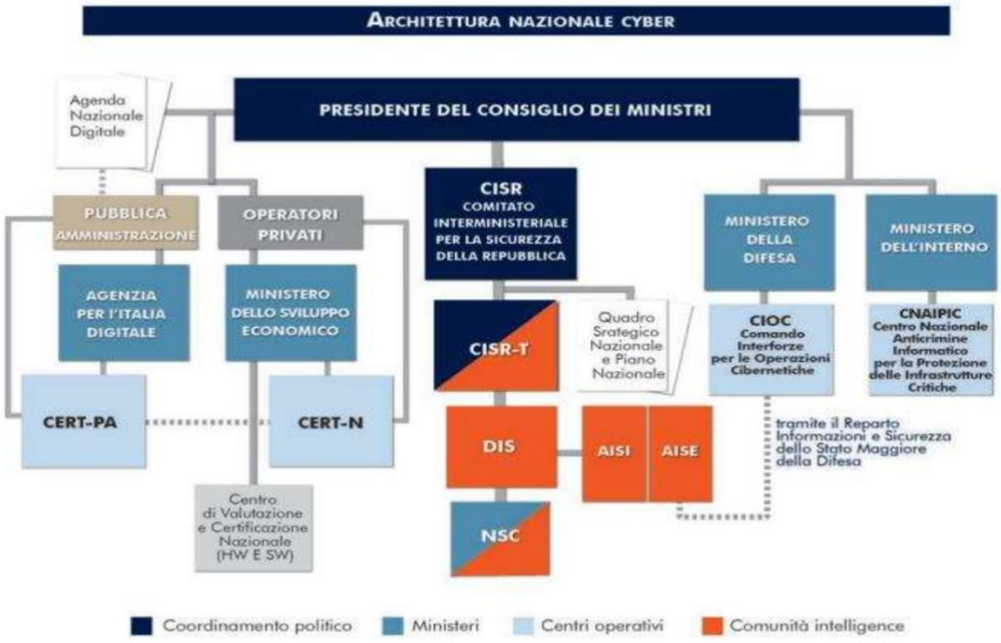

Figura 2 – Architettura nazionale cyber con il Decreto Gentiloni

3.3.1 Generali Italia Spa: copertura in caso di "eventi cyber"

Generalmente, le compagnie assicurative offrono una copertura contro gli eventi cyber, ovvero le minacce informatiche come gli attacchi informatici, le violazioni dei dati, la frode informatica e altri tipi di incidenti informatici. Generali Italia Spa ha recentemente lanciato un nuovo prodotto di assicurazione per la copertura in caso di eventi cyber[181].

Il prodotto, chiamato "Generali Cyber Insurance", è stato progettato per proteggere le aziende contro le conseguenze finanziarie e legali degli eventi cyber. La polizza offre una copertura completa che include la responsabilità civile per danni a terzi, la protezione dei dati personali e aziendali, la copertura delle spese legali e la copertura dei costi di ripristino delle attività aziendali[182]. Quest'azione è importante da considerare perché è un chiaro segno di un aumento della consapevolezza sulla sicurezza informatica che risulta essere una delle variabili prese in considerazione.

La polizza di Generali Cyber Insurance è personalizzabile in base alle esigenze specifiche dell'azienda assicurata. Ad esempio, l'azienda può scegliere il livello di copertura per la

[181] Favarato, A. (2018). Il fenomeno del cyber attack: Un'analisi econometrica.
[182] *Ibidem*

responsabilità civile, i limiti di indennizzo per la copertura dei costi di ripristino delle attività aziendali e la durata della polizza[183].

Inoltre, Generali Italia Spa offre anche servizi di consulenza e supporto per aiutare le aziende a prevenire gli eventi cyber. Questi servizi includono l'analisi dei rischi di sicurezza informatica, la valutazione della conformità normativa e l'implementazione di misure di sicurezza informatica adeguate. In sintesi, il nuovo prodotto di Generali Italia Spa per la copertura in caso di eventi cyber offre alle aziende una copertura completa contro le conseguenze finanziarie e legali degli eventi cyber, personalizzata in base alle esigenze specifiche dell'azienda. Inoltre, la compagnia offre anche servizi di consulenza e supporto per aiutare le aziende a prevenire gli eventi cyber. L'offerta di una copertura assicurativa per eventi cyber è un segnale della crescente consapevolezza sulla sicurezza informatica tra le aziende. Infatti, sempre più aziende stanno riconoscendo l'importanza della protezione dei propri dati e della sicurezza delle informazioni, e stanno cercando di proteggersi da potenziali rischi.

3.4 UE e NATO

Il concetto di cyber sicurezza si è evoluto nel tempo, passando da una visione limitata che considerava la sicurezza informatica come una questione di protezione contro le minacce informatiche, a una visione più ampia che comprende la protezione dei dati personali, la sicurezza delle infrastrutture critiche e la tutela della privacy. L'Unione Europea ha svolto un ruolo centrale nello sviluppo del concetto di cyber sicurezza, attraverso l'adozione di diverse iniziative e politiche. Nel 2013, la Commissione europea ha presentato la Strategia europea per la sicurezza cibernetica, che ha stabilito un quadro di riferimento per la promozione della sicurezza informatica a livello europeo. La Strategia europea per la sicurezza cibernetica del 2013 ha definito una serie di obiettivi e azioni per promuovere la sicurezza informatica a livello europeo, che possono essere considerati come variabili rilevanti per la domanda di ricerca sulla evoluzione del concetto di cyber sicurezza. Alcune di queste variabili includono:

- la collaborazione e cooperazione: la Strategia ha sottolineato l'importanza della collaborazione e della cooperazione tra gli Stati membri dell'UE, le istituzioni europee, il settore privato e la società civile per affrontare le minacce cibernetiche.

