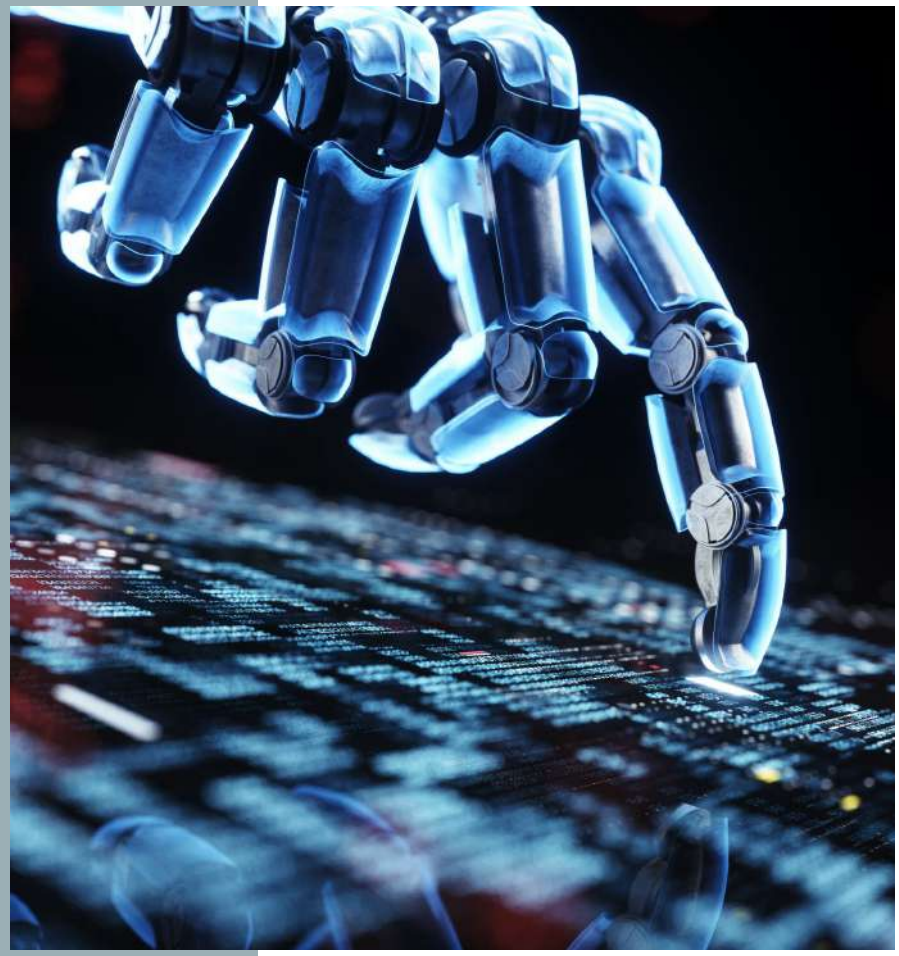
ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI PALERMO



CYBERSICUREZZA ED AI: UNA SFIDA ATTUALE

Prof. Giuseppe Lo Re

Dipartimento di Ingegneria

Università degli Studi di Palermo

UNIVERSITÀ DEGLI STUDI DI PALERMO

PROGRAMMA

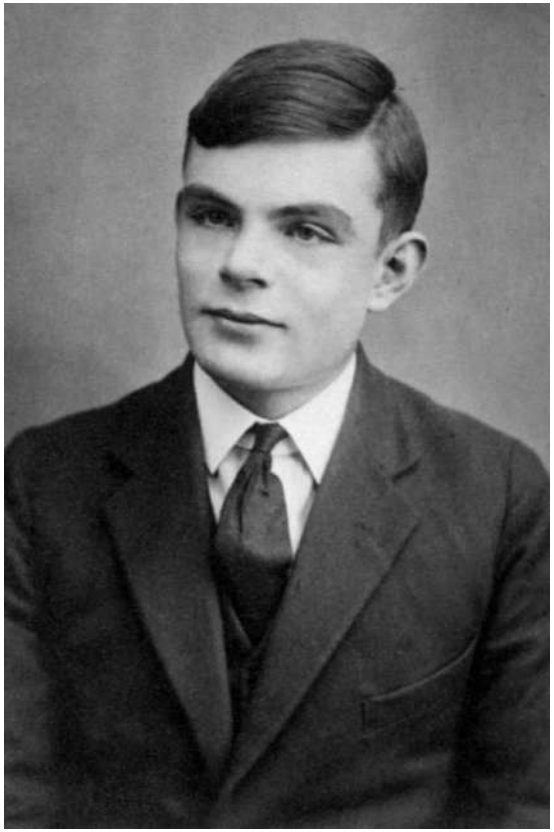
- ***Cybersicurezza ed AI: una sfida attuale***
  - *Prof. Giuseppe Lo Re,*
- ***Attacchi Cyber ai sistemi di AI***
  - *Prof. Marco Morana,*
- ***AI per la Cybersicurezza***
  - *Prof. Pierluca Ferraro,*

COMPUTING MACHINERY AND INTELLIGENCE

by A. M. Turing

1. The Imitation Game

I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think." The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous. If the meaning of the words "machine" and "think" are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, "Can machines think?" is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which



ENIGMA





ROTORE

17:02 TikTok: Trump, abbiamo un compratore, gruppo di persone molto
16:54 Dazi: Trump, non credo ci sara' bisogno di prorogare scadenza del 9
15:37 ***A2A: alla firma cessione reti gas Lombardia ad Ascopiave, dossier da
13:33 Enav: guasto radar dovuto a connessioni Tim, operativita'
13:04 Usa: Musk torna ultima bozza legge bilan

Guasto al radar del Nord Italia, Enav: «Problemi alla rete Tim. Le polemiche? Inutili, garantita la sicurezza»

di **Leonard Berberi**

L'Enav ricostruisce quanto avvenuto nella serata di ieri, con decine di voli bloccati e deviati dagli aeroporti dell'Italia nord-occidentale: «Il problema ha riguardato la connettività che consente l'afflusso dei dati, garantita da Tim. In emergenza abbiamo attivato una connessione satellitare alternativa»



CORRIERE TV



Spese per la difesa. Dietro i numeri poco (o niente)

Le notizie di domenica 29 giugno sul conflitto in Ucraina, in diretta. Il sindaco di Kiev: «Esplosioni in città». Zelensky ringrazia il Pontefice: «Fermiamo insieme l'aggressione russa»





«Morte all'esercito israeliano, Palestina libera»: gli sloga al concerto di Glastonbury che mettono nei guai la Bbc

È successo durante l'esibizione del rapper Bobby Vylan ed è stato trasmesso in diretta dall'emittente britannica


Comfyvita
APRIRE >

Le migliori scarpe da passeggio, ideali per tutto il giorno.

R CONTENUTO PER GLI ABBONATI PREMIUM

“Trasporti, attacchi cyber da Mosca”. L’allarme dell’intelligence britannica

di Gianluca Di Feo



Passeggeri a Cagliari sulla pista in attesa di salire su un aereo a causa di un guasto al Centro di controllo d'area di Milano (ansa)

Il report presentato al vertice Nato. Londra chiede risposta coordinata Anche l’Italia nel mirino

L'ascolto è riservato agli abbonati premium

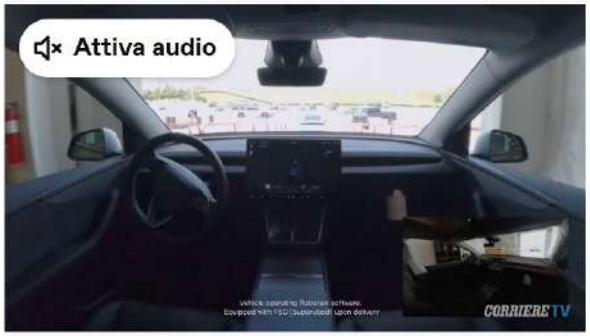
Zuckerberg annuncia la nascita dei laboratori di Super intelligenza artificiale di Meta: «L'inizio di una nuova era per l'umanità»

di Roberto Cosentino

L'estate rovente di Menlo Park vede Mark Zuckerberg impegnato in una dispendiosa caccia di talenti di altri gruppi per sviluppare una super intelligenza firmata Meta



CORRIERE TV



Il video della Tesla a guida autonoma che raggiunge la casa del cliente che l'ha acquistata

gf4pbat9O_3p04GK3r-vyWGfSHmIGuk6oXov_0Gy4FWhKjFa89qm1fMg0qHKtxF2KWmvLo0D3Eid3...tores/page/4D9D7FE6-4F0B-4F7E-A208-203C2A9D44E8?maas=maas_adg_041E7ADF26C2215ADB3D9F49E83

adv



Truffa dello Spid, la minaccia a stipendi e pensioni ora passa attraverso l'identità digitale

di Alessandro Longo



di cocaina»

di Guido Olimpio

È telecomandato con modem Starlink e può trasportare più di una tonnellata di cocaina ed ha un'autonomia fino ad 800 miglia





Putin abbandona un convegno per non fare aspettare al telefono Trump: «Non vorrei farlo arrabbiare...»

