ANTONIO ALBANESE • GRAZIELLA GIANGIULIO

Confondere cuori e menti

Guerra Cognitiva sfide contemporanee e IA

agd communication

Antonio Albanese & Graziella Giangiulio

Confondere i Cuori e le Menti

Guerra Cognitiva sfide contemporanee e IA

communication

Improvise Adapt Overcome

Sergeant Thomas Highway - Heartbreak Ridge 1986

I've given up

On the media

Feeds my hysteria

Sick of living down on my knees

I've given up

On morality

Feeds my brutality

F**k what you think about me

Wash it all away, Got your Six (2015) Five Fingers Death Punch

Sommario

INTRODUZIONE

La mente dell'uomo come campo di battaglia

Abbiamo unito in un unico volume, riflessioni e notizie relative alla manipolazione delle informazione il cui arco temporale spazia in diversi anni e tocca diversi ambiti: da quello bellico propriamente detto, al jihadismo fondamentalista islamico, per far vedere, nella maniera più semplice possibile e con un linguaggio piano come è quello pensato per un servizio giornalistico, che viviamo da sempre potremmo dire, in un ambiente in cui la manipolazione di ciò che leggiamo, vediamo o ascoltiamo, è presente in maniera più o meno evidente.

Fino ad oggi veniva chiamato, per esempio, marketing, cioè variabili comunicative tese a vendere un determinato prodotto, oggetto, idea, servizio e chi più ne ha più ne metta. Oggi questa inconsapevolezza sembra essersi tramutata in una consapevolezza a una sola direzione, in una verità che deriva "ex officio" solo da una parte del mondo che si erge a metro di paragone unico per valori, cultura e storia.

Le bugie arrivano solo da una parte, la verità solo da un'altra, tertium non datur.

Su questo assunto viviamo in una bolla informativa manipolata e incompleta, noi questa la chiamiamo disinformazione.

La definizione è però errata stando a manuali di analisi dell'informazione occidentali, e definirla "giornalistica" è riduttivo della professione giornalistica oltre che essere fuorviante, perché crea il nesso logico "giornalistico" uguale "pressapochista", cosa che nei fatti non è e non lo è sopratutto da un punto di vista deontologico.

Restando sui manuali di cui si faceva cenno prima, occorre parlare propriamente di inganno, deception, e non di disinformazione, misinformation. Sostanzialmente la differenza tra i due concetti, e le azioni relative, è la intenzionalità del soggetto agente nel fornire all'audience target una informazione non vera o non corrispondente ai fatti e quindi "falsa", anche se apparentemente vera.

Su queste azioni che ripetiamo sono sempre esistite dacché esiste la comunicazione verso un pubblico generico o individuato precisamente, si sono basate campagne d'influenza, di vendita e guerre tra i popoli.

Su questa collaudata matrice, si sono innestati via via diversi altri strumenti, e studi comportamentali, che hanno facilitato l'opera di manipolazione, fio ad arrivare ai social media. Oggi diffusissimi e pervasivi, sono uno strumento che si è rivelato talmente duttile e di facile utilizzo da esser quasi diventato sinonimo di manipolazione, nella maggior parte dei casi.

Le operazioni di guerra psicologica, Psyops, di guerra informativa, Infowar, di guerra cibernetica, Cyberwar, si sono dimostrate di efficacia monumentale negli anni a cavallo del secolo e nei primi due decenni del XXI. Si sono costruite a tavolino vittorie e sconfitte elettorali, campagne di vendita, di acquisizione di veri obiettivi sociologici e così via, utilizzando squadre di operatori, abilissimi esperti informatici uniti a sociologi e esperti di marketing e così via. Addirittura gruppi transnazionali fondamentalisti islamici come Daesh e al Qaeda ne hanno capito la basilare importanza. I mujahid della comunicazione erano e sono ancora oggi fondamentali per l'operato e il proselitismo delle due strutture, più vive e operative che mai.

Tutto questo accadeva al massino dieci anni fa e tutto adesso sembra preistoria: si è aperta l'era dell'IA. L'era della cosiddetta Intelligenza Artificiale per tutti ha dato vita ad un vero diluvio di utilizzi nei settori più disparati compreso quello quello della manipolazione dell'informazione.

La domanda da porsi è semplice: come è stato possibile? Gli algoritmi che apprendono e auto-apprendono, fino a diventare interattivi con l'ambiente esterno si muovono a velocità che definire non umane è riduttivo. Seppur sia un ambito scientifico che esiste da almeno venti anni, era fino ad oggi riservato a pochi specialisti del settore informatico. La scintilla che ha reso questa branca da settoriale a universale è stata la mole di dati cui aver accesso e la capacità di poter rispondere in maniera sensata a domande poste via via in un tono colloquiale, quasi umano. Questo ha consentito agli algoritmi in questione di potersi raffinare e quindi colmare distanze siderali di conoscenza in pochissimo tempo, relativamente parlando.

Quanto predetto dalla sociologa statunitense Shoshana Zuboff[1] in merito al capitalismo della sorveglianza è divenuto sempre più reale e vicino a noi in modi nuovi e pervasivi.

[1] S. Zuboff - The age of surveillance capitalism: the fight for the future at the new frontier of power - Profile Books, 2018

Il mondo dei mass media, sia tradizionali che social, è stato colpito in pieno da questa rivoluzione dell'informazione. Velocità della creazione e della diffusione hanno reso obsoleti i team operativi e hanno creato e dettato nuovi tempi e modi di "intossicare" le informazioni e quindi il modo di orientarsi di un soggetto target, sociale o umano che sia.

Si è giunti alla constatazione, suffragata dai fatti, che il nuovo campo di battaglia sono le menti del target, che sia un pubblico, un nemico, o un mercato di riferimento, si è arrivati a potenziare e definire quella serie di tecniche, prima appartenenti a diversi settori, Guerra Cognitiva, in quanto si cerca di modificare la percezione della realtà in diverso modo e in differenti ambiti.

Le contromisure fino ad oggi, "si limitano all'invettiva"[2], come il poeta Fabrizio de Andrè canta in un suo celebre brano, ossia si cerca di porre freni e limiti legislativi, a rendere eticamente "umano" uno strumento dalle potenzialità infinite che è in grado di aiutare lo sviluppo in proporzione geometrica. "Umano troppo Umano"[3], nel senso nicceano, è la sintesi con cui potremmo definire questi tentativi di bloccare lo sviluppo dell'IA e delle sua applicazioni informative, fino ad ora rivelatesi belle dichiarazioni e poco altro. Quando si entra nel settore della "guerra" nel senso alto del termine, le regole dei giochi mutano radicalmente.

La tendenza alla dicotomia, alla nazionalizzazione dei dati, cui stiamo assistendo, stanno facendo nascere programmi di sviluppo che prevedono la comunicazione e quindi la percezione del mondo circostante come una arma tra le tante a disposizione dei diversi contendenti. E viene infatti usata, da tutte le parti in causa con diverso successo. Se ne hanno esempi nella guerra nell'oriente europeo, sul fronte ucraino, e in quella meridionale, sul fronte israelo-palestinese e su quello del Mar Rosso.

Anche se la sua percezione non è così diffusa, e la consapevolezza di vivere in un ambiente informativo soggetto a pressione non riguarda molte parti delle società europee, assorte nel loro viver quotidiano.

Questo assieme di tecniche e manipolazioni che definiamo Guerra Cognitiva ricorda molto da vicino, se non proprio sovrapposto, a un'altra tipologia operativa nota come contro-insorgenza, counterinsurgency in linguaggio operativo anglosassone e NATO.

---

[2] F. De Andrè G.P. Reverberi, *Bocca di Rosa*, Bluebell Records, 1967

[3] F. Nietzsche, Menschliches, Allzumenschliches. Ein Buch für freie Geister, 1878

Se le campane di contro-insorgenza possono essere sintetizzate dal brocardo inglese: “Winning Hearts and Minds” (Vincere i Cuori e le Menti), quelle attuali di Guerra Cognitiva possono rientrare in questa definizione seppur con una piccola ma significativa modifica: “Confondere i Cuori e le Menti” ed è da qui che siamo partiti in questo viaggio di analisi che a questo livello non può che essere divulgativa e rivolta ad un pubblico ampio, ma che certamente non si esaurisce qui.

Buona lettura

Roma 22 Giugno 2024

Antonio Albanese e Graziella Giangiulio

WINNING HEARTS AND MINDS

L'avvento della guerra cognitiva
Da Sun Tzu alla COIN 5.0[4]

L'arte suprema della guerra è sottomettere il nemico senza combattere
Sun Tzu

"La guerra irregolare è molto più intellettuale di una carica alla baionetta."
T.E. Lawrence

"L'aspetto positivo della faccenda è solo il 25% del problema, mentre il restante 75% consiste nel portare la gente del paese dalla nostra parte."
Field Marshal Sir Gerald Templer

PROPAGANDA: UN'ARMA CON UN SOLO LATO

La situazione asimmetrica ha effetti importanti sulla propaganda. L'insorto, non avendo alcuna responsabilità, è libero di utilizzare ogni stratagemma; se necessario può mentire, imbrogliare, esagerare. Non è obbligato a dimostrare; viene giudicato da ciò che promette, non da ciò che fa. Di conseguenza, la propaganda è per lui un'arma potente. Senza una politica positiva ma con una buona propaganda, i ribelli potrebbero ancora vincere.

Chi fa controinsurrezione è legato alle sue responsabilità e al suo passato e per lui i fatti contano più delle parole. Viene giudicato per quello che fa, non per quello che dice. Se mente, imbroglia, esagera e non dimostra, può ottenere qualche successo temporaneo, ma al prezzo di essere screditato per sempre. E non può imbrogliare molto a meno che le sue strutture politiche non siano monolitiche, perché la legittima opposizione nel suo stesso campo rivelerebbe presto ogni sua manovra psicologica. Per lui la propaganda non può essere altro che un'arma secondaria, preziosa solo se intesa a informare e non a ingannare. Una

[4] A. Albanese, Intervento al seminario "Innovazione ed Etica nel cuore della rivoluzione digitale"
Roma Senato della Repubblica 19 aprile 2024

controinsurrezione raramente può coprire con la propaganda una politica cattiva o inesistente”.

COIN

“Costruire una macchina politica dalla base della popolazione in su”

David Galula, Guerra di controinsurrezione: teoria e pratica

La guerra cognitiva è ormai con noi. La sfida principale è che lo sia essenzialmente invisibile; tutto ciò che vedi è il suo impatto, e a quel punto spesso è troppo tardi.

The Cognitive Warfare Concept, Bernard Claverie François du Cluzel[5]

Anche se alcuni avversari hanno messo a punto strategie per evitare uno scontro cinetico con la NATO, ci sono nazioni che utilizzano mezzi ibridi come un modo per destabilizzare e danneggiare gli avversari. Tra questi mezzi ibridi, la guerra dell’informazione è stata spesso percepita come una sottofunzione secondaria, la pianificazione delle operazioni di gestione delle crisi, che generalmente si basano sull'esercito tradizionale.

Nel mondo di oggi, la guerra dell’informazione e la guerra cognitiva probabilmente diventano linee d'azione permanenti per ottenere lo stato finale desiderato che è la destabilizzazione di un leader politico, di una forza nemica, di un paese o persino di un’Alleanza.

In primo luogo è necessario tracciare brevemente cosa definisce Cyber Warfare, Information Warfare e Cognitive Warfare (Guerra Cognitiva) insieme ai legami che li uniscono.

La Guerra Cognitiva è la forma di manipolazione più avanzata fino ad oggi, consentendo l’influenza di un individuo o di un gruppo di individui sul proprio comportamento, con

---

[5] NATO Innovation Hub - https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf - 2023
Bernard Claverie è professore universitario, direttore onorario e fondatore dell'Ecole Nationale Supérieure de Cognitique all'Institut Polytechnique di Bordeaux e ricercatrice al Centre National de Recherche Scientifique (CNRS) — UMR5218 — Università di Bordeaux.
François du Cluzel è un tenente colonnello riservista dell'esercito francese e capo dei progetti innovativi all'interno degli Allied Command Transformation Innovation Hub a Norfolk, Virginia.

l’obiettivo di acquisire vantaggio tattico o strategico. In questo campo d'azione, il cervello umano diventa il teatro dell’azione / operazione. L'obiettivo è agire non solo su ciò che pensano gli individui target, ma anche su ciò che pensano, come pensano e, in definitiva, come agiscono. La Guerra Cognitiva è necessariamente associata con altre forme e ambiti di azione per raggiungere i “cervelli bersaglio”, come la Cyber Warfare e la Information Warfare, la Guerra dell'informazione.

In modo molto schematico, nel dominio operativo Cyber, i belligeranti penetrano nelle reti di computer per raggiungere il software avversario e interromperlo per neutralizzare ciò che questo software contribuisce a produrre.

La Guerra dell'Informazione consiste in manipolare informazioni che sempre più spesso vengono veicolate attraverso mezzi informatici e digitali (cyber appunto).

La Guerra Cognitiva, infine, agisce sul modo in cui il cervello bersaglio elabora l’informazione. Nella sua concettualizzazione, la Guerra Cognitiva integra quindi queste altre forme di guerra, alla quale si aggiunge una parte essenziale che ha visto sviluppi recenti: la neuroscienza cognitiva.

Facilitando la comprensione dei meccanismi del cervello, del modo in cui si integra ed elabora diverse categorie di informazioni, le neuroscienze renderanno possibile ottimizzare l’uso di altri tipi di guerra, in particolare la guerra dell’informazione. La manipolazione di un individuo sarà più facile se i suoi meccanismi cognitivi saranno stati correttamente analizzati e se l'informazione trasmessa per influenzarlo permette di attivare questi meccanismi nella direzione desiderata.

GUERRA COGNITIVA - DEFINIZIONE

La guerra cognitiva è un approccio combinato alle armi che integra la guerra non cinetica, capacità di cyber, informazione, ingegneria psicologica e sociale per vincere senza combattimento fisico. È un nuovo tipo di guerra definita come l’arma della pubblica opinione usata da enti esterni. Ciò viene effettuato allo scopo di influenzare e/o destabilizzare una nazione. Questi attacchi possono essere visualizzati come una matrice che abbraccia pochi e molti; influenzare il pensiero e l'azione; obiettivi che vanno dall’intera popolazione a misure individuali; tra comunità e/o organizzazioni. Gli attacchi cercano di cambiare o rinforzare i pensieri, influenzando/confermando il modo in cui le persone pensano di influenzare

l'azione nel mondo reale. Il modo in cui viene condotta differisce dai settori di guerra più tradizionali. Se la Guerra informativa tenta di controllare ciò che osserva la popolazione bersaglio, la guerra psicologica controlla ciò che vede e sente la popolazione bersaglio, la guerra informatica tenta di interrompere le capacità tecnologiche di nazioni bersaglio, mentre la guerra cognitiva si concentra sul controllo di come pensa e reagisce una popolazione bersaglio.

Un esempio attuale: la Russia ha lanciato un'invasione militare cinetica dell'Ucraina, rafforzata da attività non cinetiche come propaganda mirata, campagne di disinformazione e sostegno da parte dei suoi partner. Alcune di queste attività non cinetiche di guerra cognitiva sono ovvie e dirette: i destinatari di forze allineate con la Russia i disinformatori sperimentano un deterioramento della loro capacità di distinguere i fatti dalla finzione, diminuendo la loro resilienza mentale e con un potenziale impatto a lungo termine, come la perdita di fiducia nei media.

Altri casi non sono così chiari: la Cina sfrutta l'influenza ufficiale e allineata ai partiti per manipolare e controllare il proprio ambiente informativo interno, il che si traduce nello sviluppo di pregiudizi cognitivi. Si presenta un effetto secondario: anche i cittadini di altre nazioni sviluppano pregiudizi cognitivi nei confronti dei cittadini della Cina continentale e la loro disconnessione collettiva dalle informazioni esterne, che produce due percezioni della realtà fondamentalmente opposte. Questa forma di polarizzazione "noi contro loro" può portare a una crescente emarginazione ed esclusione delle popolazioni, nonché allo sfruttamento emotivo, che contribuisce alla strategia di guerra cognitiva della Cina.

La Guerra Cognitiva integra quindi capacità informatiche, informative, psicologiche e di ingegneria sociale. Queste attività, condotte in sincronizzazione con altri Strumenti di Potere, possono influenzare atteggiamenti e comportamenti influenzando, proteggendo o interrompendo la cognizione individuale e di gruppo per ottenere un vantaggio su un avversario.

La sensibilità alla Guerra Cognitiva solleva molte domande e preoccupazioni. Come proteggersi da tali attacchi? Ciò richiede la comprensione di ciò che rende determinati individui o gruppi più o meno suscettibili alla manipolazione cognitiva mirata. Sono necessarie nuove capacità per combattere l'aumento delle automazioni in rete (ad esempio,

botnet, IA) che distorcono e manipolano la sfera dell'informazione. Come rilevarlo? Una superficie di attacco così ampia richiede la correlazione di nuovi segnali di allarme attraverso la rete sociale, informatica e informativa per rilevare tali attacchi. Come attribuire tali attacchi a un particolare avversario è difficile. In definitiva, la Guerra Cognitiva ci costringe a comprendere la cognizione umana e l'azione sociale collettiva. Come arriviamo alle nostre conclusioni e, ad esempio, elaboriamo l'incertezza semantica, l'illusione provocata, la distorsione percettiva, la saturazione dell'attenzione, i disturbi dell'apprendimento, i bias cognitivi, la memoria di lavoro o i ricordi a lungo termine? Ma la cognizione è anche collaborativa e propositiva nei nostri sistemi sociali con processi decisionali condivisi, e in particolare nelle democrazie. Come si ottiene la comprensione condivisa, soprattutto nei social network, e perché è particolarmente fragile e suscettibile alla manipolazione? Sia individuale che collettiva, la cognizione corrisponde a tutti i processi che vengono mobilitati per modellare la nostra comprensione del mondo, prendere decisioni e agire di conseguenza.

Articoliamo il nostro mondo moderno come pieno di pensiero umano e di macchine, che si esprimono o esprimono la circolazione di pensieri e programmi. La convivenza tra intelligenza naturale e intelligenza artificiale è al centro di questo dibattito che ci costringe a concepire la guerra come un ibrido, con i nostri pensieri e le nostre società sempre più modellati dalle macchine. La guerra cognitiva è già qui e i capitoli principali sono già in fase di scrittura a causa della crescente convergenza di persone, informazioni e tecnologia attraverso i nostri social network. Le linee di tendenza includono interfacce tecnologiche che facilitano l'integrazione uomo-sistema, nuove capacità per aumentare il processo decisionale umano, crescente automazione con controlli di sistema dell'errore umano (ad esempio, guida) e intelligenza artificiale che supera i limiti dei programmi, autonomia degli attori digitali assistiti o di macchine arricchite dal pensiero umano.

Azioni di influenza, soft e smart power, azioni di disinformazione e destabilizzazione stanno diventando componenti essenziali delle strategie di conquista e dominio tra paesi, organizzazioni e attori non statali nelle relazioni internazionali: un'offuscamento intenzionale di punti di riferimento e confini, indifferenti alla realtà, sta prendendo piede.

Influenzare e manipolare l'opinione pubblica sono vere e proprie modalità d'azione per i poteri che mirano a destabilizzare gli avversari, più nel dettaglio le nostre democrazie.

L'attuale contesto di destabilizzazione è quello della "post verità", della messa in discussione della conoscenza, delle istituzioni e dei governi, della conoscenza e dell'approccio scientifico, dove i fatti contano meno delle emozioni e delle bugie di chi li pronuncia. Questi poteri (statali o meno) fanno affidamento su una tecnologia che fornisce loro potenti leve di diffusione e intrusione che possono prendere di mira ogni individuo, dando loro la capacità di influenzare e manipolare l'opinione pubblica su larga scala a loro insaputa. Le "fake news", le voci, la mistificazione e il complotto sono esempi molto concreti, la cui diffusione è moltiplicata dai social network.

Il riferimento al triangolo di Clausewitz "popolo, politica, militare" permette di identificare il posto dei militari in un tema che a prima vista sembra riguardare solo l'ambito civile. Il campo della manipolazione dell'informazione dal punto di vista militare non è infatti di per sé una novità. L'arma dell'informazione è antica e rimando nella contemporaneità è un'antica eredità della Guerra Fredda e dagli anni Sessanta – Settanta la visione del campo delle percezioni fa parte del campo dottrinale delle principali forze armate.

Il termine Guerra Cognitiva è stato utilizzato con questo significato negli Stati Uniti dal 2017 (Underwood, 2017) per descrivere in particolare le modalità di azione a disposizione di uno stato o di un gruppo di influenza che cerca di "manipolare i meccanismi cognitivi di un nemico o dei suoi cittadini al fine di indebolirlo, penetrarlo, influenzarlo o addirittura soggiogarlo o distruggerlo".

Le persone hanno tentato di influenzare l'opinione pubblica sin dall'ascesa della civiltà. È un elemento essenziale, un componente delle strutture politiche in cui ci siamo evoluti. Tuttavia, l'arma dell'opinione pubblica è uno sviluppo nuovo e minaccioso nel modo in cui interagiamo. L'avvento del Internet e i mass media hanno reso possibile la manipolazione su larga scala delle popolazioni attraverso messaggistica mirata, accessibile e multimodale, che ora può esistere sotto la maschera dell'anonimato.

In un mare di un miliardo di voci, individuare le singole fonti è diventato incredibilmente difficile. Uno sforzo che, per certi versi, è paragonabile alla difficoltà di individuare chi ha urlato "Al fuoco!" in mezzo ad una folla. Alcuni sosterranno che ciò è intenzionale, sostenendo che l'anonimato è richiesto per le risorse fornite da Internet. Altri, tuttavia, si preoccupano delle conseguenze indesiderate che ciò potrebbe comportare questa mancanza di responsabilità a lungo termine.

Social media, reti di informazione, algoritmi di automazione, intelligenza artificiale, salute mentale e, forse, anche la nostra stessa fisiologia evolveranno rapidamente nel prossimo futuro. Tutti questi strumenti stanno lavorando per renderci più connessi, più guidati dai dati e più curiosi.

Sarà una nuova entusiasmante era di interazione umana. Tuttavia, le strade nella nostra mente non sono strade a senso unico. Mentre le persone ricevono informazioni, allo stesso tempo danno informazioni e dati. Allo stato attuale, un giorno semplici righe di codici saranno in grado di identificare e descrivere tutto di noi. Le nostre abitudini, i nostri amici, le nostre fedi, le nostre culture, le nostre preferenze, e anche i nostri vizi. Per la prima volta la guerra non avrà a che fare con i corpi esposti. Si occuperà di menti esposte invece. È questa nuova via di guerra che abbiamo soprannominato Guerra Cognitiva.

L'intelligenza artificiale (AI) sta portando nuovi strumenti che facilitano la guerra cognitiva, che possono amplificarla e renderla ancora più accessibile e a basso costo, soprattutto quando si tratta di diffusione di fake news e disinformazione.

Du Cluzel ci ricorda che le campagne di fake news combinano informazioni reali e distorte, fatti esagerati e notizie inventate (disinformazione).

