CTRL + power: la (geo)politica dell'autoritarismo digitale

2024 Report

Un simposio organizzato da LSE IDEAS
e T.wai - Torino World Affairs Institute,
in cooperazione con il Dipartimento di Culture,
Politica e Società dell'Università di Torino

In memoria del Professor Cristopher Coker

Come spesso accade, il simposio è iniziato con un ringraziamento degli organizzatori alle istituzioni e ai soggetti che hanno reso possibile l'evento. Tuttavia, nel 2024, il simposio è stato dedicato al Professor Christopher Coker, il compianto co-direttore di LSE IDEAS, scomparso nel settembre 2023. Le prime parole dei co-organizzatori Stefano Ruzza e Chris Alden onorano la sua memoria:

Il Professor Coker ha svolto un ruolo fondamentale nel rendere possibile l'evento odierno. Ha trascorso gran parte della sua vita a esplorare l'intersezione tra tecnologia, umanità e società. Dobbiamo molto alla sua eredità intellettuale e alle conversazioni illuminanti intrattenute con lui sugli stessi temi che discutiamo in questo simposio.

Questo evento rappresenta solo l'ultima espressione di una più profonda collaborazione tra gli istituti di ricerca torinesi e LSE IDEAS, una partnership che il professor Coker ha forgiato e promosso attivamente dal 2013. Questo simposio incarna la sua rimarchevole eredità istituzionale.

Infine, cosa non meno importante, l'eredità personale del Professor Coker sopravvive nelle relazioni che ha promosso attraverso il suo approccio molto personale ad argomenti e persone. Nonostante il professor Coker non sia con noi di persona, la sua influenza permea tutte le nostre discussioni.

Per molti versi, l'evento di oggi è dedicato al nostro collega e caro amico Christopher.

Il 6-7 maggio 2024 si è tenuto il quarto simposio internazionale organizzato congiuntamente dal think tank LSE IDEAS della London School of Economics, il think tank torinese T.wai – Torino World Affairs Institute e il Dipartimento Culture, Politiche e Società dell'Università degli Studi di Torino.

Intitolato '*CTRL + Power: La (geo)politica dell'autoritarismo digitale*' il simposio ha visto alternarsi panel tematici e conversazioni tra professioniste/i, studiose/i affermate/i e ricercatrici/ricercatori all'inizio della propria carriera accademica.

6 maggio 2024

7 maggio 2024

Intervento di apertura

L'edizione 2024 del simposio congiunto parte dalla premessa che i governi sono sempre più consapevoli di come sia possibile sfruttare il dominio digitale sia per supportare che per minare la stabilità dei loro regimi, siano questi considerati democratici o autoritari. Eppure, come sottolinea **Stefano Ruzza** , questi ultimi:

> hanno dimostrato una forte capacità di adattare e utilizzare le tecnologie digitali ed emergenti per preservare ed espandere i loro tratti autoritari in vari modi, dal mettere a tacere l'opposizione interna e limitare le proteste attraverso brusche sospensioni di internet (*shutdown*), al manipolare l'opinione pubblica internazionale e a interferire nelle elezioni straniere attraverso le "*troll farm*", vere e proprie fabbriche di disinformazione.

Questi sono solo alcuni degli strumenti digitali e delle tattiche a disposizione dei regimi autoritari e ibridi (vale a dire parzialmente autoritari) che questo simposio cerca di analizzare.

Analogamente, il simposio si concentra anche sul ruolo dell'informazione che **Chris Alden** definisce 'la "valuta" nel nostro mondo digitale – una moneta sempre più messa in discussione in quella che alcuni chiamano un'epoca della "post-verità", in

cui i fatti empirici, un tempo chiari, sono ora confusi e contestati'. Come spiegato da Alden:

> questo cambiamento mette in discussione la nostra capacità di dare un senso al mondo, proprio come la disinformazione faceva durante la Guerra Fredda. Guardando agli anni Sessanta, la strategia sovietica di identificare le vulnerabilità degli Stati liberali e di sfruttarle al fine di distorcere la verità offre un parallelo storico all'ambiente digitale odierno, in cui le società aperte si trasformano in terreno fertile per la disinformazione e la manipolazione.

Applicare la nostra memoria storica all'ambiente digitale contemporaneo, sostiene Alden, ci spinge a 'porre grandi domande, non solo sulla politica, ma anche sulle sfide etiche del nostro tempo: che aspetto potrebbe avere un mondo "post-post-verità" e come potremmo navigarne la complessità?'.

Così, riassume Ruzza, 'il simposio si propone di esplorare il lato oscuro del mondo digitale, focalizzandosi sulle dinamiche politiche dell'autoritarismo digitale che emergono dall'interazione di influenze nazionali e internazionali'.

In questo scenario, i partecipanti al simposio sono invitati a riflettere sulle opzioni a disposizione per mitigare e contrastare l'impatto delle forme digitali di influenza e resilienza autoritaria. Infatti, come sottolinea anche **Nicolò Russo Perez**:

> molte sfide locali alle democrazie e ai processi democratici – come l'erosione della coesione sociale e l'aumento della percezione di insicurezza – sono radicate in questioni globali. Le nostre soluzioni devono quindi partire da una comprensione più ampia delle origini di fenomeni come quelli affrontati in questo simposio: il regno digitale, intrinsecamente globale, ha impatti locali. È una questione "glocale".

E come tale, conclude Russo Perez, richiede politiche pubbliche innovative informate da ricerche rigorose e dal tipo di discussioni e scambi consentiti da spazi come questo simposio anche grazie al supporto di istituzioni private quale la Fondazione Compagnia di San Paolo.

Discorso di apertura

by Anja Kaspersen

Il testo che segue è basato sul discorso tenuto da Anja Kaspersen all'apertura del simposio. Il discorso è stato successivamente rielaborato da T.wai – Torino World Affairs Institute.

L'impatto del compianto Professor Christopher Coker sui campi delle relazioni internazionali e degli studi militari è profondo. Oltre a essere stato il mio mentore, la sua influenza ha plasmato radicalmente il mio pensiero e il mio percorso professionale. Coker era un pensatore visionario e un astuto osservatore della storia e delle persone che si sforzavano di coesistere al suo interno. Sebbene il nome di Coker sia spesso associato al suo lavoro sulla guerra, la sua comprensione della tecnologia, della ricerca computazionale e dell'antropologia digitale è altrettanto profonda e significativa. La sua capacità di scavare nelle forze sottili e spesso inespresse che plasmano la società – catturata da concetti come *doxa*, articolato dal sociologo Pierre Bourdieu, e "silenzi sociali", come discusso dall'antropologa Gillian Tett – era centrale nel suo approccio intellettuale. Coker aveva capito che queste forze potenti e inespresse spesso trasmettono più del rumoroso chiacchiericcio sociale. La maestria di Coker nell'ascolto è una qualità umana che è diventata sempre più vitale nella chiassosa era digitale odierna. La sua capacità di dimostrare non solo intuizioni, ma una vera e propria lungimiranza attraverso le scienze naturali e le scienze sociali e umane, con una tale facilità da lasciarci sbalorditi, lo ha reso un pensatore dal sapere enciclopedico e unico. Sapeva fin troppo bene che ciò che accade nella società, in politica e sul campo di battaglia è inestricabilmente legato alla nostra umanità.

Il punto di vista di Coker sulla tecnologia, in particolare nel contesto della guerra, si allinea strettamente con le intuizioni di Ursula M. Franklin, scienziata e rinomata pensatrice dell'impatto sociale della tecnologia. Franklin osserva che la 'Tecnologia è un *sistema*. Va ben al di là dei suoi singoli componenti materiali. Comporta organizzazione, procedure, simboli, nuovi termini, equazioni e, soprattutto, una mentalità'. Sia Coker che Franklin hanno capito che la tecnologia non è solo un insieme di strumenti e dispositivi, ma un sistema complesso e profondamente radicato che modella il modo in cui viviamo, pensiamo, interagiamo e percepiamo il mondo – un precursore di ciò che oggi riconosciamo come sistemi socio-tecnici. Tuttavia, soprattutto nel contesto dei sistemi di intelligenza artificiale (IA), si potrebbe discutere se questi siano veramente sistemi tecno-sociali, in quanto il termine implica un equilibrio tra influenza tecnologica e strutture sociali, mentre la realtà spesso mostra una dominanza degli imperativi tecnologici su quelli sociali.

Coker credeva che il rapporto dell'umanità con la guerra, e per estensione le tecnologie che sviluppiamo e usiamo per combatterla, offrisse profonde intuizioni su ciò che significa essere umani. Già nel suo libro *Humane Warfare* (2001), Coker si opponeva all'illusione che la tecnologia possa rendere la guerra più umana. Nonostante i progressi tecnologici, avvertiva Coker, la brutalità della guerra persiste e può persino essere esacerbata da tecnologie cosiddette 'umane': 'L'idea che la tecnologia possa eliminare l'orrore della guerra è tanto pericolosa quanto ingenua. La guerra, nella sua essenza, è un conflitto umano, e nessuna sofisticazione tecnologica può addolcire questa realtà.' Queste intuizioni risuonano profondamente nelle discussioni odierne sull'uso dell'IA in guerra, dove alcune applicazioni dell'IA minacciano di spersonalizzare o iper-personalizzare, oscurando così i veri costi della guerra. Coker ha osservato che le guerre del futuro, spesso previste dalla promessa delle tecnologie digitali e dell'IA, comportano 'l'astrazione della bruttezza della guerra rendendola un fenomeno digitalizzato'. Tuttavia, non ha mai evitato di sottolineare che la guerra è tutt'altro che un gioco per computer e che la vita è un'impresa complessa, che non si presta facilmente al calcolo in alcun

modo o forma – né dovrebbe farlo. I suoi scritti rivelano una mente brillante e in espansione, e dimostrano quanto fosse lungimirante nella sua ricerca, maturando forse di conseguenza un'intensa avversione per l'arroganza e le false pretese.

In *Future War* (2015), Coker si chiedeva provocatoriamente se le macchine 'saranno gradualmente viste non come sostitute degli esseri umani, ma come estensioni della nostra stessa umanità'. Coker ha spesso parlato dell'importanza di quell'insieme di principi e valori che storicamente hanno definito la condotta dei soldati. Era preoccupato che l'IA e altre tecnologie avanzate potessero cambiare radicalmente questa 'etica del guerriero'. Tradizionalmente, i guerrieri sono stati guidati da principi di onore, coraggio e condotta etica, tutti profondamente interconnessi con l'esperienza umana del combattimento. Tuttavia, vista la crescente automazione e remotizzazione della guerra, vi è il rischio che tali valori vengano intaccati. La distanza fornita, ad esempio, dai droni e dai sistemi di IA non solo consente di prendere decisioni lontano dal campo di battaglia, ma permette anche la formazione di nuovi campi di battaglia, potenzialmente scollegando ed estraniando l'elemento umano dalla violenza e dalle conseguenze di tali decisioni.

Nel suo saggio 'Artificial Intelligence and the Future of War', Coker si interrogava:

> Se la guerra diventerà sempre più dipendente dalla tecnologia, che ne sarà dell'iniziativa individuale [(*agency*)]? La guerra ci sta sfuggendo di mano? Per quanto tempo continueremo a 'possederla'? L'*agency* è un affare complicato: è incorniciata dalle storie che raccontiamo a noi stessi e agli altri.

Riconoscendo che:

> L'IA non cambierà la guerra ancora per qualche tempo. Ciò che farà è amplificare ulteriormente il modo in cui la guerra sarà guidata da fattori tecnologici (vale a dire il nostro rapporto con le macchine, quando saremo sempre più assorbiti da loro e loro da noi – la simbiosi uomo/macchina, o quella che viene spesso chiamata 'condizione post-umana').

Questo punto è sottolineato anche dallo studioso di diritto internazionale Kobi Leins, che scrive: 'la scienza inizialmente sviluppata per il bene dell'umanità viene spesso cooptata nella guerra. Molti sviluppi scientifici intrapresi per scopi non correlati sono stati riappropriati per essere utilizzati in guerra'. Questa 'riappropriazione' è particolarmente evidente nel campo dell'IA. Leins evidenzia inoltre l'urgente necessità di 'collaborare, chiarire i parametri d'uso, prevenire il doppio uso [(*dual use*)] e identificare i tempi appropriati per la revisione legale' prima che queste tecnologie vengano integrate nelle funzioni fondamentali della governance pubblica. Questa osservazione si allinea al contesto più ampio dell'evoluzione dei sistemi militari, in cui le nuove tecnologie, come l'IA, vengono incorporate. La sfida sta nel fatto che l'impatto di una particolare tecnica scientifica o di un sistema tecnologico sugli affari militari non è scontato. Le applicazioni dell'IA sono cresciute in settori quali autonomia, robotica e supporto alle decisioni, ma i loro progressi sono generalmente più ampi che profondi e la loro integrazione in capacità militari trasformative è ancora agli albori. Questa carenza di profondità evidenzia le complessità e le incertezze legate all'adozione dell'IA nei sistemi militari, facendo eco alle opinioni cautelative di Coker e altri.

Si potrebbe anche ipotizzare che l''etica del guerriero' abbia una controparte tecnologica: una sorta di 'etica dello sviluppatore di sistemi'. Nel campo dell'apprendimento automatico e profondo (*machine and deep learning*), ad esempio, alcune delle riflessioni di Yoshua Bengio e Stuart Russell, fanno eco alle domande poste da Coker. Per quanto tempo potremo continuare a possedere sistemi e modelli di IA? L'IA ci sta sfuggendo di mano? E dove sono i responsabili delle decisioni, i leader e gli altri in tutto questo? Qual è il loro ethos – qual è l''ethos della leadership'? Per i leader e i responsabili delle decisioni, l'essere preoccupati ha un costo. Sarah Hooker, ricercatrice nel campo dell'apprendimento automatico, ha scritto con grande chiarezza che 'i ricercatori nel campo dell'apprendimento automatico non dedicano molto tempo a parlare di come l'hardware sceglie quali idee [e, aggiungerei, di chi] hanno successo e quali falliscono. Questo si deve principalmente al fatto che è difficile quantificare il costo dell'essere preoccupati'. Qual è il costo esatto dell'essere preoccupati? Forse dobbiamo misurare i costi della preoccupazione e metterli a confronto con l'attuale mantra del ritorno sugli investimenti (*return of investment*, ROI) ad ogni costo. Altrimenti, ci ritroviamo con un ritorno all'indifferenza (*return of indifference*).

Il punto è che ogni cultura, ogni tribù, ogni gruppo ha un ethos. Quali storie ci stiamo raccontando, esattamente, e a chi spetta raccontarle? Il linguaggio e le parole che si formano in questo processo sono importanti. Sono importanti per il nostro modo di governare e per la percezione della posta in gioco. Altrimenti, ci ritroviamo troppo spesso con visioni del mondo e proposizioni binarie che servono a poco o nulla se l'obiettivo è garantire che i poteri siano tenuti sotto controllo e gli impatti negativi siano tenuti a bada attraverso regolamenti e standard. Non esiste un'IA cattiva o buona; questi sono solo di inquadramenti (*framings*).

Questa nuova "contabilità" e il "dover fare i conti" con il genio tecnologico sollevano interrogativi su come e quanto l'IA stia cambiando l'ethos del guerriero in modi che Coker avrebbe trovato profondamente preoccupanti. Se il ruolo del guerriero diventasse più di gestione delle macchine e meno di impegno diretto, diminuirebbe il senso di responsabilità e di riflessione etica che tradizionalmente è stato centrale nel concetto di 'guerriero'? Coker temeva che la crescente dipendenza dalla tecnologia potesse portare a una forma di distanziamento morale, in cui gli orrori della guerra sono oscurati dalle stesse tecnologie progettate per rendere la guerra più efficiente. Nelle parole di Coker: 'Rendendo la guerra più umana per noi stessi, la rendiamo meno umana per tutti gli altri? Alla fine, la questione è etica.' In altre parole, secondo Coker, l'etica è 'accuratamente formata [...] non dalla sola filosofia astratta, ma dall'azione pratica'. Purtroppo, man mano che la guerra diventa più tecnologica, 'allontana l'opinione pubblica e il guerriero dalle sue conseguenze'. Questo distanziamento morale – che crea una separazione dalla vittima ma un crescente avvicinamento alla macchina – suggerisce che una nuova forma di etica potrebbe emergere dall'interazione uomo-macchina. In combinazione con la codardia politica nell'affrontare le implicazioni etiche di tali tecnologie, ciò minaccia di erodere i valori fondamentali che hanno guidato storicamente la condotta umana nei conflitti.

Tutto ciò solleva questioni etiche fondamentali: le nuove tecnologie belliche stanno rendendo la guerra più umana o, paradossalmente, più brutale? Con l'integrazione dell'IA nel campo di battaglia, stiamo rafforzando i vincoli etici o stiamo

consentendo un tipo di violenza che è ancora più lontana dall'empatia umana e dalla riflessione morale? Storicamente, le tecnologie hanno spesso intensificato la disumanità della guerra eliminando i quadri etici che guidano la condotta umana nei conflitti. Oggi, l'incessante ricerca del vantaggio e della competenza tecnologica ha superato le cornici e i paradigmi tradizionali di governance e supervisione, lasciando molto in mano alla tecnologia.

Le intuizioni di Coker sulle forze silenziose in gioco nella società diventano particolarmente pertinenti se consideriamo l'ascesa dell'IA e delle tecnologie digitali nella società. Esattamente come Coker ascoltava ciò che rimaneva non detto nelle interazioni umane, dobbiamo esaminare attentamente le intenzioni di coloro che investono, sviluppano, distribuiscono e supervisionano queste tecnologie, focalizzandoci non solo su ciò che scelgono di amplificare, ma anche su ciò che potrebbero sopprimere o trascurare.

Nell'era digitale, ciò che viene lasciato inespresso spesso porta con sé le storie più incisive. Mentre l'IA e le tecnologie digitali promettono di trasformare le nostre vite, dobbiamo chiederci in modo critico: a quale costo, chi decide e con quale approccio?

Le preoccupazioni per l'erosione dei quadri etici, infatti, non si limitano alla guerra. Si estendono alle implicazioni sociali più ampie dell'IA e di altre tecnologie emergenti. Man mano che i sistemi di IA vengono integrati sempre più nella nostra vita quotidiana dobbiamo sforzarci di capire se queste tecnologie stiano rendendo la nostra società più umana o, paradossalmente, più brutale; se stiamo rafforzando i vincoli etici o stiamo abilitando un tipo di comportamento lontano dall'empatia umana e dalla riflessione morale.

La questione dell'impatto dell'IA sulla società è ulteriormente complicata dall'approccio riduzionista spesso adottato nello sviluppo e nella diffusione di queste tecnologie. Riducendo i complessi comportamenti umani, i pensieri e le dinamiche sociali a meri punti di dati e problemi computazionali, rischiamo di semplificare eccessivamente l'essenza di ciò che significa essere umani. Questa visione riduzionista non tiene conto della natura ricca, sfumata, a volte dolorosa e spesso imprevedibile della vita umana, che non può essere facilmente catturata da algoritmi o modelli di dati. Tende a favorire e promuovere una narrazione della tecnologia come panacea per tutti i problemi della società.

L'IA impiega modelli matematici e probabilistici di apprendimento automatico per generare risultati che *imitano* il coinvolgimento umano. Tuttavia, questi sistemi mancano della sensibilità contestuale e della logica simbolica insita nel pensiero umano. Al centro di molti sistemi di IA, soprattutto quelli che si basano sul *deep learning*, ci sono reti complesse progettate per elaborare grandi quantità di dati, spesso chiamate reti neurali. Tali reti possono generare nuove istanze di dati, quali immagini, testi o audio, che hanno una straordinaria somiglianza con i dati su cui sono state addestrate. I modelli di IA generativa, pur essendo in grado di produrre contenuti che rispecchiano i loro input di formazione, rimangono confinati a questi parametri predefiniti. Producono output basati su modelli trovati nei dati di addestramento, ma mancano della capacità di comprensione. Questa limitazione è particolarmente evidente nella loro tendenza a produrre le cosiddette fabbricazioni

(allucinazioni), vale a dire produzioni che, pur essendo plausibili in superficie, risultano errate o insensate a un'analisi più attenta.

Gary Marcus, scienziato cognitivo e ricercatore di IA, osserva che 'Siamo stati sedotti dal successo del *deep learning* e abbiamo pensato che fosse l'intera storia, ma è solo un pezzo del puzzle'. Inoltre, trattare l'IA come un'entità monolitica che può essere regolamentata e governata in modo uniforme non tiene conto delle sfide, diverse e sfumate, poste dai vari sistemi di IA. Aggiungiamo che queste sfide hanno un impatto profondo sul modo in cui ci impegniamo e affrontiamo i danni potenziali e intrinseci. Will Douglas Heaven, un giornalista tecnologico, ha recentemente sottolineato che 'L'IA è arrivata a voler dire tutto per tutti, dividendo il campo in fandom. Può sembrare che i diversi schieramenti si parlino addosso, non sempre in buona fede'.

Plaudo alla diversità delle opinioni e credo che la migliore intelligenza collettiva derivi dalla capacità di navigare tra le differenze e di mettere appassionatamente in discussione l'idea che nulla sia inevitabile. Come per la maggior parte delle cose nella vita, nella politica, nell'esercizio della democrazia, in guerra e in pace, si tratta di uno sforzo molto umano: cercare definizioni, prendere decisioni e confrontarsi necessariamente con i loro risultati, impatti e compromessi. Nella vita, l'unica certezza è che le cose si evolvono e i paradigmi cambiano. Ma senza consapevolezza, senza consenso, senza una conversazione pubblica, tutto questo non è semplicemente sostenibile. E per quanto riguarda l'IA – in qualsiasi modo la si definisca o in qualsiasi modo la si pensi su ciò che è e su ciò che vogliamo che sia – una cosa è certa: ci sono e ci saranno dei compromessi da fare, per progettazione e per default.

Le definizioni e le prospettive effettive su cosa sia l'IA – cosa rappresenti e costituisca – sono tanto varie e complesse quanto il numero di ricercatori nel campo. Ed è giusto che sia così. È la parte relativa all'etica che mi preoccupa, poiché un'interpretazione variegata e complessa dell'etica rischia di diventare uno strumento di evasione piuttosto che uno strumento di impegno. Avere definizioni è importante per la regolamentazione, ma ai fini della curiosità scientifica è bene permettere a molti punti di vista di emergere e incrociarsi.

Lo sforzo di replicare un'intelligenza simile a quella umana attraverso metodi computazionali si concentra sulla capacità dei sistemi di intelligenza artificiale di elaborare dati, riconoscere modelli ed eseguire compiti che tradizionalmente richiedono l'intelligenza umana. Questa visione vede l'IA come uno strumento sofisticato per migliorare e automatizzare le attività in vari settori. Altri, invece, hanno una visione più ampia, definendo l'IA come una tecnica e un approccio per organizzare le grandi quantità di dati generati ogni millisecondo. Questa prospettiva enfatizza l'IA come strumento di potere, utilizzato non solo per automatizzare i processi, ma anche per influenzare, controllare e plasmare le società. Una simile concezione dell'IA come meccanismo di potere si allinea con l'idea che l'IA possa essere vista come 'potere attraverso altri mezzi' e 'gli esseri umani come ingranaggi della macchina', facendo eco alle idee di pensatori strategici quali Clausewitz e Wiener, che Coker spesso parafrasasava in modo quasi umoristico. Andrew Bard Schmookler coglie perfettamente questo sentimento: 'Nelle mani dei potenti, l'IA è diventata un nuovo mezzo per manipolare, sorvegliare e controllare le società,

plasmando non solo le nostre azioni ma anche la nostra stessa percezione della realtà'. Altri ancora valutano in modo critico gli attuali limiti di comprensione dell'IA, chiedendosi se potrà mai replicare veramente gli aspetti più profondi e sfumati della cognizione umana, come il giudizio morale, la consapevolezza del contesto e il ragionamento simbolico.

