Università degli Studi di Bari “Aldo Moro”

Dipartimento di Informatica

Corso di laurea in   
**Informatica e Tecnologie per la Produzione del Software**

Tesi di laurea in

**Cybersecurity**

**Definizione di Metodi e Tecniche per la Gestione del Rischio**

Relatori:

**Chiar.mo Prof. Danilo CAIVANO**

**Dott.ssa Vita Santa BARLETTA**

Laureando:

**Nicola BALZANO**

Anno Accademico 2023/2024

**Indice**

[Capitolo I – Stato dell’Arte 4](#_Toc162107974)

[Introduzione 4](#_Toc162107975)

[1.1 Internet of Things – Un mondo interconnesso 6](#_Toc162107976)

[1.2 Cybersecurity – Cos’è e di cosa si occupa 6](#_Toc162107977)

[1.3 Attacchi Cyber – Analisi delle tendenze 7](#_Toc162107978)

[1.4 NIS2 – L’ultima normativa nel mondo cyber 8](#_Toc162107979)

[1.5 Cyber Kill Chain – Cos’è e come usarla 9](#_Toc162107980)

[1.6 MITRE ATT&CK Framework 10](#_Toc162107981)

[1.7 MITRE ATLAS – Nuove tecnologie e nuove minacce 11](#_Toc162107982)

[Capitolo II 12](#_Toc162107983)

[Nuova Privacy Knowledge Base 12](#_Toc162107984)

[2.1 Privacy Design Pattern 13](#_Toc162107986)

[Bibliografia 14](#_Toc162107987)

# Capitolo I – Stato dell’Arte

Introduzione

Nell'era digitale in cui viviamo, **l'informatica** e la **cybersecurity** sono diventate componenti fondamentali della nostra **esistenza** **quotidiana**. Questo legame inscindibile tra tecnologia e sicurezza informatica è al centro della presente tesi, che esplora non solo come l'informatica ha plasmato il mondo moderno, ma soprattutto come la cybersecurity è diventata una materia indispensabile per proteggere i dati e le infrastrutture che sostengono la nostra società. Il mondo sta andando incontro all’evoluzione, giorno dopo giorno, mese dopo mese, anno dopo anno. L’**evoluzione** però non è solo positiva: ogni scoperta può essere interpretata sia come un progresso benefico, sia come una possibilità di impiego dannoso.

Nell'ambito della sicurezza informatica, la distinzione tra uso **legittimo** e **malintenzionato** delle nuove tecnologie è delineata da una linea estremamente sottile. Per anticipare, identificare e difendere efficacemente le infrastrutture digitali dalle minacce emergenti, diventa cruciale adottare un approccio proattivo, che sia costantemente aggiornato. In questo contesto, ciò che distingue l'uso legittimo da quello malevolo non è tanto la **conoscenza** in sé, quanto piuttosto gli **intenti** che guidano il suo impiego. Le tecniche di attacco evolvono di pari passo con le tecnologie di difesa, generando un **ciclo** **continuo** di sfide e risposte. Questa dinamica impone agli esperti di sicurezza informatica di andare oltre la semplice reazione agli incidenti, spingendoli a prevedere e prevenire attivamente le potenziali minacce.

Adottare tale approccio multidisciplinare, che integra una profonda comprensione delle **tattiche**, **tecniche** e **procedure** (**TTP**) impiegate dagli aggressori con l'uso di strumenti all'avanguardia come l'**analisi** **comportamentale**, la **threat** **intelligence** e l'**apprendimento** **automatico**, consente di anticipare e neutralizzare le minacce informatiche prima che queste si trasformino in attacchi concreti e dannosi. La capacità di rilevare precocemente le anomalie e i potenziali pericoli, analizzando e interpretando i segnali deboli all'interno del vasto mare di dati generati dalle attività di rete, rappresenta un pilastro fondamentale nella costruzione di un ecosistema digitale resiliente e sicuro.

In questo contesto, l'obiettivo primario della presente tesi è esattamente quello di esplorare e delineare l'importanza di un approccio proattivo nella sicurezza informatica, attraverso l'analisi dettagliata delle strategie offensive e difensive, insieme all'**implementazione** **di soluzioni innovative per la prevenzione e il rilevamento** di ogni possibile minaccia conosciuta.