Tra questi strumenti di facilitazione, Mad Scientist Laboratory cita i deepfake, video generati dall'intelligenza artificiale che possono mostrare una persona mentre recita un discorso che non ha mai hanno effettivamente dato: il loro pericolo è evidente, dato che qualsiasi personalità influente può essere costretta a dire qualsiasi cosa. Possono essere resi ancora più realistici mediante tecnologie che imitano il tono della voce di una persona e il suo accento. Il rischio associato ai corpi e ai volti generati dall'intelligenza artificiale è meno evidente, ma altrettanto reale: consente la creazione di numerosi account falsi sui social network con persone che non esistono e rende possibile umanizzare i robot per dare loro maggiore credibilità. Generare il volto di una persona che non esiste è istantaneo. L'ultimo strumento citato da Mad Scientist Laboratory è la generazione di testo AI, e questo strumento è stato aggiornato dall'implementazione di Chat-GPT nel novembre 2022, ed oggi avanza sempre di più. Questo tipo di strumento aiuta a diffondere informazioni false poiché può scrivere articoli, post e commenti su social network molto più velocemente e su scala più ampia di quanto potrebbe fare un gruppo di esseri umani. Pertanto, un singolo gruppo potrebbe generare migliaia o addirittura milioni di commenti e post sui social network,

orientati a sostenere o indebolire una causa; e queste azioni avrebbero "il potenziale per erodere il rapporto tra i governi e i loro cittadini, provocando gravi reazioni in tutto il mondo e portando le persone a mettere in discussione la realtà stessa in cui credono". Ad esempio, il social media X (già Twitter) ospita molti bot, che possono "perseguire obiettivi dannosi come l'interferenza elettorale e la propaganda estrema".

Un esempio della possibile applicazione delle campagne di destabilizzazione attraverso le fake news sui social network è l'influenza delle elezioni. La Russia è particolarmente attiva in questo campo e "il Cremlino considera le operazioni di disinformazione e informazione il mezzo più efficace per influenzare i risultati politici in altri paesi", sfruttando "le divisioni politiche, sociali o etniche esistenti a livello nazionale e strumentalizzandole per cambiare il modo in cui gli elettori pensano – e attraverso ciò come votano".

Esistono alcuni esempi di soluzioni individuali contro specifiche azioni di guerra cognitiva. Ad esempio, sono state elencate alcune contromisure contro l'influenza pubblica e le fake news sui social media: educazione pubblica, comunicazione sulle fake news, moderazione automatica e umana, debunking, norme legali, ecc..

Un altro modo per proteggere e prevenire è utilizzare la guerra cognitiva in modo difensivo. Gli strumenti di guerra cognitiva possono essere utilizzati per educare le popolazioni attraverso i media e i social media, migliorare la prontezza cognitiva o addirittura aumentare la cognizione dei soldati. Potremmo anche immaginare strumenti decisionali che tengano conto dei pregiudizi cognitivi e delle potenziali aggressioni da guerra cognitiva.

Il primo passo per organizzare una soluzione complessiva è analizzare l'avversario e capire come conduce le strategie di guerra cognitiva. Ciò consentirebbe a chi è sotto attacco di individuare tempestivamente le offensive di guerra cognitiva e di sollevare la nebbia della guerra. Sono necessarie ulteriori ricerche su questo argomento per costruire soluzioni sistematiche.

La guerra cognitiva può anche affrontare sfide etiche: implica influenzare il pensiero e il processo decisionale di una persona o di un gruppo di persone a loro insaputa. In questo senso può essere paragonato ai nudge (spinte promozionali), che incoraggiano l'utente di un sistema o di uno strumento a comportarsi in modo ottimale: è anch'esso uno strumento di influenza, ma è il suo utilizzo che ne determina le caratteristiche etiche.

ASPETTANDO SKYNET

Società Economia Finanza Guerra: nuovi scenari per l'utilizzo dell'Intelligenza Artificiale

Chiunque si occupi di teoria COIN, ossia di Counter-insurgency conosce benissimo il significato profondo dell'espressione che la sintetizza: Vincere i cuori e le menti. Dietro questa espressione c'è un universo filosofico e strategico, che ha le sue origini più moderne in Francia, nell'opera di David Galula, ufficiale francese e docente negli States, che dovrebbe impostare le azioni di un esercito occupante su un territorio occupato per evitare di essere al centro di operazioni resistenti all'occupazione. Anche se l'assunto sembra essere di molto facile realizzazione, nella realtà la sua messa in pratica si è rivelata assai complessa, nelle diverse e variegate situazioni storiche in cui la "piccola guerra" è stata usata.

Dopo l'abbandono di questa pratica di successo, come altro si può intendere la "manipolazione" delle publiche opinioni europee prostrate da sei anni di guerra sul territorio nazionale nel Novecento, e di grandi insuccessi, si veda anche in questa maniera il lungo periodo della decolonizzazione, è stata riportata in auge, nello studio e nella pratica, durante le prime fasi della guerra in Iraq, trovando in un ufficiale / accademico australiano, David John Kilcullen, nuova linfa ed interesse diffuso, e in un generale statunitense, David Howell Petraeus nuovi stimoli operativi in teatri come quello iracheno ed afgano. Intelligence, comunicazione e azioni militari si fondono per lo scopo che abbiamo detto prima: evitare azioni militari insorgenti e quindi pacificare un determinato scenario, convincendolo, avendo vinto i cuori e le menti, della bontà dell'operato delle forze "occupanti".

Mettendo da parte le diatribe accademiche ed operative all'utilizzo, aggiornato in molti passi dal duo Kilcullen-Petraeus, delle tecniche nate dalle osservazioni sul campo di Galula et alii, l'essenza della Counter-Insurgency ha trovato nell'espressione "Winning Hearts and Minds" la più felice sintesi proprio in quei tragici scenari contemporanei; salvo poi essere messa da parte al mutare delle dirigenze militari dell'epoca e dei diversi approcci politico-strategici nei due teatri dell'epoca: quello afgano e quello iracheno.

È sempre stata una questione di percezione del mondo, ma oggi la "narrativa" che si sta usando in Occidente sembra "bucata", non arriva a tutti, ed è percepita come fatta su misura per delle elite che perseguono propri interessi, una minoranza "potente" e "impotente" nello stesso tempo.

La narrativa è il meccanismo centrale attraverso il quale le ideologie vengono espresse e assorbite è la narrazione; è uno schema organizzativo espresso sotto forma di racconto.

Questa linea di pensiero e di operatività, *mutatis mutandis*, è reperibile in altri settori civili nella cui operatività noi siamo oggi immersi. A voler ben guardare, si tratta di una forma sofisticata di commercializzazione, rivolta ad un mercato target ben difinito, di cui con un'accurata raccolta dati, intelligence appunto, si sa praticamente tutto e quindi può essere "vinto" razionalmente ed affettivamente per un determinato scopo. È il fine appunto della pubblicità, del marketing, sofisticato che sia o meno. È una realtà che conosciamo bene, e dalla quale cerchiamo a volte di difenderci in maniera diversa cercando di mantenere mente e cuore "liberi".

In questo quadro, seppur essenziale, sia l'Insorgenza che la Contro-insorgenza usano anche strumenti informatici; in altri nostri studi abbiamo delineato l'utilizzo della Rete che fa la sfera insorgente Jihadista nella sua battaglia per vincere i cuori e le menti dei fedeli, oltre che agire sul campo reale e tangibile, e per molti aspetti il Cyber-Jihad è stato un terreno di scontro violento e fondamentale per contrastare tutti quei fenomeni che manipolando determinati messaggi religiosi portavano dalla loro parte ampie fette di simpatizzanti. Si tratta di uno scontro oggi ancora aperto nonostante le proclamate vittorie nel campo reale da parte "occidentale"[6].

In questo quadro operativo "on line" e "alive" si è andata innestando, come in molti altri aspetti della nostra vita quotidiana, una forma avanzata di algoritmi, qualcosa che la sociologa statunitense Shoshana Zuboff già tratteggiava nelle sue opere alcuni anni fa[7], come materiale su cui le Big Tech facevano affari. Si tratta di quella serie di sistemi matematici ottimizzati che simulano previsioni, che svolgono in maniera molto rapida ricerche su verticalizzazioni definite e così via.

Al di là della diatriba tra filosofi e matematici, quella che comunemente definiamo Intelligenza Artificiale generativa (con le iniziali maiuscole), è il nuovo "prezzemolo" del marketing, sta dappertutto e sta bene con tutto.

E ovviamente sta bene anche nel settore strategico militare e nel settore COIN, data la rapidità e la capacità pervasiva dello stesso strumento.

---

[6] vedi *infra*

[7] Op. Cit.

Occorre innanzitutto tenere presente che si va ad un livello superiore rispetto alla Counter-Insurgency, si entra in una dinamica, politica e militare, più ampia e complessa, definita con una espressione felice: Guerra Cognitiva.

L'ambito della Guerra Cognitiva (Cognitive Warfare - CW) tende a modificare la percezione del mondo esterno da parte di una società "target". Sembrerebbe a prima vista una operazione di marketing più ampia e complessa ma nella realtà non è proprio così. La distinzione è molto più sottile quando il campo di battaglia è il cervello umano: gli strumenti IA usati in questo ambito "bellico" possono rivelarsi indispensabili nel mutare la percezione di un fenomeno politico economico finanziario tale da mandare in tilt o da scuotere profondamente l'ambiente socioeconomico del target di riferimento, cioè il nemico.

Rischio politico? la CW è politica, è strumento politico di suo, le sua particolarità sono assimilabili al 90% a quelle della COIN, dove la politica è il primo strumento e il militare è secondario (e solo quando serve) solo che qui non c'è una insorgenza, c'è una società target che va smontata e confusa per portarla a "più miti consigli" cioè ad un atteggiamento docile verso chi sta muovendo CW nei suoi confronti.

La Guerra Cognitiva probabilmente sta diventando - è diventata una linea d'azione permanente per ottenere la destabilizzazione di un leader politico, di una forza nemica, di un'economia.

Per essere ben compresi senza fraintendimenti, in modo molto schematico, possiamo dire che nel dominio operativo cyber, i belligeranti penetrano nelle reti di computer nemiche per raggiungere il software avversario e interromperlo per neutralizzare ciò che questo software contribuisce a produrre: dalla rete elettrica ai servizi bancari e così via.

La guerra dell'informazione consiste nel manipolare informazioni che sempre più spesso vengono veicolate attraverso mezzi informatici e digitali, cyber appunto: si vedano in tal proposito, anche se oramai datate, le campagne d'influenza politica effettuate da Cambridge Analytica[8].

La Guerra Cognitiva, infine, agisce sul modo in cui il cervello bersaglio elabora l'informazione. Nella sua concettualizzazione, la Guerra Cognitiva integra quindi queste altre forme di guerra, alla quale si aggiunge una parte essenziale che ha visto sviluppi recenti: la

[8] Per una panoramice generica sull'argomento si veda https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

neuroscienza cognitiva. In pratica è il “Lato Oscuro" della scienza e della ricerca compartimentale, volendo parafrasare Star Wars.

Sempre ragionando in termini “essenziali”, possiamo dire che se la Guerra informativa tenta di controllare ciò che osserva la popolazione bersaglio, la guerra psicologica controlla ciò che vede e sente la popolazione bersaglio, la guerra informatica tenta di interrompere le capacità tecnologiche di nazioni bersaglio, possiamo dire che la Guerra Cognitiva si concentra sul controllo di come pensa e reagisce una popolazione bersaglio, per poi utilizzare tecniche altre per “vincere senza combattere”, Sun Tzu[9] docet.

Cercare di influenzare l’opinione pubblica sin dall’ascesa della civiltà è sempre stato fatto; è un elemento essenziale, una componente delle strutture politiche in cui ci siamo evoluti fino ad oggi. Tuttavia, usare l’opinione pubblica come arma è uno sviluppo nuovo e minaccioso proprio per il modo in cui oggi interagiamo. L'avvento del mix Internet - social media - mass media ha reso possibile la manipolazione su larga scala delle diverse società attraverso messaggistica mirata, accessibile e multimodale, che, soprattuto oggi può esistere sotto la maschera dell’anonimato: individuare le singole fonti è diventato incredibilmente difficile; a meno che non si disponga tecnologia adeguata.

In campo militare, per la prima volta, la guerra non avrà a che fare con i corpi esposti: si occuperà di menti esposte: è la Guerra Cognitiva, Cognitive Warfare - CW, amplificata da strumenti IA.

Se l’intelligence in ambito COIN è basilare, l’intelligence in CW è fondamentale: IA e Social Media sono lo strumento essenziale per raccogliere informazioni in breve tempo sul target, modulare le diverse operazioni e prenderne possesso in maniera “indolore”, con il tempo giusto.

L’Intelligenza Artificiale sta portando, infatti, nuovi strumenti che facilitano la Guerra Cognitiva, che possono amplificarla e renderla ancora più accessibile e a basso costo, soprattutto quando si tratta di diffusione di fake news e disinformazione.

Tutte le campagne di fake news, in termini giornalistici forse un po’ antichi “bufale”, combinano informazioni reali e quelle distorte, fatti verosimili ma esagerati e notizie del tutto inventate, da qui la disinformazione che nasce dalla confusione derivante dal non riuscire a distinguere il “vero” dal “falso”, in un continuo gioco di specchi e di rimandi.

---

[9] Sūnzǐ Bīngfǎ cioè Il metodo militare di Sun Tzi - VI-V secolo a.C.

Tra i nuovi strumenti, che vengono usati, si segnalano i deepfake, video generati dall'intelligenza artificiale che possono mostrare una persona mentre recita un discorso che non ha mai effettivamente fatto: il loro pericolo è evidente, dato che qualsiasi personalità influente può essere costretta a dire qualsiasi cosa. Possono essere resi ancora più realistici mediante tecnologie che imitano il tono della voce di una persona e il suo accento. Esempi recenti an ambito politico si sono registrati in India: è il caso, in fatti, di due attori di Bollywood i cui deep fake, virali on line, sono contro la campagna elettorale di Narendra Modi. Nonostante le smentite e le cancellazioni i video girano ancora. Lo stesso politico indiano è stato fatto oggetto di un deep fake virale e così via.

Esiste poi il rischio associato ai corpi e ai volti generati dall'intelligenza artificiale che consente la creazione di numerosi account falsi sui social network con persone che non esistono e rende possibile umanizzare i "robot" per dare loro maggiore credibilità. L'IA generativa può essere di grande aiuto se non regolamentata nel diffondere informazioni false poiché può scrivere articoli, post e commenti su social network molto più velocemente e su scala più ampia di quanto potrebbe fare un gruppo di esseri umani, le troll factory di una volta possiamo dire che sono oramai un ricordo neanche troppo lontano.

Assomiglia alla conquista di un mercato ma non lo è appieno: è la manipolazione della percezione del mondo e della vita, Weltanschauung, per sostituirvi un nuovo prodotto preconfezionato secondo uso e bisogno dell'agente.

È necessario che si faccia su grandi numeri, i Big Data di una determinata realtà: la CW si fa su gruppi target, società partito stati etc., potremmo dire che è simile alla truffa e al raggiro o alla manipolazione di una singola vittima da parte di un singolo truffatore.

L'esposizione dell'ambito economico-finanziario a simili scenari è di facile comprensione e di elevata pericolosità, da qui può essere fatta derivare la ricerca di una "sovranità" dell'IA.

È notizia recente che la Turchia ha aperto la sua prima scuola per lo sviluppo di Intelligenza Artificiale interamente turca, come i dati che utilizzerà che saranno "turchi".

Ankara in questa scia "sovranista" nello sviluppo di algoritmi presi a creare una identità ben definita nella propria IA non è la sola.

Su questa stessa strada è il Giappone: la società giapponese di telecomunicazioni SoftBank sta investendo 150 miliardi di yen entro il 2025 per dotare le sue strutture informatiche della potenza necessaria per sviluppare un'intelligenza artificiale generativa di livello mondiale.

L'intelligenza artificiale generativa sta iniziando a essere integrata in servizi e prodotti in vari settori anche economici e finanziari. Secondo le ultime previsioni di Statista, ad esempio, il mercato giapponese dell'intelligenza artificiale generativa dovrebbe crescere fino a circa 13 miliardi di dollari entro il 2030, ovvero 17 volte più grande rispetto al 2023.

Al momento, le aziende tecnologiche statunitensi come Open AI sono all'avanguardia sia in termini di prestazioni che di investimenti. Le aziende giapponesi, tra cui NTT e NEC, sono entrate nel mercato, ma il numero di parametri nei loro modelli varia da diversi miliardi a diverse decine di miliardi. Open AI viaggia su altri elevati livelli.

Il mercato azionario nipponico sta rispondendo alla mossa di SoftBank di creare una propria intelligenza artificiale. Alla fine di marzo, il prezzo delle azioni della società ha raggiunto i 2.064 yen, il livello più alto dalla sua quotazione nel 2018. Gli investitori scommettono che l'intelligenza artificiale generativa sarà positiva per gli affari.

I paesi di tutto il mondo considerano l'intelligenza artificiale generativa a livello nazionale importante per la sicurezza economica dello stato. Per di più, il governo e le aziende giapponesi stanno iniziando a concentrarsi sulla "sovranità dei dati", ovvero sulla capacità di gestire i dati all'interno dei propri confini. Affidarsi alla tecnologia di altri paesi potrebbe rallentare la risposta a eventi imprevisti, come modifiche improvvise alle specifiche ed esigenze impreviste.

Lo stesso discorso vale ad esempio per i paesi dell'area CEE (Central and Eastern Europe), cioè quelli dell'Europa centrale ed orientale, dove lo sviluppo di IA proprie è considerato un acceleratore di sviluppo economico.

Secondo un recente studio di PwC, l'intelligenza artificiale ha il potenziale per contribuire fino a 15,7 trilioni di dollari all'economia globale entro il 2030, la capacità di trascendere i tradizionali limiti del capitale e del lavoro, l'intelligenza artificiale è vista come una forza trasformativa in grado di assistere decisori, leader aziendali ed esperti del settore in sfide significative come l'invecchiamento della popolazione, investimenti inadeguati in ricerca e sviluppo, complessità normative, produttività stagnante e talento carenze.

Ma non c'è solo l'aspetto economico finanziario, con i suoi innegabili potenziali di sviluppo, a caratterizzare la spinta sovrana verso IA nazionali e verso la sovranità dei dati: parallelo ad esso e molto spesso intrecciato vi è l'aspetto militare nelle sue molteplici forme e dinamiche, come quella dell'Intelligence e delle nuove frontiere della Guerra Cognitiva.

Nel mese di marzo, i delegati di 60 paesi si sono incontrati fuori Washington e hanno scelto cinque nazioni per guidare una iniziativa comune per esplorare nuovi sistemi di sicurezza per l'intelligenza artificiale militare e sistemi automatizzati.

Con la proliferazione dell'intelligenza artificiale negli eserciti di tutto il pianeta, dai droni d'attacco russi ai comandi combattenti americani, l'amministrazione Biden sta creando una spinta globale per "un uso militare responsabile dell'intelligenza artificiale e dell'autonomia" delle armi, iniziativa lanciata nel 2023 alla conferenza internazionale REAIM dell'Aia; da allora hanno aderito altre 53 nazioni.

I rappresentanti di 46 di questi governi, compresi gli Stati Uniti, più altri 14 paesi osservatori che non hanno ufficialmente approvato la Dichiarazione, si sono incontrati fuori Washington per discutere come attuare i suoi dieci principi generali, senza imporre standard statunitensi ad altri paesi con culture strategiche, istituzioni e livelli di sofisticazione tecnologica molto diversi.

I 150 delegati partecipanti hanno formato tre gruppi di lavoro per approfondire i dettagli dell'attuazione. È ben utile vederli almeno a grandi linee, perché le ricadute sulla vita di tutti i giorni e sul quella economica saranno tangibili.

Gruppo Uno: Assicurazione. Gli Stati Uniti e il Bahrein guideranno insieme il gruppo di lavoro "assicurazione", focalizzato sull'attuazione dei tre principi tecnicamente più complessi della Dichiarazione: che l'intelligenza artificiale e i sistemi automatizzati siano costruiti per "usi espliciti e ben definiti", con "test rigorosi, " e "protezioni adeguate" contro guasti o "comportamenti non intenzionali" – incluso, se necessario, un kill switch in modo che gli esseri umani possano spegnerlo.

Gruppo due: Responsabilità. Mentre gli Stati Uniti applicano la loro immensa competenza tecnica al problema, altri paesi si concentreranno sugli aspetti personali e istituzionali della salvaguardia dell'IA. Canada e Portogallo co-condurranno il lavoro sulla "responsabilità", incentrato sulla dimensione umana: garantire che il personale militare sia adeguatamente formato per comprendere "le capacità e i limiti" della tecnologia, che disponga di una documentazione "trasparente e verificabile" che spieghi come funziona. funziona e "prestano la dovuta attenzione".

Gruppo tre: Supervisione. Nel frattempo, l'Austria (senza un co-responsabile, almeno per ora) guiderà il gruppo di lavoro sulla "supervisione", esaminando questioni politiche di ampio respiro come la richiesta di revisioni legali sul rispetto del diritto umanitario

internazionale, la supervisione da parte di alti funzionari e eliminazione di "pregiudizi involontari".

Cosa potrebbe significare nella pratica l'attuazione di questi principi astratti? Forse la creazione di enti simili al Responsible AI Toolkit online del Pentagono, parte di una spinta del Dipartimento della Difesa per sviluppare strumenti accessibili al pubblico e persino open source per implementare la sicurezza e l'etica dell'IA? Al momento non è stato chiarito.

L'amministrazione Biden ha comunque emesso un ordine esecutivo sull'uso federale dell'intelligenza artificiale ad ottobre 2023; ha aderito alla Dichiarazione di Bletchley sulla sicurezza dell'intelligenza artificiale patrocinata dal Regno Unito nel novembre successivo e ha convinto l'Assemblea generale delle Nazioni Unite ad approvare all'unanimità una risoluzione guidata dagli Stati Uniti che richiedeva un'intelligenza artificiale "sicura, protetta e affidabile" per lo sviluppo sostenibile.

Sulla carta ci sono le premesse per un controllo dell'IA "militare" separato da quella civile, come se fossero due argomenti distinti e separati, cosa che di fatto non sono. Ciò è in parte dovuto al fatto che l'intelligenza artificiale militare è più controversa, con molti che chiedono un divieto legale vincolante sui "sistemi di armi autonome letali" su cui gli Stati Uniti, i suoi alleati e avversari come Russia e Cina, vorrebbero avere un certo margine di manovra di sviluppo.

I due binari vogliono essere paralleli ma di fatto sono complementari; quando si va ad incidere sulla società nei suoi diversi aspetti, economico tra gli altri, la separazione diventa molto labile. Le possibilità infinite fornite da strumenti IA in caso di una contrapposizione non cinetica tra stati comportano una vera e propria sovrapposizione di strumenti civili per fini militari con quelli puramente militari.

La sensibilità alla Guerra Cognitiva solleva molte domande e preoccupazioni. Come proteggersi da tali attacchi?

L'IA è solo una forma evoluta di arma, punto e basta; come una pistola non è pericolosa di per sé, è pericolosa se usata da enti /soggetti singoli per offendere. Pericolosa? al momento non lo è, potenzialmente lo è: Modello Skynet.

