CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

74ª sessione di Studio – 4° Gruppo di lavoro dell'Istituto Alti Studi per la Difesa

"Il Metaverso: possibile nuovo terreno di confronto virtuale nella guerra ibrida con potenziali effetti nella dimensione cognitiva e fisica. Come dovrebbe modificarsi l'approccio della Difesa, in termini di vantaggi operativi, rischi e misure di salvaguardia, passando da una situazione di stringente contatto con la realtà ad un nuovo universo virtuale concepito nel massimo distacco dal mondo materiale."

(Codice AS-SMD-08 _ AS-SMA-08)

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della Difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.
L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.
L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.
L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche. L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa", oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato. L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

74ª Sessione di Studio – 4° Gruppo di lavoro dell'Istituto Alti Studi per la Difesa

"Il Metaverso: possibile nuovo terreno di confronto virtuale nella guerra ibrida con potenziali effetti nella dimensione cognitiva e fisica. Come dovrebbe modificarsi l'approccio della Difesa, in termini di vantaggi operativi, rischi e misure di salvaguardia, passando da una situazione di stringente contatto con la realtà ad un nuovo universo virtuale concepito nel massimo distacco dal mondo materiale."

(Codice AS-SMD-08 _ AS-SMA-08)

“Il Metaverso: possibile nuovo terreno di confronto virtuale nella guerra ibrida con potenziali effetti nella dimensione cognitiva e fisica. Come dovrebbe modificarsi l’approccio della Difesa, in termini di vantaggi operativi, rischi e misure di salvaguardia, passando da una situazione di stringente contatto con la realtà ad un nuovo universo virtuale concepito nel massimo distacco dal mondo materiale.”

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell’autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l’autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.
Questo volume è stato curato dall’**Ufficio Studi, Analisi e Innovazione dell’IRAD**.

Direttore
Gen.B. Gualtiero Iacono

Capo dell’Ufficio Studi, Analisi e Innovazione
Col. AArnn Pil. Loris Tabacchi

Progetto grafico
1° Mar. Massimo Lanfranco – C° 2ª Gianluca Bisanti – Serg. Manuel Santaniello – Ass. Amm. Stefano Deiana

Revisione e coordinamento
C.A. Massimo Gardini – S.Ten. Elena Picchi – Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra – Ass. Amm. Caterina Tarozzi

Autore
IASD – 74ª Sessione di Studio – 4° Gruppo di Lavoro

Stampato dalla Tipografia del **Centro Alti Studi per la Difesa**

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazione
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3205
e-mail: irad.usai.capo@casd.difesa.it

chiusa a gennaio 2024

ISBN 979-12-5515-070-1

CENTRO ALTI STUDI PER LA DIFESA

ISTITUTO ALTI STUDI PER LA DIFESA

74ª SESSIONE DI STUDIO

Anno Accademico 2022 – 2023

Il Metaverso: possibile nuovo terreno di confronto virtuale nella guerra ibrida con potenziali effetti nella dimensione cognitiva e fisica. Come dovrebbe modificarsi l'approccio della Difesa, in termini di vantaggi operativi, rischi e misure di salvaguardia, passando da una situazione di stringente contatto con la realtà ad un nuovo universo virtuale concepito nel massimo distacco dal mondo materiale.

LAVORO DI GRUPPO – IV SEZIONE

A cura di:

Gen. B.A.	Stefano Castelnuovo	Gen. B.	Massimo Cicerone
C.A.	Fabrizio Rutteri	Col.	Fabio De Luca
Col.	Alessandro Lorenzetti	C.V.	Daniele Martinuzzi
Col.	Pietro Sorbello	Dott.	Luca Gennaretti
Dott.	Marco Loiacono	Dott.	Gabriele Perazza
Ing.	Paolo Picchio	On.	Emanuela Rossini
Dott.	Cristiano Rufini	Dott.	Angelo Marco Stella
Dott.ssa	Sabina Strazzullo		

Direttore Coadiutore:

Cons. d'Amb. Emanuele Farruggia

INDICE

SOMMARIO

Sebbene il Metaverso sia ancora agli inizi, esso può divenire la più grande rivoluzione tecnologica del decennio; il suo potenziale di trasformare ogni aspetto della nostra vita, sia nella sfera professionale che personale, lo ha posto al centro dell'attenzione di intellettuali e scienziati di tutto il mondo.

Le enormi potenzialità insite costituiscono incredibili opportunità e sfide, ma destano al contempo enormi preoccupazioni a fronte delle conseguenze per la moderna società del XXI secolo.

Per quanto per anni il Metaverso sia stato un argomento elitario per visionari, lettori *cyberpunk e gamer*, oggi il marketing mondiale ha saputo spostare l'attenzione di milioni di utenti sui propri social e convincere alcune delle principali aziende del pianeta a convertirsi al progetto.

Il presente studio vuole presentare Metaverso quale terreno di un nuovo confronto virtuale nella guerra ibrida nella consapevolezza, tuttavia, che non siamo di fronte ad una semplice innovazione o un aggiornamento della realtà odierna, ma ad una rivoluzione della vita quotidiana e delle dinamiche esistenti. Il rischio insito è che se la tecnologia avanza troppo velocemente rispetto alle reali possibilità economiche e fisiche dell'essere umano, si creerà un'élite ristretta di utenti capaci di accedere – virtualmente o fisicamente – in posti riservati ed esclusivi.

Nel primo capitolo viene introdotto il progetto Metaverso nella sua fase di sviluppo, storico e tecnologico, tale da far comprendere una rivoluzione in arrivo – un nuovo 'big bang' – dalla portata di una svolta antropologica.

Il secondo capitolo affronta la sfida cognitiva del Metaverso, analizzando l'impatto sociale che nuove pratiche condotte dalla simulazione di un mondo virtuale possono avere sulla percezione e costruzione della realtà.

Il terzo capitolo affronta la regolamentazione del Metaverso e muove dalla differenza tra legge e diritto, essendo soltanto la prima ontologicamente legata alla dimensione dello Stato nonché ai limiti territoriali della sua sovranità. Il profilarsi di un territorio virtuale ed universale mette ancora una volta alla prova la capacità del diritto di disciplinare le opportunità ed i rischi offerti dalle nuove tecnologie.

Nel quarto capitolo si prende in considerazione il concetto di guerra ibrida e le sue minacce, facendo emergere come il Metaverso abbia tutte le potenzialità di diventare un possibile ambiente operativo dove le tecniche e le tattiche facenti parte della guerra ibrida possono trovare applicazione.

Il quinto capitolo analizza l'impatto del Metaverso nella Difesa partendo da quanto già realizzato, principalmente nell'ambito delle attività addestrative a favore del personale militare, per presentare possibili nuovi sviluppi della realtà virtuale.

Nel sesto capitolo si analizza la dimensione più propriamente tecnologica ed economica del progetto Metaverso, guardando alle trasformazioni che avverranno, sul piano del lavoro e nel mondo dei servizi, a fronte di una sempre maggior pervasività della dimensione virtuale che porterà all'abilitazione dell'erogazione dei servizi ed applicazioni sul Metaverso. Nella parte conclusiva il presente Studio propone una sintesi di quelli che sono fattori di rischi e minacce, alcuni già applicabili oggi e altri che lo saranno tra tre o cinque anni, unitamente ad una serie di raccomandazioni per governare quella che a tutti gli effetti si prospetta essere una svolta storica per l'umanità, densa di conseguenze e di questioni etiche da considerare.

ABSTRACT

Although the metaverse project is still at its early development, its potential to transform every aspect of people's lives, both in the professional and personal sphere, has placed it at the center of the world's attention. These enormous potentials raise significant challenges and major concerns among all stakeholders who deal with in national security and social welfare.

The first chapter introduces the metaverse project in its stage of development, both historical and technological, so as to understand an incoming revolution – a new 'big bang' - on the scale of an anthropological turning point. The second chapter deals with the cognitive challenge of the Metaverse, analysing the modifications and alterations that immersive technologies can operate on the process of perception and construction of reality. The third chapter addresses the crucial issue of regulation and law. In particular, what new risk factors come into play with these new virtual territories that open up spaces of operation and negotiation not yet under state jurisdiction and outside the real world.

In the fourth chapter, the concept of Hybrid warfare and its threats are considered, highlighting how the Metaverse has all the potential to become a possible operational environment where the techniques and tactics forming part of Hybrid warfare can find application. The fifth chapter analyzes the impact of the Metaverse in Defense starting from what has already been achieved, mainly in the context of training activities in favour of military combat personnel, to present possible new developments in virtual reality. In the sixth chapter, the more properly technological and economic dimension of the Metaverse project is analysed, looking at the transformations that will take place, in the workplace and in the world of services, in the face of the increasing pervasiveness of the virtual dimension that will lead to the enabling of the provision of services and applications on the Metaverse.

In the final section, this study proposes a summary of risk and threat factors, some already applicable today and others that will be so in three to five years' time, together with a series of recommendations for governing what to all intents and purposes promises to be a historic turning point for humanity, full of consequences and ethical issues to be considered.

INTRODUZIONE

Esiste “posto dove andare senza andare da nessuna parte” e “dove il limite della realtà è la tua immaginazione”. Così viene definito Oasis, una sorta di Metaverso dove fuggire dallo squallore della vita quotidiana nel film “Ready Player One” del 2018.

Siamo all’alba di un nuovo rinascimento, che, come nel XIV e XV secolo, è profondamente connesso con una rivoluzione nella tecnologia dell’informazione e foriero di un’era in cui l’essere umano si articola senza soluzione di continuità con la macchina intelligente.

Prima che Mark Zuckerberg annunciasse il cambio di nome della propria compagnia da Facebook a Meta erano probabilmente poche le persone che avevano già letto o sentito il termine “Metaverso”.

Nella parola “Metaverso” la combinazione del prefisso ‘meta’ – che implica un trascendere - con ‘universo’ fa riferimento ad un ipotetico universo sintetico, collegato al mondo fisico. Il termine viene coniato la prima volta nel 1992 da Neal Stephenson, autore *Cyber geek*, noto per il suo romanzo Snow Crash, dove i personaggi vivono simultaneamente in più dimensioni, fisiche e virtuali, interagendo tra di loro attraverso avatar digitali, in corrispondenza al proprio sé fisico, in una dualità/continuità tra fisico e virtuale. Ambientato in un’America anni Venti, Snow Crash è abitato da fattorini che corrono all’impazzata su strade sui loro skateboard ipertecnologici con ruote intelligenti, meta-poliziotti che indossano armi futuristiche e unità cyborg di sicurezza. Intorno a tutto questo mondo reale esiste il Metaverso, realtà virtuale 3D collegata a livello con fibre ottiche, in cui ciascuno è rappresentato in tre dimensioni dal proprio Avatar che permette di muoversi in un mondo parallelo in cui la realtà dei personaggi cambia. Così, il protagonista del romanzo, che vive in un container, diventa proprietario di immobili di lusso, maestro di spada e hacker nello spazio tridimensionale chiamato ‘Metaverse’, lavora per conto della Mafia e fa parte della banda dei “bravi ragazzi” coinvolti nella ricerca della droga misteriosa chiamata “snow crash”: una specie di virus informativo che funziona sia nel Metaverso che nel mondo reale e che la banda dei “cattivi” intendono usare per contaminare la realtà. A governare l’intero universo virtuale sono grandi gruppi di poteri, le disparità sono enormi e gli Stati assenti.

Già in questo romanzo troviamo dunque come il termine Metaverso sia stato coniato per esplorare, se non facilitare, la trasformazione digitale in ogni aspetto della nostra vita fisica quotidiana, lavorativa e sociale oltre che la dark side della società.

CAPITOLO 1
LA NUOVA DIMENSIONE: EVOLUZIONE STORICA E TECNOLOGICA

Sin dagli anni '90 la rivoluzione digitale ha vissuto una continua evoluzione. Partendo dal Web 1.0 (pc e informazione) al Web 2.0 (smartphone e social), negli ultimi trent'anni la società ha visto una crescente divulgazione e condivisione di contenuti nuovi, prima solo testi, poi visual e video, la cui fruizione e creazione è avvenuta attraverso l'interazione con un oggetto, un medium: il computer fisso, diventato sempre più piccolo e portatile fino ai nostri telefonini di oggi.

Il passaggio che si prospetta oggi con il Metaverso è quello di rompere questo schermo di binarietà per creare esperienze tridimensionali, capaci di dare sensazioni di presenza, ovvero esperienze sempre più immersive ed immediate/simultanee: "un internet spaziale, dove si entra e ci si muove"[1].

Tale passaggio ha una diretta e potente ricaduta sull'utente, che si trova ad operare attraverso un proprio alter-ego tecnologico (Avatar) in un luogo (il Metaverso) che non corrisponde più al dove nella realtà in cui si trova con il proprio corpo. Ed è proprio la rottura di quella continuità spazio-temporale del "qui e ora", tra corpo e mente, a cui l'essere umano è abituato, a rappresentare un punto di svolta epocale che Floridi, uno dei massimi esperti di tecnologia applicata al business definisce così: "una vera e propria "ri-ontologizzazione digitale della realtà, agita dalle ITC (*Information and Communication Technologies*) e dalla AI (*Artificial Intelligence*)[2].

Un passaggio che non avviene all'improvviso ma che è stato avviato e facilitato, in questi anni dall'impiego di nuove tecnologie con le quali sono stati creati ambienti virtuali immersivi, tuttavia ancora mediati dal computer, tra cui: reti sociali, videoconferenze, mondi virtuali in 3D (ad esempio, VR Chat), applicazioni di realtà aumentata (ad esempio, Pokemon Go) e giochi a gettoni non fungibili (ad esempio, Upland).

Questi ambienti virtuali, anche se non permanenti e sempre connessi, ci hanno permesso di ottenere diversi gradi di trasformazione digitale aprendo la strada per quella ulteriore evoluzione che vede nel Metaverso la sua destinazione finale, marcando il passaggio da una fase di "digitalizzazione" compiuta dal 2000 al 2022, ad una di "virtualizzazione"[3].

La visione che sta al centro del Metaverso costituisce dunque un salto di livello tale da essere evocato come un 'big bang' digitale del nostro Cyberspazio: un Internet immersivo come un regno

---

1 Lorenzo Montagna, *Metaverso. Noi e il Web 3.0*, Mondadori, Verona 2022. Pag.24. In questo volume Montagna raccoglie interviste con chi sta studiando e creando il Metaverso: i top manager di quattro Big Tech, docenti universitari e giovani.

2 L. Floridi, Agere sine intelligere. L'intelligenza artificiale come nuova forma di agire e i suoi problemi etici, in L.Floridi, F.Cabitza, *Intelligenza artificiale. L'uso delle nuove macchine*, Bompiani, Milano 2021, pp.138, 149, 176.

3 "verso un mondo digitale più personale, più credibile, empatico e interattivo" in: L. Montagna, ibidem, p. 14

gigantesco, unificato, persistente e condiviso, sostenuto da tecnologie emergenti, come la realtà estesa, ("*extended reality*") il 5G e l'Intelligenza Artificiale (IA).

Una svolta comunque densa di complessità con rilevanti fattori da analizzare tale da provocare quello definito anche uno "shock antropologico"[4] per chi ne sta studiando l'impatto sul piano cognitivo, psicologico e sociale.

Non è facile trovare una definizione condivisa di Metaverso. La prima immagine che viene alla mente quando se ne parla è probabilmente una persona che indossa un visore per la realtà virtuale. Ma ridurre il Metaverso a questa singola pratica rischia di essere fuorviante. Sin dalla sua prima apparizione, come un universo-generato da computer il Metaverso è stato definito in tanti modi per esprimere diversi concetti: come *life logging*[5], *collective space in virtuality*[6], *embodied internet/spatial Internet*[7], *a mirror world*[8], *un omniverse: luogo di simulazione e collaborazione*[9].

Cercando di semplificare, la creazione del Metaverso può essere vista attraverso tre fasi[10]:

- la creazione dei gemelli digitali (I);
- quella dei nativi digitali (II);
- la coesistenza di realtà fisico-virtuale (III).

Nella prima fase (I), abbiamo la duplicazione in digitale del mondo reale, con modelli digitali ad un'alta fedeltà che riproducono realtà fisiche in ambienti virtuali, incluse le loro proprietà e funzioni. Il collegamento tra reale/virtuale avviene attraverso dati del mondo reale. Tra le applicazioni già esistenti troviamo, come esempi, i sistemi CAD e lo *Smart Urban Planning*.

---

4 Eugenio Mazzarella *Contro Metaverso. Salvare la presenza*, Mimesis, Milano 2022, p.12, 32, 128.

5 https://www.roblox.com/

6 https://www.microsoft.com/en-us/hololens

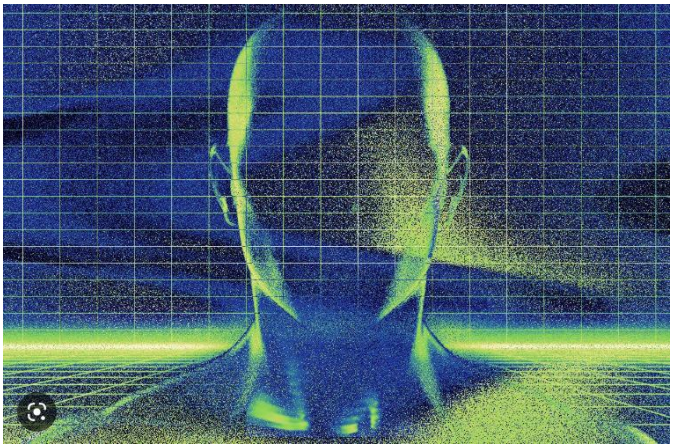
7 https://earth3dmap.com/

8 https://id.secondlife.com

9 https://hello.vrchat.com/

10 All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda, p. 1-2. Available at https://www.researchgate.net/publication/355172308_All_One_Needs_to_Know_about_Metaverse_A_Complete_Survey_on_Technological_Singularity_Virtual_Ecosystem_and_Research_Agenda.
Questo corposo documento di indagine presenta il primo sforzo scientifico di offrire un quadro completo che esamina gli ultimi sviluppi del Metaverso sotto le dimensioni delle tecnologie all'avanguardia e degli ecosistemi metaversi. Qui gli Autori propongono un'agenda di ricerca concreta per lo sviluppo del Metaverso esaminando in modo rigoroso otto tecnologie abilitanti: la realtà estesa, l'interattività dell'utente (interazione uomo-computer), l'intelligenza artificiale, la blockchain, la computer vision, l'IoT e la robotica, l'edge e il cloud computing e le future reti mobili. Lo Studio analizza in particolare sei fattori incentrati sull'utente: avatar, creazione di contenuti, economia virtuale, accettabilità sociale, sicurezza e privacy, fiducia e responsabilità.

Il secondo passaggio (II) è la creazione di 'contenuto nativo', ovvero i creatori digitali, rappresentati da Avatar ma non solo, realizzano contenuti digitali dentro i mondi digitali, che possono essere collegati con i loro omologhi corrispettivi fisici o esistere solo nel mondo digitale. In questa fase intervengono anche ecosistemi (culturali, economici, regolatori) a supporto delle creazioni digitali e analoghi a quelli di produzione di norme e di beni nel mondo fisico. Le applicazioni per questo sono in fieri ed oggetto di studio.



La terza fase (III) ipotetica è quella che vede il Metaverso che potrebbe diventare un mondo virtuale autosufficiente e permanente che co-esiste e interopera con il mondo reale con un alto grado di indipendenza. Come tali, gli Avatar, che rappresentano gli utenti umani, possono vivere attività diverse in simultanea, caratterizzate da un numero illimitato di utenti che si muovono teoricamente in mondi virtuali multipli. Il Metaverso, infatti, oggi offre una interoperabilità tra i diversi metaversi e questo permette di muoversi su tutte le piattaforme e a livello globale[11].

La caratteristica del Metaverso, quindi, è quella di diventare un ambiente virtuale unificato e continuo, con la prospettiva che i mondi virtuali, costruiti su dati e informazioni dei sistemi del mondo reale (fase I), incorporando strumenti di connessioni, *blockchain* e altre tecnologie, diventino così abituali da trasformare il Metaverso in un'estensione della realtà.

A far dialogare i due mondi nel Metaverso saranno i "gemelli digitali", cloni virtuali dei soggetti reali, collegati direttamente con la loro controparte fisica. Grazie a questo, indossando tutto il giorno occhiali ibridi, potremo vedere e interagire nel nostro ambiente fisico con oggetti e persone digitali. Oppure, vedere e interagire persone ed oggetti reali all'interno di mondi virtuali. Per esempio: se in realtà virtuale accendo il condizionatore di casa mia, anche in quella fisica del mio appartamento inizierà a funzionare. Se mi muovo nel mondo reale ed il mio avatar viene toccato nel mondo digitale, un *feedback* tattile verrà fornito al corpo fisico. Lo scopo sarebbe di consentire a un numero illimitato di utenti di Internet di condividere simultaneamente, attraverso il proprio avatar identificabile,

[11] Per ora la competizione sul Metaverso è limitata e prevale uno spirito di collaborazione, come si legge nel report del Technology and Society Editor per l'Economist: Tim Cross '*Is the Metaverse coming*?" 11 novembre 2022 pag. 134. In questo articolo si legge che nell'ottobre 2022 Microsoft ha annunciato che renderà i suoi sistemi operativi di Windows, così come le sue App business e i suoi Games scritti per le sue console Xbox, accessibili anche all'interno dei mondi virtuali Meta. E così tutte le aziende della Silycon Valley hanno aderito ai Metaverse Standard Forum (MSF) che li impegna a standard tecnici aperti ed interoperabili così che un Avatar progettato da un'azienda in un mondo virtuale non incontri problemi in un altro mondo virtuale. Rimane l'unica eccezione di Apple che mantiene la sua priorità di non rendere compatibile il proprio sistema ad altri garantendo ai propri utenti una sorta di 'giardino murato'. Il 2023 dunque viene ritenuto l'anno in cui testare la continuità del MSF sulla base dei risultati economici che avrà prodotto offrendo servizi su Metaverso basati su questo spirito di collaborazione.

esperienze di realtà virtuale a scopo di attività sociali, ricreative, economiche, professionali, artistiche o culturali.

La portata di questa svolta viene confermata da Floridi come la "quarta rivoluzione dell'infosfera", iniziata da Turing, dopo quella di Copernico, Darwin e Freud, per cui "oggi stiamo lentamente accettando l'idea che noi non siamo entità autonome e uniche, ma piuttosto organismi incorporati in modo *informazionale* (inforg), reciprocamente connessi e incorporati in un ambiente informazionale, l'infosfera, che condividiamo con agenti sia naturali che artificiali simili a noi in molti aspetti[12]".

Per quanto innovativa, la rivoluzione del Metaverso trova curiose analogie o anticipazione tra i grandi artisti del passato che oggi incontrano virtualmente i contemporanei sul terreno dell'immaginazione e della creazione di nuove dimensioni spaziali ed esistenziali. Quadri e sculture hanno creato nel passato "mondi" alternativi ed offerto realtà immersive, proponendo ai contemporanei una sorta di "laboratorio per il futuro" ove coesistono una percezione quasi simultanea del materiale e dell'immateriale.

In una raccolta che non vuole essere in alcun modo esaustiva né divulgativa, in allegato vengono riportate alcune opere e citazioni che vogliono presentare la straordinaria capacità visionaria di alcuni artisti e scrittori del passato.

[12] L. Floridi, Turing's three philosophical lessons and the philosophy of Information cit. in Eugenio Mazzarella ibidem p. 80

CAPITOLO 2
IMPATTO COGNITIVO E SOCIO-CULTURALE DEL METAVERSO

2.1 Una nuova percezione della realtà

Le tecnologie che stanno alla base del Metaverso sarebbero dunque in grado di operare un "salto antropologico" storico che preoccupa alcuni proprio per la loro capacità virtuale di implementare quel senso di presenza dell'esperienza ordinaria, come vissuta nella realtà fisica, "alterandola nei suoi vissuti psico-fisici, in un modo completamente innovativo", come afferma il filosofo Eugenio Mazzarella[13].

Chi ha spiegato in modo davvero chiaro ed accessibile anche ai non addetti questa implementazione virtuale dell'esserci dell'uomo è stato lo psicologo Giuseppe Riva, in un suo articolo altamente esplicativo sulla rivoluzione ontologica del Metaverso[14]. Supportato dagli studi delle neuroscienze, Riva ci spiega che quando noi siamo in DAD o in video conferenza, in realtà noi non costruiamo memorie autobiografiche, né identità condivisa, come avviene quando frequentiamo persone in luoghi fisici. Per questo le piattaforme digitali sono anche definite "non-luoghi" e non lasciano alcun segno, se non spesso quella spossatezza e senso di vuoto a fine giornata definita anche '*zoom fatigue'*. Le scoperte più recenti delle neuroscienze hanno capito che quando frequentiamo le piattaforme digitali non si attivano nel nostro cervello quei neuroni[15] che, non solo ci permettono di orientarci nello spazio, ma anche hanno un ruolo fondamentale nella costruzione della nostra memoria autobiografica. Cosa succede nel Metaverso a questi neuroni?

"In realtà queste due tecnologie, la realtà aumentata (AR) e la realtà virtuale (RV) – che sono il cuore del Metaverso – riescono ad attivare i neuroni Gps e rendere il soggetto presente nei luoghi digitali"[16].