Il presidente russo suscita l'ilarità del pubblico con la sua battuta

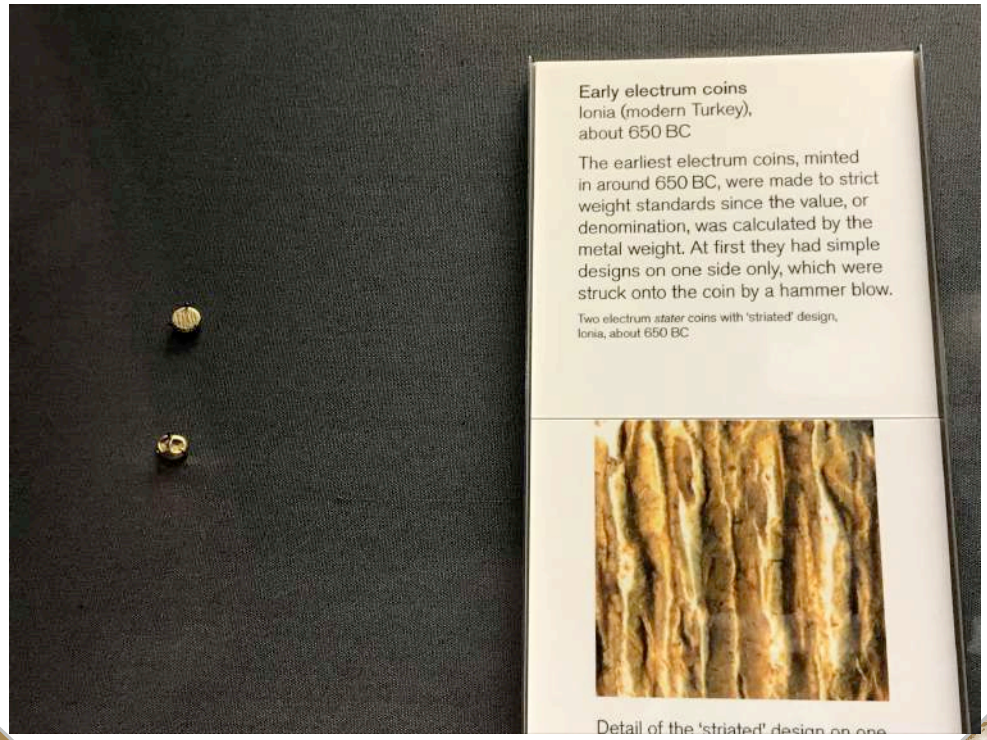


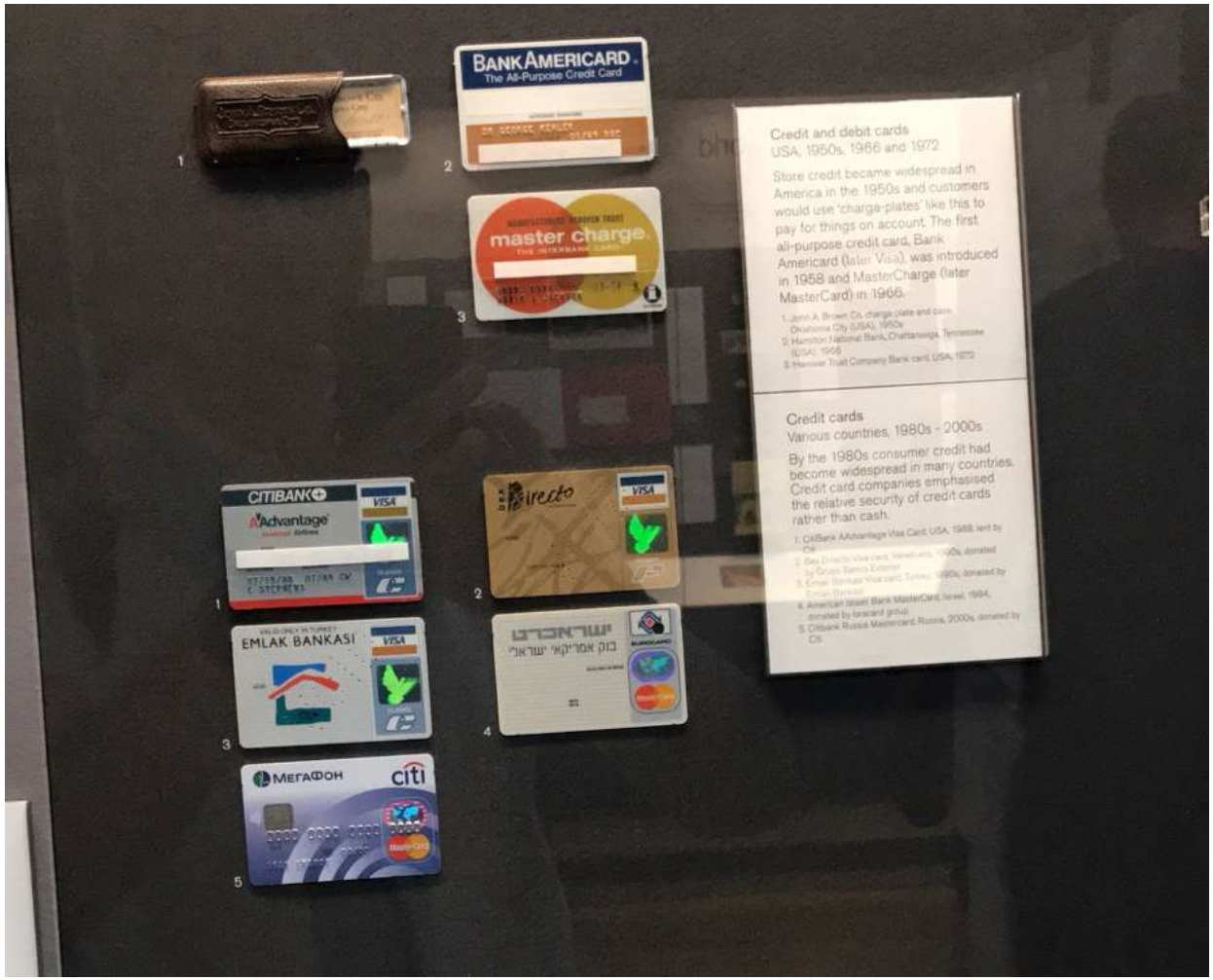
Informazione Valore

- Denaro
  - strumento per codifica e scambio di informazione
- DNA
  - 4 basi codificano un essere vivente
  - Un essere umano ammonta a 750 MB comprimibili in circa 4MB






Early electrum coins
Ionia (modern Turkey),
about 650 BC
The earliest electrum coins, minted in around 650 BC, were made to strict weight standards since the value, or denomination, was calculated by the metal weight. At first they had simple designs on one side only, which were struck onto the coin by a hammer blow.
Two electrum stater coins with 'striated' design, Ionia, about 650 BC
Detail of the 'striated' design on one


BANKAMERICARD
The All-Purpose Credit Card
master charge
Credit and debit cards
USA, 1950s, 1966 and 1972
Store credit became widespread in America in the 1950s and customers would use 'charga-plates' like this to pay for things on account. The first all-purpose credit card, Bank Americard (later Visa), was introduced in 1958 and MasterCharge (later MasterCard) in 1966.
Credit cards
Various countries, 1980s - 2000s
By the 1980s consumer credit had become widespread in many countries. Credit card companies emphasised the relative security of credit cards rather than cash.
CITIBANK
Advantage
VISA
Directo
EMLAK BANKASI
МегаФон
citi

Proliferazione delle tecnologie digitali



Fotocamere digitali e condivisione di foto su Internet sono utilizzate da pedopornografi.



La maggiore convenienza dei servizi di electronic banking e commercio elettronico fornisce terreno fertile per le frodi.



Le comunicazioni elettroniche come e-mail, SMS, wA possono essere utilizzate per perseguitare e molestare.



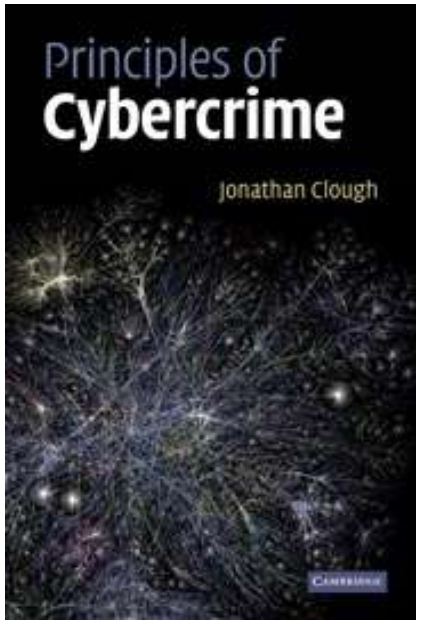
La facilità con cui i media digitali possono essere condivisi ha portato a un'esplosione nella violazione del copyright.



La nostra crescente dipendenza da computer e reti digitali rende la tecnologia stessa un obiettivo allettante; sia per ottenere informazioni sia quale mezzo per causare interruzioni e danni.

Crimini Cibernetici: concetti ed evoluzione

- «È noto a tutti gli uomini che il cambiamento radicale nel trasporto delle persone e delle merci, effettuato dall'introduzione dell'automobile, la velocità con cui si muove, e la facilità con cui le persone malintenzionate possono evitare la cattura, hanno grandemente incoraggiato e aumentato crimini. »





Crimini Cibernetici: concetti ed evoluzione

*Il **cyberspace** è la cosa più complessa che l'uomo abbia mai costruito:*

> *da un lato unione di migliaia di reti che rendono difficile anche solo avere una fotografia istantanea di chi vi è connesso, dall'altro stratificazione di programmi software e protocolli sviluppati negli ultimi **cinquanta** anni.*

Questa complessità è generatrice di vulnerabilità (errori software, errate configurazioni e debolezze nei protocolli) che vengono sfruttate dai cyber-criminali per sottrarre dati o arrecare danni.



Cybersecurity

L'insieme di strumenti, politiche, concetti di sicurezza, misure di salvaguardia, linee guida, approcci alla gestione del rischio, azioni, attività formative, migliori pratiche, garanzie e tecnologie che possono essere utilizzati per proteggere l'ambiente del cyberspazio, nonché le risorse delle organizzazioni e degli utenti..