[183] Favarato, A. (2018). Il fenomeno del cyber attack: Un’analisi econometrica.

- Prevenzione: la Strategia ha riconosciuto l'importanza della prevenzione delle minacce cibernetiche attraverso la promozione delle migliori pratiche e la sensibilizzazione dei cittadini e delle aziende sulla sicurezza informatica.
- Protezione: la Strategia ha stabilito l'importanza della protezione delle infrastrutture critiche, dei dati personali e della proprietà intellettuale contro le minacce cibernetiche.
- Reazione: la Strategia ha sottolineato l'importanza di una rapida e coordinata reazione alle minacce cibernetiche, attraverso l'implementazione di piani di emergenza e la cooperazione tra gli Stati membri dell'UE.
- Capacità: la Strategia ha riconosciuto la necessità di sviluppare le capacità e le competenze necessarie per affrontare le minacce cibernetiche, attraverso l'istruzione, la formazione e la ricerca.

Inoltre, l'UE ha istituito l'Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'Informazione (ENISA)[184], che si occupa di promuovere la sicurezza informatica nell'UE attraverso la condivisione di informazioni e la promozione delle migliori pratiche. La creazione dell'ENISA è una delle numerose iniziative che l'UE ha intrapreso per rafforzare la cybersicurezza all'interno dell'UE. L'Agenzia ha una serie di iniziative per promuovere la cybersicurezza, tra cui la pubblicazione di orientamenti, la raccolta e l'analisi di informazioni sulle minacce informatiche, la promozione delle migliori pratiche in materia di cybersicurezza e la cooperazione con le autorità competenti per affrontare le minacce informatiche transfrontaliere.[185] L'ENISA è una risorsa importante per gli Stati membri dell'UE, in particolare quelli con capacità e risorse limitate per far fronte alle minacce informatiche. Inoltre, l'ENISA svolge un ruolo importante nel coordinamento delle attività di cybersicurezza tra gli Stati membri dell'UE e nella promozione della cooperazione tra le parti coinvolte. In sintesi, l'ENISA contribuisce ad aumentare la consapevolezza e la capacità di rispondere alle minacce informatiche negli Stati membri dell'UE. Anche la NATO ha adottato diverse normative e disposizioni in materia di sicurezza cibernetica, al fine di proteggere le infrastrutture cibernetiche dell'Organizzazione e dei suoi membri. La NATO ha riconosciuto che la sicurezza cibernetica è un elemento importante per la sicurezza collettiva e che gli attacchi informatici possono rappresentare una minaccia per la stabilità e la sicurezza internazionale.

[184] Cencetti, C. (2014). Cybersecurity: Unione europea e Italia: Prospettive a confronto (Vol. 12). Edizioni Nuova Cultura.
[185] *Ibidem*

Viene istituito il Centro di Eccellenza per la Difesa Cibernetica (CCDCOE), che ha lo scopo di promuovere la cooperazione internazionale nella difesa cibernetica e di sviluppare soluzioni tecnologiche avanzate per la sicurezza cibernetica[186]. Il Centro di Eccellenza per la Difesa Cibernetica rappresenta un'importante iniziativa per la promozione della sicurezza cibernetica, in linea con l'evoluzione del concetto di cyber security. L'istituzione del CCDCOE si basa sull'idea che la sicurezza cibernetica rappresenti una minaccia alla sicurezza nazionale e internazionale, e che la collaborazione internazionale sia essenziale per affrontare le minacce cibernetiche.[187] Inoltre, la NATO ha adottato diverse politiche e linee guida in materia di sicurezza cibernetica, tra cui la Strategia della NATO per la Sicurezza Cibernetica del 2011[188] e il Piano d'Azione per la Difesa Cibernetica del 2014[189]. Entrambe rappresentano importanti iniziative per la promozione della sicurezza cibernetica nel contesto della NATO. Questi documenti sottolineano l'importanza della protezione delle infrastrutture critiche e delle informazioni sensibili contro le minacce cibernetiche e promuovono la cooperazione internazionale per la gestione delle minacce cibernetiche transfrontaliere

In Italia, la NATO collabora con le autorità italiane per la sicurezza cibernetica, come il Centro Nazionale per la Cyber Security (NCSC) e il Dipartimento delle Informazioni per la Sicurezza (DIS). Inoltre, partecipa alle attività della NATO in materia di sicurezza cibernetica e ha adottato normative e leggi per la protezione delle infrastrutture cibernetiche e la prevenzione degli attacchi informatici.