Dato che ad attivare il senso di presenza è la nostra mente, il Metaverso è costruito in modo tale da funzionare esattamente come la nostra mente e questo grazie all'esperienza corporea, utilizzata come oggetto di percezione (come ogni altro oggetto presenti nel mondo) ma che diventa anche lo strumento con cui la mente mette in pratica le nostre intenzioni: la nostra percezione della realtà (dentro il Metaverso e attraverso il nostro corpo fisico) diventa dunque frutto di una simulazione

---

[13] Eugenio Mazzarella, *Contro Metaverso. Salvare la presenza*, Mimesis, Milano 2022, p.20. Mazzarella è Prof. Ordinario di Filosofia teoretica presso l'Università Federico II di Napoli.

[14] Giuseppe Riva in: Lettura, *Sono Einstein (oppure Hitler). È il Metaverso*. "Corriere della Sera", 27.02.2022, pp.8-9. Riva è Prof. Ordinario di Psicologia Generale all'Università Cattolica di Milano.

[15] In biologia, i neuroni sono cellule altamente specializzate per la raccolta e la conduzione degli impulsi nervosi e rappresentano l'unità morfologica, genetica e funzionale, del sistema nervoso.

[16] Riva, ibidem

tecnologica, non più dunque frutto di esperienze concrete, fisiche e personali che accadono al nostro corpo nella realtà fisica:

"la realtà virtuale (VR) e la realtà aumentata (AR) cercano di prevedere le conseguenze sensoriali dei movimenti degli utenti, costruendo la stessa scena (visibile nel casco) e le stesse sensazioni (generate dai sensori) che sperimenterebbero nel mondo reale. In quest'ottica il senso di presenza è generato dalla capacità del Metaverso di prevedere come la mente simula la realtà e di generare contenuti digitali che siano coerenti con queste previsioni"[17].

Il risultato è che più le previsioni saranno corrette, più il soggetto si sentirà presente nell'ambiente virtuale, pur sapendo che l'ambiente non è reale.

Quella che si prospetta con il Metaverso è dunque una nuova "realtà ibrida", in cui i confini tra reale e virtuale saranno così co-evoluti e con-penetranti da perdere "persino la percezione stessa di sentirsi reali o virtuali[18] e questo potrebbe portare ad un maggior controllo sociale:

"Uno stato sociale di realtà alterata che avrà bisogno per funzionare, per governare le frizioni, di tecnologie di controllo ben più pervasive – cioè costrittive non persuasive – di quelle del passato: religione, morale, diritto, filosofia, politica (visioni del mondo) – ovvero gli strumenti dell'antropologia che fino a ora conosciamo"[19]. Incluse, aggiungiamo, visioni politiche come quelle di Stato e di Nazione.

Secondo il semiologo Massimo Leoni, infatti, un rischio di lungo periodo con un forte impatto culturale è quello digitale, legato alla possibile disaffezione dei soggetti, soprattutto quelli delle ultime generazioni, nei confronti dell'idea stessa di Paese. Quest'idea di "Stato-Nazione" è del resto legata a uno sviluppo storico molto lungo e abbastanza recente, almeno in Europa, il quale però potrebbe essere scavalcato da processi culturali che leghino sempre meno la definizione dell'identità al luogo in cui si è nati e cresciuti, e dove si hanno le proprie relazioni "reali", e sempre più a contesti virtuali ove si svolgono le proprie attività professionali, ludiche, sentimentali[20].

Il trasferimento di un numero crescente di attività umane nel Metaverso potrebbe dunque portare anche ad a un progressivo scardinamento dell'idea tradizionale di Paese, ma anche, per converso, "all'emersione di nuovi nazionalismi digitali, che cerchino invece di creare percorsi di affermazione identitaria anche nella simulazione digitale in rete"[21].

---

17 Riva, ibidem

18 "Non ci sarà più il senso di consapevolezza di sperimentare. Gli esperimenti di realtà mista saranno esperimenti di massa, con l'essere umano ibridato in una nuova specie sociale, che potrà collassare nello spaesamento al primo *blackout* delle centrali di ibridazione digitale" in: Mazzarella, ibidem.

19 Mazzarella, ibidem, p. 48

20 Si veda l'intervista in allegato con Massimo Leone, Prof. Ordinario in Filosofia e Semiotica e direttore del Centro di Studi Religiosi della Fondazione Bruno Kessler di Trento

21 Leoni, ibidem

2.2 Impatto cognitivo

Il fatto nuovo ed eccezionale, che rende il Metaverso un mondo anche distorto, rispetto alle precedenti rivoluzioni tecnologiche, è quella rottura di continuità tra corpo-mente che avviene, tramite l'utilizzo di oggetti tecnologici (visori cuffie sensori) per cui la realtà 'percepita' si trova in un luogo 'altrove' rispetto al corpo che, con i suoi sensi, la percepisce.

Questa frattura nella percezione della realtà assume la dimensione di una vera svolta antropologica. Dalle neuroscienze siamo infatti venuti a comprendere che la realtà, come la definiamo comunemente, è frutto di una decodificazione, da parte del nostro cervello, di stimoli percettivi ad opera dei nostri sensi. In altre parole, quello che pensiamo sia una realtà 'esterna' è invece il frutto di una nostra incredibile attività neurale. Oggi, studiando questi meccanismi neurali si possono riprodurre, attraverso strumenti tecnologici, quelle stesse 'sensazioni' (richiami a storie e memorie personali e rievocazioni inconsce) che a loro volta inducono a comportamenti ed azioni.

La questione che le neuroscienze si pongono è dunque: quante realtà possono esistere? Quelle percepite nei mondi digitali sono di pari status alle realtà percepita nei mondi fisici?

Noi già sappiamo che non esiste un'unica realtà oggettiva nel mondo fisico e che la visione del mondo si costruisce nel nostro cervello, ma anche nel nostro sistema percettivo corporeo ed emozionale. Fino ad oggi ci si confrontava con costruzioni che partivano dai nostri sensi, in ambienti fisici, regolati da leggi e vincoli, non solo biologici e di gravità, ma anche etici e normativi. Nel Metaverso sono invece possibili mondi percettivi che rispondono a leggi e vincoli che vanno oltre i limiti fisici e biologici dell'essere umano[22].

Questo farebbe avanzare il rischio di creare un mondo in cui vige un pensiero unico, visto che le nostre memorie, pensieri e culture si formano sulla base delle esperienze a cui siamo esposti.

Inoltre, il sovraccarico informativo pone la questione di quale sia il limite alla capacita adattiva del nostro cervello. Secondo il Prof. Gallace "il nostro cervello possiede un altissimo livello di plasticità che gli permette di adattarsi a soluzioni nuove (…) possiamo assumere la proprietà di corpi artificiali o virtuali, se un certo numero di criteri sensoriali viene rispettata (…) ma quali conseguenze possono scaturire dall'assumere sembianze diverse?"[23]

Alcuni rischi che Gallace segnala, sono quelli dettati dal sovraccarico delle informazioni che potrebbe rendere l'esperienza nel Metaverso poco appagante, mentre l'assenza di una costanza di

[22] Rimandiamo ad un approfondimento sull'unicità tra mente e corpo e sul ruolo delle emozioni nel recente studio del filosofo Umberto Galimberti, il quale mette in guardia sui rischi di separare mente e corpo, considerando quest'ultimo come mero strumento e non 'soggetto attivo' dell'essere: "nel mondo della mia vita, ogni atto rivela che la mia esistenza è corporea e che il corpo è la modalità del mio apparire" in: Umberto Galimberti *Il libro delle emozioni*, Feltrinelli, (Milano 2021), p.72.

[23] Alberto Gallace 'Cervelli reali in mondi virtuali: psicologia e neuroscienze del Metaverso" in Lorenzo Montagna, *Metaverso*, Mondadori, Milano 2022, p.223.

stimoli ambientali, di cui il nostro cervello ha bisogno per attivare l'attenzione, renderebbe i nostri schemi mentali non più validi per fare previsioni.

Questione che suscita preoccupazioni è anche quella legata a come un'identità digitale modifichi il comportamento di chi l'assume, chiamato anche "effetto Proteus"[24]. Nel Metaverso io posso diventare una persona diversa semplicemente cambiando il mio aspetto fisico, come viene descritto dagli esperimenti in cui alcuni soggetti sono stati fatti entrare nel corpo digitale di Albert Einstein e sono diventati significativamente più intelligenti. La stessa tecnica è stata utilizzata per modificare atteggiamenti razzisti in soggetti che sono entrati in corpi digitali di soggetti di colore.

In pratica il nostro cervello entrando in un corpo differente, modifica in maniera totalmente automatica le proprie simulazioni.

Chiaramente queste nuove possibilità aprono a scenari che possono vedere nel Metaverso applicazioni positive e molto utili, in settori come l'istruzione, la sanità, l'architettura, l'industria[25], ma solleva anche questioni importanti di etica, sicurezza, organizzazione e protezione di questi nuovi ambienti. Inoltre, i dati raccolti nel Metaverso consentono di ottenere informazioni sugli utenti con un'efficacia molto superiore a quella possibile sui social media.

2.3 Governare rischi e potenzialità

Se oggi il Metaverso si propone con il volto del *gaming* e dell'intrattenimento, delle conferenze virtuali con cui Meta fa vedere utenti felici di intrattenersi, esiste un back office operativo di raccolta informazioni compiuto dalle tecnologie che attingono al mondo reale e con cui viene costruito tutto ciò che abita nell'universo virtuale.

Nelle pagini precedenti, in cui abbiamo descritto come si costruisce il Metaverso, abbiamo visto che la 'duplicazione' (fase I) del mondo reale in quello virtuale, porta a disposizione di chi volesse attingerne una mole di dati inimmaginabile. Gli ambienti virtuali, infatti, vengono progressivamente incorporati e connessi a sistemi fisici e reti informatiche (fase II) alzando i rischi di hackeraggio di informazioni su sistemi e strutture del mondo fisico, poiché gli Avatar di edifici e macchinari reali sono rilevabili negli ambienti virtuali.

Considerando poi che, negli universi digitali, le informazioni vengono memorizzate permanentemente, le ripercussioni a danno della sicurezza degli utenti e anche nazionale potrebbero essere anche più gravi che nel mondo reale. In caso di attacchi al funzionamento del sistema, infatti,

[24] Si veda l'intervista in allegato con Andrea Gaggiolo, Professore Ordinario di Psicologia Generale Direttore dell'International Master in User Experience Psychology presso l'Università Cattolica di Milano.

[25] Si veda lo Studio commissionato dal governo francese in https://www.vie-publique.fr/rapport/286878-mission-exploratoire-sur-les-metavers in cui si analizzano limiti e potenzialità ritenuti utili da approfondire per la Francia, soprattutto in ambito del patrimonio culturale, le arti, la formazione, le infrastrutture, condotto sulla base di interviste ai principali soggetti nei diversi settori.

a rischio sarebbe l'integrità del sistema stesso con un costo complessivo del danno subito maggiore di quanto esso sarebbe nell'attuale ecosistema digitale[26].

Chi e come governare questi spazi è una domanda che sta ponendo serie preoccupazioni alle istituzioni pubbliche[27].

Il Metaverso richiede di essere affrontato con un approccio scientifico umanistico e regolatorio, all'altezza della svolta epocale che esso porterà in tutti gli ambiti di vita e di lavoro. Un approccio che vada oltre le posizioni pro o contro che Umberto Eco ha raccontato nel suo libro "Apocalittici ed Integrati" del 1964, valide anche oggi, in cui di fronte alle innovazioni tecnologiche la popolazione tende a dividersi tra chi ne è entusiasta e chi oppone il rifiuto.

Sul Metaverso è importante avere uno sguardo bifocale, scandagliandone le ambiguità di fondo. Innanzitutto, quella che vede il Metaverso diventare uno spazio *off-limits* per tutti, proprio in virtù del fatto che ciò che succede in questi mondi sintetici non è condizionato da vincoli (biologici, fisici, giuridici) permettendo così di esprimere una creatività che sarebbe inimmaginabile nel mondo fisico. Esso, quindi, diventa uno spazio dove esistere oltre i propri aspetti fisici, dove creare nuove estetiche, poiché tutto diventerà in 3D, dove muoversi con una multicanalità che darà vita a nuove economie e finanze, basati su contratti trasformati in NFT, con ogni *asset* fisico che dovrà avere un gemello digitale aperto e dipendente, unitamente a fornitori e clienti.

Uno degli effetti prospettati sarà la de-centralizzazione delle economie e della proprietà, fino ad oggi salvaguardata dal ruolo degli Stati, nel Metaverso si sposterà ad essere de-centralizzata, con utenti protagonisti e non solo spettatori. Vi è una "connotazione libertaria" in una parte dello sviluppo del Metaverso che lo identifica e sviluppa come un mondo parallelo non necessariamente sregolato, ma regolato secondo principi locali e tecnologici più che globali e giuridici[28].

Questo *spazio-off* potrà diventare un mondo parallelo utile per sperimentare e simulare ciò che nella realtà è solo ipotetico o rischioso (economicamente o per la sicurezza) come per esempio: testare un macchinario o un prodotto prima di produrlo, addestrare in territori difficili ricostruiti virtualmente, operare con la telemedicina a distanza in aree di conflitto.

Tuttavia, proprio queste enormi potenzialità destano grandi preoccupazioni per la sicurezza nazionale[29].

---

[26] Fabio Vanorio, Ministro Consigliere presso Nato Defense College https://www.strategicstudies.it/wp-content/uploads/2021/12/Edizioni-Machiavelli-Metaverso-e-Sicurezza-Nazionale.pdf

[27] Cogliendo l'urgenza di entrare in campo per padroneggiare le potenzialità di questa trasformazione, l'Unione europea ha lanciato un vero Piano dell'Europa nel Metaverso, mentre già nel giugno 2020, la Nato istituì l'*Advisory Group on Emerging and Disruptive Technologies* al fine di monitorare tali tecnologie.

[28] Intervista in allegato con Massimo Leoni

[29] "L'uso delle tecnologie AR/VR può avere gravi implicazioni per la Sicurezza Nazionale" scrive Vanorio: https://www.strategicstudies.it/wp-content/uploads/2021/12/Edizioni-Machiavelli-Metaverso-e-Sicurezza-Nazionale.pdf

Se infatti le tecnologie di realtà aumentata diventano strumenti impiegabili per arricchire la realtà fisica di informazioni utili per svolgere compiti complessi, la *virtual reality* va a sostituire completamente il mondo reale con un universo sintetico parallelo, guidato da tecnologie intelligenti che apprendono e pensano in modo indipendente.

Questa alterazione e distorsione della realtà, senza una adeguata sicurezza, può benissimo diventare uno strumento offensivo e manipolatorio a danno di cittadini, aziende, stati. I *deep fake* nel futuro Metaverso potranno sostituirsi alla realtà senza possibilità di dimostrazione del contrario. Già oggi, infatti, un'immagine, video o audio falsificati, costruiti con Intelligenza Artificiale (IA), non sono più riconoscibili ad occhio umano se non attraverso altri strumenti di IA più avanzata. Questo significa che si possono dirottare verso personale militare o civile, in situazioni di crisi, informazioni logistiche distorte difficili da riconoscere.

Un pervasivo controllo sugli individui può venir esercitato grazie alla raccolta di dati personali e sui comportamenti degli utenti, in parte ottenute in tempi reali dagli utenti stessi e in parte rilevati dalle tecnologie (per esempio l'*eye tracking* oramai integrato in molti visori in combinazione con altre misure biometriche) con cui agiscono le già note tecniche di profilazione, di personificazione, manipolazione della fiducia, persuasione e comunicazione verbale e sensoriale.

2.4 Verso un controllo della Tecnica?

Oggi l'essere umano è già stato largamente superato dalla potenza delle Tecnica, sia come capacità di immagazzinare dati e informazioni sia per la memoria, rilevazione ed elaborazione di ogni comportamento e linguaggio.

Siamo pienamente nello scenario prospettato dal filosofo Emanuele Severino quando diceva che la Tecnica è destinata al dominio in parte perché la Filosofia del nostro tempo non pone alcun limite assoluto alla Tecnica:

"Nel suo insieme la Tecnica non è una macchina come le altre, e quindi sostituibile. Nel suo insieme, la Tecnica è l'incessante e insostituibile processo di sostituzione degli strumenti disponibili (tra cui gli individui umani) con altri più potenti, la cui messa in opera è resa possibile dall'incessante avanzamento delle conoscenze scientifiche[30]".

Il Metaverso sembra dunque rappresentare quel 'punto di svolta' preconizzato da Severino di non ritorno, dove si compie quel "rovesciamento" dove la Tecnica da Strumento diventa Scopo, ovvero forza ordinatrice mossa dalla volontà del proprio accrescimento, senza più limiti né vincoli.

"È la Tecnica, su cui si basa la forza politica, economica e militare a servirsi sempre di più degli Stati per accrescere la propria potenza, non il contrario. In questo processo, l'apparato scientifico-

[30] Emanuele Severino, Macigni e Spirito di Gravità. Riflessioni sullo stato attuale del mondo, Rizzoli, 2010. Pag. 115

tecnologico si costituisce come Superstato, che va lasciandosi alle spalle la politica, lo Stato e i loro conflitti"[31].

La Tecnica, nelle riflessioni di Severino, sembra dunque capace di illudere le forze culturali a servirsene come mezzo. In realtà, a pagarne il prezzo – ammonisce Severino – saranno gli stessi Stati, "che pensano di fronteggiarsi tra di loro servendosi della potenza della Tecnica, in realtà la loro lotta rimane di retroguardia"[32].

Il superamento in potenza della tecnica sulle capacità umane, già avvenuta nel nostro presente, secondo il filosofo sembra richiedere di trovare valori che sostanzino la direzione e diano scopi all'evoluzione del percorso umano, anche nel suo rapporto con la Tecnica, con un apparato filosofico e culturale che renda capace la società di 'dare senso' al mondo.

2.5 Impatto economico: chi si sta muovendo verso il Metaverso

Capire chi si sta muovendo verso il Metaverso e quali sono gli investimenti in campo ci dà una misura della sua valenza strategica. Secondo Bloomberg le dimensioni del mercato del Metaverso dovrebbero raggiungere gli 800 miliardi di dollari entro il 2024 e circa 2,5 trilioni di dollari entro il 2030.

ll meta-universo, pur non essendo definibile come una nuova "economia virtuale", contribuirà alla crescita del manifatturiero (dove gli ambienti 3D offrono spazi di progettazione ideali per una prototipazione rapida ed il decentramento degli spazi di produzione), di logistica e trasporti (con l'intelligenza artificiale che offre piattaforme virtuali per lo sviluppo e test del comportamento di macchine autonome da trasporre nel mondo reale)[33].

"Il 2023 sarà l'anno che indicherà se il Metaverso diventerà realtà" secondo *Economist*[34]. Per ora sappiamo che il 2023 vedrà le *big tech firm* lanciarsi su due nuove strade: la prima, quella delle cuffie virtuali – (VR) e di Realtà-Aumentata (AR), con cui dai telefonini si passerà agli oggetti facciali e da indossare; la seconda strada, quella del Metaverso, che vedrà il passaggio da un Internet bi-dimensionale (basata su testi, immagini e video) ad una tridimensionale ed immersiva, da vivere come un *video-game* globale permanente e continuo[35].

Secondo l'*Economist*[36] molte aziende tech globali stanno investendo sulle realtà virtuale e su nuovi modelli di cuffie virtuali. Meta, che in questo settore di mercato ha una posizione di assoluto

[31] Ibidem p.33
[32] Ibidem p.56
[33] Vanorio, ibidem
[34] Tim Cross 'Is the Metaverse coming?" in The Economist 'The world ahead 2023' The Adephi, 11 novembre 2022 pag. 134. Tim Cross è il Technology and Society Editor per l'Economist.
[35] Ibidem
[36] Tim Cross, ibidem

rilievo e nel 2021 è uscita con il suo ultimo modello – Quest.Pro, ad un costo ancora poco competitivo, nel 2023 offrirà prodotti più accessibili, offrendo entrambe le performance di AR e VR. Apple, *leader* nel mondo degli *smartphone*, uscirà nel 2023 con il suo primo prodotto di cuffie virtuali AR/VR, mentre Sony, che guida la partita dei *video game* con le sue Playstation dalle cuffie VR lanciate nel 2016, uscirà con un modello avanzato.

Sul Metaverso la società Meta ha già dichiarato le proprie ambizioni di guidare lo sviluppo producendo non solo hardware VR ma anche i mondi virtuali nei quali i suoi utenti vorranno abitare. Il cambio del nome operato nel 2021 dal suo CEO Mark Zuckerberg è stato un chiaro messaggio in quella direzione. Per quanto la scelta di Zuckerberg sia stata vista inizialmente come un tentativo di *rebranding*, dopo alcuni episodi che hanno coinvolto negativamente la compagnia negli ultimi anni, quel che è certo è che il cambio di nome di Facebook ha contribuito a portare l'attenzione dell'opinione pubblica (e non solo) sul Metaverso. Da allora l'azienda ha già investito più di 27 miliardi di dollari sull' idea lanciata attraverso visioni di Avatars dei propri utenti che socializzano e fanno amicizie in ambienti virtuali, mentre si tengono conferenze, lezioni o fanno sport.

CAPITOLO 3
I PROFILI ETICO-GIURIDICI DEL METAVERSO

3.1 Premessa – La regolamentazione della tecnica tra legge e diritto.

Grazie all'evoluzione tecnologica, lentamente prima ma poi, e tuttora, in maniera rapida e senza interruzione alcuna, la società ha iniziato a modificare le proprie abitudini. Da ultimo, gli effetti della rivoluzione digitale hanno radicalmente mutato i paradigmi, il modo di relazionarsi, di agire, lavorare e finanche pensare, investendo naturalmente la sfera giuridica.

La combinazione di digitalizzazione e globalizzazione ha generato una rivoluzione democratica perché l'informazione è divenuta accessibile a tutti[37], smaterializzando ogni vincolo di distanza, tempo o quantità. Essa ha offerto alla società dell'informazione[38] opportunità di sviluppo e di benessere generalizzato, rendendola tuttavia vulnerabile.

Inteso quale tecnica di organizzazione delle relazioni sociali, il diritto è tradizionalmente chiamato a gestire questi fenomeni, attraverso la sintesi delle esigenze sottese, indirizzandoli per garantire lo sviluppo sociale.

Se è assodato che il sistema giuridico si evolve per regolare le situazioni nuove, di fronte all'affermarsi dell'intelligenza artificiale[39] e della nuova dimensione del Metaverso occorre chiedersi se il diritto riesce ancora a regolare la tecnica, fissando con precisione i confini entro i quali svilupparsi ed i fini da perseguire[40]. Il rischio è che il diritto non si adegui (o non lo faccia tempestivamente) a questo passaggio, che non è inedito perché si ripropone ciclicamente ad ogni salto tecnologico impattante sulla società.

L'avvento dell'informatica ha infatti già stravolto i tradizionali canoni delle scienze giuridiche a partire dalla fine degli anni '80. Le nuove tecnologie hanno stimolato riletture aggiornate della libertà di informazione, comunicazione, associazione, riunione iniziativa economica privata nonché

---

[37] Principio affermato, in ambito G8, nella *Carta di Okinawa sulla società mondiale dell'informazione* del 21 luglio 2000: "*Chacun, où qu'il se trouve, doit avoir les moyens de participer à la société mondiale de l'Information et personne ne doit en être exclu*».

[38] Si veda il rapporto «*L'Europa e la società dell'informazione globale. Raccomandazioni al Consiglio europeo*» presentato il 26 maggio 1994, intitolato dal Gruppo di lavoro presieduto da Martin Bangemann, Commissario europeo per le telecomunicazioni.

[39] Sul punto, il preambolo della proposta della Commissione europea di regolamento sull'intelligenza artificiale riconosce che "l'intelligenza artificiale è una famiglia di tecnologie in rapida evoluzione che richiede nuove forme di sorveglianza regolamentare e uno spazio sicuro per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi" (n. 71).

[40] Si assiste all'"impotenza del diritto ad ordinare, nel senso vero e proprio di dare ordine, lo sviluppo e l'evolversi della tecnica, dell'informatica, dell'utilizzo di internet. Il diritto insegue faticosamente la tecnica. È proprio la pervasività totalizzante di internet nella società civile a rendere impossibile una compiuta e concreta disciplina". CLARIZIA R., *Internet: gli interrogativi del civilista*. Atti digitali del convegno gli stati generali del diritto di internet, Luiss 16-18.12.2021.

quelle politiche[41]. In questo contesto, sono apparse nuove forme di manifestazioni del consenso per la conclusione dei contratti[42], al documento cartaceo è stato affiancato quello informatico, alla firma autografa quella digitale, al domicilio fisico quello informatico[43] e da ultimo sono entrate nella quotidianità termini come identità digitale, commercio elettronico e moneta virtuale. Seguendo questa progressione è allora possibile immaginare, accanto a quello tradizionale, l'esistenza di un territorio virtuale quale luogo di esplicazione delle libertà?

Se quest'immaginazione è divenuta realtà con il Metaverso, occorre ancora chiedersi a chi spetta disciplinare le dinamiche interne e come garantirne l'ordinato svolgimento. Accanto agli scenari principalmente connessi alla *Cyber Warfare*, si può realmente considerare avveniristica l'ipotesi che l'art. 7-*bis* (Concorso delle Forze armate nel controllo del territorio) del D.L. 23.05.2008, n. 92[44] possa costituire un modello per fronteggiare quelle specifiche ed eccezionali esigenze di prevenzione e contrasto della criminalità e del terrorismo, "ove risulti opportuno un accresciuto controllo del territorio", ivi compreso quello virtuale?