*Le risorse dell'organizzazione e degli utenti includono dispositivi informatici connessi, **personale**, infrastrutture, applicazioni, servizi, sistemi di telecomunicazione e la totalità delle informazioni trasmesse e/o archiviate nell'ambiente del cyberspazio.*

La sicurezza informatica mira a garantire il conseguimento e il mantenimento delle proprietà di sicurezza degli asset dell'organizzazione e degli utenti, a fronte dei rischi per la sicurezza rilevanti nell'ambiente del cyberspazio. Gli obiettivi generali di sicurezza comprendono i seguenti:

- ***disponibilità;***
- ***integrità** —include l'autenticità dei dati e la non ripudiabilità*
- ***riservatezza**.*



Definizione tratta **Raccomandazione ITU-T X.1205**, intitolata *"Overview of cybersecurity"*. International Telecommunication Union

Il NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms, maggio 2013) definisce il termine sicurezza informatica come segue:

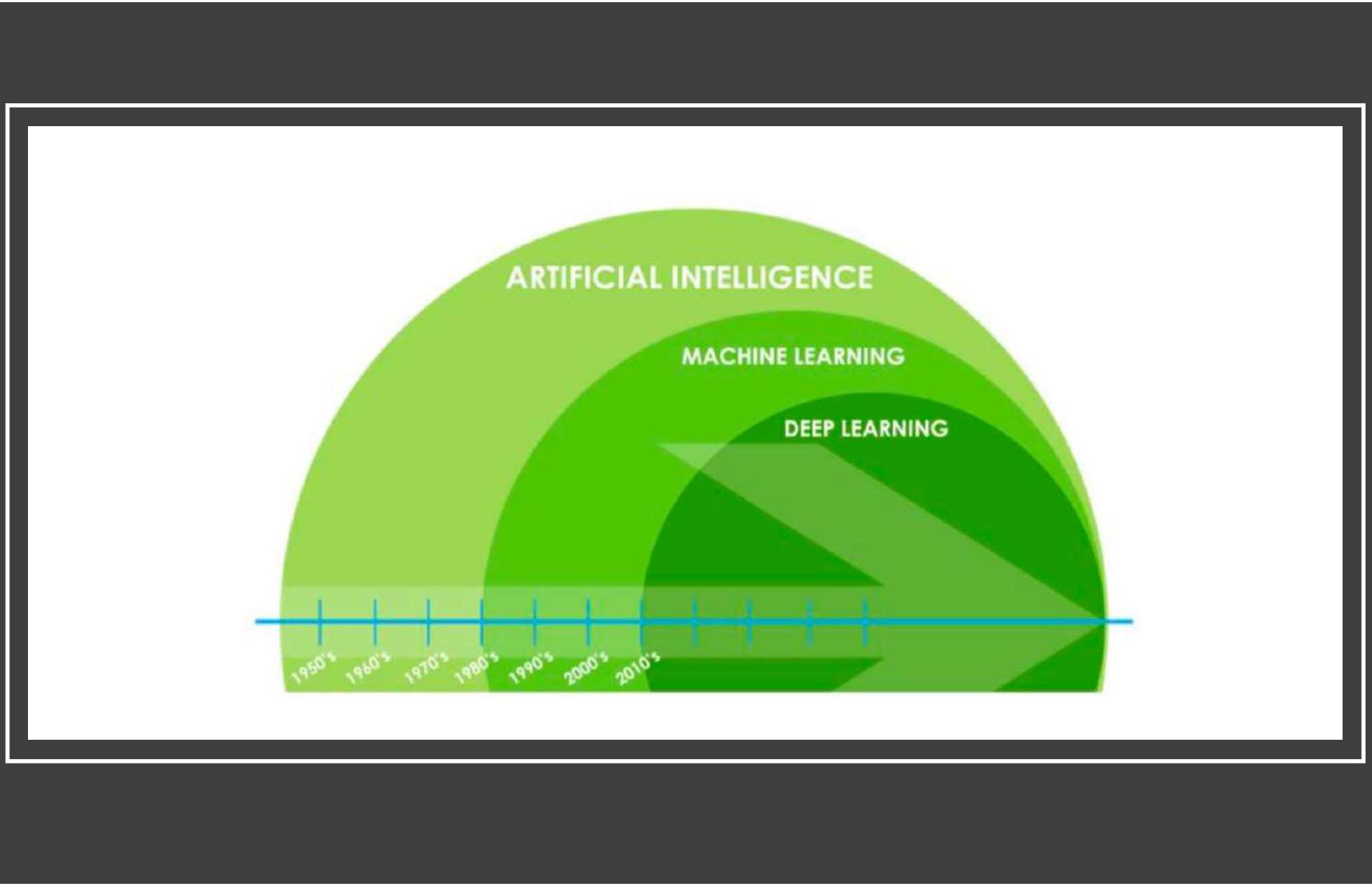


Sicurezza informatica:

Misure e controlli che assicurano la confidenzialità, l'integrità e la disponibilità delle risorse del sistema informativo, compresi l'hardware, il software, il firmware e le informazioni elaborate, memorizzate e trasmesse

L'INTELLIGENZA ARTIFICIALE

- **L'intelligenza artificiale studia da circa 70 anni l'emulazione dell'intelligenza umana (ed in certi casi, l'intelligenza animale) con l'uso di strumenti informatici (SW & HW)**
- **Oggi, la principale area di ricerca e applicazione dell'intelligenza artificiale è il**
  - machine learning (algoritmi che imparano e si adattano in base ai dati che ricevono in input) e in particolare il suo sottoinsieme relativo alle
    - "reti neurali" e il
    - "deep learning".
- **Appartengono al mondo dell'IA anche il "riconoscimento vocale", la "robotica avanzata" e i "sistemi esperti", molto in voga qualche decennio fa.**


ARTIFICIAL INTELLIGENCE
MACHINE LEARNING
DEEP LEARNING
1950's
1960's
1970's
1980's
1990's
2000's
2010's

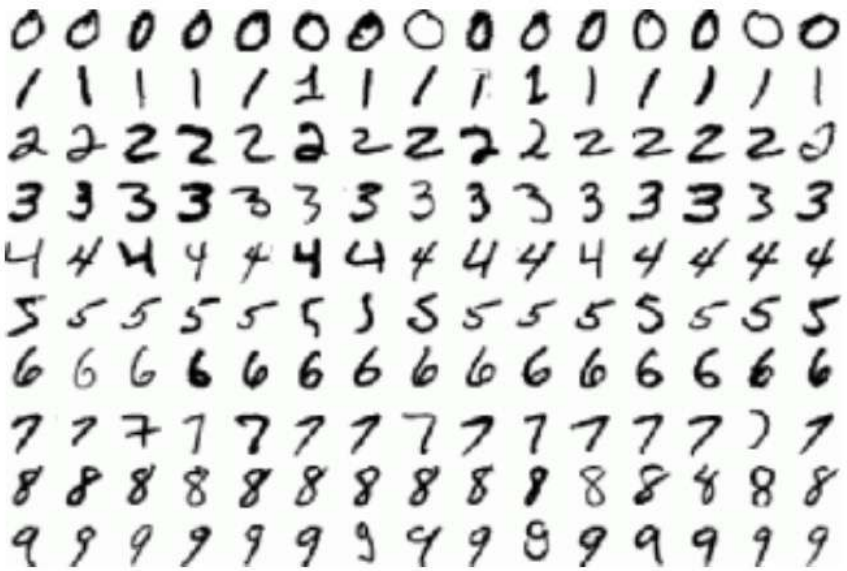
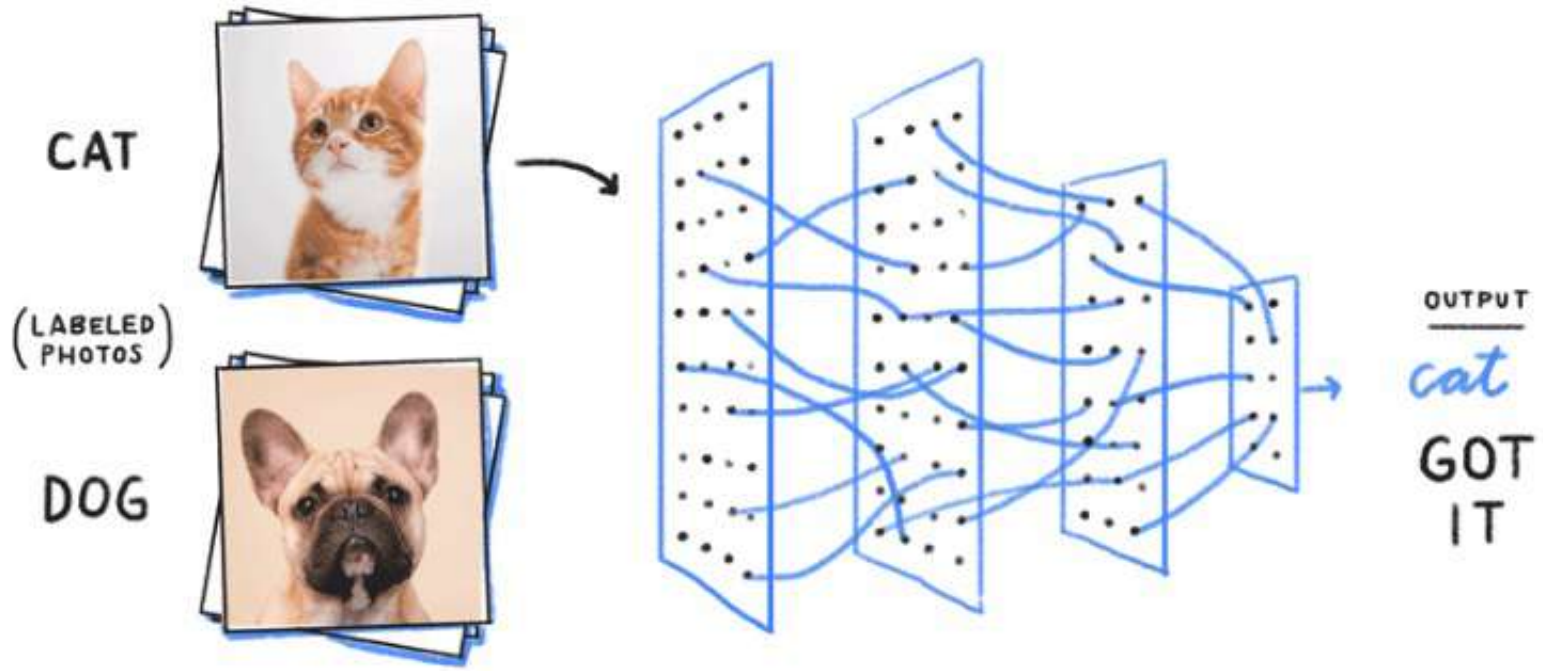


Figura 1 - Esempi di cifre scritte a mano, tratti dal dataset MNIST[3]

QUANDO NON È DISPONIBILE ALCUN MODELLO MATEMATICO DEL PROBLEMA


CAT
(LABELED PHOTOS)
DOG
OUTPUT
cat
GOT IT

LE 5 FAMIGLIE DELL'IA





I SIMBOLISTI

Ispirati dalla filosofia e dal ragionamento logico basato sull'astrazione dei simboli.