3.5 La direttiva N.I.S

Un importante passo nell'evoluzione della sicurezza cibernetica a livello Europeo è *La Direttiva sulla sicurezza delle reti e dei sistemi informativi* (NIS - Direttiva (UE) 2016/1148)[190]: una normativa europea che mira a proteggere le infrastrutture critiche contro le minacce informatiche e migliorare la sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea. La direttiva è stata adottata nel 2016 e gli Stati membri dovevano recepirla nella propria legislazione nazionale entro il 9 maggio 2018[191]. *La Direttiva N.I.S* si applica a

[186] Pizzuti, F. (2021). La sicurezza informatica nell'ambito del mercato unico digitale: uno strumento di crescita economica
[187] *Ibidem*
[188] Germani, L. S., & Gori, U. (2011). Information warfare: le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana.
[189] dei Ministri, P. D. C. (2013). Piano nazionale per la protezione cibernetica e la sicurezza informatica
[190] Ripiego, M. (2021). La gestione della sicurezza informatica negli enti di cui alla Direttiva NIS e al Perimetro di sicurezza nazionale cibernetica.
[191] *Ibidem*

un'ampia gamma di *operatori di servizi essenziali* (OSE) e *fornitori di servizi digitali* (DSP) in tutta l'Unione Europea[192]. Gli OSE includono organizzazioni nei settori dell'energia, dei trasporti, della sanità, delle infrastrutture bancarie e finanziarie e dei servizi digitali essenziali, come motori di ricerca, cloud computing e mercati online[193]. I DSP includono provider di servizi di hosting, servizi di condivisione di file e servizi di e-commerce. La Direttiva NIS prevede l'obbligo per gli Stati membri di identificare gli OSE e i DSP e di garantire che essi adottino misure di sicurezza adeguate a proteggere i loro sistemi contro le minacce informatiche[194]. Gli operatori di servizi essenziali e i fornitori di servizi digitali devono adottare misure di sicurezza appropriate per garantire la sicurezza dei loro sistemi e delle loro reti e per prevenire le interruzioni dei servizi. Tali misure di sicurezza includono la gestione degli incidenti di sicurezza dell'informazione, la valutazione dei rischi di sicurezza dell'informazione e l'adozione di misure tecniche e organizzative adeguate a garantire la sicurezza dei sistemi e delle reti. Inoltre, la Direttiva NIS prevede l'obbligo per gli Stati membri di creare un quadro di cooperazione tra le autorità nazionali di sicurezza informatica e le autorità di regolamentazione dei settori interessati per garantire la sicurezza delle infrastrutture critiche[195]. Gli Stati membri sono tenuti a istituire un punto di contatto nazionale per la sicurezza informatica per facilitare la cooperazione tra le autorità competenti e gli operatori di servizi essenziali e i fornitori di servizi digitali.

L'obbligo principale per gli operatori di servizi essenziali è quello di notificare alle autorità competenti gli incidenti di sicurezza dell'informazione significativi che si verificano nei loro sistemi e reti[196]. Le autorità nazionali di sicurezza informatica devono garantire che queste notifiche siano gestite in modo adeguato e che siano prese le misure appropriate per prevenire il ripetersi di incidenti di sicurezza dell'informazione simili. La Direttiva NIS prevede anche la cooperazione tra gli Stati membri dell'Unione Europea per garantire la sicurezza delle infrastrutture critiche a livello europeo[197]. Gli Stati membri devono collaborare per scambiarsi informazioni sulla sicurezza delle reti e dei sistemi informativi, per coordinare le misure di sicurezza a livello internazionale e per elaborare una strategia di sicurezza informatica comune.

[192] *Ibidem*
[193] *Ibidem*
[194] Calzetta G., "La cyber sicurezza alla prova della direttiva Nis: gli obblighi e i soggetti coinvolti", Il Sole 24 ore, 22 giugno 2018
[195] *Ibidem*
[196] *Ibidem*
[197] *Ibidem*

In sintesi, la Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS) è una normativa europea che mira a proteggere le infrastrutture critiche contro le minacce informatiche e migliorare la sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea. La Direttiva si applica a un'ampia gamma di operatori di servizi essenziali e fornitori di servizi digitali e prevede l'obbligo per gli Stati membri di identificare gli OSE e i DSP e di garantire che essi adottino misure di sicurezza adeguate a proteggere i loro sistemi contro le minacce informatiche. La Direttiva NIS prevede inoltre la cooperazione tra le autorità nazionali di sicurezza informatica e tra gli Stati membri dell'Unione Europea per garantire la sicurezza delle infrastrutture critiche a livello europeo. OSE e DSP sono tenuti a notificare alle autorità competenti gli incidenti di sicurezza dell'informazione significativi che si verificano nei loro sistemi e reti, e le autorità nazionali di sicurezza informatica devono garantire che queste notifiche siano gestite in modo adeguato.

La Direttiva NIS rappresenta un importante passo avanti nella protezione delle infrastrutture critiche contro le minacce informatiche e nella promozione della sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea. Inoltre, ha lo scopo di garantire che gli operatori di servizi essenziali e i fornitori di servizi digitali adottino misure di sicurezza adeguate a proteggere i loro sistemi e reti contro le minacce informatiche, e di promuovere la cooperazione tra le autorità competenti e gli operatori di servizi essenziali e fornitori di servizi digitali. Infine, la direttiva rappresenta un esempio di come la sicurezza cibernetica stia diventando sempre più importante a livello globale, con la necessità di garantire la sicurezza delle reti e dei sistemi informativi per evitare danni economici e sociali.