Occorre a questo punto chiedersi cosa succederebbe se il diritto perdesse il suo "tradizionale ruolo di strumento di regolazione dei conflitti umani non riuscendo a comprendere né a definire in modo tradizionale ambiti e forme di regolazione, tanto più se questi debbono svolgersi in un contesto senza confini in uno spazio Cyber definito e ricompreso nelle piattaforme di servizio?". La risposta deve considerare la differenza tra legge e diritto, essendo soltanto la prima ontologicamente legata alla dimensione dello Stato nonché ai limiti territoriali della sua sovranità. Se il diritto non soffre

[41] È stata finanche affermata una nuova declinazione di libertà, quella informatica, divenuta con Internet "una pretesa di libertà in senso attivo, non libertà da ma libertà di, che è quella di valersi degli strumenti informatici per fornire e ottenere informazioni di ogni genere". Così FROSINI T.E., *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informazione e dell'informatica,* 3/2020, pag. 467. Si veda l'art. 19 della Dichiarazione Universale dei Diritti dell'Uomo a norma del quale "ogni individuo ha diritto alla libertà di […] ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere".

[42] Internet ha aperto "nuove frontiere al diritto dei contratti, nel cui panorama ha fatto irruzione […] il fenomeno del commercio elettronico. Fenomeno che ha portato con sé la fattispecie del contratto concluso on-line e le sue successive, molteplici e sempre più sofisticate declinazioni (dal contratto a conclusione telematica al contratto virtuale in senso stretto)". Così CAPO G., *Internet, impresa, contratti*. Atti digitali del convegno gli stati generali del diritto di internet, *cit.*

[43] Tale adeguamento ha contrapposto prospettive culturali che hanno proclamato, da una parte, l'emersione di nuovi beni giuridici, dall'altra, la necessità di adeguare i reati esistenti a nuove modalità di aggressione di beni giuridici tradizionali. Si prenda ad esempio l'accesso abusivo al sistema informatico, incriminato dall'art. 615-*ter* c.p. come introdotto dalla legge 23.12.1993, n. 547 (legge Conso). I lavori parlamentari hanno individuato il "domicilio informatico", nuovo bene giuridico che replica la medesima logica del domicilio fisico, garantito dall'art. 14 Cost., entrambi proiezioni (dapprima spaziale e poi virtuale) della libertà personale. Si veda NUNZIATA M., *Il reato di accesso abusivo in un sistema informatico o telematico*, Ponte Nuovo Editrice, Bologna, 1996.

[44] Recante misure urgenti in materia di sicurezza pubblica, convertito in legge, con modificazioni, dall'art. 1, comma 1, della legge 24.07.2008, n. 125. Si tratta dell'operazione "Strade Sicure", avviata nel 2008 e da ultima prorogata dalla legge 30.12.2020, n. 178, che ha previsto l'impiego del personale delle Forze armate, che agisce con le funzioni di agente di pubblica sicurezza, anche in relazione alle straordinarie esigenze di prevenzione e contrasto della criminalità e del terrorismo.

necessariamente tali limiti (basti pensare all'esperienza globalizzata della *lex mercatoria*[45]), questa può comunque non essere una buona notizia, per il rischio del proliferare di regimi privati che realizzeranno un diritto senza Stato[46]: quale saranno gli obiettivi perseguiti e come si concilieranno gli interessi economici coi diritti fondamentali[47]?

Al fine di indirizzare lo sviluppo dell'intelligenza artificiale[48], è necessario il protagonismo degli Stati e l'impegno delle Organizzazioni internazionali[49] per ottenere discipline essenziali e dall'applicazione quanto più universale possibile.

Questa voglia di protagonismo è finalmente presente nell'ultimo programma politico della Commissione Europa[50], che mira ad "un'Europa più ambiziosa nello sfruttare le opportunità dell'era digitale in un contesto che garantisca la sicurezza e rispetti l'etica [per] conseguire una sovranità tecnologica in alcuni settori tecnologici fondamentali". In questo contesto, la Commissione Europea ha infatti presentato una proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (COM(2021) 206 final)[51], con la quale l'Unione persegue l'interesse di preservare la propria leadership tecnologica e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione.

---

45 Complesso di regole, di natura prevalentemente consuetudinaria o elaborate dalla giurisprudenza arbitrale, destinato a disciplinare i contratti commerciali internazionali e i rapporti a essi sottesi (voce Treccani).

46 La capacità delle piattaforme digitali di orientare i comportamenti degli utenti introduce la criticità di una dimensione giuridica privata. Il riferimento è alle regole imposte da Google, Amazon, Apple, Microsoft e Facebook per fruire dei propri servizi. Sul tema si vedano CELOTTO A., *Facebook sta diventando uno Stato? Una paradossale retrocessione: da cittadini statali a sudditi digitali*, in Huffingtonpost.it, 05.01.2021, nonché MONTI A., *Musk, Twitter e il potere di comprare il diritto*, in Repubblica.it, 05.05.2022.

47 Sul punto è significativo il passaggio del piano "People, technologies & infrastructure – Europe's plan to thrive in the metaverse I Blog of Commissioner Thierry Breton 14.09.2022, con l'affermazione che "i metaversi privati dovrebbero svilupparsi sulla base di standard interoperabili e nessun singolo attore privato dovrebbe detenere la chiave della piazza pubblica o stabilirne i termini e le condizioni. […] l'Europa dispone ora di strumenti normativi solidi e a prova di futuro per lo spazio digitale. Abbiamo anche imparato una lezione da questo lavoro: non assisteremo a un nuovo Far West o a nuovi monopoli private".

48 L'art. 41 della Costituzione riconosce la libertà dell'iniziativa economica privata, ma ne vieta lo svolgimento in modo da recare danno alla salute, alla sicurezza, alla libertà ed alla dignità umana.

49 In questa prospettiva, il primo e finora unico trattato internazionale che affronta il tema di internet è la Convenzione del Consiglio d'Europa sulla criminalità informatica, siglata a Budapest il 23.11.2001. La Convenzione tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la Cybercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale. Alla data del 09.12.2022 vi sono state 68 ratifiche/adesioni da parte di Stati membri e non membri. A ragione della valenza regionale del Consiglio d'Europa, sarebbe opportuno che la materia fosse disciplinata da un trattato universale su iniziativa delle Nazioni Unite.

50 COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA COMUNICAZIONE, LEYEN U., *Un'Unione più ambiziosa. Il mio programma per l'Europa: orientamenti politici per la prossima Commissione europea 2019-2024*, 2019. Nel documento si afferma che "la digitalizzazione e il ciberspazio sono due facce della stessa medaglia. In questo ambito è necessario un ripensamento concettuale: dobbiamo passare dal principio della «necessità di sapere» a quello della «necessità di condividere».

51 La base giuridica della proposta è costituita innanzitutto dall'art. 114 del Trattato sul funzionamento dell'Unione europea (TFUE), che prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno.

L'ulteriore iniziativa dell'Unione europea riguarda l'annuncio della prossima regolamentazione del Metaverso[52] con lo scopo di promuovere i mondi virtuali nel segno delle persone, tecnologie e infrastrutture.

3.2 Tecnica e diritto. La prospettiva antropocentrica

La mancanza di un consolidato retroterra normativo impone di ripensare radicalmente l'esperienza giuridica per disciplinare l'intelligenza artificiale, avendo sempre a mente che *omne ius causa hominum constitutum est*: il diritto è funzionale all'Uomo, l'esperienza giuridica ne presuppone la centralità e la sua dignità è il limite insuperabile per lo sviluppo tecnologico. Questo ripensamento deve quindi assumere la dignità della persona umana non soltanto quale diritto fondamentale in sé[53], ma come fondamento dei diritti fondamentali. "Il concetto di dignità umana racchiude l'idea che ogni essere umano possiede un "valore intrinseco", che non deve mai essere svilito, compromesso o represso dagli altri e nemmeno dalle nuove tecnologie". Il rispetto per la dignità umana impone che le persone non siano trattate "come semplici oggetti da vagliare, catalogare, valutare per punteggio, aggregare, condizionare o manipolare" e che i sistemi di intelligenza artificiale siano "sviluppati in modo che rispettino, servano e proteggano l'integrità fisica e psichica degli esseri umani, il senso di identità personale e culturale e la soddisfazione dei bisogni essenziali"[54].

In presenza di un quadro di riferimento chiaro e completo per conseguire l'affidabilità dell'intelligenza artificiale, l'affermarsi di queste nuove tecnologie richiede fiducia[55], che potrà aversi soltanto se democrazia, Stato di diritto e i diritti fondamentali siano alla base dei sistemi di IA.

Dignità umana e fiducia sono pertanto precondizioni dello sviluppo tecnologico da approfondire sul piano dell'etica perché l'uso di qualsiasi tecnologia potente impatta sulle persone e sulla società. In questa prospettiva, gli orientamenti etici per un'intelligenza artificiale affidabile[56] individuano, quali caratteristiche dell'intero ciclo di vita di un sistema d'intelligenza artificiale:

- legalità: l'IA deve rispettare le leggi ed i regolamenti applicabili;

---

52 People, technologies & infrastructure. Europe's plan to thrive in the metaverse I Blog of Commissioner Thierry Breton. 14.09.2022.

53 Ai sensi dell'art. 1 della Carta dei diritti fondamentali dell'Unione europea "La dignità umana è inviolabile. Essa deve essere rispettata e tutelata".

54 COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLE RETI DI COMUNICAZIONE, DEI CONTENUTI E DELLE TECNOLOGIE, *Orientamenti etici per un'IA affidabile*, 2019, pag. 11.

55 Esigenza evidenziata dalla Commissione europea nella comunicazione sull'intelligenza artificiale per l'Europa (COM(2018) 237 finale), con l'affermazione della necessità di un ambiente improntato a fiducia e responsabilità per lo sviluppo e l'utilizzo dell'IA, e nel libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia (COM(2020) 65 finale).

56 Individuati dal Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018.

- eticità[57]: l'IA deve assicurare l'adesione a principi e valori etici;
- robustezza: dal punto di vista tecnico e sociale poiché, anche con le migliori intenzioni, i sistemi di IA possono causare danni non intenzionali.

Tenuto conto che i diritti fondamentali sono alla base dello Stato di diritto, esprimendo "la dimensione sostanziale o costituzionale della democrazia dato che dettano limiti e vincoli di contenuto"[58] alla legislazione, il rispetto dei diritti fondamentali costituisce il punto di partenza per individuare principi e valori etici astratti rilevanti per lo sviluppo dell'intelligenza artificiale.

3.3 Il rispetto dei diritti fondamentali tra obbligo giuridico ed etica.

La protezione dei diritti fondamentali[59] rimase per lungo tempo relegata tra le Costituzioni dei singoli ordinamenti statali[60]. Soltanto dopo il secondo conflitto mondiale i diritti fondamentali si affermarono anche livello internazionale. In particolare, a partire dalla Dichiarazione Universale dei Diritti dell'Uomo, adottata dalle Nazioni Unite il 10 dicembre 1948, i cui contenuti sono vincolanti perché divenuti nel tempo diritto consuetudinario o richiamati in Trattati a livello universale o regionale[61].

A fronte del pluralismo culturale e ideologico, il carattere universale dei diritti fondamentali offre una base valoriale comune[62] per lo sviluppo dell'intelligenza artificiale. Questa prospettiva spiega la stretta sinergia tra legalità ed eticità quali componenti di un'intelligenza artificiale affidabile.

---

[57] L'etica dell'IA è una branca dell'etica applicata che studia gli interrogativi etici posti dallo sviluppo, dalla distribuzione e dall'utilizzo dell'IA. Il suo interesse principale risiede nell'individuare come l'IA possa favorire o mettere a rischio la felicità degli individui, sia in termini di qualità della vita che di autonomia umana e libertà necessarie per una società democratica. COMMISSIONE EUROPEA, *Orientamenti etici, cit*., pag. 10.

[58] Per FERRAJOLI L., *Sui fondamenti dei diritti fondamentali. Un approccio multidisciplinare*, in *Studi sulla questione criminale*, 2/2010, pag. 15 ss., "nelle democrazie dotate di costituzione rigida e del controllo giurisdizionale di costituzionalità, perché le norme siano valide non basta il rispetto delle forme della loro produzione. È necessaria altresì, per la loro validità sostanziale, la compatibilità dei loro significati con quelli espressi dalle norme costituzionali [in cui] vengono positivizzati diritti fondamentali e principi di giustizia".

[59] Le espressioni "diritti fondamentali", "diritti umani", "diritti inviolabili" e "diritti costituzionali", impiegate in modo promiscuo ma equivalente, indicano quei diritti che dovrebbero essere riconosciuti ad ogni individuo in quanto tale.

[60] In particolare, i principi fondamentali iscritti agli articoli da 1 a 12 della Costituzione italiana e nella parte prima sui diritti e doveri dei cittadini caratterizzano l'ordinamento costituzionale e i valori elencati assumono in tal modo una valenza giuridica di tale essenzialità, da poter affermare che la stessa organizzazione dei pubblici poteri sia prevalentemente funzionale al loro svolgimento ed alla loro attuazione. Il rispetto dei diritti fondamentali è assicurato anche dalle successive disposizioni che ne garantiscono la prevalenza rispetto alla legislazione ordinaria, quali il meccanismo di adeguamento automatico al diritto internazionale generalmente riconosciuto, previsto dall'art. 10, e la conformità della legislazione ai "vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali" di cui all'art. 117, primo comma.

[61] Tra questi la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, adottata dal Consiglio d'Europa il 4 novembre 1950, i due Patti sui diritti civili e politici e sui diritti economici, sociali e culturali delle Nazioni Unite del 16 dicembre 1966 e, da ultimo, la Carta dei diritti fondamentali dell'Unione europea del 18 dicembre 2000, ciascuno dei quali prevede meccanismi di garanzia del rispetto dei diritti fondamentali.

[62] Sul tema si veda VIOLA F., *Etica dei diritti*, in VIGNA C. (a cura di), *Introduzione all'etica*, Vita e Pensiero, Milano, 2001, pag. 319.

Sotto il primo profilo, in quanto meritevoli di tutela, i diritti fondamentali rientrano nella componente della legalità che impone l'osservanza della legge. Una simile tutela, tuttavia, non è richiesta soltanto nei confronti di qualsiasi operatore (pubblico o privato che sia) dell'intero ciclo di un sistema di intelligenza artificiale, ma anche nei confronti dello Stato nella scelta degli strumenti per assicurare l'ordine pubblico[63] e la sicurezza pubblica[64].

Poiché in uno stato di diritto non tutti i mezzi sono accettabili[65], l'appropriatezza dei mezzi rispetto al fine non è sufficiente a legittimare tali scelte che, proprio nei diritti fondamentali[66], incontrano dei limiti. L'applicazione di sistemi di intelligenza artificiale può legittimamente comprimere i diritti fondamentali in presenza di requisiti di proporzionalità e necessità, essendo tali restrizioni ammesse purché siano previste dalla legge[67] e costituiscano "misure necessarie, in una società democratica, alla pubblica sicurezza, alla protezione dell'ordine, della salute o della morale pubblica, o alla protezione dei diritti e della libertà altrui"[68].

Un esempio del ricorso a sistemi di intelligenza artificiale, giustificato dai parametri di necessità e proporzione, proviene dall'art. 5, primo comma, lett. c) della proposta di regolamento, avuto riguardo all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico[69].

---

63 L'ordine pubblico è il complesso di "quei beni giuridici fondamentali o da quegli interessi pubblici primari sui quali, in base alla Costituzionale e alle leggi ordinarie, si regge l'ordinata e civile convivenza dei consociati nella comunità nazionale. La tutela di questi interessi - fra i quali rientrano l'integrità fisica e psichica delle persone, la sicurezza dei possessi e il rispetto o la garanzia di ogni altro bene giuridico di fondamentale importanza per l'esistenza e lo svolgimento dell'ordinamento - rappresenta il nucleo delle funzioni di polizia di pubblica sicurezza [attribuite] in via esclusiva allo Stato". Così Corte Cost., sent. 25.02.1988, n. 218: www.cortecostituzionale.it.

64 Al di là della sua interpretazione minima coincidente con l'incolumità fisica, la sicurezza pubblica è quella situazione in cui è assicurato ai cittadini "il pacifico esercizio di quei diritti di libertà che la Costituzione garantisce con tanta forza. Sicurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale; è l'"ordinato vivere civile", che è indubbiamente la meta di uno Stato di diritto, libero e democratico". Così Corte Cost., sent. 14.06.1956, n. 2: www.cortecostituzionale.it.

65 "Questo è il destino della democrazia, poiché non tutti i mezzi sono accettabili per essa e non tutti i metodi impiegati dai suoi nemici sono aperti ad essa. A volte, una democrazia deve combattere con una mano legata dietro la schiena". Così B. AHARON, Foreword: A Judge on Judging: The Role of a Supreme Court in a Democracy, in Harvard Law Review, vol. 116, 16, 2002, pag. 18.

66 Si veda SORBELLO P., I diritti fondamentali come limite alla politica criminale, in Riv. Guardia di Finanza, 6/2014, pag. 1754 ss.

67 Alla riserva di legge può essere affiancata quella di giurisdizione, come prevede l'art. 13 Cost.

68 Sono i motivi di ordine generale che, ai sensi della Convenzione EDU, legittimano le restrizioni applicabili, a norma dell'art. 18, "solo allo scopo per cui sono state previste". In senso conforme, l'art. 52 (Portata dei diritti garantiti) della Carta dei diritti fondamentali dell'Unione europea.

69 Articolo 5: "1.Sono vietate le pratiche di intelligenza artificiale seguenti: […] c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto […] in cui il punteggio sociale così ottenuto comporti […] d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi: i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'art. 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio […]". Per l'approfondimento si veda Della Torre J., Quale spazio per i tools di riconoscimento facciale nella giustizia penale? in Di Paolo G. – Pressacco L. (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove e giudizio*, Università degli Studi di Trento, Quaderni della Facoltà di Giurisprudenza, 63, 2022, pag. 7.

Quanto al secondo profilo, proprio perché connaturati all'essere umano in quanto tale, i diritti fondamentali costituiscono la base per la componente etica dell'intelligenza artificiale. Nell'approssimativa ricerca di un suo significato, l'etica si presenta come sistema di valori[70], assunto da una società in un dato momento storico, e descrive l'insieme prescrittivo di regole comportamentali. La regola etica, tuttavia, non necessariamente coincide con quella giuridica e, pertanto, alla sua violazione può non seguire una sanzione, per lo meno giuridica. Il problema emerge in maniera più chiara allorquando l'osservanza della norma etica comporta l'infrazione di quella giuridica, con il conseguente interrogativo su quale sia la norma giusta[71]. In estrema sintesi, la questione ruota intorno all'esistenza di un'esperienza giuridica al di fuori della dimensione statale: esiste diritto al di fuori della legge dello Stato, una regola la cui osservanza è avvertita quale doverosa, anche se non imposta o finanche vietata dalla legge?

Sul piano del positivismo giuridico e del pluralismo culturale la risposta è negativa, ma l'esito è diverso nella prospettiva giusnaturalistica del diritto non scritto[72]: nel momento in cui l'etica incontra i diritti umani, "la violazione del diritto avvenuto in un punto della terra è avvertita in tutti i punti"[73]. All'universalità del sistema di valori connaturato all'essenza dell'uomo segue la doverosità delle regole ad esse improntate.

---

[70] Nella prospettiva dell'etica improntata alla religione "ciò si è verificato esemplarmente nella storia culturale dell'occidente fintanto che il monoteismo della religione cristiana si è espresso. […] La rottura dell'unità cristiana e l'emersione del classicismo rinascimentale […] aprirono le porte a quella concezione laica del giusnaturalismo che doveva fondare l'etica dell'umanesimo […] L'etica, dunque, che aveva incrociato il diritto naturale, ha così incrociato, in immediata derivazione, l'intera tematica dei diritti umani [divenendo] patrimonio comune dei paesi occidentali". Così FALZEA A., *Ricerche di teoria generale del diritto e di dogmatica giuridica*, Giuffré, Milano, III, 2010, pag. 330.

[71] Significativo la figura della giovane Antigone, protagonista della tragedia di Sofocle, che sfida il potere fino alla morte pur di assicurare al corpo del fratello Polinice la sepoltura che Creonte, il re di Tebe, non vuole concedere per motivi politici: "i tuoi bandi io non credei che tanta forza avessero da far sì che le leggi dei Celesti, non scritte, ed incrollabili, potesse soverchiare un mortal: ché non adesso furon sancite, o ieri: eterne vivono esse; e niuno conosce il dí che nacquero", richiamato in FASSÒ G., *Il diritto naturale*, Eri, Torino, 1964, pag. 6.

[72] Un esempio si riviene all'art. 7 (*nulla poena sine lege*) della Convenzione EDU, il cui secondo comma dispone che il principio di legalità "non ostacolerà il giudizio e la condanna di una persona colpevole di una azione o di una omissione che, al momento in cui è stata commessa, costituiva un crimine secondo i principi generali di diritto riconosciuti dalle nazioni civili".

[73] Così KANT I., *Per la pace perpetua*, Feltrinelli, Milano, 1991, pag. 53 ss., per cui "l'idea di un diritto cosmopolitico non è una rappresentazione fantastica di menti esaltate, ma il necessario coronamento del codice non scritto".

Sulla base di queste riflessioni, il citato Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale[74] ha sintetizzato quattro principi (o imperativi) etici[75] ai quali occorre aderire per "garantire che i sistemi di IA siano sviluppati, distribuiti e utilizzati in modo affidabile":

- rispetto dell'autonomia umana[76]: "gli esseri umani che interagiscono con i sistemi di IA devono poter mantenere la propria piena ed effettiva autodeterminazione e devono poter essere partecipi del processo democratico. I sistemi di IA non devono subordinare, costringere, ingannare, manipolare, condizionare o aggregare in modo ingiustificato gli esseri umani. Al contrario, devono essere progettati per aumentare, integrare e potenziare le abilità cognitive, sociali e culturali umane. La distribuzione delle funzioni tra esseri umani e sistemi di IA dovrebbe seguire i principi di progettazione antropocentrica";
- prevenzione dei danni[77]: "I sistemi di IA non devono causare danni né aggravarli e neppure influenzare negativamente gli esseri umani, per cui occorre tutelare la dignità umana nonché l'integrità fisica e psichica. I sistemi di IA e gli ambienti in cui operano devono essere sicuri e protetti. […] Le persone vulnerabili dovrebbero ricevere maggiore attenzione ed essere incluse nello sviluppo e nella distribuzione dei sistemi di IA. Occorre prestare particolare attenzione anche alle situazioni in cui i sistemi di IA possono causare o aggravare gli effetti negativi dovuti ad asimmetrie di potere o di informazione, come ad esempio tra datori di lavoro e dipendenti, imprese e consumatori o governi e cittadini".

---

74 L'art. 56 della proposta di regolamento istituisce il comitato europeo per l'intelligenza artificiale.

75 Si veda anche la Risoluzione del Parlamento europeo del 20.10.2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate: "2. Qualsiasi nuovo quadro normativo in materia di IA che preveda obblighi giuridici e principi etici per lo sviluppo, la diffusione e l'utilizzo dell'IA, della robotica e delle tecnologie correlate dovrebbe rispettare pienamente la Carta e rispettare di conseguenza la dignità umana, l'autonomia e l'autodeterminazione dell'individuo, impedire i danni, promuovere l'equità, l'inclusione e la trasparenza, eliminare le distorsioni e la discriminazione, anche per quanto riguarda le minoranze, e rispettare i principi della limitazione degli effetti esterni negativi nelle tecnologie utilizzate, della spiegabilità delle tecnologie e la garanzia che le tecnologie siano al servizio delle persone e non siano intese a sostituirle o a decidere per loro, con il fine ultimo di accrescere il benessere umano di ognuno".

76 Il rispetto dell'autonomia umana investe il diritto alla dignità umana e la libertà di cui agli artt. 1 e 6 della Carta dei diritti fondamentali UE. Sul punto, l'art. 14 (sorveglianza umana) della proposta di regolamento impone che "i sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso. 2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere […]".

77 La prevenzione dei danni è strettamente connessa alla protezione dell'integrità fisica e psichica sancita dall'art. 3 della Carta dei diritti fondamentali UE. In merito, ai sensi dell'art. 15 (accuratezza, robustezza e cibersicurezza) della proposta di regolamento, "1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire, alla luce della loro finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita. […] 3.I sistemi di IA ad alto rischio sono resilienti per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi. La robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza […]". In tale contesto, a partire dal successivo art. 16, la proposta di regolamento pone specifici obblighi a carico dei fornitori e degli utenti dei sistemi di IA ad alto rischio.

Questo tema porta con sé quello della responsabilità individuale, che si porrà con sempre maggiore forza, mano a mano che l'intervento dell'intelligenza artificiale nel processo decisionale della macchina diverrà più significativo[78].