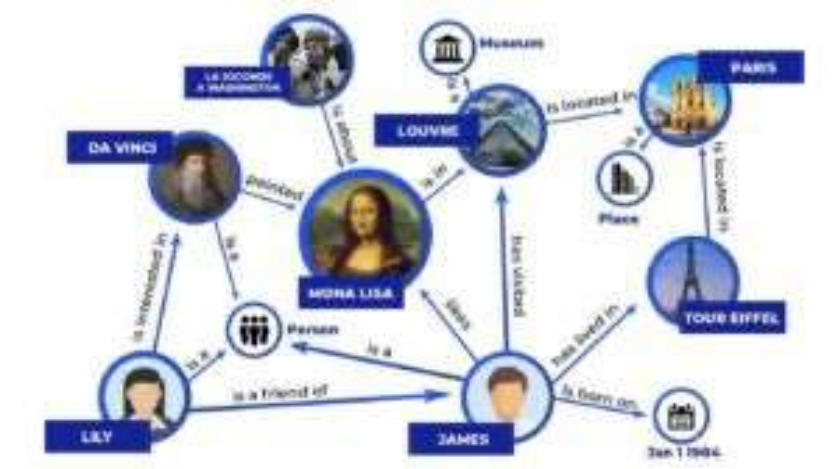
Rappresentazione della conoscenza, tramite *ontologie* e *database di conoscenza*, e di algoritmi di *ragionamento deduttivo* e *induttivo*. I metodi per la rappresentazione della conoscenza consentono di rappresentare **entità** (fatti, persone, ecc.) e **relazioni** tra esse; la rappresentazione deve essere efficiente, sia per l'interrogazione delle relazioni esistenti sia per consentire l'aggiunta di nuovi fatti, comprendenti eventualmente nuove entità e relazioni.

L'esempio più famoso di questo tipo di rappresentazione della conoscenza è il *grafo di conoscenza* (*knowledge graph*) di Google, di cui viene mostrato un frammento in ogni pagina di risultati di una ricerca.

Gli algoritmi di ragionamento, implementati solitamente sotto forma di *sistemi di regole* o di *alberi di decisione*, possono essere visti come una sequenza di **passi di deduzione**, ciascuno dei quali trae una conclusione a partire da certe ipotesi, costituite da fatti e relazioni note.

L'*IA simbolica* è stata il paradigma dominante tragli anni 1950 e 1980, e ha prodotto molti software interessanti, tra cui i cosiddetti *sistemi esperti*

I SIMBOLISTI



Ispirati dalla filosofia e dal ragionamento logico basato sull'astrazione dei simboli.

Rappresentazione della conoscenza, tramite *ontologie* e *database di conoscenza*, e di algoritmi di *ragionamento deduttivo* e *induttivo*. I metodi per la rappresentazione della conoscenza consentono di rappresentare **entità** (fatti, persone, ecc.) e **relazioni** tra esse; la rappresentazione deve essere efficiente, sia per l'interrogazione delle relazioni esistenti sia per consentire l'aggiunta di nuovi fatti, comprendenti eventualmente nuove entità e relazioni.

L'esempio più famoso di questo tipo di rappresentazione della conoscenza è il *grafo di conoscenza* (*knowledge graph*) di Google, di cui viene mostrato un frammento in ogni pagina di risultati di una ricerca.

Gli algoritmi di ragionamento, implementati solitamente sotto forma di *sistemi di regole* o di *alberi di decisione*, possono essere visti come una sequenza di **passi di deduzione**, ciascuno dei quali trae una conclusione a partire da certe ipotesi, costituite da fatti e relazioni note.

L'*IA simbolica* è stata il paradigma dominante tragli anni 1950 e 1980, e ha prodotto molti software interessanti, tra cui i cosiddetti *sistemi esperti*

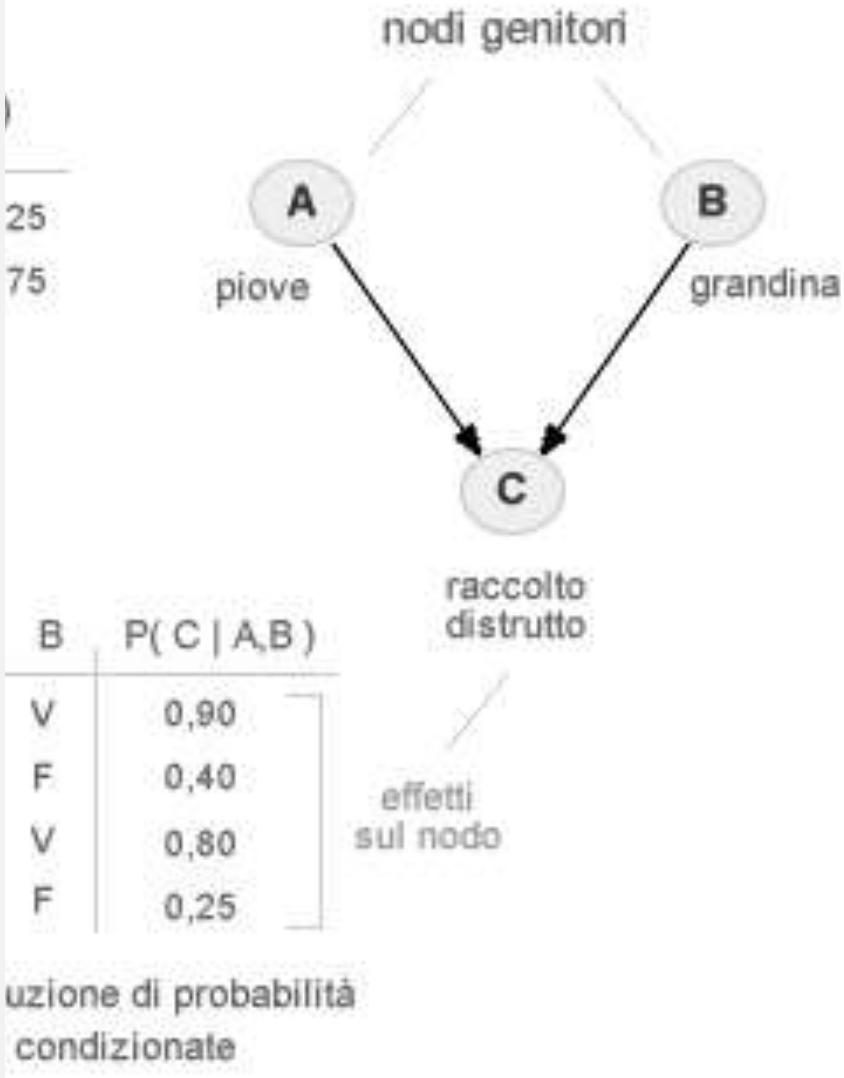
EVOLUZIONISTI

- Gli **evoluzionisti** applicano i principi della biologia evolutiva, in particolare le operazioni svolte dal DNA durante la riproduzione degli individui, nonché la nozione di *fitness*, una sorta di misura di quanto l'individuo si è adattato alle condizioni dell'ambiente in cui vive.
- Gli algoritmi di questo tipo fanno evolvere delle popolazioni di possibili soluzioni per problemi, che solitamente richiedono di massimizzare o minimizzare certe quantità, soddisfacendo contemporaneamente alcuni vincoli.
- Usando opportune operazioni di incrocio (*crossover*) e di mutazione casuale, gli individui della popolazione producono la successiva generazione di individui, che si spera siano più *adatti* a risolvere il problema.
- Oltre che per risolvere diversi problemi ottimizzazione, gli algoritmi evolutivi possono essere usati per far evolvere popolazioni di *reti neurali artificiali*, oppure di *programmi per computer*.



BAYESIANI

- I **bayesiani** adottano un approccio dettato dalla statistica e dal calcolo delle probabilità per implementare una forma di inferenza (ragionamento) probabilistica.
- Gli algoritmi di questa categoria assumono la forma di *reti causali*, o *bayesiane*, in cui vengono valutate le probabilità (condizionate) che si verifichino certi eventi a partire da certe ipotesi.
- Una volta stabilite le relazioni probabilistiche tra cause ed effetti, l'utilizzo del teorema di Bayes consente di calcolare la probabilità che una causa abbia scatenato un certo evento dato.
- L'applicazione più famosa di questo tipo di algoritmi sono i *filtri antispam* per le e-mail.

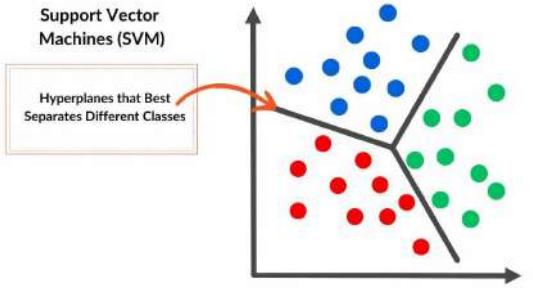


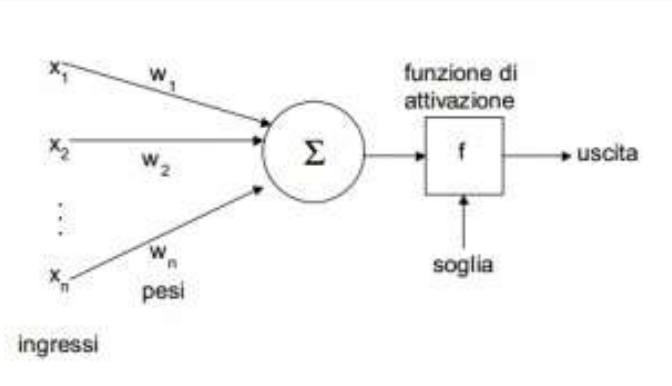
ANALOGISTI

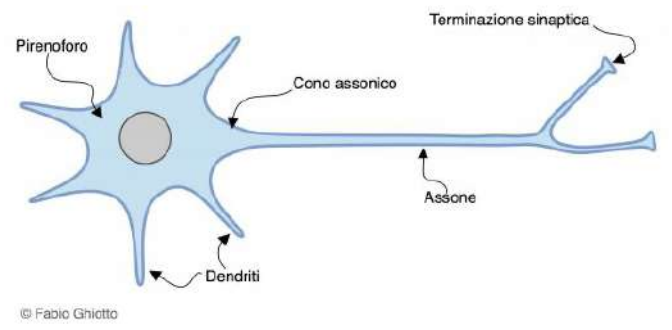
Gli **analogisti**, i cui algoritmi stabiliscono associazioni tra dati, calcolate usando le cosiddette *support vector machines* (SVM).