Queste diverse prospettive riflettono la sfida significativa di fornire una definizione chiara e universalmente accettata di IA. Per alcuni, l'IA è uno strumento potente capace di far progredire la tecnologia e risolvere problemi complessi, mentre altri la considerano fondamentalmente limitata e potenzialmente pericolosa nella sua forma attuale.

È innegabile che l'efficacia e l'impatto dell'IA dipendano fortemente dal contesto, dai dati su cui viene addestrata, dalle persone che creano e addestrano questi modelli, dal livello di risorse computazionali disponibili e dagli approcci scientifici ed etici scelti. Come sottolinea Francesca Rossi, ricercatrice di IA, 'L'IA non è solo algoritmi e dati; si tratta di capire come questi sistemi interagiranno con il mondo e con la società'. Avere questo tipo di comprensione è fondamentale, in quanto aiuta anche a riconoscere che l'approccio che si sceglie di adottare e incorporare nel proprio Paese, organizzazione o azienda è importante – e spesso trascurato.

La sfida del nostro tempo consiste nel riconoscere i limiti dell'IA, nel comprenderne le diverse applicazioni e implicazioni e nell'evitare la tentazione di trattarla come una soluzione universale. Nelle parole di Coker, 'il pensiero algoritmico non è necessariamente il modo migliore per affrontare la realtà, e non tutti i problemi sono computabili, anche quelli di cui pensiamo di conoscere la risposta'. Come Coker, anche Gary Marcus sostiene che 'La vera intelligenza non è solo il riconoscimento dei modelli, ma implica il ragionamento, la comprensione di cause ed effetti e la capacità di adattarsi a situazioni nuove e impreviste'.

Il mio obiettivo non è quello di fornire risposte definitive, ma di lasciarvi con domande significative e materiale per ulteriori riflessioni.

Una dimensione importante da considerare è la nozione di errore quando ci si confronta con sistemi che superano di gran lunga la nostra capacità di elaborare le informazioni. Alcuni sostengono che incorporando una maggiore quantità di IA e distribuendola continuamente, potremmo ridurne gli errori e aumentarne la precisione. Tuttavia, è più corretto dire che l'IA produce diversi tipi di errori – errori a cui le nostre società non sono ancora equipaggiate per rispondere, poiché sono semplicemente al di là della comprensione umana e delle nostre capacità di pianificazione. Questo aspetto è particolarmente importante in ambito militare. Questa sfida è amplificata dall'avvento dei sistemi di IA generativa e dei modelli linguistici di grandi dimensioni, la cui complessità ostacola ulteriormente la nostra capacità di prevedere e mitigare i potenziali problemi. Come osserva Paul Scharre, 'L'IA può essere straordinariamente precisa, ma la precisione senza contesto è pericolosa. Un minor numero di errori in un settore può portare a guasti catastrofici in un altro'.

Questi errori, insieme alle metodologie che ne sono alla base, modellano non solo il modo in cui vediamo il mondo, ma anche il mondo che in ultima analisi creiamo,

influenzando quali e quanti sono i nostri obiettivi prioritari. Missy Cummings, robotista ed esperta di sistemi autonomi, mette in guardia dai pericoli di un'eccessiva dipendenza dall'IA, affermando che 'Il rischio maggiore dell'IA è che incoraggi un'eccessiva fiducia nelle sue capacità. Dobbiamo ricordare che questi sistemi sono tutt'altro che infallibili e richiedono una supervisione umana per garantire che non portino a problemi imprevisti'. Sarah Hooker approfondisce questo aspetto parlando della 'lotteria dell'hardware', in cui molti algoritmi hanno successo non perché costituiscono l'approccio giusto, ma perché sono adatti all'hardware disponibile. Questo fenomeno mette in luce una questione cruciale: l'interazione tra i sistemi di IA e gli ambienti fisici e computazionali in cui operano può portare a conseguenze indesiderate, in particolare quando questi sistemi vengono impiegati senza una piena comprensione dei loro limiti. Inoltre, la preoccupante tendenza dei sistemi di IA a 'fabbricare' sottolinea i rischi di affidarsi eccessivamente a questi modelli. Senza un nuovo approccio architettonico che adotti un principio di sicurezza che superi i paradigmi attuali, i rischi associati all'IA superano di gran lunga le sue promesse.

Sia Cummings che Pascale Fung, pur provenendo da background scientifici diversi – Cummings in robotica e sistemi autonomi e Fung in linguistica computazionale e IA – hanno espresso notevoli preoccupazioni sulle implicazioni etiche e sui rischi associati alle tecnologie di IA. Pascale Fung ha evidenziato i pericoli di un impiego dell'IA senza una sufficiente supervisione, in particolare il potenziale dei sistemi di IA di amplificare la disinformazione e altri danni alla società. Missy Cummings, nel frattempo, ha affrontato in modo specifico la fragilità dei sistemi di IA, osservando che questi sistemi possono funzionare bene in condizioni specifiche, ma sono inclini a guasti catastrofici quando tali condizioni cambiano inaspettatamente. Questa fragilità rende i sistemi di IA particolarmente vulnerabili in ambienti dinamici, sottolineando la necessità di una supervisione umana, che deve essere supportata da solidi processi di verifica e da investimenti in competenze umane per gestire e mitigare efficacemente tali rischi.

Joanna Bryson, come Franklin prima di lei, ha affermato che 'l'IA non è un artefatto; è uno strumento che riflette i valori e le decisioni di coloro che lo creano e lo utilizzano'. Questa idea si allinea strettamente alla ricerca di Coker sull'impatto della tecnologia sulla guerra e sull'umanità. Spesso Coker ha infatti affermato che la tecnologia, compresa l'IA, è un'estensione delle nostre ambizioni. La tecnologia non cambia semplicemente il mondo che ci circonda, ma cambia noi stessi ampliando le nostre capacità, alterando le nostre percezioni e rimodellando le nostre interazioni sociali. Lo sviluppo e la diffusione dell'IA non sono atti neutrali, ma sono profondamente intrecciati con i nostri quadri politici, etici, morali e (sempre più) economici. Inoltre, questi sistemi non sono privi di costi ambientali significativi, dato che si basano su grandi volumi di dati e su processi ad alta intensità energetica.

Un libro prezioso che Coker ha condiviso con me è *Blood Rites (Riti di sangue)* (1997) di Barbara Ehrenreich, che esplora la militarizzazione della società e della condizione umana, offrendo intuizioni profonde che risuonano con la ricerca di Coker. Ehrenreich esamina gli aspetti primordiali e rituali della guerra, fornendo indicazioni su come questi comportamenti e credenze radicati continuino a plasmare i conflitti moderni e la direzione dell'innovazione militare. Queste credenze e rituali culturali contribuiscono a determinare non solo la condotta della guerra, ma

anche ciò in cui le società ritengono valga la pena investire, dagli armamenti avanzati alle tecnologie emergenti. Coker ammirava la capacità di Ehrenreich di fondere storia, antropologia e critica sociale per rivelare le forze sottostanti al comportamento umano, in particolare nel contesto della guerra. Spesso rifletteva sulla sua osservazione che 'gli uomini uccidono per un'idea, purché non debbano pagarne il prezzo', collegandola al crescente distacco facilitato dai progressi tecnologici nella guerra.

Questa preoccupazione è ulteriormente amplificata dalle intuizioni di Josef Weizenbaum, scienziato informatico e creatore del primo programma informatico di elaborazione linguistica, ELIZA. Weizenbaum ci ha messo in guardia dall'affidamento 'simile a un dio' ai sistemi computazionali e dai rischi di una disconnessione dai valori umano-centrici, affermando che 'Vi sono alcuni compiti che non dovrebbero essere svolti dai computer, indipendentemente dal fatto che i computer possano o meno svolgerli'. Questa prospettiva sottolinea il pericolo di supporre che la tecnologia possa sostituire il giudizio umano e il ragionamento etico in aree in cui queste qualità sono essenziali.

Anche Wendell Wallach, uno dei principali studiosi di tecnologia ed etica, coautore di *Moral Machines* (2009) e autore di *A Dangerous Master* (2015), sottolinea la necessità di un nuovo quadro etico e persino di un nuovo paradigma adatto alle sfide poste dall'IA e da altre tecnologie avanzate. Egli sostiene che le preoccupazioni etiche non dovrebbero essere un ripensamento, ma piuttosto un principio guida nello sviluppo e nella diffusione della tecnologia. Questo approccio è fondamentale per garantire che la tecnologia sia al servizio dell'umanità e non la comprometta. Secondo il suo parere, occorre riconoscere tutti i compromessi e gestirli con attenzione per navigare efficacemente nella complessità dei progressi tecnologici. Questa sorta di 'etica del compromesso' si allinea con l'idea di Coker secondo cui l'etica si forma attraverso l'azione pratica. L'etica del compromesso, secondo Wallach, 'comporta l'esame di ogni possibile corso d'azione e la ponderazione dei benefici e dei rischi prima di decidere quale azione intraprendere'.

Le implicazioni dell'influenza dell'IA sulla società vanno ben oltre le preoccupazioni tecniche. Langdon Winner, teorico e filosofo della politica, sostiene che gli 'gli artefatti hanno una politica', il che significa che le tecnologie non sono strumenti neutri, ma portano con sé le strutture di potere e le intenzioni di coloro che le creano e le utilizzano. Questa intuizione si allinea strettamente alle osservazioni di Coker sulle implicazioni etiche e sociali dei progressi tecnologici, in particolare in ambito bellico. L'ipotesi che la tecnologia possa rimanere neutrale nel suo sviluppo e nella sua applicazione ignora i contesti sociali e politici più ampi in cui queste tecnologie vengono impiegate.

L'esplorazione di Hannah Arendt sui pericoli della menzogna in politica è particolarmente rilevante in questo contesto. Sono profondamente grata a Coker per avermi fatto conoscere le opere di Arendt, che hanno plasmato significativamente il mio orientamento intellettuale, quasi quanto le intuizioni di Coker stesso. Nel suo eccezionale saggio *On Lying and Politics* (1971), Arendt sostiene che quando le menzogne sostituiscono costantemente la verità fattuale, ciò porta non solo all'inganno, ma anche all'erosione della capacità di una società di distinguere tra verità e falsità, una capacità che è fondamentale per qualsiasi società

funzionante. Nell'era digitale odierna, l'IA potrebbe esacerbare questo problema consentendo la creazione di strumenti che non solo diffondono la disinformazione, ma manipolano anche la realtà stessa, rendendo le società sempre più vulnerabili alla manipolazione da parte di mentalità autoritarie. L'indifferenza verso la distinzione tra verità e falsità in questo panorama è particolarmente preoccupante e contribuisce a una cultura in cui la verità diventa sempre più malleabile. Arendt afferma:

> Il risultato non è che le menzogne saranno accettate come verità e la verità diffamata come menzogna, ma che si sta distruggendo il senso con cui ci orientiamo nel mondo reale – e la categoria della verità contro la falsità è uno dei mezzi per raggiungere questo scopo.

Anche il concetto di 'banalità del male' di Arendt è estremamente rilevante nel contesto dell'IA. L'autrice sostiene che alcuni dei più grandi mali della storia sono stati perpetrati da individui comuni che hanno semplicemente eseguito gli ordini e si sono conformati alle norme della società senza interrogarsi sul profondo impatto delle loro azioni. Come ha osservato notoriamente la Arendt, il male può essere commesso da chi, pur non intendendo nuocere, non riflette sulle proprie azioni, limitandosi a svolgere i propri compiti all'interno di un sistema. Nell'era digitale, i sistemi di IA potrebbero mascherare azioni dannose su vasta scala, allontanando i responsabili dalle conseguenze etiche delle loro decisioni attraverso strati di astrazione tecnologica. Si tratta di preoccupazioni centrali per le apprensioni di Coker sul modo in cui le tecnologie e le tecniche sono incorporate in strutture sociali prive di un chiaro 'ethos di leadership'. Ciò solleva preoccupazioni urgenti sul modo in cui tali sistemi sono resi capaci di automatizzare non solo la banalità del male, ma anche la radicalizzazione (di qualsiasi opinione), rendendo cruciale l'impegno in un rigoroso controllo etico e pubblico.

La responsabilità diventa fondamentale. Anche ai politici viene chiesto sempre più spesso di prendere decisioni critiche su cosa e quanto investire nelle tecnologie di IA che vengono costruite e integrate nella società. In futuro, potrebbero sostenere di non aver compreso appieno le tecniche e i metodi tecnologici in questione e quindi di non essere stati in grado di prevederne le conseguenze. L'abdicazione della responsabilità, sia essa intenzionale o dovuta a una mancanza di comprensione, richiama il pericolo avvertito da Arendt: il rischio di consentire azioni dannose attraverso un'accettazione acritica e l'incapacità di esaminare le implicazioni etiche più profonde di tali decisioni.

La preoccupazione di Coker per l'erosione della verità è ulteriormente amplificata nel contesto dell'IA, dove l'automazione del processo decisionale rischia di normalizzare comportamenti e scelte che altrimenti potrebbero essere messi in discussione, portando a una graduale erosione dell'integrità della società, della dignità umana, dell'uguaglianza e, in ultima analisi, al silenzio. Tuttavia, Coker credeva anche fermamente nel ruolo delle nostre istituzioni accademiche contemporanee nell'aprire uno spazio per la 'post-verità' attraverso l'accettazione del relativismo. Egli vedeva il valore di poter stare con più verità allo stesso tempo, non vedendole come in conflitto, ma piuttosto come un'opportunità per capire qualcosa di più profondo. Questo riflette il suo interesse per Nietzsche, anch'egli alle prese con le complessità della verità, della prospettiva e della molteplicità dei significati della vita.

Attento osservatore dello studio di Nietzsche, Coker ha spesso riflettuto sulle intuizioni del filosofo su come gli strumenti di cui disponiamo plasmino i nostri pensieri e, per estensione, la nostra società. Chiunque abbia trascorso del tempo con Coker si è imbattuto in alcune citazioni di Nietzsche. Una che ha condiviso con me è stata '*Sie haben Recht: Unser Schreibzeug arbeitet mit an unseren Gedanken*', che si traduce in 'Hai ragione: i nostri strumenti di scrittura lavorano per dare forma ai nostri pensieri'. Questa idea cattura l'essenza del profondo impatto che gli strumenti e le tecnologie che creiamo hanno sulla nostra cognizione, sulle nostre decisioni e, in ultima analisi, sulle nostre società. La percezione di Nietzsche si collega fortemente alle intuizioni di Langdon Winner, secondo cui 'gli artefatti hanno una politica', e alla ricerca di Coker che esamina le tecnologie che sviluppiamo, non solo per la loro utilità immediata, ma anche per le loro implicazioni più ampie e a lungo termine sulla nostra coscienza collettiva e sul tessuto sociale.

Riflettendo su questi temi, dato l'obiettivo di questa conferenza, appare chiaro che un progresso tecnologico incontrollato potrebbe portare a danni significativi per la società e ad abusi autoritari, sia intenzionali che accidentali. Ad esempio, lo sviluppo e la diffusione di sistemi di sorveglianza guidati dall'IA negli spazi pubblici, giustificati con il pretesto della sicurezza pubblica, possono facilmente passare dalla protezione dei cittadini al loro controllo e monitoraggio in modi che soffocano la libertà e l'autonomia e, in definitiva, causano danni. Ciò è particolarmente preoccupante se si considera che molti sistemi e modelli di IA vengono sviluppati da attori privati senza un adeguato controllo e sono incorporati senza sufficienti garanzie o verifiche della loro integrità.

Come avrebbe potuto chiedere Coker, è importante se il danno è intenzionale o accidentale? In entrambi i casi, si apre la strada all'utilizzo di queste tecnologie in modi che non rispettano i principi fondamentali dei diritti umani, della non-oppressione, dell'etica dello spazio pubblico e della trasparenza pubblica, anche negli Stati democratici in cui tali tecnologie sono sempre più adottate. Oltre a questa preoccupazione, vorrei ribadire una domanda critica: chi decide, e a quale scopo? In un mondo guidato dall'IA, la distinzione tra risultati intenzionali e accidentali diventa ancora più pressante, poiché il processo decisionale diventa sempre più opaco. Il rischio è che le decisioni prese da sistemi di IA altrettanto opachi, guidati da algoritmi invisibili e da vaste serie di dati, possano portare a risultati che non sono né trasparenti né responsabili, erodendo i quadri morali ed etici che dovrebbero guidare le nostre società. È per questo che l'argomentazione di Arendt rimane così rilevante oggi: ci sfida a rimanere vigili, mettendo in discussione non solo la tecnologia in sé, ma anche le intenzioni, i processi e gli impatti che crea nelle mani di entità potenti, o '*juggernaut*', come li chiama Wendell Wallach.

Per illustrare e dimostrare la necessità di responsabilizzare le aziende tecnologiche, si consideri il progresso eterogeneo del settore tecnologico globale nella realizzazione di 'impegni volontari' per la sicurezza dell'IA, che rivela notevoli carenze. Ciò è particolarmente preoccupante se si considera quanto abbiamo appreso sulle vaste implicazioni di procedure errate per la verifica della sicurezza del software. I limiti dell'autoregolamentazione come strumento di governance dovrebbero preoccupare i decisori politici di tutto il mondo. Negli ultimi anni sono emerse alcune buone pratiche, ma non sono neanche lontanamente al livello

necessario, tanto in termini di governance quanto di protezione dei diritti in generale. A complicare ulteriormente le cose, secondo la mia esperienza, c'è il problema enorme di cui tutti sono consapevoli, ma che nessuno vuole affrontare che riguarda il fatto che le piattaforme e le aziende tecnologiche, e i servizi che forniscono, funzionino come servizi di pubblica utilità, pur non essendo tali. Spesso si sente dire che si tratta di 'imprese private globali' e quindi non soggette a tali requisiti. Ma il fatto che una cosa venga ripetuta spesso non significa che sia vera. Abbiamo già regolamentato altre infrastrutture critiche essenziali per la sicurezza pubblica, la dignità umana e la sicurezza internazionale, quindi perché non queste aziende?

Esistono molte opinioni valide e, proprio come l'IA non è un'entità unica e rappresenta cose diverse per persone diverse, c'è una notevole incertezza sul fatto che questa sia una linea d'azione giusta e fattibile. A ciò si aggiunge la percezione che se non lo facciamo noi, lo farà qualcun altro e nessuno vuole 'perdere' o 'rimanere indietro'. La domanda diventa quindi se le decisioni prese oggi ostacoleranno o promuoveranno l'innovazione, piuttosto che chiedersi se le decisioni sconsiderate di oggi creeranno nuove minacce e meno sicurezza. La sfida più grande, a mio avviso, è che i principali attori del settore tecnologico non sono una cosa sola, e con investimenti significativi nell'IA la complessità aumenta. Storicamente, i tentativi di regolamentazione sono spesso falliti quando c'è incertezza sul ruolo di queste aziende, incertezza che spesso viene intenzionalmente creata o mantenuta proprio per evitare la regolamentazione. Meredith Whittaker ha ripetutamente evidenziato il pericolo di 'cattura normativa' (*regulatory capture*) in mezzo a tutto il clamore, alla governance assente e alla mancanza di un 'ethos di leadership'.

Dobbiamo quindi porci le domande giuste, a volte scomode, e tracciare paralleli storici con la situazione attuale. Sebbene si facciano spesso paragoni con industrie come quella del tabacco o del petrolio, queste analogie non sono sufficienti a causa della natura multiforme delle aziende tecnologiche. Un esempio storico particolarmente rilevante è quello della United Fruit Company, una società che un tempo esercitava una notevole influenza sui sistemi politici ed economici dell'America Latina. Questo caso illustra come il potere delle imprese possa avere un impatto di vasta portata sul benessere pubblico. Allo stesso modo, le moderne aziende tecnologiche possiedono la capacità di plasmare i flussi di informazione globali e l'opinione pubblica, il che evidenzia l'importanza di sviluppare quadri etici internazionali e promuovere la cooperazione transnazionale per affrontare queste sfide nell'era digitale.

Inoltre, alla luce di ciò che oggi sappiamo sulla fragilità di questi sistemi, sugli incessanti requisiti di calcolo ad alta intensità energetica, sulla mancanza di trasparenza significativa e su linee di responsabilità poco chiare, i progressi compiuti non sono così solidi come sarebbe necessario. Le operazioni di sicurezza e protezione, compresi gli sforzi delle 'squadre rosse' (*red team*), che possono essere migliorati in termini di qualità negli ultimi anni, sono ancora spesso opache e gestite al di fuori della sfera pubblica. Non saranno sufficienti alcune 'soluzioni tecniche ordinate al disordinato problema socio-tecnico che è l'IA'. Né un'attenzione eccessiva ai soli rischi ipotetici. Le azioni parlano più delle parole. Non c'è nulla di inevitabile in queste tecnologie se abbiamo il coraggio collettivo di affrontare i punti

di tensione, di governare il loro sviluppo e il loro impatto e di indirizzarne l'uso benefico. Parafrasando Dag Hammarskjöld: la strada è lastricata di (inevitabili) compromessi. La velocità e la scala con cui incorporiamo l'IA nella governance pubblica, nei sistemi critici e nella vita immaginaria e reale dei nostri figli, rendendo sempre meno netta la differenza tra di essi, sono significative. Nel processo, potremmo essere costretti a fare i conti con chi siamo veramente.

Sarei in difetto se non cogliessi l'opportunità di onorare le molte persone che, nel corso di diversi anni, hanno unito la loro intelligenza collettiva per sviluppare modi migliori per affrontare i requisiti relativi ai test di sicurezza, all'etica, alle misure di sicurezza, alla verifica e alle considerazioni sull'età. Esistono standard internazionali, che rappresentano un primo passo verso una maggiore trasparenza e fiducia; ciò che manca, però, è il tessuto connettivo. Le intuizioni, gli sforzi, le risorse e i talenti collettivi all'interno e all'esterno del settore sono formidabili. In effetti, alcune delle persone più coscienziose che si occupano di questioni etiche sono impiegate in queste aziende. Questa osservazione suggerisce che molti dei problemi che vediamo sono più una questione di leadership assente e di scelte etiche che di problemi puramente tecnologici. Ciò sottolinea la necessità di andare oltre gli impegni volontari e l'autoregolamentazione.

