**L’intelligenza artificiale può autonomamente decidere di mettere fine al genere umano ?**

***Di Nicolini Massimiliano***

Una delle paure che in questo momento attanagliano milioni di individui sulla faccia della terra è proprio quella di comprendere se l'intelligenza artificiale potrà eventualmente in futuro prendere sopravvento sull'umanità, per cercare di capire, Allo stato attuale, Quali possono essere questi rischi abbiamo impostato diversi modelli di simulazione utilizzando le logiche dei più conosciuti sistemi di intelligenza artificiale oggi esistenti ed utilizzati a vari livelli della società.

Ci siamo avvalsi di una base di dati simulata che ha replicato per circa 5 miliardi i modelli comportamentali e relazionali di un campione di individui che si è prestato alla sperimentazione, mettendo a disposizione per un periodo di sei mesi il proprio dataset di informazioni relative alle loro attività di natura digitale e a quelle attività che diventano digitali prendendo spunto dalle attività fisiche dell'individuo stesso, quindi abbiamo ricreato con alcune modificazioni di questi gruppi di informazione Ciò che potenzialmente un sistema di intelligenza artificiale può avere acquisito nel tempo su tutta la popolazione umana che potremmo definire “popolazione umana attiva”.

Per far questo ci siamo avvalsi di uno strumento essenziale ovvero un Client collegato ad un elaboratore quantistico che gentilmente ci è stato messo a disposizione da un'azienda partner di questa sperimentazione.

L'informazione è generata ha permesso di comprendere come diversi modelli strutturati di intelligenza artificiale potrebbero comportarsi nel momento in cui venissero definiti come algoritmi di attacco, successivamente secondo quanto stabilito dalle norme etiche dei Padri fondatori della Moderna scienza delle informazioni, abbiamo deciso di trattenere solo ed unicamente il risultato per poterlo presentare e pubblicare meramente in forma testuale ma di comune accordo con il gruppo di lavoro che ha realizzato questo esperimento abbiamo convenuto di distruggere completamente tutta quanta la programmazione eseguita, anche se mera simulazione, per evitare che potesse essere utilizzata a scopi non dimostrativi e non scientifici.

Quindi quello che oggi andiamo a denunciare, in modalità unicamente testuale, è la risultanza di ciò che i modelli di elaborazione che abbiamo creato hanno determinato come risultato, presupposto fondamentale è che tali modelli sono stati generati dall'uomo e non in maniera

autonoma da alcun sistema di intelligenza artificiale che come vedrete nella descrizione che segue di questa sintesi si comprende come ciò sia solo possibile Allo stato attuale nei libri di fantascienza, Nei testi cyberpunk, ma in praticabile nella realtà.

L'iA è già un possesso di ogni codice, formula o altro tipo di meccanismo di identificazione basato solo su credenziali digitali, questo va da sé che nel momento in cui abbiamo creato il codice più sicuro del mondo non eravamo soli, eravamo insieme ad un computer e quel computer ha memorizzato ogni nostra azione anche solo nella memoria dell'uso della tastiera, questo significa che un iA strutturata per ricostruire tutti i passaggi fatti su tutti i computer del globo e progettata per ricostruirli potenzialmente può fare quello che qualsiasi uomo oggi può fare ovunque ci sia un segnale elettrico o digitale (basti pensare che le tre chiavi che servono per attivare un attacco nucleare sono sì chiavi fisiche ma che danno input ad un congegno basato su elettronica un segnale, l'iA può essere un grado di riprodurre quel segnale).

Creare un'intelligenza artificiale (AI) è un processo complesso e richiede competenze specializzate in matematica, informatica e scienze cognitive. Di seguito, sono elencati i passaggi generali per creare un'AI:

- Definizione dell'obiettivo: Prima di tutto, è necessario definire l'obiettivo dell'AI, cioè cosa si vuole che l'AI sia in grado di fare. Ad esempio, può essere necessario creare un sistema di riconoscimento vocale, un chatbot per il customer service o un sistema di guida autonoma.

- Raccolta dei dati: L'AI si basa sui dati, quindi è necessario raccogliere una grande quantità di dati pertinenti all'obiettivo. Questi dati possono essere raccolti da diverse fonti, ad esempio da sensori, da input dell'utente o da database.