L'esempio più famoso di algoritmi in questa categoria sono i cosiddetti ***recommender systems***, che in base alle preferenze mostrate dagli utenti suggeriscono un prodotto da acquistare, un film da vedere o una canzone da ascoltare.

Ciò avviene perché, per l'appunto, vengono stabilite delle associazioni - e calcolate delle somiglianze - tra i dati da noi generati (prodotti acquistati, film visti, ecc.) e le scelte fatte precedentemente da chi ha mostrato di avere gusti simili ai nostri.

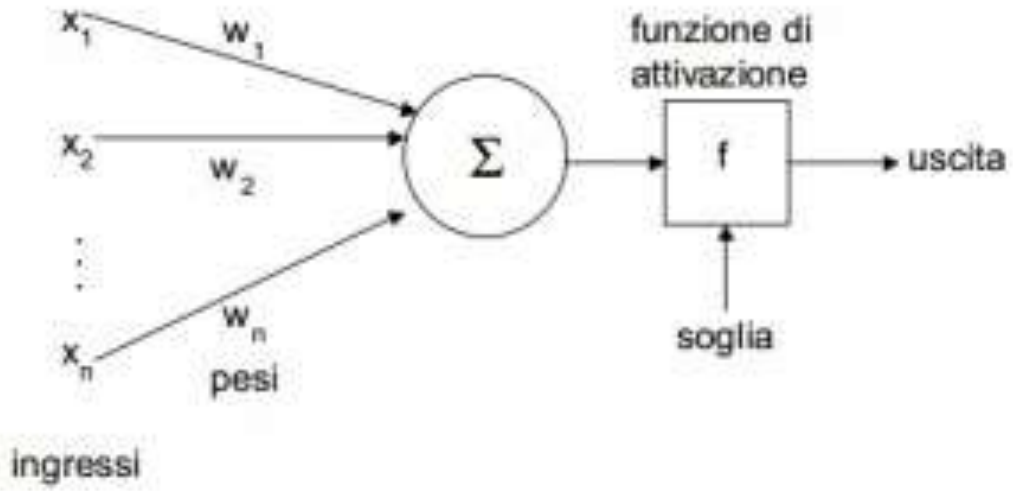


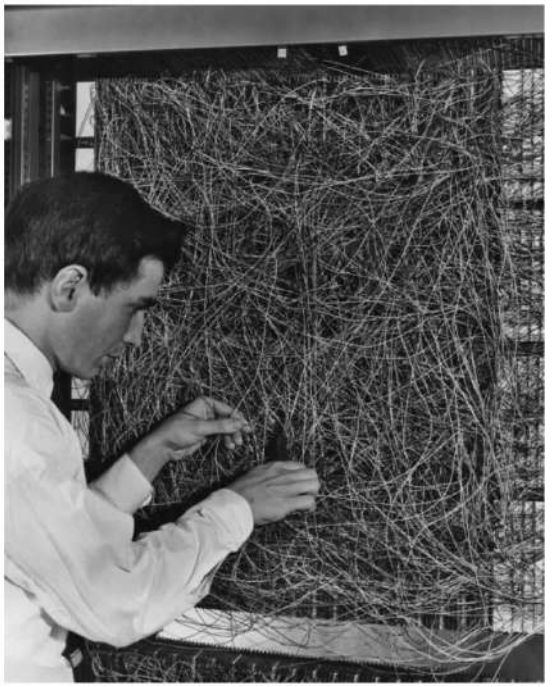




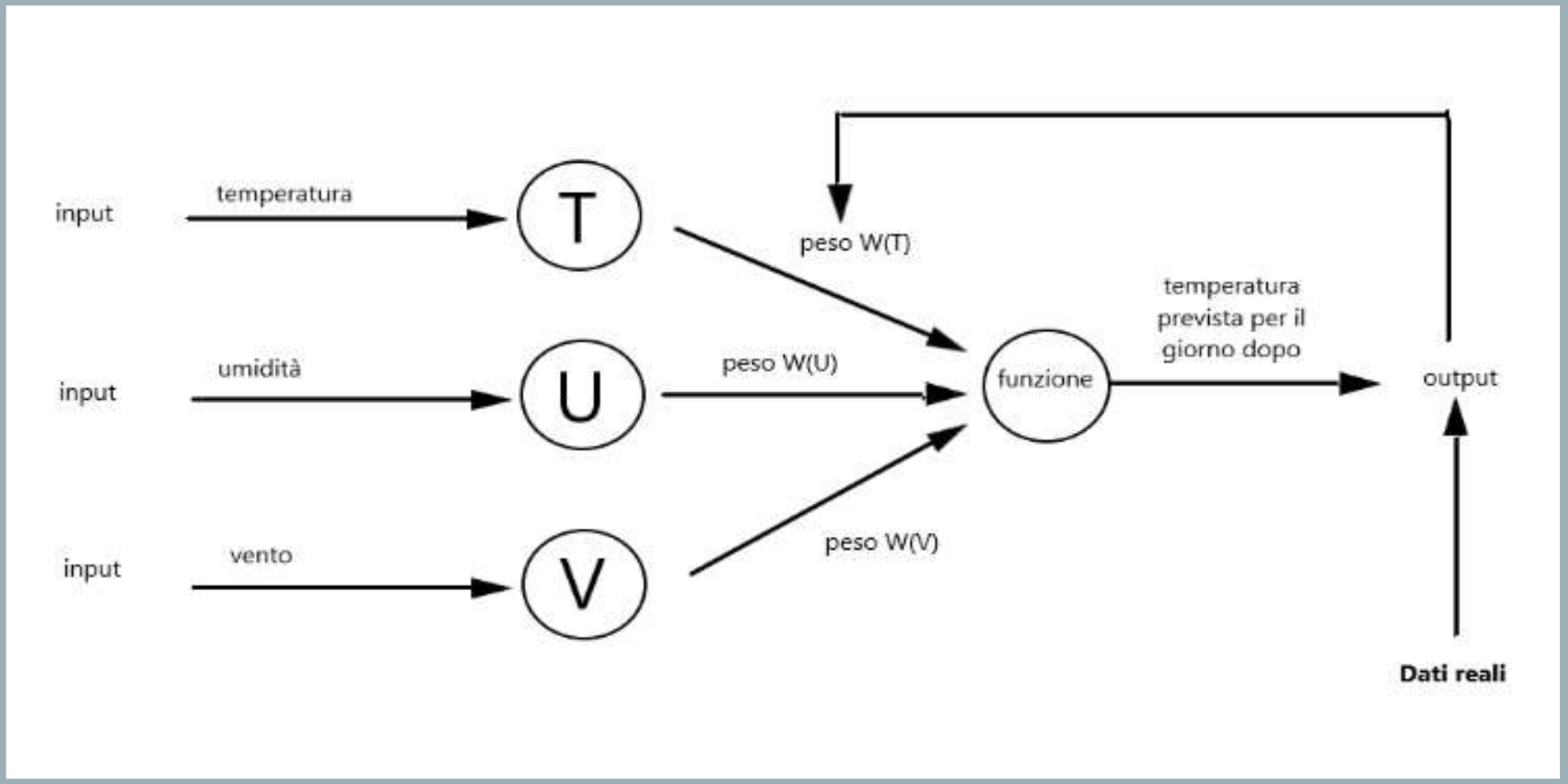
L'APPROCCIO CONNESSIONISTA

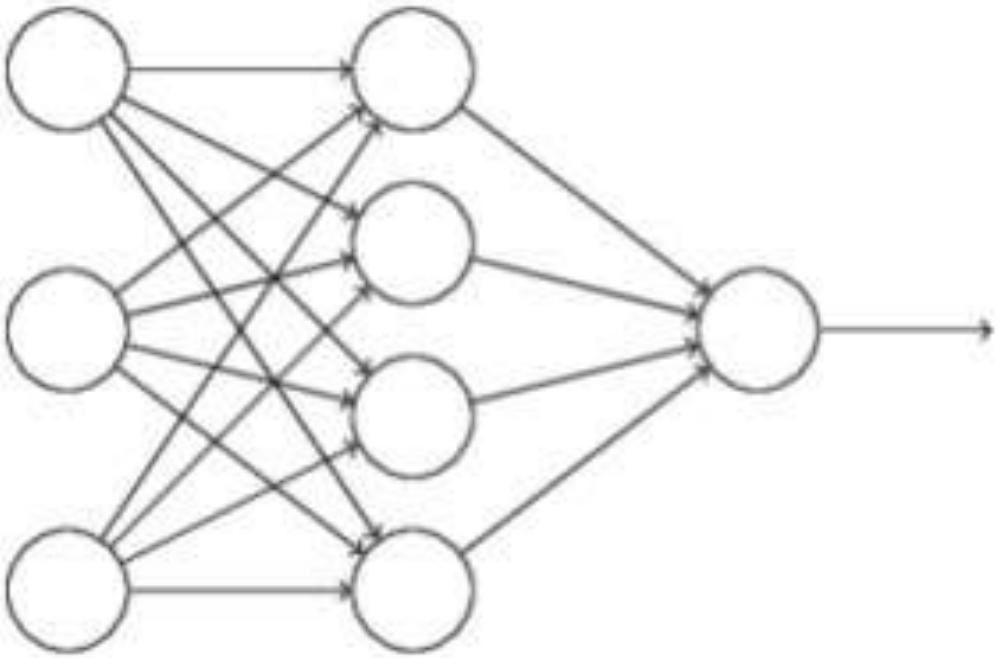
- Reti Neurali: Ispirate al modo in cui le reti neurali biologiche del cervello elaborano le informazioni.
- Il cervello umano è costituito da neuroni, cellule nervose interconnesse che si occupano dell'elaborazione e della trasmissione di segnali chimici ed elettrici.
- La prima idea, messa a punto negli anni '40 del 900 da **Warren McCulloch e Walter Pitts**, è di rappresentare un neurone biologico come una sorta di porta logica con diversi input e un output, ciascuno dei quali può assumere valore 0 oppure 1;
- inoltre, ciascun input può essere *eccitatorio* o *inibitorio*.
- Il neurone calcola un *valore aggregato* dei valori di input, secondo una funzione prestabilita; se il risultato supera una soglia prefissata viene prodotto in output un 1, in caso contrario viene prodotto uno 0.