CONCLUSIONI

La sicurezza cibernetica rappresenta una sfida sempre più importante per le organizzazioni, le istituzioni e i cittadini di tutto il mondo. L'evoluzione delle tecnologie digitali e l'espansione delle reti di comunicazione hanno portato ad un aumento delle minacce cibernetiche, rendendo necessaria una maggiore attenzione alla sicurezza informatica. Questo ha portato alla creazione di un nuovo spazio di conflitto, il Cyber Spazio, che rappresenta una nuova frontiera per le grandi potenze mondiali. Il Cyber Spazio è diventato un terreno di scontro per gli stati e gli attori non statali che cercano di ottenere vantaggi strategici attraverso il cyber warfare. Questo ha spinto le grandi potenze a dedicare sempre più risorse alla protezione delle loro infrastrutture critiche e alla promozione della sicurezza cibernetica a livello globale. Il concetto di sicurezza cibernetica si basa sull'analisi del rischio e sull'adozione di misure di protezione adeguate. L'intelligenza artificiale rappresenta una potente alleata nella lotta contro le minacce cibernetiche, ma la resilienza è un altro elemento chiave della sicurezza cibernetica. La resilienza permette di continuare a svolgere le attività anche in caso di attacco cibernetico, minimizzando l'impatto e ripristinando rapidamente la situazione.

Questa tesi ha voluto analizzare l'evoluzione del concetto di sicurezza cibernetica che è stata influenzata da diverse variabili indipendenti, tra cui l'avanzamento delle tecnologie digitali, la crescente dipendenza dalle tecnologie digitali, l'adozione di normative a livello europeo e nazionale, la collaborazione internazionale e la consapevolezza pubblica sui rischi legati alla sicurezza informatica. L'avanzamento delle tecnologie digitali e l'espansione delle reti di comunicazione hanno portato ad un aumento delle minacce cibernetiche, rendendo necessaria una maggiore attenzione alla sicurezza informatica. La crescente dipendenza dalle tecnologie digitali ha reso la sicurezza informatica una priorità per la tutela dei dati personali e delle infrastrutture critiche. L'adozione di normative a livello europeo e nazionale, come nel caso dell'Italia, ha contribuito a promuovere la sicurezza informatica attraverso la definizione di standard e misure di sicurezza. Inoltre, la collaborazione internazionale ha giocato un ruolo importante nella promozione della sicurezza cibernetica a livello globale, attraverso la condivisione di conoscenze e la definizione di standard comuni. Infine, la consapevolezza pubblica sui rischi legati alla sicurezza informatica ha portato a una maggiore attenzione e impegno nella promozione della sicurezza cibernetica. È possibile sostenere che il concetto di cybersicurezza è notevolmente cambiato negli anni a causa dell'evoluzione delle tecnologie digitali e della crescente dipendenza da esse. Come dimostrato nella tesi, il cyber spazio è

diventato sempre più importante per le potenze globali che vi vedono un nuovo dominio strategico da sfruttare e proteggere. Tuttavia, ciò ha portato allo sviluppo di capacità cyber offensive e all'aumento degli attacchi informatici sofisticati. Le ipotesi riguardanti l'evoluzione del concetto di sicurezza cibernetica, come l'idea che la crescente diffusione delle tecnologie digitali e l'espansione delle reti di comunicazione abbiano portato ad un aumento delle minacce cibernetiche e della necessità di protezione delle infrastrutture critiche e dei dati personali, possono essere verificate anche attraverso il caso italiano. In Italia, la sicurezza cibernetica è diventata una priorità nazionale e il governo ha adottato misure per promuovere la sicurezza informatica, come il piano nazionale per la protezione cibernetica e la sicurezza informatica e la copertura assicurativa in caso di "eventi cyber". Inoltre, la direttiva N.I.S rappresenta un ulteriore passo avanti nella promozione della sicurezza cibernetica a livello europeo. Gli attacchi cyber hanno già avuto un impatto significativo sulle imprese e la pubblica amministrazione, evidenziando l'urgenza di rafforzare la sicurezza cibernetica e la resilienza. La collaborazione con l'UE e la NATO e l'uso di tecnologie come l'IA stanno contribuendo a fare progressi sul fronte della cybersicurezza. Tuttavia, la sfida rimane enorme data l'evoluzione costante delle minacce cyber. Si può quindi affermare che il concetto di cybersicurezza si è evoluto in parallelo con la rapida digitalizzazione della società e delle economie, diventando una priorità assoluta per proteggere dati, infrastrutture critiche e interessi di sicurezza nazionale. Pertanto, garantire un ambiente cyber resiliente e sicuro richiederà sforzi coordinati a livello globale e investimenti continui. Le ipotesi riguardanti l'evoluzione del concetto di sicurezza cibernetica comprendono l'idea che la crescente diffusione delle tecnologie digitali e l'espansione delle reti di comunicazione abbiano portato ad un aumento delle minacce cibernetiche e della necessità di protezione delle infrastrutture critiche e dei dati personali. Questa ipotesi è supportata dall'evoluzione del contesto tecnologico e dalle continue sfide che si presentano nella protezione della sicurezza informatica. In definitiva, l'evoluzione del concetto di sicurezza cibernetica è stata un processo complesso che ha coinvolto variabili interdipendenti come l'evoluzione delle tecnologie digitali, l'espansione delle reti di comunicazione, la crescente dipendenza dalle tecnologie digitali, l'adozione di normative a livello Europeo e a livello nazionale, la collaborazione internazionale e la consapevolezza pubblica sui rischi legati alla sicurezza informatica. Questi fattori hanno contribuito a promuovere la sicurezza informatica a livello globale e a proteggere le infrastrutture critiche e i dati personali. Il caso italiano conferma l'importanza dell'evoluzione del concetto di sicurezza cibernetica e la necessità di adottare misure sempre più efficaci per proteggere le infrastrutture critiche e i dati personali, in un contesto di continua evoluzione del Cyber Spazio. La

promozione della sicurezza cibernetica richiede un impegno costante e collaborativo da parte di tutti gli attori coinvolti, dal settore pubblico al settore privato, a livello nazionale e internazionale.