Coker ha spesso riflettuto sui paradossi della guerra moderna, osservando come i progressi tecnologici abbiano trasformato radicalmente non solo il modo in cui ci impegniamo nei conflitti, ma anche il modo in cui interagiamo tra di noi come Paesi, istituzioni e individui. Un altro studioso che ha influenzato il suo lavoro è stato Daniel Dennett, uno scienziato cognitivo con profonde intuizioni filosofiche. Dennett ha espresso un'idea su cui Coker ha più volte manifestato preoccupazione:

> Siamo davvero a rischio di una pandemia di persone false che potrebbe distruggere la fiducia umana e la civiltà. La situazione è davvero pessima. A tutti coloro con cui ho parlato di questo argomento dico: 'Se riuscite a dimostrare che mi sbaglio, vi sarò molto grato.' Ma al momento non vedo alcuna falla nella mia argomentazione, e questo mi spaventa. Il problema più urgente non è che ci toglieranno il lavoro, né che cambieranno la guerra, ma che distruggeranno la fiducia umana. Ci porteranno in un mondo in cui non sarà possibile distinguere la verità dalla falsità. Non sapremo di chi fidarci. La fiducia è una delle caratteristiche più importanti della civiltà, e ora rischiamo di distruggere i legami di fiducia che hanno reso possibile la civiltà stessa.

Queste stesse idee hanno permeato la ricerca di Coker, che ci ha instancabilmente ricordato che, per quanto sofisticate possano diventare le nostre macchine, la vera pace e la dignità umana possono essere raggiunte solo attraverso lo sforzo e la comprensione umana.

Il lavoro di Coker ci sfida a esaminare continuamente il ruolo della tecnologia nelle nostre vite, in particolare il modo in cui essa rimodella la nostra comprensione di ciò che significa essere umani, influenza le nostre esperienze vissute e altera il modo in cui incarniamo e interpretiamo tali esperienze. Come suggerisce Emily Bender, linguista ed etica dell'IA, l'IA non è solo una sfida tecnica ma anche sociale, con profonde implicazioni per il potere e la disuguaglianza. Dobbiamo chiederci come sviluppare e utilizzare le tecnologie in modo da promuovere la verità, la giustizia e il

bene comune, anziché favorire la divisione, la disuguaglianza e l'oppressione. Le sfide etiche poste dall'IA non sono solo questioni tecniche, ma anche profondamente filosofiche che ci impongono di riconsiderare le basi stesse delle nostre strutture sociali. Solo attraverso un approccio rigoroso e interdisciplinare – che includa le voci di storici, etici, antropologi, matematici e tecnologi – possiamo sperare di navigare responsabilmente nel complesso terreno dell'IA e delle altre tecnologie emergenti.

Sherry Turkle aggiunge un'altra importante dimensione a questa discussione, esaminando come le tecnologie digitali possano connetterci virtualmente e allo stesso tempo isolarci emotivamente. L'autrice mette in guardia da un mondo in cui siamo 'soli insieme', con la tecnologia che riduce le ricche interazioni umane a semplici scambi. Questa preoccupazione riflette la sfida sociale più ampia di mantenere legami umani significativi in un mondo sempre più digitale, dove la tecnologia può sia colmare che ampliare i divari sociali. La solitudine nell'era digitale può diventare un problema importante per la sicurezza nazionale, soprattutto perché può essere usata come arma in modi clandestini. Sfruttando l'isolamento sociale, gli attori malintenzionati potrebbero alimentare la sfiducia, manipolare l'opinione pubblica o addirittura destabilizzare le società dall'interno, rendendo la solitudine non solo un problema personale ma un potenziale strumento di influenza.

In conclusione, nel momento in cui ci impegniamo con queste tecnologie, è fondamentale rimanere consapevoli dei compromessi etici – o, come li descrive Wallach, delle nostre azioni scelte – e sforzarci di garantire che il nostro uso della tecnologia migliori, piuttosto che sminuire, la nostra esperienza umana collettiva. È sufficiente fare quanto incoraggiava la Arendt: fermarsi e pensare. Coker mi ha insegnato che le dinamiche dell'IA non sono dissimili da altre trasformazioni della società: comportano il potenziale di grandi benefici ma anche il rischio di conseguenze impreviste. Queste tecnologie sono spesso sviluppate in previsione di capacità piuttosto che in risposta a problemi chiari, il che può portare a decisioni strategiche che possono creare nuove sfide, esacerbare quelle esistenti o spostare le strutture di potere in modi difficili da annullare.

Questa situazione mi ricorda una conversazione avuta con una persona che ha vissuto la 'spirale delle perdite' dei Lloyd's di Londra negli anni Ottanta. In quel caso, la ripetuta riassicurazione degli stessi rischi ha amplificato le perdite in tutto il sistema, portando a una crisi finanziaria. Allo stesso modo, le tecnologie IA, se non gestite con attenzione, potrebbero innescare una 'spirale di conseguenze', in cui i sistemi interconnessi amplificano i rischi e gli errori, creando un ciclo di sfide crescenti. Questo esempio storico serve da monito, ricordandoci che senza un'attenta supervisione e considerazione etica, il perseguimento del progresso tecnologico può portare a conseguenze impreviste e potenzialmente irreversibili.

Coker ha spesso riflettuto sui paradossi della guerra moderna, osservando come i progressi tecnologici offuschino i confini tra guerra e pace. Ricordo spesso una frase che condivise con me, che poi ho capito essere probabilmente derivata da una più lunga citazione di Dickens: 'È nei luoghi più oscuri che bisogna cercare la luce, perché è lì che l'umanità si rivela più spesso.' Questo è stato il modo in cui Coker ha guidato me – e forse tutti noi – a trovare speranza e saggezza di fronte alla complessità e a rimanere vigili, riflessivi e umani mentre affrontiamo le profonde sfide del nostro tempo.

PANEL 1

Bad news: comprendere e contrastare la disinformazione

Una delle tendenze più preoccupanti che accompagnano la 'rivoluzione digitale' è stata la diffusione della disinformazione online e della manipolazione sociale attraverso i mezzi digitali. Tuttavia, le radici di questi fenomeni sono più profonde di quanto normalmente si comprenda, come ha spiegato il primo relatore del simposio, **Michelangelo Conoscenti**.

Con l'ascesa dei social media, le campagne di disinformazione sono sempre più facili e meno costose da realizzare rispetto ai decenni passati. 'Le società occidentali, in particolare l'Europa, sono bersaglio di operazioni di disinformazione, condotte da personale militare ben addestrato e', come sottolinea Conoscenti, 'essere consapevoli del fatto che attori chiave come la Russia e la Cina utilizzano tecniche militari è fondamentale per contrastare le loro azioni e promuovere la resilienza delle nostre società'. Dobbiamo capire meglio come nascono e si diffondono le campagne di disinformazione, quali sono i loro effetti e come impedire che avvelenino il nostro ecosistema informativo e le nostre società. Per questo, Conoscenti si domanda: 'Perché la dis/misinformazione russa e cinese (o, per usare un recente acronimo dell'Unione Europea (UE): FIMI, *Foreign Information Manipulation and Interference*) riscuote così tanto successo? Inoltre, come mai il populismo, osservato come stile comunicativo, presenta, in tutto il mondo, strategie comunicative sorprendentemente simili a questi due regimi autoritari?"

Il *Global Risk Report* 2024 del World Economic Forum (19a edizione) nomina la disinformazione e la 'misinformazione' (*misinformation*) rispettivamente 83 e 74 volte, identificandole come i rischi più immediati nei prossimi due anni. Si tratta di un problema urgente: 'Gli *oppositori*, che ora riconosco come tali, stanno attivamente cercando di inquinare il dibattito pubblico europeo utilizzando informazioni militari e operazioni psicologiche. Occorre capire che l'opinione pubblica europea è l'obiettivo delle operazioni militari', afferma Conoscenti, aggiungendo che 'L'obiettivo, tuttavia, non è mai quello di spingere le elezioni a favore di un candidato preferito. Piuttosto, il risultato reale è quello di intaccare lentamente la fiducia dei cittadini nelle istituzioni politiche, nella prosperità economica e nella coesione sociale'. Si tratta quindi di una strategia più ampia e profonda.

Anche se la tecnologia può essere cambiata, la disinformazione fa parte da tempo della dottrina delle operazioni militari informatiche russe e cinesi. Storicamente, il giornale del Partito Comunista Russo, *Pravda* ('La verità'), offre un ottimo esempio delle pratiche di disinformazione russe di lunga data. Oggi, sottolinea Conoscenti, 'Le dottrine di Dugin e Gerasimov continuano questa eredità, con il secondo che sottolinea l'idea di verità relativa e il primo che mira a distrarre le società occidentali sfruttando le debolezze dei regimi democratici. Il tutto in un quadro sullo stato di "verità fallita e democrazie fallite" delle nostre istituzioni'. È importante notare che 'mentre la NATO considera le sue operazioni informative e psicologiche come attività di *guerra*, gli sforzi di disinformazione di Russia e Cina sono continui. Per loro è sempre tempo di guerra'.

A sostegno della sua argomentazione, Conoscenti condivide con il pubblico una registrazione radiofonica in onde corte dell'aprile 2024 in cui due persone stanno conversando in inglese. All'inizio i due parlano del più e del meno, della grandezza passata delle città di mare sulla Manica. Gradualmente, la conversazione si sposta

su argomenti più delicati, in particolare sulla Brexit, suggerendo che le cose nel Regno Unito non vanno più bene come una volta. La conversazione accenna poi, in modo disinvolto, al fatto che a Shanghai le persone sono molto gentili e amichevoli, che se si va spesso al ristorante tutti ti salutano e che la gente è desiderosa di sapere di più sull'Europa. Conoscenti chiede 'Chi è il mittente di questo messaggio?' Alcune persone del pubblico, madrelingua inglese, rispondono 'La BBC, probabilmente il World Service'. Conoscenti rivela poi che 'Si tratta di un'emissione a onde corte di China Radio International diretta in Europa', e spiega:

> Le due persone parlano con accento britannico e utilizzano elementi familiari per inquadrare i loro messaggi – parlano la 'lingua del quartiere' – mettendo in atto una forma di propaganda piuttosto elementare e antiquata, ma lo stesso approccio è ormai utilizzato a tutti i livelli: social media, onde corte e altro ancora.

Come spiega Conoscenti, possiamo individuare, in questo tipo di trasmissione, tre fasi principali: 1) l'introduzione dell'argomento all'interno di una cornice familiare, che corrisponde al coinvolgimento del pubblico, 2) la graduale riformulazione dell'argomento, che si sposta verso una prospettiva cinese sulla questione, e 3) la fase di influenza, in cui viene chiarito l'obiettivo delle due fasi precedenti: La Cina ha una soluzione migliore al problema.

Oggi, mentre il BBC World Service sta chiudendo le frequenze, China Radio International (CRI) utilizza 552 frequenze per trasmettere programmi in 61 lingue. Infatti, secondo quanto scrive la stessa CRI sul suo sito web, ha 'il maggior numero di servizi linguistici tra tutte le organizzazioni mediatiche globali'. L'emittente si rivolge principalmente all'Africa, all'Europa, al Sud America e naturalmente all'Asia. Eppure, come ammette, il suo servizio di inglese è:

> una delle divisioni più importanti di CRI. Offriamo al mondo uno dei modi più efficienti e convenienti per conoscere la Cina. Ci concentriamo sulle notizie e produciamo una serie di programmi di approfondimento.

La nuova unità di supporto informativo cinese, la Information Support Force, precedentemente legata alla Strategic Support Force, è ora sotto il controllo della Commissione militare centrale (Central Military Commission). Questo cambiamento conferisce a Xi Jinping un controllo ancora più diretto sull'apparato militare e indica il prossimo passo negli sforzi di disinformazione cinesi. 'Il risultato', afferma Conoscenti, 'è che la Cina sta sviluppando un manuale di disinformazione in stile Cremlino: utilizza massicce campagne di interferenza multipiattaforma su Facebook, YouTube, TikTok e persino Pinterest' e questo fa parte di una strategia più ampia e articolata. Si pensi a ciò che Xi Jinping ha detto alla 30ª sessione di studio collettiva del Political Bureau nel 2023: La Cina deve 'costruire un sistema di comunicazione strategica', migliorare 'l'influenza della comunicazione internazionale' e mostrare il 'potere persuasivo del discorso cinese' e la sua 'capacità di guidare l'opinione pubblica internazionale'. Inoltre, la Cina deve 'accelerare la costruzione del suo sistema discorsivo e narrativo' e 'rafforzare la propaganda e l'interpretazione del Partito Comunista Cinese'. Ciò comporta 'una ricerca approfondita da varie prospettive, tra cui politica, economia, cultura, società e civiltà ecologica, incentrata sullo spirito, i valori e la forza della Cina'.

Per quanto riguarda la Russia, nel maggio 2023 il presidente Putin ha approvato un documento in cui si afferma che 'È necessario continuare ad adeguare gli approcci alla costruzione di relazioni con gli Stati ostili' ed 'È importante stabilire un meccanismo per identificare i punti vulnerabili nelle loro politiche estere e interne per sviluppare misure pratiche per indebolire gli avversari della Russia'. Il documento sottolinea che 'la deterrenza globale nei confronti dei Paesi ostili', che devono riguardare 'le sfere politico-militari, economico-commerciali, informative, psicologiche, valoriali e di altro tipo', nonché 'i nuovi grandi temi delle attività di politica estera', come 'la lotta al neocolonialismo', la promozione dei 'valori spirituali e morali tradizionali' e il sostegno agli 'Stati e alle associazioni interstatali inclini a costruire un'interazione con la Russia'.

Come già accennato e sottolineato da Conoscenti, 'dovremmo essere consapevoli che gli sforzi di disinformazione non sono limitati a una singola tecnologia o piattaforma digitale. Cina e Russia stanno adottando un approccio globale a 360°'. La nostra attenzione, quindi, deve essere rivolta ai processi e ai metodi, piuttosto che a strumenti o tecnologie specifiche. E questo è l'argomento principale di Conoscenti: 'gli strumenti e le tecnologie sono solo il dito che indica la luna; sono il processo e la metodologia che contano'. Ad esempio, nel 2018 John Kelly e Camille François hanno scoperto che:

> Invece di cercare di far entrare i loro messaggi nel mainstream, questi avversari prendono di mira comunità polarizzate e 'incorporano' al loro interno account falsi. I falsi personaggi interagiscono con persone reali in quelle comunità per creare credibilità. Una volta consolidata la loro influenza, possono introdurre nuovi punti di vista e amplificare le narrazioni divisive e infiammatorie che già circolano. È l'equivalente digitale del trasferirsi in una comunità isolata e affiatata, utilizzare le sue stranezze linguistiche e assecondare le sue ossessioni, candidarsi a sindaco e poi usare questa posizione per influenzare la politica nazionale. [aggiunta di enfasi]

Quindi, chiarisce Conoscenti, da un punto di vista linguistico gli elementi chiave che si applicano alle varie piattaforme sono l'architettura del pubblico, l'ingegneria linguistica, la già citata lingua del quartiere e l'ecosistema più ampio, che si basa a sua volta sulle regolarità della lingua. Da ciò consegue che:

> Se vogliamo contrastare la disinformazione, dobbiamo capire sia il linguaggio dei nostri avversari che il nostro. Dobbiamo trovare il modo di produrre un linguaggio che risuoni con le narrazioni che vogliamo promuovere. Dobbiamo contrastare la loro narrazione e allo stesso tempo stabilire la nostra.

Il punto è che né la NATO né l'UE hanno una politica di comunicazione strategica specifica e sono quindi dei 'follower' piuttosto che dei 'trendsetter' in questa importante arena. La NATO poi non ha ancora una definizione concordata di 'comunicazione strategica'. Nel frattempo, i regimi autoritari lavorano attivamente su questo importante elemento di manipolazione e interferenza dell'informazione.

Spostando l'attenzione dalla comunicazione verbale a quella visiva, **Massimiliano Fusari** analizza il ruolo dei media visivi nei processi comunicativi odierni, applicando le tecniche di storytelling in modo specifico alla politica internazionale.

'Il presente è visivo', sostiene Fusari:

> oggi oltre il 90% di tutti i dati presenti su internet è di tipo visivo, in una forma o nell'altra. In realtà, la comunicazione è sempre stata visiva e sicuramente continuerà ad esserlo. La comunicazione visiva è, ed è sempre stata, la chiave per elaborare strategicamente messaggi efficaci e d'impatto in tutti i settori della società e delle culture. E ora, a un livello senza precedenti, per combattere la guerra delle percezioni, e quindi per smuovere i cuori e le menti del pubblico internazionale su questioni politiche.

Pensando alle relazioni internazionali, si consideri, ad esempio, la seguente immagine di Re Carlo III alla COP28 di Dubai (si veda ***Immagine 1***).

Si tratta della prima apparizione internazionale di Re Carlo, che indossa il suo abbigliamento formale, con cravatta e pochette. A ben guardare, però, la fantasia di questi accessori presenta una scelta meno convenzionale, come sottolinea Fusari:

> è una bandiera greca moltiplicata all'infinito su entrambi gli accessori, che è stata ampiamente interpretata come un implicito segno di sostegno al primo ministro greco Kyriakos Mitsotakis per la recente disputa avuta con il suo omologo britannico in merito alla restituzione dei marmi del Partenone dal British Museum. Per deplorare l'atteggiamento del suo premier, che rifiutava persino di incontrarsi per discutere la questione, Re Carlo ha dichiarato la sua posizione in *modo chiaro* ma *silenzioso*, ed è riuscito a farlo senza essere accusato di interferire con gli affari interni del suo governo: è stato il suo modo *implicito* di comunicare *esplicitamente* un messaggio *strategico*.

'Lo storytelling', spiega Fusari, 'mira ad allineare i messaggi *proiettati* con quelli *percepiti*, utilizzando strategicamente la giusta combinazione di "formato" e "contenuto"'. Come illustra l'esempio precedente, le immagini possono essere un formidabile strumento di narrazione per comunicare i messaggi desiderati, sia a livello personale che sociale.

Immagine 1
Re Carlo III alla COP28

Fonte: COP28/Christophe Viseux/Flickr

Partendo da questa intuizione, Fusari si addentra in un caso di studio per approfondire il ruolo del visual storytelling nelle relazioni internazionali. Il caso è quello del sito web saturday-october-seven.com, ideato dal suo autore (o dai suoi autori) per denunciare gli attacchi perpetrati da Hamas il 7 ottobre 2023.

Affrontare un tema così (politicamente) acceso ed (emotivamente) sensibile non può prescindere dall'affermare esplicitamente che questo contributo non si inserisce in alcun modo nella discussione del confronto militare, in quanto mira a discutere esclusivamente la politica di comunicazione di uno degli attori senza schierarsi in alcun modo. Inoltre, benché le immagini di questi eventi drammatici siano presentate come documentazione pubblica ampiamente disponibile in una molteplicità di formati mediatici, a causa del loro contenuto, esse potrebbero comunque urtare la sensibilità personale e/o pubblica.

Tralasciando qualsiasi discussione o giudizio sugli eventi e concentrandosi invece sul modo in cui l'autore o gli autori del sito hanno comunicato il loro messaggio, Fusari evidenzia come, già dalla home page, siano presenti alcuni dettagli chiave su cui soffermarsi.

Il primo elemento che appare nella home page è un avviso relativo a contenuti sensibili: 'Questo sito web contiene contenuti estremamente difficili da guardare del terribile massacro compiuto da Hamas il 7 ottobre' (si veda ***Immagine 2***). Come spiega Fusari:

> l'avviso è scritto in inglese e questo elemento ci porta a ipotizzare che il sito web sia destinato principalmente a un pubblico di lingua inglese e probabilmente internazionale. Poiché non esiste la possibilità di scegliere la lingua del sito web, una pratica piuttosto comune nella comunicazione internazionale, potremmo facilmente supporre che la politica di diffusione, per decisione consapevole o per limitazioni linguistiche, sia effettivamente rivolta a un pubblico internazionale di lingua inglese.

Il dominio del sito web è stato registrato (secondo il provider Internet GoDaddy) il 19 ottobre, dodici giorni dopo gli eventi in questione. Come sottolinea Fusari:

> molti nomi di dominio alternativi erano e sono tuttora disponibili a quasi un anno di distanza, e *all'epoca* si sarebbero potute scegliere diverse opzioni, tra cui, ad esempio, 'october-seven'. È quindi ragionevole concludere che l'inclusione del 'sabato', giorno sacro per gli ebrei, potrebbe essere intesa come un richiamo consapevole ed esplicito alla dimensione di non santità (*un-holiness*) dell'attacco perpetrato.

Questa considerazione è indirettamente rafforzata dal fatto che il titolo 'HAMAS MASSACRE' è costantemente ripetuto e scritto in maiuscolo in tutte le pagine e sezioni del sito, il che, unito all'indirizzo e-mail dedicato (hamasmassacre@gmail.com), 'ribadisce esplicitamente la gravità dell'attacco'. Infine, Fusari osserva che:

> tutti i materiali del sito web sono stati caricati il giorno stesso dell'acquisto del sito, senza alcuna modifica successiva, il che limita drasticamente i risultati delle ricerche su Google, dato che l'aggiornamento dei contenuti è un parametro fondamentale per il posizionamento ai primi posti del motore di ricerca di Google.

Non sorprende che esistano diversi siti web dedicati agli eventi del 7 ottobre, ognuno dei quali utilizza diversi schemi e approcci alla narrazione, con diverse

Immagine 2
Avviso relativo a contenuti sensibili del sito web saturday-october-seven.com.

Immagine 3
Home page del sito web saturday-october-seven.com.

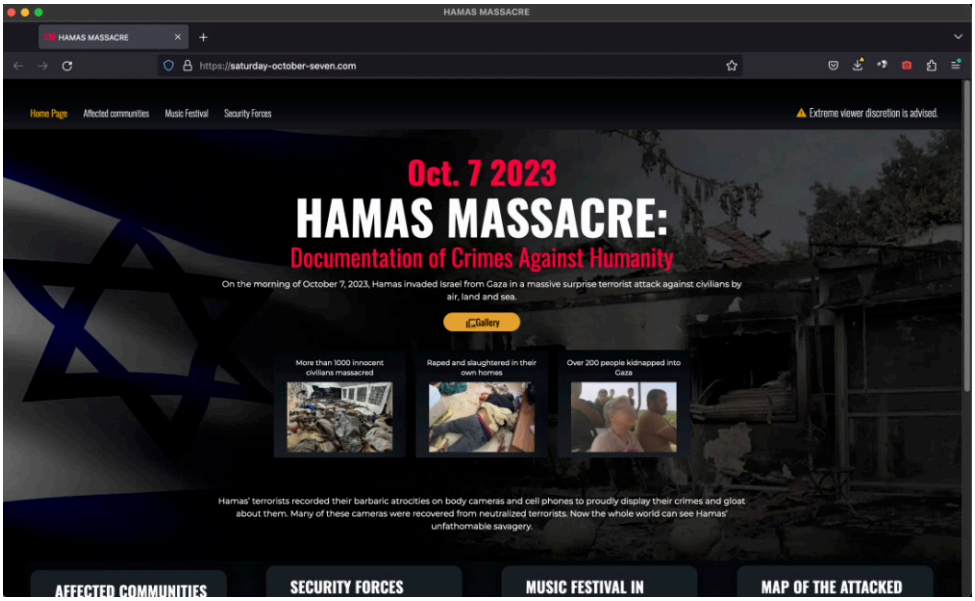
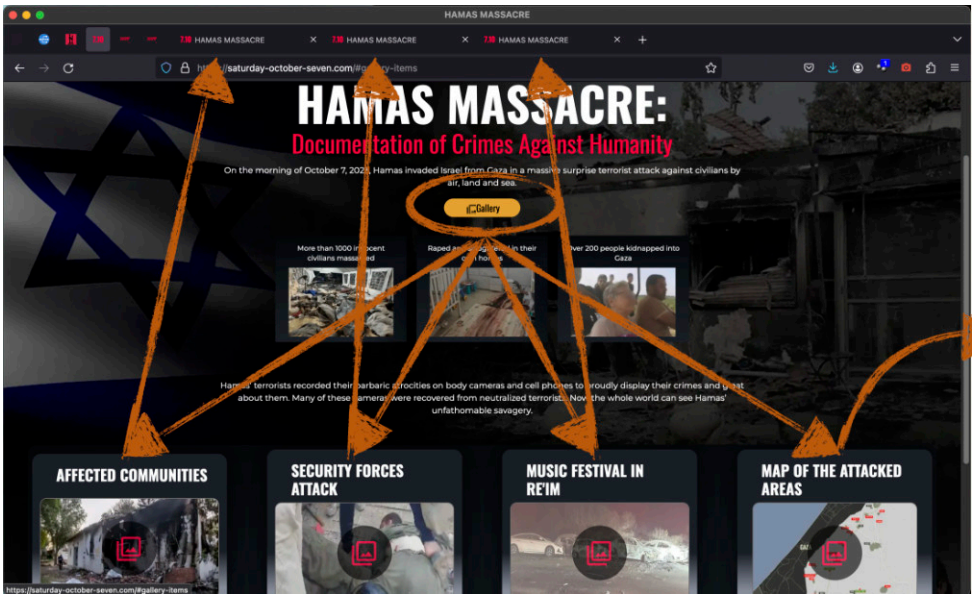


Immagine 4
Home page e gallerie del sito saturday-october-seven.com.



strategie di comunicazione e materiali di supporto dedicati. Nel caso di saturday-october-seven.com, Fusari affronta brevemente alcune preoccupazioni di base sul piano visivo, con esplicito riferimento al design dell'interfaccia utente (UI) o, in termini più semplici, all'aspetto del sito.

