INTELLIGENCE E INFOSFERA

Strategie per la sicurezza nazionale in mondo governato dall'Intelligenza Artificiale

Fabio Vanorio

Unimarconi
LA PRIMA UNIVERSITÀ DIGITALE ITALIANA

UNIVERSITÀ DELLA CALABRIA

INTELLIGENCE LAB

Geopolitica dell'Infosfera

Paolo Savona e Fabio Vanorio

Unimarconi
LA PRIMA UNIVERSITÀ DIGITALE ITALIANA

UNIVERSITÀ DELLA CALABRIA

INTELLIGENCE LAB

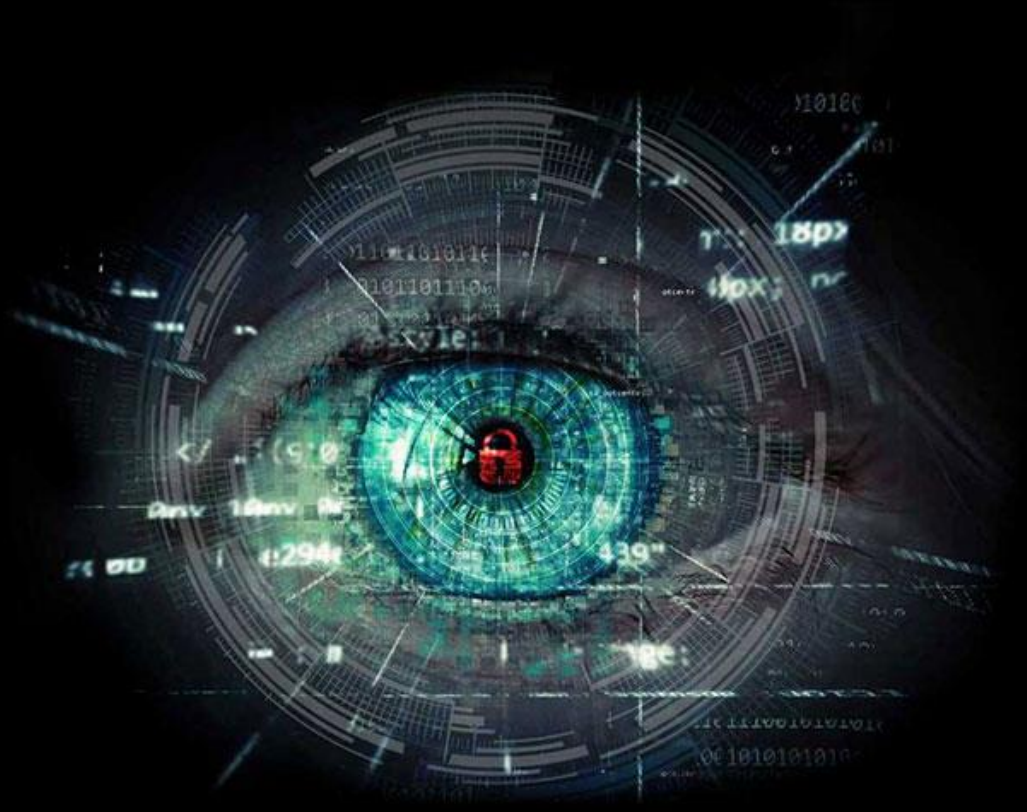
Geopolitica dell'Infosfera

Paolo Savona e Fabio Vanorio

CONTENUTI

CONTENUTI

CONTENUTI



Disclaimer

Fabio VANORIO

Dirigente del Ministero degli Affari Esteri e della Cooperazione Internazionale, attualmente in servizio presso l'Ambasciata d'Italia a Bruxelles.

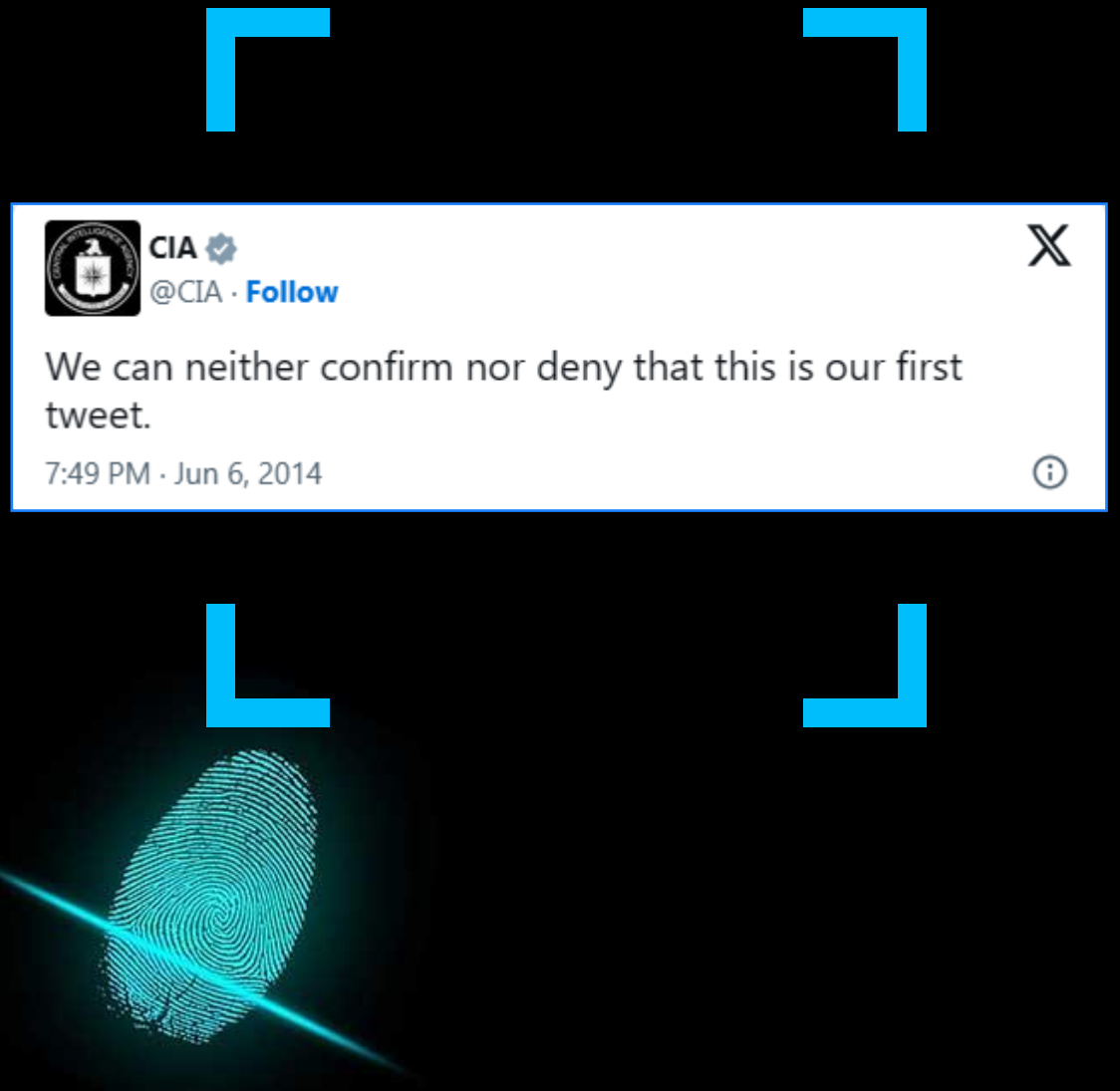
I contenuti di questa presentazione rappresentano **opinioni personali** e non impegnano in alcun modo il Ministero degli Affari Esteri e della Cooperazione Internazionale.

CONCETTI INTRODUTTIVI

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

In che modo l'Infosfera, ossia l'insieme delle tecnologie immersive della Quarta Rivoluzione Industriale, ha un impatto sull'Intelligence e sulla tutela della sicurezza nazionale?

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)



PRIMO TWEET DELLA CIA

Il testo utilizzato nel tweet è un gioco di parole basato sulla famigerata «**risposta Glomar**», una tattica utilizzata dalla CIA fin dagli anni Sessanta. A fronte di richieste di informazioni, la risposta Glomar non conferma, né smentisce, mantenendo sempre un'ambiguità a tutela della segretezza.

Il tweet è una svolta rispetto alla consueta postura prevalentemente rivolta alla clandestinità => dimostrazione di Langley di una forte volontà di engagement => **67.000 follower nel giro di un'ora dall'ingresso in X.**

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

PRIMO TWEET DELL'ASD

Analogo esordio lo ha realizzato l'agenzia di SIGINT australiana. L'importanza dell'ASD è cruciale in quanto rappresenta la frontiera, in termini di SIGINT (Signal Intelligence) dell'**Alleanza Five Eyes** contro la Cina.