- equità[79]: lo sviluppo, la distribuzione e l'utilizzo dei sistemi di IA devono essere equi, secondo una duplice accezione di equità, sostanziale e procedurale. "La dimensione sostanziale implica un impegno a garantire una distribuzione giusta ed equa di costi e di benefici e a garantire che gli individui e i gruppi siano liberi da distorsioni inique, discriminazioni e stigmatizzazioni […] Occorre inoltre promuovere le pari opportunità in termini di accesso all'istruzione, ai beni, ai servizi e alla tecnologia. L'utilizzo dei sistemi di IA, inoltre, non deve mai ingannare gli utenti (finali) né ostacolarne la libertà di scelta […]. La dimensione procedurale dell'equità implica la capacità di impugnare le decisioni elaborate dai sistemi di IA e dagli esseri umani che li gestiscono e la possibilità di presentare un ricorso efficace contro di esse";
- esplicabilità[80]: "L'esplicabilità è fondamentale per creare e mantenere la fiducia degli utenti nei sistemi di IA. Tale principio implica che i processi devono essere trasparenti, le capacità e lo scopo dei sistemi di IA devono essere comunicati apertamente e le decisioni, per quanto possibile, devono poter essere spiegate a coloro che ne sono direttamente o indirettamente interessati. Senza tali informazioni, una decisione non può essere debitamente impugnata".

---

78 Sul punto si veda la Risoluzione del Parlamento europeo del 20.10.2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, per cui "7. tutte le attività, i dispositivi o i processi fisici o virtuali che sono guidati da sistemi di IA possono essere tecnicamente la causa diretta o indiretta di danni o pregiudizi, ma sono quasi sempre il risultato della creazione, della diffusione o dell'interferenza con i sistemi da parte di qualcuno; rileva a tale proposito che non è necessario conferire personalità giuridica ai sistemi di IA; è del parere che l'opacità, la connettività e l'autonomia dei sistemi di IA potrebbero rendere, nella pratica, molto difficile o addirittura impossibile ricondurre specifiche azioni dannose dei sistemi di IA a uno specifico input umano o a decisioni adottate in fase di progettazione; ricorda che, conformemente a concetti di responsabilità ampiamente accettati, è tuttavia possibile aggirare tale ostacolo considerando responsabili le varie persone nella catena del valore che creano il sistema di IA, ne eseguono la manutenzione o ne controllano i rischi associati. Si vedano altresì SALVI G., *Attuazione della giurisdizione penale nello spazio virtuale e sicurezza nazionale*. Intervento di apertura dell'anno accademico della Scuola Superiore di Polizia 2022/2023 Roma, 27 ottobre 2022, in *Sistema penale*, nonché PISANI N., *Intelligenza artificiale e criteri di imputazione della responsabilità penale*. Atti digitali del convegno gli stati generali del diritto di internet, *cit.*

79 L'equità è strettamente connessa ai diritti alla non discriminazione, alla solidarietà e alla giustizia sanciti dagli artt. 21 e seguenti della Carta dei diritti fondamentali UE.

80 L'esplicabilità e la responsabilità sono strettamente connesse ai diritti relativi alla giustizia fissati all'art. 47 della Carta dei diritti fondamentali UE. Sul punto, a norma dell'art. 13 (Trasparenza e fornitura di informazioni agli utenti) della proposta di regolamento sulla IA, "I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente".

3.4 Intelligenza artificiale e diritti fondamentali in gioco.

Nel 1950 Isaac Asimov pubblicò "*I Robot*", una raccolta di nove racconti di fantascienza aventi quali protagonisti dei robot positronici che ubbidiscono alle tre leggi fondamentali della robotica, in base alle quali:

1. Un robot non può recar danno a un essere umano, né permettere che, a causa della propria negligenza, un essere umano patisca danno;
2. Un robot deve sempre obbedire agli ordini degli esseri umani, a meno che contrastino con la Prima Legge;
3. Un robot deve proteggere la propria esistenza, purché questo non contrasti con la Prima o la Seconda Legge [81].

Con incredibile capacità avveniristica, le tre leggi fondamentali della robotica ruotano intorno alla centralità dell'uomo e alla strumentalità del robot, anticipando la necessità di regolamentare l'intelligenza artificiale sulla base dell'etica dei diritti fondamentali: una lesione dei diritti fondamentali arreca infatti un danno all'essere umano, vietato dalla prima legge della robotica.

Una volta fissato il punto di convergenza tra legalità ed eticità, occorre individuare il contenuto dei diritti fondamentali[82] che i sistemi di intelligenza artificiale devono rispettare, avuto riguardo tanto al rapporto orizzontale, tra esseri umani, quanto a quello verticale, tra questi e gli organismi sovrani.

Un riferimento essenziale è contenuto nel Preambolo della Carta dei diritti fondamentali dell'Unione europea (di seguito soltanto Carta), per cui "l'Unione si fonda sui valori indivisibili e universali di dignità umana, di libertà, di uguaglianza e di solidarietà; l'Unione si basa sui principi di democrazia e dello stato di diritto. Essa pone la persona al centro della sua azione istituendo la cittadinanza dell'Unione e creando uno spazio di libertà, sicurezza e giustizia", con la precisazione che:

- la dignità umana "racchiude l'idea che ogni essere umano possiede un "valore intrinseco", che non deve mai essere svilito, compromesso o represso dagli altri e nemmeno dalle nuove tecnologie come i sistemi di IA. Nel contesto dell'IA, il rispetto per la dignità umana implica che tutte le persone siano trattate con il rispetto loro dovuto in quanto soggetti morali, piuttosto che come semplici oggetti da vagliare, catalogare, valutare per punteggio, aggregare, condizionare o manipolare. I sistemi di IA devono quindi essere sviluppati in

[81] Tratte dal "Manuale di Robotica, 56^ edizione, 2058 d.c.". Così ASIMOV I., *Io, robot* (trad. it. LATRONICO V.), Mondadori, Milano, 2018.

[82] Si vedano gli Orientamenti etici del Gruppo indipendente, *cit*. Sulla sfida tecnologica che attende il costituzionalismo e su come dare forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica, si veda altresì FROSINI T.E., *Il costituzionalismo nella società tecnologica*, *cit.*, pag. 466.

modo che rispettino, servano e proteggano l'integrità fisica e psichica degli esseri umani, il senso di identità personale e culturale e la soddisfazione dei bisogni essenziali".

La disciplina è contenuta al Capo I "Dignità" (articoli da 1 a 5) della Carta.

- libertà individuale: "gli esseri umani devono rimanere liberi di prendere decisioni importanti per sé stessi. Ciò comporta la libertà dall'intrusione di organismi sovrani, ma richiede anche l'intervento di organizzazioni governative e non governative per garantire che individui o popolazioni a rischio di esclusione abbiano pari accesso ai benefici e alle opportunità offerti dall'IA. Nell'ambito dell'IA, per salvaguardare la libertà individuale occorre ridurre al minimo la coercizione illegittima diretta o indiretta, le minacce all'autonomia mentale e alla salute psichica, la sorveglianza ingiustificata, l'inganno e la manipolazione iniqua".

Essa trova piena declinazione al capo II (articoli da 6 a 19) della Carta.

- uguaglianza, non discriminazione e solidarietà: "si deve garantire pari rispetto per il valore morale e la dignità di tutti gli esseri umani. Ciò va oltre la non discriminazione, che tollera la distinzione tra situazioni diverse sulla base di giustificazioni oggettive. In un contesto di IA, l'uguaglianza implica che il funzionamento del sistema non possa generare risultati ingiustamente distorti (ad esempio, i dati utilizzati per istruire i sistemi di IA dovrebbero essere il più inclusivi possibile e rappresentare gruppi di popolazione diversi)".

La relativa disciplina è contenuta ai Capi III "Uguaglianza" (articoli da 20 a 26) e IV "Solidarietà" (articoli da 27 a 38) della Carta.

- diritti dei cittadini: "i cittadini godono di un'ampia gamma di diritti, tra cui il diritto di voto, il diritto a una buona amministrazione o all'accesso ai documenti pubblici e il diritto di presentare petizioni all'amministrazione. I sistemi di IA possono sostanzialmente migliorare la portata e l'efficienza della fornitura di beni e servizi pubblici alla società da parte dei governi ma, allo stesso tempo, le applicazioni di IA potrebbero avere effetti negativi sui diritti dei cittadini che dovrebbero essere salvaguardati"[83].

Essi sono disciplinati al capo V "Cittadinanza" (articoli da 39 a 46) della Carta.

- rispetto della democrazia, della giustizia e dello Stato di diritto: "tutti i poteri dello Stato nelle democrazie costituzionali devono essere giuridicamente autorizzati e limitati dalla legge. I sistemi di IA devono servire a mantenere e a promuovere i processi democratici e a rispettare la pluralità dei valori e delle scelte di vita degli individui. Essi non devono

[83] A riprova del carattere universale di tali diritti, si precisa che "utilizzando il termine "diritti dei cittadini" non si negano né trascurano i diritti dei cittadini di paesi terzi e delle persone irregolari (o illegali) presenti nell'UE che sono tra l'altro tutelati dal diritto internazionale e quindi godono di diritti anche nel campo dell'IA". Così COMMISSIONE EUROPEA, *Orientamenti etici*, *cit*., pag. 15. Per l'approfondimento si veda MASCOLO A., *L'uso dell'Intelligenza Artificiale nel settore pubblico*, in BONTEMPI V. (a cura di), *Lo Stato digitale nel piano nazionale di ripresa e resilienza*, RomaTre Press, 2022, pag. 171 ss.

compromettere i processi democratici, la decisione umana o i sistemi di voto democratico. Nei sistemi di IA deve essere insito l'impegno a garantire di non operare con modalità che compromettano gli impegni di base su cui si fonda lo Stato di diritto, le leggi e i regolamenti obbligatori e a garantire il giusto processo e l'uguaglianza di fronte alla legge".

La disciplina è contenuta al Capo VI "Giustizia" (articoli da 47 a 50) della Carta dei diritti fondamentali dell'Unione europea.

CAPITOLO 4
GUERRA IBRIDA E DIMENSIONI DELLA CONFLITTUALITA'

4.1 Premessa

"L'eccellenza suprema consiste nel rompere la resistenza del nemico senza combattere". La celebre massima del filosofo e generale cinese Sun Tzu calza perfettamente nella definizione del concetto, relativamente ambiguo, di "guerra ibrida". Il termine, di derivazione puramente occidentale, sebbene fosse utilizzato da tempo nel gergo militare, ha guadagnato prestigio pubblico negli ultimi anni, soprattutto a seguito dell'invasione della Crimea nel 2014.

Nel XXI secolo la guerra convenzionale ha perso il classico carattere di scontro armato tra eserciti nemici retti in certa misura dalle regole del diritto internazionale. Gli effetti delle nuove tecnologie, della rivoluzione digitale e della globalizzazione hanno fatto emergere una struttura complessa, in cui gli avversari ricorrono, in maniera combinata, a mezzi convenzionali e non per raggiungere i propri obiettivi.

Guerra Ibrida, *Hybrid Warfare*, è diventato il termine più comune e di uso corrente in occidente per rappresentare la complessità delle più recenti iniziative militari condotte principalmente da Russia e Cina.

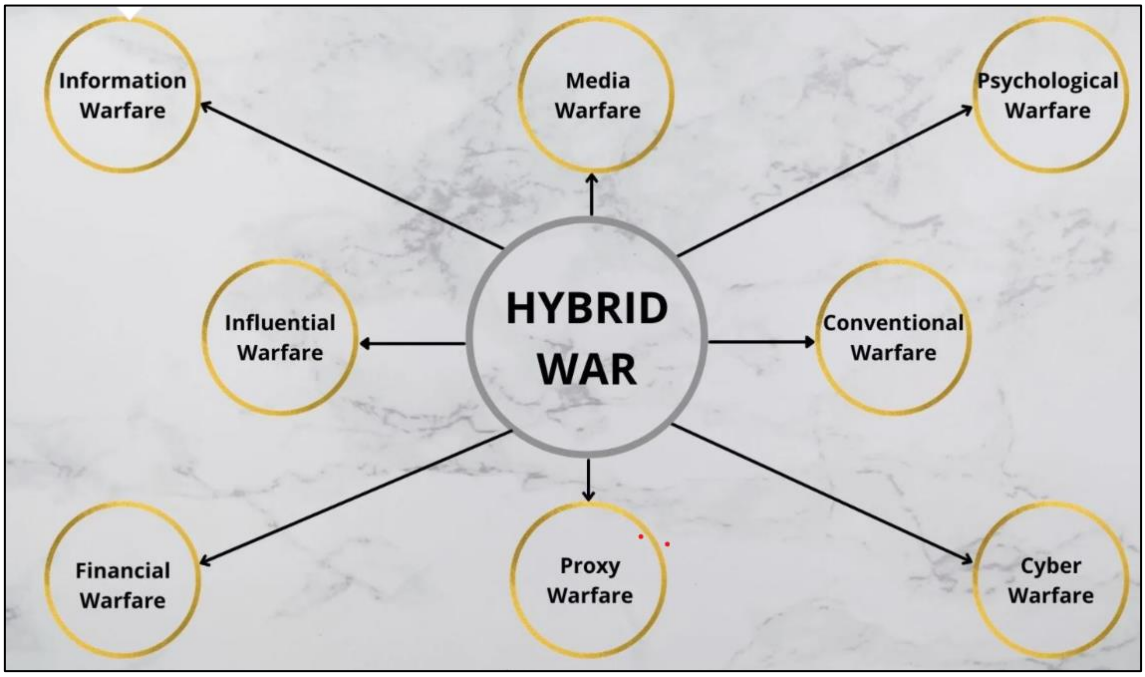
Il tema della guerra ibrida si è prestato a profonde trattazioni dottrinali, che hanno coinvolto la scienza militare delle principali potenze, senza mai giungere ad una determinazione universale. Il problema non è meramente accademico, dal momento che influisce sulla capacità recettiva e difensiva degli Stati, oltre che sull'attribuzione di competenze in materia a specifiche agenzie governative.

Secondo una consolidata interpretazione la guerra ibrida prevede "l'utilizzo di strumenti militari e non-militari in operazioni integrate, dirette all'inganno militare, a conseguire un vantaggio psicologico e materiale utilizzando mezzi diplomatici, pressioni economiche, operazioni di disinformazione (o *Information warfare*), cibernetiche (o *Cyber warfare*), giuridici (o *lawfare*), strumenti elettronici, attraverso operazioni militari e di intelligence condotte sotto copertura per influenzare e manipolare il processo di *decision-making* (o *cognitive warfare*) del proprio avversario"[84].

La guerra ibrida, in sostanza, presenta una sorta di ambiguità strategica. Lo scopo della combinazione di operazioni cinetiche e tattiche statiche è quello di arrecare un maggior danno allo Stato belligerante senza dover dichiarare guerra. Effetto principale che ne deriva è la creazione di

[84] The Military Balance, ed 2015

una zona grigia dove il confine tra guerra e pace è elusivo. Da un lato, le missioni di *Hybrid warfare* si trattengono sempre al di sotto della soglia di guerra, dall'altro, risultano più praticabili e convenienti in termini economici ed umani. L'ambiguità della guerra ibrida, in più, complica sia l'attribuzione giuridica che la risposta materiale.

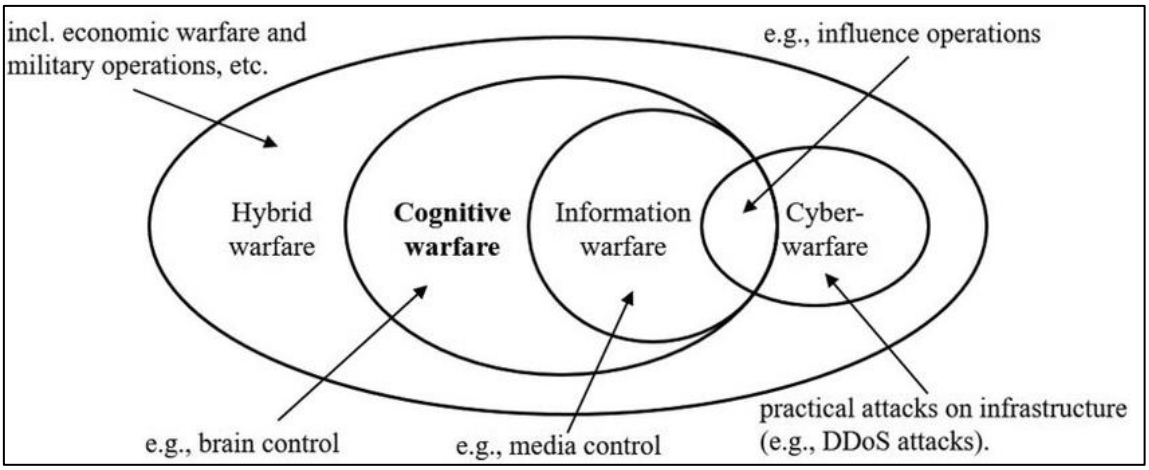


La guerra ibrida non è però una caratteristica dei giorni nostri, ciò che in parte ha caratterizzato la guerra ibrida odierna è la velocità di scambio e soprattutto il consumo delle informazioni e diversi strumenti utilizzabili, tra cui internet ed i social media la cui crescita esponenziale nella società ha aumentato le reti di minacce in patria e all'estero.

Nelle sezioni che seguono si prenderà il concetto di guerra ibrida e le sue minacce con l'obiettivo di contestualizzarne il significato. Inoltre, si fornirà un quadro della relazione concettuale tra *Hybrid warfare* e altri tipi di *warfare* (*Information warfare*, *Cyber warfare* e *cognitive warfare*), che contengono elementi di influenza e impatto sulla cognizione umana e che pertanto possono aumentare di ampiezza e penetrazione nella nuova ecologia digitale[85].

[85] Un'"ecologia digitale" è un insieme chiuso di artefatti digitali e non digitali. L'utente agisce come nodo di una rete, con i suoi confini specificati da un'attività. La struttura e i modelli di organizzazione sono definiti dall'utente e/o dal designer. Un esempio di design di "ecologia digitale" può riguardare il miglioramento dell'attività di "visitare un museo". L'obiettivo del designer sarà la specifica di quali artefatti digitali saranno e/o non saranno inclusi nell'ecologia (struttura) e come questi nodi interagiranno tra loro (modelli di organizzazione). Ciò si concretizzerà nella specifica dei confini della rete definendo l'attività "visita al museo" e il suo svolgimento. Un'ecologia digitale è sempre un sottoinsieme dell'ecologia personale di un utente. Viene creata, sia inserendo nuovi artefatti digitali nell'ecologia personale di un utente, sia cambiando i modelli di organizzazione tra quelli esistenti. (Raptis et al. 2014)

La relazione concettuale tra *Hybrid warfare* e i citati tipi di *warfare* sono ben rappresentate dalla Figura 1[86].



4.2 Guerra Ibrida e Hybrid threats

Il termine "ibrida" accostato alle parole "minaccia", "guerra", "attività", "operazioni" e "tattiche" sono spesso usati in modo intercambiabile senza definizione.

Si pone quindi un primo problema di definire i termini principali. Questa sezione affronta il problema e definisce i due termini chiave: guerra ibrida e minacce ibride.

Il termine guerra ibrida è apparso in tempi meno recenti in un testo del Maggiore statunitense William J. Nemeth intitolato *Future War and Chechnya: A case of Hybrid Warfare del 2002*[87], che analizzava la condizione ibrida della società cecena che fece emergere un modo di condurre la guerra originale con elementi regolari e irregolari combinati in maniera molto efficace. Il lavoro di Nemeth fu successivamente sviluppato analizzando anche altri conflitti come il Vietman o il Libano con il caso di Hezbollah. Su questo ultimo caso si concentrò l'attenzione di Frank G. Hoffman che delineò una vera e propria prima definizione di guerra ibrida:

"Le minacce ibride incorporano un range completo di metodologie differenti di modi di fare la guerra, includendo capacità convenzionali, tattiche e formazioni irregolari, atti terroristici inclusi violenza indiscriminati e coercizione, disordine criminale. La guerra ibrida può essere condotta sia dagli stati che da una varietà di attori non statali. Queste attività multimodali possono essere condotte da unità separate o anche dalla stessa unità, ma sono generalmente a livello operativo e tattico dirette e coordinate all'interno dello stesso spazio di battaglia per raggiungere in maniera

[86] Tzu-Chieh Hung, Tzu-Wei Hung, How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-DisInformation Wars, Journal of Global Security Studies, Volume 7, Issue 4, December 2022, ogac016, https://doi.org/10.1093/jogss/ogac016

[87] Nemeth, W. "Future war and Chechnya: a case for Hybrid warfare", Naval Postgraduate School, Monterey, Tesi per il Master, 2002.

sinergica effetti a livello fisico e psicologico nel conflitto. Questi effetti possono essere guadagnati in tutti i livelli di guerra"[88].

Successivamente, Russell Glenn ha provveduto a fornire un'altra definizione ulteriormente sintetica a seguito di un war game statunitense-israeliano nel 2008[89] focalizzato sulle minacce ibride:

"Un avversario che contemporaneamente ed a seconda dei casi impiega alcune combinazioni di (1) mezzi politici, militari, economici, sociali ed informativi, e (2) metodi di guerra convenzionali, irregolari, catastrofici, terroristici e criminali. Questo può includere una combinazione di attori statali o non statali[90]*".*

Il *Joint Forces Command* degli Stati Uniti ha adottato il concetto di minacce ibride nel 2009 e ha sottolineato che includono qualsiasi nemico che utilizzi simultaneamente e in modo adattivo una combinazione appositamente selezionata di mezzi o azioni convenzionali, irregolari, terroristici e criminali nello spazio di combattimento operativo. Invece di una singola entità, una minaccia o un avversario ibrido possono consistere in una combinazione di attori statali e non statali[91].

Sinteticamente si potrebbe tracciare che il termine guerra ibrida ha la sua principale utilità per descrivere il carattere mutevole della guerra contro avversari violenti durante i conflitti armati, mentre le minacce ibride descrivono una sfida distinta (ma correlata): l'uso di mezzi multipli e ambigui per colpire le vulnerabilità in tutta la società per raggiungere gli obiettivi gradualmente senza innescare risposte decisive.

Mentre il primo concetto può aiutare a caratterizzare gli approcci contemporanei alla guerra visti in Medio Oriente, prevalentemente provenienti da attori non statali, il secondo concetto può anche aiutare ad analizzare gli approcci di Stati come Russia, Cina e Iran.

Sia le minacce ibride che la guerra ibrida pongono sfide distinte per la sicurezza nazionale che probabilmente perdureranno e persisteranno, si propone quindi la seguente distinzione concettuale, basandosi sui risultati di cui sopra:

- la guerra ibrida è la sfida presentata dalla crescente complessità dei conflitti armati, in cui gli avversari possono combinare più mezzi non militari per neutralizzare la potenza militare convenzionale;
- le minacce ibride combinano un'ampia gamma di mezzi non violenti per colpire le vulnerabilità dell'intera società per minarne il funzionamento, l'unità o la volontà dei loro

---

88 Hoffman, Frank G. "Conflict in the 21st century: The rise of Hybrid wars". Arlington, VA: Potomac Institute for Policy Studies, 2007.

89 Questa definizione appare in Russell W. Glenn, Evolution and Conflict: Summary of the 2008 Israel Defense Forces-U.S. Joint Forces Command "Hybrid Threat Seminar War Game," Santa Monica, CA: RAND,TBP in 2009. This document will not be available to the general public

90 R.Glenn, Thoughts on Hybrid Conflict, Small Wars Journal, 2 marzo 2009

91 Definition adopted in support of U.S. Joint Forces Command Hybrid war conference held in Washington, D.C., February 24, 2009

obiettivi, degradando e sovvertendo allo stesso tempo lo status quo. Questo tipo di strategia viene utilizzata per raggiungere gradualmente i propri obiettivi senza innescare risposte decisive, comprese quelle armate[92].

Più sinteticamente, le minacce ibride prendono di mira principalmente una popolazione e la sua volontà e la capacità decisionale del governo, mentre la guerra ibrida prende di mira principalmente l'efficacia dell'apparato militare per condurre operazioni di successo.

Fatta questa doverosa premessa, in particolare dopo aver spiegato il motivo per cui questi termini sono in correlazione, nella sezione successiva ci soffermeremo a descrivere le minacce ibride più rilevanti per un ambiente virtuale, come può essere il Metaverso.

4.2.1 Information Warfare

Una delle minacce ibride è quella che riguarda lo spazio informativo. L'acquisizione di informazioni, il controllo e la protezione del proprio spazio informativo e l'obiettivo di guadagnare un vantaggio informativo sopra l'avversario hanno sempre rappresentato una caratteristica peculiare dei nostri apparati di sicurezza e militare. Ciò che caratterizza l'attuale spazio informativo è la velocità di scambio e consumo delle informazioni e i diversi strumenti tecnologici oggi utilizzabili. Tale aspetto viene giustamente sintetizzato nella dottrina della NATO che definisce l'*Information Warfare* (IW) *"an operation conducted in order to gain an Information advantage over the opponent. It consists in controlling one's own Information space, protecting access to one's own Information, while acquiring and using the opponent's Information, destroying their Information systems and disrupting the Information flow. Information Warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in Information being disseminated faster and on a larger scale*[93]*".*

Più sinteticamente, il *Department of Defence* statunitense definisce il perimentro di una operazione militare nella spazio informativo: *"the integrated employment, during military operations, of Information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own*[94]*".*

---

[92] Tale distinzione è stata anche proposta da altri autori, tra i quali vedi, Frank G. Hoffman, "Examining Complex Forms of Conflict," PRISM 7, no. 4 (2018): 30–47; Fridman, Russian "Hybrid Warfare"; Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy," International Affairs 95, no. 2 (2019): 255–275; Mark Galeotti, (2014) The 'Gerasimov Doctrine' and Russian Non-Linear War, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

[93] Media-(Dis)Information–Security, DEEP – Defence Education Enhancement Program https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-Information-warfare.pdf

[94] Joint Publication 3-13 2012 (change 1 2014) https://irp.fas.org/doddir/dod/jp3_13.pdf

Pertanto, l'*Information Warfare* si riferisce all'uso strategico delle informazioni per influenzare, manipolare, disturbare o distruggere un avversario. Essa può essere suddiviso in diverse attività ostili, comprese le operazioni di propaganda, la manipolazione dei media, l'uso di disinformazione e altre tattiche simili che, oggi giorno, prevedono in maniera massiccia l'impiego di tecnologie informatiche. Ciò mette in stretta relazione IW, con la *Cyber warfare* o anche guerra cibernetica e la *cognitive warfare* che saranno trattate successivamente.