La convivenza tra intelligenza naturale e intelligenza artificiale è al centro di un nuovo dibattuto che ci sta costringendo a concepire la guerra come un ibrido, con i nostri pensieri e le nostre società sempre più modellati dalle macchine. La Guerra Cognitiva è già tra noi e i capitoli principali sono già in fase di scrittura a causa della crescente convergenza di

persone, informazioni e tecnologia attraverso i nostri social network. Parlando di Guerra Cognitiva, politica ed economica, e IA, con tutti i rischi “bellici” cinetici e non, la mente corre subito a Skynet.

Nella saga cinematografica di *Terminator*, Skynet, un'intelligenza artificiale superintelligente e una rete neurale progettata per la difesa nazionale, diventa auto-cosciente il 29 agosto 1997, alle 02:14, EDT.. Mentre i suoi operatori umani tentano di spegnerla, Skynet lancia un attacco nucleare contro la Russia per provocare una guerra nucleare, considerandola il modo più efficace per eliminare i nemici su tutti i fronti.

Ma nella “realtà effettuale delle cose”, oltre a essere un corriere, Skynet è un programma della National Security Agency degli Stati Uniti che esegue analisi di apprendimento automatico sui dati di comunicazione per estrarre informazioni su possibili sospetti terroristi. Lo strumento, nelle sue diverse varianti, viene/veniva utilizzato per identificare obiettivi che si spostano tra le reti cellulari.

Infine, Skynet è anche la capacità di comunicazione satellitare della difesa britannica, e in particolare una famiglia di satelliti per comunicazioni militari che forniscono servizi di comunicazione strategica alle forze armate del Regno Unito e alleati. I satelliti Skynet 5 sono la generazione più recente di satelliti militari del Regno Unito.

In conclusione facciamo nostro l’augurio del Maestro Yoda, personaggio della saga succitata: “May the Force be with us!”.

Il modello ucraino della Guerra cognitiva[10]

La guerra ha molte sfaccettature. C’è quella reale che si combatte al fronte dove muoiono i soldati e i civili, poi c’è la guerra economica fatta di analisi, studi della concorrenza, spionaggio industriale, e infine c’è la guerra cognitiva.

E mentre in Occidente ci si occupa delle declinazioni del termine in alte parti del mondo la guerra cognitiva ha delle branche e si occupa di temi specifici e si va dalle simulazioni delle epidemie all’annullamento della volontà, dalle campagne mediatiche per appoggiare un brand, un politico, una società fino a difendere o negare i diritti di un popolo. Sembra assurdo ma con i giusti algoritmi siamo in balia di giudizi che altri hanno scelto per noi e noi,

[10] AgcNews 12 maggio 2024

le vittime di questi bias cognitivi, studiati apposta per noi agiamo, convinti di scegliere invece stiamo facendo il gioco del nostro carnefice.

Quello che una volta era fantascienza ora è scienza. I primi a fare un largo uso della guerra cognitiva a Occidente quanto a Oriente sono stati i militari.

Tra i maestri in campo, che ci piaccia o no, ci sono i russi e i loro team del Center for Information and Psychological Operations. Ma anche gli ucraini non sono da meno, d’altronde la scuola è la stessa, in una chat di riferimento si apprende che le TsIPSO ucraine hanno dei gruppi di lavoro specifici.

“Durante la preparazione degli attacchi, lavora un intero gruppo, agendo secondo algoritmi chiari. E per sopprimere rapidamente la volontà di una persona, diversi uomini dei team TsIPsO partecipano ad un attacco psicologico, interpretando lo scenario del "poliziotto buono e cattivo", intimidendo allo stesso tempo la vittima e offrendo immediatamente una soluzione "semplice" al problema”.

Gli scenari per il funzionamento di TsIPsO sono molteplici, ma per gli attacchi di massa vengono utilizzati semplici algoritmi basati sulla sorpresa, l'aggressività e la rapida repressione della volontà di un interlocutore scoraggiato.

Secondo il team le fasi principali dell’attacco cognitivo sono tre: “In primo luogo, vengono studiate le reti sociali delle future vittime, vengono identificate le relazioni (professionali, familiari) e viene determinata una gamma di interessi e hobby”.

Nella seconda fase: “Si stabilisce un contatto diretto con la vittima e si forma un “ponte di fiducia””.

La terza fase: “è chiamata "PNL da combattimento" - la base delle tecniche manipolative è il forte impatto emotivo iniziale sulla vittima ("tuo marito è in prigionia", "è stato avviato un procedimento penale contro di te", ecc. .)”.

Secondo il team TsIPSO “Non dobbiamo permettere pause nel fare pressione su una persona: dopo aver preso in mano una vittima, la teniamo sempre in contatto, non permettendole di liberarsi. Questa continua esposizione a fattori psicologici subconsci aiuta gli aggressori a neutralizzare i meccanismi di difesa della vittima”.

Tra i segreti di una operazione ben riuscita: “Un gruppo sociale che soffre regolarmente di attacchi TsIPsO sono i parenti del personale militare russo che partecipa alla SVO (l’invasione dell’Ucraina, ndr). Sotto la minaccia di ritorsioni contro i loro cari, prigionieri in Ucraina, sono incoraggiati a intraprendere azioni illegali” in Russia.

Per reclutare i giovani, TsIPsO utilizza uno scenario diverso: “gli adolescenti vengono reclutati attraverso giochi di rete di computer. Agganciano le loro vittime a varie missioni e giochi nel sistema ARG (Alternate Reality Games), quando al giocatore vengono assegnati determinati compiti legati alla realtà di una particolare città o regione. Di conseguenza, per relativamente pochi soldi, agli adolescenti può essere affidata, ad esempio, la ricognizione sul campo, nonché alcune piccole missioni di sabotaggio”.

Information stuffing e Guerra Cognitiva[11]

Tra i problemi più rilevanti rispetto alla guerra cognitiva o guerre di informazioni-psicologiche c’è l’approccio sistematico, mentale e cognitivo sia in Occidente che in Oriente.

In attesa di un lavoro che porti a delle sistematizzazioni della materia con tanto di manuali ad uso e consumo del privato cittadino, gli analisti di PSYOP/CW hanno cercato di aiutare le persone a rispondere alla domanda: come riconoscere le bufale informative?

Tra le prime operazioni che consigliano gli esperti c’è il riconfigurare i localizzatori per una gamma di segnali ampia. Un analista riferisce: “Stanno succedendo troppe schifezze perché chiunque possa capirlo da solo. L’incertezza è presente letteralmente in ogni aspetto della vita, e si ritiene che lo diventerà solo di più in futuro”.

Una delle regole fondamentali dell'informazione e delle operazioni psicologiche e quindi anche della creazione di bufale è che una “psyop deve essere sempre pubblicata nella lingua del pubblico target a cui è diretta la psyop.”

Ad esempio, se mostri agli studenti di un corso sull'analisi delle informazioni e sulle operazioni psicologiche un’immagine degli indiani oppressi e chiedi informazioni sul pubblico di destinazione, molti studenti iniziano a esitare e dicono che il pubblico di destinazione sono gli indiani.

Questo è sbagliato. Perché il tuo meme presentato è scritto in italiano. Il pubblico target siamo tu ed io, cittadini italiani. L’obiettivo invece è ricordare alla gente che gli americani sono stati occupanti e oppressori del popolo indiano.

Tra le tecniche più utilizzate e di moda l'*information stuffing* è un metodo di diffusione delle informazioni, espresso nel riempimento improvviso del numero massimo di fonti con

---

[11] AgcNews 19 maggio 2024

informazioni che hanno una forte colorazione emotiva e servono a creare risonanza nella società. Il fattore più importante per indebolire tali tecniche è riconoscerle nella fase iniziale.

Saper riconoscere "l'imbottitura" e vedere per quali scopi è stata realizzata. Non siate una staffetta di informazioni "calde" – aspettate la risposta ufficiale dall'altra parte. Non affrettiamoci a dimostrare a tutti coloro che conosciamo che capiamo il problema a livello di esperto o superiore, senza nemmeno averne la minima idea. Ecco alcuni modi per evitare di diventare vittima di bufale informative.

Una cosa importante è capire che "la fuga di notizie" non significa che la notizia sia sicuramente falsa o provocatoria. Anche i fatti veri vengono spesso utilizzati per conferire credibilità a un messaggio falso. Ciò significa che sono necessarie una massima attenzione alle notizie, un ulteriore controllo dei fatti e la comprensione degli obiettivi e delle motivazioni dei partecipanti per capire se una notizia è una bufala oppure no.

Tra i segnali a cui dovremmo prestare attenzione è la mancanza di prove dell'informazione, ma vi sono fotografie di accompagnamento che suscitano, provocano forti emozioni - reazione di indignazione, rabbia, vergogna/disgusto, evitando appunto di fornire prove di quanto narrato.

Per esempio su Facebook: "un medico afferma che c'è un rimedio contro la caduta dei capelli che si chiama xyz". Un medico nell'immaginario collettivo è una figura affidabile, conoscitore della materia. Ma in questo caso: "un medico" senza nome ne cognome, senza dire specializzato in cosa, dove esercita ha molti elementi di una bufala.

Altro esempio notizie con foto e video, dove non c'è nulla che dimostri quanto riportato dal testo. Le notizie che si riferiscono a una persona, ma sono assenti dai canali personali e dalle pagine pubbliche, non hanno prove video. La dichiarazione o l'opinione di qualcuno, non correlata a eventi reali, ma diffusa attivamente. Come spesso accade nelle citazioni di personaggi famosi poi rivelatesi false. Notizie con una fonte volutamente nascosta. Spesso si legge: "una fonte ha detto al giornale". A volte i giornali non vogliono rivelare le fonti a volte nell'*information stuffing* si diffondono su molti canali social notizie in cui viene messo un dato reale affidabile ma la notizia è falsa per esempio: "Una fonte ha detto alla *CNN* che....". La testata giornalistica è famosa in tutto il mondo e quindi se lo dice la CNN acquisisce un elemento di affidabilità ma il messaggio ripotato così da una fonte anonima potrebbe celare il fatto che lo stesso messaggio riportato è falso.

In ogni caso se non si hanno a disposizioni software o IA per verificare le notizie a volte, fermarsi e riflettere su cosa ci vogliono dire ci aiuta a capire se un messaggio è falso o meno.

Nel 1200 in Giappone, i monaci buddisti leggevano i testi su tre livelli: 1) il dato enunciato dalla lettura della notizia: "una mela al giorno toglie il medico di torno"; 2) perché la notizia è arrivata a me qual'è il messaggio: la mela è un alimento sano e poco calorico; 3) qual'è l'obiettivo di chi mi da la notizia per esempio se a darmi l'informazione è un venditore di mele, l'obiettivo è vendere; se l'informazione mi viene data da un medico nutrizionista è insegnarmi a mangiare meglio.

È un antico metodo per verificare una tecnologica bufala.

Guerre cognitive a fumetti[12]

Nel 2021 si è tenuta la Conferenza NATO Innovation Network ed esattamente il 9 novembre 2021. E nella sessione dei lavori sull'open Innovation hanno presentato dei casi d'uso di Guerra cognitiva.

Tra i casi presentati c'è stato quello di Kristina Soukupova, presidente del Def Sec Innovation Hub della Repubblica Ceca. Soukupova, ha dichiarato di essere riuscita a creare un progetto educativo chiamato NATO Virtual Academy che è stato presentato agli studenti di relazioni internazionali e diplomazia.

Di conseguenza, DefSec ha lanciato il primo corso aperto online di massa che ha formato il personale civile e militare della NATO sulla sicurezza dei social media. Inoltre, il presidente Soukupova ha informato e presentato agli spettatori e ai partecipanti gli argomenti e i progetti portati avanti da DefSec. Ha inoltre affermato che il campo della guerra cognitiva è ancora relativamente nuovo e richiede quindi all'organizzazione di cercare costantemente nuove risposte.

Il team di DefSec ha ideato un nuovo progetto chiamato HACK THE MIND, che segue i principi di HACKATHON. Per spiegarci hackathon è un evento in cui persone diverse si riuniscono per risolvere problemi: è una maratona creativa dove di solito partecipano ingegneri e informatici e dove in tempi contemporanei si sono aggiunti sociologi, psicologi esperti di marketing.

---

[12] Agcnews 25 maggio 2024

HACKATHON è esso stesso un nome relativamente recente, se si pensa che il primo evento con questo nome è stato l'OpenBSD Hackathon a Calgary, in Canada, il 4 giugno 1999. Il termine "hackathon" viene dalla fusione delle parole hack, intesa come programmazione sperimentale e destrutturata, e "marathon", maratona. L'origine del nome spiega le due principali caratteristiche di questo evento: l'ambito informatico in cui nasce, e la resistenza, intesa come dedizione al raggiungimento dell'obiettivo.

Un hackathon dura dalle 24 alle 48 ore: posso durare anche di più, ma la norma è che rimangano limitati alla durata di un weekend. I partecipanti vengono divisi in team e messi di fronte ad una sfida. Hanno infatti un obiettivo comune: creare qualcosa che risolva un problema specifico, entro il tempo stabilito. Ciascun partecipante mette in gioco le proprie conoscenze ed abilità, a prescindere dal ruolo che occupa nella vita professionale al di fuori.

L'evento di DefSec ha avuto l'intento di raccogliere spunti legati ai temi della guerra cognitiva. È durato cinque mesi durante i quali hanno ricevuto molte richieste in forme diverse. Questo progetto li ha aiutati a creare la *Cognitive Warfare Dashboard*. DefSec ha deciso per il futuro di utilizzare l'idea di comunicare il proprio messaggio attraverso i fumetti. Pertanto, creando 4 eroi e attualmente se ne aspettano altri 4, al fine di presentare al grande pubblico una prospettiva diversa sulla guerra cognitiva. Dopo averlo stabilito, il materiale verrà valutato dal mondo accademico e dalla NATO.

DefSec non ha avuto una idea rivoluzionaria, quella dei fumetti, ma di certo è vincente per plagiare le menti e vincere una guerra senza combattere, perché a combattere saranno gli eroi.

Gli Stati Uniti in questo sono stati maestri in modo particolare con i Supereroi arrivati al grande pubblico a seconda delle necessita sociali del momento. Durante gli anni della Seconda Guerra mondiale mentre sul fronte europeo i militari morivano, in patria, cioè negli Stati Uniti nascevano i supereroi: Flash, Lanterna Verde e Blue Beetle debuttarono in quest'epoca.

Quest'era vide il debutto di uno dei primi supereroi femminili, il personaggio Fantomah dello scrittore-artista Fletcher Hanks, di un'antica donna egiziana senza età dei giorni nostri che poteva trasformarsi in una creatura dalla faccia di teschio con superpoteri per combattere il male. L'invisibile Scarlet O'Neil, un personaggio senza costume che combatteva il crimine e i sabotatori in tempo di guerra usando il superpotere dell'invisibilità creato da

Russell Stamm, avrebbe debuttato nell'omonimo fumetto del giornale pochi mesi dopo, il 3 giugno 1940.

Forse tra tutti il supereroe di cui tutti avevano bisogno in America a quei tempi era Capitan America che apparve per la prima volta stampato nel dicembre 1940, un anno prima dell'attacco a Pearl Harbor da parte del governo giapponese, quando l'America era ancora isolazionista. Creato da Joe Simon e Jack Kirby, il supereroe era l'incarnazione fisica dello spirito americano durante la Seconda guerra mondiale.

Ed ora riflettendo chi di noi non è cresciuto con un supereroe che ha guidato i nostri sogni e quindi plasmato innocentemente, forse le nostre menti? Siamo stati vittime dunque inconsapevoli di una guerra cognitiva che presentava un modello vincente, affascinante, modello che può essere sempre rivisto.

Ad esempio la serie a fumetti X-Men fu creata negli anni 60 del Novecento per l’accettazione della diversità dal modello sociale dominante: i protagonisti, quasi un cross over di altre serie a fumetti, erano caratterizzati da anomalie fisiche o psichiche che li rendevano totalmente diversi dal contesto sociale di riferimento e quindi, nella vita reale, vittime predestinate. Fumetti, serie tv, videogiochi e fortunatissime serie di film hanno contribuito a rendere “normale” la diversità.

Il segreto, nella guerra cognitiva è quello di imporre un messaggio senza farsi capire che dietro c’è una manipolazione mentale. Immedesimarsi in un supereroe significa comportarsi come lui, vivere come lui e quindi portare avanti una condotta sociale imposta.

Vogliamo fare un altro esempio. Quando si è iniziato a parlare di donne al potere si sono costruiti dei nuovi modelli di supereroi. A partire dagli anni 80’ dello corso secolo nascono personaggi famosi come Dazzler, She-Hulk, Elektra, Catwoman, Witchblade, Spider-Girl, Batgirl e Birds of Prey sono diventati protagonisti di titoli omonimi di lunga durata. I personaggi femminili iniziarono ad assumere ruoli di leadership in molte squadre di supereroi. Sono il riflesso di una società che chiede un cambiamento ma che è ancora guidata dagli uomini, le eroine non a caso sono tutte frutto di mani maschili, il riflesso del desiderio maschile di come vogliono le donne al potere: belle, magre, intelligenti, forti. Come i maschi ma belle come le donne, sensuali come le donne. Ma soprattutto devono fare ciò che disegna l’uomo.

La guerra cognitiva, dunque, ha anche un’altra caratteristica deve essere impiegata su larga scala e possibilmente nessuno deve capire di fare parte di quella “larga scala”.

Smart Phone con IA: comfort Zone o manipolazione? Dual use della call to action[13]

Da quando Russia e Stati Uniti per interposta persona, Ucraina, hanno di nuovo alzato la Cortina di Ferro, la questione della disinformazione, dei suoi meccanismi, o della manipolazione delle informazioni è tornata di gran moda senza pensare che di fatto nella disinformazione o manipolazione ci viviamo tutti i giorni.

Il metodo attraverso algoritmi e intelligenza artificiale che consente alle aziende di indurci a comprare ha un nome molto simpatico : "call to action" e ne siamo tutti vittime. La "call to action" significa persuadere le persone a compiere un'azione, acquistare un prodotto o accedere ad un servizio, rendendo ancora più efficaci Programmatic Advertising, Marketing Automation e Customer Care: sostanzialmente significa applicare l'Intelligenza Artificiale nel Marketing.

Esempi per i non addetti ai lavori: cercare un paio di scarpe on line, avere di ritorno per "x" giorni tutte le proposte di scarpe simili a quelle che stavate cercando; parlare con un'amica di un hotel raccomandato da amici per le vacanze e scoprire che sui tuoi social ci sono solo pubblicità di hotel con le caratteristiche e la zona di provenienza di quello da te citato al cellulare in una conversazione.

Ai nostri smart phone è stato insegnato dall'algoritmo e ora dalla IA a compiacerci, ai fini della vendita e del comfort e così nascono le app specializzate che fanno quello che una volta facevi benissimo da solo: cercano un ristorante, profilano una mappa per un percorso, ti consigliano le 10 cose più belle da vedere in vacanza. Tutto, tutto quello che vi viene in mente l'algoritmo lo può fare più velocemente e può ricercare in data base che voi nemmeno immaginate, e quindi vi risponde e vi compiace. Poi abbiamo gli assistenti che se abbiamo dei problemi e l'IA non ha risposto come vorremmo, ci aiutano, implementano dunque la capacità compiacerci.

In un articolo di *digital4.biz* si legge: "Dalle evidenze dell'ultimo censimento effettuato dagli Osservatori del Politecnico di Milano emerge che, ad oggi, la maggior parte delle progettualità legate all'impiego degli algoritmi AI nelle aziende riguarda le aree dell'assistenza clienti operata attraverso assistenti virtuali e chatbot. In particolare, i chatbot sono utilizzati da ben l'81% delle organizzazioni e sono, quindi, parecchio diffusi come pure gli assistenti vocali

[13] Agcnews 1 giugno 2024

(83%). Cresce, tuttavia, l'interesse verso i sistemi di raccomandazione per l'eCommerce, in virtù dell'efficacia dimostrata "sul campo" – un utente su quattro, secondo quanto dichiarato dagli intervistati, ha finalizzato un nuovo acquisto online dopo aver ricevuto un consiglio mirato". Insomma più è bravo il consigliere IA più le aziende vendono.

Nello stesso articolo: "Si chiama invece Artificial Intelligence Marketing (AI Marketing) il Marketing che usa l'Intelligenza Artificiale per interagire con i clienti, migliorare la comprensione del mercato e delle persone e suggerire – più rapidamente dell'uomo – le azioni da intraprendere per affinare le tecniche di persuasione".

"L'Intelligenza Artificiale nel Marketing sfrutta le più moderne tecnologie che rientrano nell'ambito dell'AI, come Machine Learning e Nlp – Natural Language Processing, integrate a tecniche matematiche/statistiche (come quelle delle reti bayesiane, modello grafico probabilistico che rappresenta un insieme di variabili con le loro dipendenze condizionali) e di Marketing comportamentale (behavioral targeting). Il tutto con un obiettivo molto chiaro e diretto: migliorare la capacità di persuasione per portare gli utenti a "convertire" la "call to action" aziendale, ossia a compiere un'azione che genera valore per l'utente stesso ma che ha un risvolto positivo anche per l'azienda".

E se questo per il marketing IA è il risvolto positivo, si vende di più facendo scegliere al cliente; c'è l'altra faccia della medaglia: se cerco informazioni su Hamas, il mio algoritmo IA cercherà di compiacermi e mi parlerà di Hamas, se poi il mio orientamento è filo palestinese mi proporrà su tutti i miei social solo la questione del conflitto in corso in chiave Hamas. La macchina mi deve compiacere e quindi sceglie per me le notizie che mi piacciono. Di fatto tutto quello che ha da dire Israele sulla questione rimane fuori dalla mia sfera di informazione e viceversa naturalmente. In questo modo si vanno creando nuove divisioni sociali: noi e loro. Ritorniamo al 0-1; 0-0; 1-1 del linguaggio booleano, mentre nella vita ci sono in ogni istante almeno 3000 diverse possibili scelte, come insegna il buddismo.

Situazioni intellettualmente molto pericolose perché poi quei noi e loro, una volta profilati con i giusti messaggi, possono essere animati e esposti a scelte apparentemente personali ma di fatto indotte senza conoscere fino in fondo le questioni per cui si stanno scontrando con l'altro.

Un esempio eclatante è stata la questione COVID 19. I no vax e pro vax si sono arrabbiati gli uni contro gli altri e tutti adducevano - parliamo di social sfera e non di dati scientifici - gli uni contro gli altri, le notizie che apparivano nella propria social sfera. Il tutto spesso senza

avere basi scientifiche né da una parte né dall'altra semplicemente fidandosi della loro comfort zone algoritmica. La macchina alla fine ti dice sempre quello che vuoi sapere.

La comfort zone può dunque essere un Grande Fratello a cui nessuno di noi può sfuggire. E se nel marketing per ovviare alla "call to action" ci basta spegnere il telefonino e fare una passeggiata per negozi, diventa più difficile sfuggire alla auto manipolazione che ci creiamo nella bolla informativa.

Oramai le notizie che vengono dalla social sfera sono anche accompagnate spesso da deepfake, fotografie manipolate, che esperti del settore infilano nella nostra bolla informata per avvallare la "correttezza" della informazione che leggiamo e che noi abbiamo chiesto alla macchina di trovarci e a quel punto convinti di avere ragione perché abbiamo informazioni e foto al seguito iniziamo la nostra battaglia per perorare cause che in realtà sono nella migliore delle ipotesi parzialmente veritiere.