WHAT IS FIVE EYES?
MEMBERS

"INTELLIGENCE & INFOSFERA"

(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

INTELLIGENCE E BIG DATA

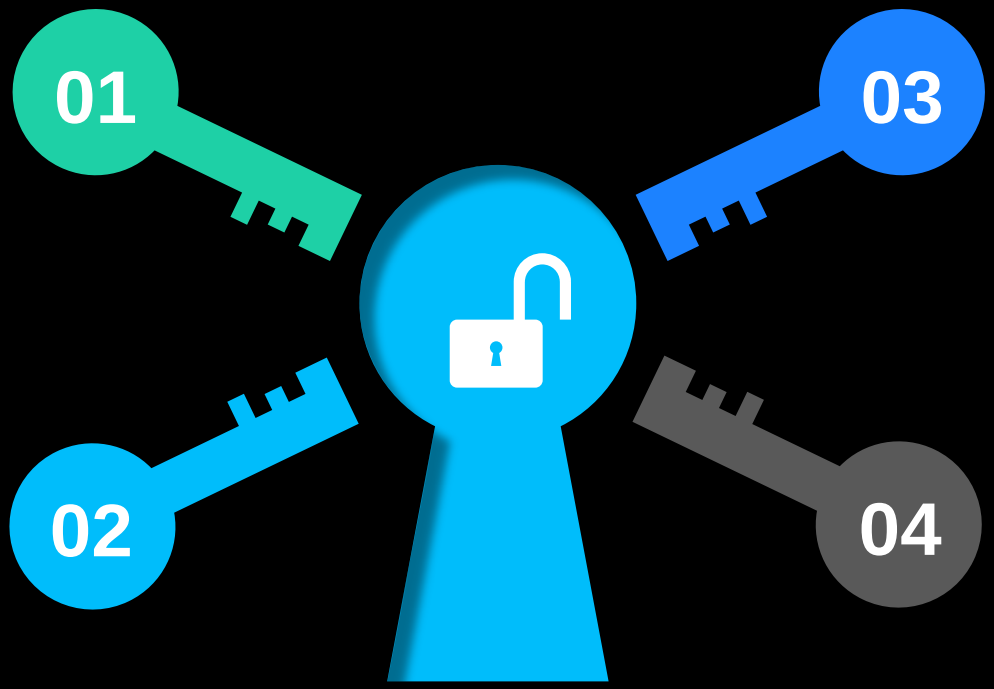
"INTELLIGENCE & INFOSFERA"

(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

SIGNIFICATI DELL'INTELLIGENCE

CONOSCENZA

ATTIVITA' E PRODOTTI DI ORGANIZZAZIONI CHE PRODUCONO CONOSCENZA



ORGANIZZAZIONE CHE PRODUCE CONOSCENZA

SUPPORTO COGNITIVO AL DECISORE

Intelligence Cycle

1.
PIANIFICAZIONE E DIREZIONE

2.
RACCOLTA INFORMATIVA

3.
TRATTAMENTO

4.
TRASFORMAZIONE IN "*ACTIONABLE INTELLIGENCE*"

La quantità e la varietà di informazioni è in continua espansione

- **2014** => entro il 2020 nell'universo digitale ci saranno tanti bit quante stelle nell'universo fisico;
- **2019** => il numero di byte sarà 40 volte le stelle nell'universo osservabile.
- **2026** => più di 220 miliardi di Terabyte di dati aggiunti ogni anno (quasi tre volte gli 83 miliardi di Terabyte prodotti nel 2021, con una crescita del 21% all'anno)

Le stime sul numero di dispositivi connessi a Internet ha superato quello della popolazione globale: nel 2022, il numero di dispositivi connessi era di 23,6 miliardi; nel 2028, la stima è di 45,8 miliardi.

BIG DATA

Immensi Patrimoni di Dati

Progressi tecnici nell'archiviazione, velocità di raccolta e analisi dei dati

Dati come elementi mutanti

Dati raccolti continuamente, infinitamente collegabili in rete e altamente flessibili.

Le 6V dei Big Data

Volume (aumento della potenza di calcolo), **Velocità** (nuova progettazione dei database), **Varietà** (archiviazione distribuita), **Veridicità** (certezza e coerenza dei dati), **Variabilità** (i dati sono crescenti, in diversi formati e da contesti differenti), e **Valore** (intuizioni sui dati e dai dati)

Nell'analizzare informazioni in modo rapido e accurato, date le limitate capacità umane, non c'è abbastanza tempo per dare un senso a tutti i dati e svolgere le altre attività necessarie del ciclo di intelligence.

IA

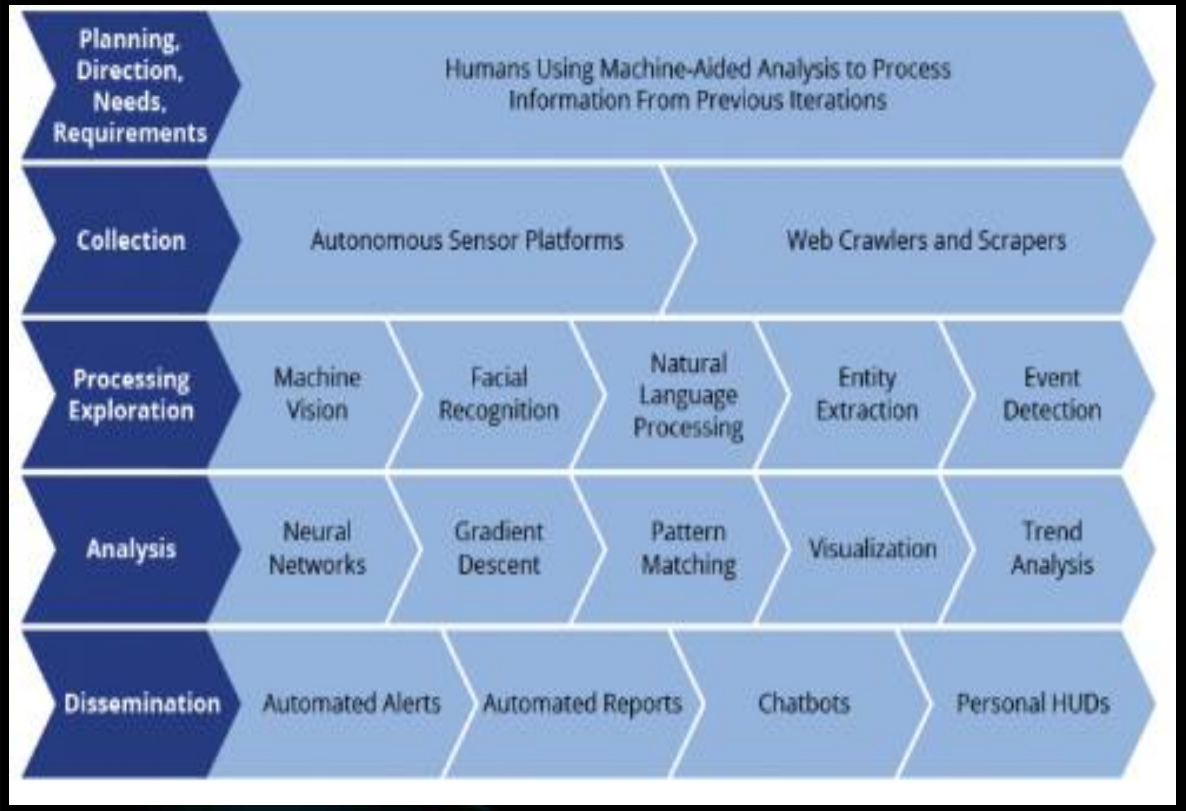
Un analista "all-source" supportato da sistemi IA può risparmiare fino a 364 ore o più di 45 giorni lavorativi all'anno rispetto all'analogo svolgimento di attività senza l'ausilio dell'IA

"INTELLIGENCE & INFOSFERA"