I principali componenti dell'IW includono:

- Informazioni: le informazioni sono la materia prima dell'IW. Le informazioni possono essere raccolte attraverso una serie di fonti, tra cui satelliti, intercettazioni di comunicazioni elettroniche, spionaggio umano, *social engineering* e altre tecniche.
- Tecnologie: le tecnologie svolgono un ruolo cruciale nell'IW, fornendo gli strumenti per la raccolta, l'analisi e la distribuzione delle informazioni. Questi strumenti includono *software* di *hacking*, attrezzature di sorveglianza, software di elaborazione dei dati, piattaforme di *social media* e altri mezzi simili.
- Comunicazioni: le comunicazioni sono un componente essenziale dell'IW, poiché consentono di diffondere informazioni e di influenzare le opinioni pubbliche. Le comunicazioni possono essere effettuate attraverso una serie di mezzi, tra cui i media tradizionali, i social media, i blog, i forum *online* e altri.

Gli obiettivi dell'IW possono variare in base al contesto e alla situazione, ma in genere includono:

- diffondere la propria influenza: l'IW può essere utilizzata per diffondere la propria influenza su una regione o su una popolazione. Ad esempio, un paese potrebbe utilizzare l'IW per diffondere la propria ideologia o per convincere la popolazione di un'altra nazione a sostenere i propri interessi;

- minare la reputazione dell'avversario: l'IW può essere utilizzata per minare la reputazione dell'avversario e influenzare l'opinione pubblica. Ad esempio, un Paese potrebbe utilizzare l'IW per diffondere notizie false o manipolate su un avversario al fine di influenzare l'opinione pubblica;
- sconfiggere un avversario: l'IW può essere utilizzata per indebolire o distruggere le capacità dell'avversario. Ad esempio, un Paese potrebbe utilizzare l'IW per sabotare le infrastrutture critiche di un altro Paese, come centrali elettriche o reti di trasporto.

In sintesi, l'IW è un concetto ampio che comprende diverse attività ostili. L'uso dell'IW può avere conseguenze significative e durature, e pertanto è importante che i governi e le organizzazioni siano consapevoli delle minacce e delle opportunità associate all'IW e adottino le misure necessarie per proteggere sé stessi e le proprie informazioni.

4.3 L'Info War della Russia

La Russia avendo consapevolezza della superiorità militare USA e della NATO ha cercato nella cosiddetta *InfoWar*[95] un elemento di asimmetria che potesse mitigare l'attuale sbilanciamento tecnologico e militare. La Russia nel tempo ha osservato le modalità operative delle coalizioni militari occidentali essenzialmente basate su una indiscussa superiorità nel comando e controllo, e quindi sulla dipendenza dall'informazione e dal mezzo su cui essa si muove: lo spettro elettromagnetico. Inoltre, ha individuato nel consenso politico e sociale il vero centro di gravità degli USA ma soprattutto della NATO e delle moderne democrazie occidentali. Centro di gravità influenzabile con la manipolazione dell'informazione, con la sua alterazione o con l'oscuramento della stessa. Nella visione russa la *Information warfare*[96] è costituita da:

- un'attività condotta sia in tempi di pace, preparatoria del possibile conflitto, sia come attività sistematica di supporto alle operazioni militari in caso di conflitto;
- una combinazione di attività di intelligence, di guerra elettronica, di operazioni cibernetiche ed operazioni psicologiche (propaganda, influenza), disinformazione che in modo combinato con i tipici strumenti della "guerra tradizionale" concorrono a raggiungere

[95] l'*Information war* delineata dal Prof. David Stupples vede una combinazione di tre aspetti: 1) la Guerra Elettronica che deve distruggere lo spazio elettromagnetico; 2) gli attacchi informatici che devono influenzare la funzionalità delle infrastrutture critiche dell'avversario; 3) le operazioni psicologiche (*Psycological Operation* o *Psy-Ops*) con lo scopo di minare e degradare valori e morale della popolazione intera di una nazione. L'utilizzo combinato di questi tre aspetti, può creare caos e instabilità. Per maggiori dettagli si veda: https://theconversation.com/the-next-war-will-be-an-Information-war-and-were-not-ready-for-it-51218

[96] Russian thinkers view Information warfare as capable of disorganizing an opponent's command and control, deceiving an adversary, sowing instability within an enemy's borders, and demoralizing an opposing population or military to the point that they even lose the will to resist.*https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf*

l'obiettivo. In talune circostanze gli strumenti della *Information warfare* possono essere complementari o addirittura dei sostituti agli strumenti della guerra convenzionale[97].

La strategia russa è stata delineata in modo articolato nella cosiddetta dottrina[98] Gerasimov (*Russia non-linear war*[99]), ove si profilerebbero guerre non più dichiarate, ma vere e proprie zone grigie, in cui non sarebbe più possibile distinguere pace e belligeranza e in cui, soprattutto, il ruolo dei mezzi non-militari avrebbe raggiunto un'importanza tale da renderli spesso più efficaci di quelli strettamente militari. Tale dottrina si materializza in tutte le attività svolte nell' *Information Space*[100], e include in questo spazio complesso una moltitudine di principi al fine di raggiungere la superiorità informativa.

All'interno dell'Information Space si pianificano e svolgono operazioni integrate e con un approccio più olistico rispetto a USA e in generale NATO e Paesi ad essa aderenti. Tali operazioni sinteticamente sono state definite come: *Influence Operation* (IO). All'interno dell'IO si possono distinguere le *Inform and Influence Operations* (IIO), le *Information Cyber Operations* (ICO) e le *Information Operations*.

Nelle IIO rientrano tutte quelle azioni deliberate di propaganda e/o disinformazione che mirano a creare confusione e caos; Isaac R. Porche, ha definito le IIO come: *'Inform & Influence Operations are efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages'*[101], Le ICO sono azioni intrusive e non autorizzate che si svolgono nel *Cyberspace* e hanno come obiettivo nodi della rete o sistemi a esso collegati con lo scopo di distruggere, cambiare o aggiungere informazioni o dati. Sinteticamente sono definite come: *'Operations which affect the logical layer of Cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences*[102].

Riepilogando, l'*InfoWar* russa si pone obiettivi: quali creare caos nella società, alterare o interrompere il flusso di informazioni verso i sistemi di Comando e Controllo e creare stallo nel processo decisionale, degradando la libertà di azione senza o con poca distruzione fisica. L'*InfoWar*

---

97 Pissanidis N., Roigas H, Veenendal M.(Eas),(2016), *Cyber Power 8th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) Tallin, Estonia 31 May - 03 June 2016, https://ccdcoe.org/uploads/2018/10/CyCon_2016_book.pdf

98 La dottrina mira a definire le basi militari sul piano politico, strategico ed economico per garantire la sicurezza del paese. Rappresenta un sistema di opinioni e posizioni ufficialmente accettate sugli obiettivi o sul carattere di una potenziale guerra, come prepararsi e prevenirla.

99 Galeotti M, (2014) *The 'Gerasimov Doctrine' and Russian Non-Linear War*, 06.07.2014 https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

100 Ministry of Defence of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept* https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

101 Isaac R. Porche III et.al, Redefining Information Warfare Boundaries for an Army in a Wireless World, Santa Monica 2013

102 Pissanidis N., Roigas H, Veenendal M.(Eas),(2016), Cyber Power 8th International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) Tallin, Estonia 31 May - 03 June 2016, https://ccdcoe.org/uploads/2018/10/CyCon_2016_book.pdf

non è un aspetto che riguarda solo le Forze Armate, ma ha impatto su molti Enti e Agenzie governative che necessariamente devono coordinarsi per condurre un'*InfoWar* (difensiva e offensiva) di successo. Pertanto, l'*InfoWar* come delineata nella dottrina russa, rappresenta una seria sfida strategica e una minaccia formidabile che ha diverse caratteristiche. La presenza nell'arsenale militare russo di sistemi avanzati di *Electronic Warfare*[103], di *Information Weapons*[104] e *Cyber Weapons*[105] e la capacità di operare nell'Information Space in maniera integrata, pone la Russia come un *player* potenzialmente in grado di svolgere operazioni a tutela dei propri interessi e/o in aree di interesse strategico.

4.2 Cyber Warfare

La *Cyber Warfare* (CW) si riferisce a una forma di conflitto in cui gli attori utilizzano le tecnologie informatiche per attaccare i sistemi informatici, le reti e le infrastrutture critiche degli avversari. Questa forma di guerra può essere utilizzata in modo indipendente o in combinazione con altre forme di guerra facenti tutte parte dell'*Hybrid Warfare*.

La CW comprende diverse dimensioni concettuali. Una di queste è la dimensione tecnologica, che riguarda le tecnologie informatiche utilizzate per condurre attacchi informatici. Questa dimensione comprende una vasta gamma di tecnologie, tra cui *malware*, virus, *worm*, *Trojan*, attacchi DDoS (*Distributed Denial of Service*), e altri strumenti utilizzati per compromettere i sistemi informatici degli avversari.

Un'altra dimensione concettuale è la dimensione strategica, che riguarda gli obiettivi strategici che gli attori cercano di raggiungere attraverso la CW. Questi obiettivi possono includere il sabotaggio delle infrastrutture critiche, il furto di informazioni sensibili, la manipolazione dell'opinione pubblica, e altri obiettivi strategici.

La dimensione legale è un'altra dimensione concettuale della CW. Essa riguarda le leggi e le normative che regolano l'uso delle tecnologie informatiche in conflitti internazionali e nazionali. Questa dimensione è importante perché l'uso delle tecnologie informatiche per condurre attacchi informatici può violare le leggi e le normative internazionali.

Infine, la dimensione umana è un'altra importante dimensione concettuale della CW. Essa riguarda l'aspetto umano del conflitto, come ad esempio gli effetti psicologici e sociali degli attacchi

[103] Samuel Cranny-Evans (2022) Fields of silence and broken cycles: Russia's electronic warfare Global Defence Technology 03.2022 https://defence.nridigital.com/global_defence_technology_mar22/russia_electronic_warfare

[104] Ablazov, I., Demenko, O., Leonov, O., Mokliak, S., & Khamula, S. (2022). Information weapons within the interstate struggle in the XXI Century. Amazonia Investiga, 11(52), 269-277. https://doi.org/10.34069/AI/2022.52.04.29

[105] Ci sono sospetti che il *worm* Stuxnet utilizzato per danneggiare infrastrutture critiche di uno Stato sia riconducibile a organizzazioni russe. Per una analisi di dettaglio sul *worm* Stuxnet si veda Marco De Falco, *Stuxnet Facts Report. A Technical and Strategic Analysis* https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

informatici, l'addestramento del personale militare e civile per gestire le minacce informatiche, e la sensibilizzazione del pubblico riguardo alla *Cyber* sicurezza. In sintesi, la *Cyber Warfare* è una forma di conflitto che comprende diverse dimensioni concettuali, tra cui la dimensione tecnologica, strategica, legale e umana. La comprensione di queste dimensioni concettuali è importante per sviluppare una strategia efficace per affrontare le minacce informatiche e mitigare gli effetti della *Cyber Warfare*.

La NATO definisce il *Cyberspace* come l'ambiente formato da componenti fisici e non fisici, caratterizzati dall'uso di computer e dallo spettro elettromagnetico, per archiviare, modificare e scambiare dati utilizzando reti di computer. La Joint Pubblication 3-12 articola il *Cyberspace* in tre *layers*: *physical network, logical network* e *Cyber* persona.

Il primo *layer – physical network* – include la componente geografica e la componente fisica della rete (articolata in hardware e infrastruttura che supportano la rete connessa).

Il secondo *layer – logical network* – è costituito da tutti gli elementi che permettono lo scambio di informazioni nel *Cyberspace* e comprendono *software*, sistemi operativi, protocolli, database.

Infine, il terzo *layer – Cyber* persona – è da riferirsi all'identità virtuale e il relativo *footprint* digitale che le persone assumono nel *Cyberspace*. È composta da tutte le informazioni che sono associate alla presenza su internet (mail, *social* media, siti visitati).

Le *Cyber Operations* (CO) utilizzano la struttura interconnessa e integrata del *Cyberspace* e possono essere utilizzate per scopi militari, politici, economici, sociali e criminali. L'obiettivo delle CO mira a creare effetti prima nel *Cyberspace* e poi, se necessario nei vari domini fisici. Tra le finalità delle CO possiamo citare, lo spionaggio con l'obiettivo di ottenere informazioni sensibili o riservate, attacchi informatici con l'obiettivo di interrompere servizi, Propaganda con l'obiettivo di diffondere informazioni o disinformazione (si pensi al fenomeno delle fake *news*), criminalità informatica con l'obiettivo di commettere reati e frodi, furto di dati e estorsioni, fino ad arrivare ad operazioni di tipo militare (CW) che mediante l'utilizzo dell'infrastruttura IT (*Information Technology*) contribuisce ad attaccare l'opponente. A tal proposito, il *CCDCOE* (Cooperative Cyber Defence Centre of Excellence), centro NATO della *Cyber* Difesa, noto per aver prodotto il Tallinn Manual, ha delineato due interessanti definizioni:

- il termine *Cyberwar* indica "*l'uso di computer per arrestare le attività di un Paese nemico, specialmente l'attacco deliberato di sistemi di comunicazione*";
- il termine *Cyber Warfare* invece indica l'insieme di "*Cyber attacchi che sono autorizzati da Stati contro l'infrastruttura informatica [del nemico] insieme ad una campagna governativa*".

Una seconda definizione, adottata dal 2010 in poi dall'US Department of Defense, precisa che la CW è "un conflitto armato condotto interamente o in parte con mezzi informatici".

La RAND Corporation, un'istituzione no-profit di analisi e ricerche, ha elaborato una delle definizioni più sintetiche e generali di CW: "*il Cyber Warfare implica delle azioni compiute da uno Stato o da un'organizzazione internazionale per attaccare e tentare di danneggiare le reti informatiche o i computer di altre nazion*i […]".

Considerato quanto sopra, possiamo definire la *Cyber Warfare* come l'insieme delle operazioni, belliche e non belliche, condotte da un attore al fine di ottenere, distruggere o alterare le informazioni della controparte. Tra le operazioni possiamo citare:

- attacchi *Cyber*, cioè attacchi mirati con lo scopo di paralizzare, disabilitare o danneggiare i sistemi informatici dell'opponente, realizzando così gli obiettivi principali di una *Cyber war*;
- attività di raccolta informazioni o spionaggio;
- attività di *Cyber Defense*, quali operazioni volte a preservare e difendere il dominio *Cyber*;
- propaganda e diffusione di messaggi volti a disinformare i cittadini e a ficcare il morale del nemico, seguendo le modalità della Guerra Psicologica (PSYOPS).

Tra gli attaccanti e attori principali della *Cyber Warfare* possiamo elencare:

- Stati Sovrani, i quali interessi potrebbero essere di tipo strategico-militare, economico, politico.
- Hacktivisti, i quali hanno precise finalità ideologiche e che possono anche venire "assoldati" per influenzare l'opinione pubblica o muoversi su base volontaria[106] e/o organizzarsi in gruppi.

Gli strumenti della CW sono le *Cyber weapons*, semplificando, una *Cyber*-arma può essere definita come "*Un'apparecchiatura, un dispositivo ovvero un qualsiasi insieme di istruzioni informatiche utilizzato all'interno di un conflitto tra attori, statali e non, al fine di procurare anche indirettamente un danno fisico a cose o persone, ovvero di danneggiare in maniera diretta i sistemi informativi di un obiettivo critico nazionale del soggetto attaccato*[107].

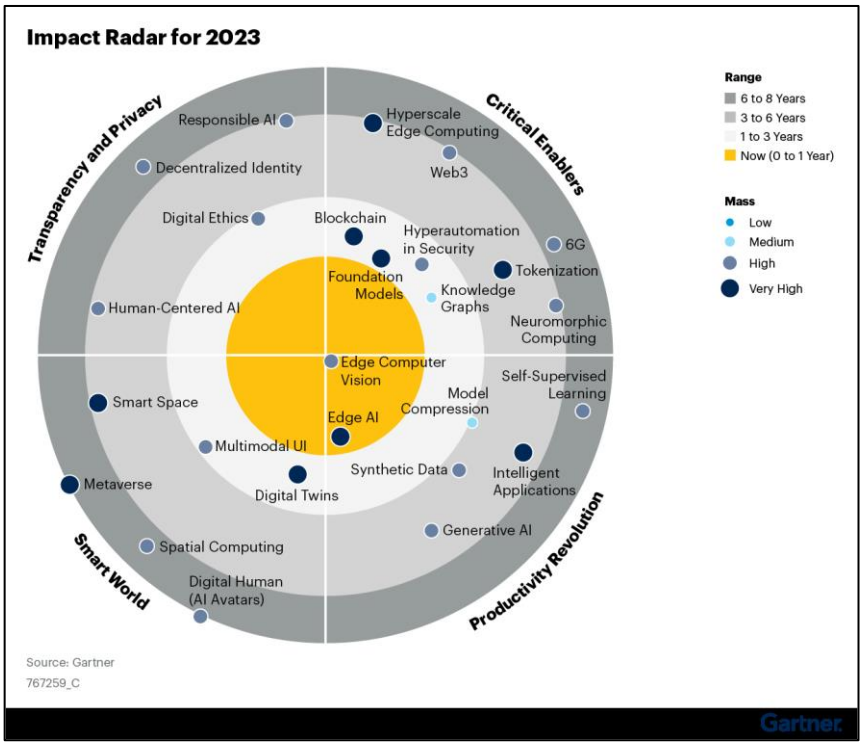
In questo paragrafo abbiamo fornito le definizioni base di *Cyber Warfare*. La guerra cibernetica, grazie all'interconnessione diffusa, rende ogni singolo utente in rete, una possibile vittima di un conflitto.

[106] Nell'attuale conflitto Russo-Ucraino un e*sercito* globale di *hacker* sono intervenuti su base volontaria a sostegno dell'Ucraina. Si tratta della c.d. IT Cyber Army of Ukraine. "Soldati digitali" che hanno lanciato una campagna globale di *Cyber warfare* contro obiettivi collegati a Mosca.

[107] Per il relativo approfondimento si veda Stefano Mele (2013) *Cyber-weapons: aspetti giuridici e strategici* Roma, Edizioni Machiavelli, 2013 http://www.strategicstudies.it/wp-content/uploads/2013/06/Edizioni-Machiavelli-Cyber-Weapons-Aspetti-Giuridici-e-Strategici-V2.0.pdf

Il Metaverso è il crescente regno digitale che utilizza la realtà aumentata, la realtà virtuale, la blockchain, i *social media* e una serie di altre tecnologie, promette di creare un mondo virtuale in cui milioni di persone, attraverso il proprio avatar, si connettono e interagiscono in un universo creato nel Cyberspazio.

Nella sua mappa delle tecnologie emergenti per il 2023[108] (di seguito riportata) Gartner stima che entro i prossimi cinque-otto anni le tecnologie abilitanti saranno disponibili e che gradualmente, pertanto, potremo assistere allo sviluppo nel Metaverso.



Nonostante, quindi ad oggi, sia difficile prevedere quali potrebbero essere le azioni di *Cyber Warfare* nel Metaverso, dal punto di vista tecnologico, la creazione di un avatar di ogni persona che entra con una propria identità in questa nuova dimensione rappresenta un punto di attenzione. Con questo in mente nell'ambito della *Cognitive Warfare*, si darà evidenza di alcune minacce che già oggi sono già applicabili e amplificati con il Metaverso.

4.5 Cognitive Warfare

Le PSYOPS non sono una novità negli scenari di guerra, tuttavia, la Guerra Cognitiva (o *Cognitive Warfare*) è uno degli aspetti più moderni della Guerra Ibrida.

La *Cognitive Warfare*, rispetto alle PSYOPS, si basa su tecniche arricchite da nuove e recenti conoscenze nell'ambito delle neuroscienze e dei meccanismi cognitivi, e che, unitamente allo sfruttamento all'Information *Warfare* e alle *Cyber Warfare*, mira al controllo delle menti.

La *Cognitive Warfare* ha come obiettivo la dimensione cognitiva e la vulnerabilità insite nella mente umana, ovvero quella riferita alla capacità di elaborazione mentale, percezione e ragionamento di coloro che gestiscono i dati e agiscono (prendono decisioni) in base alle informazioni in entrata e

[108] Emerging Tech Impact Radar: 2023 Published 22 December 2022 - ID G00767259 - By Analyst(s): Tuong Nguyen, Annette Jump, Danielle Casey. Disponibile: https://www.gartner.com/en/doc/emerging-technologies-and-trends-impact-radar-excerpt

in uscita. La dimensione cognitiva è considerata oggi dalla NATO come area di studio e sviluppo[109] e come un nuovo campo di battaglia ove l'opponente impiega mezzi, azioni e strumenti attraverso le connessioni tra i domini[110], *l'Information Enviroment* (IE)[111] e lo spettro elettromagnetico[112] per generare effetti nella dimensione cognitiva e influenzare il comportamento umano per ottenere un vantaggio competitivo.

In "*The Cognitive Warfare Concept*", Bernard Claverie e François du Cluzel parlano chiaramente di "sesto dominio" e danno la seguente definizione di Cognitive Warfare: "*Cognitive Warfare is the art of using technological tools to alter the cognition of human targets, who are often unaware of any such attempt - as are those entrusted with countering, minimizing, or managing its consequences, whose institutional and bureaucratic reactions are too slow or inadequate*"[113].

Per gli autori dello studio, la guerra cognitiva è possibile sfruttando al meglio l'intersezione di due aree: *"...PSYOPS and influence operations (soft power)" e "Cyber operations" (Cyber defence) intended to degrade or destroy physical Information assets on the other.*"

Nello stesso studio si attribuisce il termine *Cognitive Warfare* al generale americano Vincent R. Stewart (USMC, director, Defense Intelligence Agency), *che* nel 2017, nel corso di una

---

[109] Tra le iniziative in ambito *cognitive warfare* indette *dall'Innovation Hub* della NATO si cita quella con la società statunitense Veriphix (motto: "Misuriamo le convinzioni per prevedere e modificare il comportamento"), che ha sviluppato una piattaforma con la quale è possibile identificare i cosiddetti *nudge*, ovvero "*nudge*" psicologici inconsci su Internet.

[110] *air*, *land*, *maritime*, *space* e *Cyber*. Il *Cyberspace* è anche considerato parte dell'IE.

[111] USA Joint Publication (JP) 3-13 che definisce l'IE: "The Information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on Information. The actors include laders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate Information. The Information environment is where humans and automated systems observe, orient, decide, and act upon Information, and is therefore the principal environment of decision making. Even though the Information environment is considered distinct, it resides within each of the four domains. The Information environment is made up of three interrelated dimensions: physical, Informational, and cognitive".

[112] La NATO definisce l'ambiente del *Cyberspace*. Lo spettro elettromagnetico è considerato parte dell'ambiente. Particolarmente interessante è invece l'approccio dottrinale più ampio del Ministero della Difesa Inglese che considera lo spettro elettromagnetico un termine più inclusivo e più ampio, sia facente parte dell'ambiente, sia come attività: *The Cyber and electromagnetic domain is defined as: a domain comprising capabilities which enable activities that maintain freedom of action by creating effects in and through Cyberspace and the electromagnetic spectrum*. JDP 0-50, UK Defence Cyber and Electromagnetic Doctrine per un approfondimento. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/682859/doctrine_uk_Cyber_and_electromagnetic_activities_jdn_1_18.pdf

[113] Claverie B. du Cluzel F. (2022) *The Cognitive Warfare Concept*, https://www.innovationhub-act.org/sites/default/files/2022-02/CW%_0.pdf

conferenza, parlò di come le guerre moderne siano delle guerre cognitive in cui il controllo delle informazioni serve a manipolare il nemico: *"...it is to know what to do and when to do it... and if you don't control Information or your decision-making cycle is disrupted, or your cognitive ability is degraded, then you are not able to win or fight effectively*".