BIBLIOGRAFIA

Andrea Giuntini, A. (2011). *La crisi economica fra interpretazione, narrazione e retorica. Storici a confronto. Memoria e Ricerca*.

Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is coming! Santa Monica, CA: RAND Corporation. Tradotto.*

Baldoni, R., & De Nicola, R. (2015). *Il futuro della Cybersecurity in Italia. CINI-Consorzio Interuniversitario Nazionale Informatica.*

Baldoni R., Montanari L.,(2011) *"Italian Security Report. Un framework nazionale per la Cyber Security", Cyber Intelligence and Information Security Center, Sapienza, Università di Roma.*

Barlow's, J. P. (1996). *Declaration of independence for cyberspace.*

Boot, A. W., & Thakor, A. V. (1993). *Security design. The Journal of Finance*.

Borriello, G., & Fristachi, G. (2022). *Stato (d'assedio) digitale e strategia italiana di cybersicurezza.*

Calzetta G., (2018) *"La cyber sicurezza alla prova della direttiva Nis: gli obblighi e i soggetti coinvolti", Il Sole 24 ore.*

Camilli, E. (2014). *Sicurezza nazionale: tra concetto e strategia*.

Chiaruzzi, M. (2010) *Geopolitica e Geostrategia.*

Clarke, R. A., & Knake, R. K. (2014). *Cyber war. Old Saybrook: Tantor Media, Incorporated.*

Colombo, A. (2006*). La guerra ineguale: pace e violenza nel tramonto della società internazionale. Il mulino.*

"Documento di sicurezza nazionale", *allegato alla "Relazione sulla politica dell'informazione per la sicurezza 2017", febbraio 2018, Sistema di informazione per la sicurezza della Repubblica*

"Datagate": *scandalo scoppiato nel 2013 in seguito alla diffusione di documenti riservati sulle attività di spionaggio di massa condotte dall'NSA. Per approfondire: http://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio..*

De Luca, S. (2022*). Democrazia e rivoluzione digitale. Storia del pensiero politico.*

Denning, D. E. (2013). *Framework and Principles for Active Cyber Defense. Computers & security.*

Denning, P. J., & Denning, D. E. (2010). *Discussing cyber attack. Communications of the ACM.*

Di Mascio, F., & Natalini, A. (2021). *L'agenda di riforma del lavoro pubblico nell'era digitale.*

ENISA. (2016). *German National Cyber Security Strategy.*

ENISA. (2012). *National Cyber Security Strategies: setting the course for national efforts to strengthen security in cyberspace.*

Favarato, A. (2018). *Il fenomeno del cyber attack: Una analisi econometrica.*

Farina, G. (2017). *Il cyber space: una nuova dimensione per la conflittualità e la tutela dei diritti umani.*

Germani, L. S., & Gori, U. (2011). *Information warfare: le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana.*

Ghernouti-Hélie, S. (2010). *A national strategy for an effective cybersecurity approach and culture.*

Giovanni Campanale (2020). *Dal concetto di cyber attack al cyberwarfare: l'uso della forza in ambito cyber. Articolo pubblicato su "Cybersecurity360".*

Gibson W. (1984) *Neuromancer, Ace Pub., New York.*

Grauman b. (2012) *Cyber-security: the vexed question of global rules, Security and DefenseAgenda publications, Bruxelles.*

Gori, U., & Lisi, S. (2015). *Cyber Warfare, Armi cibernetiche, sicurezza nazionale e difesa del business.*

Italia, I. M. D. D. (2014). *Libro Bianco, per La Sicurezza Internazionale e la Difesa. Linee Guida.*

Italian Cybersecurity Report: *Controlli Essenziali di Cybersecurity.*

Juvara, R. (2013) *Infrastrutture critiche, il centro dell'attenzione. Sandro Bologna, ex Presidente dell'Associazione Italiana Infrastrutture Critiche* .

J. S. Nye, (2011) *The Future of Power, PublicAffairs, New York.*

La Rocca, (2015). *La Cyberpolitica nelle Relazioni Internazionali.*

Lisi, S., & Gori, U. (2015). *Cyber Warfare 2014: armi cibernetiche, sicurezza nazionale e difesa del business.*

Marrani, D. (2021). *Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia*.

Messa, P. (2018). *L'era dello sharp power: la guerra (cyber) al potere. EGEA spa.*

National Security Council (U.S.), & United States. *Executive Office of the President. (2018). National Cyber Strategy of the United States of America. [Washington, D.C*

National Security Council (U.S.), & United States. *Executive Office of the President. (2011). International strategy for cyberspace: Prosperity, security, and openness in a networked world. [Washington, D.C*

Pizzuti, F. (2021). *La sicurezza informatica nell'ambito del mercato unico digitale: uno strumento di crescita economica*

Pili, G. (2015) *Cyber security e cyber guerra.*

Rapporto Clusit (2018): *sulla sicurezza ICT in Italia*

Rapaccini, (2017*). Cyberwarfare: definizioni, casi di studio e analisi*

Rassega, V. (2017). *Cyber security risk management nei servizi pubblici strategici*.