Tra gli esempi più eclatanti di "call to action" non applicata al marketing: ci sono le campagne elettorali che hanno come obiettivo quello di convincerci a votare per un candidato piuttosto che per un altro. Attraverso i social media le aziende che possono comprare i nostri dati da altre "aziende specializzate" a cui noi abbiamo dato il consenso di raccogliere dati personali attraverso il "sì" ai cookie daranno un primo profilo della nostra vita: maschio, femmina, transgender, omosessuale, lesbica; tendente a destra o sinistra o incerto; vegano, vegetariano, onnivoro; magro, grasso, normale; e così via. La profilazione della nostra personalità è semplicissima: chi di noi non ha una app sulla salute dove abbiamo inserito a richiesta dati personali; chi di noi non ha mai partecipato a un sondaggio, una raccolta firme, un programma di dimagrimento o tonificazione, chi di noi non ha mai interpellato il cellulare per una ricetta di cucina?

Se avete risposto sì a tutte le domande siete stati profilati e siete pronti anche per essere manipolati da voi stessi e da coloro he hanno fatto della "persuasione on line" un mestiere. L'educazione all'uso della IA non dovrebbe essere ad appannaggio delle sole aziende che devono vendere - qualsiasi sia il prodotto - ma dovrebbe diventare una materia scolastica dove tutti noi dovremmo avere l'opportunità di imparare a interrogare l'IA senza essere vittime di manipolazioni.

Cyber mercenari al servizio della guerra reale[14]

La guerra cognitiva ha bisogno di strumenti. Per annichilire il nemico bisogna azzerare le difese: tutte a partire dalle infrastrutture critiche fino a cascata ai pacchetti di informazione che vanno veicolati nella social sfera e nei media tradizionali, o anche rubare pacchetti di informazioni volti al ricatto. Le operazioni informatiche sono spesso propedeutiche se non contemporanee a quelle cognitive.

Il CBO (Campaign Budget Optimization) ha dimostrato che le decisioni sulla struttura delle forze relative agli operatori informatici devono affrontare dei compromessi. Le operazioni di combattimento stanno rapidamente iniziando a superare la velocità con cui possono essere eseguite operazioni informatiche offensive. Ciò, a sua volta, riduce la capacità degli operatori informatici altamente qualificati di ottenere risultati.

Il modello CBO anche nel settore "vendita" si avvale di algoritmi intelligenti per distribuire in maniera automatica il budget tra i vari set di annunci, focalizzandosi sulle campagne performanti. Se sostituite la parola Budget con quella di costo per obiettivo il giro è fatto. La CBO analizza continuamente le performance dei vari ad set, allocando più risorse su quelli che stanno ottenendo risultati migliori.

Secondo *Usni.org* "All'inizio del conflitto, la Russia ha utilizzato operatori informatici d'élite per condurre sofisticate operazioni informatiche a sostegno dei suoi obiettivi militari. Tuttavia, il ritmo di queste operazioni è rallentato poiché la Russia ha ampliato le proprie capacità di accesso alla rete, lasciandola con capacità limitate mentre la guerra entra in una fase prolungata. Al contrario, le capacità informatiche dell'Ucraina erano inizialmente meno sviluppate, ma col tempo grandi forze, per lo più volontarie, si sono mobilitate a sostegno dell'Ucraina. I risultati preliminari della guerra russo-ucraina suggeriscono che il giusto equilibrio di potere potrebbe determinare se le forze informatiche rimarranno rilevanti dopo la salva iniziale o saranno relegate in secondo piano".

E ancora scrivono: "Per dirla senza mezzi termini, la guerra russo-ucraina mette l'una contro l'altra due diverse strutture di cyberpower: il modello russo orientato alle élite e il modello ucraino orientato ai volontari. L'approccio russo ha tradizionalmente enfatizzato un

[14] Agcnews 10 giugno 2024

corpo d'élite di operatori informatici che sviluppano capacità uniche progettate per operazioni ad alto impatto. Questo personale lavora principalmente nelle organizzazioni di sicurezza governative. Al contrario, le forze armate ucraine non disponevano di un corpo dedicato di personale informatico offensivo addestrato e hanno scelto di concentrare le loro limitate risorse governative sulle capacità difensive. In seguito all'invasione russa, l'Ucraina ha anche creato un'ampia rete di operatori civili volontari per condurre attività informatiche contro la Russia. I due modelli non si escludono a vicenda, ma ciascuno ha i propri punti di forza e di debolezza che diventano evidenti man mano che la guerra avanza".

Noi di AGC non siamo del tutto d'accordo, a dire il vero i volontari ucraini fanno parte per lo più dei cyber mercenari o di veri e propri gruppi mobilitati da fondi e capitali stranieri che sono accorsi a sostegno all'Ucraina contro la Russia. Tra i più famosi cyber mercenari, che non sappiamo se hanno o no preso parte alle campagne per l'Ucraina, ci sono, secondo il centro analitico globale Observer Research Foundation (ORF) l'NSO Group (israeliano) e Lazarus (Corea del Nord) .

Il think tank, con sede a Delhi, ritiene che gruppi di hacker come "Lazarus e fornitori di spyware o come NSO Group possano essere facilmente classificati come "mercenari informatici"", afferma il rapporto ORF. "Il mercato dei mercenari informatici si sta sviluppando rapidamente, poiché gli stati vogliono rafforzare la loro offensiva informatica potenziale per condurre vari tipi di operazioni, pur mantenendo "negabilità plausibile per evitare l'identificazione"".

Un cybermercenario è considerato un attore economicamente vantaggioso, poiché il cliente non deve) spendere soldi per il reparto risorse umane, manutenzione permanente e formazione. I paesi meno sviluppati non possono permettersi capacità informatiche offensive avanzate, quindi spesso ricorrono ai loro servizi per essere un attore a pieno titolo nell'arena geopolitica.

Nel 2019, il mercato dei servizi cyber mercenari era stimato a 12 miliardi di dollari. Il concetto di "mercenario" è stato ampliato a "mercenario informatico": una persona, un gruppo di persone o individui assunti dai clienti per condurre operazioni offensive o difensive informatiche contro determinate reti e infrastrutture.

Ci sono filiali e centri di ricerca di mercenari informatici nei paesi UE a causa di lacune e lacune nella legislazione. Molti governi non esitano a ricorrere ai servizi di mercenari

informatici con il pretesto di proteggere la sicurezza nazionale, e gli strumenti utilizzati possono essere utilizzati per scopi contraddittori.

I mercenari informatici oggi offrono una vasta gamma di servizi, tra cui cyber intelligence, digital forensics e pentesting. Possono anche sferrare attacchi informatici distruttivi come danni alle infrastrutture e furto di informazioni. L'uso di servizi cyber mercenari sta diventando popolare nelle guerre ibride, poiché gli stati non vogliono sporcarsi direttamente, cercando di ridurre al minimo la possibilità di imputazione, proteggendo così il proprio paese da conseguenze legali.

Quando la guerra cognitiva serve agli hacker…[15]

Google Mandiant ha pubblicato un rapporto sull'APT42 iraniano (aka Mint Sandstorm, Charming Kitten, TA453), analizzando in dettaglio i suoi tre cluster di attività principali, nonché una panoramica degli attacchi recenti e dell'attuale arsenale di malware.

APT utilizza vari schemi di ingegneria sociale per ottenere l'accesso alle reti delle vittime, compresi gli ambienti cloud, prendendo di mira le ONG occidentali e mediorientali, i media, il mondo accademico, i servizi legali e gli attivisti. In alcuni casi, gli hacker si sono spacciati per giornalisti e organizzatori di eventi, consegnando inviti a conferenze o documentazione alle vittime.

Questo è un caso classico di "ottenimento della fiducia". Nelle lezioni di marketing avanzato o di analisi comportamentale ti dicono che la prima cosa che bisogna fare per costringere qualcuno a fare qualcosa che "vuoi tu" è quello di entrare nella sfera della fiducia della "vittima". In questo caso hanno consegnato qualcosa per entrare nella sfera della fiducia come inviti a conferenza per entrare nei loro cloud. E le vittime hanno consegnato in fiducia i loro segreti senza saperlo.

Schemi avanzati di ingegneria sociale hanno consentito all'APT42 iraniano di raccogliere credenziali e ottenere l'accesso agli ambienti cloud. Successivamente, i dati di interesse strategico per l'Iran sono stati rubati, facendo affidamento su funzioni integrate e strumenti open source per eludere il rilevamento.

Inoltre, i ricercatori notano le recenti operazioni APT42 che coinvolgono malware, tra cui due nuove backdoor: NICECURL e TAMECAT. Forniscono agli hacker l'accesso iniziale come interfaccia per eseguire comandi o distribuire malware aggiuntivo.

---

[15] Agcnews .eu del 17 Giugno 2024

Mandiant ha identificato e descritto tre cluster di infrastrutture APT42 per la raccolta di credenziali da obiettivi nei settori politico e pubblico, media e ONG.

Hanno tutti TTP simili per prendere di mira le credenziali delle vittime (e-mail di spear phishing), ma differiscono in diversi domini, modelli di cloaking, trappole e temi.

Queste backdoor forniscono un'interfaccia flessibile di esecuzione del codice che può essere utilizzata come punto di partenza per distribuire malware aggiuntivo o eseguire manualmente comandi sul dispositivo.

NICECURL è scritto in VBScript e può caricare moduli aggiuntivi per l'esecuzione, incluso il data mining e l'esecuzione di comandi arbitrari.

È stato rilevato per la prima volta nel gennaio 2024 e la catena di infezione è stata precedentemente documentata anche da Volexity

Più tardi, a marzo, Mandiant trovò un campione di TAMECAT. Serve come fulcro per l'esecuzione di contenuti PowerShell o C# arbitrari.

Entrambi sono stati utilizzati in una campagna di spear phishing su larga scala per prendere di mira organizzazioni non governative, governative e intergovernative in tutto il mondo.

Nel rapporto sono presentati in dettaglio esempi di phishing e un'analisi tecnica completa degli attacchi monitorati e degli strumenti IOC.

La Distopia nasce dalla confusione controllato-controllore[16]

Tra i pericoli preannunciati nello sviluppo dell'Intelligenza Artificiale la questione di creare cittadini di serie B e cittadini di serie A. Ovvero quelli che detengono la tecnologia e quelli che la useranno per non parlare poi dei cittadini di serie C, ovvero quelli che non avranno accesso all'IA.

La questione sul tavolo di oggi parte da un vecchio adagio pronunciato da Alberto Sordi uno dei suoi film: "La Guera è Guera": OpenAI ha nominato l'ex direttore della US NSA, il generale Paul Nakasone, oggi in quiescenza, nel suo consiglio di amministrazione.

A farne notizia il blog aziendale di OpenAI[17] che ha pubblicato informazioni sulla nomina del generale a quattro stelle Paul M. Nakasone come membro del consiglio di amministrazione della società. Ex direttore della NSA e contemporaneamente capo del Cyber

[16] AgcNews 22 giugno 2024

[17] https://openai.com/index/openai-appoints-retired-us-army-general/

Command statunitense (2018-2024), Nakasone è diventato ampiamente noto grazie alla sua dichiarazione: "Sto conducendo operazioni informatiche offensive contro la Russia ".

"La nomina di Nakasone, uno dei principali esperti di sicurezza informatica, riflette l'impegno di OpenAI per la sicurezza e la protezione ed evidenzia la crescente importanza della sicurezza informatica poiché l'impatto delle tecnologie di intelligenza artificiale continua a crescere", come si legge sul blog OpenAI.

Nakasone diventerà membro del Comitato per la Sicurezza sotto il Consiglio di Amministrazione della società. Sarà responsabile di illuminare il consiglio di amministrazione sulle decisioni critiche in materia di sicurezza, inclusi "tutti i progetti e le operazioni OpenAI".

OpenAI spera di capire come l'Intelligenza Artificiale possa essere utilizzata per rafforzare la sicurezza informatica rilevando e rispondendo rapidamente alle minacce dirette contro di essa.

Dal blog si evince che che l'Intelligenza Artificiale abbia il potenziale per apportare vantaggi significativi in questo settore a molte istituzioni che sono spesso prese di mira da attacchi informatici, come ospedali, scuole e istituti finanziari. Non si fa cenno però delle opportunità al contrario. Eppure la nomina Nakasone porta anche nell'immaginario collettivo attacchi informatici a tutela degli Stati Uniti.

Il Generale è uno dei massimi esperti di sicurezza informatica, sviluppo tecnologico e difesa informatica globale. Durante la sua carriera come ufficiale dell'esercito, ha svolto un ruolo chiave nella creazione dello U.S. Cyber Command. È stato il direttore più longevo di USCYBERCOM e ha anche guidato la National Security Agency, dove è stato incaricato di proteggere l'infrastruttura digitale degli Stati Uniti e di sviluppare le capacità di difesa informatica statunitense. Ha ricoperto posizioni di comando e di staff a tutti i livelli dell'esercito americano, prestando servizio in unità informatiche d'élite negli Stati Uniti, nella Repubblica di Corea, in Iraq e in Afghanistan.

OpenAI ora ha una potente leva per promuovere i propri interessi tra i militari attraverso l'ex vertice del Comando Informatico, che nel corso degli anni ha sviluppato connessioni significative in tutte le più alte sfere del potere negli Stati Uniti. È possibile quindi che i militari spingano un domani per l'utilizzo di robot basati su ChatGPT e fare lobbying usando le tecnologie OpenAI.

C'è però un problema di fondo relativo al conflitto di interesse: il controllato e il controllante sono la stessa cosa. Ciò potrebbe significare la creazione di uno immaginario scenario distopico, tenendo conto del fatto che il Generale supervisionerà la sicurezza informatica dell'azienda: a priori si può pensare che tutto ciò che viene stampato, tutto ciò di

cui si parla, qualsiasi codice e richiesta non solo privata ma anche pubblica, verranno elaborati e monitorati da algoritmi che ha generato OpenAI. Se ciò si realizzasse, lo spionaggio degli utenti starebbe raggiungendo un nuovo livello piuttosto che garantirne la sicurezza la riservatezza.

Le IA entrano direttamente in politica. Votereste per loro? [18]

Non solo India tra le elezioni che hanno visto l'utilizzo si IA nella campagna elettorale; Molti paesi asiatici hanno visto l'utilizzo di strumenti IA in momenti delicati delle elezioni.

Ad esempio, quando Prabowo Subianto ha voluto ammorbidire la sua immagine tra i giovani elettori indonesiani, il team della sua campagna ha tirato fuori un volto sorridente: una versione digitale di se stesso in stile cartone animato, riporta *Nikkei*.

Nelle sue due precedenti candidature senza successo, il generale in pensione ha cercato di presentarsi come un leader forte, immagine che non bucava l'elettorato giovanile che anzi vedevano il generale come un pericolo. Il suo avatar digitale, parte di una corsa per la presidenza dell'Indonesia quest'anno, ha dimostrato come il potere dell'Intelligenza Artificiale sia basilare in contesti delicati per diversi motivi come ad esempio nelle elezioni in Asia quest'anno.

La traduzione tramite intelligenza artificiale ha avuto un ruolo importante nelle recenti elezioni generali in un'India linguisticamente diversificata. Il partito al potere Bharatiya Janata ha utilizzato l'intelligenza artificiale per doppiare i discorsi del primo ministro Narendra Modi, pronunciati in hindi, in altre otto lingue, inclusa un'interpretazione in tempo reale in tamil.

Anche il Giappone, dove la tecnologia ha un ruolo minore in politica, ha trovato usi per l'intelligenza artificiale. Nel frattempo, il Regno Unito ha prodotto il primo "candidato AI" al mondo. L'uomo d'affari Steve Endacott è in corsa per un seggio a Brighton nelle elezioni generali del mese prossimo, ma si è impegnato a lasciare le decisioni effettive a "AI Steve", un alter ego digitale sviluppato dalla sua azienda. AI Steve può ricevere feedback dai suoi elettori 24 ore su 24 e elaborare politiche basate su di esso.

Alcuni usi della tecnologia non sono così benigni. Prima delle primarie statali americane per le imminenti elezioni presidenziali, gli elettori democratici hanno ricevuto chiamate automatizzate da una riproduzione AI della voce del presidente Joe Biden che diceva loro di non votare.

[18] Agcnews 02 luglio 2024

La Federal Communications Commission ha affermato che le chiamate robotiche che utilizzano tali deepfake sono illegali. Un gruppo di 20 aziende tecnologiche, tra cui Microsoft e Meta, si sono impegnate a collaborare per combattere le interferenze elettorali legate all'intelligenza artificiale.

Alcuni stanno lavorando su misure di salvaguardia come limitare le domande a cui i chatbot possono rispondere sulle elezioni e implementare filigrane digitali per identificare i contenuti creati dall'intelligenza artificiale.

Altri usi dell'intelligenza artificiale nelle elezioni rientrano in un'area grigia dal punto di vista legale. In Indonesia, un deepfake del defunto dittatore Suharto ha esortato gli elettori a sostenere il suo ex partito in un video realizzato con l'intelligenza artificiale generativa.

Dopo le elezioni in Pakistan a febbraio, è circolato sui social media un video AI di un discorso di vittoria dell'ex primo ministro Imran Khan, che è in carcere con l'accusa di corruzione.

I ricercatori stanno esaminando l'idea di utilizzare l'intelligenza artificiale per assumere alcuni ruoli di elettori e di politici in quella che è stata soprannominata "democrazia aumentata".

Cesar Hidalgo, capo del Centro per l'apprendimento collettivo di Tolosa, in Francia, ha proposto di incorporare nel processo decisionale i "gemelli digitali" formati sulle preferenze politiche degli individui. Queste rappresentazioni digitali permetterebbero agli elettori di fornire feedback sulle politiche proposte in modo più diretto rispetto alla scelta dei rappresentanti ogni pochi anni.

A maggio, durante le elezioni indiane, il think tank Policy 4.0 ha pubblicato i risultati di un esperimento utilizzando "gemelli AI". Una volta fornite le opinioni politiche e le priorità dei singoli elettori, sono stati in grado di prevedere per quale delle due principali coalizioni ciascuno avrebbe votato con una precisione superiore al 90%.

La politica 4.0 sostiene che questi gemelli IA possono aiutare gli elettori a scegliere candidati che effettivamente corrispondono alle loro convinzioni politiche senza essere influenzati dalla disinformazione.

Sarà vero o saranno anch'essi frutto di manipolazione informativa?

L'OGGI VISTO CON GLI OCCHI DI IERI: SCENARI

Attore principale di questa rivoluzione bellica è l'utilizzo di algoritmi complessi che definiamo con un terminologia semplicistica: Intelligenza artificiale. Questo utilizzo diffuso, dalla gestione e programmazione di una dieta alimentare a quello della difesa di una nazione ha avuto e avrà un grosso impatto sulla vita reale e tangibile di tutta la popolazione mondiale. Scopriamo che quanto era temuto nel 2015 è divenuto realtà, o incubo, nel 2024, e le visioni sull'impatto della IA sulla percezione del mondo contemporaneo che tutti noi abbiamo sono attorno a noi, sempre di più.

Le IA e il futuro del lavoro[19] (2015)

Con la diffusione della robotica e del prossimo avvento delle intelligenze artificiali si capovolgerà il nostro sistema socio-economico, legato sul lavoro e sulla produzione.

Questa riflessione arriva dal polemologo statunitense John Robb e da una serie di studi, sempre effettuati negli Usa, e raccolti in un testo, non ancora uscito in lingua italiana: The future of the professions, scritto da Richard e Daniel Susskind [20] .
Per Robb: «Fino a trecento anni fa, il mondo è stato basato sul lavoro svolto dalle persone, in gran parte a mano. Le competenze e i metodi necessari per farlo erano in gran parte nelle menti delle persone che facevano il lavoro. Abbiamo poi creato organizzazioni per aggregare le persone necessarie per fare lo stesso lavoro su larga scala e creato delle corporazioni per proteggere la conoscenza.

Per superare i limiti di un mondo fatto a mano, abbiamo sviluppato qualcosa di nuovo: l'automazione. Abbiamo trasformato il mondo attraverso la costruzione di macchine (sia hardware che software) che non lavorano per noi. L'automazione si basa su un processo scientifico che comprende come funzionano le cose e su di un processo di progettazione che trasforma le idee scientifiche in macchine che funzionano nella realtà.
Tuttavia, ora abbiamo raggiunto i limiti dell'automazione. Come mai? Perché l'automazione è

---

[19] Agcnews 22 Ottobre 2015

[20] Susskind Richard, Susskind Daniel, *The Future of the Professions. How Technology Will Transform the Work of Human Experts*, Updated Edition, Oxford University Press 2015 - seconda edizione 2022 . Edizione italiana, successiva alla pubblicazione dell'articolo: *Il futuro delle professioni*, Rubettino, 2023

limitata dalla capacità degli esseri umani di costruire modelli cognitivi (sia scientifici che ingegneristici) necessari per costruire le macchine che creano.

Per superare questi limiti, ora stiamo costruendo macchine cognitive che possono costruire i propri modelli di funzionamento e realizzazione. A differenza delle macchine che ci forniscono automazione, queste macchine non sono costruite in modo tradizionale e possono affrontare problemi molto più complessi di qualsiasi cosa fatta dall'automazione. Il grande cambiamento è che queste macchine si costruiscono. Hanno sviluppato le loro abilità nello stesso modo in cui gli esseri umani hanno fatto: attraverso l'apprendimento, la formazione e l'esperienza. Tuttavia, possono imparare molto più velocemente (apprendimento profondo) di noi e una volta fatto, possono condividere le loro nuove abilità con altre macchine in tutto il mondo istantaneamente (...)

È il più grande cambiamento nella tecnologia che abbiamo visto (...) sta andando a sconvolgere le regole dell'economia, della guerra e della politica che pensavamo immutabili». Su questo cambiamento epocale, che riguarderà anche e soprattutto, le professioni liberali intervengono i due studiosi statunitensi con la loro analisi su "Come la tecnologia trasformerà il lavoro degli esperti umani" come riporta il sottotitolo del libro, *The Future of the professions*.

I Susskind predicono il declino delle professioni di oggi e descrivono le persone e i sistemi che li sostituiranno. In una società interconnessa dalla Rete, non avremo bisogno di medici, insegnanti, contabili, architetti, religiosi, consulenti, avvocati, e molti altri, come invece è avvenuto nel XX secolo.

Sistemi sempre più capaci, dalla tele-presenza all'intelligenza artificiale, porteranno un cambiamento fondamentale nel modo in cui il "know-how" degli specialisti è disponibile nella società, spezzando i monopoli del professionismo di oggi perché antiquati, opachi e non più convenienti. Al loro posto, si proporranno sei nuovi modelli per la produzione e distribuzione di competenze nella società.

L'indagine dei Susskind solleva importanti questioni pratiche e morali relative sopratutto alle prospettive per l'occupazione. Gli interrogativi dei Susskind e di Robb vengono confermate dalle previsioni del Boston Consulting Group secondo cui entro il 2025, fino a un quarto dei posti di lavoro sarà sostituito da una software intelligente o robot, e da uno studio dell'Università di Oxford secondo cui il 35% dei posti di lavoro esistenti nel Regno Unito sono a rischio di automazione nei prossimi 20 anni.