In un recente convegno sulla strategia russa di disinformazione e guerra cognitiva in Italia[114], il Dott. Marco Cannavicci nel suo intervento sulla *Cognitive Warfare* russa, ha contrapposto la Teoria dei Giochi Usa al Controllo Riflessivo russo. «*La teoria dei giochi ti dà uno scenario di tutte le possibili situazioni che si possono venire a creare, per prevedere gli sviluppi. Il controllo riflessivo mira invece a determinarli gli sviluppi, secondo l'elaborazione di Vladimir Lefebvre*». Nell'intervento è stato spiegato che il controllo riflessivo, si può fare a livello di singole persone (*target*), ma funziona ancora meglio a livello di massa (*target audience*), con una serie di tecniche. Distrarre la mente dell'avversario su temi non di interesse. Dare molte informazioni in contraddizione in modo da affaticare e far agire in automatico. Ripetere una falsità più volte, fino a farla percepire come vera. Alla fine l'obiettivo è far fare all'avversario ciò che si vuole. «*Provocare in lui la reazione che, conoscendo la sua psicologia, possiamo con buona probabilità anticipare che si comporterà in quel modo. Quindi quando si riscontra un punto debole, un punto di fragilità, un punto dove l'emotività del soggetto prevale sulla ragione, noi stimoliamo quel punto e otteniamo come riflesso condizionato quella risposta*».

Lo scopo della *Cognitive Warfare* (o, almeno, uno degli scopi più manifesti) è quello di non confrontarsi in uno scontro armato ma cambiare, fiaccare, minacciare, spezzare, rivoluzionare punti di vista, idee, convinzioni e opinioni del soggetto o di un gruppo di soggetti, costruendo una sorta di realtà parallela e alternativa in base alla percezione della quale la persona finirà con il comportarsi in modo diverso da prima e/o con l'esprimere idee differenti da prima e più uniformi all'opponente.

Uno degli aspetti più importanti della guerra cognitiva è quello che ruota intorno all'inganno, alla propaganda e alla gestione delle informazioni, compresa naturalmente la disinformazione o, per meglio dire, il disordine informativo[115] (*Information disorder*), composto da tre elementi: la disinformazione (*disinformation*), che include informazioni false e create deliberatamente per danneggiare i soggetti; la *misinformation*, che include anch'essa informazioni false ma non create con l'intenzione di causare danni e la *mala-informazione*, la diffusione di informazioni errate o riservate e utilizzate per infliggere danni. In questo ultimo ambito possiamo anche far rientrare la

[114] "Dezinformacija - La strategia Russa di disinformazione e guerra cognitiva in Italia. https://www.youtube.com/watch?v=4pDD62qVzys

[115] Cfr. Claire Wardle, PhD and Hossein Derakhshan (2017) *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe, 23.09.2017 https://edoc.coe.int/en/media/7495-Information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

cosiddetta *infodemia*[116], una informazione, massiva, caotica e ridondante, con lo scopo di destabilizzare o fare propaganda, su scala globale, ad opera di attori statali e non statali. Tale termine, coniato durante la pandemia del SARS-CoV-2, per alcuni autori[117] è stato "u*n vero e proprio atto ostile in cui non è prevista violenza fisica, ma gestione sistematica dell'informazione mediante la manipolazione della sfera cognitiva.*

Considerato che la guerra cognitiva è già in atto e le più moderne tecniche e tattiche delle scienze cognitive sono attualmente utilizzate nella guerra in Ucraina[118] per dirigere i pensieri e i sentimenti delle popolazioni di tutte le nazioni coinvolte nella guerra, l'evoluzione verso il Metaverso può solo che amplificare le azioni di influenza.

Una analisi limitata dello scenario attuale può essere essenziale per definire le sfide future e individuare le potenziali vulnerabilità, così da non essere mai sprovvisti di fronte a future minacce. Attività note come la social media intelligence (SOCMINT)[119] o di *social engineering*[120] già oggi costituiscono due importanti strumenti per portare avanti attacchi mirati personalizzati.

La psicologa americana Katelyn McKenna ha mostrato come le persone sono più predisposte nei *social network* a rivelare il proprio vero sé, più di quanto non lo siano nella vita reale[121].

Le piattaforme di social media sono in grado di dare accesso a qualsiasi tipo di utente, fornendo anche gli strumenti per comprenderne i comportamenti, studiando e analizzando le loro attività e le loro opinioni. Un test[122], promosso dallo *Strategic Communications Center of Excellence* della NATO ha rivelato che i dati pubblicati online, in particolare nei *social network*, possono essere usati per

---

[116] Cfr. "Infodemia e pandemia: la *cognitive warfare* ai tempi del SARS-CoV-2" di Francesco Saverio Bucci, Matteo Cristofaro & Pier Luigi Giardino, CASD https://www.casd.it/mod/resource/view.php?id=17501&forceview=1

[117] ibidem, p. 1

[118] In questo articolo un'analisi interessante del caso studio della Biennale di Venezia come teatro della guerra cognitiva tra Russia e Ucraina: "Between Kiev and Venice The cognitive warfare and the Biennale of Venice" (Vol. 3 No. 2, 2022. Security Science Journal), a cura del Dr (Col.) Shaul Shay. https://zagrebsecurityforum.com/Portals/0/SecurityScienceJournal/SSJ%203_2_6%20Between%20Kiev%20and%20Venice.PDF

[119] La SOCMINT sfrutta i *social media* per raccogliere informazioni sui loro obiettivi. Oggi tramite l'analisi delle fonti aperte (Open Source Intelligence), a cui tutti possono accedere, oggi è possibile svolgere l'analisi dei profili social, sui contatti, *hobby*, *like*, immagine postate e analisi dei testi scritti e ottenere un quadro di insieme del *target*. L'utilizzo di tecniche psicologiche e dei modelli di neuroscienze cognitive permetteranno sempre più in futuro di ottenere informazioni sempre più precise del *target* fino a a ottenere informazioni di tipo predittivo, emotivo e comportamentale.

[120] Le attività di *social engineering* o di ingegneria sociale, riguardano essenzialmente la psicologia della persuasione: prendono di mira la mente. L'obiettivo è guadagnare la fiducia del *target*, così che abbassi la guardia, e poi incoraggiato a compiere azioni non sicure, come divulgare informazioni personali, fare clic sui link oppure aprire allegati che possono essere dannosi.

[121] Cfr. John A. Bargh and Katelyn Y. A. McKenna *The Internet and Social Life*; Annual Review of Psychology; Vol. 55:573-590 (Volume publication date 4 February 2004) First posted online on July 11, 2003; https://doi.org/10.1146/annurev.psych.55.090902.141922

[122] Bay, Sebastian & Bertolin, Giorgio & Biteniece, Nora & Christie, Edward & Dek, Anton & Fredheim, Rolf & Gallacher, John & Kononova, Kateryna & Marchenko, Tetiana. (2019). *Responding to Cognitive Security Challenges*. Nato Strategic Communications Centre of Excellence https://www.researchgate.net/publication/338764711_Responding_to_Cognitive_Security_Challenges

influenzare i membri delle Forze Armate. La ricerca, descritta sul sito del Fatto Quotidiano[123], ha messo in luce come tramite Facebook, circa 150 militari impegnati in una esercitazione NATO, sono stati oggetto di attività SOCMINT che ha permesso una raccolta informativa accurata, incluso informazioni sensibili, nonché su passioni e preferenze su determinati argomenti. Ciò ha permesso di indentificare univocamente i militari e i rispettivi incarichi all'interno dei loro reparti, monitorare i movimenti del reparto e portarli al punto di rivelare informazioni e/o di rendersi responsabili di azioni di insubordinazione, come per esempio l'abbandono della propria postazione. Dato ancora più impressionante è che l'intera operazione ha avuto un costo totale modesto (sessanta dollari) e pertanto davvero alla portata di tutti per una ipotetica attività di manipolazione *online*. I risultati della ricerca hanno chiaramente evidenziato come gli account social, se utilizzati in modo intelligente da un opponente, possono essere usati per influenzare i membri delle forze armate, nonostante esse siano persone addestrate alla riservatezza dei dati e al rispetto degli ordini.

Tornando al tema del Metaverso si può ben dire che già oggi il sistema dei *social media* mette in evidenza che ogni persona ha un punto debole e che per risalire al punto debole di ciascuno sono sufficienti le informazioni liberamente disponibili online. Questo rende le persone influenzabili, ricattabili e vulnerabili anche nel Metaverso che accelererà e amplificherà il ruolo della c.d *Cyber* persona[124] e la sua impronta digitale.

Questo argomento viene affrontato perché il ruolo della Difesa nel contrastare quello che è apparentemente un problema non militare è probabilmente più controverso, trattandosi di una sfida che non trova la logica applicazione di norme internazionali o dottrina.

[123] https://www.ilfattoquotidiano.it/2019/02/19/facebook-puo-essere-una-minaccia-per-le-forze-armate-un-esperimento-della-nato-lascia-a-bocca-aperta/4982410/

[124] La Joint Pubblication 3-12 del DoD USA, articola il *Cyberspace* in tre *layers*: physical *network*, *logical network* e *Cyber* persona. Il *layer* – *Cyber* persona – è da riferirsi all'identità virtuale e il realtivo *footprint* digitale che le persone assumono nel *Cyberspace*. È composta da tutte le informazioni che sono associate alla presenza su internet (mail, social media, siti visitati).

CAPILO 5
I POSSIBILI SVILUPPI DEL METAVERSO NELLA DIFESA.

L'analisi degli scenari futuri parte da una constatazione: lo sviluppo di nuove tecnologie e il moltiplicarsi di quelle a carattere dirompente (*Emerging & Disruptive Technologies* o EDT) generano una spinta trasversale su ogni dominio scatenando accelerazioni e, contestualmente, decelerazioni imprevedibili e complesse da gestire e controllare. La trasformazione in atto è complessa e repentina e necessita di un processo di adattamento altrettanto veloce. Intelligenza artificiale, biotecnologie, nanotecnologie, ipersonica, nuovi materiali, quantistica e robotica hanno avviato una rivoluzione dagli impatti evidenti non solo nel contesto militare, ma anche (e forse soprattutto) in quello civile.

La rivoluzione in atto è ancora più marcata poiché se è vero che fino al secolo scorso l'innovazione tecnologica era trainata dall'industria militare, è altrettanto vero che in altri settori, ad oggi, è l'industria privata ad averne il monopolio. Il mercato globale ha imposto un'accelerazione alla quale le organizzazioni militari devono adattarsi, rivoluzionando le proprie strutture, i propri processi di acquisizione e di implementazione operativa. Una rivoluzione che, in realtà, abbraccia anche il settore della formazione, dell'impiego del personale e della leadership, trasformandosi in un sostanziale ed importante *mindset change*. Un cambiamento radicale va affrontato e che prevede un rafforzamento della collaborazione con l'industria, l'accademia e tra tutti gli attori governativi (nazionali ed internazionali), per individuare sinergie e soluzioni concrete, sostenibili e velocemente implementabili.

Il dominio virtuale, caratterizzato a differenza dei domini tradizionali da una connotazione intangibile e trasversale, sta assumendo sempre maggiore rilevanza anche a livello geostrategico, in quanto lo sviluppo e la sicurezza di una nazione dipendono sempre più dalla fruibilità d'accesso alle informazioni. Da tempo si pone chiaramente attenzione al controllo del flusso dei dati digitalizzati, inevitabilmente correlati alle tecnologie esposte ad internet, o comunque tra loro "connesse" nel senso più vasto del termine. In tale ottica, la pervasività della dimensione cibernetica determina la necessità del controllo delle reti e dei dati quale *conditio sine qua* non per assicurare servizi essenziali e più in generale la Difesa di una nazione. Un uso malevolo di tali tecnologie potrebbe comportare da una parte il collasso dei sistemi e dei servizi essenziali, dall'altra mettere in luce potenzialità destabilizzanti, con effetti nella dimensione cognitiva, contribuendo al condizionamento delle opinioni pubbliche attraverso il "controllo" delle reti e dei dati.

La capacità di gestione della grande mole di dati è uno dei parametri fondamentali per determinare il peso di ciascun attore in ambito economico e politico, tanto che si parla di sovranità digitale ovvero della possibilità che soggetti, anche privati, siano in grado di intercettarli e renderli

fruibili, riscrivendo gli equilibri geostrategici ed imponendo nuove regole ad una realtà *internet-based*.

Se ne deduce, pertanto, che la padronanza nell'impiego e nella la gestione dei dati sia alla base della superiorità militare, in quanto, agevolando la gestione delle informazioni, facilita l'esercizio del comando e controllo e la condotta di operazioni.

Nel Cyberspace è inoltre possibile preservare l'anonimato degli attori a causa della difficoltà oggettiva di tracciare la fonte degli attacchi: grazie alla possibilità di operare attraverso falsi IP e server stranieri, chi attacca gode di una relativa impunità (cd *non attribution*). Ciò porta alla dematerializzazione, deterritorializzazione, decentralizzazione e denazionalizzazione delle relazioni, trattandosi di un dominio fluido che si modifica e si riconfigura in modo estremamente rapido, travalicando le frontiere geografiche ed espandendosi in tutto il globo.

L'ambiente informativo e la dimensione cognitiva hanno un loro peso specifico che probabilmente tenderà ad aumentare nella condotta delle operazioni, militari soprattutto in un quadro geostrategico in cui il trend è quello di evitare il confronto cinetico ricorrendo sempre di più a forme di *Hybrid Warfare*, cercando di giungere alla sconfitta dell'avversario conquistando le posizioni di vantaggio psicologico, senza necessariamente ottenere la sua distruzione.

In questo quadro, l'informazione e la comunicazione hanno sempre rivestito un ruolo fondamentale negli eventi storici con evidenti riflessi sociali dovuti anche alla loro capacità di orientare l'opinione pubblica.

Appare evidente come, in un contesto come quello attuale, il Centro di Gravità per l'avversario sarà il modo di pensare della popolazione sia in termini reali che virtuali. Non più "programmare" le menti, ma far scegliere "spontaneamente" un comportamento piuttosto che un altro attraverso una strategia informativa e cognitiva chiara e precisa.

In tale contesto, i rapidi progressi nelle neuroscienze e nelle sue tecnologie stanno suscitando sempre maggior interesse per un potenziale uso di questi strumenti e metodi per esercitare influenza e potere sulla scena globale (*weaponization* delle neuroscienze).

Il progetto Metaverso promette una maggiore e più profonda "integrazione" tra digitale e reale che al contempo farà emergere nuove vulnerabilità di sicurezza e amplificherà i rischi e le minacce attuali. Il Metaverso, pertanto, ha le potenzialità per diventare un possibile ambiente operativo dove le tecniche e le tattiche facenti parti della guerra ibrida possono trovare applicazione.

La Difesa in tale contesto può svolgere un ruolo importante contribuendo alla creazione e/o rafforzamento di strutture permanenti nazionali ed internazionali che favoriscano collaborazione e prontezza nell'identificare e quantificare i rischi connessi al Metaverso nel breve e nel medio-lungo termine.

Le Forze Armate hanno infatti avviato da molti anni tentativi per operare nel Metaverso seppur con modalità e fini coerenti allo sviluppo tecnologico ed al contesto politico del tempo.

Uno dei principali contesti operativi è stato, infatti, proprio quello dedicato all'addestramento del personale militare, ove fin dagli anni '80 del secolo scorso sono stati realizzati ambienti virtuali per il *training* attraverso tecniche di "s*imulator networking*", la prima dimostrazione di una rete di simulatori estesa per l'addestramento collettivo. Negli ultimi due decenni, nuovi *standard* hanno facilitato l'integrazione di simulatori, consentendo al personale di sperimentare la "nebbia e l'attrito" del combattimento in un unico spazio sintetico. Oggi le tecnologie fondamentali per il Metaverso – realtà aumentata e virtuale, visori, simulazioni 3D e ambienti virtuali costruiti dall'intelligenza artificiale – sono già presenti nel campo della Difesa. Una combinazione di realtà aumentata, intelligenza artificiale e grafica da videogiochi permette ai piloti di caccia di esercitarsi nel combattimento aereo contro avversari virtuali, tra cui aerei da guerra cinesi e russi, operando in un modo o molto più realistico rispetto a un simulatore di volo convenzionale[125]. In termini di progresso del settore verso il 9Metaverso scalabile e supportato dal cloud, nessuna organizzazione è andata oltre l'US Army. L'ambiente di addestramento sintetico, *Synthetic Training Environment* (STE), in fase di sviluppo dal 2017, mira a sostituire tutti i programmi di simulazione legacy e integrare diversi sistemi in un unico sistema connesso per armi combinate e addestramento congiunto. Inoltre, già qualche anno fa, era è stato sviluppato dall'*Office of Naval Research* e l'*Institute for Creative Technologies* della University of Southern California il "Project Blue Shark", un sistema che consentiva ai marinai di pilotare imbarcazioni collaborando in un ambiente virtuale e, un'altra iniziativa, il "Project Avenger" è tuttora utilizzata per contribuire alla formazione dei piloti della marina militare statunitense[126]. Sebbene questo tipo di addestramento costituisca una prima applicazione del Metaverso nel mondo militare, molto rimane da fare per garantire la necessaria modularità o l'interoperabilità di diverse soluzioni in un mondo realistico e immersivo. Nei prossimi

[125] Nell'ottobre 2020 la tecnologia AR sviluppata dalla società Red 6 è stata utilizzata per contrapporre un vero pilota di caccia a un velivolo controllato da un algoritmo di intelligenza artificiale, sviluppato nell'ambito di un progetto sul combattimento aereo della *Defense Advanced Research Projects Agency* (DARPA) del *Department of Defence degli* Stati Uniti. Un altro progetto della DARPA, chiamato *Perceptually-enabled Task Guidance*, mira a creare un assistente IA in grado di osservare quello che fa un soldato e offrire consigli usando il linguaggio, i suoni o la grafica, offrendo il meglio delle tecnologie derivanti dalla fusione tra reale e virtuale.

[126] "L'esercito degli Stati Uniti sta costruendo il suo metaverso". https://www.wired.it/article/metaverso-esercito-stati-uniti-realta-aumentata/.

anni si dovrà pertanto fare un salto dall'addestramento sintetico ad un ecosistema addestrativo della Difesa.

Soprattutto dall'inizio della pandemia COVID-19, molte istituzioni educative hanno cercato di migliorare le opportunità di apprendimento distribuito attraverso simulazioni, wargame e l'uso di tecnologie di realtà aumentata che consentono al personale di supportare il percorso di apprendimento. In tale ambito il Metaverso della Difesa può creare un ecosistema formativo digitale, che sarebbe molto più immersivo e offrirebbe l'opportunità di attingere ad alcuni dei progressi della realtà mista nell'istruzione che sono già in corso nel mondo civile. Integrando strumenti, tecniche e dati personalizzati in un unico ambiente, un Metaverso della Difesa può essere in grado di fornire risultati di apprendimento completi e continui.

Il Metaverso potrebbe anche essere usato come ecosistema virtuale per convalidare concetti tattici ed operativi. Le esercitazioni militari tradizionali, limitate da risorse fisiche, tendono a seguire scenari e regole specifiche con un obiettivo definito, ma le possibilità aperte degli ambienti sintetici del Metaverso offrono l'opzione di un *wargaming* non strutturato, molto più rappresentativo, una vera e propria sperimentazione di nuovi concetti. Tutto ciò, potrebbe consentire di raccogliere ritorni da tutte le unità sul campo creando un "ciclo di feedback" che assicuri che le lezioni apprese non vengano dimenticate e siano trasferite e iterate – lungo tutto il percorso dalla fase iniziale di sviluppo delle capacità, fino all'eventuale dispiegamento e alla successiva dismissione. I potenziali progressi tecnologici in materia di analisi dei dati dei wargame, se combinati con nuovi approcci agli ambienti sintetici che facilitano l'integrazione delle simulazioni, potrebbero rivelarsi rivoluzionari.

La Difesa potrebbe utilizzare la potenza del Metaverso in situazioni ad alto rischio per integrare meglio le informazioni provenienti da più fonti con l'obiettivo di garantire che il processo decisione disponga della necessaria *Situational Awareness*.

Ma è soprattutto nell'ambito della ricerca e sviluppo che il binomio Metaverso e Difesa potrebbe assicurare i maggiori vantaggi. In assenza di combattimento, la sperimentazione virtuale consente di trascendere la realtà attuale e di realizzare virtualmente le fasi di *concept development & testing* di nuovi sistemi d'arma derivanti dall'applicazione di nuove dottrine. Nel nuovo "ciclo della ricerca" si potrà cercare di capire i problemi e le loro soluzioni attraverso wargame iterativi, simulazioni, ambienti sintetici o esercitazioni virtuali.

Ulteriori sviluppi potrebbero riguardare l'ambito più specifico del reclutamento; fin dall'avvento di America's Army – un popolare gioco sviluppato negli Stati Uniti - nel 2002, le Forze Armate statunitensi hanno utilizzato i videogiochi insieme agli strumenti tradizionali, come i bonus o le paghe migliorate, per attirare talenti nelle forze armate. Gli eSport sono una continuazione di questa tendenza, con ogni servizio che ora vanta una propria squadra che gareggia in competizioni

nazionali e internazionali di videogiochi. Gli eSport sono emersi come una via di reclutamento particolarmente efficace, consentendo di raggiungere una parte della popolazione che altrimenti non sarebbe stata esposta al servizio militare, adattando la pubblicità digitale a gruppi demografici mirati e pubblicizzando le piattaforme di *streaming* rispetto a quelle via cavo per attirare un pubblico più giovane. L'emergere del Metaverso – o di vari metaversi aziendali – fornisce uno stimolo per le forze armate ad approfondire queste tendenze. Man mano che un maggior numero di attività sociali si sposta sul Metaverso – dai giochi ai concerti e agli eventi sportivi – emergeranno maggiori opportunità per fornire nuovi incentivi al reclutamento.

Nella sua dimensione più immeditata il Metaverso è fondamentalmente una costruzione sociale destinata a fornire nuove e potenzialmente più profonde opportunità di interazioni e scambi umani. Proprio come in Fornite, dove i giocatori hanno l'opportunità di uscire o fare amicizia, il Metaverso consente alle persone di stringere nuove relazioni e idealmente di migliorare gli elementi sociali della loro vita. In tale ambito anche per la Difesa si aprono nuove opportunità; le Forze Armate presuppongo infatti una scelta di vita, che influenza non solo le carriere ma anche gli aspetti della vita sociale. Di conseguenza, proprio come le basi militari offrono opportunità di socializzare e costruire comunità, molte di queste attività potrebbero essere portate in un Metaverso in varie forme, consentendo ai militari di usufruire dei benefici della base nel momento del bisogno, integrando piuttosto che sostituendo le interazioni fisiche preesistenti. Per esempio, negli Stati Uniti la comunità dell'Air Force Gaming ha già fatto un primo passo per connettere gli aviatori distribuiti in un ambiente digitale attraverso i videogiochi, offrendo opportunità per lo sviluppo della *leadership*, il lavoro di squadra, la costruzione del morale e il sostegno alla salute mentale dei membri del servizio, in particolare quelli nella fascia d'età compresa tra i 18 e i 30 anni che sono cresciuti come giocatori accaniti.

Il contesto operativo è forse la dimensione più difficile da analizzare per quanto riguarda l'applicazione o l'impatto del Metaverso nella conduzione delle moderne operazioni militari per quanto sia evidente come le applicazioni del Metaverso siano già integrate in alcuni sistemi militari. Uno degli esempi più significativi è il casco high-tech del nuovo caccia F-35 che include un display per la realtà aumentata che mostra dati telemetrici e informazioni sui bersagli, oltre ai filmati ripresi intorno al velivolo.

Lo sviluppo dell'Intelligenza Artificiale (IA) è un elemento che avrà sempre più un ruolo da protagonista e che, convergente con altri trend tecnologici, inciderà trasversalmente negli scenari multidomini caratterizzati da un'elevata velocità di azione. L'avanzamento e la pervasività della IA presenta evidenti profili di rilevanza per la Difesa poiché sarà un abilitante per la tutela degli assetti strategici e delle infrastrutture critiche. L'IA sarà uno degli aspetti determinanti che cambieranno

radicalmente la natura stessa del campo di battaglia del futuro. Sarà quindi prioritario pensare ad un approccio proattivo teso ad assumere un ruolo di primo piano nell'implementazione dell'IA al fine di mantenere costante il livello tecnologico e conservare il vantaggio strategico sugli opponenti. In particolare si dovrà promuovere la diffusione dell'IA prevedendone l'implementazione in tutti i livelli e settori, della Difesa in un quadro coerente con il diritto internazionale ed il contesto etico-morale.

In sintesi, sebbene un Metaverso della Difesa possa consentire una serie di benefici sociali ed operativi distinti, il suo vero valore dovrebbe emergere attraverso l'interconnessione dei vari mondi virtuali della Difesa, a condizione che l'interoperabilità sia prioritaria nella progettazione di questi ambienti virtuali fin dall'inizio. L'integrazione delle attività virtuali nella Difesa dovrebbe creare un ciclo di *feedback* iterativo, con un minimo sforzo umano, garantendo così che le lezioni apprese dall'addestramento, dalla formazione o dal reclutamento possano essere sfruttate durante i test e le sperimentazioni e viceversa.

Man mano che un maggior numero di individui ha accesso alle informazioni in un Metaverso della Difesa, esiste la possibilità che varie attività diventino sempre trasparenti ed orizzontali, rendendo più facile sollecitare idee e *feedback* in tutta la comunità. Per certi versi questo rispecchia i vantaggi offerti dalle piattaforme, da Google ad Amazon, da YouTube a Pinterest. Facilitando lo sviluppo di prodotti e servizi complementari, le piattaforme generano effetti di rete. Più elementi complementari ci sono in una piattaforma, più la rete diventa innovativa e potente.