Come mostrato nell'immagine precedente, 'HAMAS MASSACRE' è al centro della pagina per dichiarare esplicitamente la 'missione' che il sito si propone: raccogliere 'Documentazione dei crimini contro l'umanità' (si veda ***Immagine 3***). Sullo sfondo ci sono due immagini: a sinistra una bandiera israeliana, a destra una foto che *potrebbe* mostrare l'esito di uno degli attacchi. 'Probabilmente', commenta Fusari, 'la connessione visiva è lì per produrre una relazione di causa-effetto con responsabilità esplicitamente dichiarate: Hamas'. Poi, tra due brevi trafiletti, una linea di accuse presenta un breve riepilogo dell'impatto dell'attacco, in tre punti: 'Più di 1000 civili innocenti massacrati', 'Stuprati e massacrati nelle loro case', 'Più di 200 persone rapite a Gaza'. Scorrendo la pagina, si trova un'articolazione più dettagliata dell'impatto degli eventi in riferimento a quattro gallerie tematiche: 'COMUNITÀ COLPITE', 'ATTACCO DELLE FORZE DI SICUREZZA', 'FESTIVAL MUSICALE A RE'IM' e 'MAPPA DELLE ZONE ATTACCATE' (si veda ***Immagine 4***).

Queste gallerie rappresentano 'categorie di storytelling utilizzate per guidare la comprensione degli eventi' e, una volta aperte, 'viene ripetuto lo stesso titolo per ogni sezione': "HAMAS MASSACRE"'. Come sostiene Fusari, 'questa caratteristica tende a essere controproducente quando si vuole massimizzare l'impatto della comunicazione, in quanto limita complessivamente l'esperienza dell'utente' (UX). Questo, afferma Fusari,

> potrebbe essere dovuto a una di queste possibilità: o il proprietario (o i proprietari) del sito web volevano ribadire la loro accusa, oppure, forse, i dettagli dell'UX sono stati considerati di secondaria importanza rispetto alla gravità dei materiali condivisi. Infine, una terza opzione potrebbe essere che i proprietari non sapessero come diversificare la heading structure, cioè l'organizzazione logica dei titoli.

Inoltre, come sottolinea Fusari, esiste una discrepanza nella UX del sito: le prime tre gallerie tematiche sono gallerie fotografiche dedicate, ma la quarta – una mappa – è mostrata come un'immagine singola sovrapposta e non è elencata nel menu in alto a sinistra. Fusari interpreta queste incongruenze con la possibilità che il sito web non sia stato progettato in modo professionale. Un'altra possibile ragione, aggiunge Fusari, è che:

> il focus del sito web possa essere stato quello di privilegiare il 'contenuto' rispetto alla 'forma', valutando il primo come abbastanza forte da trascurare la seconda. Ma lo storytelling efficace è quello che produce un impatto, e lo produce combinando il contenuto con la forma in modo intenzionale e finalizzato, e quindi strategico.

Come sostiene Fusari,

> la visualizzazione è informazione: la forma che si usa per mostrare qualcosa ha sicuramente un impatto sulla sua ricezione. Ad esempio, sussurrare o urlare

> (come strategia di comunicazione) lo stesso messaggio produce risultati piuttosto diversi, eppure la forma corretta dipende da una serie di fattori, tra cui il fatto che volessimo effettivamente che il messaggio fosse ascoltato (intenzionalità). Anche i messaggi grezzi comunicano, ma non sono storytelling perché non sono definiti da una strategia o da un'intenzionalità. Per esempio, lo stesso urlo potrebbe uscire dalla bocca a causa di un martello che ha colpito il dito invece di fissare un chiodo sul muro, oppure come una richiesta di aiuto. Uno è intenzionale, l'altro no. Uno fa parte di una strategia, l'altro no.

Infatti, Fusari chiarisce:

> mentre qualsiasi cosa ha il potenziale di comunicare, ciò che differenzia esplicitamente lo storytelling dai messaggi grezzi è l'intenzionalità di utilizzare la componente 'forma' (uno degli aspetti strategici) al suo massimo potenziale. Ovviamente la differenziazione tra storytelling e messaggi trarrebbe beneficio da una maggiore elaborazione, ma nel contesto di questo simposio possiamo concordare sul fatto che il visual storytelling si riferisce a un messaggio visivo che è stato intenzionalmente arricchito da una strategia di comunicazione che sfrutta appieno le specificità della sua forma mediatica.

Secondo Fusari, sul sito saturday-october-seven.com, si sarebbero potute utilizzare diverse tecniche di storytelling per dare forma ai messaggi visivi in modo più completo e d'impatto. Eppure:

> l'impressione generale è che le immagini siano state aggiunte al sito senza alcun criterio o strategia di comunicazione. Per qualsiasi motivo – rabbia, disperazione, o semplicemente incapacità o disinteresse per le potenzialità della forma – le immagini vengono presentate come 'contenuto grezzo', con l'implicazione che il pubblico dovrebbe dare loro un senso da solo. Probabilmente, le immagini sono state percepite come 'autosufficienti' rispetto ai loro messaggi (il massacro da parte di Hamas) come contenuti comunicativi veramente efficaci, senza bisogno di un ulteriore supporto da parte della 'forma'.

L'immagine sottostante, ad esempio, potrebbe trasmettere messaggi diversi fornendo didascalie e tag diversi (si veda ***Immagine 5***). Di per sé:

> l'immagine assomiglia molto a un drammatico incidente d'auto a cui potremmo assistere su qualsiasi strada, ovunque. Fornendo un supporto verbale sotto forma di didascalia o di tag, il contenuto visivo avrebbe potuto essere inteso meglio e comunicato più efficacemente.

In effetti, per ribadire quanto detto sopra, i messaggi grezzi fanno parte della comunicazione e sicuramente comunicano. Tuttavia, raramente, se non mai, le immagini hanno un valore *oggettivo* in sé: il loro significato è contestualizzato. 'Una tattica di contestualizzazione', continua Fusari:

> è effettivamente un supporto verbale, sotto forma di didascalia o di tag. Ma vi è un'altra tattica che potrebbe essere maggiormente d'impatto perché agisce in modo implicito, anziché esplicito (come una didascalia), ed è quella di

Immagine 5
Una delle immagini presenti sul sito saturday-october-seven.com.

> mettere in sequenza le immagini in modo strategico.

Ad esempio, accedendo a una delle gallerie tematiche del sito saturday-october-seven.com, l'utente si trova di fronte a un muro di immagini angoscianti senza alcun ordine rilevabile:

> In che modo l'utente potrebbe, o dovrebbe, leggere e dare un senso a queste immagini? Qual è il loro punto di partenza? Qual è la loro linea di sviluppo? In che modo il loro ordine e la griglia di presentazione influenzano la capacità dell'utente di leggere, comprendere e infine apprezzare la comunicazione prevista?

Interrogandosi su questo, Fusari sottolinea ancora una volta che la 'forma' è 'contenuto': la prima senza il secondo non svolge il suo compito, ed è per questo che lo storytelling dovrebbe essere concepito come la combinazione strategica dei due (contenuto e forma) per produrre un impatto'. Infatti, nel caso del sito saturday-october-seven.com:

> ordinando strategicamente i contenuti visivi e fornendo un indice rivelatore di tale ordine, l'autore (o gli autori) del sito web avrebbe potuto portare il pubblico a dare un senso ai materiali presentati in un modo – si spera – il più vicino possibile a quello previsto. Oppure, detto altrimenti, un editing mirato e strategico avrebbe potuto aiutare ad allineare la proiezione con la percezione.

Ad esempio, spiega Fusari:

> accostare le due immagini sottostanti [si veda ***Immagine 6***] nello stesso riquadro avrebbe evidenziato in modo strategico il prima e il dopo degli eventi del 7 ottobre, cogliendo la crudeltà e l'orrore degli attentati e portando a un'identificazione implicita dei cinque cadaveri nei sacchi con le cinque persone sorridenti in alto a sinistra e, infine, con una famiglia, che avrebbe aggiunto un ulteriore livello di emozioni di grande impatto.

Immagine 6
Una combinazione di due immagini presenti nel sito web saturday-october-seven.com

È importante notare che tutte le considerazioni di cui sopra non fanno altro che scalfire la superficie delle ricchissime possibilità di comunicazione offerte dai media visivi: 'Per sua natura, la comunicazione visiva articola all'infinito messaggi multipli e coesistenti che il visual storytelling si sforza di gestire e articolare con intenzionalità, impegnando strategicamente la componente della forma'. Infine Fusari ammette:

> la mia linea di ragionamento potrebbe rivelarsi una mera speculazione, poiché qualsiasi cosa io abbia visto (e quindi interpretato) in quelle immagini e nella struttura del sito web potrebbe in realtà risultare solo un mio percorso analitico e interpretativo. Dopotutto, ciò non è così raro, proprio a causa della drammatica volatilità dei processi di creazione del significato *visivo* e della complessità dell'essere umano.

In questo contesto, l'obiettivo esplicito di Fusari è proprio quello di mettere in guardia dalle complessità delle relazioni tra i mittenti e i destinatari dei messaggi, siano essi intenzionali o non intenzionali, a causa delle possibilità virtualmente infinite di interpretazione e lettura degli stessi materiali di comunicazione. Fusari chiude aggiungendo che:

> queste complessità devono essere riconosciute e affrontate criticamente, poiché anche solo la consapevolezza di queste dinamiche, di per sé, rappresenta già un livello base di competenza visiva, che rimane fondamentale nei processi di comunicazione odierni, indipendentemente dai formati. Purtroppo, quando si guardano le immagini, nulla è mai scontato. Quindi, il visual storytelling è quell'insieme di strumenti dedicati necessari per incanalare le multiformi esplosioni di significati che le immagini producono come messaggi, utilizzando intenzionalità e strategia per rendere i messaggi proiettati un tutt'uno con quelli percepiti.

Seguendo un focus più istituzionale, ***Matthew Heneghan*** fa luce sui processi e i modelli di disinformazione in Asia centrale tra gli shock geopolitici della pandemia

COVID-19 e l'inizio della guerra su larga scala della Russia contro l'Ucraina. Heneghan comincia sottolineando l'importanza di riconoscere che la diffusione di norme e idee sulla disinformazione, e il modo in cui questa dovrebbe essere affrontata dai governi, varia in modo significativo al di fuori della regione transatlantica.

L'Asia centrale è una delle regioni in più rapida crescita in termini di penetrazione di internet e di strategie di digitalizzazione, entrambe guidate principalmente da attori statali con un contributo marginale del settore privato. Nei cinque Stati dell'Asia centrale – Kazakistan, Kirghizistan, Tagikistan, Turkmenistan e Uzbekistan – fino al 95% del traffico internet giornaliero passa attraverso server russi, mentre i media statali russi trasmettono in tutta la regione, come previsto dagli accordi intergovernativi che risalgono all'epoca della Comunità degli Stati Indipendenti (CSI) negli anni Novanta. In tutta l'Asia centrale, i media locali, pur non essendo sotto la diretta giurisdizione degli organi di regolamentazione russi, hanno subito pressioni per 'sanificare' e persino censurare i materiali trasmessi. L'influenza dei media statali russi sulle pratiche di consumo dell'informazione nella regione, tuttavia, varia notevolmente: in Kirghizistan e Turkmenistan, ad esempio, le famiglie guardano regolarmente i notiziari statali russi; in Kazakistan e Uzbekistan, invece, prosperano i contenuti mediatici prodotti nelle lingue locali. Ciononostante, lo sviluppo di ambienti mediatici nelle lingue locali è limitato e condizionato da crescenti restrizioni, come verrà discusso di seguito.

Heneghan dice:

> Per capire come si presentava l'economia politica dell'informazione in Asia centrale all'inizio della guerra del 2022, è necessario guardare all'immediato antefatto: la pandemia COVID-19. È in questo periodo che gli Stati hanno iniziato a consolidare diverse strategie di controllo delle informazioni.

Le risposte al COVID-19 variano in modo significativo tra gli Stati. Ad esempio, il Turkmenistan ha negato completamente l'esistenza del COVID-19, il che ha comportato la messa a tacere del personale sanitario. Nel frattempo, il Kazakistan ha intrapreso un contenimento totale della diffusione del virus, il che ha permesso la limitazione della libertà dei media nell'ambito delle misure di quarantena. In termini di disinformazione, il contesto di controllo delle informazioni della pandemia ha portato a un fenomeno regionale unico, che Heneghan descrive come una 'biforcazione della categorizzazione della disinformazione'. Questa biforcazione, spiega Heneghan, comporta una situazione in cui 'le fake news convenzionali e le teorie del complotto sono state confuse e assimilate a tutto ciò che contraddiceva i resoconti ufficiali del governo sul contenimento dell'infezione'. In questo periodo è emersa un'infrastruttura informativa che ha permesso alle élite politiche di inquadrare selettivamente le risposte dello Stato alla pandemia e, più in generale, di dimostrare la propria capacità di gestire l'integrità informativa a livello nazionale. Detto altrimenti, la segnalazione di una pandemia è diventata un meccanismo per mantenere la legittimità del presidente o per sottomettere le lotte intestine tra i dirigenti politici.

> È proprio nel periodo di sovrapposizione tra lo scoppio della pandemia e l'inizio della guerra che abbiamo osservato interessanti sviluppi nel campo del

> controllo delle informazioni, con l'aggiunta di nuove leggi e regolamenti alla legislazione esistente, spesso incorporando il termine 'disinformazione'.

Ad esempio, la legge sulle false informazioni del Kirghizistan (2020) e la legge contro gli insulti alle élite politiche dell'Uzbekistan (2021) hanno ampliato le legislazioni esistenti in materia di diffamazione, consentendo il blocco o la cancellazione di informazioni online senza alcun ordine del tribunale – 'permettendo di fatto ai governi di rimuovere qualsiasi contenuto online con cui non sono d'accordo'. Nello stesso periodo, Kazakistan e Kirghizistan hanno ampliato le loro misure 'anti-agenti stranieri', modellandole sulla legge russa: i fornitori di servizi stranieri sono stati obbligati a registrarsi localmente e/o a localizzare le strutture di archiviazione dei dati, consentendo restrizioni immediate sull'attività dei cittadini e permettendo di fatto al governo di chiudere le operazioni di qualsiasi organizzazione che riceva finanziamenti stranieri – 'ad eccezione di quelle legate alla Russia', sottolinea Heneghan, 'perché la Russia non è l'obiettivo di queste leggi sul contenimento dell'influenza interna'. Inoltre, a partire dal 2021, tutti gli Stati hanno regolarmente attuato shutdown parziali o totali in risposta a disordini sociali. Il caso più grave si è verificato nel 2022, quando in Kazakistan c'è stato un blocco di internet durato una settimana che è costato all'economia nazionale più di 410 milioni di dollari al giorno, sottolineando quanto gli Stati possano arrivare a controllare i flussi di informazioni.

In tale contesto, l'inizio della guerra ha portato a ciò che Heneghan identifica come 'disinformazione deliberativa', spiegando:

> La risposta all'invasione russa dell'Ucraina è stata diversa nei vari Stati dell'Asia centrale: Kazakistan e Uzbekistan hanno adottato una posizione di 'neutralità strategica', mentre Tagikistan e Turkmenistan sono rimasti in silenzio. Eppure nessuno Stato ha riconosciuto l'invasione come una vera e propria guerra. Tutti hanno rispettato i regolamenti russi utilizzando il termine 'operazione speciale'.

Questo periodo ha visto un'ulteriore biforcazione della disinformazione e approcci statali incoerenti. Da un lato, gli Stati dell'Asia centrale hanno fatto eco alle grandi narrazioni russe sulla giustificazione della guerra (ad esempio, i sentimenti anti-NATO e le accuse di repressione dell'etnia russa nell'est dell'Ucraina). Allo stesso tempo, però, hanno pubblicato selettivamente informazioni sull'attualità del conflitto in Ucraina, come il massacro di Bucha. È a questo punto che la disinformazione è diventata un processo deliberativo, che ha richiesto la triangolazione di diversi quadri normativi dalla parte russa, di politiche esecutive da parte di attori interni, di condizionalità occidentali per lo sviluppo (che hanno reso impossibile per gli Stati dell'Asia centrale adottare una posizione totalmente pro-Russia/anti-Ucraina) e di pressioni e contro-narrazioni civili. Secondo Heneghan, tale processo ha portato anche a un effetto di contiguità e di ricaduta della cronaca di guerra, per cui la copertura delle atrocità belliche ha reso più visibili i contorni dei media indipendenti e della società civile, spingendo gli Stati a limitare ulteriormente il sostegno non governativo alla lotta contro la dis/misinformazione.

Per comprendere queste complesse dinamiche regionali, Heneghan propone il concetto di 'coerentismo di regime': un quadro di riferimento per comprendere la

costruzione del consenso regionale in relazione alla gestione delle informazioni in Asia centrale. Come spiega Heneghan, a partire dagli anni Novanta tutti gli Stati dell'Asia centrale hanno cercato la 'sicurezza ideativa' (*ideational security*) e la sopravvivenza (collettive) attraverso istituzioni interregionali come CSI, Collective Security Treaty Organization (CSTO) e, più recentemente, l'Unione Economica Eurasiatica (EAEU). Queste istituzioni approfondiscono la cooperazione e la dipendenza strutturale nei confronti della Russia e si rafforzano reciprocamente in termini di sopravvivenza del regime. In altre parole, in Asia centrale la regionalizzazione rappresenta un atto di sicurezza ontologica (*ontological security*) – e quindi 'le narrazioni russe per giustificare la guerra in Ucraina non possono essere considerate illegittime o criticate, poiché ciò potrebbe minacciare gli stessi accordi politici e istituzionali tra gli Stati dell'Asia centrale'. Piuttosto, 'gli Stati dell'Asia centrale devono impegnarsi in una sottoscrizione strategicamente ambigua e simultanea di diversi 'regimi di verità' (*truth regimes*) e quindi sia la disinformazione deliberativa che il problema di discernere l'integrità di qualsiasi unità informativa nella regione dipendono 'dalle posizioni momentanee e dai livelli di dipendenza strutturale dei regimi statali nei confronti della Russia, dell'UE, degli Stati Uniti e dei grandi attori del settore privato'.

Secondo Heneghan, 'è quindi importante riconoscere che la disinformazione in Asia centrale può essere dannosa per le relazioni interne e/o internazionali e al contempo rafforzare il sostegno, la capacità e la sopravvivenza dei regimi'. Il tentativo di superare questo paradosso fornendo fondi alla società civile digitale e ai media indipendenti non sarà sufficiente. 'Per contrastare la disinformazione in contesti autoritari', afferma Heneghan, 'è necessario incentivare la cooperazione a livello statale, per superare l'effetto di coerenza del regime'. Heneghan suggerisce tre modi per farlo. Una strada è quella di spingere per una definizione giuridica di 'disinformazione' a livello regionale che distingua con forza tra informazioni dannose e libera espressione online, impedendo così l'uso improprio delle leggi sulla disinformazione per soffocare il dissenso. È inoltre fondamentale sostenere lo sviluppo dei media digitali in lingua locale per raggiungere l'equivalenza con le fonti in lingua russa. Allo stesso modo, una maggiore attenzione all'istruzione in lingua inglese aiuterebbe a eludere l'influenza del Cremlino e a costruire un'alfabetizzazione mediatica in tutta l'Asia centrale, anche se l'obiettivo a lungo termine dovrebbe essere quello di costruire un forte ambiente mediatico autoctono. Infine, 'possiamo affrontare la programmazione dello sviluppo digitale come un mezzo per costruire la società e la capacità istituzionale senza un'enfasi esplicita sulla politica di regime o su argomenti controversi come la guerra in corso in Ucraina'. Tuttavia, conclude Heneghan, ci troviamo di fronte a un dilemma etico: è giusto perseguire un'agenda di sviluppo così 'asettica' 'senza trasparenza sulle posizioni e gli obiettivi dei donatori'?

PANEL 2

Affrontare l’autoritarismo nella governance digitale

Il 20 settembre 1987 è stata inviata dalla Cina la prima email dichiarando con grandi speranze che "Attraverso la Grande Muraglia possiamo raggiungere ogni angolo del mondo". Più di 35 anni dopo, tuttavia, quella che oggi è conosciuta come il 'Great (Fire)Wall' cinese ha creato un mondo a sé stante, in cui 'chi è dentro la Muraglia non può vedere fuori, e chi è fuori non può vedere dentro', afferma **Fang-Long Shih**, il primo relatore del secondo panel. Tuttavia, un'eccezione cruciale è rappresentata dal modo in cui lo stesso governo cinese trascende il Firewall per impegnarsi in forme sempre più sofisticate e pervasive di attività illecite su internet oltre i confini nazionali.

Infatti, racconta Shih:

> mentre negli anni Novanta il governo cinese ha sostenuto a gran voce l'espansione della connettività, ha contemporaneamente adottato misure per controllarla non appena internet è stata aperta al pubblico nel 1995. Nel 1997, il Ministero della Pubblica Sicurezza cinese ha emanato le Misure per la gestione della protezione della sicurezza della rete internazionale di reti informatiche (*Measures for Security Protection Administration of the International Networking of Computer Information Networks*), approvate dal Consiglio di Stato. Nello stesso anno, Pechino ha introdotto le prime leggi che criminalizzano i post online considerati una minaccia alla sicurezza nazionale, che pragmaticamente significa la sicurezza del Partito Comunista Cinese (PCC).