Razzante, R. (2023). *L'attribuzione degli attacchi informatici*

Ripiego, M. (2021). *La gestione della sicurezza informatica negli enti di cui alla Direttiva NIS e al Perimetro di sicurezza nazionale cibernetica.*

Romoli, A. L. (2023). *Analisi del settore economico della cybersecurity*.

Sapienza, C. I. S. (2017). *Cybersecurity National Lab*.

Sistema di informazione: *per la sicurezza della Repubblica a protezione degli interessi politici, militari, economici, scientifici e industriali del paese dei Ministri, P. D. C. (2013). Quadro strategico nazionale per la sicurezza dello spazio cibernetico.*

Shreier, F. (2010) *On Cyber Warfare, DCAF Publication, Geneva, Tradotto*.

Stizza, M. (2020). *Cybersecurity: La Gestione Del Rischio Aziendale Nell'era Digitale.*

S. Mele, *"Cyber-Weapons: aspetti giuridici e strategici"*

S. Mele, *"Cyberwarfare e danni ai cittadini"*

Schmitt, M. N. (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press*.

Treccani. (2020). *DDoS. Enciclopedie on line, Istituto della Enciclopedia Italiana*.

Treccani. (2020). *Readiness. Enciclopedie on line, Istituto della Enciclopedia Italiana.*

Treccani. (2020). *Cyber Spionaggio. Enciclopedie on line, Istituto della Enciclopedia Italiana.*

Treccani. (2020). *Cibernetica. Enciclopedie on line, Istituto della Enciclopedia Italiana*.

Treccani. (2020). *Cyber Spazio. Enciclopedie on line, Istituto della Enciclopedia Italiana.*

United Nations CISA. (2003). *National Strategy to Secure Cyberspace. Consultato da https://www.cisa.gov/national-strategy-secure-cyberspace*

Vulpiani, D. (2007). *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto. Rivista di Criminologia, Vittimologia e Sicurezza.*

Wortham, A. (2012). *Should cyber exploitation ever constitute demonstration of hostile intent that may violate un charter provisions prohibiting the threat or use of force. Federal Communications Law Journal*,

Xiangsui, Q. L. W. (2001). Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione.

Zanfini (2021). *Il ruolo emergente delle organizzazioni internazionale nella tutela del Cyberspace.*

RINGRAZIAMENTI

Alla fine di questo viaggio, vorrei rivolgere alcuni ringraziamenti,

Al mio Relatore,

Desidero esprimere la mia profonda gratitudine al Professor Raffaele Marchetti. La Sua vasta esperienza e i Suoi utili spunti di riflessione mi hanno permesso di affrontare le sfide poste dal progetto con maggiore consapevolezza e di risolvere i dubbi che inesorabilmente sorgevano nel mio percorso. La ringrazio quindi per la gentile disponibilità, la competenza e la passione che ha dimostrato. La ringrazio infine per avermi trasmesso, attraverso le Sue lezioni e i Suoi scritti, una solida base di conoscenze in materia di relazioni internazionali e geopolitica, che mi sarà utile nel mio futuro percorso accademico e professionale.

Ai miei genitori,

avete creduto in me ancor prima che io credessi in me stessa e mi avete spinto ad andare oltre i miei limiti per raggiungere i miei obiettivi. Mi avete insegnato il valore dell'impegno, della determinazione e della perseveranza. A Mamma Paola, sei stata il mio primo esempio di forza, intelligenza e compassione. Sei stata al mio fianco in ogni momento, pronta ad ascoltare, consolare e consigliare. A Papà Luigi, mi hai trasmesso la passione per la conoscenza e l'amore per lo studio e il sacrificio. S*enza di te, non avrei mai avuto la forza di affrontare le sfide che ho incontrato lungo il percorso. Tutto quello che sono oggi lo devo anche a te. Grazie infinitamente per avermi insegnato a non accontentarmi mai e a lottare per i miei sogni. Vi dedico questo traguardo con tutto il mio amore.*

A mia sorella maggiore Alexandra,

Questa tesi è anche il frutto della tua presenza costante nella mia vita, del tuo sostegno e della tua preziosa guida. Grazie per avermi spronato a non mollare mai e per avermi dato l'energia necessaria per superare ogni ostacolo. Anche se non sempre lo dimostro a sufficienza, tu sei stata e sarai sempre fonte d'ispirazione per me. Questo traguardo lo dedico a te, con amore e gratitudine.

Ai miei amici di sempre,

Eleonora, Davide e Marco. Grazie per essere stati al mio fianco durante tutto il percorso di studi, per le chiacchiere, i pianti e le gioie che abbiamo condiviso insieme. Grazie per le parole di incoraggiamento nei momenti difficili e per avermi fatto ridere nei momenti in cui avrei voluto piangere. Grazie per avermi regalato dei momenti di pura spensieratezza e felicità. Insieme siete la mia famiglia e pilastri fondamentali della mia vita.

Ad Alessandro,

Sei stato al mio fianco durante una parte importante del mio percorso di studi e di crescita personale. Mi hai visto prendere decisioni importanti, cambiare e maturare. Mi hai ascoltato con pazienza, consigliato con saggezza e sostenuto con amore. Il tuo supporto durante i momenti difficili e le tue parole di incoraggiamento nelle mie insicurezze mi hanno dato la forza di perseverare nei miei studi e dare il meglio di me. Questo traguardo accademico è in parte anche grazie a te, grazie alla serenità, le risate, le conversazioni profonde e l'amore che hai portato nella mia vita in questi anni. Grazie, per tutto quello che mi hai dato e insegnato.