(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

Intelligence Cycle potenziato con l'IA

STRUMENTI



FLUSSO

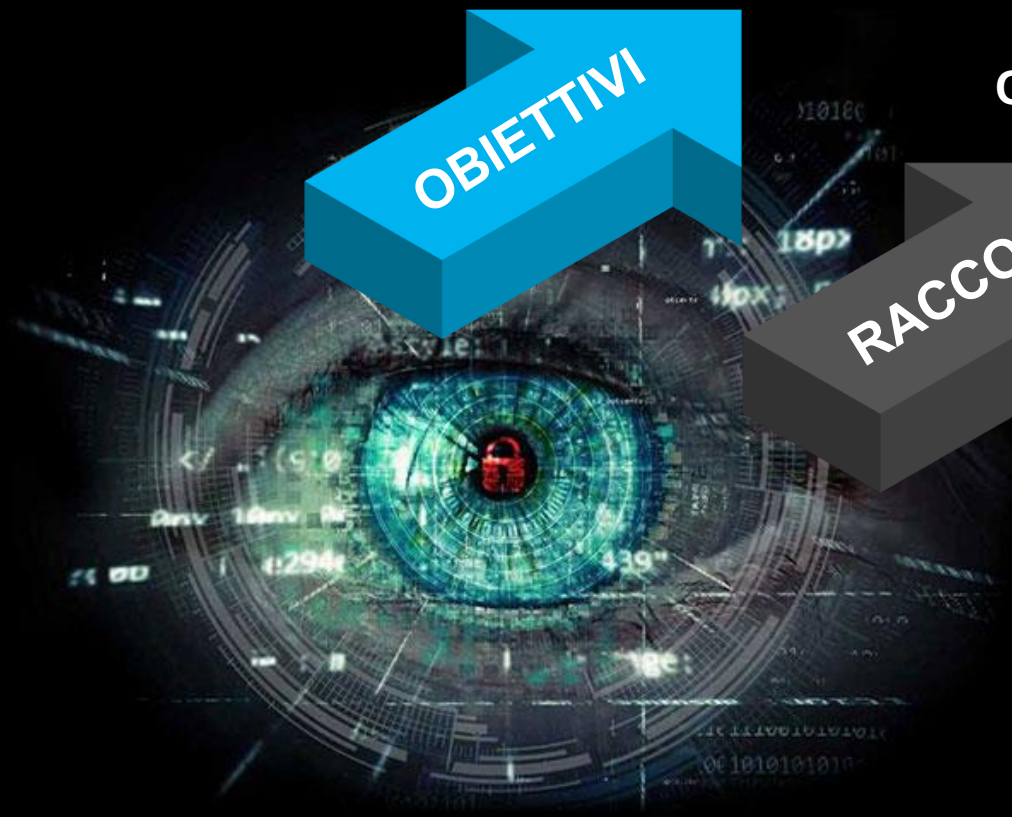
INTELLIGENCE E ARTIFICIAL INTELLIGENCE

DEFINIZIONE DI “SISTEMA DI INTELLIGENZA ARTIFICIALE” SECONDO IL NUOVO REGOLAMENTO DELL’UNIONE EUROPEA (“AI ACT”)

*«sistema basato su **macchine**, progettato per operare con vari livelli di **autonomia**, che può mostrare capacità di **adattamento** dopo l'implementazione e che, per obiettivi espliciti o impliciti, **deduce**, dagli input ricevuti, come **generare output** quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»*

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

COME L'INTELLIGENZA ARTIFICIALE CAMBIA L'INTELLIGENCE



CAMBIA CIO' CHE SPIAMO

OBIETTIVI

CAMBIA COME SPIAMO

RACCOLTA

CAMBIA COME OSTACOLIAMO

CONTRASTO

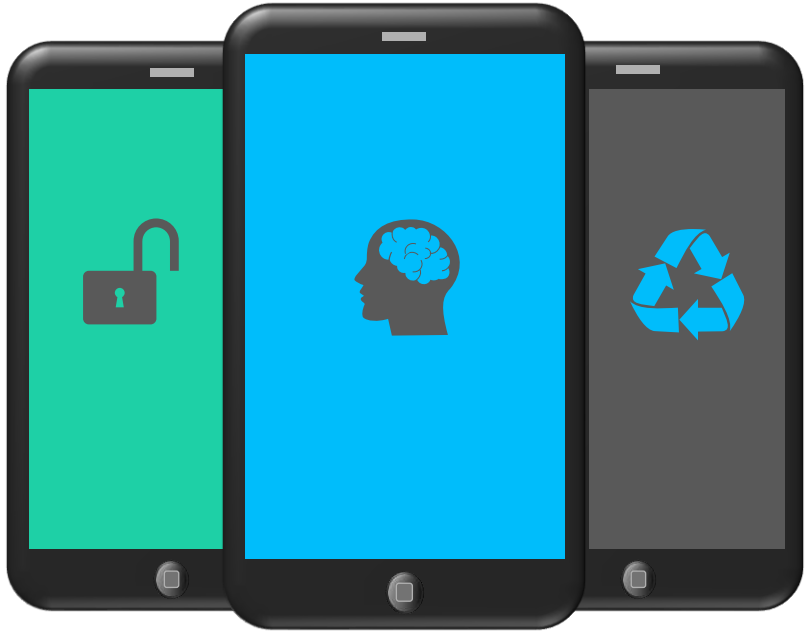
CAMBIA DOVE SPIAMO

MISSIONE

VETTORI DIREZIONALI DELLA QUARTA RIVOLUZIONE INDUSTRIALE NELL'INTELLIGENCE

AUTONOMIA

Rimuove gli umani dal ciclo intelligence, rendendo possibile avere entità differenziate che agiscono in operazioni c.d. "in sciame".



TECNOLOGIE UBIQUE

Consentono una interazione senza soluzione di continuità tra umani e oggetti capaci di sentire, comunicare, analizzare e agire.

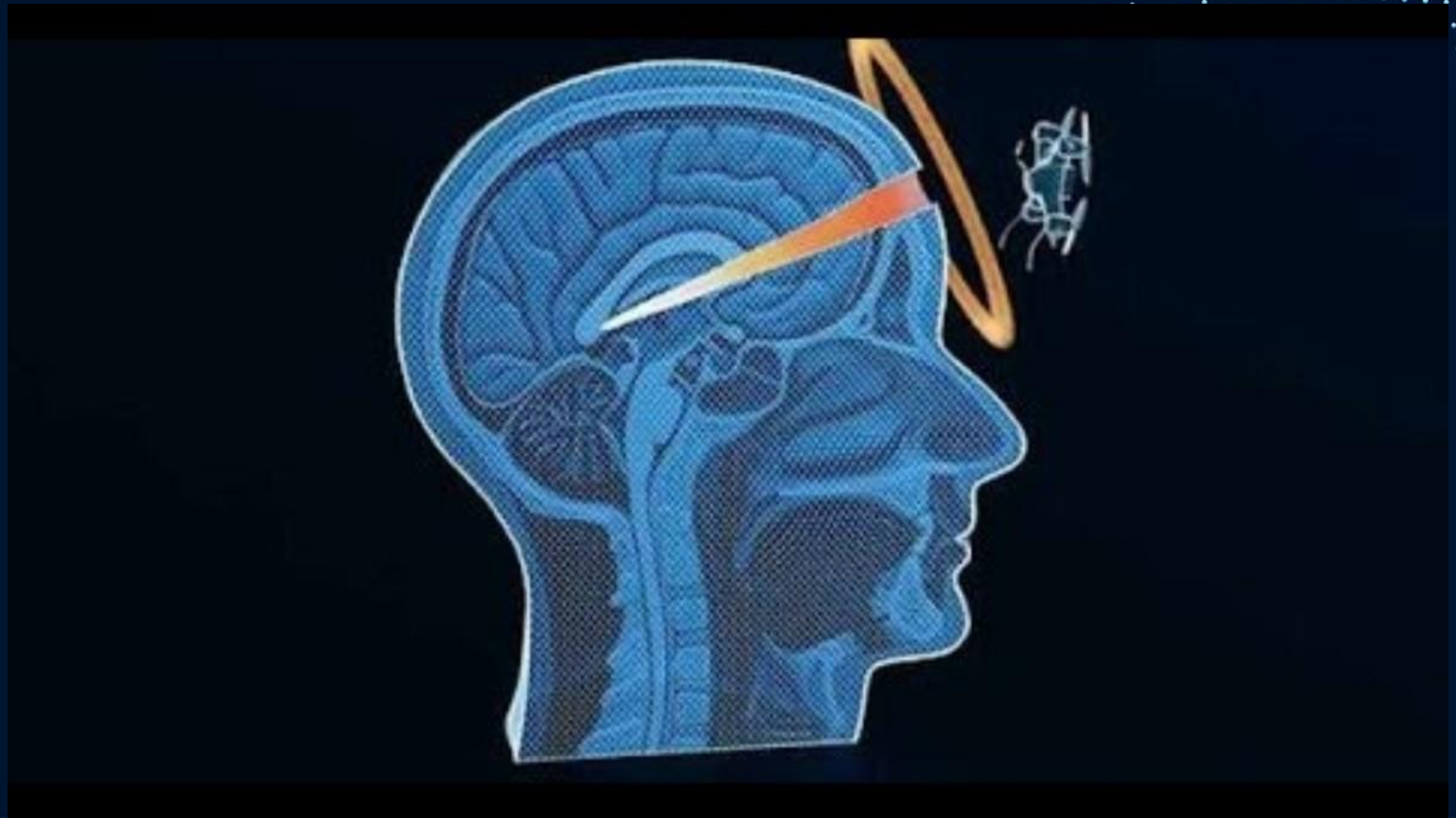
IA

*Tecniche di intelligence **aumentate con l'IA** sono fondamentali nella raccolta di informazioni, in particolare, nel SIGINT, di impronte dello spettro elettromagnetico e di comunicazioni da tracciare e cifrare. La rimozione degli umani dal ciclo è utile a gestire, in maniera puramente tecnica, l'intera scala e la complessità dell'operazione.*