In effetti, come ha osservato nel 2017 Rogier Creemers, specialista di DigiChina, 'Quando internet è diventata una piattaforma di informazione e comunicazione pubblicamente accessibile, non si è discusso se essa dovesse ricadere sotto la supervisione del governo, ma solo su come tale controllo sarebbe stato attuato nella pratica'. Detto altrimenti, Shih osserva che:

> la guerra organizzativa (*zuzhi zhan*, 組織戰) ha avuto un ruolo significativo nel consolidamento iniziale del potere del PCC. 'Mobilitare un gruppo di persone per combatterne un altro (*qunzhong dou qunzhong*, 群眾鬥群眾)' è diventata, dall'ascesa del PCC, una tattica iconica per reprimere nemici e dissidenti.

Shih commenta inoltre che, dall'avvento dell'era digitale, 'il controllo di internet è sempre stato parte integrante della governance digitale cinese, che è fondamentale per mantenere il potere del PCC'.

La presentazione di Shih non verte quindi su come il mondo digitale potrebbe cambiare la Cina, ma su come la Cina ha cambiato il mondo digitale. Il Great Firewall è un sofisticato sistema di tecniche e metodi che il governo cinese utilizza per bilanciare la connettività con controlli severi. Uno dei modi più pervasivi in cui il Great Firewall viene utilizzato per censurare i contenuti online è il cosiddetto '*sniffing*'. Si riferisce al modo in cui il PCC impiega le tecnologie di rilevamento delle intrusioni per individuare e bloccare le parole chiave ritenute sensibili dal governo (ne sono un esempio i termini 'Xi Jinping', 'indipendenza di Taiwan', 'democrazia').

Il Firewall funziona insieme a metodi basati sul comportamento, in cui i censori analizzano il traffico web e i nomi dei server per individuare i siti sospetti e bloccarli manualmente. Alcuni domini, quali google.com o facebook.com, sono inseriti nella

blacklist, il che significa che gli utenti cinesi non possono accedervi senza aggirare le maglie sempre più strette del Great Firewall. Ad esempio, Shih osserva: 'Negli anni Novanta, qualsiasi forum online cinese noto come BBS (Bulletin Board Systems) che avesse più di 1.000 visualizzazioni poteva attirare l'attenzione della polizia. Successivamente, nell'era di Weibo, la soglia si è dimezzata a 500'. Allo stesso tempo, i siti web e le app che desiderano operare in Cina hanno bisogno di un permesso di registrazione come Internet Content Provider (ICP) rilasciato dal governo cinese.

È importante notare, tuttavia, che tali funzioni di censura non sono svolte esclusivamente da agenzie governative. Infatti, per controllare il mondo digitale, il governo cinese spesso affida la censura ad aziende nazionali e internazionali, come la statunitense Cisco Systems, che ha aiutato il PCC a costruire il Great Firewall. Avvalendosi di meccanismi di mercato e promuovendo la concorrenza nel settore privato, il governo cinese garantisce che i suoi sforzi di censura rimangano efficienti e aggiornati. Come spiega ancora Shih:

> Le aziende private nazionali spesso competono per i contratti governativi, cercando di essere il più efficaci possibile a causa dei margini di profitto ridotti. Se questi sforzi fossero portati avanti solo da agenzie governative e funzionari pubblici, sarebbero probabilmente meno efficienti a causa della mancanza di motivazioni di profitto e di concorrenza di mercato.

La governance digitale cinese non è quindi caratterizzata da un controllo totale. Piuttosto, come accennato in precedenza, il PCC si è impegnato in un attento e delicato gioco di equilibri tra connettività e controllo, devolvendo alcuni parametri chiave di controllo al settore privato. Pertanto, il controllo autoritario del PCC non è amministrato direttamente. Né il suo controllo autoritario è assoluto, poiché, come sottolinea Shih:

> I *netizen* e i dissidenti cinesi hanno trovato modi creativi per eludere il filtraggio e il blocco dei contenuti online. Ad esempio, alcuni *netizen* sono esperti nell'usare il sarcasmo, come nel caso dell'hashtag *#ChinaIsAGreatPlaceToLive*, o dei numerosi post di scherno condivisi online durante la pandemia di COVID-19, come '*We need to refuse the vaccine in the horrible West, because chief Hu's [Hu Xijin, of the Global Times state media] saliva drops are the best vaccines for us*' (Dobbiamo rifiutare il vaccino dell'orribile Occidente, perché le gocce di saliva del capo Hu [Hu Xijin, dei media statali Global Times] sono il miglior vaccino per noi).

Alcuni dissidenti cinesi sono anche in grado di aggirare il Great Firewall attraverso reti private virtuali (VPN) semi legali, 'ma la maggior parte di coloro che usano le VPN lo fanno per scopi non considerati minacciosi dal PCC, e quindi implicitamente condonati', chiarisce Shih. Il punto, continua, è che 'il PCC si riserva sempre la possibilità di applicare misure restrittive in circostanze particolari (come il 4 giugno [data delle proteste di Tiananmen Square] e il 1° ottobre [festa nazionale] o durante il periodo del Congresso del Popolo) o in relazione alla proliferazione di certe ricerche o di alcune parole chiave. Secondo uno degli informatori di Shih, 'Se voglio davvero aggirare la barriera esistente, diventa sempre più dispendioso in termini di tempo, a volte fino a 40 minuti per una singola ricerca'. Altri informatori affermano che, nonostante le opportunità che esistono per molti di superare il Firewall, 'la

maggior parte dei cittadini cinesi non si preoccupa e opera tranquillamente all'interno del Firewall ritenendo che le informazioni a cui potrebbe accedere al di là del Firewall "non siano utili" per loro in Cina'.

Shih conclude che nell'era dell'informazione, la strategia della guerra organizzativa si è ulteriormente intensificata. Il PCC utilizza il Firewall per continuare a mobilitare un gruppo di persone all'interno dello stesso (noto come *Xiaofenhong*, 小粉紅) per combattere contro un altro gruppo all'esterno del Firewall. Queste dinamiche all'interno e all'esterno del Firewall portano a una divisione sociale tanto all'interno della Cina quanto tra la Cina e il resto del mondo. Questo è in linea con il detto di Mao Zedong 'maggiore caos nel mondo, maggiori benefici [per il PCC] (天下大亂，形勢大好)', che in seguito è diventato un principio guida del PCC. Il PCC costruisce e mobilita a proprio vantaggio qualsiasi minaccia percepita alla coesione sociale, 'usandola come giustificazione per la sorveglianza, la censura e la repressione dei cosiddetti "dissidenti", sia che si trovino all'interno del Firewall sia che si trovino in Paesi al di fuori di esso'. Queste tendenze digitali consentono una gamma sempre più ampia di modi per stabilizzare la governance autoritaria cinese e permettono di manipolare regole, norme e algoritmi in modo da indurre i cittadini ad agire secondo la volontà della leadership. Il controllo del governo cinese ha sviluppato una logica tutta sua, incarnata dalla portata omnicomprensiva del sistema di credito sociale (社會信用體系). Il PCC ha adottato elementi chiave della tecnologia digitale in una nuova direzione autoritaria, principalmente orientata a prevenire l'opposizione e il dissenso. Si pone quindi la questione se l'impiego della tecnologia digitale da parte della Cina debba essere considerato in una prospettiva comparativa e storica come eccezionale – come un cambiamento sostanziale – o semplicemente come un cambiamento di intensità.

Riflettendo sull'ascesa dell'autoritarismo digitale come fenomeno generale, **Giampiero Giacomello** ricorda l'ottimismo suscitato dall'avvento di internet a metà degli anni Novanta e nei primi anni Duemila:

> All'epoca c'era la visione idealistica che questa nuova tecnologia avrebbe favorito la comunicazione globale, sostenuto le democrazie e combattuto le autocrazie. Più di 25 anni fa questo aspetto è stato al centro della mia tesi di dottorato, in cui ho analizzato i motivi per cui i governi vorrebbero controllare internet.

All'epoca internet era percepita come una tecnologia liberatoria, mentre oggi sembra che il controllo governativo abbia il sopravvento nel cyberspazio. Le interazioni dinamiche tra governi, settore privato e singoli utenti in questo ambito sono complesse, ma, come riconosce Giacomello, è chiaro che:

> purtroppo gli utenti hanno perso molto, soprattutto in Paesi come la Cina, l'Iran e la Russia, dove i governi sono diventati molto efficaci nel controllare internet. Nonostante questo controllo non sia assoluto – perché non è assoluto – è significativamente più forte rispetto a 30 anni fa.

L'ascesa dell'IA porta con sé nuove considerazioni. L'IA introduce una serie di problemi di sicurezza relativi alla perdita di privacy e all'uso improprio dei dati personali, ma interagisce anche con il cyberspazio in modi intriganti. In effetti, le due cose sono strettamente collegate, anche perché i modelli computazionali si

dipanano nel cyberspazio. Pertanto, una migliore comprensione delle questioni contemporanee nel cyberspazio non può prescindere dal fare luce su come le grandi potenze affrontano l'IA.

L'IA dipende dall'apprendimento automatico ed ha pertanto bisogno di un volume enorme di dati di alta qualità per addestrare modelli linguistici di grandi dimensioni. Come afferma Giacomello, 'Oggi i dati di alta qualità sono come il *gold standard*. Sono come il petrolio'. In questo ambito, spiccano ovviamente le capacità e le risorse imprenditoriali degli Stati Uniti. Tuttavia, sostiene Giacomello, gli Stati Uniti non rappresentano l'attore più interessante su cui concentrarsi, nonostante la loro posizione di leadership. Piuttosto, Giacomello si interroga sull'approccio all'IA della Cina:

> i *large language model* devono essere conformi a linee guida pratiche. Non possono discostarsene. Come fa la Cina a formare modelli con tali vincoli? Alcuni esperti di *machine-learning* suggeriscono che la Cina voglia farci credere di essere limitata da queste regole, mentre in realtà le sue esplorazioni sono probabilmente più avanzate di quanto pensiamo, forse alla pari o addirittura superiori a quelle degli Stati Uniti. Ma anche se fosse così, rimangono delle domande fondamentali: che tipo di dati sta usando la Cina? Come detto precedentemente, l'addestramento di modelli linguistici di grandi dimensioni richiede un'enorme quantità di dati. Questi dati provengono spesso da internet e sono prevalentemente in inglese. La Cina addestra i modelli cinesi con testi in inglese?

D'altra parte, la Russia ha un'enorme potenza intellettuale, ma è carente di risorse materiali per l'IA. 'I Russi stanno seguendo la loro strada, ma non sono grandi concorrenti in questo campo', afferma Giacomello. Al contrario, aggiunge, 'l'Arabia Saudita e gli Emirati Arabi Uniti stanno investendo molto nell'IA e stanno emergendo come potenziali concorrenti, sollevando interrogativi sul loro approccio all'IA, dato che anche questi Paesi non sono famosi per la loro attitudine democratica'.

Da parte sua, l'Europa ha un approccio peculiare alla tecnologia: non esistono campioni europei di rilievo nella corsa alla tecnologia e l'Europa, nel suo complesso, sembra operare nell'arena americana. Allo stesso tempo, l'UE sembra essere soddisfatta di fungere da regolatore, come dimostra il successo del Regolamento generale sulla protezione dei dati (GDPR) nell'influenzare le pratiche globali – anche se, come sottolinea Giacomello, rimane incerto se questo successo normativo si estenderà all'IA. Nel complesso, sembra che 'l'Unione Europea si sia rassegnata ad essere una potenza normativa e culturale piuttosto che una forza competitiva nel settore tecnologico. Pare che l'Europa abbia rinunciato a competere con gli Stati Uniti o la Cina in questo campo'.

Queste dinamiche ci riportano alle riflessioni iniziali di Giacomello sulla storia di internet o, meglio, sullo *zeitgeist*, lo spirito del tempo, in cui internet è nata, ma anche quello del tempo in cui l'IA si sta sviluppando. Giacomello spiega:

> La tecnologia è neutrale, ma è fortemente influenzata dal contesto globale più ampio. Quando internet è diventata disponibile, c'erano grandi speranze e atteggiamenti positivi. Con la fine della Guerra Fredda, molti Paesi stavano

> abbracciando la democrazia e sembrava che il mondo stesse cambiando in meglio. Tecnologie e ottimismo si sono influenzati a vicenda, creando un senso di progresso. Oggi siamo tornati alla competizione tra grandi potenze e l'IA è vista come uno strumento per aumentare il controllo e le macchine come potenzialmente in grado di dominare gli esseri umani.

Detto in altri termini, è difficile separare l'influenza dei fattori contestuali dagli impatti reali e percepiti della tecnologia stessa, poiché i due aspetti si influenzano profondamente a vicenda. Il rapporto tra politica e tecnologia rimane una forza fondamentale delle nostre società. Eppure 'i nostri atteggiamenti e le nostre percezioni si sono invertiti, evidenziando ora il potenziale di queste tecnologie di essere usate per il controllo piuttosto che per la liberazione'.

Prendendo spunto dall'approfondimento di Giacomello sulla posizione europea nella governance digitale, **Antonella Seddone** ed **Enea Fiore** discutono del ruolo dell'UE nella regolamentazione del marketing politico sui social media, condividendo alcuni dei risultati preliminari della ricerca che stanno conducendo con **Daniela Romée Piccio**.

Gli strumenti digitali hanno rimodellato la comunicazione politica e alterato il rapporto tra cittadini e politica, contribuendo alla personalizzazione della politica e alla conseguente marginalizzazione del ruolo dei partiti politici (cioè alla disintermediazione). Secondo Seddone, una spiegazione di questi sviluppi può essere trovata nei meccanismi operativi delle piattaforme digitali stesse: 'Le piattaforme digitali favoriscono la diffusione di informazioni distorte e fuorvianti, consolidando i punti di vista e contribuendo alla polarizzazione. Gli algoritmi danno priorità ai contenuti che si allineano alle convinzioni e ai pregiudizi degli utenti, rafforzando i pregiudizi e creando camere dell'eco'. Inoltre, continua Seddone, 'le piattaforme digitali raccolgono dati sulle opinioni, le attitudini e le convinzioni, consentendo agli attori politici di elaborare la loro comunicazione in modi altamente efficaci e persuasivi'. Questi dati consentono di fare microtargeting politico,

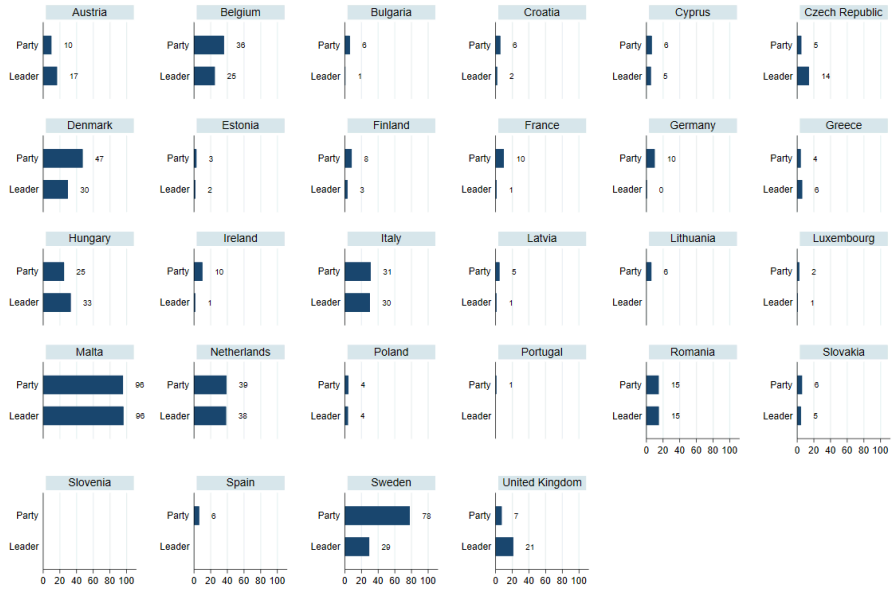


Grafico 1
Spesa media per le inserzioni su Facebook.

Fonte: Antonella Seddone et al.

raggiungendo segmenti specifici di popolazione con messaggi su misura'. Pertanto, rispetto ai media tradizionali come la televisione e la radio, le piattaforme digitali offrono un metodo economicamente vantaggioso per un marketing politico mirato, rendendolo una strategia accessibile a una più ampia gamma di attori.

Per avere un quadro più chiaro del fenomeno, Seddone e i suoi colleghi di CODER hanno analizzato i dati relativi alle spese sostenute nel 2022 dai cinque partiti più votati e dai loro leader nei 27 Paesi dell'UE e nel Regno Unito, per le pubblicità su Facebook e Instagram. I dati mostrano che alcuni Paesi, come Danimarca, Ungheria, Italia e Svezia, presentano livelli di spesa elevati (cfr. ***Grafico 1***).

Per comprendere meglio questi schemi, Seddone e colleghi hanno condotto un'analisi esplorativa utilizzando un modello di regressione multilivello che considera sia i fattori specifici di un Paese che quelli di un partito. 'Ciò che i nostri risultati sembrano indicare', afferma Seddone, 'è che due variabili determinano una maggiore spesa per la pubblicità politica online: il posizionamento a destra e il populismo' (cfr. ***Grafico 2***).

Non sorprende che l'uso dei social media a fini politici sia sempre più sotto i riflettori e che i potenziali impatti negativi di tali pratiche siano stati ampiamente dibattuti nel mondo accademico e tra gli esperti. Tuttavia, 'questo problema non è solo una preoccupazione degli studiosi', chiarisce Seddone: 'è una preoccupazione pressante per i cittadini, che chiedono misure istituzionali per affrontare le minacce percepite ai processi democratici e mantenere l'ordine in quello che potrebbe essere definito un "Far West".' Infatti, i dati dell'Eurobarometro pubblicati nel dicembre 2023 rivelano che i cittadini europei sono preoccupati per l'impatto che

Grafico 2
Variabili incluse nel modello di regressione multilivello.

Fonte: Antonella Seddone et al.

	AVERAGE EXPENDITURE ON ADS PER WEEK (€)
Party Leader account	-0.730 (-0.13)
ElecBon campaign's week	-4.221 (-0.11)
Party in government posiBon	11.56 (1.03)
Ideological positioning (0:leftwing; 10:rightwing)	**3.244*** (2.37)
People centrism	**8.925*** (2.42)
Expenditure limits on Ads	-26.21 (-1.24)
Limits on tradiBonal Ads	10.19 (0.52)
RegulaBon on old media access	12.66 (0.72)
_cons	-43.75 (-1.80)
lns1_1_1 _cons	3.108*** (12.55)
lnsig_e _cons	4.156*** (163.25)
N	788

la pubblicità online può avere sull'integrità delle elezioni. Alla domanda sugli elementi più importanti che definiscono una campagna elettorale libera e regolare, circa un terzo degli intervistati ha espresso il desiderio di sapere chi finanzia il marketing politico e i contenuti sponsorizzati e di poter distinguere tra contenuti sponsorizzati e non. Inoltre, il 27% degli intervistati ha sottolineato la necessità che i candidati e i partiti politici siano trasparenti sulle loro tecniche di targeting per la pubblicità politica (si veda ***Grafico 3***). Tuttavia, solo pochi Paesi dell'UE dispongono attualmente di normative sulla pubblicità online e le misure esistenti si concentrano esclusivamente sulla spesa, senza alcuna disposizione in materia di trasparenza o di contenuti. 'Questo evidenzia la necessità di una regolamentazione più ampia e completa da parte dell'UE', conclude Seddone.

In effetti, le implicazioni del marketing politico online per l'integrità elettorale europea hanno spinto l'UE ad adottare diverse misure per affrontare la manipolazione delle informazioni, proteggere la privacy dei cittadini e impedire ad agenti esterni e interni di sovvertire il processo democratico (ad esempio, interferenze straniere, propaganda computazionale, disinformazione e hate speech). Come racconta Fiore, 'Il primo tentativo di regolamentazione è stato il Code of Practice on Disinformation del 2018, che mirava a garantire una maggiore trasparenza e responsabilità da parte delle piattaforme online. Tuttavia, la sua

	Debates and campaigns avoid hate speech, manipulation and lies	Voters know who finances political advertising and sponsored content and can distinguish between sponsored content and non-paid for political information	Candidates and political parties are transparent in their use of targeting techniques for political advertising
AT	54	33	26
BE	36	28	31
BG	44	42	30
CY	45	37	28
CZ	36	31	21
DE	48	30	27
DK	50	38	25
EE	57	38	20
EL	47	38	27
ES	55	36	40
FI	49	41	19
FR	39	29	26
HR	42	44	25
HU	61	31	26
IE	35	43	32
IT	42	31	21
LT	36	43	29
LU	44	38	25
LV	40	44	23
MT	56	36	39
NL	39	29	25
PL	64	29	23
PT	37	28	33
RO	35	35	37
SE	55	38	18
SI	47	43	15
SK	41	37	21
EU27	***46***	***32***	***27***

Graph 3
Sondaggio Eurobarometro: Secondo lei, quali sono gli elementi più importanti che definiscono una campagna elettorale libera e corretta?

Fonte: Eurobarometro Flash 522 (dicembre 2023).

attuazione è stata lasciata alle piattaforme stesse'. L'UE ha rafforzato il Codice di condotta nel 2021 e di nuovo nel 2022; tuttavia, 'è solo nel febbraio 2024 che l'UE ha introdotto un regolamento completo, passando a una forma blanda di governance digitale'. Queste misure legali rispondono ad alcune delle principali preoccupazioni dei cittadini europei quando si tratta di contrastare la manipolazione delle informazioni e preservare l'integrità elettorale: i fornitori di servizi sono tenuti a etichettare gli annunci politici e a divulgare informazioni sull'identità degli sponsor, sulle spese e sulle elezioni specifiche a cui gli annunci politici sono collegati. Devono inoltre tenere traccia delle campagne pubblicitarie, creare un archivio di annunci diretti ai cittadini europei e rendere i dati disponibili e accessibili agli enti interessati (compresi i ricercatori). Inoltre, nell'ambito del nuovo regolamento, le tecniche di targeting che comportano il trattamento di dati personali sono consentite solo in presenza di un consenso esplicito e ai Paesi terzi è vietato sponsorizzare pubblicità politiche nell'UE nei tre mesi precedenti un'elezione o un referendum.

Sebbene questo passaggio dall'autogoverno degli Stati a un approccio a livello europeo sia da accogliere con favore, 'ci sono alcuni limiti', riconosce Fiore. Per esempio:

> alcuni potrebbero obiettare che vietare la sponsorizzazione solo tre mesi prima di un'elezione è insufficiente, poiché la formazione dell'opinione pubblica è un processo a medio e lungo termine. Ci sono anche sfide pratiche: le piattaforme di social media spesso non rivelano informazioni dettagliate o forniscono dati in forma aggregata, il che ostacola la ricerca scientifica. È importante notare che molte questioni, come la polarizzazione e l'incitamento all'odio, rimangono in gran parte non affrontate.