## Internet of Things – Un mondo interconnesso

Per acquisire una piena comprensione del panorama della cybersecurity bisogna conoscere l’ambiente in cui ormai l’uomo da anni si muove.

Il concetto dell’**Internet delle Cose** [1] (**IoT**[[1]](#footnote-1)) è alla base della vita smart[[2]](#footnote-2) che l’uomo vive ogni giorno, descrive dispositivi dotati di sensori, capacità di elaborazione, software e altre tecnologie che collegano e scambiano dati con altri dispositivi e sistemi su Internet o altre reti di comunicazione.

La riflessione su chi detenga la vera conoscenza, se **siamo noi a esplorare il mondo o** se **è il mondo a scrutarci dettagliatamente**, assume un rilievo particolare nell'era attuale, dominata dalla presenza capillare di dispositivi connessi. Questi strumenti, progettati per agevolare la nostra esistenza, entrano nella sfera della nostra **privacy** per nostra stessa scelta, sollevando interrogativi imprescindibili: quali dati raccolgono su di noi? Con quale precisione possono anticipare i nostri interessi e desideri di acquisto? E come fanno a mappare così accuratamente le nostre routine quotidiane? Ancor più cruciale è comprendere le potenziali implicazioni legate alla divulgazione di queste informazioni personali.

Il compito della materia d’argomento di questo elaborato è proprio quello di rispondere all’ultima domanda.

## Cybersecurity – Cos’è e di cosa si occupa

La **Cybersecurity** [2]è una materia che ha il compito di **proteggere**, nel senso più ampio del termine, **infrastrutture** **digitali** come sistemi, reti e programmi software da attacchi informatici, finalizzati all’ottenimento, trasformazione, distruzione, di informazioni sensibili e/o interruzione di processi aziendali.

Al cuore della cybersecurity vi è la triade **CIA** [3] (Confidentiality, Integrity, Availability) che funge da pilastro per la sicurezza delle informazioni. Questo modello si prefigge di garantire la riservatezza (**Confidentiality**) proteggendo le informazioni sensibili dall'accesso non autorizzato, l'integrità (**Integrity**) assicurando che i dati non vengano alterati o distrutti in modo improprio, e la disponibilità (**Availability**) mantenendo l'accesso continuo e ininterrotto alle informazioni e ai sistemi per gli utenti autorizzati.

Insieme, questi principi formano il framework su cui si basano le strategie di difesa contro gli attacchi informatici, che puntano a violare queste fondamenta per infliggere danni o trarre vantaggi illeciti.

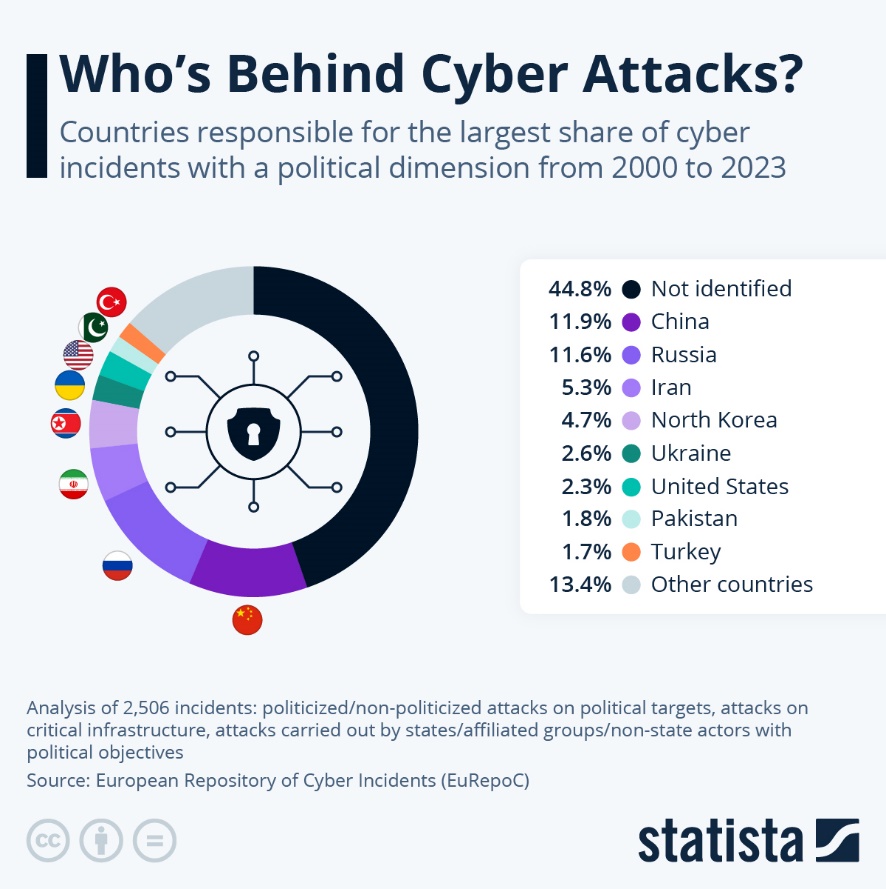
## Attacchi Cyber – Analisi delle tendenze