"INTELLIGENCE & INFOSFERA"

(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

WARFARE BASATO SU DRONI POTENZIATI CON IA



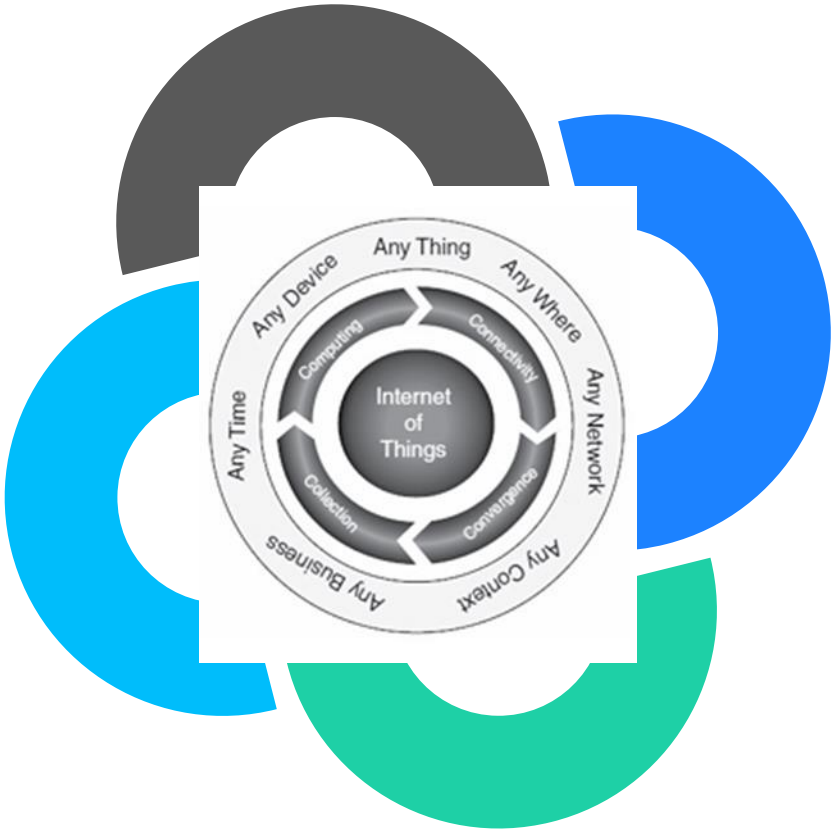
TECNOLOGIE UBIQUE

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

CALCOLO UBIQUO

L'IoT è una rete di dispositivi interagenti tra loro (smart things), identificabili in modo univoco tramite indirizzi IP (Internet Protocol), e rappresentabili in termini di A e C, dove le A riflettono il concetto di ubiquità dell'IoT (Any Thing, Any Where, Any Time, Any Network) e le C le sue caratteristiche (Connectivity, Computing, Convergence).

L'IoT collega gli oggetti fisici attraverso reti digitali. Fonde sensori, processori, archiviazione dati, algoritmi intelligenti e attuatori per osservare e modificare fisicamente il mondo e le persone che lo abitano.



Il conflitto tra Russia e Ucraina iniziato il 24 febbraio 2022 rappresenta il passaggio di Internet da tecnologia trasformativa a tecnologia di guerra con un impiego diffuso dell'intero spettro tecnologico caratterizzante la Quarta Rivoluzione Industriale, in particolare nell'impiego di Big Data in sistemi di IoT militari.

L'IoT militare sconta due problemi, uno di connettività, l'altro di decisione.

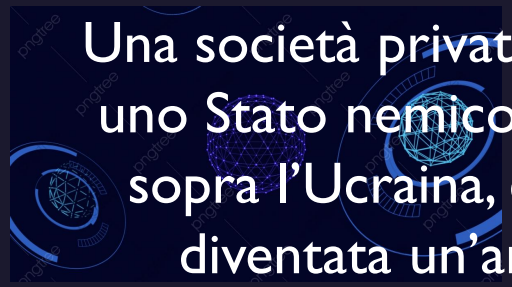
TEMPORAL INTELLIGENCE

Nuovo paradigma di intelligence che contempla la trasformazione da parte dell'IoT delle discipline di raccolta consolidate (HumInt, SigInt, MasInt, ImInt)

Dal monitoraggio degli individui è possibile ripercorrere le attività svolte e conoscere immagini, video, suoni, indirizzi IP, posizionamento geo-spaziale e simili a lui riconducibili attraverso dispositivi IoT a lui collegati o che in qualche modo l'hanno tracciato

Applicazione IoT al SIGINT spaziale
Case Study: Starlink nel conflitto russo-ucraino

Nel conflitto russo-ucraino, il vero cambiamento di paradigma tecnologico nello spettro militare è stato rappresentato dall'intervento operato da Starlink, società di Elon Musk.



Una società privata ha consentito (e sta consentendo) a uno Stato sovrano di potersi contrapporre a uno Stato nemico grazie alla concessione di uso di un gruppo di satelliti che volano fino a 130 miglia sopra l'Ucraina, consentendo l'accesso a Internet ad alta velocità, un'alleanza Stato-mercato che è diventata un'ancora di salvezza per Kiev, sia sul campo di battaglia che nella guerra mediatica .

Applicazione IoT al SIGINT spaziale
Case Study: Starlink nel conflitto russo-ucraino

Finora, il problema con le comunicazioni spaziali è stato sempre connesso:

- al costo insostenibile dell'infrastruttura,
- alla sua eccessiva visibilità al nemico (e quindi alla sua vulnerabilità),
- al suo essere causa di ritardi significativi alla rete.

Poiché la maggior parte dei satelliti si muove in orbita, essi possono ricevere dati solo mentre si trovano sopra un'unità che desidera trasmettere e non possono poi spingere i dati verso il basso fino a quando non si trovano sopra la stazione base ricevente desiderata. **Condividere i dati tra i satelliti è possibile, ma ogni collegamento aggiuntivo nella rete impone più ritardi tra la trasmissione e la ricezione.**

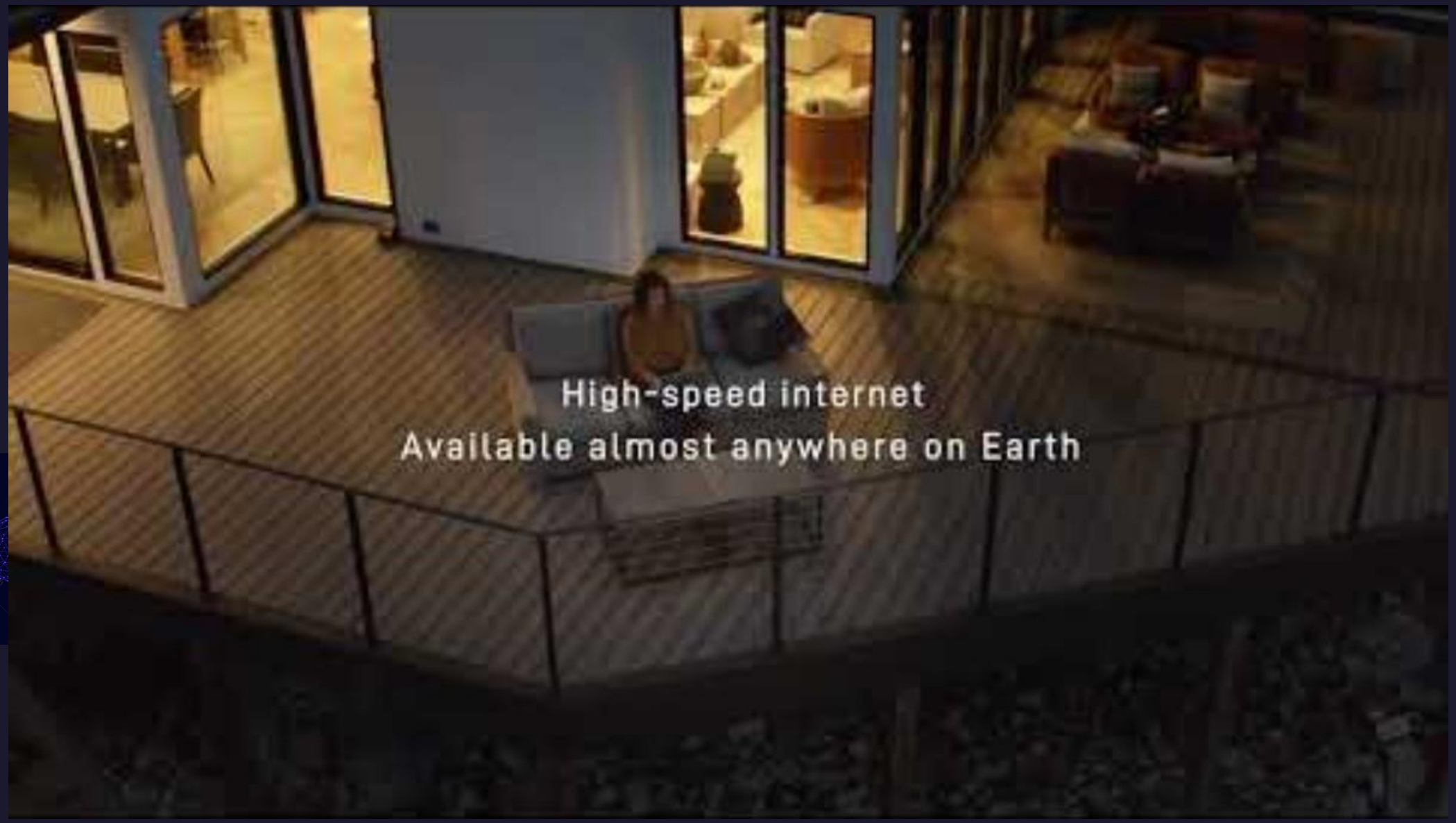
Applicazione IoT al SIGINT spaziale
Case Study: Starlink nel conflitto russo-ucraino

L'aspetto che distingue Starlink è il suo impiego di una nuova generazione di satelliti in orbita bassa (LEO), funzionanti come **una costellazione**.