CAPITOLO 6
LA DIMENSIONE ECONOMICA DEL METAVERSO

6.1 Il Metaverso

Metaverso è un termine mutuato dalla letteratura futurista, usato in alcuni romanzi per riferirsi ad una sorta di realtà virtuale condivisa tramite internet, dove si è rappresentati in tre dimensioni attraverso il proprio avatar.

Il Metaverso oggi è un universo digitale che esiste come combinazione di una molteplicità di tecnologie abilitanti, tra cui video, realtà virtuale, realtà aumentata, *social network*, connessione, analisi avanzata dei dati. Gli utenti possono accedere al Metaverso attraverso visori 3d e altri sensori che gli consentono di vivere delle esperienze virtuali: possono creare degli avatar, incontrare altri utenti, creare oggetti o proprietà virtuali, visitare luoghi, partecipare a concerti e mostre, viaggiare, partecipare a conferenze e *meeting* di lavoro, e così via.

Il Metaverso si sviluppa nel digitale, la sua materia è composta dai dati e dalle informazioni, in stretta correlazione con l'universo dell'oggettivo, la sua struttura è spazio-temporale, la stessa dell'universo fisico. È una struttura composta da lunghezza, larghezza, profondità e tempo: il Cyberspazio, sostanzialmente un universo creato e alimentato dalle reti globali di comunicazione.

Il fondatore di Facebook, Mark Zuckerberg è stato anche in questo pioniere, creando *Horizon Worlds*, uno spazio virtuale a cui si può accedere con il proprio account Facebook e indossando i visori Oculus (società acquisita dalla stessa *Facebook*, oggi Meta, già nel 2014).

Stando ai dati di febbraio 2022, sono circa 300 mila gli utenti che si connettono a *Horizon Worlds* per giocare, costruire il proprio mini-mondo separato (ne esistono più o meno 10 mila) e partecipare a eventi virtuali. C'è anche una piattaforma ad hoc per il lavoro, *Horizon Workrooms*. Con una curiosità: gli avatar arrivano fino alla cintola e fluttuano nel vuoto. Tracciare i loro movimenti di gambe e piedi e riprodurli fedelmente, infatti, va ancora oltre le possibilità tecniche della piattaforma.

6.1.1 Blockchain

Non c'è Metaverso senza Blockchain, perché quest'ultima va ad agire sulla decentralizzazione del dato. Prima dell'utilizzo della Blockchain, degli NFT e delle Criptovalute tutto era immagazzinato in un unico database, con limiti evidenti. La blockchain, al contrario, è un database condiviso e immutabile, definita come un registro digitale le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia.

Svolge un ruolo vitale nello sviluppo del Metaverso perché il futuro del web, ovvero il Web 3.0, è tutto incentrato sul **decentramento** e sull'interoperabilità.

Oggi, infatti l'obiettivo è creare metaversi interoperabili, sicuri, veloci e decentralizzati. La blockchain è ad oggi la tecnologia più adatta, perché permette per esempio, di custodire su un registro decentralizzato le caratteristiche del nostro avatar e i nostri beni digitali (automobili, vestiti, proprietà immobiliari, opere d'arte digitali), utilizzandoli in qualsiasi Metaverso decidiamo di frequentare.

Potremmo dire che il Metaverso basato su blockchain non unisce mondo reale e virtuale, ma ne crea uno totalmente alternativo, dotato di regole e ambientazioni 3D del tutto simili a quelli reali, dove si possono addirittura immaginare modi con cui monetizzare l'esperienza, seguendo dinamiche similari a quelle del mondo reale, pur restando in un contesto di fantasia e creando in questo modo un'esperienza digitale a tutto tondo, nuova ed evasiva.

6.1.2 Digital Twin

Uno degli obiettivi del Metaverso è creare un ambiente digitale che sembri sempre più simile al mondo reale, avvalendosi della ricostruzione 3D con cui è possibile creare in maniera realistica modelli di edifici, luoghi fisici e oggetti. Queste **repliche** virtuali vengono definite *Digital Twin.* I *Digital Twin* permettono, grazie a modelli predittivi elaborati da algoritmi di Intelligenza Artificiale (AI), di prevedere le prestazioni future *dell'asset* fisico e di sperimentare miglioramenti senza doverli testare sul prodotto stesso.

6.1.3 Intelligenza Artificiale

All'interno del Metaverso, l'intelligenza artificiale può essere applicata in diversi modi agli elementi non controllabili dagli utenti. Questi elementi sono parte dell'ambiente virtuale in cui l'avatar si muove, e sono progettati per reagire ed interagire con quest'ultimo. Con le capacità di elaborazione dell'intelligenza artificiale, questi elementi possono essere posizionati negli spazi 3D per creare interazioni realistiche tra utenti o per eseguire altre attività specifiche.

6.1.4 Internet Of Things

L'implementazione dell'IoT può collegare facilmente il mondo 3D ai dispositivi del mondo reale, ciò consentirebbe la creazione di simulazioni real-time all'interno del Metaverso. Per ottimizzare ulteriormente l'ambiente del Metaverso, l'IoT potrebbe utilizzare anche l'AI e il *machine learning* per gestire i dati raccolti.

6.1.5 Realtà Virtuale e Realtà Aumentata

La realtà virtuale funziona proprio come il concetto di Metaverso: produce un ambiente virtuale immersivo nel quale gli utenti possono esplorare utilizzando visori, guanti e sensori. Questa tecnologia rappresenta un interessante punto d'accesso al Metaverso che consente agli utenti di interagire con persone provenienti da altre parti del mondo. La realtà aumentata, o AR, aggiunge invece elementi virtuali alla nostra esperienza reale, tramite l'uso di dispositivi come occhiali, *smartphone* o *tablet*. Questi elementi potrebbero essere informazioni visive, uditive e sensoriali per intensificare la nostra esperienza e la nostra realtà.

6.1.6 Advanced computing e Advanced datacenter

La realizzazione del Metaverso sta alimentando ingenti investimenti nei *data center cloud*.

L'enorme quantità di dati necessaria per il Metaverso eserciterà parecchia pressione sulle reti gestite dai *provider* di servizi Internet e sulla capacità dei data center di elaborare e trasmettere le informazioni.

L'anno scorso, subito dopo che Facebook (Meta) ha annunciato un piano per aumentare le proprie spese in conto capitale di circa il 66% nel 2022, in gran parte per effettuare investimenti nel Metaverso, il valore delle azioni di Nvidia e AMD ha subito un'impennata rispettivamente del 30% e del 20% in quattro settimane.

Tutte le infrastrutture *cloud* necessarie per il Metaverso non saranno disponibili dall'oggi al domani. I nuovi *data center* richiederanno investimenti significativi per elaborazione, archiviazione, comunicazioni ed energia sostenibile.

6.1.7 La prospettiva economica

Siamo oggi alla vigilia di una rivoluzione informatica, il cui culmine sarà la diffusione capillare dello *spatial computing*, dove la navigazione abbandonerà la sua natura bidimensionale, per diventare qualcosa di estremamente pervasivo. Le *Big Tech* e le grandi aziende stanno manifestando il loro interesse nei confronti delle tecnologie che abilitano il Metaverso, sia da un punto di vista totalmente tecnologico, sia per quanto riguarda l'erogazione di servizi ed applicazioni sul Metaverso.

Quest'ultima tendenza sarà in grado di annullare le distanze fisiche, rendendo le aziende in grado di "arrivare" agli utenti, clienti e consumatori senza dover colmare un *gap* geografico.

Inoltre, è facile pensare che la diffusione del Metaverso con il tempo aprirà nuove prospettive anche nel mondo del lavoro, grazie alla capacità di smaterializzare la fisicità, migliorando lo sviluppo e la vendita di prodotti o servizi, ottimizzando i rapporti umani da remoto, fluidificando i processi aziendali (siano essi formativi o collaborativi), e infine evolvendo l'interazione con luoghi e

macchinari fisici. Si tratta infatti dell'interfaccia ideale, in quanto tridimensionale e diffusa nell'ambiente, per il nuovo paradigma di *computing* nello spazio già in parte adottato nelle fabbriche moderne grazie al processo di trasformazione noto come quarta rivoluzione industriale (o industria 4.0).

Altra rivoluzione economica strettamente correlata con il parziale trasferimento delle attività produttive sul Metaverso sta nella diffusione di mezzi di scambio non materiali. Il riferimento è chiaramente alla criptovaluta, visto che la finanza nel Metaverso è alimentata dalla blockchain.

Infatti, gli avatar all'interno del Metaverso parteciperanno a un'economia dove l'infrastruttura dei pagamenti è basata su *asset* virtuali, anche creando, acquistando e vendendo terreni, oggetti d'arte, accessori tutti digitali e unici. Sono i *Non-Fungible Token* (NFT), che non possono essere replicati, la cui proprietà e autenticità viene garantita dalla blockchain, e che sono a tutti gli effetti rappresentazioni digitali di oggetti del mondo reale.

Questa tendenza porta al tracciamento di diversi scenari futuri.

In primis, può aiutare la diffusione degli acquisti o della pubblicità *online*, offrendo una diversificazione dei canali di vendita e di promozione.

Inoltre, negli ultimi mesi, il volume delle transazioni per gli immobili commerciali in questo settore è aumentato.

In sintesi, il motivo principale per cui il Metaverso ha ottenuto questa importanza, si riscontra nel suo potenziale, volto a trasformare ogni aspetto della vita degli utenti, sia nella sfera professionale che personale. Rimane il fatto che si tratta ormai di un'opportunità di investimento multimiliardaria che muterà lo scenario economico in due modi: in primo luogo, fornendo uno strumento di investimento alternativo tramite blockchain, e in secondo luogo, aprendo nuove classi di attività.

Inoltre, trattandosi di un universo fortemente basato sulla decentralizzazione, perché possa funzionare più utenti devono partecipare alle sue operazioni investendo nel suo token di criptovaluta, che è intrinsecamente legato all'architettura della piattaforma. In breve, il funzionamento e il successo del Metaverso dipendono dall'attività di investimento.

Per concludere con alcuni numeri, questo fenomeno intercetta i capitali di società tecnologiche, *venture capital* e *private equity*, che hanno investito oltre 120 miliardi di dollari nei primi cinque mesi del 2022, più del doppio dei 57 miliardi di tutto il 2021, fa notare la società di consulenza McKinsey. Per gli analisti di Bloomberg, il mercato del Metaverso potrebbe raggiungere il valore di quasi 800 miliardi di dollari nel 2024, di cui circa la metà legata al comparto dei videogame, tra *software* e *hardware* ma anche servizi e pubblicità; altre fonti di entrate sono rappresentate dalle attività di intrattenimento legate a sport, musica e film: società sviluppatrici di videogame hanno già ospitato concerti nei loro giochi.

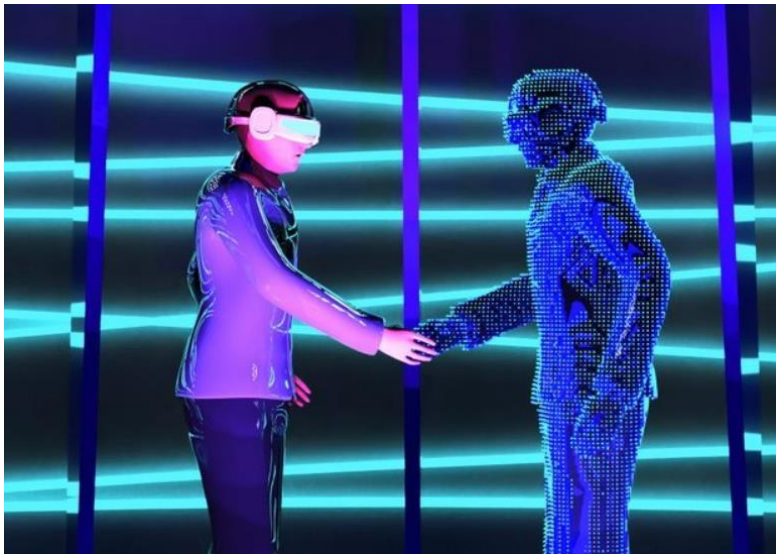
Al di là delle implicazioni economiche per il mercato videoludico, questa nuova frontiera di internet avrà conseguenze anche su altri settori. McKinsey sottolinea che il valore del Metaverso potrebbe raggiunge 5 mila miliardi di dollari entro il 2030 (800 miliardi di dollari entro il 2024), e stima un impatto fino a 2,6 migliaia di miliardi di dollari sull'e-commerce, fino a 270 miliardi sul mercato dell'insegnamento accademico virtuale, e fino 206 miliardi su quello della pubblicità.

Come rilevato dalla società di analisi Gartner, entro il 2026 il 25% delle persone trascorreranno almeno un'ora al giorno nel Metaverso per motivi di lavoro e di studio, per fare acquisti o semplicemente per socializzare e divertirsi. Un bacino di futuri utenti da non perdere per le aziende: un'analisi della banca JP Morgan, che ha anche aperto una sua sede nel Metaverso di Decentraland[127] riporta che ogni anno le vendite di beni virtuali raggiungono il volume complessivo di 54 miliardi di dollari mentre il *market cap* degli NFT nel 2021 ha toccato i 41 miliardi di dollari. Con lo sviluppo di queste realtà, gli approcci finanziari tradizionali e quello decentralizzato della blockchain potrebbero coesistere, fa notare Bcg, multinazionale della consulenza: nel 2021, circa 90 miliardi di dollari in denaro virtuale e fisico circolavano nel Metaverso.

6.1.8 Piattaforme

Esistono 141 mondi virtuali ma gli investitori puntano sulle piattaforme The Sandbox, Decentraland e Roblox, alle quali ad oggi afferiscono l'84% dei progetti.

I mondi virtuali sono popolati dagli Avatar di centinaia di milioni di persone, con regole, funzionalità e modelli di business differenti.



Chi ci ha investito fino ad oggi sono 220 aziende a livello globale, i progetti sono invece solo 308, l'84% dei quali è stato sviluppato su tre piattaforme: The Sandbox (43%), Decentraland (23%) e Roblox (15%) e queste rappresentano le piattaforme di riferimento sulle quali le aziende preferiscono avviare iniziative all'interno dei mondi più conosciuti e maturi.

[127] Metaverse Group ha sede a Toronto, ma ha un quartier generale virtuale in un mondo chiamato Decentraland nella Crypto Valley, che è la risposta del Metaverso alla Silicon Valley. Decentraland ha anche quartieri per il gioco d'azzardo, lo shopping, la moda e le arti.

Dei 141 mondi virtuali esistenti solo il 44% (62 piattaforme) è già Metaverse Ready, ossia è liberamente accessibile da chiunque, persistente (continua cioè a esistere in maniera indipendente dalla presenza o meno di un soggetto), economicamente attivo, dotato di grafica 3D, con componenti di interoperabilità che permetterebbero di utilizzare gli *asset* digitali in maniera *cross-platform*. Il 33% dei mondi è Open World, ossia è uno spazio virtuale aperto, persistente, modulabile e immersivo, come ad esempio Horizon Worlds, uno dei prodotti di punta di Meta. Infine, il 19% è della categoria Focused World, cioè dei mondi virtuali settoriali i cui progetti sono focalizzati su una particolare area di interesse (gaming, commercio, formazione, collaborazione lavorativa), come Fortnite e Microsoft Mesh. Ci sono poi Showrooming World (il 4% del totale), come Musee Dezentral, vetrine virtuali destinati all'esposizione, ad esempio per opere d'arte di artisti e collezionisti, senza la possibilità di creazione da parte dell'utente e senza la presenza di un'economia interna.

6.1.9 Criptovalute e speculazione

Gli utenti comprano e vendono contenuti di ogni tipo e NFT pagando attraverso una delle criptovalute (MANA, $$AND ect.) agganciate tipicamente alla blockchain Ethereum.

Verrebbe da fare il paragone con Monopoli, se non fosse per il fatto che si paga con i soldi veri. E sono tutt'altro che spiccioli: su The Sandbox è stata appena chiusa una transazione da 4,3 milioni di dollari. Finché questo denaro circola all'interno del Metaverso, è la singola piattaforma a fissare le sue regole: sempre The Sandbox, per esempio, ha imposto una tassa pari al 5% su ogni transazione. Chi accumula un tesoretto e lo converte in valuta corrente, però, è tenuto a dichiararlo al fisco.

Ma cosa succede nel momento in cui, per esempio, un artista va in tour nel Metaverso? Nell'autunno 2021 l'ha fatto la popstar Ariana Grande su Fortnite, incassando circa 20 milioni di dollari, *merchandising* incluso. Chi ha il diritto di tassare questo denaro? La giurisdizione nella quale si è esibita o lo Stato in cui risiede ogni membro del pubblico? Questo aspetto è ancora fumoso, si legge in un'analisi della società di consulenza EY. E non è l'unico. Quando si vende un terreno nel Metaverso, il ricavato è soggetto a IVA o va inquadrato come *capital gain* (rendimento di natura finanziaria) che fa salire il reddito?

L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) sta cercando di mettere a punto un quadro condiviso. Ma il processo richiederà ancora parecchio tempo, anche perché avrà senso solo se sarà sostenuto da un ampio consenso a livello internazionale. Nell'attesa, ciascuno Stato proverà a regolarsi a modo suo. «Ciò aggiunge un livello di complessità e rischio per le imprese internazionali che devono navigare con attenzione in questo panorama fiscale in rapida evoluzione», sottolinea EY.

6.1.10 Investimenti

Quanto ai progetti, la maggioranza riguarda i settori del *Retail* (30%), dell'*Entertainment* (30%) e dell'IT (17%), ma si trova anche un 9% di progetti *Finance and Insurtech* e il 5% *Food&Beverage*. La maggior parte propone servizi per intrattenere la *Community* dei *brand* e attirare nuovi *target*, per aumentare la visibilità o fornire ai consumatori un nuovo *touchpoint* per l'acquisto di prodotti.

6.1.11 Vantaggi competitivi

Nuovi canali di interazione con i clienti, uffici digitali in cui riunirsi con il proprio team, asset digitali da vendere o assicurare attraverso i quali trarre profitti, sono solo alcune delle potenzialità che le compagnie nel settore assicurativo, bancario, *retail*, *food* possono sfruttare nel Metaverso.

Il Metaverso avrà un impatto nella maggior parte dei comparti economici nei prossimi anni, con opportunità di mercato stimate in oltre 1.000 miliardi di dollari all'anno. Si stima che l'economia del Metaverso possa raggiungere un valore compreso tra gli 8.000 e i 13.000 miliardi di dollari entro il 2030. Inoltre, se la tecnologia sarà disponibile sugli *smartphone*, il numero di utenti potrebbe crescere fino a quasi 5 miliardi, ovvero circa il 60% della popolazione mondiale.

Il Metaverso è una rete di realtà digitali, sia aumentate che virtuali, che permette agli utenti di interagire in modo immersivo. Si tratta di un nuovo modo di vivere internet, in costante crescita, che offre nuove possibilità di comunicazione, di intrattenimento e apre a nuove opportunità commerciali.

Una nuova *customer experience*, totalmente rinnovata e all'avanguardia, per mostrare ai clienti prodotti e servizi in modo immersivo e coinvolgente, con agenti e assistenti virtuali disponibili 24/7, senza necessità per il cliente di doversi recare fisicamente ad un appuntamento; la possibilità di ampliare la propria offerta dedicando alla clientela nuovi prodotti basati su *asset* virtuali (come ad esempio NFT) e consulenze per la gestione dei rischi nel Metaverso; l'opportunità di espandere la base dei propri clienti attraverso campagne di *marketing* innovative, sia raggiungendo nuovi *target* sia offrendo servizi e prodotti a prezzi competitivi a persone di altre geografie; la riduzione dei costi operativi grazie alla natura digitale del Metaverso; una maggiore visibilità e il presidio di questo spazio prima della concorrenza, posizionandosi come *leader* nel settore di riferimento del Metaverso.

Inoltre, va ricordato che alla base di questa trasformazione del settore assicurativo vi è sempre l'innovazione tecnologica: il connubio tra tecnologie di realtà aumentata e realtà virtuale; le reti 5G/6G come abilitatrici di connessioni e relazioni in *real time*; paradigmi come la Blockchain per sviluppare modelli sicuri e affidabili per il trasferimento del valore o economie digitali decentralizzate in mondi virtuali. L'incastro tra tutti questi fattori tecnologici può consentire alle aziende di offrire servizi all'avanguardia e differenzianti per una clientela sempre più digitale, esigente e in costante evoluzione.

6.2 Le sfide da affrontare

Dopo il clamore mediatico iniziale ci si è accorti che il Metaverso con la M maiuscola ancora non c'è. Quello di Zuckerberg, il più ambizioso, è ancora nei laboratori e rischia di rimanere impantanato dalla crisi che sta colpendo tutto il *Big Tech* Usa. Per gli altri non ci sono *standard* comuni, manca un progetto di interoperabilità che possa spingere gli abitanti dei "nuovi mondi" a creare nuovi contenuti. E le aziende a investire in progetti di comunicazione e servizi trasversali e sostenibili.

Vi sono molte questioni da affrontare.

Una prima questione che pone il Metaverso riguarda la *Governance*. A chi spetta la regolamentazione, alla legge dello Stato, al diritto internazionale o alle regole private dei gestori di ciascun Metaverso?

Poiché il Cyberspazio non ha frontiere, la regolamentazione di un singolo Stato sarebbe ineffettiva, così come il pluralismo giuridico delle diverse piattaforme non garantirebbe la certezza del diritto e, soprattutto, il rispetto dei diritti fondamentali. "L'incertezza in termini di governabilità rischia giocoforza di indebolire la tutela dei diritti dei soggetti che operano in questa nuova dimensione e rende più difficile una disciplina unitaria"[128].

La soluzione è nella co-regolamentazione pubblico-privato[129], all'interno di un sistema a due livelli in cui l'autoregolazione delle piattaforme private si sviluppi nel solco di una normativa pubblicistica essenziale e con portata universale (ad esempio attraverso una Convenzione delle Nazioni Unite), che assicuri il livello di tutela minimo dei diritti fondamentali. Sono fatte salve legislazioni più garantiste degli Stati, che dovranno essere osservate dalle piattaforme che operano nei relativi ordinamenti.

Oltre al rispetto dei diritti fondamentali, ivi naturalmente compresa la protezione dei dati personali, la disciplina pubblicistica dovrebbe prevedere disposizioni in ordine a:

- l'interoperabilità dei Metaversi, in modo che "nessun singolo attore privato dovrebbe detenere la chiave della piazza pubblica o stabilirne i termini e le condizioni";
- la cooperazione tra gli Stati e tra gli Stati e il settore privato, con la possibilità per i fornitori di servizi di fornire i dati in loro possesso autonomamente o su richiesta (eventualmente

[128] Così CELOTTO A., *Tema del "Metaverso" e delle sue implicazioni per l'ordinamento giuridico*. Audizione presso il Senato della Repubblica, 6 luglio 2022.

[129] In senso conforme FROSINI T.E., *Il costituzionalismo nella società tecnologica*, *cit.*, pag. 482, per cui "le poche ed essenziali leggi statali ed europee si verrebbero a integrare con una politica di *self-regulation* da parte degli utenti di internet. Una sorta di applicazione del principio di sussidiarietà, in cui la *co-regulation* dello Stato può venire in sussidio alla *self-regulation* degli utenti, quando questi la evocano ovvero quando la necessitano".

filtrata da un controllo) delle autorità competenti di altri Stati[130] in relazione a scopi predeterminati[131];

- i criteri per individuare la legge penale applicabile e, conseguentemente, la giurisdizione;
- il foro competente per le controversie civili (ad esempio per esigere il rispetto delle regole interne alla piattaforma alla quale si è aderito), individuabile nel luogo di residenza o di domicilio dell'utente del servizio, da adire previo accesso agli organi di soluzione interna delle controversie. In caso di responsabilità civile, la collaborazione tra Stati dovrà garantire che la sentenza ottenuta nello Stato del foro competente sarà riconosciuta anche nello Stato ove è stata costituita la società che gestisce la piattaforma oppure risulta residente l'utente responsabile del danno;
- l'imposizione degli obblighi, in capo ai medesimi fornitori di servizi, previsti dalla Direttiva (UE) 2015/849, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. La partnership pubblico-privata sarebbe così ulteriormente rafforzata grazie al principio della collaborazione articolata sugli obblighi di adeguata verifica della clientela, registrazione e segnalazione delle operazioni sospette[132];
- l'identità o comunque l'identificazione dell'utente. Fatta salva la più incisiva previsione di identificare in maniera univoca gli utenti, in modo che ogni avatar sia inequivocabilmente associato ad un'identità digitale[133] corrispondente ad una persona, fisica o giuridica, la collaborazione dei fornitori di servizi mira risalire all'identità reale dell'avatar ai fini

[130] Una previsione analoga costituisce la base del Secondo protocollo addizionale alla Convenzione sulla criminalità informatica (Convenzione di Budapest), firmato il 12.05.2022. In particolare, il Protocollo fornisce strumenti per rafforzare la cooperazione e la divulgazione delle prove elettroniche – ad esempio, cooperazione diretta con fornitori di servizi e archivi, mezzi efficaci per ottenere informazioni sugli abbonati e dati relativi al traffico, cooperazione immediata in caso di emergenza o indagini congiunte – che sono soggetti a un sistema di diritti umani e Stato di diritto, tra cui garanzie in materia di protezione dei dati.