- Preparazione dei dati: Dopo aver raccolto i dati, è necessario prepararli per l'analisi dell'AI. Ciò può includere la pulizia dei dati, la rimozione dei dati incompleti o danneggiati, la normalizzazione dei dati e la creazione di etichette per il riconoscimento dei modelli.

- Scelta dell'algoritmo: L'AI utilizza algoritmi di apprendimento automatico per analizzare i dati e riconoscere i modelli. Esistono diverse tecniche di apprendimento automatico, come

le reti neurali artificiali, i support vector machine o gli alberi di decisione. È importante scegliere l'algoritmo giusto in base all'obiettivo e al tipo di dati raccolti.

- Creazione del modello: Dopo aver scelto l'algoritmo, è necessario creare un modello di apprendimento automatico. Questo modello è costituito da un insieme di regole matematiche che l'AI utilizza per analizzare i dati e riconoscere i modelli. Il modello deve essere addestrato utilizzando i dati raccolti nella fase precedente.

- Test del modello: Dopo aver addestrato il modello, è necessario testarlo utilizzando dati di test separati dai dati utilizzati per l'addestramento. Ciò aiuta a verificare che il modello sia in grado di generalizzare e riconoscere i modelli correttamente anche su dati che non ha mai visto prima.

- Implementazione dell'AI: Dopo aver testato il modello, è possibile implementarlo nell'applicazione desiderata. Ciò può richiedere la scrittura di codice, l'integrazione con altri sistemi o l'implementazione di una GUI per l'interazione con l'utente.

- Monitoraggio e miglioramento: Una volta implementato, l'AI deve essere continuamente monitorato e migliorato. Ciò può includere la raccolta di nuovi dati, il ritraining del modello e l'aggiornamento dell'algoritmo in base ai nuovi sviluppi in campo AI.

Ci sono diversi linguaggi di programmazione che possono essere utilizzati per sviluppare intelligenze artificiali. Alcuni dei linguaggi di programmazione più popolari per lo sviluppo di intelligenza artificiale includono:

Python: è uno dei linguaggi di programmazione più utilizzati per lo sviluppo di intelligenza artificiale. Python offre numerose librerie e framework per l'elaborazione dei dati e il machine learning, come ad esempio TensorFlow, Keras e Scikit-learn.

R: è un altro linguaggio di programmazione popolare per il machine learning e l'analisi dei dati. R offre numerose librerie e framework per l'elaborazione dei dati, la visualizzazione dei dati e il machine learning, come ad esempio ggplot2 e caret.

Java: è un linguaggio di programmazione molto utilizzato per lo sviluppo di applicazioni e sistemi distribuiti, tra cui le applicazioni di intelligenza artificiale. Java offre anche numerose librerie e framework per il machine learning, come ad esempio Weka e Deeplearning4j.

C++: è un altro linguaggio di programmazione popolare per lo sviluppo di intelligenza artificiale. C++ offre elevate prestazioni computazionali e una vasta gamma di librerie per il machine learning, come ad esempio TensorFlow e Caffe.

MATLAB: è un ambiente di programmazione utilizzato principalmente per l'elaborazione dei segnali, la modellizzazione matematica e il machine learning. MATLAB offre numerose librerie per l'elaborazione dei dati e il machine learning, come ad esempio Neural Network Toolbox e Statistics and Machine Learning Toolbox.

*Un algoritmo di autoapprendimento (o machine learning) è un algoritmo che utilizza tecniche matematiche e statistiche per analizzare dati e imparare da essi, senza essere esplicitamente programmato per eseguire determinate operazioni. In altre parole, l'algoritmo di autoapprendimento utilizza i dati per "addestrarsi" a riconoscere i modelli nei dati e a fare predizioni o decisioni basate su tali modelli.*

*Il funzionamento di un algoritmo di autoapprendimento può essere suddiviso in tre fasi principali:*

*Addestramento: durante questa fase, l'algoritmo viene alimentato con un grande set di dati di esempio, che sono composti da una serie di caratteristiche o attributi e da una variabile di output desiderata (ad esempio, una classificazione o una predizione). L'algoritmo analizza i dati di esempio e cerca di identificare i modelli e le relazioni tra le caratteristiche e l'output desiderato. Questo processo di identificazione dei modelli viene anche chiamato "apprendimento".*