A differenza dei tradizionali satelliti ad alta orbita, che ruotano a migliaia di chilometri sopra la terra, si librano sopra un punto del suolo e trasmettono segnali radio, la configurazione di Starlink rende più difficile, se non impossibile, la messa offline, perché un aggressore dovrebbe individuare tutti i satelliti, in una volta sola, per paralizzare l'intero sistema. Starlink, inoltre, è più adattabile rispetto alle alternative, perché il codice informatico di ogni dispositivo può essere rapidamente modificato in risposta a possibili hack.

“INTELLIGENCE & INFOSFERA”

(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)



Applicazione IoT al SIGINT spaziale
Case Study: Starlink nel conflitto russo-ucraino

L'intervento di Elon Musk nel conflitto Russia-Ucraina può essere ricondotto a un segno distintivo dell'influenza effettiva con cui attori non statali causano colpi importanti al modello di relazioni internazionali, risultato combinato dell'accelerazione digitale e della decentralizzazione del potere globale.

Tecnologia, Big Data e le relative capacità di elaborazione e analisi sono diventati fonti fondamentali di nuova influenza. Laddove la distribuzione del potere globale ha riguardato anche gli attori non statali (dotati di risorse e conoscenza più concentrate rispetto a quanto disponibile agli Stati in maniera frammentata) è principalmente causato dalle vistose mancanze mostrate dalla governance globale a fronte dei maggiori rischi.

INFOSFERA E SEGRETEZZA

INFOSFERA E SEGRETEZZA

I big data aumentano rischi e conseguenze delle violazioni della sicurezza, mettendo in discussione le pratiche fondamentali dell'archiviazione dell'intelligence, dei NOS e della compartimentazione delle informazioni.

Il rischio associato alla digitalizzazione delle informazioni è che volumi maggiori di intelligence sensibile siano trasmessi a velocità elevata a livello mondiale in un modo impossibile prima della digitalizzazione.

Un impatto chiave del panorama dei big data è che molto poco rimarrà segreto per sempre. La crescente declassificazione sta cambiando la pratica della segretezza nel processo decisionale dell'intelligence e della sicurezza nazionale.

Il processo decisionale nella sicurezza nazionale si svolge sempre più spesso nel settore privato, in particolare all'interno delle aziende tecnologiche. Ciò crea dispersioni nella sicurezza e aumenta le vulnerabilità.

I Big data hanno ampliato la «superficie di attacco» in settori ed entità commerciali, ognuno dei quali ha la capacità di influenzare il processo decisionale in materia di sicurezza nazionale del governo, dell'impresa, dell'industria.

INFOSFERA E OPERATIVITA’

INFOSFERA E OPERATIVITA'

L'abbondanza di dati cambia il significato di "conoscere" e quindi le lacune nella conoscenza; aumenta l'incertezza nelle valutazioni di intelligence; cambia il modo in cui l'intelligence viene compresa dai decisori.

L'intelligence utile è contestuale, cioè consapevole di ciò che sta accadendo. I "piccoli" dati segreti, difficili da ottenere e in grado di cambiare interi scenari, continueranno a svolgere un ruolo cruciale.

Per un analista, il valore maggiore dell'IA deriva dal c.d. "dividendo dell'automazione", ossia dai modi migliori in cui utilizzare il maggiore tempo a disposizione grazie all'alleggerimento del carico di lavoro.

L'analista fornisce all'IA un argomento lasciando la generazione automatica di mappe o immagini, la predisposizione di outline rilevanti per un briefing e di brevi riassunti degli eventi di fondo.

Con i big data si passa da un'attività incentrata sulla raccolta di segreti alla ricerca di un equilibrio tra sensing (capacità di osservare) e sense-making (capacità di orientare).

La competizione tra analisti diventerà ancora più serrata tra chi è in grado di aggiungere valutazioni in quanto conoscitore degli argomenti in trattazione, e chi è un mero collettore e trasmettitore di informazioni pulite e commentate.

Infosfera e Analisi Operativa

Solo l'analista ha consapevolezza dei contenuti dei documenti originali.
Lavorando con sistemi di IA, è suo il compito di mantenere separate le diverse parti. Facendo questo, l'analista filtra il lavoro dell'IA arrivando ad evidenziare il valore aggiunto dell'IA al proprio documento.

La qualità di un vero analista intelligence è nella capacità di discernere da dove proviene cosa, riuscendo in tal modo a tutelarsi dalle strumentalizzazioni esterne.

In passato, la creazione e l'aggiornamento di complessi modelli di comportamento richiedeva mesi, con un conseguente lungo ciclo di intelligence. Oggi l'analisi avviene più rapidamente, a un passo dal tempo reale. Analisti intelligence che dispongono di modelli di IA in grado di simulare rapidamente anche scenari complessi sono in grado di rispondere immediatamente ai responsabili delle decisioni.

SFIDE NELL'ANALISI OPERATIVA GENERATE DALL'IA

Fiducia nei risultati dei Modelli di IA

Le organizzazioni devono convalidare i risultati dell'IA in modo che gli analisti possano avere fiducia nel loro utilizzo.

Chiarezza nel ruolo dell'IA nell'Organizzazione

Occorre evitare di investire in "tecnologie vuote", ovvero di utilizzare l'IA senza avere accesso ai dati di cui ha bisogno.

Fiducia tra Analisti e IA

Gli analisti nutrono una comprensibile riluttanza a dare fiducia a qualcosa che non possono spiegare e difendere.

INFOSFERA E CONTROSPIONAGGIO

Infosfera e Controspionaggio

Elementi iniziali di un'attività di CS sono:

- la definizione del set di asset da tutelare;
- l'area geografica o i settori dell'economia, di riferimento;
- la specifica delle rispettive vulnerabilità di tali asset;
- eventuali mitigazioni in atto delle vulnerabilità stesse.

Opzioni per sterilizzare/sfruttare attività ostili:

- reclutamento di fonti già reclutate da operativi stranieri ("agenti doppi");
- espulsione sia di cittadini stranieri sia di diplomatici stranieri;
- indottrinamento e assistenza nei confronti di individui/organizzazioni oggetto di una intelligence ostile.

L'unica costante è <u>la perenne osservazione tra le parti</u>.

Infosfera e Controspionaggio

Nel caso di asset ad elevato contenuto di Intelligenza Artificiale, obiettivi di CS sono:

1. come proteggere il contenuto di IA in asset nazionali da una sottrazione/corruzione da parte di agenti stranieri ostili?
2. come salvaguardare la collettività da un impiego ostile di IA nei suoi confronti da parte di agenti stranieri?

Aspetti significativi del rapporto tra IA e CS:

- stretta dipendenza dei sistemi di IA dai Big Data
- Superiorità temporale;
- Potenza geopolitica derivante.

Nuova Equazione di Potenza Geopolitica

IA + Big Data + Calcolo ad Alta Velocità

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

La natura della potenza che IA, Big Data ed elaborazione ad alta velocità producono è infinita, limitata solo dai ritardi nelle decisioni umane. Questa potenza viene esercitata attraverso tre concetti, tra loro interdipendenti e alla base delle attività di controspionaggio in un sistema di IA: comprensione, previsione e manipolazione di individui e gruppi.

Comprensione di individui/gruppi

La sorveglianza all-source rende disponibile una ricchezza di dettagli per ogni individuo su associazioni familiari, politiche, professionali, religiose e sessuali.