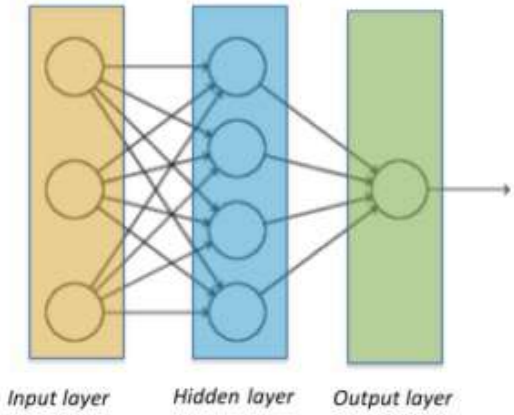


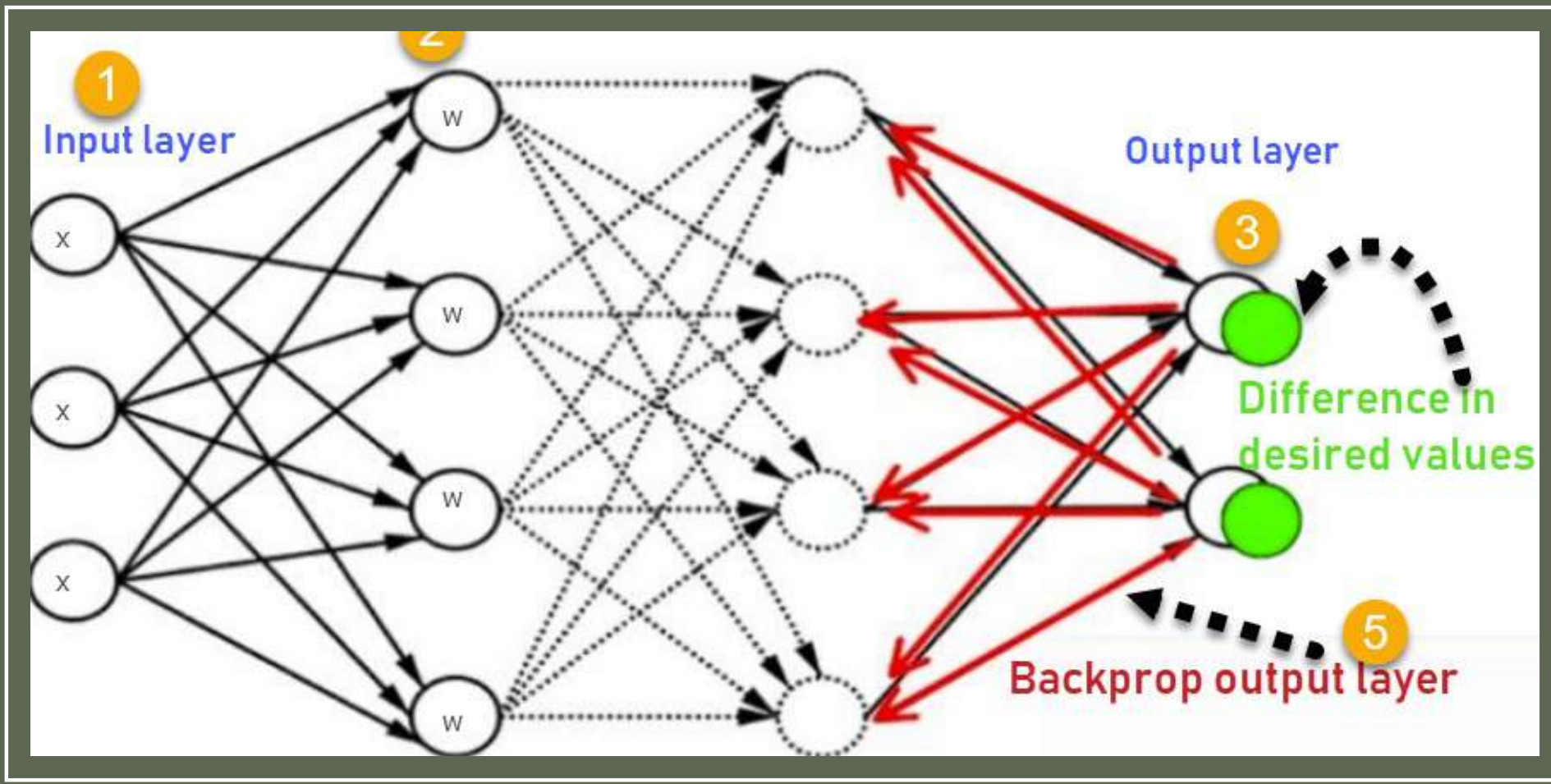


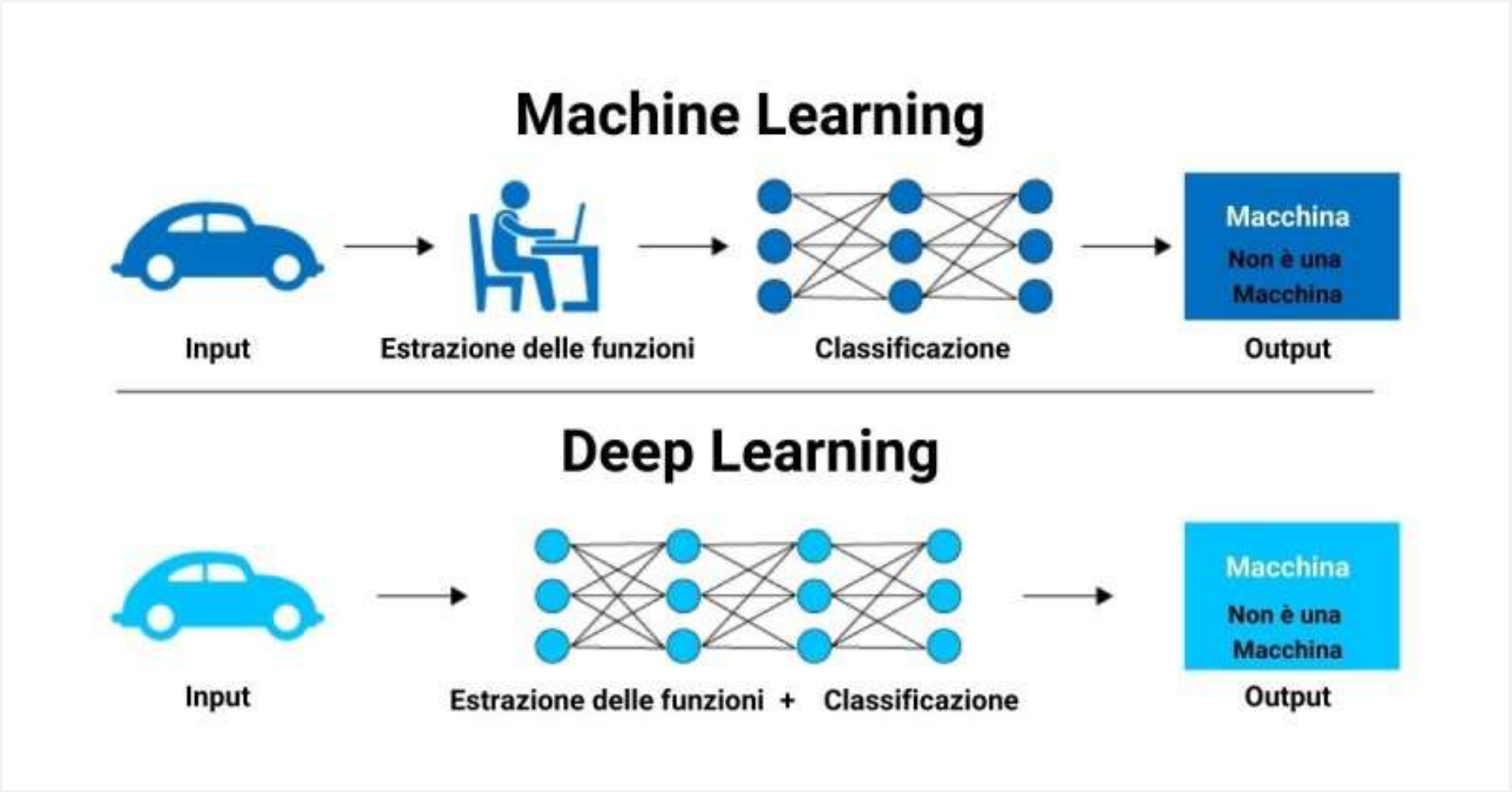
Frank Rosenblatt con un computer Perceptron Mark I nel 1960


input
temperatura
T
peso W(T)
input
umidità
U
peso W(U)
funzione
temperatura prevista per il giorno dopo
output
input
vento
V
peso W(V)
Dati reali




Input layer
Hidden layer
Output layer


1
Input layer
x
x
x
w
w
w
w
Output layer
3
Difference in
desired values
5
Backprop output layer


Machine Learning
Macchina
Non è una
Macchina
Input
Estrazione delle funzioni
Classificazione
Output
Deep Learning
Macchina
Non è una
Macchina
Input
Estrazione delle funzioni + Classificazione
Output