Un esempio è dato dai tassisti che a breve, entro il 2015 afferma la *Bbc*, nel Regno Unito saranno sostituiti da taxi completamente automatizzati e il governo starebbe modificando il codice della strada per consentirne la circolazione. In Cina esiste la prima fabbrica robot, oggi in costruzione a Dongguan. La Sehnzhen Evenwin Precision Technology mira a ridurre del 90% l'attuale forza lavoro di 1.800 unità. Da settembre 2014, poi, 505 fabbriche a Dongguan hanno investito 4,2 miliardi di yuan nei robot, con l'obiettivo di sostituire più di 30mila lavoratori. Inoltre, la Foxconn, produttore di dispositivi elettronici come l'iPhone di Apple, prevede una forza lavoro robotica del 30% nei prossimi cinque anni.

I droni e la guerra futura[21] (2016)

Un interessante post del polemologo John Robb su *Global Guerrillas* ci fa entrare direttamente nel futuro dei robot intelligenti.

Per Robb, «la rivoluzione in corso nella robotica è dovuta a rapidi progressi nella capacità dei robot di pensare. Ciò significa che la maggior parte dei grandi miglioramenti che vedremo nell'uso di robot autonomi in guerra sarà dovuto alla ricerca di loro nuovi utilizzi (...) È ora possibile trasformare un semplice drone a basso costo in un'arma, quasi efficace come un missile guidato di precisione (Precision Guide Missile, Pgm) che costa centinaia di migliaia di dollari (...) più intelligente è il drone, meglio può simulare le prestazioni dei molto più costosi Pgm (...) i droni low cost sono ormai abbastanza intelligenti per approssimare le prestazioni di sistemi missilistici con un po 'di creatività (...) Dieci droni potrebbero decollare autonomamente a intervalli di 1 minuto.

Ogni drone potrebbe seguire un piano di volo su una porzione prescelta di un aeroporto. All'arrivo, una fotocamera digitale potrebbe identificare l'ala più vicina di un aeromobile. Il drone potrebbe atterrare autonomamente nel mezzo di quell'ala e bruciare il carburante all'interno (...) La maggior dell'aeroporto e quasi tutti gli aerei sarebbero distrutti (...) Anche i semplici piattaforme robotiche di oggi possono essere estremamente efficaci come armi. Al ritmo attuale di miglioramento in intelligenza artificiale, la situazione sarà molto più interessante molto, molto presto.

[21] Agcnews 14 febbraio 2016

È possibile operare in modo creativo con l'intelligenza delle macchine a basso costo (...) Abbiamo bisogno di riconoscerlo prima che lo facciano i cattivi». Stiamo assistendo a qualcosa di simile fatta in Siria e in Iraq dai combattenti di Daesh, terribile a dirsi.

La notte buia dell'informazione è all'orizzonte[22] (2017)

Una nuova riflessione del polemologo John Robb ci illumina sui rischi, gravi, che la neonata campagna social contro le informazioni "dirompenti", cioè che creano disturbo nella rete, potrebbe creare in un post su *Global Guerrillas*. Si tratta di riflessioni che presagiscono un futuro cupo e arido, sul modello di quanto narrato da George Orwell in 1984; un Grande Fratello planetario omni-invasivo.

«Facebook ha appena dichiarato guerra alle informazioni "dirompenti". Oltre a centinaia di nuovi censori umani, stanno formando dei censori IA (*Intelligenza Artificiale*, ndr) capaci di identificare e cancellare informazioni "inaccettabili" trovate nelle discussioni di tutti e due i miliardi di membri in tempo reale. Questo sviluppo mette in luce il pericolo reale rappresentato da un mondo socialmente collegato in rete. Il pericolo reale che un mondo interconnesso dai social network deve affrontare non è la perturbazione della rete.

Come abbiamo visto in numerose occasioni, il pericolo posto dalle informazioni e dagli eventi dirompenti dura poco. Il turbamento, anche se potenzialmente doloroso e a breve termine, non dura nel tempo, né è veramente dannoso a lungo termine. Infatti, il vero pericolo posto da un mondo che lavora su Internet è proprio l'opposto di una perturbazione.

Questo pericolo è un'ortodossia on line che abbraccia tutti. Un' identicità di pensiero e di approccio applicata da centinaia di milioni di utenti socialmente collegati a Internet. Un'ortodossia globale e spietata che restringe il pensiero pubblico ad un quadro ideologico unico, sterile e arido. Una rete dirigente che previene il dissenso e ci blocca nella stagnazione e nell'inevitabile fallimento (...)

Questa rete decisionale esiste già. Ha già milioni di membri online e sta crescendo e approfondendosi ogni giorno che passa – estendendo i suoi viticci ai media, al servizio pubblico, alle società di tecnologia e al mondo accademico. Non c'è dubbio che col tempo eserciterà un'influenza decisiva anche sull'intero governo.

---

[22] Agcnews 25 Settembre 2017

Tuttavia, per esercitare un controllo autoritario sul nostro processo decisionale, ha bisogno di controllare il flusso di informazioni nella nostra società. Il semplice controllo del dibattito online è insufficiente. Per il potere reale, la rete dominante deve controllare i flussi di informazioni sulla nostra infrastruttura di informazione – Facebook, Google e Amazon – e questo è esattamente il potere che sta ottenendo ora.

Tuttavia, per quanto grande e potente sia già questa rete, continuo a credere che questo futuro sia reversibile. Abbiamo ancora poco tempo prima che una lunga notte scenda in tutto il mondo».

L'Intelligenza Artificiale batte l'uomo nel comprendere la lingua[23] (2018)

L'Intelligenza Artificiale sviluppata dall'Alibaba Group ha vinto in una gara di comprensione della lettura di un testo con gli esseri umani.

È la prima volta che le macchine pensanti hanno superato le prestazioni degli umani. La più grande società cinese di commercio online ha sviluppato un modello di apprendimento che ha ottenuto un punteggio più alto sul Dataset Stanford Question Answering, un test di comprensione della lettura su larga scala, con più di 100.000 domande, secondo un comunicato di Alibaba ripreso da *Scmp*.

L'11 gennaio, il software IA di Alibaba ha ottenuto 82,44 punti sul test, rispetto a 82,304 raggiunto dagli esseri umani.

Fino ad ora il linguaggio era generalmente considerato un terreno difficile da padroneggiare per le macchine.

Questa vittoria ha implicazioni ampie per il modo in cui le aziende utilizzeranno l'apprendimento automatico per i lavori di assistenza clienti, finora affidati a dipendenti dei call center per gestire le richieste di informazioni.

Alibaba ritiene, inoltre, che la tecnologia di base possa essere applicata gradualmente a numerose applicazioni come il servizio clienti, i tutorial museali e la risposta online alle richieste dei clienti.

Le machine IA potrebbero identificare le domande poste dai consumatori e cercare le risposte più rilevanti nei documenti già preparati; il sistema attualmente funziona meglio

---

[23] Agcnews 17 Gennaio 2018

solo con domande che offrono risposte chiare. Se la lingua o le espressioni sono troppo vaghe o se non c'è una risposta preparata, il bot potrebbe non funzionare correttamente; fino ad ora.

Alibaba ha impiegato macchine IA con tecnologia di base nel corso degli anni, rispondendo a enormi volumi di richieste di informazioni in entrata durante il periodo di vendita; oltre ai servizi online, un certo numero di aziende tecnologiche cinesi, tra cui Alibaba, hanno prodotto altoparlanti musicali intelligenti in grado di identificare comandi vocali e trovare risposte e soluzioni. Gli sviluppi e gli impatti sul mondo del lavoro sono tutti da verificare, comunque.

L'incubo Terminator è dietro l'angolo. L'Onu lancia l'allarme[24] (2019)

Il Segretario Generale delle Nazioni Unite António Guterres ha esortato gli esperti di intelligenza artificiale riuniti a Ginevra a portare avanti il loro lavoro per limitare lo sviluppo di sistemi di armi letali autonomi, o Laws (Lethal Autonomous Weapons Systems). In un messaggio al gruppo di esperti che si occupa dello sviluppo di simili tecnologie, il segretario Generale Onu ha detto che «le macchine con il potere e la discrezione di prendere vite senza coinvolgimento umano sono politicamente inaccettabili, moralmente ripugnanti e dovrebbero essere proibite dal diritto internazionale».

Nessun paese o forza armata è a favore di sistemi d'arma "completamente autonomi" che possono togliere la vita umana, ha insistito Guterres, prima di accogliere con favore la dichiarazione del gruppo dell'anno scorso, secondo cui «la responsabilità umana per le decisioni sull'uso dei sistemi d'arma deve essere mantenuta, poiché la responsabilità non può essere trasferita alle macchine». Sebbene questo annuncio del 2018 sia stata un'importante linea rossa del gruppo di esperti della Convenzione sulle armi convenzionali, Ccw, Gutierres ha detto che, mentre alcuni Stati membri ritengono necessaria una nuova legislazione, altri preferirebbero misure e orientamenti politici meno rigorosi che potrebbero essere concordati, riporta un comunicato Onu.

[24] Agcnews 27 Marzo 2019

Tuttavia, è giunto il momento che il gruppo di esperti «dia seguito» alla legge, ha detto Gutierres aggiungendo: «È vostro compito ora di restringere queste differenze e trovare la via più efficace per andare avanti».

La riunione Laws era una delle due previste per il 2019, e fa seguito alle precedenti riunioni di esperti governativi nel 2017 e 2018 alle Nazioni Unite a Ginevra. L'agenda del gruppo riguarda questioni tecniche relative all'uso di sistemi d'arma autonomi e letali, comprese le sfide che la tecnologia pone al diritto umanitario internazionale, così come l'interazione umana nello sviluppo, nel dispiegamento e nell'uso della tecnologia emergente.

Nei precedenti commenti sull'Intelligenza artificiale, il segretario Generale ha paragonato la tecnologia a «una nuova frontiera» con «progressi che si muovono a velocità di curvatura». «L'intelligenza artificiale ha il potenziale per accelerare i progressi verso una vita dignitosa, in pace e prosperità, per tutte le persone», aveva detto al vertice mondiale sull'AI for Good Global Summit del 2017, aggiungendo che ci sono anche questioni etiche come la sicurezza informatica, i diritti umani e la privacy.

Anche l'IA metterà l'uniforme per andare in guerra[25] (2021)

Iniziamo a vivere nell'era delle Intelligenze artificiali. Questo periodo presenta nuove opportunità anche per i militari: per le truppe d'élite cominciano però a esserci i primi problemi; per esempio, la potenza e la connettività dei computer dietro le linee nemiche, o la portata dell'attenzione umana in ambienti pericolosi e stressanti.

Lo U.S. Special Operations Command, o Socom, sta lavorando con la Defense Advanced Research Projects Agency, Darpa, su nuovi progetti ed esperimenti per portare l'intelligenza artificiale agli operatori che lavorano nei tipi di ambienti in cui la potenza di calcolo e i dati per eseguire applicazioni AI commerciali non sono presenti, riporta Defense One.

Gran parte dell'intelligenza artificiale che i consumatori usano ogni giorno funziona collegando il dispositivo a grandi capacità di cloud computing altrove: i più comuni sono Siri e Alexa che derivano il loro potere dall'elaborazione del linguaggio naturale, un sottoinsieme in rapida crescita dell'IA che applica l'apprendimento automatico al linguaggio parlato. Ma ci sono centinaia di altri strumenti di IA che i consumatori usano senza nemmeno rendersene

[25] Agcnews 10 Maggio 2021

conto: come i programmi di geolocalizzazione per evitare ingorghi stradali; la maggior parte degli sviluppatori in questo campo si basano sull'essere in grado di raggiungere attraverso una rete enormi database e potenti centri di cloud computing. È infatti un ambiente civile e commerciale.

Quel tipo di connettività è spesso carente dove operano le forze speciali statunitensi, ma l'AI potrebbe ancora fare una grande differenza nel raggiungimento delle missioni. Così l'U.S. Socom sta sviluppando una comprensione completamente nuova non solo di come espandere l'intelligenza artificiale, ma di come ridurla, determinando quali problemi gli operatori affrontano potrebbero essere superati con una piccola quantità di intelligenza artificiale. Questa è una sfida fondamentalmente diversa da quella del mondo commerciale.

Darpa sta lavorando su "dare al computer i problemi che sono appena oltre la scala dell'operatore umano". Non è il tipo di scelte di progettazione che i programmatori affrontano nella Silicon Valley, dove le capacità di cloud off-platform sono sempre disponibili.

Ma non è solo la larghezza di banda ad essere limitata in questi ambienti. Anche l'attenzione umana è un bene scarso. Ecco perché Socom sta lavorando con gli operatori per capire meglio quando hanno più attenzione da dare alla comunicazione della macchina cercando un compromesso di carico cognitivo umano-macchina adeguato alla situazione e alla persona.

Le IA ora si mettono a fare le giornaliste[26] (2021)

In Cina, come altrove si ottengono sempre più notizie tramite video inoltre la pubblicità si sposta verso le piattaforme online; in Cina si spostano molto verso la piattaforma di Tencent Holdings.

Per far questo, Pechino ha trovato la soluzione. Xinhua Zhiyun Technologies ha sviluppato una soluzione per i fornitori cinesi di notizie: un sistema automatizzato alimentato da intelligenza artificiale per generare video clip di notizie, il Media Brain.

Xinhua Zhiyun ha come azionista di controllo *Xinhua News Agency* seguita a ruota da Alibaba Group Holding. Si tratta di una combinazione potente, riporta NIkkei, dato che i siti web e le

---

[26] Agcnews 9 Giugno 2021

applicazioni in Cina sono spesso chiamati a fare affidamento su notizie *Xinhua*, mentre Alibaba è stato uno dei principali sviluppatori e investitori del paese nelle tecnologie Ai, riporta *Nikkei*.

Media Brain in 15 secondi può preparare un video di due minuti dall'applicazione mobile di *Xinhua* con un giornalista virtuale, supportato da grafica animata, musica e foto. Tale velocità è un vantaggio dato che 873 milioni di cinesi hanno guardato video clip online l'anno scorso, secondo il China Internet Network Information Center ufficiale.

Le funzioni Ai come il riconoscimento vocale sono in grado di trascrivere e digitalizzare i discorsi; il sistema rileverà quale parte del discorso è importante o degna di essere evidenziata attraverso segni tra cui il battito delle mani.

Alibaba è nota per lo sviluppo di funzioni AI come l'apprendimento automatico e l'esperienza di big data attraverso la piattaforma di cloud computing di e-commerce. La Cina ha adottato l'Intelligenza Artificiale, impiegando la tecnologia per valutazioni mediche a distanza e nei tribunali per valutare le prove e guidare i giudici verso la coerenza nei loro giudizi.

Nel settore delle notizie, l'app Jinri Toutiao di ByteDance, il più grande successo della società prima di TikTok e la controparte cinese Douyin, ha attirato l'attenzione utilizzando l'Ia per far emergere articoli strettamente legati ai gusti degli utenti. Sogou, la seconda più grande società di ricerca del paese, il mese scorso ha lanciato un'app animata alimentata dall'intelligenza artificiale per fornire notizie con il linguaggio dei segni cinese.

Xinhua Zhiyun ha circa 900 clienti aziendali tra cui pubblicazioni provinciali come *Zhejiang Daily* e *Xinjiang Daily*. Secondo *Xinhuanet.com*, la joint venture ha generato entrate l'anno scorso di 87 milioni di yuan, in crescita del 74% rispetto all'anno precedente, mentre la sua perdita netta è quintuplicata a 37 milioni di yuan. *Xinhuanet.com* valuta l'impresa, che ha 380 dipendenti, a 2,4 miliardi di yuan nei suoi libri. Recentemente ha venduto il 6% della sua quota originale del 51% a Chinese Universe Publishing and Media Group, un'altra società statale.

Secondo la società, i giornalisti non dovrebbero temere Media Brian: «Si tratta solo di standardizzare alcuni processi banali, liberando risorse in modo che i reporter possano concentrarsi sul reportage sul campo (...) Originariamente, per produrre una notizia, i reporter potrebbero passare il 70% del tempo sul campo e il 30% in redazione. Ma con la tecnologia, possiamo aumentare questo rapporto a 80/20 o addirittura 90/10».

La guerra è affare troppo serio per lasciarlo ai robot[27] (2022)

I russi starebbero sperimentando armamenti con Intelligenza Artificiale, nella guerra russo-ucraina. Ma non in maniera estensiva.

Ci sono diverse ragioni potenziali per questo. La più probabile è che non si fidino dell'IA per un uso indipendente sul campo di battaglia. Sappiamo anche che i cinesi e gli iraniani stanno esaminando la militarizzazione dell'IA, ma non ci sono molte informazioni aperte.

L'IA killer è ben presente nel futuribile fantascientifico.

Film come *The Terminator* e *WarGames* erano avvertimenti su simili armi fuori dal controllo umano. In un famoso episodio di Star Trek, all'IA viene permesso di controllare l'astronave Enterprise durante un'esercitazione militare e provoca morte e distruzione finché il capitano Kirk e il suo equipaggio non riprendono il comando. Fino ad oggi, questo tipo di questioni erano solo fiction. Oggi i progressi tecnici ci costringono ad affrontarli davvero.

Gli Stati Uniti si sono dimostrati riluttanti a permettere alle IA di operare in modo indipendente sul campo di battaglia senza la supervisione di un umano. Tuttavia, la situazione potrebbe cambiare se un avversario mostrasse un deciso vantaggio tattico e operativo nell'uso dell'IA. Non c'è dubbio che l'IA possa prendere decisioni più velocemente degli operatori umani, ma resta da chiedersi se tali decisioni siano le migliori.

La fuga di Osama bin Laden nel 2001 dalle montagne di Tora Bora, in Afghanistan, è stata in gran parte attribuita al ponderoso processo decisionale della cellula di puntamento del Comando Centrale degli Stati Uniti, in cui un comitato di ufficiali non riusciva a mettersi d'accordo per sparare finché l'obiettivo previsto non era scomparso nelle sue caverne.

Il Center for Emerging Threats and Opportunities, Ceto, del Corpo dei Marines ha intrapreso un esperimento per verificare se un processo decisionale simulato dall'intelligenza artificiale potesse migliorare il problema del targeting. A due squadre è stata data una serie identica di 20 problemi di puntamento che simulavano un velivolo senza pilota Predator armato di missili Hellfire. I problemi variavano da semplici a molto complessi. Alcuni coinvolgevano civili mescolati a combattenti nemici ostili.

La prima squadra era una cellula di puntamento umana composta da personale di intelligence, un avvocato operativo e uno specialista di affari pubblici, e guidata da un ufficiale operativo esperto, simile al gruppo decisionale nella situazione di Tora Bora. La

[27] Agcnews 21 Novembre 2022

seconda squadra ipotizzava che il Predator avesse a bordo un'intelligenza artificiale con capacità decisionale di sparare o non sparare. Il singolo umano che simulava l'IA aveva una serie di criteri rigorosi su cui basare le decisioni, simulando la programmazione del computer. I risultati sono stati molto interessanti. Non sorprende che la simulazione dell'IA abbia preso decisioni più velocemente della squadra di puntamento, ma entrambe hanno preso la decisione sbagliata circa il 20% delle volte. Le situazioni in cui le due squadre sbagliavano erano generalmente diverse ma, come nel combattimento reale, nessuna delle due era immune da errori.

La grande differenza era la responsabilità. La squadra umana poteva essere ritenuta responsabile delle sue decisioni e in genere ha scelto la strada della sicurezza quando sembravano essere presenti civili innocenti. L'IA era meno vincolata e doveva agire rigorosamente entro i limiti delle istruzioni di programmazione. In un caso, ha sparato contro una tenda da sole sotto la quale un gruppo di insorti armati si era riparato, uccidendo un gruppo di acquirenti in un souk simulato. Situazioni come questa sollevano la questione di chi sarebbe responsabile delle morti.

Sarebbe la persona o le persone che hanno programmato l'IA? Sarebbe il produttore? Potremmo sempre smantellare il velivolo, ma cosa risolverebbe?

Il vero problema rimane quello morale. Tranne che nel caso di combattimenti tra robot, l'uso dell'IA richiederà che il robot decida di eliminare vite umane.

In una certa misura, oggi utilizziamo un limitato processo decisionale computerizzato nelle armi. I missili Cruise e altri sistemi "spara e dimentica" volano da soli verso gli obiettivi, ma la decisione iniziale di ingaggiare è ancora presa con la presenza di un uomo. Se vengono uccisi degli innocenti, c'è una catena di responsabilità.

I danni collaterali ai civili si verificheranno sempre in guerra, e si faranno dei compromessi in termini di vite amiche salvate, ma si tratta di decisioni umane. Lasciare gli esseri umani fuori dal gioco non dovrebbe basarsi solo su considerazioni tecniche. Si tratta di una questione potenzialmente seria quanto le mine terrestri e le armi chimiche e nucleari.

Se la guerra è troppo importante per essere lasciata solo ai generali, dobbiamo chiederci se la vogliamo nelle mani dei robot.

Il conflitto ucraino accelera la corsa alle armi autonome[28] (2023)

L'esercito americano sta intensificando il suo impegno per lo sviluppo e l'uso di armi autonome, come confermato da un aggiornamento di una direttiva del Dipartimento della Difesa. L'aggiornamento, rilasciato il 25 gennaio 2023, è il primo in un decennio a concentrarsi sulle armi autonome di intelligenza artificiale.

Segue un relativo piano di attuazione rilasciato dalla Nato il 13 ottobre 2022, volto a preservare il "vantaggio tecnologico" dell'alleanza in quelli che a volte vengono chiamati "robot assassini".

Entrambi gli annunci riflettono una lezione cruciale che i militari di tutto il mondo hanno imparato dalle operazioni di combattimento in Ucraina e Nagorno-Karabakh: l'intelligenza artificiale armata è il futuro della guerra, riporta *AT*.

Queste armi, che sono un incrocio tra una bomba e un drone, possono librarsi per lunghi periodi in attesa di un bersaglio. Per ora, tali missili semi-autonomi vengono generalmente utilizzati con un significativo controllo umano sulle decisioni chiave.

Ma, mentre le vittime aumentano in Ucraina, aumenta anche la pressione per ottenere vantaggi decisivi sul campo di battaglia con armi completamente autonome: robot che possono scegliere, dare la caccia e attaccare i loro obiettivi da soli, senza bisogno di alcuna supervisione umana.

Questo mese, un importante produttore russo ha annunciato l'intenzione di sviluppare una nuova versione da combattimento del suo robot da ricognizione Marker, un veicolo terrestre senza equipaggio, per aumentare le forze esistenti in Ucraina. Droni completamente autonomi sono già utilizzati per difendere le strutture energetiche ucraine da altri droni.

I fautori di sistemi d'arma completamente autonomi sostengono che la tecnologia manterrà i soldati fuori pericolo tenendoli fuori dal campo di battaglia. Consentiranno inoltre di prendere decisioni militari a velocità sovrumane, consentendo capacità difensive radicalmente migliorate.

Attualmente, le armi semi-autonome, come le munizioni vaganti che inseguono e si fanno esplodere sui bersagli, richiedono un "umano nel giro". Possono raccomandare azioni, ma richiedono ai loro operatori di avviarle.