Negli ultimi anni, il panorama globale ha testimoniato l'urgente richiesta di avanzamenti tecnologici nel campo della difesa informatica, volti a proteggere dati, procedure e infrastrutture critici. Un'**indagine comparativa** recente [4], che confronta i dati relativi agli attacchi informatici noti fino al Q2[[3]](#footnote-3) 2022 e quelli registrati nel Q2 2023, ha evidenziato un incremento esponenziale nella media settimanale degli attacchi informatici a livello globale, interessando diversi settori industriali. Questo trend allarmante sottolinea non solo la crescente sofisticatezza e frequenza delle minacce informatiche, ma anche l'impellente necessità per le organizzazioni di ogni ambito di rafforzare le loro misure di sicurezza per contrastare efficacemente tali pericoli.

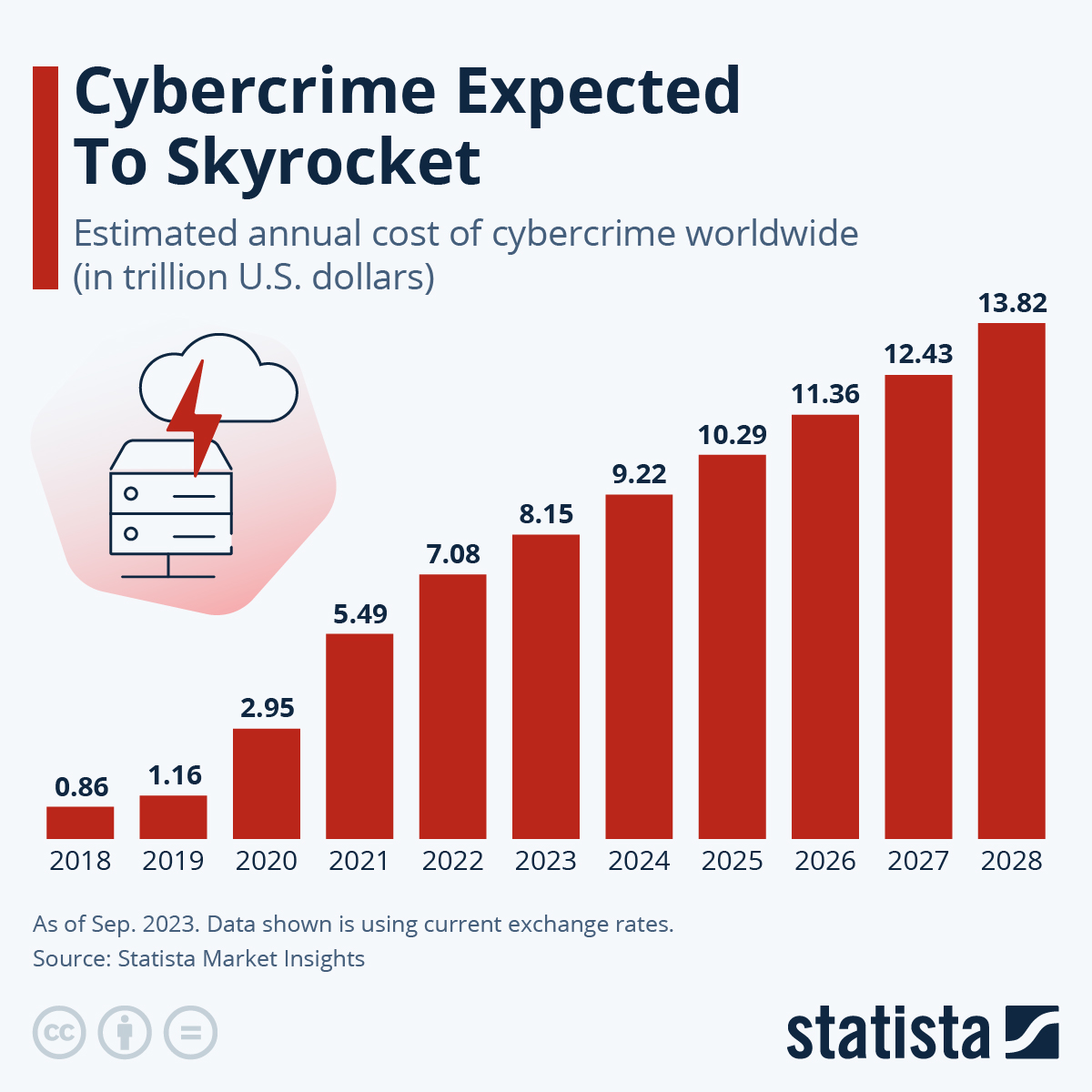


I dati allarmanti emersi dallo studio mostrano un incremento significativo degli attacchi informatici, con particolare enfasi sui settori delle consulenze, bancario e sanitario. Tra questi, il **settore** **sanitario** emerge come particolarmente **critico**, non solo perché rappresenta il terzo settore più colpito da questa ondata di attacchi, ma anche per l'ampia quantità di introiti che genera a livello globale e per il **vasto** **volume** **di** **informazioni** **sensibili** che gestisce. Questa situazione mette in luce l'urgenza con cui il settore sanitario deve affrontare le sfide legate alla cybersecurity, sottolineando l'importanza di implementare misure di protezione avanzate per salvaguardare dati di vitale importanza.