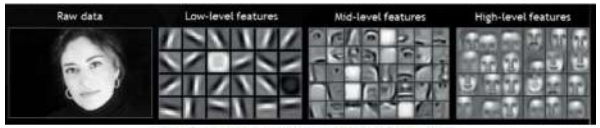
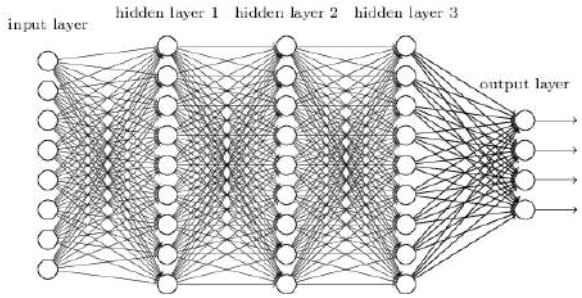
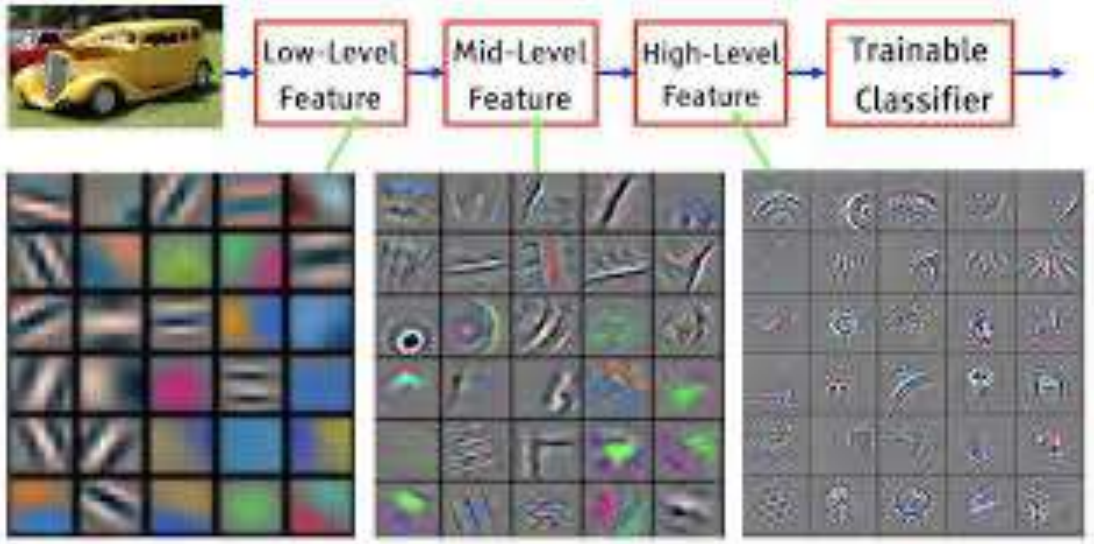
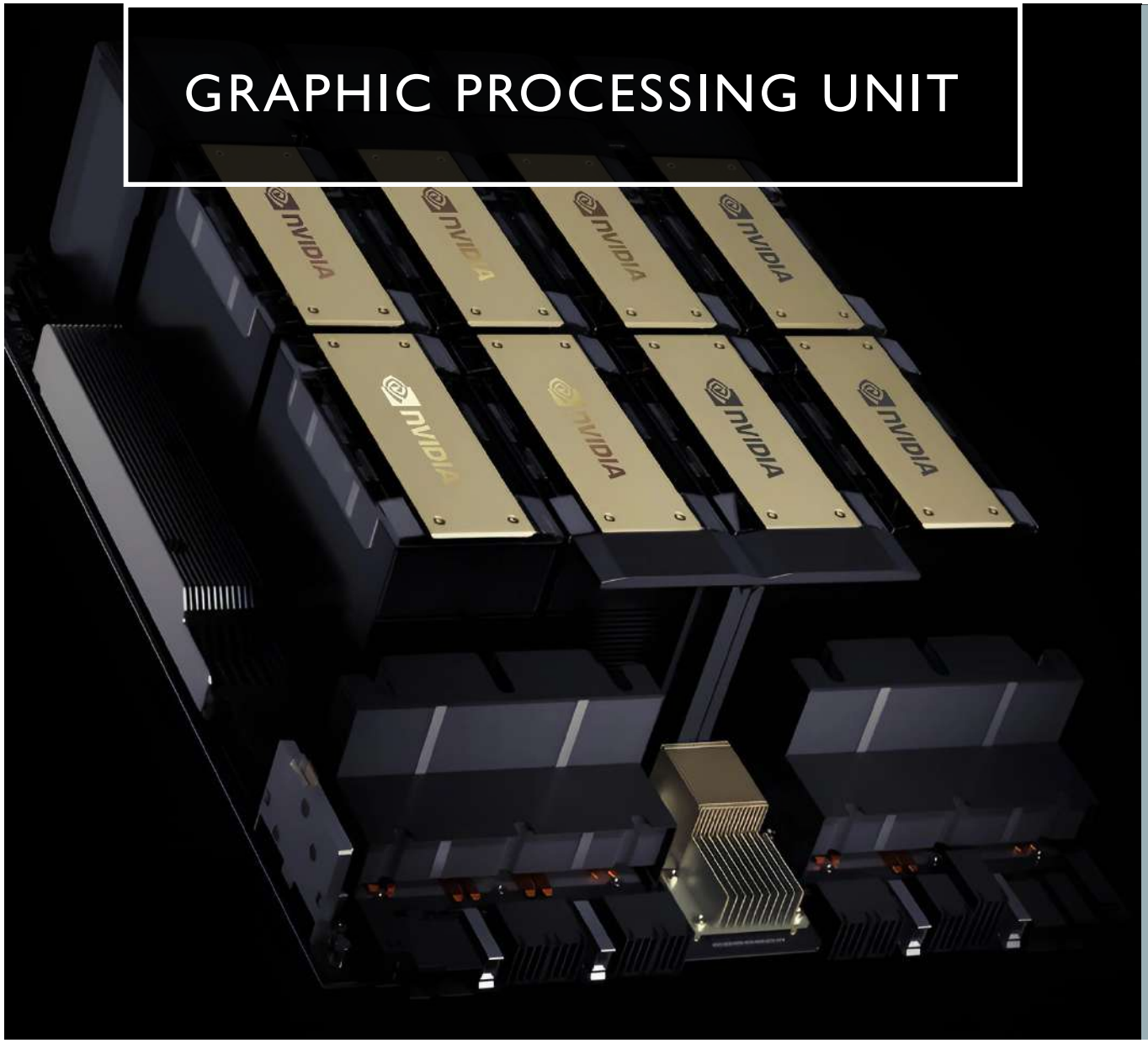


Figura 4 - Dall'immagine di input alle high-level features[39]





GRAPHIC PROCESSING UNIT



processori altamente specializzati che possono effettuare **calcoli intensivi e paralleli** molto velocemente e, al contempo, **gestire una vasta mole di dati**.

L'uso delle GPU ha permesso agli **sviluppatori di AI** di creare reti neurali artificiali molto più complesse ed efficienti,

la **GPU** può svolgere un **gran numero di compiti simultaneamente**: possiede molti core specializzati in diverse modalità di calcolo e può gestire **ingenti quantità di dati in parallelo**.

Oggi infatti esistono **GPU per l'AI** dotate di un'**alta efficienza nell'elaborazione** in parallelo di grandi set di dati, migliorando nettamente le prestazioni rispetto alle CPU

DEFINIZIONE E PANORAMICA DELL'INTELLIGENZA ARTIFICIALE GENERATIVA

- Algoritmi avanzati in grado di creare contenuti originali, come testo, immagini e musica, apprendendo da insiemi molto estesi di dati, distinguendosi così dall'intelligenza artificiale tradizionale che analizza o classifica principalmente i dati esistenti.



MODELLI LINGUISTICI DI GRANDI DIMENSIONI

- I sistemi di intelligenza artificiale che generano testo, come il famoso ChatGPT, sono basati su modelli linguistici di grandi dimensioni (LLM). Gli LLM sono addestrati su un vasto corpus di dati per rispondere a domande o eseguire attività basate su probabilità statistiche. Invece di cercare e sintetizzare le risposte, utilizzano modelli matematici per prevedere la parola successiva o l'output più probabile.

COSA VUOL DIRE GRANDE???

- Questi modelli sono “large” (grandi) in due sensi principali:
- **Dimensione del modello**: Gli LLM contengono un numero enorme di parametri, spesso nell’ordine di miliardi o addirittura trilioni. Questi parametri sono i “pesi” che il modello utilizza per processare e generare il linguaggio.
- **Quantità di dati di addestramento**: Questi modelli sono addestrati su dataset di dimensioni colossali, che possono includere libri, articoli, pagine web e altri testi in diverse lingue.



MODELLI DEL LINGUAGGIO: CAPACITÀ SOVRUMANE O PAPPAGALLI STATISTICI?

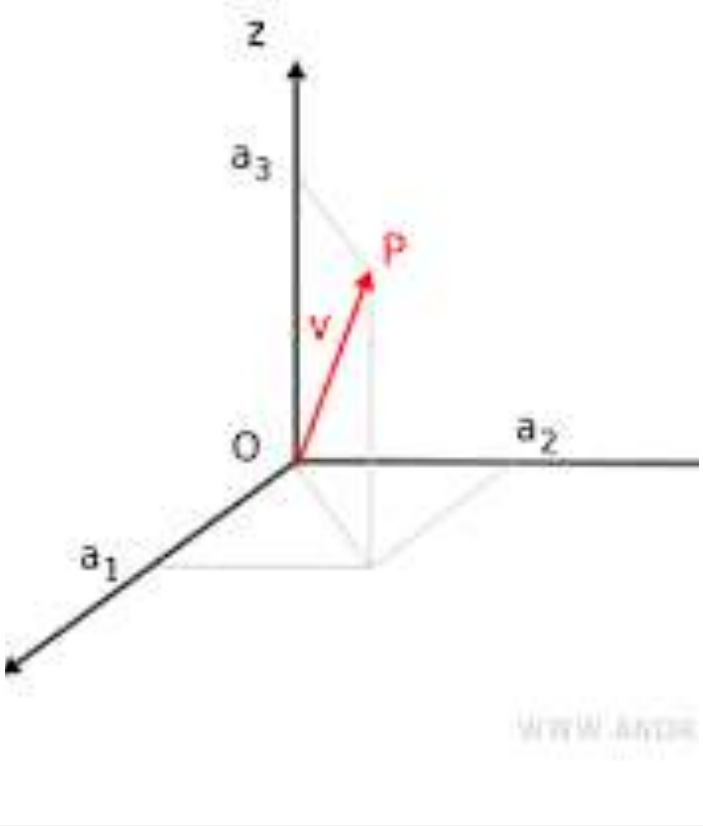
Il modello GPT-3 è stato addestrato su 45 terabyte di testo raccolto da diverse fonti online, una quantità che richiederebbe oltre 600 anni per essere letta dal più veloce lettore umano

(il signor Howard Berg, che appare nel Guinness World Record per essere riuscito a leggere 25.000 parole al minuto).