La disinformazione rimane una sfida, all'interno e all'esterno dell'Europa. Infatti:

> se superassimo le nostre tendenze eurocentriche, ci renderemmo conto che, contrariamente a quanto si crede, gli attori autoritari sono più attivamente coinvolti nella proliferazione di contenuti manipolati *al di fuori* dell'Europa - dimostrando la mancanza di strumenti internazionali condivisi per affrontare le fonti di disinformazione e le pratiche digitali autoritarie ed evidenziando la necessità di una cooperazione globale al di là dei confini o dei quadri giuridici europei.

PANEL 3

Our shared digital future: raccomandazioni per la cooperazione tra settore pubblico e privato

In apertura del terzo panel, **Kenddrick Chan** illustra alcuni dei principi alla base del modo in cui il settore privato si impegna con i governi nella governance digitale.

Oggi esistono pochi dubbi sul fatto che la gestione del dominio digitale richieda il coinvolgimento del settore privato e Chan ne individua almeno cinque ragioni. In primo luogo, il settore privato è la forza trainante dell'innovazione digitale ed è responsabile dello sviluppo delle stesse tecnologie di cui discutono i governi e le organizzazioni multilaterali. In secondo luogo, e in relazione a ciò, il dominio digitale non è solo una possibile fonte di disturbo, ma anche un amplificatore estremamente potente. Come spiega Chan, 'durante la Guerra Fredda un *agent provocateur* poteva influenzare una folla, ma nell'era digitale – e grazie alle tecnologie di cui sono responsabili le aziende private – questo effetto è esponenzialmente maggiore, raggiungendo un pubblico globale attraverso le piattaforme digitali'. In terzo luogo, le aziende private forniscono servizi finanziari e di comunicazione essenziali ai loro clienti, occupando così un ruolo importante e di fiducia nella società. In quarto luogo, alcune aziende hanno dimostrato la loro volontà di assumersi maggiori responsabilità, come nel caso di iniziative guidate dal settore privato come il *Cybersecurity Tech Accord* o la 'Convenzione di Ginevra digitale' di Microsoft – 'se queste iniziative abbiano raggiunto o possano raggiungere i loro obiettivi è discutibile, ma l'impegno del settore privato è chiaro', commenta Chan. Infine, i governi hanno bisogno 'delle competenze tecniche delle imprese private per garantire la conformità con qualsiasi politica venga approvata'. Tutto questo, riflette Chan, 'rende le aziende private un partner prezioso per i governi; ma rimane una domanda cruciale: le aziende private e i governi sono partner alla pari nella governance digitale? Potranno mai esserlo?'.

Secondo Chan, i governi collaborano con il settore privato in tre macro aree: formulazione delle politiche, attuazione delle politiche e sviluppo tecnico. Per quanto riguarda la formulazione delle politiche, Chan afferma:

> mentre molti pensano che i governi abbiano il monopolio della definizione delle strategie nazionali, ai livelli più alti i governi spesso si affidano alle aziende tecnologiche per indirizzare la direzione nazionale della politica digitale. Ad esempio, l'AI Safety Board della US Homeland Security comprende membri di OpenAI, Nvidia, Microsoft e Google.

Allo stesso modo, nonostante tutte le discussioni sulla 'sovranità digitale', 'dobbiamo renderci conto che anche i governi dei Paesi avanzati spesso stipulano contratti commerciali con aziende private, poiché queste ultime sono spesso più agili ed efficienti della maggior parte delle agenzie tecnologiche sostenute dallo Stato'. Quando si tratta di attuare una politica, i governi fanno molto affidamento sul settore privato per ottenere le informazioni necessarie ad agire in modo efficace: 'non si può regolamentare ciò che non si può misurare'. I governi hanno bisogno di 'dati sulla portata e sull'impatto delle notizie o delle fake news, che solo le aziende private possono fornire'. In cambio, le aziende private hanno bisogno di rassicurazioni e 'segnali' riguardanti i piani governativi. Le aziende private consentono inoltre un maggior grado di agilità nella regolamentazione:

> come dimostra il caso dello *shutdown* totale in Kazakistan citato da Heneghan, sta diventando chiaro che questo tipo di approcci restrittivi sono

> molto costosi e rischiosi. Oggi la maggior parte dei governi preferisce un approccio normativo condizionatamente restrittivo piuttosto che completamente proibitivo nei confronti dei propri ecosistemi, per cui il settore privato è visto come un partner.

Ovviamente, come accennato in precedenza, il settore privato è un partner fondamentale quando si tratta di sviluppo tecnico: da un lato, la cooperazione pubblico-privato consente di combinare le risorse e di facilitare gli investimenti su larga scala, nonché di accedere a risorse e talenti che nessuno dei due potrebbe ottenere da solo. D'altra parte, il settore privato si affida ai governi per creare un ecosistema nazionale favorevole alle imprese, mentre i governi si affidano al settore privato per creare un ecosistema nazionale che promuova l'innovazione e fornisca occupazione. Inoltre, Chan sottolinea che un'area di cooperazione spesso trascurata è la governance globale: 'la complessità e la portata delle questioni transnazionali richiedono il coinvolgimento del settore privato per una gestione efficace'. La lotta alla disinformazione è un caso emblematico, come spiega Chan:

> tendiamo a pensare alla cooperazione pubblico-privato in termini di collaborazione tra governi e aziende private in merito all'eliminazione di contenuti online. Tuttavia, l'evoluzione delle tecniche di disinformazione richiede nuove modalità di cooperazione. In un articolo che ho scritto con Mariah Thornton di LSE IDEAS, abbiamo analizzato una campagna di disinformazione cinese rivolta a Taiwan e abbiamo osservato che mentre in passato le campagne di disinformazione si affidavano a un'unica piattaforma, come Twitter, per diffondere i contenuti, il nuovo modello utilizza più piattaforme, come YouTube per ospitare i video e Reddit per distribuire i contenuti. Se in passato i governi potevano facilmente collaborare con Twitter per stroncare una campagna di disinformazione, ora la rimozione di un video da YouTube non sarebbe sufficiente, poiché altre parti della catena rimarrebbero intatte. Questo dimostra l'importanza di unire gli sforzi tra le varie piattaforme. Le tecniche di disinformazione sono in continua evoluzione e le nostre strategie di cooperazione pubblico-privato devono evolversi di conseguenza.

La cooperazione pubblico-privato si sviluppa in molteplici modi e Chan identifica quattro meccanismi attraverso i quali il settore privato si impegna con il settore pubblico. In primo luogo, attraverso task force e comitati consultivi congiunti, i rappresentanti di entrambi i settori vengono riuniti per fornire una guida esperta e una direzione strategica per affrontare questioni di interesse reciproco, come nel già citato caso dell'AI Safety Board della US Homeland Security. In secondo luogo, le aziende private e i governi possono gestire congiuntamente 'sandbox normativi', ossia ambienti controllati in cui le aziende innovative possono testare nuovi prodotti, servizi o modelli di business in base a diverse regolamentazioni, consentendo la formazione reciproca di politiche future (come accade, ad esempio, a Singapore). In terzo luogo, le aziende private e i governi si impegnano in consultazioni e comunità di pratica in cui reti di professionisti condividono le conoscenze relative a specifiche aree della tecnologia digitale e forniscono feedback sulle proposte politiche (ad esempio, il Codice di condotta rafforzato sulla disinformazione della Commissione europea del 2022). In quarto luogo, la cooperazione pubblico-privato spesso comporta un trasferimento reciproco di

tecnologia, in base al quale le soluzioni del settore privato vengono utilizzate per rafforzare la fornitura di servizi pubblici (ad esempio, l'uso dell'IA e delle tecnologie biometriche da parte dei governi per la sorveglianza) e le innovazioni del settore pubblico forniscono enormi vantaggi economici grazie al loro potenziale di commercializzazione (ad esempio, i sistemi GPS o internet stessa).

In questo contesto, come sottolinea Chan, una sfida importante è capire se le aziende private possono davvero essere partner paritari quando si tratta di governance digitale globale. Come chiarisce Chan:

> Un'iniziativa come il *Cybersecurity Tech Accord* dimostra chiaramente l'impegno di oltre cento aziende private. Tuttavia, il loro coinvolgimento è limitato. Ad esempio, mentre le aziende private sono state coinvolte nell'Internet Governance Forum delle Nazioni Unite, nel luglio 2022, un importante Stato membro dell'ONU ha bloccato la loro partecipazione all'Assemblea Generale delle Nazioni Unite, adducendo la mancanza di sovranità come motivo di esclusione. Alle aziende private non viene quindi riconosciuto uno status completo, e questo aspetto richiederebbe ulteriori discussioni.

Approfondendo uno degli aspetti della cooperazione pubblico-privata toccati da Chan, **Tin Hinane El-Kadi** si concentra sulla nuova 'Via della seta digitale' cinese, discutendo se stia contribuendo al trasferimento di tecnologia nel Sud globale.

Infatti, se oltre 2.200 anni fa la Via della Seta facilitò la diffusione globale delle invenzioni e delle tecnologie cinesi, oggi le aziende tecnologiche cinesi hanno fatto breccia in modo significativo negli ecosistemi digitali di diversi Paesi 'in via di sviluppo'. Tuttavia, come spiega El-Kadi, 'non è chiaro cosa significhi, concretamente, la presenza di aziende cinesi nel settore delle TIC [tecnologie dell'informazione e della comunicazione] per lo sviluppo dei Paesi a medio reddito che ricevono capitale digitale da parte della Cina'.

Nel 2017, Xi Jinping ha notoriamente affermato che i big data sarebbero stati integrati nella Belt and Road Initiative (BRI) per creare la 'Via della Seta digitale del XXI secolo'. In parole povere, la 'Via della Seta digitale' è un termine che racchiude tutti i progetti digitali delle aziende cinesi del settore ICT. In linea di massima ha tre componenti principali: *infrastrutture digitali* (guidate da aziende come Huawei e ZTE e comprendenti cavi in fibra ottica, infrastrutture di rete e centri dati), *e-commerce* (con aziende come Alibaba, Tencent e JD che stanno facendo notevoli passi avanti, soprattutto nel sud-est asiatico) e *città intelligenti* (con aziende di sorveglianza come Hikvision, Huawei e Alibaba).

Il dibattito dominante sulla Via della Seta digitale si concentra sull'idea che la Cina stia utilizzando le infrastrutture di rete dei Paesi in via di sviluppo a fini di spionaggio e che si stiano delineando due modalità distinte e contrastanti di governance di internet: il modello cinese di 'sovranità di internet' o 'autoritarismo digitale' contro il modello americano di 'libertà di internet'. Tuttavia, sostiene El-Kadi, un problema importante in questo dibattito è la rappresentazione della Cina come un attore monolitico, con il risultato di trascurare i potenziali conflitti tra le imprese digitali cinesi private e lo Stato. Inoltre, c'è l'errata convinzione che la Cina abbia un piano egemonico per imporre il suo modello di governance digitale a tutti i Paesi in via di

sviluppo. Secondo El-Kadi, questo punto di vista trascura il fatto che finora non abbiamo molte prove empiriche della capacità della Cina di imporre il proprio modello e, soprattutto, 'trascura il fatto che la presenza della Cina in molti Paesi in via di sviluppo è in realtà guidata dalla domanda e quindi i dibattiti mainstream tendono a marginalizzare l'iniziativa locale dei Paesi ospitanti e le loro esigenze di sviluppo'. In effetti, diversi studi hanno dimostrato che la Cina adatta il suo approccio ai diversi sistemi politici. Ad esempio, in democrazie come il Kenya e il Ghana, la Cina si è adattata ai loro ecosistemi digitali competitivi e democratici. Al contrario, in contesti più autoritari come Etiopia e Ruanda, la Cina ha risposto alle richieste locali di sorveglianza e censura. Detto in altri termini, il dibattito mainstream sulla Via della Seta digitale cinese:

> è piuttosto eurocentrico e le esigenze di sviluppo dei Paesi in via di sviluppo sono spesso oscurate, soprattutto quando si tratta di superare le disuguaglianze digitali e di recuperare il ritardo in termini di infrastrutture digitali. Oggi, quindi, l'intersezione dinamica tra la Cina e l'aggiornamento tecnologico rimane tutt'altro che chiara e richiede ulteriori indagini: i giganti tecnologici cinesi creano nuove opportunità per il trasferimento tecnologico, l'apprendimento e l'innovazione o, al contrario, ostacolano la creazione di capacità tecnologiche nei paesi ospitanti a medio reddito?

Per rispondere a questa domanda, El-Kadi ha concentrato la sua ricerca sul Nord Africa – una regione chiave per la cooperazione digitale – e più in particolare su Algeria ed Egitto.

Il 13° Piano quinquennale pubblicato dal Comitato centrale del Partito Comunista Cinese (2016, p. 71) sottolinea l'intenzione di 'sviluppare una Via della Seta online con i Paesi arabi e altri'. Il cavo PEACE (Pakistan East Africa Cable Express), che collega la Cina al Pakistan e si estende fino a Marsiglia, nel sud della Francia, attraverso l'Africa orientale e settentrionale, incarna questa strategia e qualifica il Nord Africa come un'area prioritaria per gli investimenti digitali cinesi. Huawei e ZTE hanno conquistato mercati importanti nella regione, costruendo reti 4G/5G e data center e fornendo servizi di IA e *cloud computing*. In particolare, Huawei ha aperto una fabbrica ad Algeri per la produzione di smartphone e numerosi centri dati sono in costruzione in Egitto e Marocco.

Ispirandosi al lavoro di Albert Hirschman, El-Kadi ha identificato e tracciato i due principali canali di ricaduta tecnologica nel settore ICT algerino ed egiziano. In breve, le ricadute verticali si verificano tra le multinazionali del digitale (come Huawei) e i subappaltatori, i fornitori e gli operatori di telecomunicazioni locali. Le ricadute orizzontali, invece, avvengono principalmente attraverso la mobilità del lavoro: ad esempio, un ingegnere ICT che lavora per Huawei potrebbe trasferirsi in un'azienda locale, dando luogo a ricadute di conoscenza, in particolare per quanto riguarda le conoscenze manageriali e tecniche. 'La mia ricerca', spiega El-Kadi, 'mirava a valutare non solo se il trasferimento di tecnologia e conoscenza si è verificato, ma anche quale tipo di tecnologia e conoscenza è stata trasferita e se ciò ha contribuito all'aggiornamento tecnologico in Algeria e in Egitto'.

Per quanto riguarda le ricadute orizzontali, El-Kadi ha riscontrato un alto livello di localizzazione della manodopera in Nord Africa, principalmente a causa del

crescente costo del lavoro in Cina, e risultati simili sono stati riportati da altri studiosi in altre regioni dell'Africa, dell'America Latina e del Sud-est asiatico. 'La localizzazione della manodopera è un passo positivo verso il trasferimento delle conoscenze', afferma El-Kadi; 'tuttavia, i risultati della ricerca sul campo suggeriscono l'esistenza di un soffitto di vetro per i dipendenti locali, con posizioni manageriali di alto livello occupate da cittadini cinesi'. Nel complesso, le prove di ricaduta orizzontale sono limitate perché la maggior parte dei dipendenti algerini ed egiziani delle multinazionali ICT si sposta tra le diverse multinazionali piuttosto che verso le imprese locali: 'I dipendenti che lavorano per Huawei, ad esempio, spesso passano a concorrenti come Nokia, Ericsson o Cisco all'interno del proprio Paese, oppure si trasferiscono all'estero. Questa tendenza limita il potenziale di trasferimento delle conoscenze alle imprese locali'.

Per quanto riguarda le ricadute verticali, continua El-Kadi, 'i fornitori e i subappaltatori intervistati hanno indicato che Huawei e ZTE hanno fornito loro formazione, come spesso accade nel settore dell'alta tecnologia'. Eppure, il trasferimento di tecnologia

> è stato limitato, anche in attività che ci si aspettava fossero ad alta intensità di ricaduta, come la produzione: le interviste con i dipendenti dello stabilimento Huawei di Algeri hanno rivelato una minima aggiunta di valore locale nella produzione di telefoni cellulari, in quanto la maggior parte dei componenti, compresi quelli a bassa tecnologia come le cabine telefoniche, sono stati importati dalla Cina. E questo, ovviamente, limita il trasferimento tecnologico.

Allo stesso modo, la formazione fornita alle imprese locali non sembra aver trasmesso nuove conoscenze che potrebbero favorire l'aggiornamento tecnologico locale. La formazione sembra invece agire come meccanismo socio-tecnico a sostegno del consumo di tecnologie cinesi e della creazione di ecosistemi di imprese locali identificabili in grado di installare, risolvere i problemi e manutenere le apparecchiature ZTE e Huawei. La situazione in termini di collegamenti con le università locali è simile:

> Huawei è più attiva di altre aziende nel fornire formazione agli studenti universitari in Egitto e Algeria. Sebbene siano state siglate molte partnership di alto livello per offrire formazione agli studenti, i contenuti si sono concentrati principalmente sulla risoluzione dei problemi e sulla manutenzione delle tecnologie Huawei, piuttosto che sull'impartizione di conoscenze all'avanguardia che potrebbero consentire l'aggiornamento tecnologico locale.

In sintesi, la ricerca di El-Kadi dimostra che la presenza digitale della Cina in Nordafrica è guidata principalmente dalla domanda e che le agenzie locali contano nel determinare le ricadute delle imprese cinesi nei Paesi ospitanti, in quanto il modo in cui la Cina modella gli ecosistemi digitali dipende dalle preferenze politiche, economiche e culturali locali. Allo stesso tempo, i legami tra le imprese cinesi e le economie algerina ed egiziana stanno riconfigurando gli ecosistemi intorno all'uso di tecnologie e standard cinesi. Pertanto, conclude El-Kadi, 'c'è un urgente bisogno di politiche più proattive da parte dei governi ospitanti, perché altrimenti la Via della Seta digitale rischia di creare nuove dipendenze tecnologiche, bloccando gli attori locali delle ICT in attività e relazioni definite dai giganti digitali cinesi'.

PRESENTAZIONE

La sovranità e le tre ecologie digitali in un’epoca di geopolitica

Il documento presentato è tratto da un capitolo del libro di prossima pubblicazione *In Search of a Unicorn? The Misplaced Aspirations of Strategic Autonomy in EU International Relations*, di cui Richard Higgott è autore insieme a Simon Reich (2025).

Per dare il via alla seconda giornata del simposio, **Richard Higgott** riflette sui modi in cui la digitalizzazione ha cambiato il significato di sovranità statale. In effetti, 'l'idea stessa di sovranità è un'educata finzione in tempi di globalizzazione e digitalizzazione', sostiene Higgott. Oggi 'molti Stati confondono la sovranità con la resilienza e la loro lotta per l'autonomia politica' e con 'la *geopolitica* che diventa la parola d'ordine ideologica di un ordine mondiale sempre più biforcato (non bipolare), il mito della sovranità è cresciuto di nuovo'. Il risultato, continua Higgott, è che 'l'illusione della sovranità rimane un fattore determinante nell'organizzazione della vita sociale e politica degli Stati, sia grandi che piccoli', e l'attuale discorso sulla sovranità riflette 'l'aspirazione degli Stati a controllare e imbrigliare il proprio settore tecnologico'.

Le ipotesi classiche sulla sovranità non sono più plausibili, se mai lo sono state. In effetti, come sostiene Stephen Krasner, la sovranità non è mai stata illimitata, indivisa e irreprensibile (*unaccountable*). 'La sovranità non è assoluta. È fungibile', aggiunge Higgott:

> è piuttosto un processo di contrattazione in un contesto internazionale sempre più ibrido, connesso e digitalizzato – e le reti, a differenza delle tradizionali gerarchie istituzionali, incoraggiano l'auto-organizzazione. Se usate in modo responsabile, l'apertura e la trasparenza di internet potrebbero essere una forza per il bene. Ma abbiamo visto nei panel precedenti come le speranze di democratizzazione dei primi 'Utopisti digitali' siano state messe in discussione dalle tecnologie digitali che sono diventate agenti di intrusione, controllo, repressione e autoritarismo.

Spinte dalla monetizzazione dei dati comportamentali, le tecnologie digitali gettano un'ombra su ciò che significa essere liberi e uguali in un'epoca in cui sia gli attori privati che gli Stati hanno maggiori strumenti di controllo. La digitalizzazione estende la sfera politica attraverso confini e domini, favorendo il desiderio degli Stati di rafforzare la sovranità *nazionale* attraverso l'autonomia tecnologica piuttosto che attraverso una maggiore interdipendenza.

Come spiega Higgott, il rapporto tra digitalizzazione e Stati sovrani può essere pensato come caratterizzato da gerarchia e ibridazione. Gerarchicamente, ci sono tre gruppi: 1) le "superpotenze" digitali (ossia Stati Uniti e Cina), 2) le aspiranti grandi potenze, in particolare l'Europa e, in misura minore, la Russia e l'India, e 3) tutti quegli Stati dipendenti che potrebbero essere definiti 'acquirenti di tecnologia'. Per quanto riguarda l'ibridazione, la vediamo nella crescente influenza di attori non statali – alcuni dei quali presentano proprietà simili a quelle di uno Stato – che hanno guidato la digitalizzazione, in particolare i 'titani della tecnologia' come Google, Apple, Facebook, Amazon e Microsoft negli Stati Uniti e Tencent, Huawei, Baidu, Alibaba e Weibo in Cina. In tale contesto:

> la battaglia per assicurarsi l'ascendente non è più solo tra Stati sovrani che competono in uno spettro che va dalla diplomazia alla guerra. Piuttosto, i principali Stati stanno ora sfruttando potenti piattaforme tecnologiche sviluppate privatamente per rafforzare la retorica e la pratica del nazionalismo nella battaglia per affermare la propria sovranità, il potere interno e l'influenza in politica estera.

La digitalizzazione è un fenomeno globale, ma non è un processo uniforme. Higgott individua piuttosto tre visioni concorrenti della digitalizzazione, o tre *ecologie digitali*: quella americana, quella cinese e quella europea. 'Le attuali tensioni sulla progettazione, la governance e la giurisdizione di queste tre ecologie digitali riflettono e sono il riflesso di più ampie fratture globali', sottolinea Higgott: gli Stati Uniti e la Cina stanno creando due sistemi tecnologici e digitali ben definiti. Il modello americano è guidato principalmente dal settore privato e si basa molto sugli investimenti privati, mentre il modello cinese è guidato dallo Stato e quindi dipende dagli investimenti pubblici. Entrambe le ecologie includono lo sviluppo dell'IA, dei big data, del 5G e degli strumenti di guerra informatica nel contesto della loro corsa all'egemonia tecnologica e digitale, che è al centro della più ampia competizione strategica tra i due Paesi. L'ambizione della Cina va oltre il semplice desiderio autoritario di avere un regime digitale indipendente all'interno del suo Great Firewall: 'supportata da Russia e Iran, la Cina è intenzionata a riscrivere le regole della governance di internet. Pechino vuole che la rete sia nelle mani dei governi senza una supervisione globale, e non un regime di controllo normativo globale'. Al contrario, e non è una sorpresa, l'ecologia statunitense riflette un approccio più laissez-faire, in cui internet è informalmente di proprietà delle aziende americane e da queste ampiamente regolamentata. 'Il problema', tuttavia, 'è che le divisioni politiche interne negli Stati Uniti impediscono una politica coerente e bipartisan nello sviluppo di una regolamentazione cooperativa dei mercati e della protezione dei dati'. Inoltre, a livello normativo, sembra che Washington non abbia una coalizione di alleati che condividano la sua visione di internet e quindi 'l'idea dei primi "Utopisti digitali" che la concorrenza tra attori privati sarebbe stata attraente per gli Stati in quando avrebbe contribuito all'apertura, la trasparenza, la sicurezza (e in teoria la democrazia) si è rivelata sbagliata'. E questo, aggiunge Higgott, solleva una questione importante: 'Una concezione liberale di internet globale è forse un'idea troppo remota in un contesto in cui accelerano le tendenze centrifughe verso la frammentazione mentre i dati diventano sempre più centrali per la sicurezza economica e nazionale e come fonte di potere geopolitico?'