Un altro grande problema dilemma è dovuto alla provenienza di questi attacchi. Uno studio [5] in cui sono coinvolte la Cybersecurity and Infrastructure Security Agency (**CISA**), la National Security Agency (**NSA**) e il Federal Bureau of Investigation (**FBI**) evidenzia che circa il 45% di questi attacchi ha origine ignota, perciò la **tracciabilità** e l'**identificazione** **degli aggressori** rappresentano sfide significative nel contrasto alle minacce informatiche.



Basandosi sulle valutazioni della fonte che ha fornito i dati menzionati in precedenza, il **costo annuale globale associato alla mitigazione dei crimini informatici** [6] nei prossimi 4 anni è destinato ad aumentare in maniera lineare di circa **1,5 trilioni di dollari statunitensi** all’anno.



## NIS2 – L’ultima normativa nel mondo cyber

## Cyber Kill Chain – Cos’è e come usarla

## MITRE ATT&CK Framework

## MITRE ATLAS – Nuove tecnologie e nuove minacce

# Capitolo II

Nuova Privacy Knowledge Base



## Privacy Design Pattern

sium

# Bibliografia

[1] *Cisco*. (2022). https://www.cisco.com/c/it\_it/products/security/what-is-cybersecurity.html

[2] *Wikipedia*. (2024, Marzo 11). https://it.wikipedia.org/wiki/Internet\_delle\_cose

[3] *Cisco*. (2023). https://www.learncisco.net/courses/iins/common-security-threats/information-security-and-common-threats.html

[4] Check Point (2023, Luglio ). https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

[5] Statista (2024, Febbraio 23). https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

[6] Statista (2024, Febbraio 22). https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

1. Acronimo del neologismo **Internet of Things** [↑](#footnote-ref-1)
2. Si riferisce a uno stile di vita reso più efficiente e comodo attraverso l'uso di dispositivi connessi e tecnologie intelligenti. [↑](#footnote-ref-2)
3. Secondo semestre [↑](#footnote-ref-3)