[28] Agcnews 24Febbraio 2023

Al contrario, i droni completamente autonomi, come i cosiddetti "cacciatori di droni" ora schierati in Ucraina, possono tracciare e disabilitare i veicoli aerei senza pilota in arrivo giorno e notte, senza bisogno dell'intervento dell'operatore e più velocemente dei sistemi d'arma controllati dall'uomo.

Molte ong si oppongono al loro uso sostenendo che le forze armate che investono maggiormente in sistemi d'arma autonomi, inclusi Stati Uniti, Russia, Cina, Corea del Sud e Unione Europea, stanno lanciando il mondo in una nuova corsa agli armamenti costosa e destabilizzante. Una conseguenza potrebbe essere che questa nuova e pericolosa tecnologia cada nelle mani di terroristi e altri al di fuori del controllo del governo.

La direttiva aggiornata del Dipartimento della Difesa cerca di affrontare alcune delle principali preoccupazioni. Dichiara che gli Stati Uniti utilizzeranno sistemi d'arma autonomi con "livelli adeguati di giudizio umano sull'uso della forza".

Human Rights Watch ha rilasciato una dichiarazione affermando che la nuova direttiva non chiarisce cosa significhi la frase "livello appropriato" e non stabilisce linee guida per chi dovrebbe determinarlo.

La direttiva aggiornata include anche un linguaggio che promette un uso etico di sistemi d'arma autonomi, in particolare istituendo un sistema di supervisione per lo sviluppo e l'impiego della tecnologia e insistendo sul fatto che le armi saranno utilizzate in conformità con le leggi internazionali di guerra esistenti.

Ma il diritto internazionale attualmente non fornisce un quadro adeguato per comprendere, tanto meno per regolamentare, il concetto di autonomia delle armi.

L'attuale quadro giuridico non chiarisce, ad esempio, che i comandanti sono responsabili di capire cosa attiverà i sistemi che utilizzano o che devono limitare l'area e il tempo in cui tali sistemi opereranno.

L'aggiornamento del Pentagono dimostra un impegno simultaneo a dispiegare sistemi d'arma autonomi e a rispettare il diritto internazionale umanitario. Resta da vedere come gli Stati Uniti bilanciano questi impegni, e se un tale equilibrio è possibile.

Il Comitato internazionale della Croce Rossa, custode del diritto internazionale umanitario, insiste sul fatto che gli obblighi legali di comandanti e operatori «non possono essere trasferiti a una macchina, un algoritmo o un sistema d'arma».

In questo momento, gli esseri umani sono ritenuti responsabili della protezione dei civili e della limitazione dei danni da combattimento assicurandosi che l'uso della forza sia proporzionato agli obiettivi militari.

Se e quando le armi artificialmente intelligenti vengono schierate sul campo di battaglia, chi dovrebbe essere ritenuto responsabile quando si verificano morti civili inutili? Non c'è una risposta chiara a questa domanda molto importante.

L'FMI prevede molti rischi nel mondo del lavoro[29] (2023)

Anche l'FMI si preoccupa dell'Intelligenza Artificiale e die suoi impatti socioeconomici.

Il vicedirettore generale del Fondo Monetario Internazionale, Gita Gopinath, ha chiesto martedì la definizione di regole globali per evitare gli elevati costi sociali derivanti dalla massiccia perdita di posti di lavoro dovuta all'uso dell'intelligenza artificiale. «Quando si parla di IA, abbiamo bisogno di più di nuove regole», ha sottolineato la direttrice.

Secondo il FMI, non solo l'intelligenza artificiale rivoluzionerà i mercati del lavoro, ma lo farà in modo insospettabile e molto negativo, perché anche le posizioni altamente qualificate sono a rischio. Gopinath ha avvertito che non c'è alcuna garanzia che i benefici alla fine supereranno i costi e ha chiesto una serie di regole "veramente globali" per evitare tensioni sociali derivanti da massicce perdite di posti di lavoro.

In un discorso tenuto a Glasgow in occasione del 300° anniversario della nascita di Adam Smith, Gopinath ha affermato che l'IA potrebbe contribuire a invertire il rallentamento della crescita della produttività globale, automatizzando alcuni compiti cognitivi e dando origine a nuove funzioni a più alta produttività da far svolgere all'uomo. Ma questo potrebbe avere un costo significativo in termini di occupazione.

Oltre ai potenziali aumenti di produttività, Gopinath ha osservato che l'IA potrebbe "scuotere il mercato del lavoro in modi senza precedenti", avvertendo che, dopo la recente perdita di posti di lavoro a media qualifica a causa dell'automazione, l'IA potrebbe influenzare le occupazioni e i settori in modo diverso rispetto alle precedenti ondate di automazione.

---

[29] Agcnews 8 Giugno 2023

A questo proposito, ha ricordato che studi recenti suggeriscono che l'IA potrebbe ridurre la polarizzazione del mercato del lavoro, esercitando una pressione al ribasso sui salari per i posti di lavoro a più alta retribuzione, nonché appiattendo la struttura gerarchica delle aziende, aumentando il numero di lavoratori in posizioni junior e diminuendo il numero di quelli in posizioni dirigenziali medie e alte.

«Il numero di posti di lavoro interessati potrebbe essere schiacciante», ha dichiarato l'alto funzionario del FMI, per il quale non è possibile garantire che i guadagni dei vincitori siano sufficienti a compensare i perdenti. «È molto probabile che l'IA sostituisca semplicemente i posti di lavoro umani senza alcuno sforzo per creare nuovi posti di lavoro più produttivi per gli esseri umani», quindi, nonostante il potenziale dell'IA, ha esortato a considerare l'ampio effetto negativo che potrebbe avere sull'occupazione e lo sconvolgimento sociale che potrebbe causare, riporta *MercoPress*.

Parlando di Adam Smith, l'economista del FMI ha sostenuto che la "mano invisibile" da sola potrebbe non essere sufficiente a garantire ampi benefici alla società dall'introduzione dell'IA, per cui vede l'urgente necessità di regolamentazioni forti e intelligenti per garantire che questa innovazione sia sfruttata a beneficio della società.

«Quando si parla di IA, non bastano nuove regole. Dobbiamo riconoscere che potrebbe essere un gioco completamente nuovo e che richiederà un approccio completamente nuovo alle politiche pubbliche», ha affermato, aggiungendo che la proposta presentata dall'UE è un inizio incoraggiante.

A questo proposito, ha trovato "incoraggiante" che il G7 abbia formato un gruppo di lavoro per studiare l'IA. «Abbiamo bisogno di un insieme di regole veramente globale», ha difeso Gopinath, sottolineando che, data la velocità con cui la tecnologia avanza, il tempo è essenziale.

IA: Rischio esiziale per l'uomo o evoluzione dell'intelligenza?[30] (2023)

L'intelligenza artificiale rappresenta un rischio esistenziale per l'umanità e deve essere incatenata prima che sia troppo tardi? Ma quali sono questi scenari di disastro e in che modo le macchine potrebbero spazzare via l'umanità?

[30] Agcnews 16 Luglio 2023

La maggior parte degli scenari letterari, e quindi filmici su simili disastri iniziano nello stesso modo: le macchine supereranno le capacità umane, sfuggiranno al controllo umano e si rifiuteranno di essere spente, riporta *NST*.

«Una volta che abbiamo macchine che hanno un obiettivo di autoconservazione, siamo nei guai», ha detto Yoshua Bengio, informatico canadese, noto soprattutto per il suo lavoro sulle reti neurali artificiali e sul deep learning. È professore presso il Department of Computer Science and Operations Research dell'Université de Montréal e direttore scientifico del Montreal Institute for Learning Algorithms.

Ma poiché queste macchine non esistono ancora, immaginare come potrebbero condannare l'umanità è spesso lasciato alla filosofia e alla fantascienza.

Il filosofo Nick Bostrom ha scritto di una "esplosione di intelligenza" che dice accadrà quando macchine superintelligenti inizieranno a progettare macchine proprie.

Ha illustrato l'idea con la storia di un'intelligenza artificiale superintelligente in una fabbrica di graffette. All'intelligenza artificiale viene assegnato l'obiettivo finale di massimizzare la produzione di graffette e quindi «procede convertendo prima la Terra e poi pezzi sempre più grandi dell'universo osservabile in graffette».

Le idee di Bostrom sono state respinte da molti e definite come fantascienza, anche perché separatamente Bostrom ha sostenuto che l'umanità è una simulazione al computer e ha sostenuto teorie vicine all'eugenetica.

Di recente Bostrom si è anche scusato dopo che è stato portato alla luce un messaggio razzista che ha inviato negli anni '90 del Novecento. Tuttavia, i suoi pensieri sull'intelligenza artificiale sono stati estremamente influenti, ispirando sia Elon Musk che il professor Stephen Hawking.

Se le macchine superintelligenti devono distruggere l'umanità, hanno sicuramente bisogno di una forma fisica. Tutti ricordiamo il cyborg dagli occhi rossi interpretato da Arnold Schwarzenegger, inviato dal futuro per porre fine alla resistenza umana da un'intelligenza artificiale nella saga di *The Terminator*; quel tipo di macchina è sì un'immagine seducente, ma gli esperti hanno spazzato via l'idea.

«È improbabile che questo concetto di fantascienza diventi realtà nei prossimi decenni, se non mai», ha scritto il gruppo della campagna Stop Killer Robots in un rapporto del 2021. Tuttavia, il gruppo ha avvertito che dare alle macchine il potere di prendere decisioni sulla vita e sulla morte è un rischio esistenziale; come capita col dibattito sui robot killer.

L'esperta di robot, Kerstin Dautenhahn, della Waterloo University in Canada, ha minimizzato queste paure. Ha detto che è improbabile che l'intelligenza artificiale fornisca alle macchine capacità di ragionamento più elevate o le infonda il desiderio di uccidere tutti gli umani, riporta *AFP*.

«I robot non sono malvagi», ha detto, anche se ha ammesso che i programmatori potrebbero fargli fare cose malvagie. Uno scenario meno apertamente fantascientifico vede "cattivi attori" che usano l'intelligenza artificiale per creare tossine o nuovi virus e scatenarli nel mondo.

Modelli di linguaggio di grandi dimensioni come GPT-3, che è stato utilizzato per creare ChatGPT, risultano essere estremamente bravi a inventare nuovi agenti chimici dagli effetti devastanti.

Un gruppo di scienziati che utilizzavano l'intelligenza artificiale per aiutare a scoprire nuovi farmaci ha condotto un esperimento in cui hanno ottimizzato la loro intelligenza artificiale per cercare invece molecole dannose. Sono riusciti a generare 40.000 agenti potenzialmente velenosi in meno di sei ore, come riportato nella rivista *Nature Machine Intelligence*.

Joanna Bryson, esperta di intelligenza artificiale della Hertie School di Berlino ha affermato di poter immaginare qualcuno che elabori un modo per diffondere più rapidamente un veleno come l'antrace.

Le regole di Hollywood impongono che i disastri epocali debbano essere improvvisi, immensi e drammatici, ma se la fine dell'umanità fosse lenta, silenziosa e non definitiva?

«La nostra specie potrebbe finire senza successore», afferma il filosofo Huw Price in un video promozionale per il Centro per lo studio del rischio esistenziale dell'Università di Cambridge. Ma ha detto che c'erano "possibilità meno desolate" in cui gli esseri umani potenziati dalla tecnologia avanzata potevano sopravvivere. «Le specie puramente biologiche alla fine finiscono, in quanto non ci sono umani in giro che non hanno accesso a questa tecnologia abilitante», ha detto. L'apocalisse immaginata è spesso inquadrata in termini evolutivi.

Stephen Hawking ha sostenuto nel 2014 che alla fine la nostra specie non sarà più in grado di competere con le macchine di intelligenza artificiale, dicendo alla *BBC* che potrebbe "significare la fine della razza umana". Geoffrey Hinton, che ha trascorso la sua carriera costruendo macchine che assomigliano al cervello umano, ultimamente per Google, parla in

termini simili di "superintelligenze" che semplicemente sorpassano gli umani. Di recente ha detto all'emittente statunitense *PBS* che è possibile che "l'umanità sia solo una fase passeggera nell'evoluzione dell'intelligenza". E adesso poi arriva la nuova fondazione di Elon Musk sull'intelligenza artificiale, sembra quasi un altro blockbuster di fantascienza.

Sembra...

In Finanza non ci può fidare dell'IA[31] (2024)

Non ci si può ancora fidare dell'intelligenza artificiale per prendere decisioni sui tassi di interesse, ha affermato un importante capo di un'autorità bancaria, sostenendo che il software manca ancora di capacità di giudizio.

Ma l'intelligenza artificiale potrebbe rendere più semplice per i criminali lanciare attacchi informatici, ha avvertito Chia Der Jiun, capo dell'Autorità monetaria di Singapore, riporta *AF*.

Ha affermato che l'intelligenza artificiale viene utilizzata in alcuni modelli economici e in aree come il rilevamento delle frodi, ma ha sottolineato che non è in una fase in cui potrebbe "soppiantare il giudizio umano".

"Sebbene non sotto forma di agenti conversazionali, l'intelligenza artificiale è già ampiamente utilizzata per aiutare a rilevare e prevenire le truffe attraverso modelli di apprendimento automatico. La grande flessibilità di questi algoritmi di intelligenza artificiale consente inoltre loro di adattarsi efficacemente all'evoluzione dei metodi di truffa online. Consentendo di analizzare enormi volumi di dati in tempo reale e aiutando a identificare modelli che potrebbero indicare attività fraudolente, "i chatbot potranno contribuire a migliorare le indagini svolte dagli analisti", riporta la società LexinNexis.

"C'è molta capacità di giudizio necessaria per comprendere e avere una visione del percorso futuro dell'inflazione (...) e della trasmissione della politica monetaria", ha detto Chia durante una sessione del panel della Banca dei Regolamenti Internazionali sull'uso dell'intelligenza artificiale.

"Forse un giorno si potrà incolpare l'intelligenza artificiale per gli errori di politica monetaria", ha scherzato l'amministratore delegato della banca centrale di Singapore. "Ma se la colpa è dell'uomo, allora sarà l'uomo a dover giudicare".

[31] Agcnews 13 Maggio 2024

Chia, che ha assunto la carica di capo del MAS all'inizio dell'anno, ha anche avvertito che il rischio principale è che l'intelligenza artificiale venga utilizzata dai criminali informatici.

"Un'altra dimensione di cui non si parla molto è che l'intelligenza artificiale ha il potenziale per democratizzare – non in senso positivo – ma per democratizzare l'accesso al malware", ha affermato Chia.

C'erano già strumenti disponibili online, ha detto, "per persone che non sono troppo sofisticate nelle loro competenze tecniche" da utilizzare per lanciare attacchi informatici. "È uno spazio che dobbiamo guardare".

FMI: a rischio il 60 % dei posti di lavoro per l'IA[32] (2024)

Il direttore del Fondo monetario internazionale ha espresso preoccupazione per l'impatto dell'intelligenza artificiale sui mercati del lavoro, aggiungendo che il mondo ha avuto poco tempo per "prepararsi" alla tecnologia.

L'intelligenza artificiale sta colpendo la forza lavoro globale "come uno tsunami", ha dichiarato il 13 maggio il direttore generale del FMI Kristalina Georgieva durante un evento a Zurigo. "Abbiamo pochissimo tempo per preparare le persone e le aziende", ha aggiunto, riportano *Reuters* e *AF*.

Intervenendo all'Istituto svizzero di studi internazionali, Georgieva ha osservato che l'intelligenza artificiale potrebbe avere un impatto sul 60% dei posti di lavoro nelle economie avanzate e sul 40% dei posti di lavoro in tutto il mondo nei prossimi due anni.

Per molte aziende, tuttavia, tale impatto ha già iniziato a manifestarsi. La società di collocamento Challenger, Gray & Christmas, Inc. ha osservato in un rapporto di febbraio che i tagli di posti di lavoro legati all'intelligenza artificiale sono in aumento negli Stati Uniti da maggio 2023. Ciò è dovuto al fatto che le aziende si stavano muovendo verso lo sviluppo della tecnologia o dipendevano da essa per sostituire alcune tecnologie, compiti e ruoli.

Il rapido progresso dell'intelligenza artificiale sta attualmente influenzando l'occupazione nei media e nella tecnologia, ma i suoi effetti "cominciano a farsi sentire" in altri settori, aggiunge il rapporto. A marzo, secondo quanto riferito, IBM ha iniziato a licenziare i

[32] Agcnews 15 Maggio 2024

dipendenti in ruoli non a contatto con i clienti, con l'obiettivo di sostituirli con l'intelligenza artificiale.

L'anno scorso il capo dell'azienda aveva dichiarato che l'azienda stava pianificando di rallentare o sospendere le assunzioni in 26.000 ruoli che potrebbero essere svolti tramite intelligenza artificiale e automazione, ha riferito la rivista *CRN*. Quel numero rappresentava circa il 10% della forza lavoro dell'azienda.

Nel frattempo, circa il 40% e il 26% dei posti di lavoro rispettivamente nei mercati emergenti e nei paesi a basso reddito sono a rischio a causa dell'intelligenza artificiale, ha osservato in precedenza il Fondo monetario internazionale.

Secondo PwC, l'intelligenza artificiale e le tecnologie correlate potrebbero sostituire circa il 26% dei posti di lavoro esistenti in Cina.

Georgieva ha precedentemente invitato i politici a gestire questa "tendenza preoccupante" e a impedire che la tecnologia "alimenti le tensioni sociali".

Nel suo intervento del 13 maggio, ha ribadito l'allarme: l'intelligenza artificiale "potrebbe portare a un enorme aumento della produttività se gestita bene, ma può anche portare a una maggiore disinformazione e, ovviamente, a una maggiore disuguaglianza nella nostra società".

Guerra cognitiva, Operazione Olympia: Parigi nel mirino di Baku[33] (2024)

Secondo le agenzie di intelligence francesi: Russia, Turchia e Cina vengono monitorate come potenziali istigatori di campagne di disinformazione, ma la Francia non si aspettava di incontrare problemi in questo settore con l'Azerbaigian.

Di conseguenza, sono rimasti completamente sorpresi quando Viginum, un servizio creato all'interno del Segretariato generale della difesa e della sicurezza nazionale (SGDSN) per proteggere il paese dalle interferenze digitali straniere, ha scoperto il coinvolgimento di Baku in una serie di operazioni di disinformazione e influenza effettuate contro la Francia negli ultimi mesi.

Queste operazioni sono state analizzate dal dipartimento tecnico e innovazione del servizio segreto estero francese DGSE per scoprire chi si nascondeva dietro gli account sui social

[33] AGCNews 30 giugno 2024

media coinvolti. Secondo fonti francesi, le indagini hanno rivelato una serie di istituzioni con stretti legami con il presidente dell'Azerbaigian. La Francia è infatti un obiettivo di Baku.

La prima spiacevole sorpresa è arrivata nel luglio 2023, quando è stata rivelata una campagna per diffamare i Giochi Olimpici del 2024 a Parigi, a cui Viginum ha dato il nome di "Olympia". Centinaia di messaggi sono stati inviati su X (ex Twitter) con l'hashtag #BoycottParis2024. Spesso arrivavano con fotografie della violenza urbana seguita alla morte della giovane Nahel Merzouk, uccisa da un agente di polizia il 27 giugno 2023 a Nanterre, un sobborgo di Parigi. La seconda fase della campagna di disinformazione di Baku ha preso la forma di denunciare il neocolonialismo francese in Nuova Caledonia sulla base delle dichiarazioni dei sostenitori dell'indipendenza di questo territorio francese d’oltremare. Ne ha parlato *le monde* già nel 2023 in un articolo.

Queste operazioni sono state effettuate sullo sfondo di un grave deterioramento delle relazioni tra Francia e Azerbaigian dopo che la Francia ha sostenuto l’Armenia nella disputa con l’Azerbaigian sul Nagorno-Karabakh. All'inizio di dicembre 2023, l'uomo d'affari francese Martin Ryan è stato arrestato e imprigionato a Baku. È stato accusato di spionaggio dopo essere entrato in contatto con due ufficiali della DGSE inviati in Azerbaigian sotto copertura diplomatica. Da allora è in custodia e il suo processo, che avrebbe dovuto svolgersi ad aprile, è stato rinviato di quattro mesi.

Due “diplomatici” dell’intelligence sono stati espulsi dall’Azerbaigian tra Natale e Capodanno, lasciando la stazione francese di Baku senza alti ufficiali. In risposta, Parigi ha dichiarato persona non grata due diplomatici azeri. Uno ha coordinato operazioni per intimidire gli oppositori del regime del presidente Ilham Aliyev che si erano rifugiati in Francia.

La terza fase delle operazioni prevedeva la "strumentalizzazione" delle rivolte avvenute in Nuova Caledonia a maggio, utilizzando accuse secondo cui la polizia aveva commesso crimini contro i sostenitori dell'indipendenza. Viginum ha osservato che gli account dei social media coinvolti erano gli stessi utilizzati nell’Operazione Olympia 10 mesi fa.

Nel frattempo, la DGSE ha conosciuto i contatti del Baku Initiative Group (BIG) e del suo direttore generale Abbas Abbasov. Quest'ultimo, che ha lavorato in precedenza per il fondo petrolifero statale Sofaz e poi per la holding Neqsol, di proprietà dell'imprenditore Nasib Hasanov, è considerato vicino ai servizi segreti azeri.

BIG ha sviluppato legami con movimenti indipendentisti tra cui il Kanaka e il Fronte socialista di liberazione nazionale (SFNLF). Sono stati creati nell’estate del 2023 dopo una conferenza guidata dal think tank azerbaigiano Centro per l’analisi delle relazioni

internazionali, guidato dall'ex ambasciatore dell'Azerbaigian in Canada e nella Repubblica ceca Farid Shafiyev.

In questa fase della crisi caledoniana, la disinformazione "internazionale" ha cominciato a farsi sentire nella campagna azera. Hanno cominciato a lanciare le stesse accuse i media turchi, poi quelli russi. Per cercare di rispondere a queste accuse e limitare la portata della manipolazione, la Francia ha scelto di condannare pubblicamente l'Azerbaigian.

Il colonnello francese Bruno Cunat, intervenendo al "Forum APRI 2024: costruire il domani", ha dichiarato: "La Francia ha l'obiettivo politico di partecipare ai processi della regione del Caucaso meridionale; La Francia vuole aumentare i costi per attaccare l'Armenia; La Francia non vuole gettare benzina sul fuoco, ma esprime rammarico e preoccupazione per le narrazioni aggressive dell'Azerbaigian riguardo ai nuovi accordi militari franco-armeni; Una settimana prima dell'inizio delle proteste in Nuova Caledonia, uno dei deputati della Nuova Caledonia ha visitato Baku. Per la Francia questo è un segnale e la Francia ritiene che l'Azerbaigian sia coinvolto in queste questioni. Le autorità francesi stanno lavorando in questa direzione".

CYBERWARFARE E GUERRA COGNITIVA DELLA SFERA JIHADISTA

Non dobbiamo commettere l'errore, per ignoranza o pressappochismo, che la rivoluzione IA e gli aspetti correlati tocchino solo la sfera dei "buoni", anzi.