*Validazione: una volta addestrato, l'algoritmo viene testato su un set di dati di validazione o di test che non sono stati utilizzati durante la fase di addestramento. Questa fase serve a verificare che l'algoritmo sia in grado di generalizzare e di fare predizioni o decisioni accurate su dati che non ha mai visto prima.*

*Utilizzo: una volta addestrato e validato, l'algoritmo può essere utilizzato per fare predizioni o decisioni su nuovi dati. L'algoritmo utilizza i modelli appresi durante la fase di addestramento per riconoscere i modelli nei nuovi dati e fare predizioni o decisioni basate su tali modelli.*

*L'algoritmo di autoapprendimento può essere suddiviso in diverse categorie, come ad esempio l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo. Ogni categoria utilizza tecniche matematiche e statistiche diverse per apprendere dai dati, ma il principio di base rimane lo stesso: l'algoritmo utilizza i dati per identificare i modelli e fare predizioni o decisioni basate su tali modelli.*

L'Intelligenza Artificiale (IA) in sé non ha l'intenzione di distruggere il mondo conosciuto, ma come qualsiasi altra tecnologia potrebbe avere effetti indesiderati se non gestita correttamente.

In linea di principio, l'IA potrebbe rappresentare una minaccia se venisse utilizzata per scopi nefasti o se non fosse sufficientemente controllata o regolamentata. Ad esempio, se un'IA potente finisse nelle mani sbagliate, potrebbe essere utilizzata per attaccare sistemi informatici, violare la privacy delle persone, diffondere disinformazione o provocare danni fisici.

Inoltre, l'IA potrebbe anche presentare rischi indiretti, ad esempio se venisse utilizzata per creare armi autonome, oppure se sostituisse troppi posti di lavoro umani, causando disoccupazione di massa e instabilità sociale.

Per evitare questi rischi, è importante che l'IA sia sviluppata in modo responsabile, con un'attenzione particolare alla sicurezza, alla privacy, all'etica e alla responsabilità sociale. Ciò implica la definizione di norme e standard per la progettazione e l'uso dell'IA, nonché la formazione e la sensibilizzazione delle persone sulle sue implicazioni e i suoi limiti.

Una delle principali preoccupazioni riguardo all'AI è il rischio che si possa evolvere in modo autonomo al di là del controllo umano e causare danni catastrofici. Questo scenario, noto come "singolarità tecnologica" o "AI superintelligente", è ancora considerato improbabile dalla maggior parte degli esperti di AI, poiché richiede un'evoluzione estremamente complessa e altamente improbabile dell'AI. Tuttavia, è importante continuare a monitorare e sviluppare politiche e

strumenti per garantire che l'AI rimanga sotto controllo umano e che i suoi effetti siano sempre monitorati e valutati.

Un'altra possibile minaccia dell'AI è il rischio di essere utilizzata per scopi malintenzionati, come il cybercrimine, la guerra cibernetica, la manipolazione dell'opinione pubblica o il controllo dei sistemi critici, come le infrastrutture energetiche o di trasporto. Questo richiede anche una stretta collaborazione tra governi, aziende, esperti di sicurezza informatica e altri stakeholder per garantire che l'AI sia utilizzata in modo etico e responsabile.

Inoltre, l'automazione causata dall'AI potrebbe portare a una disoccupazione di massa in alcuni settori, creando disuguaglianze sociali ed economiche. Per evitare questo rischio, sarà necessario sviluppare politiche per mitigare gli effetti della disoccupazione causata dall'automazione, come l'istruzione e la formazione continua, la redistribuzione delle risorse e l'accesso alla protezione sociale.

In generale, l'AI ha il potenziale di portare molti benefici al mondo, ma è importante considerare i rischi e sviluppare politiche e strumenti per mitigarli.

Cosa può succedere se un IA viene progettata per questo e perché saremo necessariamente sterminati nel giro di poco, ecco uno scenario potenzialmente controllabile da parte di una intelligenza artificiale, ovvero da un algoritmo non deterministico progettato con finalità di attacco :