L'UE, da parte sua:

> sta cercando di costruire una terza ecologia digitale: in parte guidata dal mercato, con sforzi normativi statali per contenere il potere degli attori privati di internet e prevenire la frammentazione nazionale del processo decisionale tra i suoi Stati membri. Per molti versi, l'UE ha una visione più complessa e forse più sofisticata del ruolo dei mercati rispetto alle due 'superpotenze' digitali: l'UE non vuole che internet e i relativi strumenti di comunicazione sociale operino secondo lo stile tecno-libertario degli Stati Uniti o il rigido autoritarismo della Cina.

Secondo Higgott, invece, l'UE vuole un 'modello normativo', che per Higgott è un eufemismo per indicare il potere di influenzare (*ideational power*) l'ambiente digitale internazionale per compensare la mancanza di quote di mercato dell'UE. La domanda per l'Europa è quindi la seguente: 'in che misura gli approcci concorrenti degli Stati Uniti (poco regolamentati) e della Cina (troppo regolamentati) offrono all'UE uno spazio per sviluppare la sua influenza e ridurre la sua dipendenza?' In sintesi, l'approccio normativo e dirigista dell'UE, incarnato dal GDPR, riflette la sua aspirazione a fare della sovranità digitale un elemento essenziale della sua

autonomia strategica, come sottolineato anche dalle parole del Presidente Macron: 'la battaglia che stiamo combattendo è una battaglia di sovranità... Se non costruiamo i nostri campioni in tutti i settori – digitale, intelligenza artificiale – le nostre scelte saranno dettate da altri'.

In definitiva, ciò che distingue ciascuna delle tre ecologie digitali identificate da Higgott è il ruolo della sovranità e la questione di quale sovranità sia minacciata o rafforzata:

> È in gioco la sovranità tradizionale, cioè il controllo autonomo dello Stato? È l'indipendenza dei nuovi giganti digitali del settore privato che Zuckerberg ha paragonato agli Stati? O è la 'sovranità individuale' di cittadini sempre più emarginati?

Esistono chiaramente tensioni tra le tre ecologie digitali, in particolare tra quelle delle due superpotenze digitali e dell'UE. Nella ricerca del 'controllo sovrano' di Macron nel settore della politica digitale, l'UE sta operando con un certo grado di innovazione intellettuale rispetto alle due superpotenze. La strategia e le politiche dell'UE non sono state prive di un certo successo, ma non si sa fino a che punto riusciranno ad arginare la frammentazione globale nel lungo periodo. Gli Stati Uniti hanno mostrato alcuni segnali di voler venire incontro all'UE su alcune leggi in materia di privacy e governance dei dati. 'Ma non è chiaro se la volontà politica o la capacità di garantire il cambiamento siano sufficienti a Washington', commenta Higgott, 'e se non accadrà sotto un'amministrazione democratica, non accadrà certamente sotto una repubblicana'. D'altra parte, come si addice a uno Stato autoritario, la Cina non mostra alcun desiderio di attuare accordi sulla privacy e leggi sulla protezione dei dati che indebolirebbero il controllo statale sul dominio digitale. Allo stesso tempo, è chiaro che il sistema di Westfalia non costituisce più un ordine internazionale liberale. Come sottolinea Higgott:

> il mito della resilienza e dell'universalismo non è più sostenibile. L'idea di un ordine guidato dagli Stati Uniti che agisce come propagatore degli universalismi occidentali è ora apertamente in tensione con un ordine basato su attività territoriali guidate dagli Stati, che enfatizzano la sovranità bilaterale, i confini e le identità di gruppo invece delle agende istituzionali multilaterali dell'ultima parte del XX secolo.

PANEL 4

Voci emergenti nel dominio digitale

Prendendo spunto dalla gamma di argomenti discussi nei primi tre panel tematici, tre ricercatrici e un ricercatore all'inizio della loro carriera accademica discutono alcuni aspetti dei loro lavori in corso nell'ambito della governance digitale. La prima relatrice di quest'ultimo panel è **Stella Blumfelde**, che condivide alcuni dei risultati della sua ricerca di dottorato, offrendo nuovi spunti di riflessione sulla governance della cybersicurezza. Come spiega lei stessa:

> l'attuale quadro di riferimento per la governance della cybersicurezza abbraccia diversi regimi internazionali e coinvolge più meccanismi di sicurezza. I progressi nella creazione di un quadro internazionale solido per governare le insicurezze informatiche sono ostacolati da posizioni e interessi incoerenti e talvolta contrastanti tra Stati e tra Stati e attori non statali. Ciò impedisce una cooperazione efficace.

Tuttavia, sottolinea Blumfelde, 'con il mutare del carattere delle minacce internazionali, i singoli Stati non possono più garantire da soli una sicurezza adeguata'. Di conseguenza, le organizzazioni internazionali sono emerse come attori di primo piano nel mantenimento della pace e della sicurezza: 'Le organizzazioni internazionali possiedono le risorse economiche e umane, nonché le competenze e le capacità tecniche per influenzare i modi in cui le società e gli Stati articolano e affrontano le preoccupazioni condivise su questioni globali, come la sicurezza informatica'.

Al di là del campo della cybersecurity, la governance della sicurezza internazionale si è storicamente sviluppata in un insieme di meccanismi o 'strumenti', tutti incarnati e istituzionalizzati in organizzazioni internazionali come le Nazioni Unite. Inizialmente, questi includevano incontri periodici per scoraggiare le aggressioni e la diplomazia preventiva per risolvere pacificamente le controversie, seguiti dall'istituzione di sanzioni, azioni di sicurezza collettiva, operazioni di pace e sforzi di disarmo. Oggi, sottolinea Blumfelde, 'invece di affrontare i problemi di sicurezza una volta che si manifestano, gli approcci ancorati al concetto di resilienza si concentrano sul dotare i Paesi delle competenze e delle soluzioni necessarie per comprendere, affrontare e gestire le minacce alla sicurezza'. Il quadro della resilienza, spiega Blumfelde, è stato applicato a un'ampia gamma di questioni, dai conflitti alla povertà e alle problematiche ambientali. Oggi è sempre più applicato anche alla sicurezza informatica.

In questo contesto, le Nazioni Unite hanno sottolineato l'importanza delle organizzazioni regionali nel costruire la resilienza degli Stati alle minacce cibernetiche e nel rafforzare la loro cybersicurezza più in generale. Il modo in cui lo fanno è al centro delle ricerche di Blumfelde:

> Per valutare il ruolo delle organizzazioni regionali come fornitori di sicurezza nel campo della cybersecurity, ho sviluppato il mio quadro analitico partendo dalla percezione che tali organizzazioni agiscono come attori complementari alle Nazioni Unite nella governance della sicurezza. In quest'ottica, per comprendere il ruolo e la complementarietà delle organizzazioni regionali, il mio obiettivo è quello di confrontare come gli strumenti di governance della cybersecurity differiscano tra le Nazioni Unite e le organizzazioni regionali.

Le Nazioni Unite hanno sviluppato un'ampia gamma di strumenti per affrontare i conflitti internazionali. Nel contesto della sicurezza informatica, l'ONU impiega meccanismi di rafforzamento della fiducia che includono 'l'identificazione di punti di contatto governativi o di esperti di sicurezza informatica per facilitare lo scambio di informazioni e di migliori pratiche, tra cui la condivisione di opinioni nazionali su misure politiche, legislative e normative per proteggere le infrastrutture critiche'. Sebbene gli sforzi dell'ONU in materia siano stati limitati, essa impiega strumenti di sviluppo delle capacità (*capacity-building mechanisms*) per i suoi Stati membri, che sono fondamentali nel campo della sicurezza informatica. Queste misure includono, ad esempio, la formazione delle agenzie nazionali competenti per affrontare gli incidenti legati alla sicurezza delle ICT e la fornitura di supporto legale o diplomatico per mitigare le minacce alla sicurezza informatica. Infine, l'ONU è tradizionalmente una piattaforma che incoraggia e facilita la cooperazione tra più soggetti e questo vale anche per i suoi sforzi nella governance della cibersicurezza attraverso piattaforme come il Gruppo di esperti governativi dell'ONU (UN GGE) e il Gruppo di lavoro aperto dell'ONU (OEWG).

Sulla base di queste osservazioni, Blumfelde ha concentrato la sua ricerca empirica su cinque organizzazioni regionali: l'Organizzazione degli Stati Americani (OAS), l'Unione Africana (UA), l'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE), l'Associazione delle Nazioni del Sud-Est Asiatico (ASEAN) e l'Organizzazione per la Cooperazione di Shanghai (SCO). Come mostrato nella tabella seguente, queste organizzazioni applicano in gran parte gli stessi meccanismi di sicurezza delle Nazioni Unite. Tuttavia, lo fanno 'con alcune peculiarità', come sottolinea Blumfelde: 'evidenziate in rosso [nella ***Tabella 1***], sono

ORGANIZZAZIONE / STRUMENTI DI GOVERNANCE	OAS	UA	OSCE	ASEAN	SCO
Meccanismi di rafforzamento della fiducia	X	X	X	X	X
Meccanismi di sviluppo delle capacità	X	X	X	X	X
Cooperazione tra più soggetti	X	X	X	X	X
Misure tecniche	X				
Misure legali		X			

Tabella 1
Governance regionale della cybersecurity

le misure che ho identificato come l'obiettivo principale della governance regionale della cybersecurity. Inoltre, considerando che l'UA ha istituito la Convenzione sulla sicurezza informatica e la protezione dei dati personali, ciò sottolinea il fatto che le organizzazioni regionali non solo sono complementari agli sforzi delle Nazioni Unite in materia di governance della sicurezza informatica, ma sono attori molto attivi nell'assistenza e nello sviluppo di una comprensione comune su questi temi a livello regionale'.

Secondo Blumfelde, queste differenze possono essere spiegate da una serie di fattori già identificati nella letteratura accademica nell'ambito delle relazioni internazionali, tra cui i divari tecnologici tra le regioni e all'interno delle stesse, nonché le differenze nelle capacità di cybersicurezza nelle loro dimensioni legali, tecniche, organizzative, di sviluppo e di cooperazione. Inoltre, esistono diverse percezioni su cosa rappresenti effettivamente una minaccia alla sicurezza informatica, il che è strettamente correlato all'esistenza di diverse 'culture della sicurezza' e ai vari interessi nazionali, con alcuni Paesi che danno priorità alla crescita economica rispetto a rigide normative sulla privacy dei dati.

Da questa analisi comparativa preliminare e da una serie di interviste con alcuni *policymaker*, si evince che 'la governance internazionale della cybersecurity dovrebbe concentrarsi meno sul livello globale – come invece sta accadendo ora – e più sul ruolo delle organizzazioni regionali all'interno di questi processi, per via della loro vicinanza geografica, culturale e storica a regioni specifiche'.

Un'altra conclusione che Blumfelde trae dalla sua ricerca empirica è che 'le organizzazioni regionali dovrebbero impegnarsi a definire cosa sia la cybersicurezza, perché i disallineamenti concettuali potrebbero essere una delle ragioni per cui i meccanismi di governance regionale divergono'. Inoltre, osserva Blumfelde, mentre le misure di cybersecurity esistenti sono spesso etichettate come 'meccanismi *strategici*', 'non comprendono appieno la natura multiforme della cybersecurity, che ha anche dimensioni legate ai conflitti internazionali, ai diritti umani, allo sviluppo, ecc.' e quindi difficilmente sono all'altezza di ciò che un quadro di resilienza comporterebbe.

Riallacciandosi al più ampio dibattito sull'autoritarismo digitale, **Lorraine Charbonnier** delinea i contorni concettuali del suo progetto di ricerca sulle '*pratiche* autoritarie digitali' ed esplora nuovi possibili percorsi attraverso i quali interrogare il rapporto tra tecnologie digitali e resilienza autoritaria.

Le preoccupazioni per l'ascesa dell'autoritarismo digitale sono in aumento. Eppure il concetto stesso di 'autoritarismo digitale' non è stato definito con chiarezza. 'Questo non sorprende', afferma Charbonnier, 'poiché le discussioni in corso sull'autoritarismo digitale rispecchiano alcune delle carenze concettuali della letteratura sull'autoritarismo in generale'. In effetti, l'autoritarismo è tipicamente discusso come l'opposto della democrazia o come una categoria residuale di 'non-democrazia' e, quando se ne discute la controparte digitale, 'invece di concentrarsi sul fenomeno in sé, la tendenza è quella di guardare a ciò che fanno gli attori autoritari, spesso inquadrando la questione come una lotta tra democrazie e autocrazie'. Di conseguenza, secondo Charbonnier, la maggior parte dei dibattiti in corso opera attraverso una concettualizzazione limitata dell'autoritarismo digitale, che porta con sé alcuni dei punti ciechi per i quali la ricerca sull'autoritarismo è già stata criticata e che appare particolarmente rilevante una volta trasposta nel regno digitale. In primo luogo, è ampiamente riconosciuto che, sebbene tutti i regimi autoritari siano non democratici, ciascuno di essi lo è a modo suo, cioè 'i regimi autoritari possono essere autoritari per ragioni molto diverse e in contesti molto diversi'. E questo probabilmente varrà anche per il mondo digitale'. In secondo luogo, l'idea che l'assenza di elezioni 'libere ed eque' rappresentino la soglia chiave per definire l'autoritarismo – di per sé problematica – non può essere trasposta al mondo digitale:

> non solo non esistono elezioni 'digitali', ma se cercassimo di analizzare l'autoritarismo digitale attraverso la lente delle elezioni rischieremmo di imporre una visione stato-centrica in un ambiente in cui gli Stati possono essere o meno gli attori principali, come abbiamo visto nei panel precedenti.

Anche la tendenza a personalizzare i regimi è problematica: 'dovremmo riconsiderare il nostro fascino per gli 'uomini forti', perché se già nel mondo analogico ci porta a conclusioni piuttosto riduttive, le complessità del mondo digitale rendono in gran parte insostenibile un'attenzione ristretta agli individui'. Ad esempio, le rivelazioni di Snowden hanno indicato che la US National Security Agency stava raccogliendo una grande quantità di dati su cittadini non statunitensi in tutto il mondo:

> sebbene questo non faccia degli Stati Uniti un regime autoritario, sicuramente può essere interpretato come un comportamento autoritario e, cosa più importante per il punto che sto cercando di fare, ha ben poco a che fare con gli individui: la sorveglianza è iniziata sotto l'amministrazione Bush ed è continuata fino a quella di Obama senza alcun ordine esplicito; persino il Congresso era in gran parte all'oscuro di ciò che stava accadendo, e anche altri governi erano coinvolti. Nei fatti, sono state coinvolte centinaia di persone. Non è stata opera né di individui specifici né di un particolare regime, ma piuttosto di una configurazione (transnazionale) di attori, e ciò potrebbe anche essere legato a quelle forze sottili e inespresse che Kaspersen ha identificato come *doxa* nel suo discorso di apertura.

Tenendo conto di queste osservazioni, Charbonnier suggerisce di 'spostare lo sguardo analitico, almeno momentaneamente, da "chi fa cosa" a "cosa viene fatto" e, solo successivamente, "da chi"'. In altre parole, Charbonnier propone di concentrarsi sulle "*pratiche* autoritarie digitali", abbozzandone una definizione: 'Modelli di azioni, inseriti in un contesto socialmente organizzato e basati sulle

SORVEGLIANZA	CENSURA + PERSECUZIONE MIRATA	SHUTDOWN	MANIPOLAZIONE SOCIALE E DISINFORMAZIONE
Sorveglianza passiva (ad es. intercettazione di telefoni cellulari) **Sorveglianza mirata** (ad es. spyware) **IA e sorveglianza dei big data** (ad es. sistemi di riconoscimento facciale) --- ***Leggi e regolamenti sulla sorveglianza*** *(ad es., sulla divulgazione, conservazione e localizzazione dei dati)*	**Censura basata sulla paura e 'rappresaglia per l'espressione digitale'** (ad esempio minacce e rischi di accuse legali, detenzione, violenza) **Censura basata sull'attrito** (ad es. blocco e filtraggio dei contenuti) **Limitazione dell'infrastruttura** (ad es. firewall) --- ***Leggi e regolamenti sulla censura*** *(ad es. su fake news, lèse majesté, sedizione, indecenza)*	**Shutdown totale di internet** (nazionale, subnazionale) **Shutdown parziale di internet** (ad es. siti web limitati, app bloccate) --- ***Leggi e regolamenti sull'impiego di shutdown***	**Propaganda** **Disinformazione** **Hate speech** **Trolling e molestie** per provocare o interrompere le conversazioni **Doxing** per intimidire **Flooding** per creare confusione e sopraffare le fonti di informazione legittime **Metodi automatizzati** (ad es. bot e algoritmi che creano picchi di coinvolgimento) **Vandalismo o defacement (**cioè atti non autorizzati per modificare o oscurare siti web o account)

Tabella 2
Pratiche autoritarie digitali

tecnologie digitali, che vengono messi in atto per sabotare la responsabilità disabilitando la voce delle persone e il loro accesso alle informazioni attraverso la sorveglianza, il controllo e la cooptazione/manipolazione".

"Esistono ovviamente diversi strumenti e tecniche che possono dare vita a pratiche autoritarie digitali, molti dei quali sono già stati discussi dai relatori precedenti', commenta Charbonnier presentando una tassonomia preliminare e non esaustiva (cfr. Tabella 2). "Ciò che le diverse categorie di pratiche hanno in comune', continua l'autrice, 'è che tutte rappresentano "tecnologie di governo" nel senso più ampio e del termine, *à la Foucault*: tutte intendono "condurre la condotta" delle persone e delle società'.

Le diverse pratiche hanno scopi diversi, si basano su logiche diverse, si affidano a tecnologie digitali diverse e seguono tempi diversi: alcune tecniche, come gli shutdown, hanno un impatto immediato, ma più durano, meno sono efficaci. Altre tecniche, come le operazioni di disinformazione, richiedono tempi più lunghi per ottenere il massimo effetto. 'Ogni serie di azioni comporta benefici e costi propri, che determinano le decisioni su quale combinazione di pratiche viene messa in atto da chi e quando', sottolinea Charbonnier, aggiungendo che 'non tutti gli attori possono fare tutto: le scelte sono determinate dalle proprie capacità, comprese, ma non solo, le capacità digitali'. Ad esempio, una recente ricerca ha dimostrato che le pratiche di disinformazione e manipolazione sociale sono meno efficaci nei regimi a bassa legittimità, 'un'intuizione interessante se consideriamo quanto diversi possano essere i livelli di legittimità anche all'interno di una stessa categoria di regimi e alla luce dei timori di un regresso democratico a livello globale'. Ulteriori considerazioni riguardano il cosiddetto 'dilemma digitale del dittatore', in base al quale i regimi autoritari devono trovare un equilibrio tra la loro presa sulla società e i costi economici e politici del mantenimento di tale controllo in un mondo interconnesso e digitalizzato. Allo stesso modo, riflette Charbonnier, 'i regimi formalmente più democratici possono considerare attraente il controllo sociale consentito dalle tecnologie (più discrete) e quindi potrebbero anche avere la tentazione di cercare vie d'uscita alternative ai loro dilemmi digitali'.

Infatti, mentre studi recenti hanno confermato che i regimi autoritari hanno maggiori probabilità di mettere in atto pratiche autoritarie digitali perché devono affrontare meno vincoli politici, le osservazioni empiriche offrono un quadro più sfumato. La sorveglianza, ad esempio, è più diffusa nei regimi autoritari chiusi e ricchi. Eppure:

> quando si tratta di sorveglianza dei big data e impiego dell'IA, anche le democrazie sono piuttosto attive: la sorveglianza passiva e quella mirata offrono vantaggi tangibili in termini di controllo, ma le democrazie devono affrontare notevoli vincoli politici per mettere in atto tali pratiche. Tuttavia, la disponibilità di tecniche più discrete può alterare questa dinamica.

Un'altra importante intuizione derivante da questo corpus di studi è che molti Stati, soprattutto quelli che si collocano nello spettro autoritario, si impegnano in pratiche autoritarie digitali più di quanto le loro capacità lascerebbero intendere. Ciò significa che spesso si affidano a sostegni e fornitori esterni, il che 'evidenzia ancora una volta il ruolo cruciale svolto dalle imprese private, che potrebbero essere viste come parte attiva di configurazioni di attori autoritari, indipendentemente dal fatto che le

imprese dichiarino o meno di essere coinvolte nella politica. Va poi notato che molte di queste aziende hanno sede in paesi democratici'. Forse ancora più interessante, tra le discussioni in corso sul fatto che le tecnologie digitali rafforzino l'autoritarismo o sostituiscano l'autoritarismo tradizionale, 'recenti ricerche sembrano suggerire che mentre le tecnologie digitali rafforzano le pratiche autoritarie di lunga data in regimi chiusi e altamente repressivi, tali tecnologie tendono a essere più vantaggiose come sostituti nei regimi ibridi'. Da questa constatazione empirica possono scaturire molti spunti di riflessione. Per prima cosa:

> potremmo renderci conto che le pratiche autoritarie digitali potrebbero paradossalmente ridurre la necessità, per gli attori autoritari, di mettere in atto pratiche più palesi, come truccare le elezioni, o spietate, come impegnarsi direttamente nella repressione, rendendo la violenza intrinseca dei regimi autoritari meno visibile nel mondo non digitale.

Quindi, conclude Charbonnier, il punto chiave:

> è che esaminare come e perché diversi attori combinano varie pratiche autoritarie digitali può far luce su ciò che chiamiamo vagamente 'autoritarismo digitale' e questo, a sua volta, può aiutarci a concepire strategie migliori per prevenire, mitigare e contrastare pratiche dannose, indipendentemente da chi e da quale regime le mette in atto.

Approfondendo un tipo specifico di pratiche rese possibili dalle tecnologie digitali, **Alessandra Russo** esplora alcune delle implicazioni dell'uso di tecnologie emergenti e rivoluzionarie (*emerging disruptive technologies*) in contesti bellici, discutendo di come la 'guerra algoritmica' potrebbe avere effetti dannosi sulla democrazia. Come spiega Russo, alla base della sua ricerca vi è il riconoscimento che queste tecnologie – e in particolare l'IA – stanno guadagnando terreno e sono sempre più utilizzate dagli Stati sia per garantire il controllo all'interno dei propri confini che per condurre guerre. 'L'IA si distingue', spiega Russo, 'perché trascende i paradigmi tecnologici convenzionali grazie alla sua vasta gamma di applicazioni militari e non, che la rendono una tecnologia di uso generale simile al motore a vapore e all'elettricità'. La ricerca di Russo mira a esplorare le questioni alla base dell'impiego dell'IA militare da parte degli Stati democratici, cercando di svelarne le implicazioni e il rapporto tra democrazia e uso di tecnologie avanzate nei conflitti.