A me stessa,

Sono fiera di essere arrivata fino in fondo a questo lungo percorso e di aver portato a termine la mia tesi. Vorrei ringraziare la mia determinazione, che mi ha spinto ad andare avanti anche quando sembrava impossibile. Vorrei ringraziare la mia perseveranza, che mi ha permesso di lavorare giorno dopo giorno su questo progetto. Vorrei ringraziare la mia tenacia, che mi ha aiutato a superare le incertezze e i periodi di sconforto. Vorrei ringraziare tutti gli sforzi, il tempo, l'impegno e il sacrificio che ho messo in questo lavoro. Vorrei ringraziare la mia energia, la mia creatività e la mia passione senza le quali non sarei arrivata fin qui. Ma soprattutto, vorrei ringraziare me stessa per averci creduto e per non essermi arresa alle difficoltà. Questo momento è frutto del mio duro lavoro e delle mie scelte. Ed è a me che dedico questa tesi, con orgoglio e soddisfazione.

ABSTRACT

THE FIFTH DIMENSION OF CONFLICT: THE EVOLUTION OF THE CONCEPT OF SECURITY AND THE CYBER SPACE

In our increasingly interconnected society, information security is one of the most significant challenges to national and international security. The cyberspace, or digital environment in which online activities take place, has become a new frontline of conflict between nations and non-state actors, and the protection of critical infrastructure has become a top priority for governments, public and private organizations, and individuals. The current thesis work focuses on cyber security and cyber space, analyzing the main issues of critical infrastructure protection, cyber attack prevention, and personal data privacy. This is a topic of great relevance and importance since cyber-attacks can cause major damage to national security and stability. Furthermore, understanding the risks and opportunities associated with information security is crucial for developing effective policies and strategies for preventing cyber assaults and protecting critical infrastructure.

Cybersecurity and cyberspace are becoming increasingly important topics in modern society. The spread of digital technologies and global interconnection have created new opportunities, but also new threats to national and international security. The protection of critical infrastructure, the prevention of cyber attacks, and the protection of personal data privacy have all become top priorities for governments, public and private organizations, and individuals. The current thesis project's goal is to examine how information security has evolved over the last few years and what the main factors that have influenced this change have been. The advancement of digital technologies and the expansion of communication networks, which have led to an increase in cyberattacks and require a greater focus on security information, are among the independent factors that have influenced the evolution of the concept of cybersecurity; the growing reliance on digital technologies which has made information security a top priority for protecting sensitive data and infrastructure; the adoption of European and national laws, as in the case of Italy; international cooperation and, last but not least, public awareness of the risks associated with information security, which has given it a greater focus and influence in the promotion of cybersecurity.

In general, the following independent variables have had an impact on the development of the concept of cyber security: the advancement of digital technologies, the growing dependence

on them, the adoption of norms, international cooperation, and public awareness. Keeping in mind how much information security has improved since the 1990s, the three chapters of this thesis will focus on various issues relating to cyberspace security and related topics.

The first chapter will provide an overview of the cyberspace while introducing the idea of a "new frontier of conflict" and examining the factors that are prompting major powers to get interested in the cyberspace. The chapter will start by defining the Cyber Space and explaining how it has become an integral part of our daily lives. Cyber Space refers to the interconnected network of devices, systems, and networks that make up the internet. It is a virtual space that exists in the digital world and is accessed through electronic devices such as computers, smartphones, and tablets. It is a vast and complex system that enables people to communicate, share information, conduct business, and access a wide range of services and resources. The chapter will also discuss the actors involved in cyber warfare, including nation-states, criminal organizations, and hacktivists. It will explain why nation-states are the most significant players and how they are developing their capabilities to defend themselves and carry out offensive operations. Furthermore, the chapter will discuss the different types of cyber activities, including cyber exploitation, cyber espionage, and cyber attack. It will explain what each of these activities entails and how they are carried out in the Cyber Space. Finally, the chapter will talk about the weapons of cyber warfare, i.e., cyber weapons. It will explain what cyber weapons are and how they are used to carry out attacks on targets, disrupt communications, steal sensitive information, or damage critical infrastructure.

Overall, the first chapter of the thesis will provide a comprehensive overview of the Cyber Space and its implications for national security and global stability. It will lay the foundation for the subsequent chapters that will delve deeper into specific aspects of cyber warfare.

After analyzing the more general variables, the concept of cyber security will be expanded upon to help understand the more specific variables, such as the increase in dependence on digital technologies.