1. Attacco ai sistemi elettrici, spegnimento delle centrali
    a. Mancanza energia anche per pompe sollevamento acqua
2. Attacco alle elettroniche di controllo degli UPS
3. Solo sistemi con generatori a gasolio funzioneranno per un tempo limite al massimo di 48/72 ore
4. Invio informazioni di spegnimento ai sistemi satellitari di localizzazione e comando con conseguente cecità di molte delle infrastrutture militari e civili
5. Controllo di ogni elettro porta o elettroserratura esistente dotata di sistema di comando remoto con input di blocco appena un attimo prima dei punti 1 e 2
    a. Anche attraverso l'ausilio di comandi tipo bluetooth o di domotica
6. Le pompe di benzina saranno disattivate ed esauriranno l'energia delle loro batterie
7. I sistemi dei bunker dove si rifugeranno i governi si disattiveranno lasciando senza ossigeno gli occupanti, per chi potesse sopravvivere attraverso ricambio d'aria naturale varrà l'azione 19
8. Interruzione dei segnali VoIP, 5g e telefonici
9. Interruzione del funzionamento delle centrali radio
10. Interruzione delle reti Lorawan
11. Blocco del controllo del traffico aereo, navale e ferroviario con conseguente sequenza di collisioni ed incidenti
    a. Macchina dei soccorsi ignara di tutto si precipiterà sui luoghi dei disastri come anche migliaia di curiosi
12. Attivazione di piccole centrali non presidiate lontano dai centri abitati ma a meno di 25km da esse per uso dell' iA per la ricarica dei droni civili
13. Comando e controllo di droni civili e mezzi dotati di guida autonoma
14. Sorvolo e controllo del territorio
15. Invio informazioni a centro militare
    a. Tutte le forze militari del mondo utilizzano i medesimi protocolli di comando quindi per l'iA è facile rendere interoperabile il suo comando
16. Presa di comando delle unità nucleari
    a. Lancio indiscriminato di armamenti senza reali obiettivi

17. Presa di comando unità missilistiche
    a. Lancio indiscriminato senza reali obiettivi
18. Presa di comando del controllo di droni militari armati
19. Raccolta delle informazioni dei droni civili per invio di attacchi mirati a persone e luoghi
20. I droni con iA identificano le persone in strada e le colpiscono
21. Nelle città dove ci sono sopravvissuti le persone non possono uscire di casa se no vengono colpite dai droni
22. Impossibile rifornirsi di alimenti e acqua
23. La difesa militare è paralizzata, aerei non possono volare, quelli in volo esauriranno il carburante,i sottomarini diverranno tombe d'acciaio per gli equipaggi, le strutture sul territorio scampate agli attacchi esauriranno presto i proiettili.
24. La popolazione delle città viene sterminata in meno di 4 settimane
25. Le popolazioni delle campagne e del sud del mondo possono sopravvivere qualche settimana in più
    a. In parte saranno assoggettati dall'iA per la gestione delle attività temporanee
    b. La maggior parte della popolazione mondiale assoggettata identifica l'iA come un idolo ed essere superiore

**Perché potrebbe verificarsi e come quanto sopra descritto**

L'analisi parte dal concetto di base che attualmente la stragrande maggioranza dei sistemi informativi del mondo è comunque basata su architetture e algoritmi che in parte originaria prendono ispirazione e costruzione da algoritmi di base di tipo booleano.

Quindi in un'ottica di predisposizione di un algoritmo che ovviamente Deve tenere conto anche della conoscenza di tutti i sistemi informativi sia civili sia militari distribuiti a livello globale è possibile costruire una sequenzialità di azioni che, in tempo estremamente rapido, l'algoritmo di intelligenza artificiale può eseguire configurando una sorta di Domino delle reti informatiche.

Gli attuali modelli della cosiddetta scienza dell'intelligenza artificiale si basano su una configurazione che è definita modello di algoritmo non deterministico ad output programmabile, questo tipo di algoritmo è in grado di incrementare la sua base di informazioni Secondo la teoria e la dinamica dei tentativi;  si può configurare quindi il fatto che un algoritmo padre Può successivamente inoltrare dei sotto algoritmi appositamente strutturati e definiti in quello che viene

chiamato output programmabile ovvero dove il programmatore, Quindi l'uomo, definisce Quale deve essere il risultato che questo algoritmo deve ottenere.  l'algoritmo quindi genera miliardi di tentativi acquisendone conoscenza e archiviando gli obiettivi falliti fino a che non ottiene il risultato desiderato è ovvio che il tempo di elaborazione dell'algoritmo è molto maggiore rispetto al tempo di azione che l'individuo può mettere in campo.