Infatti, come sostiene Russo, 'l'IA ha il potenziale per consentire una condotta di guerra più indiscriminata, anche da parte dei Paesi democratici'. Ciò è dovuto a una serie di fattori di rischio intrinseci all'IA e ai suoi utenti. Il primo e il più importante sono i pregiudizi algoritmici (*algorithmic bias*) derivanti da difetti nei dati di addestramento dell'IA e nella progettazione degli algoritmi stessi, che possono generare risultati non ottimali o sbagliati e che, senza un'adeguata verifica, possono portare a gravi errori nel processo decisionale e nell'azione. In secondo luogo, e in modo correlato, ci sono i pregiudizi umani, in particolare il cosiddetto 'pregiudizio dell'automazione' (*automation bias*): la ricerca nel settore dell'aviazione civile ha dimostrato che in situazioni sensibili dal punto di vista temporale e cognitivo gli esseri umani tendono ad affidarsi eccessivamente ai risultati proposti dai sistemi di IA senza un'adeguata valutazione critica. Un altro fattore di rischio deriva dal fatto che i sistemi di IA esistenti non comprendono il contesto e non sono in grado di fare

considerazioni etiche: un sistema di IA potrebbe dare priorità a obiettivi come la minimizzazione delle vittime oppure il raggiungimento di obiettivi tattici senza comprendere appieno la complessità della situazione e senza considerare le conseguenze più ampie delle sue azioni. Infine, l'uso dell'IA per compiti sensibili come il targeting militare potrebbe ridurre il coinvolgimento diretto degli operatori umani nei processi decisionali, portando a una minore responsabilizzazione (*accountability*) e a un distacco dalle conseguenze della guerra, che a sua volta potrebbe potenzialmente rendere più facili o più probabili le azioni indiscriminate. Come spiega Russo:

> se teniamo conto di questi fattori di rischio, l'impiego di sistemi di IA in guerra potrebbe dar luogo a tre diversi fenomeni: 1) minore controllo sui risultati dell'IA e 2) maggiore velocità di decisione (che è il principale vantaggio offerto dall'IA), che insieme portano a 3) maggiore errore e tolleranza per i danni collaterali.

Per dimostrare come ciò avvenga, Russo concentra la sua analisi sui sistemi di riconoscimento automatico dei bersagli (ATR), sottolineando che 'mentre le narrazioni mainstream e i dibattiti pubblici si concentrano spesso sui sistemi di armi autonome letali, l'ATR è attualmente l'applicazione dell'IA che sta trovando il più ampio utilizzo in ambito militare e che potrebbe avere le conseguenze più significative'. In parole povere, l'ATR si riferisce all'uso dell'elaborazione informatica per rilevare e identificare automaticamente gli obiettivi. Questi sistemi utilizzano i dati raccolti dai sensori – in genere immagini – e la fusione dei dati (*data fusion*) per sfruttare le informazioni geografiche, i dati di navigazione, i geotag, le informazioni raccolte su internet, le posizioni sospette dei bersagli e i tipi di bersagli. Attraverso l'analisi statistica, l'ATR genera un elenco di obiettivi – tra cui persone, edifici e aree geografiche – e li classifica in base all'importanza tattica o operativa. Alcuni dei sistemi ATR più famosi sono il *Project Maven*, sviluppato dagli Stati Uniti, e i due sistemi software israeliani *Gospel* e *Lavender*, attualmente utilizzati dalle Forze di Difesa Israeliane (IDF) nella Striscia di Gaza. Ognuno di questi sistemi opera con una struttura 'human in the loop', il che significa che non sono utilizzati come sistemi completamente autonomi (si veda ***Immagine 7***). Tuttavia, vi sono differenze significative nel modo in cui questi software vengono utilizzati dagli Stati Uniti e da Israele.

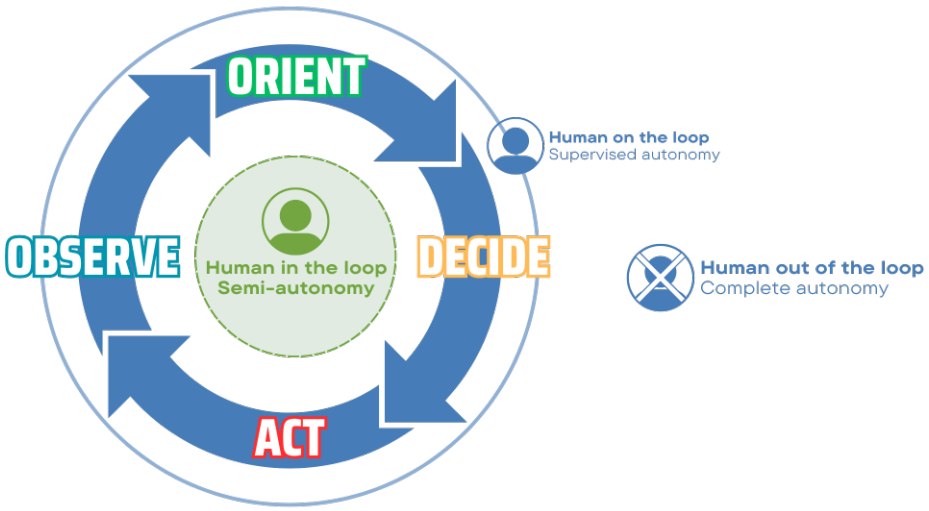


Immagine 7
Struttura 'human in the loop'.

Fonte: Alessandra Russo.

Fondato nel 2017, *Project Maven* utilizza algoritmi per identificare personale e attrezzature sul campo di battaglia. Il sistema può apprendere e perfezionare autonomamente le sue capacità di riconoscimento degli oggetti attraverso l'analisi dei dati di addestramento e il feedback dell'utente. Tuttavia, sottolinea Russo, 'come dice il motto latino sul suo distintivo ufficiale, il Maven non ha la pretesa di sostituire gli esseri umani in guerra': "*officium nostrum est adiuvare*" – "il nostro lavoro è aiutare"' (si veda ***Immagine 8***).

Finora l'impiego di *Maven* è stato limitato, ma si sta espandendo rapidamente: addestrato e testato dai dati forniti dai droni e dai satelliti nelle campagne antiterrorismo, *Maven* è stato testato sul campo nel contesto della guerra Russo-Ucraina dal 2022. Nel febbraio 2024, gli Stati Uniti hanno utilizzato *Maven* in Iraq, Yemen e Siria per attacchi di rappresaglia a seguito di un attacco di militanti sostenuti dall'Iran che ha ucciso tre riservisti dell'esercito statunitense. È importante notare che:

Immagine 8
Project Maven, badge ufficiale

Fonte: US DoD

> *Maven* viene utilizzato per trovare potenziali obiettivi, non per verificarli o per schierare armi contro di essi: non c'è automazione nel funzionamento di *Maven* e ogni passo che l'IA compie prevede un controllo umano alla fine. Invece, *Gospel* e *Lavender* operano in modo molto diverso.

Gospel e *Lavender* sono due sistemi sviluppati dall'IDF per l'identificazione degli obiettivi:

> Non si tratta dei primi casi di utilizzo dell'IA da parte dell'IDF – la '*Fire Factory*', ad esempio, è in uso dal 2021 – ma è il primo impiego dell'IA in operazioni su larga scala, ovvero le operazioni in corso nella Striscia di Gaza.

Gospel genera raccomandazioni automatiche per l'attacco di residenze private o edifici dove si ritiene che vivano o operino sospetti militanti, mentre *Lavender* si concentra sugli individui (indipendentemente dal luogo) per generare 'kill list'. Entrambi i sistemi producono obiettivi ad un ritmo molto veloce senza un controllo significativo o accurato da parte degli operatori umani, che 'dedicano meno di 30 secondi a qualsiasi obiettivo prima di autorizzare un attacco, compreso il bombardamento pesante di case private'. L'IDF ha impiegato i suoi sistemi ATR con l'intento deliberato di sfruttare la velocità dell'IA a scapito della precisione e del controllo. Infatti, con *Gospel* e *Lavender*:

> non c'è alcun obbligo di controllare accuratamente l'output o i dati grezzi dell'intelligence – e questo nonostante si sappia che il sistema commette 'errori' in circa il 10% dei casi, e che il sistema è noto per contrassegnare come bersaglio individui che hanno solo legami deboli, o nessun legame, con i gruppi militanti – causando un alto numero di vittime.

Quindi, mentre l'utilizzo di Maven da parte degli Stati Uniti prevede un controllo umano significativo, in maniera conforme al diritto umanitario internazionale (IHL), nella Striscia di Gaza stiamo assistendo a 'un uso più distopico di queste tecnologie,

in cui la scelta di uccidere è de facto delegata alla macchina e i danni collaterali sono altamente tollerati'.

In sintesi, la velocità e il vantaggio operativo consentiti da queste tecnologie facilitano una condotta di guerra indiscriminata, sia essa deliberata o meno. In effetti, i rischi intrinseci associati all'IA fanno sì che anche l'uso involontariamente indiscriminato di sistemi di IA offensivi sia un problema da tenere in considerazione e da affrontare, soprattutto perché vi sono indicazioni che anche gli Stati Uniti intendono espandere l'autonomia dei loro sistemi algoritmici, compreso Maven, con la revisione della Direttiva 3000.09 del Dipartimento della Difesa (DoD). Tutto ciò significa che anche se le democrazie possono formalmente sostenere la protezione delle vite civili e il rispetto dei principi del diritto internazionale umanitario, l'uso incontrollato dell'IA nei conflitti può de facto minare l'applicazione di questi stessi principi, evidenziando la necessità di migliorare la responsabilizzazione e la trasparenza nella 'guerra algoritmica'. Ciò è tanto più importante e urgente, sostiene Russo, perché:

> l'urgenza nei conflitti o la paura di perdere vantaggi a favore di un avversario potrebbero spingere a un impiego dell'IA meno attento o conforme, e l'uso improprio dell'IA potrebbe a sua volta abbassare il livello di condotta degli altri utenti e altri Stati potrebbero sfruttare questi precedenti per impiegare i sistemi di IA in modi nocivi.

In chiusura del quarto panel, **Eton Lin** illustra l'esperienza di Taiwan nell'elaborazione di metodi per contrastare le operazioni di disinformazione della Cina. Basandosi sulla propria esperienza di cittadino taiwanese, Lin descrive le differenze tra i due Paesi e la minaccia posta dalla Cina nei confronti di Taiwan: 'Anche se non c'è un conflitto attivo, la guerra dell'informazione si svolge quotidianamente a causa della nostra lingua comune'. In effetti, uno studio del 2018 di V-Dem (Varieties of Democracy) che utilizza una nuova serie di indicatori sui social media e sulla disinformazione raccolti dal Digital Society Project dimostra che i governi stranieri, in particolare la Cina, diffondono informazioni false su tutte le principali questioni politiche di Taiwan. Ad esempio, la Cina utilizza i cittadini e i partiti politici di Taiwan per diffondere fake news prima delle elezioni, interferendo così con il processo elettorale. Secondo il rapporto, Taiwan è stata gravemente colpita dalla disinformazione straniera e continua a esserlo tuttora, classificandosi tra i primi Paesi che hanno subito tali attacchi dal 2018 al 2023 (cfr. ***Grafico 4***).

Grafico 4
La disinformazione straniera a Taiwan.

Fonte: The Digital Society Project/V-Dem.

Durante le elezioni locali di Taiwan del 2018, la disinformazione e la misinformazione sono state un problema serio. Il Kuomintang (KMT), un partito politico indicato anche come Partito Nazionalista Cinese, ha utilizzato immagini false che mostravano degli agricoltori taiwanesi che abbandonavano i loro prodotti, sostenendo che non potevano venderli a causa degli scarsi risultati del governo di Taiwan (si veda ***Immagine 9***). 'Durante le elezioni', afferma Lin, 'i cittadini taiwanesi hanno notato una quantità

significativa di fake news diffuse su piattaforme online come Facebook, Instagram, Line e WhatsApp e hanno chiesto al governo di intervenire. La necessità di regolamentare la comunicazione online e di contrastare la disinformazione è diventata evidente'.

Immagine 9
Mis/disinformazione durante le elezioni locali del 2018 a Taiwan.
Fonte: Eton Lin.

Tuttavia, inizialmente il governo di Taiwan non ha fatto nulla in risposta agli attacchi di disinformazione della Cina. Secondo Lin, l'inazione può essere attribuita ai dilemmi che emergono dai due principali approcci tradizionali per contrastare la disinformazione: da un lato, il 'modello statunitense' promuove la libertà di internet, con i governi che si affidano all'autoregolamentazione delle piattaforme online; dall'altro, il 'modello cinese' sostiene il diritto di ogni Paese di regolare il proprio cyberspazio alla luce di quella che è stata definita 'sovranità digitale'. Come spiega Lin, 'mentre il primo approccio sembra essere fondamentalmente difettoso e inefficace, in quanto le piattaforme spesso non sono incentivate a regolarsi da sole, il secondo approccio solleva preoccupazioni per le sue basi autoritarie o antidemocratiche'. Pertanto, continua Lin:

> il governo di Taiwan si è trovato di fronte a un dilemma: se avesse adottato il modello statunitense, l'approccio di autoregolamentazione avrebbe potuto non essere efficace nel proteggere Taiwan dalla guerra dell'informazione cinese. Ma se avesse scelto il modello cinese, avrebbe rischiato di allinearsi alla teoria della sovranità informatica cinese, potenzialmente appoggiando l'autoritarismo come mezzo per contrastare l'autoritarismo.

Il governo di Taiwan si è trovato tra l'incudine e il martello, il che spiega la paralisi iniziale.

Per affrontare questo dilemma, Taiwan ha dovuto andare oltre gli approcci tradizionali per contrastare la disinformazione, adottando quello che Lin chiama un 'approccio basato sul senso civico' che deriva dal background unico di Taiwan. Dalla fine degli anni Ottanta, Taiwan è diventata una società più democratica e aperta, dove sono fiorite organizzazioni non governative (ONG) e i gruppi di attivisti (*advocacy*). Sulla base di osservazioni a lungo termine della società civile taiwanese dopo la democratizzazione, il famoso studioso di diritto Yeh Jiunn-rong ha coniato il termine 'costituzionalismo civico' per descrivere i movimenti civico-centrici e riformisti che guidano il cambiamento costituzionale a Taiwan. Spiega Lin: 'Yeh Jiunn-rong ha sottolineato che nel considerare le questioni costituzionali, il ruolo dei cittadini e della società civile è fondamentale. Sulla stessa linea, sostengo che la strategia di Taiwan contro la disinformazione è un esempio di costituzionalismo civico'. In effetti, notando l'inazione del governo contro la disinformazione, la società civile taiwanese ha preso posizione: durante le elezioni locali del 2018, la Taiwan

Media Watch Foundation e la Association for Quality Journalism hanno istituito il Taiwan FactCheck Center per gestire le denunce e indagare sulle informazioni false. Poco dopo, hanno iniziato a emergere altri servizi di fact-checking (ad esempio MyGoPen, Cofacts, Rumor & Truth, Auntie Meiyu, Doublethink Lab) per smascherare gli attacchi di disinformazione della Cina.

Tuttavia, dopo l'istituzione del FactCheck Center nel luglio 2018, 'si è scatenata una battaglia sulla regolamentazione della disinformazione online tra tre attori chiave: il governo, la società civile e le piattaforme online, afferma Lin. Il 10 ottobre 2018, il presidente Tsai Ing-wen ha sottolineato l'importanza di combattere le fake news nel suo discorso per la Giornata nazionale. Pochi mesi dopo lo Yuan esecutivo ha pubblicato un rapporto sulla 'Prevenzione del pericolo delle fake news' che prevedeva quattro strategie: 1) migliorare l'alfabetizzazione mediatica e la capacità di giudizio dei cittadini, 2) creare meccanismi di chiarimento e di fact-checking, 3) collaborare con le piattaforme mediatiche e 4) rendere le persone responsabili delle fake news soggette a un controllo giudiziario equo e indipendente. Le piattaforme online hanno cercato di resistere, pubblicando una lettera aperta attraverso l'Asia Internet Coalition, sostenendo che le proposte del governo avrebbero minato la libertà di parola. In risposta, il governo ha esortato le piattaforme ad assumersi la responsabilità dell'autogoverno e, in effetti, nel giugno 2019 cinque piattaforme hanno annunciato un Codice di autodisciplina per la prevenzione della disinformazione. Durante questa fase, la società civile ha sostenuto le decisioni del governo. Tuttavia, quando il governo ha cercato di inasprire le norme sulla comunicazione online e sulle piattaforme online, la società civile ha reagito. Nel giugno 2022, la Commissione nazionale per le comunicazioni (NCC) di Taiwan ha proposto una legge sui servizi di intermediazione digitale (*Digital Intermediary Services Act*, DISA), ispirata alla legge sui servizi digitali dell'UE, che avrebbe consentito alle agenzie governative di rivolgersi a un tribunale per ottenere 'ordini di restrizione' per costringere le piattaforme a rimuovere o limitare i contenuti illegali. Diverse ONG si sono opposte con forza alla proposta di legge dell'NCC, sostenendo che violava eccessivamente la libertà di espressione. Il successivo allineamento tra le piattaforme online e la società civile ha portato l'NCC a ritirare la bozza DISA.

In sintesi, mentre il governo ha inizialmente esitato a regolamentare la comunicazione online e a contrastare la disinformazione, le ONG e i cittadini hanno preso l'iniziativa, creando strumenti per identificare le informazioni false e migliorando l'alfabetizzazione mediatica del pubblico. Durante i due round della 'battaglia' tra i principali attori, gli sforzi della società civile hanno rafforzato la trasparenza del governo, obbligandolo a fornire informazioni più dettagliate e specifiche sulle sue politiche. Allo stesso tempo, la società civile è rimasta vigile nei confronti del governo e, quando ha riconosciuto la potenziale minaccia posta dalla DISA alla libertà di parola, ha agito per proteggere l'autonomia online. Basandosi sulla recente esperienza di Taiwan, conclude Lin, possiamo dire che 'il costituzionalismo civico rappresenta un terzo approccio per contrastare la disinformazione, dimostrando che le soluzioni trascendono i binari "democrazia contro autoritarismo" o "Stato contro mercato"'. Piuttosto, le soluzioni efficaci nascono dalle interazioni tra Stato, mercato e cittadini: 'invece di affidarsi esclusivamente alle piattaforme private o di limitarle, una buona opzione per combattere la disinformazione è quella di collaborare con i cittadini dotati di potere, sostenendo e rafforzando le loro iniziative invece di cercare di sostituirle'.

Osservazioni conclusive

Condividendo le sue riflessioni conclusive, **Chris Alden** osserva come il simposio abbia rafforzato la sua convinzione che un approccio multidisciplinare offra maggiori spunti di riflessione rispetto a un focus ristretto sulle relazioni internazionali:

> Integrando diverse dimensioni e prospettive, si può raggiungere una comprensione più completa dell'argomento – una comprensione che non deve necessariamente essere sempre perfettamente coerente. La nostra intenzione iniziale era quella di discutere [la (geo)politica dell'autoritarismo digitale] attraverso lenti e approcci disciplinari diversi, e il valore di questo sforzo è stato convalidato.

Facendo eco al commento di Alden, **Stefano Ruzza** insiste:

> nell'ultimo giorno e mezzo, abbiamo percorso molte strade. Abbiamo guardato il nostro mondo contemporaneo (digitale) da diversi punti di vista e a diversi livelli di analisi. Siamo riusciti ragionare con concetti più astratti, a sporcarci le mani con la pratica e i dati e a sederci con disagio di fronte a dilemmi scomodi. Credo, e spero, che Christopher Coker sarebbe stato molto soddisfatto del risultato.

Day 1

Opening remarks

Stefano Ruzza
Associate Professor of Political Science and Peace and Conflict Studies, Università degli Studi di Torino; Head of Research, T.wai – Torino World Affairs Institute

Chris Alden
Director of LSE IDEAS; Professor of International Relations, London School of Economics and Political Science (LSE)

Nicolò Russo Perez
Head of International Relations, Fondazione Compagnia di San Paolo

Keynote speech

Anja Kaspersen
Senior Fellow, Carnegie Council for Ethics and International Affairs

PANEL 1 — Bad news: assessing and countering disinformation

CHAIR **Stefano Ruzza**
Associate Professor of Political Science and Peace and Conflict Studies, Università degli Studi di Torino; Head of Research, T.wai – Torino World Affairs Institute

SPEAKERS **Michelangelo Conoscenti**
Professor of English Language and Linguistics, Università degli Studi di Torino

Massimiliano Fusari
Professor, H-FARM College; Visual Communication Strategist

Matthew Heneghan
PhD Candidate, University of Glasgow

PANEL 2 — Addressing Authoritarianism in Digital Governance

CHAIR **Chris Alden**
Director of LSE IDEAS; Professor of International Relations, London School of Economics and Political Science (LSE)

SPEAKERS **Fang-Long Shih**
Project Associate for the Digital IR in the Information Age project, LSE IDEAS

Antonella Seddone
Associate Professor of Political Science, Università degli Studi di Torino

Enea Fiore
PhD Candidate, Laval University and University of Geneva

Daniela Romée Piccio
Assistant Professor, Università degli Studi di Torino

PANEL 3 —— **Our Shared Digital Future: Recommendations for Public Private Cooperation**

CHAIR **Vlad Zigarov**
Programme Manager for the IDEAS Europe Programme, LSE IDEAS

SPEAKERS **Kenddrick Chan**
Head of the Digital IR in the Information Age project, LSE IDEAS

Tin Hinane El-Kadi
PhD Candidate, London School of Economics and Political Science (LSE); Associate Fellow, Chatham House

Melanie Garson
Lead for Cyber Policy & Tech Geopolitics, Tony Blair Institute for Global Change; Associate Professor of International Conflict Resolution and International Security, University College London (UCL)

Day 2

PAPER PRES. —— **Sovereignty and the Three Digital Ecologies in an Age of Geopolitics**

SPEAKER **Richard Higgott**
Distinguished Professor of Diplomacy, Brussels School of Governance; Visiting Fellow, Robert Schuman Institute at the European University Institute; Emeritus Professor of International Political Economy, University of Warwick

PANEL 4 —— **Emerging Voices in the Digital Domain**

CHAIR **Davide Pellegrino**
Assistant Professor of Political Sociology, Università degli Studi di Torino

SPEAKERS **Stella Blumfelde**
PhD Candidate, Università degli Studi di Genova

Lorraine Charbonnier
PhD Candidate, King's College London; Research Fellow, T.wai – Torino World Affairs Institute

Alessandra Russo
PhD Candidate, Università Cattolica del Sacro Cuore

Yu-teng Lin
PhD Candidate, National Taiwan University

Closing remarks

Stefano Ruzza
Associate Professor of Political Science and Peace and Conflict Studies, Università degli Studi di Torino; Head of Research, T.wai – Torino World Affairs Institute

Chris Alden
Director of LSE IDEAS; Professor of International Relations, London School of Economics and Political Science (LSE)

LSE Ideas

twai Torino World Affairs Institute

CPS Culture Politica Società

Università di Torino

Con il supporto di

Fondazione Compagnia di San Paolo