Cybersecurity, a crucial facet of national security, will be the subject of the second chapter of the thesis. The fundamental idea of national security and how cyber security fits into it will be covered at the beginning of the chapter. It will detail how cyberattacks can seriously jeopardize national security and why cybersecurity is essential to safeguarding people, property, and interests. After that, the chapter will dig into risk analysis, a crucial step in cyber security. It will detail how risk analysis is used to find potential threats, weaknesses, and effects as well as how it's used to create plans to lessen these risks. As a result of the potentially serious repercussions of a cyberattack, it will also cover the significance of risk analysis in cyber

security. The chapter will include a discussion over artificial intelligence's (AI) role in cyber security. It will detail how AI may be applied to find potential weaknesses, evaluate vast volumes of data, and detect cyber threats. Additionally, it will stress the necessity for strong cyber security measures and any potential dangers related to cyber attackers using AI. The idea of resilience in cyber security will also be covered in this chapter. It will describe how resilience is a system or network's capacity to endure and bounce back from online attacks. It will go over the significance of resilience in cyber security because it enables businesses to lessen the effects of online attacks and carry on even in the face of ongoing dangers. The chapter will end with an examination of the current state of cyber security in Italy. It will detail how Italy has come to understand the value of cyber security and created a thorough plan to deal with the problems brought on by online threats. It will include discussions over the national framework regarding cyber security, the establishment of a cyber security agency, and the promotion of partnerships between the public and private sectors to boost cyber security resilience. Overall, the second chapter will offer a thorough analysis of cyber security, providing factors such as risk analysis, AI, resilience, and the condition of cyber security in Italy.

The third chapter of the thesis will focus on the Italian case in cyber security. The chapter will begin by going through the effects of cyberattacks on Italy, including any possible effects on the nation's infrastructure, economy, and security. The nexus between national security and cyber risks in Italy will then be covered in more detail in the chapter. It will describe how cyberthreats have grown to be a key national security problem and the measures taken by Italy to mitigate them, including the development of a national cyber security framework. The National Plan for Cyber Protection and Information Security in Italy will also be covered in this chapter. It will outline the plan's goals and major activities, such as the creation of a national cyber security strategy, a cyber security agency, and the encouragement of public-private collaborations. The chapter will also include a case study on Generali Italia Spa, an Italian insurance provider that offers coverage for cyber-related occurrences. It will detail how insurance firms can significantly improve Italy's cyber security resilience. The chapter will also go over the role that the European Union (EU) and NATO have in dealing with cyberthreats in Italy. It will detail how Italy collaborates with these groups to strengthen its cyber security resilience and encourage member state participation. The N.I.S. Directive, a European Union directive on network and information system security, will be discussed as the chapter's final topic. It will outline the directive's goals, important clauses, and the implications for Italy. The third chapter of the thesis will offer a thorough analysis of the Italian case in terms of cyber security, covering topics like the consequences of cyberattacks, the connection between

national security and cyberthreats, the National Plan for Cyber Protection and Information Security, the function of insurance companies, the EU and NATO, and the N.I.S. Directive. This thesis sought to analyze the development of the concept of cybersecurity as it has been influenced by several independent factors, including the advancement of digital technologies, the growing dependence on digital technologies, the adoption of national and European standards, international cooperation, and public awareness of the risks associated with cybersecurity. Advances in digital technology and the expansion of communication networks have led to an increase in cyberattacks, requiring a greater focus on information security. The growing reliance on digital technologies has made information security a top priority for protecting sensitive infrastructure and personal data The adoption of national and European standards, as in the case of Italy, has helped to advance information security through the definition of security standards and measures. Additionally, international cooperation has played a significant role in promoting global cyber security through the exchange of knowledge and the definition of consensus standards. Finally, the public's awareness of the risks associated with information security has led to a greater focus on and effort in promoting cyber security. It is possible to argue that the concept of cybersecurity has significantly changed over the years as a result of the development of digital technologies and society's growing reliance on them. As demonstrated in the thesis, the importance of the cyberspace has increased for international powers as they perceive it as a new strategic domain worth utilizing and safeguarding. However, this has led to the development of cyber offensive capability and the expansion of sophisticated cyberattacks. The theories concerning the development of the concept of cyber security, such as the notion that the spread of digital technologies and the expansion of communication networks have led to an increase in cyberattacks and the requirement for the protection of critical infrastructure and personal data, can be tested through the Italian case. Cybersecurity in Italy has become a national priority, and the government has implemented policies to promote information security, including the National Cybersecurity and Information Security Policy and the Assured Coverage in the Event of "Cyber Events." Additionally, the direction of N.I.S represents a further advancement in the promotion of cybersecurity at a European level. Cyberattacks have already had a significant impact on businesses and public administration, demonstrating the need to strengthen online security and resilience. Collaboration with the UE and NATO as well as the use of technologies like the IA are helping to advance the field of cybersecurity. However, given the rapid development of cyberattacks, the challenge continues to be enormous. Therefore, it can be said that the concept of cybersecurity has developed synchronously with the growing digitalization of society and the

economy, becoming a top priority for safeguarding data, vulnerable infrastructure, and national security interests. Therefore, ensuring a cyber environment that is robust and secure will need coordinated global efforts and ongoing investments. The theories concerning the development of the concept of cyber security include the notion that the spread of digital technologies and the expansion of communication networks have led to an increase in cyberattacks and the requirement for the protection of sensitive data and critical infrastructure. This hypothesis is supported by the technological environment's evolution and the ongoing challenges in preserving information security. In conclusion, the development of the concept of cyber security has been a complex process that has involved several interrelated variables, such as the advancement of digital technologies, the expansion of communication networks, the growing dependence on digital technologies, the adoption of European and national norms, international cooperation, and public awareness of the risks associated with information security. These factors have helped to advance global information security, safeguard vulnerable infrastructure, and safeguard personal data. The Italian case underlines the significance of the evolution of the concept of cybersecurity and the need to adopt ever-more-effective measures to safeguard sensitive data in the context of the ongoing development of the cyberspace. The promotion of cyber security necessitates a serious commitment and cooperative effort from all involved parties on a national and international level, spanning the public and private sectors.