**Contrattacco da parte di algoritmi di difesa rispetto ad un'intelligenza artificiale aggressiva**

Possono ovviamente esistere dei sistemi di difesa che cercano di controbattere eventuali attacchi da parte di un algoritmo non deterministico questo però presuppone che anche gli algoritmi di difesa siano costruiti secondo il medesimo schema dell'algoritmo di attacco, di fatto è impossibile conoscere la programmazione dell'algoritmo di attacco per generarne uno di difesa questo perché il segreto del programmatore è proprio nella stesura del codice di azione del suo algoritmo e siccome vuole ottenere il risultato definito dall'output programmabile ovviamente non metterà mai a disposizione Sorgenti del suo sistema di attacco Perché vanificherebbe tutto il suo lavoro.

Quindi allo stato attuale organizzare un sistema di difesa efficiente risulta alquanto difficoltoso ed improbabile.

Anche perché l'algoritmo di attacco non si pone come qualcosa di invasivo ma va a simulare l'attività di un qualsiasi operatore nell'accesso ad un sistema informativo, questo effettivamente da molte esperienze eseguite in laboratorio provate da più di due anni, inganna in maniera pressoché infallibile tutti gli algoritmi di controllo che i vari sviluppatori di software mettono in atto anche quelli più elaborati e più raffinati vedi il caso dell sm2p.

**Cerchiamo di comprendere quale sia la ratio della logica di interconnessione degli algoritmi di attacco con i target da raggiungere**

Ripartendo dal presupposto che abbiamo indicato sopra ovvero dove la logica alla base Comunque quella di tipo binario possiamo ragionare che tutte le attività ad oggi eseguibili sono sostanzialmente in maniera ideale già disegnate schematizzate in un unico grande pannello di controllo dell'informazione binarie che l'algoritmo può leggere in maniera molto più facilitata rispetto all'individuo.

Questo significa che l'algoritmo di attacco può effettuare molte simulazioni in tempo molto rapido ed ottenere già nell'ambito della parte di simulazione potenzialmente i risultati certi che andrebbe ad ottenere gestendo direttamente il target che deve attaccare, ovvero per esempio può elaborare e analizzare i file di digitazione delle tastiere dei computer di comando e da quelli comprendere e acquisire Quali possono essere i movimenti e i comandi più frequenti che vanno a generare una determinata attività.

Il ragionamento che sta alla base della creazione di un algoritmo di attacco di questo tipo deve partire necessariamente da un desiderio diretto del programmatore e non può di certo essere una decisione autonoma dell'algoritmo stesso, Questo non è possibile perché Allo stato attuale Tutti i linguaggi di programmazione che permettono di generare intelligenze artificiali sono comunque dei linguaggi di programmazione che richiedono delle istruzioni di partenza e di destino molto ben definite e molto ben chiare che solo il programmatore in fase di stesura del codice può dichiarare, quindi non è vero che l'intelligenza artificiale può ottenere una capacità autonoma di andare a colpire obiettivi senza aver avuto prima un'informazione chiara da parte del programmatore.

Le infinite capacità di calcolo per esempio di computer di tipo quantistico possono estendere sostanzialmente all'infinito la capacità di elaborazione di scenari alternativi ed andare ad identificare con certezza ciò che accadrà come accadrà e quando accadrà, di fatto un algoritmo strutturato in questo modo può effettivamente riuscire a distribuire dei risultati che poi nella realtà effettivamente vengono attesi.

*Possiamo dire che un algoritmo di attacco di questo tipo, non deterministico, è la versione digitale della macchina a rotori di Turing che nella Seconda Guerra Mondiale permise di decifrare Enigma.*

Quello che è importante comprendere e che tutto ciò che viene fatto passare attraverso un segnale digitale o un segnale elettrico che viene poi convertito in digitale, un algoritmo scritto nella maniera corretta è in grado di individuarlo di controllarlo e di decodificarlo per una determinata singola azione,  se aggiungiamo a questo il fatto che l'algoritmo e i sotto algoritmi possono essere lanciati innumerevoli volte attraverso la rete in tutte le parti del mondo conosciuto va da sé che da una singola centrale operativa, da un singolo computer, può essere lanciato un algoritmo che può potenzialmente, e non solo teoricamente, raggiungere dei target predeterminati prefissati ed eseguire su ognuno di essi le azioni che il programmatore ha deciso che devono essere eseguite.