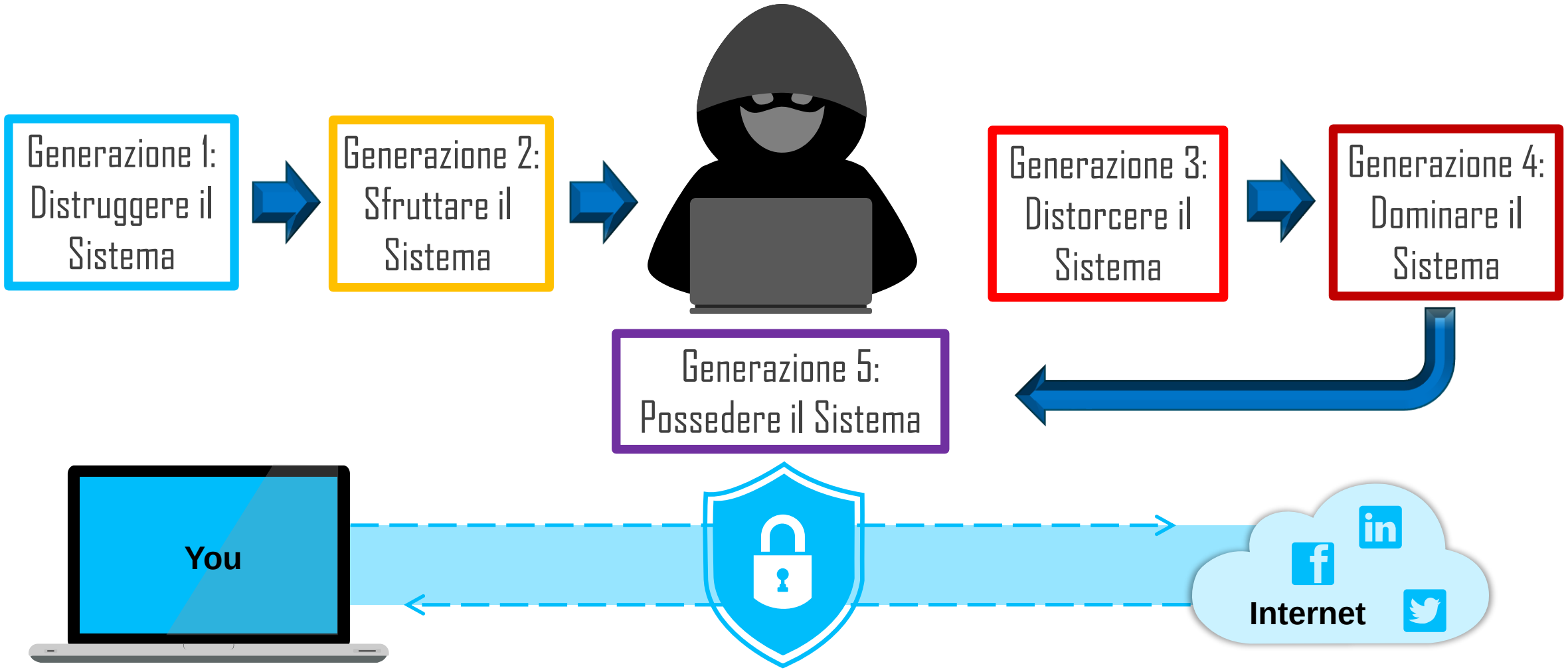
Previsione di comportamenti di individui/gruppi

Controparti ostili traggono dagli stessi dataset, una previsione di pensieri e azioni della collettività target.

Manipolazione di individui/gruppi

- **offuscamento della realtà;**
- **sovraccarico dei sensi della collettività;**
- **disinformazione calibrata;**
- **alimentazione di animosità e paure.**

PROGRESSIONE GENERAZIONALE DELLE MODALITA' DI HACKING



"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

NUOVO TERRENO DI SCONTRO PER IL CONTROSPIONAGGIO

Le principali agenzie di intelligence si sono già adattate ad un nuovo terreno di scontro in cui il principale avversario sia una macchina, e non un essere umano.

Le spie di oggi hanno lo stesso problema di ieri: la necessità di essere invisibili. Cio' che è cambiato è l'avversario. Invece di ingannare le persone con documenti falsi e narrazioni fasulle ben impostate, gli agenti di oggi devono ingannare i computer capaci di scegliere una sola faccia in mezzo alla folla.

Le attuali difficoltà sono nel mantenere identità coperte nell'era del tracking digitale e dei social media. Se tramite il riconoscimento facciale, è possibile tracciare ogni movimento di ogni persona, questo rende difficile per un agente operare in maniera coperta. Cellule ostili identificano agevolmente sia agenti stranieri sia informatori locali, creando data set informativi sui comportamenti abituali di entrambi, presi individualmente e in coppia.

INFOSFERA E GUERRA COGNITIVA

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

GUERRA COGNITIVA

GUERRA COGNITIVA

I media online hanno acquisito il potere di trasferire il processo di disinformazione dal mondo virtuale al mondo reale. La manipolazione e la disinformazione oggi condizionano ogni partecipazione alla vita pubblica.

L'emergere della cultura digitale globale dell'alterità attraverso il targeting e il trolling sulle piattaforme online è causa di danni a livello sociale, economico e politico.

METAVERSO

interpretazione di Internet quale mondo virtuale, immersivo e solitario, utile nel mediare condotte agli antipodi quali, da un lato, il libero sfogo delle proprie opinioni, e dall'altro, la partecipazione garbata nei social media digitali

SUPREMAZIA COGNITIVA

Nella sfida cognitiva, le modalità di conflitto sono basate su idee, storie, narrazioni, virus evolutivi e attacchi epistemici.
Tipi di guerra cognitiva vengono deliberatamente progettati per confondere gli analisti e le forze sociali, per sfruttare le debolezze dei governanti, delle istituzioni e delle società nel loro complesso.

Il warfare cognitivo integra capacità cibernetiche, informative, psicologiche e di ingegneria sociale per raggiungere gli scopi. Sfrutta Internet e i social media per seminare il dubbio, introdurre narrazioni contrastanti, polarizzare l'opinione, radicalizzare i gruppi, e motivarli a realizzare atti che possono interrompere o frammentare la società.

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

SUPREMAZIA COGNITIVA

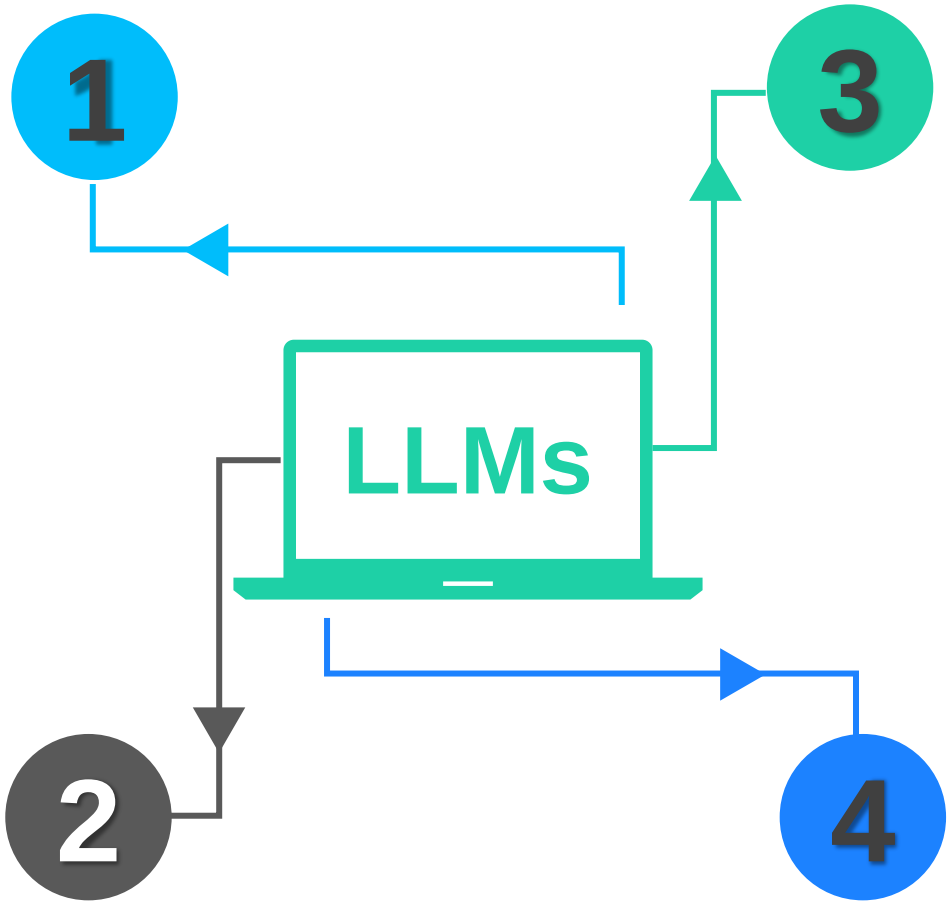
LA MENTE UMANA E' IL CAMPO DI BATTAGLIA

L'obiettivo è cambiare **ciò che la gente pensa**, **come pensa** e **come agisce**.
Il warfare cognitivo modella e influenza le credenze e i comportamenti individuali e di gruppo per favorire gli obiettivi tattici o strategici di un aggressore, fratturando e frammentando l'intera società, in modo che **non abbia più la volontà collettiva di resistere alle intenzioni di un avversario**.
Fake news, deep fakes, trojan horse e avatar digitali aiutano a creare nuovi sospetti che chiunque può sfruttare, riducendo la capacità degli esseri umani di mettere in discussione qualsiasi dato/informazione presentata, con una tendenza crescente verso il pregiudizio a scapito di un processo decisionale libero.