Il mondo jihadista ha da subito colto le possibilità insite nella social sfera per fare proselitismo, la Osint Unit di AGC Communication se ne è occupata in diversi libri[34] e documentari internazionali[35] oltre che a dedicarle ampio spazio nell'edizione quotidiana e dedicandole una serie di oltre 80 articoli e approfondimenti sul legame tra comunicazione e operatività dello Stato Islamico[36]. L'opportunità fornita dalla semplice e miracolosa moltiplicazione degli strumenti di persuasione e proselitismo, vera Guerra Cognitiva, è stata colta appieno, fin dall'inizio da al Qaeda e ancora di più da Daesh. Oggi Daesh è arrivata a produrre i primi video con Avatar IA e sta utilizzando IA per diffondere il proprio messaggio in rete. Per Daesh è solo l'evoluzione del suo CyberJihad, in cui i munasirin, cioè i combattenti della Rete operano quotidianamente.

Il punto di partenza è dettato dalle parole dei padri fondatori di al Qaeda: Usamah bin Laden e Ayman al Zawahiri. In una lettera al Mullah Omar nel 2002, Usama bin Laden scrisse: "È ovvio che la guerra mediatica in questo secolo è uno dei metodi più forti; infatti, la sua percentuale può raggiungere il 90% della preparazione totale per le battaglie."[37] Sostenendo questo punto di vista, Ayman al-Zawahiri ha affermato nel 2005: "Più della metà di questa battaglia si sta svolgendo sul campo di battaglia dei media. Siamo impegnati in una battaglia mediatica in una corsa per i cuori e le menti della nostra Umma."[38] Il recentemente

---

[34] AA.VV *Lo Stato Islamico. Chi sono Da Dove Vengono Quanti sono Quali obiettivi*, AGC COMMUNICATION 2014:
A. Albanese, G. Giangiulio, E. Molle, L. Scigliano, E. Valdenassi *Daesh Matrix Cosa è cambiato? Stanno vincendo o perdendo? Che fine fanno i rifugiati?* AGC Communication, 2016

[35] *Stato Islamico - Nascita di un format. Nascita di un format*, Todos Contentos Y Yo Tambien - Magnolia, AGC Communication, 2015;
Stato Islamico. Morte di uno Stato Mai Nato? Ruvido Produzioni - Agc Communication, 2016

[36] https://www.agcnews.eu/?s=speciale+daesh+matrix

[37] Questo documento si trova nel database Harmony situato presso il Centro di lotta al terrorismo presso l'Accademia militare degli Stati Uniti, West Point. L'ID del documento è AFGP-2002-600321.

[38] "Lettera da al-Zawahiri ad al-Zarqawi", GlobalSecurity.org, 9 luglio 2005. Questo documento è stato rilasciato dall'Ufficio statunitense del Direttore dell'intelligence nazionale nell'ottobre 2005

scomparso pediatria egiziano usa gli stessi termini che abbiano visto usare nella definizione della Coin e poi della Guerra Cognitiva: Vincere i Cuori e le Menti.

Qui di seguito le pietre miliari della diffusione e manipolazione del target audience di riferimento usato negli anni scorsi per attrarre, convincere e arruolare nuovi combattenti da diverse parti del mondo. Un buon modo per iniziare a orientarsi nel complesso mondo della Guerra Cognitiva jihadista.

Cyberjihad all'orizzonte[39] (2012)

Assieme ai cambiamenti radicali avvenuti negli Stati investiti dalla Primavera araba, si sono aperti nuovi interessanti fronti della guerra cibernetica che da anni imperversa nel web.

Nel 2011, i conti di Bashar al Assad, il contestato presidente siriano, sono stati hackerati più volte così come la sede centrale della Central Bank degli Emirati Arabi Uniti, lasciando in chiaro e facile preda migliaia di numeri di carte di credito. In questa parte del mondo, inaspettatamente, le istituzioni finanziarie si trovano in prima linea. Simili "violenti" attacchi hanno convinto il mondo finanziario arabo, lontano dalle magie della rete, a investire maggiormente in sicurezza informatica. I rischi per la sicurezza cibernetica vanno di pari passo con l'allargarsi dei conflitti sociali e politici spesso fusi con l'animosità e la radicalità degli scontri tra arabi ed israeliani, ad esempio. Blocchi di siti, attacchi Dod, e simili manovre belliche on line coinvolgono migliaia di attori, proprio come una volta le guerre di posizione combattute nel mondo reale. I governi coinvolti si stano attrezzando. Negli Emirati è stata creata una squadra d'emergenza contro simili crimini, e Abu Dhabi si candida ad ospitare l'edizione regionale della conferenza dedicata all'argomento (la Black Hat conference).Simili eventi hanno lo scopo di diffondere la consapevolezza del rischio di questi attacchi e della vulnerabilità del sistema, che registra un incremento esponenziale nel numero degli hacker. Lo scorso gennaio, è stato lanciato, ad esempio, uno dei primi attacchi informatici con epicentro il Medio Oriente, attraverso botnet per scatenare un attacco Dod in grande stile verso server israeliani. La ricchezza delle economie di questa regione sono al centro dell'interesse di questa nuova guerra informatica, esattamente come altre regioni del mondo

[39] Agcnews27 Marzo 2012

con la differenza che qui la ricchezza è tangibile, vera e quasi indifesa. Gli hacker, politicizzati o meno, ne sono attratti in maniera incredibile.

Dalla piazza al cyberjihad[40] (2012)

Nel corso dell'ultima settimana di settembre Bank of America, JPMorgan Chase, Citigroup, U.S Bank, Wells Fargo e PNC, sono state bersaglio di un attacco informatico a causa del video anti-islamico *Innocence of Muslim*. Nonostante il disagio creato non si sia spinto oltre una parziale interruzione della connessione internet, capace di creare alcuni ritardi sul servizio di on-line banking, il fenomeno lascia intendere un'ulteriore reazione dell'estremismo islamico al caso "cinematografico" apertosi nell'ultimo mese. Un gruppo di hacker mediorientali, sotto il nome di "Izz ad-Din al-Qassam Cyber Fighters"[41], avrebbe infatti rivendicato il gesto tramite dei post, affermando che i colossi bancari americani siano l'obbiettivo della recente rappresaglia al video anti-islam.

Un'ulteriore reazione alla pellicola realizzata nel 2011, tuttavia distribuita solo lo scorso mese di settembre (2012, ndr), che ha innescato accese proteste di piazza in alcuni paesi a maggioranza musulmana; la quale sarebbe alla base anche degli episodi di violenza di Bengasi, culminati con l'attentato al consolato statunitense dove ha perso vita l'ambasciatore Christopher Stevens assieme ad altri tre funzionari americani.

Si tratta della stessa pellicola che ha visto il suo produttore dissimulare la propria l'identità di "Nakoula Basseley Nakoula", sotto lo pseudonimo di "Sam Bacile". Un egiziano di confessione cristiano copta, che sosterrebbe di aver raccolto per la realizzazione del film circa 5 milioni di dollari offerti da donatori anonimi, operando in California per tre mesi con una troupe di 60 attori e 45 tecnici. Numeri che, nonostante non sembrerebbero confermati dalla qualità del video, continuano a ingenerare instabilità a livello planetario.

In Europa, dove si avvertono avvisaglie di spostamento della reazione, i credenti di diverse fedi si sono uniti nella protesta contro il film antislamico, con manifestazioni persino in Norvegia, dove alla testa del corteo di dissenzienti era presente lo stesso sindaco di Oslo. Il tutto, mentre ad Atene si verificavano disordini durante una manifestazione di immigrati

[40] Agcnews 1 Ottobre 2012

[41] Attualmente parte della malassai Hamas

musulmani che mostravano il proprio risentimento verso il filmato ritenuto offensivo della dignità del Profeta Maometto, cercando di rompere il cordone della polizia per marciare verso l'ambasciata americana situata a circa due chilometri da piazza Omonia.

Non sono mancati momenti di tensione neanche in Turchia, dove la protesta verso *Innocence o Muslims* si è sommata al malcontento per le caricature raffiguranti il Profeta pubblicate dal settimanale satirico francese *Charlie Hebdo*, con evidenti effetti sull'ordine pubblico.

In questo contesto internazionale e conoscendo la conformazione sociale d'oltralpe, il ministro degli interni francese Manuel Valls ha maturato la decisione di proibire ogni tipo di manifestazione contro la pellicola, diffondendo la scelta tramite una dichiarazione ufficiale rilasciata subito dopo che una folla di persone di religione musulmana ha cercato di assaltare l'ambasciata statunitense a Parigi. Gesto che ha portato a fermare e poi interrogare circa 150 persone, per fare chiarezza sull'accaduto.

Anche nel vicino Belgio gli scontri con le forze dell'ordine nel corso di una manifestazione analoga – in questo caso non autorizzata dal ministero degli interni fiammingo – avvenuta nel quartiere Borgerhout di Anversa ha portato all'arresto di 230 partecipanti, la quasi totalità subito rilasciata. Sembrerebbe in ogni caso, stando le autorità belghe, che a provocare gli scontri sarebbe alle stata la stessa cellula salafita "Sharia per il Belgio", che aveva incitato a creare disordini al consolato statunitense di Amsterdam.

Controversi gli animi nella capitale tedesca, dove il pastore statunitense Terry Jones – noto per i suoi gesti d'intolleranza verso il mondo musulmano – nonostante l'invito ricevuto dal movimento tedesco di destra "Pro Deutchland", ha visto interdetto dal ministero degli interni il suo accesso sul suolo della Repubblica Federale, in quanto ritenuto potenzialmente in contrasto con l'ordine pubblico. Timori non privi di fondamento a seguito dell'incendio dell'ambasciata della Repubblica Federale a Karthum in Sudan assimilabile all'attacco contro l'ambasciata britannica con sede nella stessa città.

L'opposizione tedesca, nei rappresentanti della SPD e dei Verdi, si è tuttavia schierata contro la censura della pellicola *Innocence of Muslims*, sostenendo che il suo divieto costituirebbe una violazione delle libertà di parola e pensiero. Concettualmente, non si vorrebbe dunque anteposta una prudenza in politica estera a una priorità di politica interna, soprattutto perché costituirebbe una reazione capace di dare peso a un non meritevole di un processo mediatico. Nettamente in contrasto restano tuttavia dichiarazioni del ministro degli

interni tedesco Hans – Peter Friedrich, sostenuto dal ministro degli esteri Guido Westerwelle, che ritiene necessaria un'escamotage governativa per rendere penale la diffusione del video.

Quanto all'Italia, il fenomeno si è presentato in forma edulcorata con proteste avvenute a Roma e a Milano senza particolari conseguenze: i dimostranti hanno chiesto rispetto per l'Islam senza creare disagi per l'ordine pubblico. Il nostro ministro degli Esteri, a conferma delle note sensibilità sul tema, ha comunque sottolineato come restino obbiettivi sensibili le sedi diplomatiche statunitense e israeliana ospitate sul territorio italiano.

Cyberjihad: operazione Ababil[42] (2013)

Secondo le autorità statunitensi, l'Iran starebbe continuando gli attacchi informatici contro le istituzioni finanziarie made in Usa e, secondo fonti a stelle e strisce il governo degli Stati Uniti non sono riusciti a prendere adeguate misure per fermarli.

Attacchi informatici denial-of-service (Dod) sono in corso da diversi mesi e hanno come attori hacker di origine iraniana che inondano i siti web finanziari delle istituzioni statunitensi con massicci tentativi di log-in che ostacolano o bloccano i servizi di remote banking. L'amministrazione Obama è stata messa sotto accusa per non aver protetto le aziende americane dagli attacchi informatici sia da appartenenti alla pubblica amministrazione che da compagnie private.

Ad oggi incaricate della difesa del sistema informatico statunitense sono una serie di agenzie governative: i militari dello US Cyber Command, le agenzie di intelligence degli Stati Uniti, il Dipartimento per la Sicurezza Nazionale, e l'Fbi. È la Casa Bianca ha il compito di dirigere i contrattacchi informartici ma finora ha negato l'autorizzazione ad azioni aggressive, come ritorsione ad attacchi informatici. Secondo fonti interne all'amministrazione democratica, l'amministrazione Obama sarebbe riluttante ad intervenire a causa di "politiche concilianti" del presidente verso l'Iran. Il presidente Barack Obama non è riuscito a sostenere l'opposizione democratica in Iran nel 2009 e ha limitato la sua azione a solo quella diplomatica contro il programma nucleare iraniano. Nella cosiddetta "operazione Ababil" gli hacker hanno intensificato i loro attacchi agli inizi di gennaio 2013,

[42] Agcnews 7, Gennaio 2013

costringendo Pnc Bank ad avvertire la clientela su possibili interruzioni. Pnc Bank, in una dichiarazione del 3 gennaio, ha annunciato che un certo numero di banche americane, tra cui anche lei, registravano un «volume insolitamente elevato di traffico alle loro connessioni Internet (...) Questo volume di traffico è in linea con gli attacchi informatici ed è progettato per causare ritardi di accesso a clienti Internet legittimi», ha detto la banca. La banca ha annunciato che alcuni clienti non sono stati in grado di lavorare in remoto proprio a causa degli sforzi di protezione per attenuare gli effetti degli attacchi. I cyber-analisti della sicurezza made in Usa hanno detto che un gruppo iraniano chiamato al-Qassam Cyber Fighters avrebbe compiuto gli attentati. Sul forum hacker pastebin.com, il gruppo ha rivendicato il 25 dicembre 2012 che era in corso una "seconda fase" dell'attacco nelle settimane seguenti.

Il gruppo ha detto di aver preso di mira JPMorgan Chase & Co., Bank of America Corp, Citigroup Citibank, Wells Fargo & Company, US Bancorp, Pnc Financial Services Group, Bb & T Corporation, SunTrust Banks, e Regions Financial Corporation.

Stando a fonti ufficiali di Washington, il gruppo Izz ad-Din al-Qassam Cyber Fighters è sì un gruppo di hacker privati, ma le sue attività sembrano sponsorizzata dallo Stato. Gli hacker hanno mosso nei loro attacchi fino a 70 gigabyte di dati al secondo; gli attacchi Dod utilizzano dei computer collegati in rete dirottati a svolgere una massa di log-in nei siti web bancari.

Cyber Jihad warfare[43] (2013)

Dopo oltre un decennio di contrasto bellico e di polizia al jihad e al jihad media warfare dalla rete di al Qaeda, andando a ben guardare il fenomeno, ci si scontra con un vistoso paradosso: il movimento è sì ispirato da una filosofia del XIV secolo, ma è propagandata attraverso un uso sapiente della tecnologia dell'informazione del XXI secolo. Per raccontare la loro sacra missione volta a ridurre il potere occidentale (statunitense per lo più) nel mondo musulmano, per il reclutamento alla jihad, per l'e-learning della jihad, il fenomeno riconducibile ad al Qaeda ha fatto ampio uso del cyberspazio.

---

[43] Agcnews 2 maggio 13

Nonostante più di un decennio di vera caccia all'uomo sul piano reale, in quello virtuale il fenomeno qaedista gode di ampia libertà di manovra. Si tratta di un teatro altrettanto importante di quelli reali del Waziristan, dello Yemen o di altri impervi teatri.

Il dramma di Boston ha mostrato come il cyberspazio porti grandi benefici al movimento; i fratelli Tsarnaev, jihadisti on line, non sono stati certo i primi. Gli attentati di Londra nel 2005 (che uccisero 52 persone), il tentato attentato al Glasgow Airport nel 2007, quello sventato contro Fort Dix, nel 2007, il caso di Nidal Hasan a Fort Hood nel 2009 (che uccise 13 colleghi), e altri episodi hanno un dato in comune: tutti i "terroristi" hanno usato largamente gli strumenti on line della rete jihadista, tutti si erano fornita tramite materiale on line preparato da Anwar al-Awlaki, ucciso nel 2011, e di Abu Musab al-Suri.

Se l'influenza di al-Awlaki come propagandista sembra essere morta con lui, il concetto strategico di al-Suri sulla nascita di una "rete senza leader" jihadista, esposta nel suo Global Islamic Resistance Call (1600-pagine web) è diventato un best-seller qaedista.

Al-Suri era stato catturato dalle forze statunitensi, interrogato da personale dell'intelligence Usa, quindi consegnato ai siriani. Da qui la sua vicenda si perde nelle nebbie. Importante resta il fatto che al-Suri, e con lui il suo progetto. è seguito. Lo testimonia l'aumento di cellule terroristiche relativamente piccole che agiscono in luoghi inaspettati; si tratta spesso di jihadisti non particolarmente abili, ma motivati, dedicati, e sufficientemente esperti da causare danni e da catturare l'attenzione dei media mondiali.

Nonostante siano passati più di dieci anni dagli eventi del settembre 2001, le domande al centro dell'attenzione delle squadre antiterrorismo di tutto il mondo sono sempre le stesse: come può essere bloccata una jihad connessa in rete? Al Qaeda può essere guidata dal cyberspazio?

Gli Stati Uniti hanno svolto, fino ad ora, un ruolo di primo piano nel formulare una strategia politica che dividesse il fronte jihadista dall'Islam religioso. Nonostante il 95 per cento dei 1,3 miliardi di musulmani nel mondo già oggi rifiuta al Qaeda e simili estremismi, anche una scheggia di esso assomma a diversi milioni su cui fanno leva i jihadisti per riempire le loro fila, per avere personale motivato che non vacilli di fronte ai messaggi inviati per separare l'Islam religioso dai fondamentalisti.

Le motivazioni poste dai jihadisti agli atti di terrorismo, poi, come l'invasione dell'Iraq, gli abusi di Abu Ghraib, le uccisioni di innocenti fatte dai droni, e così via, si sono dimostrate molto efficaci.

Anche il blocco dei siti jihadisti si è rivelato inefficace e forse controproducente. In questo gioco del gatto col topo, è fin troppo facile far apparire su nuovi siti il materiale presente in quelli oscurati.

A questa facilità c'è da aggiungere che, ormai, gli stessi siti propongono più o meno le stesse cose nel settore tecnico non essendoci più, a detta di molti esperti di analisi del fenomeno, molto da imparare e che converrebbe monitorarli piuttosto che oscurarli. Restano, tuttavia, margini di analisi sui flussi finanziari che alimentano le possibilità operative e sui profili delle potenziali reclute.

Allora come dare nuova linfa alla ricerca? Utile potrebbe essere l'esempio britannico di Bletchley Park, il variegato staff che decifrò il codice Enigma durante la Seconda guerra mondiale.

Oggi, un nuovo "Bletchley Park" dovrebbe vincere la sfida di comprendere i "back hack" (processo di identificazione preventiva di un attacco sistemico e se possibile identificarne l'origine), geo-localizzarli e accedervi.

Se i primi cervelloni includevano militari, matematici, maestri di scacchi e anche maghi, tra gli altri, quelli del XXI secolo richiedono figure professionali diverse, da porre accanto agli analisti d'intelligence propriamente detti, come master hacker, software designer, maestri di scacchi e Go, analisti dell'informazione, sociologici, filosofi e musicisti (vedasi il caso della primavera araba) e così via.

Si tratta, in estrema sintesi di porre le basi per un nuovo approccio strategico per il contrasto alla Cyber Jihad e alle sue manifestazioni nel mondo reale, perché semplicemente, la strategia fin qui seguita non funziona più.

IS lancia il cyberjihad[44] (2015)

Postato ieri da you tuber giordano la nuova minaccia ai "crociati", gli Stati Uniti e ai sui alleati. Nel video messaggio, di controinformazione, la nuova casa di produzione Al Azm

[44] Agcnews 15 Gennaio, 2015

Media Center, nata nel 1426 Hejra (2015), dichiara che il Cybercaliphate è l'altra faccia del Califfato che sconfiggerà i "crociati".

Da un lato dunque gli attacchi militari, dall'altro gli attacchi ciberneticai a infrastrutture degli alleati. Nel video sono riprese immagini di servizi di Tv arabe che commentano l'attacco cibernetico ai danni del US Central Command, in cui i giornalisti affermano che IS ha tecnici informatici di alto livello. Alla fine si sente la voce di Al-Adnani, che ripete quanto già detto in altri video minacciando la coalizione. Viene rimandato in onda il discorso del "boia" trasmetto dopo l'esecuzione di Peter Kassig.

ISIS: cyberjihad africana[45] (2015)

AQIM, Boko Haram, Shebab somali utilizzano la cyberjihad. A quanto pare i jihadisti africani sono andati a scuola da ISIS ed ora mettono in pratica la loro tecnica: fare affidamento su Internet per la propaganda e il reclutamento.

Fino al 23 settembre 2014, nessuno al di fuori di una manciata di specialisti, aveva sentito parlare di Jund al-Khilafa. Il giorno successivo, il gruppo terroristico algerino è finito sulle prime pagine dei giornali dopo la trasmissione di un video in cui veniva mostrata la decapitazione di Hervé Gourdel. Intitolato "Messaggio di sangue per il governo francese". Il video mostrava l'ostaggio, il 55enne francese, in ginocchio con alle spalle quattro uomini armati di Kalashnikov. In 12 ore con sottotitoli in 48 lingue, il video, ha fatto il giro di 170 Paesi. A quanto pare tra i terroristi jihadisti, ricordiamo che Boko Haram ha fatto giuramento di fedeltà a ISIS lo scorso agosto, si è diffusa la conoscenza tecnologica con annessi e connessi. «I terroristi utilizzano spesso chip telefonici acquistati con identità false, acquistano anche smart phone e poi trasmettono tramite un'unica rete 3G», ha detto alla testata Jeune Afrique, Akram Kharief, algerino specialista reti jihadiste. «Possono anche farlo da un Internet café», ha aggiunto.

A questo dato va aggiunto il fatto che per i territori in cui sventola la bandiera ci sono gli internet point gratuiti. Dove arriva ISIS, vedi il Caso Libia con Derna, sono arrivati gli internet point. Nei video diffusi via web dei giovani combattenti distribuiscono da un furgone che fa da hub password e user per la connessione a Internet e invitano i giovani a mandare i loro filmati. Per quanto concerne il "format" invece, «vi sono dei video tutorial disponibili sul

[45] Agcnews 28 Gennaio 2015

Web: così raggiungere in breve tempo milioni di utenti via Internet è molto facile» chiosa Kharief.

«Nel 2010, ci fu una flotta di 40 milioni di computer che approdarono in Nigeria», ha dichiarato alla testata Jeune Afrique, Nick Ridley, autore di un libro sul terrorismo in Africa orientale e occidentale. Abubakar Shekau, il leader di Boko Haram ha utilizzato internet per promuovere la sua causa e sfidare direttamente il presidente Goodluck Jonathan. «Il Video in cui Boko Haram rivendicava il rapimento di 200 studentesse delle scuole superiori a Chibok era stato facile da realizzare (rapire le ragazze) e allo stesso tempo efficace da un punto di vista della comunicazione, ha commosso il mondo». Ha continuato Ridley.

Boko Haram è un po' più "discreto": si limita a reclutare forzatamente i giovani "nella vita reale" , soprattutto nel nord del Camerun. Come Al-Qaeda nel Maghreb Islamico (AQIM), mentre i combattenti dello Stato Islamico sono quelli che più hanno internazionalizzato la loro strategia, creando un vero e proprio ministero della propaganda, Al-Hayat Media Center. Il loro reclutamento è tutt'altro che casuale. Come nel settore della pubblicità i loro messaggio varia a seconda del pubblico. «Hanno affinato le loro tecniche, in modo che possano avere successo ad offrire un'offerta personalizzata», a dirlo è il rapporto del Centro francese per la prevenzione contro le aberrazioni settarie in materia di Islam. Tra le "capacità" di Al-Hayat adattare la propaganda al profilo di giovani da raggiungere: «può essere altruista (quando si parla di quelli che sognano di partecipare a missioni umanitarie), incentrato sulla onnipotenza (tramite l'immagine del "cavaliere eroico" e videogiochi, per il ragazzo più "duro") o la ricerca di un leader ("portatore d'acqua" per i valori più bassi)». Si legge ancora nel rapporto.