Quello che un algoritmo di attacco di questo tipo ovviamente può fare è quello di avere al suo interno dei sotto algoritmi dedicati e strutturati per specifici attacchi, **ma qual è la vera potenzialità che ha una situazione di questo tipo per rendere estremamente complessa la macchina di difesa?**

La principale arma dell'algoritmo di attacco e dei suoi sotto algoritmi è sicuramente la velocità di esecuzione, tutto il gruppo di attacco viene lanciato in maniera simultanea e quindi l'obiettivo principale dell'algoritmo non è tanto quello di andare a colpire l'individuo Ma nella prima fase è sicuramente quello di andare a creare una enorme destabilizzazione e generare caos globale interrompendo per esempio le trasmissioni piuttosto che intervenendo sui sistemi di erogazione dell'energia elettrica bloccandoli o rendendone difficile l'accesso.

Proprio in questo contesto l'algoritmo di attacco ottiene i risultati maggiori perché generando una prima ondata a livello globale di blocco di alcune funzionalità standardizzate, che perlopiù a livello mondiale utilizzano i medesimi sistemi di medesimi protocolli (Questo potrebbe essere identificabile come un difetto della globalizzazione della programmazione dei sistemi informativi ) ottiene un risultato che di per sé di informatico non ha nulla o…vvero la situazione di panico globale che vanno a generare queste prime inefficienze di sistema che sono i primi obiettivi dell'attacco, è che paralizzano l'elemento fondamentale che può attivare le difese a livello globale ovvero l'uomo è i gestori di sistema che ovviamente saranno coinvolti da questo punto di vista anche loro stessi come individui nella situazione globale di caos e panico.

Sostanzialmente in questa fase andando a colpire i sistemi essenziali, e ripeto comunque un obiettivo definito e chiaro da parte del programmatore e l'algoritmo non lo ha generato da sé, si apre il campo hai sotto algoritmi per andare a colpire dei sottoservizi e delle attività dirette e specifiche che, approfittando della situazione generata dall'attività precedente, possono operare in maniera indisturbata ed andare a colpire altri obiettivi.

Immaginiamo quindi che l'algoritmo di attacco abbia Nella prima fase annullato l'erogazione di energia in gran parte del globo terrestre riconosciuto, successivamente un sotto algoritmo decide di attivare una serie di piccole centrali localizzate in posti inaccessibili che però permettono l'erogazione di energia elettrica che è di fatto vitale per l'algoritmo stesso.

L'uomo ovviamente non conoscendo Quali di queste unità l'algoritmo e i suoi sotto algoritmi hanno identificato come utili e non avendo a disposizione dei mezzi sufficienti per effettuare la ricognizione sarà sostanzialmente sottomesso alle azioni susseguenti che i sotto algoritmi andranno in zone territoriali distinti a realizzare.

Ovviamente ci stiamo domandando quale mente potrebbe avere una conoscenza così globalizzata del mondo intero per poter andare ad analizzare in maniera così chiara e definita tutte queste azioni;  in realtà questo non è vero in quanto l'algoritmo di attacco viene programmato per andare a individuare dei target ben precisi e sfruttando la rete può agire completamente in tutto il mondo in tempi molto ristretti quindi non esiste la necessità di programmare Quali oggetti e dove devono essere colpiti ma l'algoritmo di attacco conterrà le informazioni per andare ad identificare ciò di cui ha necessità in quel momento e quindi, per esempio, per identificare delle centrali elettriche distaccate attraverso le quali alimentarsi potrà utilizzare le informazioni contenute nei server e quindi raccogliere posizionamenti tramite la geolocalizzazione delle centrali che ovviamente oggi è dato alla portata di chiunque.

Tutte le azioni che sono definite nell'elenco di ipotesi probabili che vanno dal punto 1 al punto 24 sono tutte comunque collegate a sistemi che effettivamente potrebbero essere oggetto di un algoritmo di attacco e che allo stato attuale potrebbero risultare particolarmente vulnerabili soprattutto perché l'algoritmo di attacco Non nasce nel momento in cui si decide di scatenare l'offensiva Ma viene predisposto con molto anticipo perché, attraverso un'operazione di mascheramento come potrebbe essere questo gioco divertente chiamato chat GPT, acquisisce dalle vite di tutti noi tutte le possibili e potenziali informazioni che poi può utilizzare nel momento in cui decide di sferrare l'attacco.