MODELLI DI LINGUAGGIO DI GRANDI DIMENSIONI E ANALISI INTELLIGENCE

MODELLI DI LINGUAGGIO DI GRANDI DIMENSIONI - LLMs

1. Rappresentano **uno dei principali strumenti di guerra cognitiva** in particolare nel conseguimento di **un livello competitivo di supremazia cognitiva**



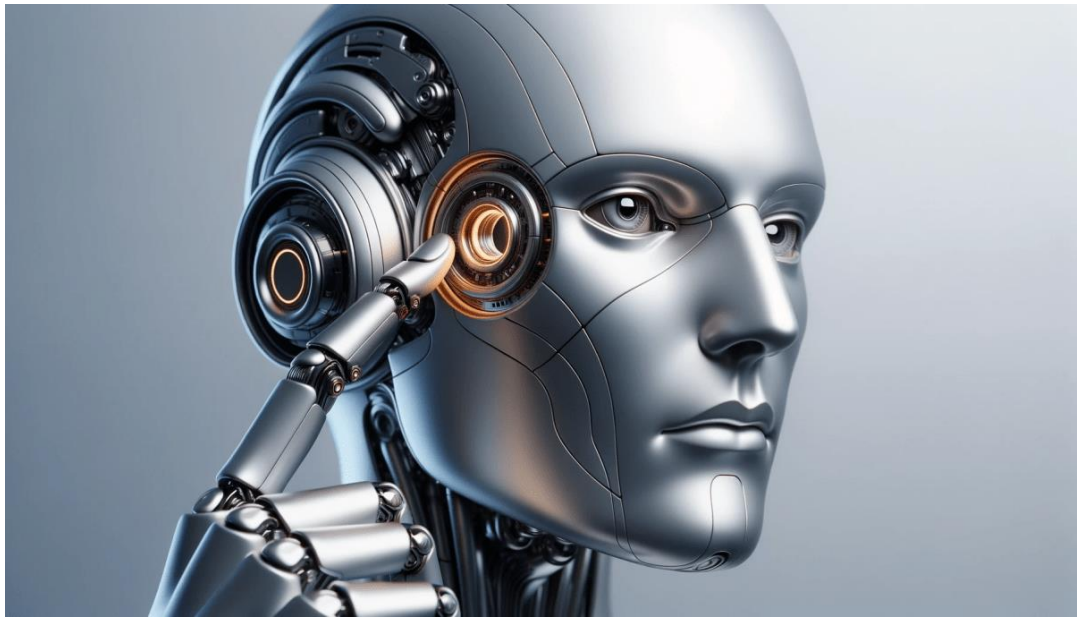
3. Hanno l'obiettivo di **emulare l'intelligenza cognitiva** dell'essere umano.

2. Attualmente, poiché le reti neurali sono intrinsecamente probabilistiche, **non hanno capacità di "inferenza pragmatica"** (ossia non codificano la comprensione di causa-effetto e le relazioni tra gli oggetti)

4. Per usi operativi (militari, polizia, intelligence, diplomatici) richiedono **un addestramento personalizzato su dati specifici**, in modo da garantire un livello più elevato di competenza nel dominio, accuratezza e pertinenza del testo generato

"INTELLIGENCE & INFOSFERA"
(Master in Intelligence, XIII Edizione, Università della Calabria, Anno Accademico 2023-2024)

IMPORTANTE



ADDESTRAMENTO DI UN LLM PER USO INTELLIGENCE

Caratteristiche che un LLM (basato sull'IA generativa) deve disporre per garantire rigore, fattualità e confidenzialità dell'analisi intelligence

Spiegare in modo affidabile come è arrivato alle sue conclusioni, fornendo fonti verificabili per le sue affermazioni

Per interrogare il patrimonio di conoscenza del modello è necessario identificare (1) **da quali fatti ha dedotto le informazioni che fornisce**, (2) **perché crede a quei fatti** e (3) **quali prove supportano e contraddicono le sue conclusioni**.

Disporre di meccanismi algoritmici e Big Data specifici per aggiornarsi in tempo reale con nuove informazioni.

I modelli commerciali sono addestrati su un corpus enorme di dati ma generico e limitato nel tempo (anche se per un lungo periodo). Di conseguenza, le informazioni più aggiornate sono confinate al momento dell'addestramento.

Supportare il ragionamento laterale e controfattuale

Il modello deve essere stato testato (1) nella sua capacità di pensiero creativo e non convenzionale (**ragionamento laterale**) mediante prompt che inducano all'associazione di idee apparentemente non correlate o l'esplorazione di possibilità inaspettate, sia (2) nella sua capacità di elaborare situazioni ipotetiche o alternative diverse dalla realtà considerata (**ragionamento controfattuale**).

CHATGPT

IA GENERATIVA

L'IA generativa si concentra sulla creazione di contenuti originali, come testi o immagini, sulla base degli input dell'utente. Questa branca dell'IA comprende modelli potenti come **ChatGPT** e **Bard** per la generazione di testi e **Dall.E**, **MidJourney** e **Stable Diffusion** per la generazione di immagini. Questi strumenti innovativi stanno democratizzando l'accesso all'IA, consentendo agli utenti di guidare le loro interazioni utilizzando il linguaggio umano di tutti i giorni.

Casi d'Uso di ChatGPT

La "G" di ChatGPT sta per «Generativo», il che significa che questo strumento di IA non si limita a copiare e incollare informazioni esistenti, ma **genera qualcosa di nuovo ogni volta che gli parliamo**.

Casi d'uso di ChatGPT possono essere:

- Recupero e riassunto delle informazioni
- Traduzione linguistica in tempo reale
- Formazione e sviluppo delle competenze
- Simulazione e pianificazione di scenari

Limiti nell'utilizzo di ChatGPT

ChatGPT non è stato progettato per trattare dati e/o informazioni sensibili e il suo utilizzo in tali contesti potrebbe portare a potenziali violazioni della sicurezza e compromettere dati critici. L'incapacità dell'IA generativa di distinguere tra informazioni classificate e non classificate la rende inadatta ad attribuire priorità nel trattamento di materiale riservato.

Modalità di utilizzo di ChatGPT

Per capire come funziona ChatGPT, è utile pensare a come gli esseri umani imparano e danno un senso al mondo. Quando leggiamo un libro, non memorizziamo le parole, ma ne costruiamo e ricordiamo il significato.

ChatGPT segue un approccio simile all'apprendimento del linguaggio. I suoi modelli linguistici sono stati alimentati con trilioni di parole e, invece di memorizzarle, ChatGPT ha ricavato il significato sotto forma di relazioni tra le parole.

Nei modelli linguistici di grandi dimensioni come ChatGPT, **queste relazioni sono chiamate "parametri"** e ognuno di essi rappresenta la comprensione di ChatGPT di come le parole si relazionano tra loro.

Meccanismi di comprensione di ChatGPT – 1/2

Attraverso il processo di addestramento, ChatGPT costruisce una complessa comprensione del linguaggio e delle relazioni tra le parole, consentendogli di generare risposte simili a quelle umane.

ChatGPT si nutre del contesto per fornire un'ipotesi istruita su ciò che dovrebbe essere detto successivamente. Maggiore è il contesto, migliore è la capacità di indovinare la parola successiva.

Ciò significa che **scrivere un singolo prompt non sempre genera il risultato migliore**. Un «approccio conversazionale» può aiutare ChatGPT a migliorare la comprensione del contesto e consentire di produrre risposte più pertinenti.

Meccanismi di comprensione di ChatGPT – 2/2

Una parte del set di dati di pre-addestramento di ChatGPT è stata estratta da **Reddit**, piattaforma online per la discussione di vari argomenti, usata per far lavorare il modello con un linguaggio molto umano.

L'utilizzo di un approccio basato su parole chiave o di un linguaggio robotico, come quello utilizzato per una ricerca su Google, non produce i risultati migliori con ChatGPT.

Per massimizzare il suo potenziale, invece, è necessario **un approccio conversazionale con ChatGPT**, come se stesse conversando con un essere umano.

Approccio conversazionale con ChatGPT

Step di costruzione di un approccio conversazionale con ChatGPT.