«In Francia, circa il 90% dei candidati sarà reclutato per la jihad attraverso i social network e forum. Questa percentuale supera il 50% in Algeria». A dirlo è Lotfi Ben Jeddou, tunisino ministro dell'Interno secondo cui Internet è il bacino di reclutamento principale dei circa 3.000 combattenti impegnati in Siria. «Il giovane a cui mirano è istruito. La maggioranza di quelli reclutati sta finendo gli studi universitari in ingegneria o economia e commercio e in particolare nel settore IT», ha dichiarato Abdellatif Hannachi, uno studioso tunisino reti jihadiste. AQIM Shebab e molto attivo su Twitter. Nel mese di luglio 2014, Tunisi ha annunciato di aver creato «una cellula di agenti per la lotta contro le minacce terroristiche sul Web». Le autorità hanno inoltre adottato misure per chiudere questi siti indesiderati. «Ma per una piattaforma distrutta, nuove nascono! È complicato per la Tunisia, data la debolezza

delle sue capacità tecniche e le risorse finanziarie», sconfiggere i jihadisti cibernetici ha detto Hannachi.

Tutti gli occhi sono ora puntati sui giganti di Internet, social network o host. Ma mentre tutti gli operatori hanno recentemente rafforzato la loro censura politica, i jihadisti hanno già trovato una soluzione. Pubblicando i loro video su piattaforme secondarie, quali Archive, VidMe o meno attenti su YouTube, che permettono ai loro fan di copiare "il video" e poi condividerlo nelle piattaforme più note come quelle statunitensi. La rimozione dell'intera catena rientra nel puzzle ed è sempre più difficile da ricostruire.

Gli Shebab somali per esempio durante l'attacco al Westgate Nairobi nel settembre 2013 nonostante la chiusura di un loro account riuscirono a pubblicare e rivendicare l'attacco da altri account twitter. A ogni chiusura di account, Shebab è resuscitato con un nuovo pseudonimo.

Come se non bastasse a questi jihadisti cibernetica vanno aggiunti gli hacker di professione che vedono nel continente africano un bacino di "clienti inenarrabili" capaci anche di destabilizzare i governi pur di fare soldi. Se Boko Haram o AQIM non hanno il tempo né le risorse tecniche e competenze per attaccare uno stato lo possono fare, dunque, dietro compenso gli hacker in cambio di compenso adeguato. Ne sa qualcosa il Marocco che mentre si prepara a lanciare "Digital Marocco 2020" deve fare i conti con violazioni alle caselle mail di politici. È successo a Salaheddine Mezouar, Ministro degli Affari Esteri: un hacker, pseudonimo di Chris Coleman, ha manipolato la sua posta elettronica per un po' di tempo. Alcuni paesi hanno già adottato misure di protezione, come la Costa d'Avorio, Nigeria, Kenya e Sud Africa.

Nel mese di settembre 2013 Microsoft ha avvertito che il Marocco è stato 3,5 volte più suscettibile di essere colpito da malware rispetto alla media globale. All'inizio del 2014, Kaspersky Lab ha rivelato che il regno aveva subito 384 attacchi di Careto virus, in sette anni. Alla testa delle sue vittime, il governo e le missioni diplomatiche. «L'infezione da Careto può essere catastrofica, ha assicurato una società di stampa di sicurezza informatica. Intercetta tutti i canali di comunicazione e raccoglie le informazioni più essenziali dal computer delle sue vittime».

Isis vince la sua Cyberwar[46] (2017)

Il trend della comunicazione è stato guidato dell'attacco subito da ISIS contro *A'maq*, agenzia di Stampa dello Stato Islamico. ISIS ha confessato che gli hacker hanno disabilitato le applicazioni per Firefox e Chrome. Ma, nel contempo, ISIS ha mandato on line i link di *A'maq* per poter leggere o scaricare i file di interesse in tutti i suoi gruppi facilmente raggiungibili da tutta l'utenza. ISIS, dunque, sapendo che sarebbe stata attaccata ha preparato, come sempre, una via di "salvezza". Ed ha funzionato, con buona pace degli hacker che a loro volta sono stati attaccati e resi "innocui".

È fallito, dunque, il tentativo di disabilitare "ISIS virtuale". Quello che l'Occidente non vuole comprendere è che dietro i "server" di ISIS ci sono gli uomini di ISIS che salvano tutto su diverse postazioni e hanno l'opportunità di poter utilizzare server locati in diverse parti del mondo, che ISIS non usa mai contemporaneamente. Paradossalmente si può asserire che oramai nemmeno ISIS sa dove sono locati i suoi file, visto che l'ordine è per tutti i munasserin "jihadisti virtuali" di salvare i file sui server personali non rintracciabili. Comunque ISIS ha scritto un comunicato ufficiale dove dice che il nemico, pur penetrando la rete, ha fallito perché ISIS usa codici criptati per le sue comunicazioni. E ha canali di riserva per ripristinare la rete comunicativa.

Un altro dato interessante non nuovo, ma significativo, è "il censimento" di chi fa azioni pubbliche contro ISIS. Per censimento si intende scheda anagrafica del giornalista, premier, uomo politico o d'arme, religioso. ISIS oggi ha postato una breve nota sulla giornalista uccisa in Siria che aveva pubblicato tempo fa un post di denuncia-derisione contro le fatwe di ISIS. Ritorna la voce di al Baghdadi, al Adnani e bin Laden, in cui si chiede ai combattenti di essere forti, resistere e combattere fino alla vittoria o alla morte (nella foto). E in tal senso, oggi sono state editate molte grafiche che rappresentano combattenti a prendere in mano la spada o il fucile per combattere.

Infine, continua la campagna di odio contro i cristiani e gli israeliani con un video che mostrerebbe come questi cerchino di rendere il messaggio del Corano impuro.

---

[46] Agcnews 20 Novembre 2017

ISIS apre la caccia all'uomo[47] (2017)

In questo periodo, gli account di ISIS hanno avuto due grandi obiettivi: spiegare ai jihadisti della rete jihadista on line che ISIS non è morta e dall'atra parte chiamare alle armi i mujahidin sparsi per il mondo "impuro" a compiere attentati.

Di fatto ISIS, dopo le ultime sconfitte in Iraq e Siria, caduta Rawa e Albu Kamal, deve assolutamente portare a casa un "trofeo" e quindi, da oggi, è aperta la caccia all'uomo da uccidere fuori dai confini ISIS.

Lo Stato Islamico c'è per rimanere e quindi farà di tutto per far parlare di sé. Non a caso, tra le pubblicazioni comparse, ci sono le operazioni ISIS compiute negli ultimi due anni e le grafiche dedicate a Dei Ez Zor, gli articoli che spiegano ai jihadisti di avere pazienza per arrivare alla vittoria. E, ancora, link a canali dedicati ai file audio e video dei leader ISIS, morti per lo Stato Islamico. Un grande "Amarcord" che ha come obiettivo quello di sollevare il morale delle truppe, oramai rifugiatesi in sparute località desertiche, tra Siria, Iraq e Afghanistan, pronti per ripartire per le prossime battaglie.

Non solo, ritroviamo on line molte grafiche contro i campionati del mondo di calcio (nella foto), quelle contro il Papa, ritornano quelle edite su *Rumiyah* che spiegano come attaccare e quali obiettivi. Oggi, poi, si è aggiunta una grafica contro un giornalista degli Emirati Arabi Uniti. Molti i post dedicati a *A'maq*, ovvero a distinguere il vero dal falso, i link originali di *A'maq* da quelli postati, per ingannare e ostacolare la comunicazione jihadista.

È stato editato, senza avere nessun clamore ufficiale, il primo numero della rivista *Anfal*, che porta lo stesso nome del genocidio iracheno di Saddam Hussein contro i curdi. Molto simile, per la grafica ad *An Naba*, Anfal posta articoli di cronaca e indicazioni sui materiali ISIS pubblicati. La domanda è: sostituirà An Naba? Oppure è una pubblicazione amatoriale?

Daesh punta a pubblicare su Instagram e Tiktok[48] (2023)

Il terrorismo di cui nessuno parla più molto non ha cessato di esistere. Ha cambiato interessi ha cambiato continente. Dal Medio Oriente dove continua comunque a compiere

[47] Agcnews 22 Novembre 2017

[48] Agcnews 9 Maggio 2023

attacchi in Siria e Iraq ora vede il cuore del suo business del terrore in Africa. E Continente che vai social che trovi.

Durante il mese del Ramadan mentre l'occidente tentava di attaccare i server di ISIS con attacchi Ddos ai siti di ISIS; Daesh ha messo in pausa i suoi server e i suoi siti e ha ha fatto un restyling editoriale.

Ritornano on line dopo un mese, le pubblicazioni e gli *Art Work* che oramai hanno preso il posto delle "campagne mediatiche ISIS" che sono assenti per la prima volta da quando è stato indetto il martirio per il periodo del Ramadan, ovvero un incremento degli attentati terroristici mentre i musulmani di tutto il resto del mondo praticano il digiuno.

Non vi è stata infatti per il Ramadan 2023 la proclamazione di una campagna in segno di vendetta per qualcosa, e di conseguenza non vi sono state grafiche che preparavano la campagna mediatica. Non ne sappiamo le motivazioni, di certo c'è un'importante ristrutturazione interna volta a migliorare il posizionamento di Daesh sulle nuove piattaforme social media.

Daesh dunque è ancora una volta in trasformazione. Il nuovo materiale è adatto per la pubblicazione su Instagram, *Art Work* verticali, e ancora a TikTok , brevi video con primi piani: fino ai podcast che sono espressi sotto forma di file audio della rivista ufficiale *al Naba* giunta al suo 389 numero. Sono audio che durano 8 o 40 minuti editi tutti da al *Battar Media Foundation*.

Daesh dunque ancora una volta dimostra di avere all'interno dell'organizzazione persone che continuano a studiale il marketing del terrore e a cercare nuovi strumenti per divulgare il loro Verbo. L'ultima campagna mediatica e *Art Work* invita ad uccidere gli israeliani e a confutare Hezbollah come gruppo jihadista e a connotarlo come popolo di Satana.

Per quanto riguarda gli scenari ricordiamo che nell'ultimo mese sono stati compiuti attacchi nelle Filippine, Afghanistan, Pakistan, Iraq, Siria, Somalia, Mozambico, Repubblica Democratica del Congo, Nigeria, Niger, Mali, Burkina Faso.

PROFILI DEGLI AUTORI

ANTONIO ALBANESE

Direttore Responsabile Direttore Unità OSINT

Competenze

- Giornalista professionista ed analista politico-militare
- Studi Internazionali e Politici
- Studi Militari e Diplomatici
- Comunicazione istituzionale ed aziendale
- Relazioni Esterne e Organizzazione Eventi
- Inglese livello C/2 e spagnolo livello B/2

Personal background

Laureato in Scienze politiche nel 1992 presso l'Università degli Studi di Roma, La Sapienza con tesi sull'organizzazione del partito di Francesco Crispi nella Capitale. È ufficiale riservista della Guardia di Finanza, in questa veste ha ricoperto numerosi incarichi di prestigio nella CIOR (Confederazione Interalleata degli Ufficiali della Riserva, struttura NATO che riunisce gli ufficiali riservisti dell'Alleanza Atlantica), e dall'ottobre 2012 al Febbraio 2013 è stato a capo della delegazione italiana. Diplomato PIO (Public Information Officer) presso lo SHAPE (Supreme Headquarters Allied Powers Europe) di Mons (Be), è stato Segretario Generale del MEDFOR (Mediterranean Forum for Reserve Officers) e dell'ARPa (Adriatic-Ionian Reserve Officers Partnership), due organizzazioni internazionali che riuniscono le associazioni degli ufficiali riservisti dei Paesi del Mediterraneo.

Nel 2012 frequenta il corso Psyops - Cimic organizzato da NATO-CIOR presso il Comando di guerra psicologica dell'Alleanza Atlantica di Bydgoszcz (Polonia).

Grazie a questi incarichi ha maturato una esperienza internazionale diplomatica creata dal confronto continuo con diverse realtà sociopolitiche europee e Atlantiche. Nel frattempo, dal gennaio 2011 è Presidente nazionale di URFI (Associazione Nazionale Ufficiali Riservisti Finanzieri d'Italia), e da ottobre 2011 è iscritto all'Albo Nazionale degli Analisti d'Intelligence (ANAI). È analista politico-militare per diverse organizzazioni e istituzioni italiane ed estere; accanto ad un'intensa attività pubblicistica professionale per diverse testate, nel 2008, è uscito *L'imbarazzo afgano* (Bietti Media), analisi della presenza italiana nello scenario afgano-pakistano, prefato dal Generale Fabio Mini.

Giornalista pubblicista dal 1997 e professionista dal 2001, nella sua carriera professionale ha maturato esperienze di direzione di testate locali radiofoniche e cartacee; oggi è anche direttore della testata radiofonica di Radio Antenna 1, dopo essere stato per oltre un decennio caporedattore del mensile *Area*. Nel 2012 fonda con la collega Graziella Giangiulio, l'agenzia giornalistica AGC COMMUNICATION srl, proprietaria del portale on-line www.agcnews.eu

Nel febbraio 2014 è stato relatore, unico italiano, all'Africa Security & Counter Terrorism 2014 svoltosi a Londra, con la relazione Risk assessment of terrorism coming from Africa to Europe. An Italian Perspective.

Nel Settembre 2014 ha partecipato come delegato al NIAS 2014 presso lo SHAPE NATO.

Nel 2018 è stato rappresentante italiano alle European Army Reserve Forces Conference svoltesi in Danimarca e nel 2020 è stato designato per lo stesso incarico ed evento per la Conferenza da svolgersi in Estonia, poi sospesa a causa della pandemia.

Nel luglio 2021 ha partecipato in qualità di Segretario Generale della Delegazione Italiana all'incontro con Gen. C.A. Claudio Graziano, Presidente del Comitato Militare dell'Unione Europea.

Nel febbraio 2022 è stato nominato responsabile del gruppo di lavoro bilaterale sulla sicurezza ITALIA - GERMANIA UNUCI - VdRBw (Verband der Reservisten der Deutschen Bundeswehr e. V.)

Nell'Ottobre 2022 ha partecipato in qualità di Segretario Generale della Delegazione Italiana all'Autumn Meeting della Gaminger Initiative tenutosi a Stans (CH) presso SWISS INT (Obersdorf) Centro Peacekeeping Internazionale delle Forze Armate della Confederazione Elvetica.

Nell'ottobre 2022, è stato il responsabile del Cerimoniale per il Primo Raduno Nazionale UNUCI, svoltosi in Roma presso l'Altare della Patria - Monumento al Milite Ignoto (29 Ottobre 2022).

Nell'ottobre 2023, ha partecipato in qualità di Segretario Generale della Delegazione Italiana all'Autumn Meeting della Gaminger Initiative tenutosi a SIBIU (RO) presso l'Accademia Militare dell'esercito rumeno e presso il Centro addestrativo delle forze speciali rumene, tenendo una serie di presentazioni su tematiche geopolitiche e di sicurezza.

È relatore su temi concernenti lotta la terrorismo di matrice fondamentalista islamica presso istituzioni accademiche e di sicurezza italiane e straniere (tra le altre Università La sapienza - Master Geopolitica e Sicurezza; Università Roma 3 - Cattedra Relazioni Internazionali, Facoltà Scienze Politiche; Direzione Investigativa Antimafia - DIA, Arma dei Carabinieri - Scuola Ufficiali; CIFIGE - Centro Interforze di Formazione Intelligence; Scuola di Polizia Economico-Finanziaria della Guardia di Finanza).

Coautore del libro *Lo Stato Islamico*, edito da AGC COMMUNICATION nel Novembre 2014.

Ideatore del del primo corso OSINT in e-learning (technical partner LINFA), on line nel Febbraio 2015.

Coautore del documentario *Stato Islamico. Nascita di un Format* – Prodotto da Todos Contentos Y yo Tambien e Magnolia – trasmesso da La 7 all'interno del programma PiazzaPulita l'8 Giugno 2015.

Gennaio 2016, coautore del secondo documentario sullo Stato Islamico, prodotto da Ruvido, dal titolo: *Stato Islamico. Morte di uno Stato mai nato?*

Novembre 2016, coautore del libro *Daesh Matrix* edito da AGC COMMUNICATION.

2019 - 2021: co-autore del libro: *Migranti. Storie di un fenomeno*, AGC Communication editore.

2019: co-autore di *Yemen, nonostante la Guerra,* documentario sullo Yemen basato sul raconto delle migrazioni, degli sfollati yemeniti e sulla tragedia di questo paese. Il documentario è stato trasmesso da RAI DOC (RAI 3) il 19 settembre 2019.

2020 -2021: Co-autore e commentatore di *RISIKO*, trasmissione su temi di Difesa e Sicurezza, in collaborazione con Radio Sparlamento

2021 - 2023: Curatore e commentatore di *Geopolitica on The Rocks*, spazio settimanale di analisi dei fatti internazionali all'interno della trasmissione *I fatti del week end* - *The Travelling Show* in onda su Radio Rock.

2021 - 2022: Co-autore e commentatore della rubrica geopolitica *Kender, Gli Occhi sul Mondo Che Cambia*, in onda su *Camp Italia*, Italian Community della piattaforma social *Second Life*.

2021: co-autore del libro: *Drones' & Co*, AGC Communication editore.

2021: co-autore del libro: *Diario Geopolitico: AFGHANISTAN*, AGC Communication editore.

2023 - Autore del saggio *Difesa Europea. È il momento di fare sul serio*, inserito nel volume collettaneo, *Percorsi di politiche pubbliche. Proposte e idee per ricordare parole a volte perdute* (Febbraio 2023).

2023 - 9 settembre conferito il Premio BOOKFORPEACE 2023 per il lavoro svolto in ambito geopolitico

2024 - Curatore e commentatore di *Caffè Geopolitico*, spazio settimanale di analisi dei fatti internazionali all'interno della trasmissione *Animal House* in onda su Radio Rock.

GRAZIELLA GIANGIULIO

Condirettore
Analista Business Intelligence

Competenze

- Giornalista professionista economico e finanziario
- Studi umanistici e in scienze della comunicazione
- Problem solving, creativo in ambito pubblicitario
- Gestione di uffici stampa, gestione eventi
- Coordinamento editoriale e/o di testate giornalistiche, web editor
- Relazioni Esterne, comunicazione aziendale
- Inglese e francese livello B/2

Personal background

Laureata in Filosofia nel 1999 all'Alma Mater Studiorum di Bologna con tesi in materia di teoria dei modelli matematici prosegue la sua formazione, filosofico-scientifica con due scuole estive di filosofia in: “Fondamenti della meccanica quantistica” e l’anno successivo, “Fondamenti delle teorie relativistiche”, presso il Centro Interuniversitario di Filosofia e Fondamenti della Fisica a Cesena, a cura della Società Italiana di Logica e Filosofia delle scienze (Silfs). Inizia la sua carriera in agenzie di comunicazione della Regione Emilia Romagna sin dal 1999 occupandosi di gestione eventi e uffici stampa per dedicarsi poi al giornalismo a partire dal 2001 presso la redazione di San Marino Fixing nella Repubblica di San Marino, nel 2004 diventa giornalista pubblicista iscritta all'Ordine dei Giornalisti dell'Emilia Romagna e nel 2005 è a Roma dove inizia la carriera di giornalista professionista e dove consegue l'abilitazione alla professione del 2008. Nel 2010 si laurea in Scienze della Comunicazione all'Università di Cassino. Nel frattempo ricopre il ruolo prima di Caposervizio all'economia del quotidiano Linea e poi nel 2011 diventa direttore responsabile del mensile l'Officina. Nel 2012 fonda con il socio Antonio Albanese l'agenzia giornalistica AGC COMMUNICATION srl, proprietaria del portale on-line www.agcnews.eu.

È relatrice su temi concernenti lotta la terrorismo di matrice fondamentalista islamica presso istituzioni accademiche e di sicurezza italiane e straniere (tra le altre Università La sapienza - Master Geopolitica e Sicurezza; Università Roma 3 - Cattedra Relazioni Internazionali, Facoltà Scienze Politiche; Direzione Investigativa Antimafia - DIA, Arma dei Carabinieri - Scuola Ufficiali; CIFIGE - Centro Interforze di Formazione Intelligence; Scuola di Polizia Economico-Finanziaria della Guardia di Finanza).

Coautrice del libro *Lo Stato Islamico*, edito da AGC COMMUNICATION nel Novembre 2014.

Ideatrice del del primo corso OSINT in e-learning (technical partner LINFA), on line nel Febbraio 2015.

Coautrice del documentario *Stato Islamico – Nascita di un Format* – Prodotto da Todos Contentos Y yo Tambien e Magnolia – trasmesso da La 7 all'interno del programma PiazzaPulita l'8 Giugno 2015.

Gennaio 2016, coautrice del documentario sullo Stato Islamico, prodotto da Ruvido, dal titolo: *Stato Islamico. Morte di uno Stato mai nato?*

Novembre 2016, coautrice del libro *Daesh Matrix*, edito da AGC COMMUNICATION.

Autrice di romanzi gialli e racconti noir, con cui ha vinto premi letterari tra il 2001 e il 2003.

2019 - 2021: co-autrice del libro: *Migranti. Storie di un fenomeno*, AGC Communication editore.

2019: co-autore di *Yemen, nonostante la Guerra,* documentario sullo Yemen basato sul raconto delle migrazioni, degli sfollati yemeniti e sulla tragedia di questo paese. Il documentario è stato trasmesso da RAI DOC (RAI 3) il 19 settembre 2019.

2020: Co-autore e commentatore di *RISIKO*, trasmissione su temi di Difesa e Sicurezza, in collaborazione con Radio Sparlamento www.sparlamento.it

2021: Co-autore dello spazio settimanale di analisi dei fatti internazionali all'interno della trasmissione *I fatti del week end* in onda su Radio Rock.

2021: Co-autore e commentatore della rubrica geopolitica *Kender, Gli Occhi sul Mondo Che Cambia*, trasmessa su Camp Italia, comunità italiana della piattaforma social Second Life.

2021: Co-autore del libro: *Drones' & Co*, AGC Communication editore.

2021: Co-autore del libro: *Diario Geopolitico: AFGHANISTAN*, AGC Communication editore.

2022: Ufficio stampa per Primo Raduno Nazionale UNUCI

2022: Corso Geopolitica nell'era 2.0: Intelligence e OSINT tenuto presso Istituti di Studio della Repubblica di San Marino.

2023: Autrice di *GeoTweets*, pillole di geoeconomia in onda su *beconomytv*

ANTONIO ALBANESE • GRAZIELLA GIANGIULIO

Confondere cuori e menti

Guerra Cognitiva sfide contemporanee e IA

ISBN 978-88-947984-1-8

€ 25,00

ACTA MUNDI

agd communication