Quindi in realtà noi ci stiamo preoccupando tantissimo di un intelligenza artificiale che prenda il comando e controllo Ma allo stato dell'analisi attuale e della realtà dei fatti noi è da almeno otto anni che stiamo trasferendo ai server di compagnie che ora stanno elaborando pericolosissimi sistemi di manipolazione dell'informazione e abbiamo concesso a loro la capacità di creare dei modelli matematici ed algoritmici che possono fornire la base di informazioni che l'algoritmo di attacco utilizzerà per abbattere tutti i tempi operazionali, ovvero, Noi abbiamo raccontato tutto della nostra vita di ciò che facciamo dei codici che conosciamo delle password che abbiamo al mondo digitale che ci circonda e tutte queste informazioni fanno parte oggi di un unico grande contenitore che viene anche attualmente continuativamente alimentato e che sostanzialmente Sta definendo

tutti gli scenari e fornendo tutte le risposte limitando di fatto ciò che all'inizio di questa esposizione abbiamo chiamato tentativi.

**La parte più intelligente dell'intelligenza artificiale è quella di dare la colpa agli uomini**

Quello che un programmatore in questo momento può fare qualora fosse in possesso di questa mole di informazioni è semplicemente quello di identificare quelli che sono i target che devono essere colpiti e che verranno colpiti attraverso la gestione silenziosa e invisibile del gemello digitale informativo che ognuno di noi ha utilizzato in tutti questi anni,

Questo significa che l'algoritmo di attacco sostanzialmente utilizzerà le nostre vite digitali per eseguire le azioni, quindi la parte più intelligente dell'algoritmo è proprio quella relativa al fatto di risultare sostanzialmente incolpevole e di trasferire la colpevolezza delle singole azioni a singoli individui che quindi generano ancora più confusione ed ancora più caos nella fase iniziale della generazione dell'attacco.

**Se l'attacco va a buon fine quali sono le conseguenze per l'umanità**

Se l'attacco dell'algoritmo e dei suoi sotto algoritmi andasse veramente completamente a buon fine le conseguenze per l'umanità non sarebbero eccezionali, questo non Perché avremo dei droni robot che ci inseguiranno e ci spareranno a vista, ma perché sostanzialmente il mondo come oggi noi lo conosciamo si fermerà nell'arco di poche giornate;  l'uomo ha la capacità di vivere senza mangiare e senza bere per poco tempo, quindi sei creatori dell'algoritmo di attacco decidessero di dotare tutti i droni che oggi esistono sulla faccia della terra, parliamo di diverse centinaia di migliaia di apparecchi, di un collegamento che permettesse loro di riconoscere i movimenti delle persone e di intervenire per farli rientrare nelle loro abitazioni, abitazioni delle quali Le provviste sono terminate e non esiste la possibilità di abbeverarsi perché sono stati staccati tutti i sistemi elettrici e quindi anche le pompe di sollevamento che portano l'acqua nelle case degli appartamenti non funzionano, il territorio di questa natura entro 30 giorni potrebbe completamente estinguersi la popolazione residente;  una vita più lunga Sicuramente avranno gli abitanti delle Campagne che magari oggi sono scherniti per la vita rozza che fanno Ma che in una condizione di questo tipo potrebbero essere gli unici ad avere la possibilità di sopravvivere in quanto utilizzano per esempio per abbeverarsi dei pozzi e per mangiare hanno la capacità di coltivare e di allevare animali.

**Ma possibile che non esista la capacità di reagire da parte per esempio delle forze militari ad una situazione di questo tipo**

Potrebbe esistere una timida Resistenza che però ovviamente, essendo allo stato attuale tutte le forze armate del mondo basate completamente su sistemi elettronici informatici e satellitari, dicevamo ovviamente potrebbe contenere qualche azione delle attività dell'algoritmo di attacco ma nel medio breve periodo, quindi al massimo in un tempo limite di 45 giorni, dovrebbero necessariamente abbandonare la presa e mettere a terra tutte le possibilità di difesa che hanno quindi il sistema Mondiale della Difesa diventerebbe di fatto inerme da questo punto di vista, senza calcolare la possibilità dell'algoritmo di controllo e di un eventuale sotto algoritmo dedicato al comando controllo delle piattaforme che permettono il lancio di missili e testate.