- Fornire il contesto, delineando le esigenze e aspettative. **Maggiore il numero di idee fornito, più ampio il contesto delineato, migliore l'output desiderato.**

- Dopo aver ricevuto la prima bozza, fornire a ChatGPT un **feedback**, indicando modifiche e miglioramenti desiderati in termini di esempi specifici, maggiori dettagli, rimozione/aggiunta di elementi.

La chiave è comunicare con ChatGPT come se fosse una persona, con chiarezza, sintesi e un tono colloquiale.

Prompt [Act As] – 1/3

Un vantaggio dell'impostazione di un gioco di ruolo con ChatGPT utilizzando un prompt "Act As" è **la coerenza del personaggio e del comportamento che dimostra durante la chat**.

Stabilendo il ruolo e le aspettative nel prompt di apertura, state essenzialmente istruendo ChatGPT sul personaggio e sul comportamento desiderato per l'intera conversazione.

Ciò consente di fornire più contenuti o argomenti e ChatGPT si atterrà costantemente al ruolo e alle aspettative comportamentali iniziali, rendendolo un modo efficiente ed efficace per richiedere assistenza o generare contenuti in un ambito specifico.

Prompt [Act As] – 2/3

Il modo migliore per imparare a impostare un gioco di ruolo perfetto con ChatGPT è quello di commettere errori, capire come il prompt avrebbe potuto essere migliorato e riprovare.

Sebbene esistano numerosi creatori di contenuti che sviluppano elenchi di prompt «Act As» precostituiti per un'ampia varietà di ruoli, questi prompt potrebbero non essere perfettamente adatti alle vostre esigenze specifiche o ai vostri casi d'uso.

Il mio consiglio è concentrarsi sul processo di apprendimento del modello per scrivere migliori prompt «Act As» che rispondano alle vostre esigenze specifiche.

Prompt [Act As] - 3/3

Comprendendo i principi che stanno alla base di un'efficace ingegnerizzazione dei prompt e affinandoli attraverso un processo iterativo, potrete creare **prompt personalizzati** che si allineino ai vostri obiettivi specifici e generino risposte accurate e pertinenti da parte di ChatGPT.

Investendo tempo e fatica nello sviluppo dei prompt, otterrete una comprensione più approfondita delle capacità e dei limiti di ChatGPT.

Affinare i prompt e fornire un contesto chiaro è essenziale per ottenere il massimo dalle interazioni con ChatGPT. Con la pratica dell'iterazione e del perfezionamento delle richieste, si svilupperà anche una migliore comprensione di come comunicare le nostre esigenze in generale.

Prompt [Format] - 1/3

Per capire come ottenere il meglio da ChatGPT è necessario non solo sapere **come chiedere i contenuti**, ma anche **come guidare la struttura dei contenuti stessi**.

[Format] è una tecnica di prompt engineering che consente di controllare le capacità di sviluppo dei contenuti di ChatGPT. Definita da OpenAI anche [Insert], prevede la costruzione di meta-prompt che danno luogo a output di qualità superiore e consentono di ridurre il numero complessivo di parole dell'output.

Riconoscendo il contenuto all'interno delle parentesi come un'istruzione separata, ChatGPT può generare risposte che si riferiscono a quel prompt, senza la necessità di un linguaggio riempitivo aggiuntivo.

Prompt [Format] - 2/3

Le basi di [Format] consistono nel creare dei segnaposto nel prompt che ChatGPT può riempire con contenuti appropriati.

Utente
"Ieri sono andato al negozio e ho comprato un po' di spesa. [*Descrivi un incontro interessante al negozio*]. Quando sono tornato a casa, ho iniziato a preparare la cena".

ChatGPT
Ieri sono andato a fare la spesa. [*Mentre giravo nel supermercato, ho incontrato un vecchio amico che non vedevo da anni.*] Quando sono tornato a casa, ho iniziato a preparare la cena.

Prompt [Format] - 3/3

Utilizziamo [Format] per decostruire e schematizzare un argomento. Questo è utile in vari aspetti dell'analisi intelligence, dalla stesura di report alla preparazione di briefing.

Prendiamo uno scenario argomentativo inerente **la valutazione delle potenziali conseguenze delle sanzioni economiche su un Paese**.

[Premessa 1: Condizione economica della Corea del Nord] «La Corea del Nord ha registrato una crescita economica costante nell'ultimo decennio, tuttavia, [*impatto delle sanzioni sull'economia della Corea del Nord*].»

[Premessa 2: La risposta internazionale] Considerando la struttura economica globale, [*possibili reazioni degli altri Paesi e delle organizzazioni internazionali alle sanzioni in Corea del Nord*].

[Sulla base delle Premesse 1 e 2, [*le potenziali conseguenze dell'imposizione di sanzioni economiche alla Corea del Nord*].

Intelligence Reporting con ChatGPT - 1/5

Lavorare nella Comunità Intelligence richiede spesso di passare al setaccio numerosi documenti per selezionare informazioni critiche o per ottenere una comprensione completa dell'argomento.

Passare in rassegna questi documenti richiede tempo e fatica.

Non condividete MAI con ChatGPT informazioni sensibili. Concentratevi invece sul suo utilizzo per aiutarvi solo con documenti open source.

Piuttosto che limitarsi a chiedere a ChatGPT di riassumere un documento (con risultati indubbiamente mediocri senza sfruttare appieno le sue capacità), si possono avanzare richieste migliori e più efficienti.

Intelligence Reporting con ChatGPT - 2/5

«Summary»
Summarize this press release:
(Press Release)

«Bullet Points»
Summarize this press release using bullet points:
(Press Release)

«Key Quotes»
Give me some key quotes from this press release:
(Press Release)

Intelligence Reporting con ChatGPT - 3/5

«Riassunto di facile comprensione»
Summarize this press release using language a 10-year-old would understand:
(Press Release)

«Table»
Summarize this press release using a text-based table:
(Press Release)

«Format»
Take this press release:
(Press Release)
And format it in the following way: [two sentences to summarise the press release] [three bullet points covering the most important information] [two key quotes from the text] [a text-based table to visualize some of the information]

Intelligence Reporting con ChatGPT - 4/5

Adattamento del Prompt alle dimensioni del documento

- Nell'ambito della Comunità Intelligence, è possibile imbattersi in documenti brevi, come briefing, executive summary o brevi commenti di analisi. Per i testi inferiori alle 1.000 parole (<20 pagine), ChatGPT è in grado di riassumerli efficacemente in una sola volta. Documenti più lunghi vanno trattati con approcci diversi.

- **Tecnica Summary-ception** consente di aggirare queste limitazioni condensando parti più piccole del documento e poi riassumendo i riassunti stessi.

Intelligence Reporting con ChatGPT - 5/5

Tecnica Summary-ception

1. Dividere il documento in paragrafi che rientrino nei limiti di input di ChatGPT.

2. Chiedere a ChatGPT di riassumere singolarmente ogni paragrafo, utilizzando stile o formato di riassunto preferito.

3. Copiare e incollare il riassunto di ChatGPT in un file separato, creando una versione condensata del documento originale.

4. Chiedere a ChatGPT di riassumere l'intera collezione di riassunti, producendo così un sunto finale condensato e coerente dell'intero documento.

Argomentazioni

Le argomentazioni svolgono un ruolo cruciale nella Comunità Intelligence, in quanto:

- aiutano gli analisti a sviluppare valutazioni logiche e ben supportate sulla base delle informazioni disponibili;

- consentono ai decisori di comprendere situazioni complesse e di fare scelte informate.

Fornendo assistenza nel perfezionamento delle domande, offrendo informazioni di base, strutturando le argomentazioni e identificando spiegazioni alternative, **ChatGPT può migliorare il processo di costruzione delle argomentazioni**.

Case Study

Elaborazione di un Report sull'Iran.
Tra le varie fonti bibliografiche, avete selezionato un rapporto del DNI statunitense 2024 Annual Threat Assessment of the U.S. Intelligence Community (odni.gov)

- Fase 1: Informazioni sulle fonti utilizzate per l'analisi
- Fase 2: Eventuali ipotesi di lavoro presenti nel Report
- Fase 3: Argomentazioni per sostenere le valutazioni del report (ipotesi, affermazioni, sotto-affermazioni, prove e assunzioni)
- Fase 4: Pregiudizi e/o fallacie logiche che influenzano l'analisi
- Fase 5: Domande/linee di indagine integrative al Report

Il report finale di IA generativa sarà non confidenziale, ben strutturato, realmente analitico, con prospettive da più angolazioni, e supervisionato da voi sia nei contenuti, sia nella struttura.

Con l'output finale di ChatGPT in mano, lo integrerete con le vostre informazioni intelligence confidenziali mantenendo sempre ben chiaro e dettagliato **quale parte è frutto di OSINT, quale di HUMINT, quale di SIGINT, e soprattutto quali sono le vostre valutazioni personali.**

www.linkedin.com/in/fabiovanorio/

@FabioVanorio

LET'S GET GOING!

fabio.vanorio@esteri.it

fabio.vanorio@gmail.com