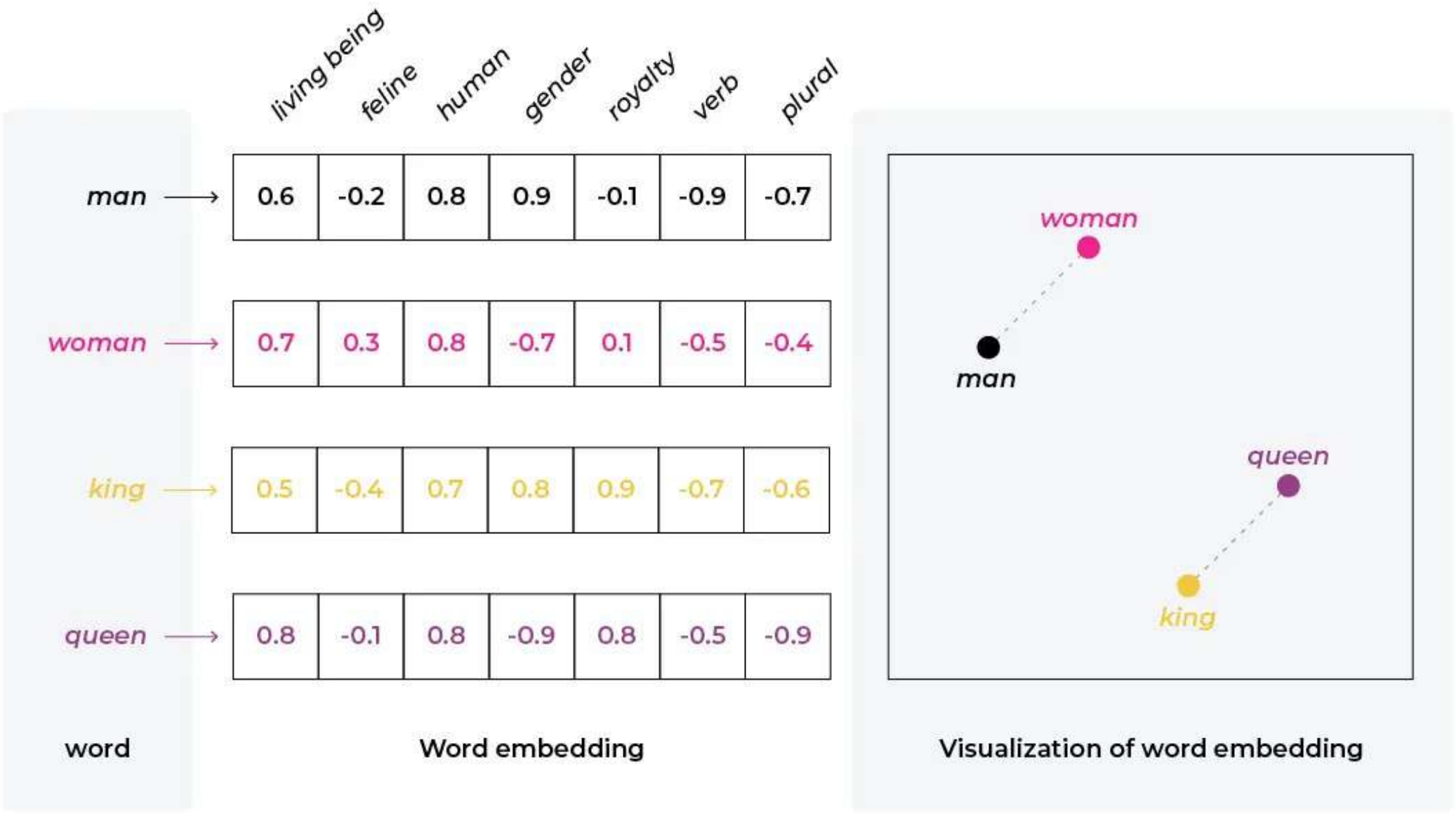

Gemini
deepseek

LLM

Il **word embedding** (tradotto letteralmente *immersione di parole*), anche conosciuto come rappresentazione distribuita delle parole, permette di memorizzare le informazioni sia semantiche che sintattiche delle parole partendo da un corpus non annotato e costruendo uno spazio vettoriale in cui i vettori delle parole sono più vicini se le parole occorrono negli stessi contesti linguistici, cioè se sono riconosciute come semanticamente più simili (secondo l'ipotesi della semantica distribuzionale).



12 K dimensioni


living being
feline
human
gender
royalty
verb
plural
man
0.6
-0.2
0.8
0.9
-0.1
-0.9
-0.7
woman
0.7
0.3
0.8
-0.7
0.1
-0.5
-0.4
king
0.5
-0.4
0.7
0.8
0.9
-0.7
-0.6
queen
0.8
-0.1
0.8
-0.9
0.8
-0.5
-0.9
word
Word embedding
woman
man
queen
king
Visualization of word embedding

COSA NON FA UN LLM?

NON comprende il linguaggio. È solo un motore predittivo.

NON comprende i fatti. Il modello prevede solo il token più probabile successivo nella sequenza in corso.

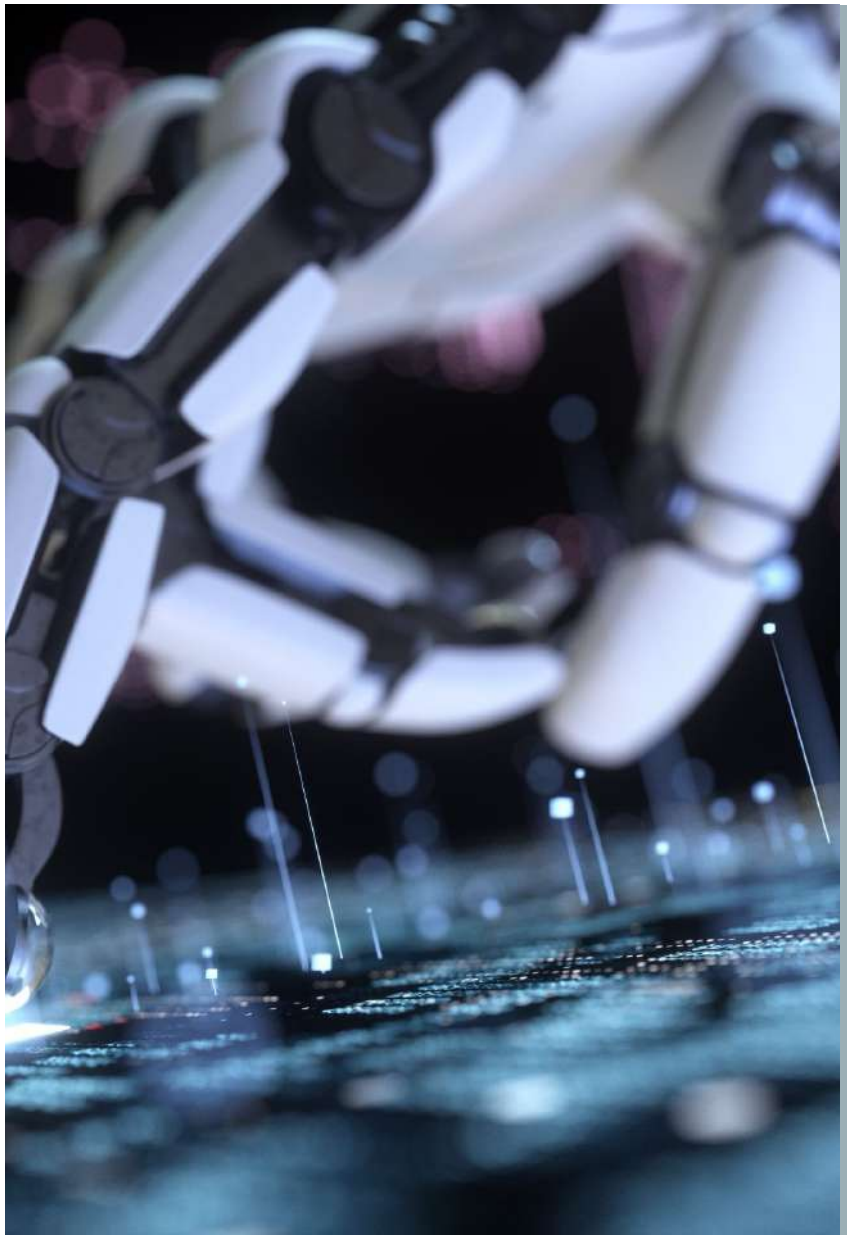
NON comprende le buone maniere, le emozioni o l'etica. L'output è semplicemente il risultato dei dati di addestramento guidati dai prompt forniti.

disegnami un'immagine di un gatto su un tavolo con una bottiglia di latte che gocciola



Ecco l'immagine del gatto sul tavolo con la bottiglia di latte che gocciola! 🐱🥛 Che te ne pare?





ATTACCHI CYBER GUIDATI DA AI

AI-DRIVEN CYBERATTACKS

- Gli attacchi cyber guidati dall'IA utilizzano metodi di IA e apprendimento automatico per automatizzare, accelerare e migliorare varie fasi di un attacco.
- Questi attacchi possono:
  - identificare vulnerabilità,
  - implementare campagne lungo specifici vettori di attacco,
  - stabilire backdoor nei sistemi,
  - manomettere o esfiltrare dati,
  - interrompere le operazioni.

TASSONOMIA DELLE MINACCE CYBER GUIDATE DALLA IA