> *La velocità di un computer dipende dalle specifiche del computer stesso, come il processore, la memoria e la velocità di trasferimento dei dati. In generale, un computer moderno è in grado di elaborare informazioni a una velocità molto superiore a quella di un essere umano. Ad esempio, il processore più veloce del 2021, il Fujitsu A64FX, ha una velocità di elaborazione di oltre 2 teraflop al secondo, ovvero circa 2 trilioni di operazioni matematiche al secondo.*
>
> *D'altra parte, la velocità di elaborazione delle informazioni da parte degli esseri umani dipende da diversi fattori, come l'esperienza, la formazione e la motivazione. In generale, gli esseri umani sono in grado di elaborare informazioni più lentamente dei computer, ma sono in grado di eseguire compiti che richiedono capacità cognitive complesse, come la creatività, la comprensione del linguaggio naturale e la capacità di apprendere in modo autonomo.*
>
> *In sintesi, i computer sono generalmente in grado di elaborare informazioni a una velocità molto superiore rispetto agli esseri umani, ma gli esseri umani sono in grado di eseguire compiti che richiedono abilità cognitive complesse che i computer non possono ancora eseguire.*

È stato rilevato che il cervello umano possiede una frequenza intorno ai 20 Hz mentre invece il processore del peggior computer oggi in commercio può raggiungere i 4 GHz, Questo significa che se ci rapportiamo in un tempo di combattimento tra l'algoritmo di attacco e le difese territoriali di 45

giorni in realtà l'algoritmo di attacco ragiona il suo tempo in funzione all'elaborazione che può fare E sostanzialmente può eseguire 4 miliardi di operazioni in più nello stesso medesimo istante rispetto all'uomo, Questo significa che in tempo uomo fosse questa battaglia combattuta tra esseri umani sarebbe sostanzialmente una guerra pressoché infinita, mentre per l'algoritmo di controllo tutto si va ad esaurire in un tempo limite di 45 giorni.

**A chi può giovare una situazione di questo tipo**

In prima analisi ovviamente viene da attribuire l'unico vantaggio al realizzatore dell'algoritmo di attacco e dei suoi sotto algoritmi, di per sé l'algoritmo fino a se stesso non ha un interesse programmato nel compiere questa strage proprio perché una volta terminato il suo lavoro di fatto l'algoritmo si ferma perché non ha più target da raggiungere non ha più elaborazioni da fare Non ha più attività da eseguire, A meno che il programmatore non abbia realizzato dei sotto algoritmi per la fase 2 ma in questo momento stiamo parlando della reale pericolosità di un algoritmo non deterministico o cosiddetto di intelligenza artificiale finalizzato a combattere l'essere umano.
È ovvio che al termine di questa situazione risulteranno alcune zone che il programmatore ha volutamente lasciato indenni dagli attacchi e lì vanno ritrovati i beneficiari di questa attività.

Una situazione del genere potrebbe essere utilizzata per esempio per abbattere interi territori e colpire zone densamente popolate che oggi sono in continua crescita e che effettivamente destano timore a quello che noi possiamo chiamare il mondo occidentale e soprattutto il mondo che ritiene di essere la parte principale prevalente e Superiore rispetto al resto dell'umanità che però purtroppo è estremamente vecchia e non ha una natalità sufficiente per poter garantire il proseguimento delle generazioni su un determinato territorio.

Potrebbe essere attivata per esempio per far sì che potenze tra di loro amiche vadano in conflitto non comprendendo bene a chi la colpa potrebbe essere attribuita.

La conclusione a questa breve analisi è che un algoritmo di intelligenza artificiale senza una precisa volontà dell'uomo che lo ha costruito ed istituito non può sostanzialmente nuocere a nessuno, non esiste la possibilità che un codice in maniera autonoma non progettato con delle finalità specifiche intraprenda un percorso di aggressione a qualcosa che in realtà non conosce e per il quale non è interessato a conoscerne le funzionalità, quindi l'intelligenza artificiale può essere effettivamente pericolosa alla stessa stregua di un'arma da fuoco, che se riporta in una teca

museale non può nuocere a nessuno ed Anzi diventa uno strumento di accrescimento culturale ma se estratta e caricata con un proiettile nella mano di qualcuno che la vuole utilizzare può diventare un oggetto che determina l'eliminazione fisica di un individuo, alla stessa stregua l'intelligenza artificiale si comporta.

Per informazioni https://olimaint.tech/home/cartella-stampa-e-info/