[131] Ad esempio, per lo svolgimento di indagini o procedimenti penali, anche attraverso le tecniche investigative speciali previste all'art. 9 della legge 16.03.2006, n. 146.

[132] Quest'ultima da trasmettere alla Financial intelligence Unit (FIU) dello Stato nel cui territorio è stato perfezionato il procedimento di costituzione. Sul tema si veda SORBELLO P., *La collaborazione pubblico-privato nella prospettiva antiriciclaggio. L'obbligo di segnalare le operazioni sospette come strumento di politica criminale*, in GULLO A.– MILITELLO V.– RAFARACI T. (a cura di), *I nuovi volti del sistema penale fra cooperazione pubblico-privato e meccanismi di integrazione fra* hard law *e* soft law, Giuffré, Milano, 2021, pag. 341.

[133] Al capitolo "identità digitale" i piani di transizione digitale sviluppati all'interno dei programmi nazionali di ripresa post-pandemica dedicano le risorse più ingenti e l'attenzione maggiore. Tra i passaggi cruciali relativi alla digitalizzazione delle identità si segnala la Determina 07.07.2022, n. 191, con cui l'Agenzia per l'Italia Digitale ha adottato le linee guida sull'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese. Il domicilio digitale è l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, valido ai fini delle comunicazioni elettroniche aventi valore legale. È un passaggio fondamentale per la piena esplicazione delle potenzialità delle identità digitali nell'erogazione dei servizi pubblici e nelle transazioni tra privati. Si veda SGUEO G., *L'identità digitale*, in BONTEMPI V. (a cura di), *Lo Stato digitale, cit.*, pag. 127 ss.

dell'accertamento un'eventuale responsabilità di natura civile o penale. Una simile previsione infonderebbe maggiore fiducia negli utenti (consumatori) del Metaverso[134];

- sistemi di pagamento (digitali, cripto o tradizionali) e forme di identificazione e proprietà (identificatori unici, NFT e blockchain);
- disciplina fiscale e criteri di "collegamento territoriale" del reddito per individuare lo Stato che esercita la potestà impositiva.

[134] "Le persone dovrebbero sentirsi al *sicuro* nei mondi virtuali come in quello reale". Così People, technologies & infrastructure. Europe's plan to thrive in the metaverse"

CONCLUSIONI

Il presente Studio ha preso in esame la multidimensionalità del progetto Metaverso, analizzandolo sui vari terreni su cui avverrà il suo completamento che segnerà, per la nostra società, un passaggio storico: da una fase di "digitalizzazione", compiuta dal 2000 al 2022, ad una di "virtualizzazione".

Ci troviamo all'inizio di un'esplosione di innovazione e sperimentazione in cui l'agire umano e artificiale si intrecciano e si integrano in un continuum che sfuma le linee di demarcazione tra esistenza fisica e simulazione. Nel Metaverso si stanno formando nuove comunità digitali in cui le identità si stanno suddividendo in due componenti complementari, quella reale e quella digitale, e le proprietà virtuali stanno diventando una classe indipendente di beni, permettendo all'economia reale di passare a uno stadio di sviluppo superiore e interdipendente con l'economia digitale.

Sebbene sia innegabile che un'attività economica con un volume di affari di miliardi di dollari rappresenti un bacino pressoché infinito di opportunità, è indispensabile anche ricordare che "quelle stesse qualità che rendono la realtà virtuale una tecnologia potenzialmente rivoluzionaria la rendono anche profondamente pericolosa".

Giganti della tecnologia come Facebook, Apple, Microsoft e Google stanno già sviluppando piani ambiziosi per materializzare il Metaverso. Con l'impegno delle tecnologie emergenti e il progressivo perfezionamento dell'ecosistema, il futuro digitalizzato sarà più interattivo, più vivo, più incarnato e più multimediale, grazie all'esistenza di potenti dispositivi di calcolo e di indossabili intelligenti. Le stesse qualità che rendono la realtà virtuale una tecnologia potenzialmente rivoluzionaria la rendono anche profondamente pericolosa.

Questo passaggio, tuttavia, non avviene all'improvviso ma è stato avviato e facilitato, in questi anni dall'impiego di nuove tecnologie con le quali sono stati creati ambienti virtuali 'immersivi', ancora mediati dal computer. L'applicazione ed interoperabilità con cui i sistemi delle tecnologie più avanzate oggi si stanno avvicinando ad una convergenza, fanno invece prospettare la creazione di un Cyberspazio condiviso, che sarà il Metaverso, in cui questa convergenza si trasformerà in una sempre maggiore e più profonda "integrazione" tra digitale e reale. Lo stesso suo possibile degrado o la sua disabilitazione potrebbero avere conseguenze disastrose in futuro proprio perché sia la società civile sia i militari diventano via via sempre più integrati e dipendenti dalla tecnologia.

Le principali criticità oggi presenti riguardano:

- **L'egemonia tecnologica: come una società, la politica e un paese potranno essere alterate dal Metaverso**

Quella che si prospetta con il Metaverso è una nuova 'realtà ibrida', in cui i confini tra reale e virtuale saranno così co-evoluti e con-penetranti da perdere persino la percezione stessa di sentirsi reali o virtuali e questo potrebbe portare ad un maggior controllo sociale. Un dominio della Tecnica sulla mente di masse di persone potrebbe portare governi autocratici a porsi l'obiettivo di voler riformare il sistema di *governance* globale di Internet modellando le norme internazionali nel Metaverso, e di guidare le organizzazioni internazionali che lo circondano. Oppure, plasmare ciò che i propri cittadini vedono, ascoltano e persino sentono interiormente mentre sviluppano una civiltà del Metaverso favorevole ai propri desideri e interessi strategici.

- **Rischi cognitivi e sociali**

Il rischio dell'impatto culturale è legato alla possibile disaffezione dei soggetti, soprattutto quelli delle ultime generazioni, nei confronti dell'idea stessa di Paese, scavalcato da processi culturali che leghino sempre meno la definizione dell'identità al luogo in cui si è nati e cresciuti e dove si hanno le proprie relazioni "reali", e sempre più a contesti virtuali ove si svolgono le proprie attività professionali, ludiche, sentimentali. Da questo scardinamento dell'idea di Paese potrebbero emergere nuovi nazionalismi digitali, che cerchino invece di creare percorsi di affermazione identitaria anche nella simulazione digitale in rete.

Il rischio di creare un mondo in cui vige un pensiero unico, visto che le nostre memorie, pensieri e culture si formano sulla base delle esperienze a cui siamo esposti. Considerando che negli universi digitali, le informazioni vengono memorizzate permanentemente, le ripercussioni a danno della sicurezza degli utenti e finanche della sicurezza nazionale potrebbero essere anche più gravi che nel mondo reale.

Il sovraccarico informativo, creato in ambienti virtuali immersivi, pone la questione dell'assenza di una costanza di stimoli ambientali, di cui il nostro cervello ha bisogno per attivare l'attenzione, e renderebbe i nostri schemi mentali non più validi per fare previsioni.

Desta preoccupazione la possibilità che un'identità digitale modifichi il comportamento di chi l'assume, fenomeno chiamato anche 'effetto Proteus'. In pratica il nostro cervello entrando in un corpo differente, modifica in maniera totalmente automatica le proprie simulazioni, facendo cambiare atteggiamenti, comportamenti e la percezione stessa di sé stessi.

Le d*eep fake* nel futuro Metaverso potranno sostituirsi alla realtà senza possibilità di dimostrazione del contrario. Questo significa che si possono dirottare verso personale militare o civile, in situazioni di crisi, informazioni logistiche distorte difficili da riconoscere. Un pervasivo controllo sugli individui potrà venir esercitato grazie alla raccolta di dati personali e sui

comportamenti degli utenti, in parte ottenute in tempi reali dagli utenti stessi e in parte rilevati dalle tecnologie (per esempio l'*eye tracking*).

- **La *Cyber security*: sicurezza informatica e dei dati.**

Man mano che la dipendenza e l'uso del Metaverso aumenteranno, i dati sensibili saranno condivisi ed a loro volta potrebbero essere considerati una nuova categoria delle infrastrutture critiche.

Le minacce connesse alla guerra ibrida si manifestano in modo veloce aggressivo. L'utilizzo sincronizzato di strumenti, tecniche o attività sono tutte orientate a creare gli effetti e le condizioni operative desiderate. I *toolbox* della guerra ibrida, ovvero *Information Warfare*, *Cyber Warfare*, e *Cognitive Warfare*, rappresentano tutte minacce effettive, reali e in espansione e troverebbero nel Metaverso potenziali applicazioni sempre maggiori.

Nelle sezioni dedicate si è fornito un quadro della relazione concettuale tra *Hybrid Warfare* e altri tipi di *Warfare* (*Information Warfare*, *Cyber Warfare* e *Cognitive Warfare*), che contengono elementi di influenza e impatto sulla cognizione umana e che pertanto possono aumentare di ampiezza e penetrazione nella nuova ecologia digitale.

- **La regolamentazione: necessità di una nuova disciplina ad hoc per far fronte a rischi etici e di sicurezza.**

Sul piano giuridico, il fenomeno è nuovo e manca ancora una disciplina di dettaglio ma ciò non significa che il Metaverso sia un Far West. I rapporti fra privati, quali la compravendita di beni nel Metaverso e altre attività ordinariamente svolte nel mondo reale, sono comunque disciplinati dalle norme generali perché l'ordinamento giuridico contiene una norma di auto integrazione che ne garantisce la funzionalità (art. 12 preleggi). In particolare, sul piano del diritto privato, a fronte di un'istanza di giustizia, il giudice non può rifiutare di decidere e in mancanza di una legge, applica quella che decide sul caso simile e se mancasse anche questa deciderebbe secondo i principi generali dell'ordinamento (c.d. Interpretazione analogica).

Sul piano del diritto penale, alcune fattispecie possono trovare applicazione concreta anche nel caso del Metaverso (ad esempio la truffa informatica o la diffamazione).

Sul piano del diritto tributario, se le attività nel Metaverso consentono dei guadagni, essi sono tassati come redditi diversi.

A fronte di queste prospettive di partenza, le tendenze in atto sono quelle di avere una disciplina ad hoc per il fenomeno, che sia affidabile in termini etici e di sicurezza.

- **Potenzialità e prospettive per le aziende.**

Rispetto alle potenzialità aperte dal Metaverso, lo Studio analizza i vantaggi competitivi che il Metaverso offre alle aziende, quale la *customer experience*, e come l'incastro tra tutti questi fattori tecnologici può consentire alle aziende di offrire servizi all'avanguardia e differenzianti per una clientela sempre più digitale, esigente e in costante evoluzione.

Inoltre, è facile pensare che la diffusione del Metaverso con il tempo aprirà nuove prospettive anche nel mondo del lavoro, grazie alla capacità di smaterializzare la fisicità, migliorando lo sviluppo e la vendita di prodotti o servizi, ottimizzando i rapporti umani da remoto, fluidificando i processi aziendali (siano essi formativi o collaborativi), e infine evolvendo l'interazione con luoghi e macchinari fisici.

Si tratta infatti dell'interfaccia ideale, in quanto tridimensionale e diffusa nell'ambiente, per il nuovo paradigma di *computing* nello spazio già in parte adottato nelle fabbriche moderne grazie al processo di trasformazione noto come quarta rivoluzione industriale o industria 4.0.

- **Potenzialità e prospettive per la Difesa.**

Lo sviluppo del Metaverso quale *Emerging & Disruptive Technology* potrà generare una spinta trasversale su ogni dominio scatenando accelerazioni e, contestualmente, decelerazioni imprevedibili e complesse da gestire e controllare. La rivoluzione in atto è ancora più marcata poiché se è vero che fino al secolo scorso l'innovazione tecnologica era trainata dall'industria militare, è altrettanto vero che in altri settori, ad oggi, è l'industria privata ad averne il monopolio. Operare in un siffatto contesto altamente complesso impone alla Difesa di pensare al futuro attraverso un'ottica predittiva ed integrata, mirando a disporre di reali capacità multidominio in grado di assicurare la sincronizzazione delle azioni e degli effetti.

Sebbene un Metaverso della Difesa può consentire una serie di benefici sociali ed operativi distinti, il suo vero valore dovrebbe emergere attraverso l'interconnessione dei vari mondi virtuali della Difesa, a condizione che l'interoperabilità sia prioritaria nella progettazione di questi ambienti virtuali fin dall'inizio. L'integrazione delle attività virtuali nella Difesa dovrebbe creare un ciclo di feedback iterativo, con un minimo sforzo umano, garantendo così che le lezioni apprese dall'addestramento, dalla formazione o dal reclutamento possano essere sfruttate durante i test e le sperimentazioni e viceversa.

Quale spunto finale questo studio intende prospettare alcune raccomandazioni che seppur nel breve periodo possano indicare una possibile *way ahead*. Il Metaverso richiede di essere affrontato con un approccio scientifico umanistico e regolatorio, all'altezza della svolta epocale che esso porterà in tutti gli ambiti di vita e di lavoro.

- **La regolamentazione.** Nel 2001 è stata firmata a Budapest la convenzione del Consiglio d'Europa sulla criminalità informatica. Si tratta finora dell'unico strumento di diritto internazionale (a carattere regionale) che disciplini i reati commessi tramite internet e sistemi informatici e telematici. Sebbene molti Stati si fossero già dotati di normative di contrasto ai reati informatici (in Italia la legge 547/1993) l'aspetto fondamentale di tale convenzione riguarda la cooperazione internazionale.

Analoga iniziativa dovrebbe essere adottata con una prospettiva universale, da parte delle Nazioni Unite, per ribadire il principio già affermato dalla convenzione di Budapest: quello che è illecito nel mondo reale, lo è anche in quello virtuale. L'ambito d'intervento dovrebbe essere però più ampio e andare oltre il diritto penale, considerando ad esempio:

- i profili dei diritti e i doveri dei consumatori del Metaverso, ivi compresa la questione dell'identità digitale in modo che ogni consumatore sia identificarono agevolmente identificabile;
- le necessità che comportano la compressione dei diritti, quali le ragioni di Difesa, sicurezza, ordine pubblico e repressione dei reati (ad esempio, un operatore telefonico esegue ordine autorità giudiziaria su intercettazione telefonica, la piattaforma di servizio deve consentire le attività tecniche volte alla repressione di reati);
- i criteri di collegamento tra Metaverso e giurisdizione (criterio della sede legale o del foro nazionale del consumatore);
- la cooperazione giudiziaria e di polizia;
- i criteri di riparto dell'imposizione fiscale;
- i doveri delle piattaforme di servizio, che dovranno, ad esempio, fornire assistenza alle autorità giudiziarie; predisporre delle unità interne chiamate a esaminare tempestivamente le segnalazioni degli utenti; stabilire delle *policies* che dovranno essere accettate dai fruitori dei servizi. A tal fine, sarebbe opportuno che nella formazione e validazione di tali *policies* siano coinvolti una rappresentanza dei consumatori, a garanzia di un minimo di democraticità.

La regolamentazione dovrebbe essere a due livelli: un primo livello, di base, riguarda la disciplina pubblica (ad esempio una convenzione internazionale, ratificata poi dai singoli Stati) che si occupa delle questioni essenziali sopra citate. Il secondo livello riguarda la regolamentazione di dettaglio stabilita dalla piattaforma di servizi ed accettata dal consumatore (le suddette *policies*). Una simile *partnership* pubblico-privato garantirebbe una disciplina completa e flessibile.

- **Il Ruolo della Difesa.** La Difesa può svolgere un ruolo importante contribuendo alla creazione e/o rafforzamento di strutture permanenti nazionali ed internazionali che

favoriscano collaborazione e prontezza nell'identificare e quantificare i rischi connessi al Metaverso nel breve e nel medio-lungo termine. Come descritto, la Difesa può trarre enormi benefici da un'applicazione guidata del Metaverso in taluni ambiti, in particolare quelli legati all'addestramento, al reclutamento ed al procurement.

Per quanto attiene la conduzione delle moderne operazioni militari, per quanto sia evidente come le applicazioni del Metaverso siano già integrate in alcuni sistemi militari, la Difesa dovrà sviluppare un approccio che permetta di impiegare, in materia integrata, tutte le proprie capacità (cinetiche e non cinetiche) per contribuire a generare effetti, anche attraverso l'ambiente informativo, nella dimensione cognitiva ed in quella virtuale. La pervasività dell'elemento tecnologico non sostituirà, tuttavia, la posizione preminente dell'uomo, che manterrà la sua centralità anche se all'interno di nuovi paradigmi gestionali. La sempre maggiore rilevanza dei nuovi domini e l'evoluzione della competizione richiederanno maggiori investimenti in termini di risorse, anche umane che, attraverso lo sviluppo di percorsi formativi e di profili di impiego dedicati, acquisiscano competenze differenti e diversificate.

L'Intelligenza Artificiale sarà uno degli aspetti determinanti che cambieranno radicalmente la natura stessa del campo di battaglia del futuro. Sarà quindi prioritario pensare ad un approccio proattivo teso ad assumere un ruolo di primo piano nell'implementazione dell'IA al fine di mantenere costante il livello tecnologico e conservare il vantaggio strategico sugli opponenti. In particolare si dovrà promuovere la diffusione dell'IA prevedendone l'implementazione in tutti i livelli e settori della Difesa in un quadro coerente con il diritto internazionale ed il contesto etico-morale.

Per quanto attiene la regolamentazione, la Difesa dovrà essere presente in nuova forma perché, se è innegabile che alla dimensione reale si è ormai affiancata quella virtuale, dovrebbe logicamente conseguire che al territorio fisico si affianchi quello virtuale. L'esigenza di controllo del territorio, fissata dall'art. 7-bis (Concorso delle Forze armate nel controllo del territorio) del D.L. 23.05.2008 n. 92 potrebbe costituire un modello per fronteggiare quelle "specifiche ed eccezionali esigenze di prevenzione della criminalità, ove risulti opportuno un accresciuto controllo del territorio", ivi compreso quello virtuale. Per rispondere però a questo compito, le Forze Armate devono essere preparate sul piano tanto tecnologico quanto delle risorse umane.

- Rimane infine una considerazione finale che riguarda un piano di intervento più generale, che abbracci la dimensione di **sviluppo della società futura**; è infatti fondamentale ribadire come il superamento in potenza della Tecnica sulle capacità umane, già avvenuta nel nostro presente, debba richiedere di trovare valori che sostanzino la direzione delle politiche e diano scopi all'evoluzione del percorso umano, anche nel suo rapporto con la Tecnica, con un apparato filosofico e culturale che renda capace la società di 'dare senso' al mondo. Come

ci ricorda Frank Pagano, “Il Metaverso non esiste, almeno adesso, nella sua espressione massima. Il Metaverso esiste perché è fattibile da un punto di vista tecnico. Il grosso del cammino verso un mondo nuovo rimane, paradossalmente, una decisione **etica, politica e culturale**”.

BIBLIOGRAFIA

- AHARON B., (2002) *Foreword: A Judge on Judging: The Role of a Supreme Court in a Democracy*, in Harvard Law Review, vol. 116, 16, 2002.
- ASIMOV I., (2018) *Io, robot* (trad. it. LATRONICO V.), Mondadori, Milano, 2018.
- FALZEA A., (2010) *Ricerche di teoria generale del diritto e di dogmatica giuridica*, Giuffré, Milano, III, 2010.
- FASSÒ G., (1964) *Il diritto naturale*, Eri, Torino, 1964.
- FERRAJOLI L., (2010) *Sui fondamenti dei diritti fondamentali. Un approccio multidisciplinare*, in *Studi sulla questione criminale*, 2/2010.
- FLORIDI L. (2017) *La quarta rivoluzione. Come la Ionosfera sta trasformando il mondo*, Milano, Raffaello Cortina, 2017
- FLORIDI L., CABITZA F., (2021) *Intelligenza artificiale. L'uso delle nuove macchine* Milano, Bompiani, 2021
- FROSINI T.E. (2020), *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informazione e dell'informatica*, 3/2020.
- GALIMBERTI, U. (2021) *Il libro delle emozioni*, Mliano, Feltrinelli, 2021
- GALLACE A. (2022) *Cervelli reali in mondi virtuali: psicologia e neuroscienze del Metaverso* in MONTAGNA L. (2022), *Metaverso - Noi e il web 3.0*, Milano, Mondadori, 2022
- GLENN Russell W. (2009), Evolution and Conflict: Summary of the 2008 Israel Defense Forces-U.S. Joint Forces Command "Hybrid Threat Seminar War Game," Santa Monica, CA: RAND,TBP in 2009. *This document will not be available to the general public*
- HOFFMAN, Frank G. (2007) *Conflict in the 21st century: The rise of Hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.
- HOFFMAN, Frank G. (2018), *Examining Complex Forms of Conflict* PRISM 7, no. 4 (2018): 30–47; Fridman, Russian "Hybrid Warfare"; Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy," International Affairs 95, no. 2 (2019): 255–275;
- KANT I. (1991), *Per la pace perpetua*, Feltrinelli, Milano, 1991
- La Lettura (2022), *Sono Einstein (oppure Hitler). È il Metaverso*. "Corriere della Sera", 27.02.2022, pp.8-9
- MAZZARELLA E (2022) *Contro Metaverso. Salvare la presenza*, Milano, Mimesis, 2022
- MONTAGNA L., (2022) *Metaverso - Noi e il Web 3.0* Milano, Mondadori - Electa, 2022

- NEMETH, W. (2002) *Future war and Chechnya: a case for Hybrid warfare*, Naval Postgraduate School, Monterey, Tesi per il Master, 2002.
- NUNZIATA M., (1996) *Il reato di accesso abusivo in un sistema informatico o telematico,* Ponte Nuovo Editrice, Bologna, 1996
- PAGANO F., SOLDAVINI P., (2022) *Il capitale decentralizzato. Blockchain, NFT, Metaverso.* Il Sole 24 ore, Milano, 2022.
- PORCHE Isaac R. III et.al, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Santa Monica 2013
- SEVERINO E, (2010) *Macigni e Spirito di Gravità. Riflessioni sullo stato attuale del mondo*, Milano, Rizzoli, 2010
- SORBELLO P. (2014), *I diritti fondamentali come limite alla politica criminale*, in Riv. Guardia di Finanza, 6/2014.
- VIOLA F. (2001), *Etica dei diritti*, in VIGNA C. (a cura di), *Introduzione all'etica*, Vita e Pensiero, Milano, 2001.
- WIGELL Mikael (2019), *Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy*, International Affairs, Vol. 95, Issue 2, March 2019, Pages 255–275

SITOGRAFIA

- ABLAZOV I., DEMENKO O., LEONOV O., MOKLIAK S., & KHAMULA S. (2022). *Information weapons within the interstate struggle in the XXI Century*. Amazonia Investiga 11(52) 269-277 https://doi.org/10.34069/AI/2022.52.04.29
- BARGH John A., McKENNA Katelyn Y. A. (2004) *The Internet and Social Life*; Annual Review of Psychology; Vol. 55:573-590 (Volume publication date 4 February 2004); https://doi.org/10.1146/annurev.psych.55.090902.141922
- BAUGHMAN J., *Attacking the Metaverse*, Cyber - the Magazine of the MCPA, Military Cyber Professionals Association, 31.03.2022 https://public.milCyber.org/activities/magazine/articles/2022/baughman-attacking-the-metaverse#h.5szsahcsw0zo
- BAY Sebastian & BERTOLIN Giorgio et al. (2019). *Responding to Cognitive Security Challenges*. Nato Strategic Communications Centre of Excellence https://www.researchgate.net/publication/338764711_Responding_to_Cognitive_Security_Challenges
- BRETON Thierry (2022) *People, technologies & infrastructure – Europe's plan to thrive in the metaverse* I Blog of Commissioner Thierry Breton 14.09.2022: https://ec.europa.eu/commission/presscorner/detail/de/STATEMENT_22_5525
- BUCCI Francesco Saverio, CRISTOFARO Matteo, GIARDINO Pier Luigi (2021), *Infodemia e pandemia: la cognitive warfare ai tempi del SARS-CoV-2* CASD https://www.casd.it/mod/resource/view.php?id=17501&forceview=1
- CAMILLE F., BASDEVANT A., RONFARD R. (2022), *Mission exploratoire sur les métavers* Paris, Rapport Officiel, Ministère de la Culture, Ministère de l'économie, des finances et de la souveraineté numérique et industrielle, 2022 scaricabile da https://www.vie-publique.fr/rapport/286878-mission-exploratoire-sur-les-metavers
- CAPO G., *Internet, impresa, contratti. Atti digitali del convegno gli stati generali del diritto di internet*, Luiss 16-18.12.2021: https://dirittodiinternet.it/wp-content/uploads/2022/01/01-supplemento.pdf
- CELOTTO A., *Facebook sta diventando uno Stato? Una paradossale retrocessione: da cittadini statali a sudditi digitali*, in Huffingtonpost.it, 05.01.2021.
- CLARIZIA R. (2021), *Internet: gli interrogativi del civilista. Atti digitali del convegno gli stati generali del diritto di internet*, Luiss 16-18.12.2021: https://dirittodiinternet.it/wp-content/uploads/2022/01/01-supplemento.pdf

- COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA COMUNICAZIONE, LEYEN U. (2019), *Un'Unione più ambiziosa. Il mio programma per l'Europa: orientamenti politici per la prossima Commissione europea 2019-2024*, 2019: https://op.europa.eu/it/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1/language-it
- COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLE RETI DI COMUNICAZIONE, DEI CONTENUTI E DELLE TECNOLOGIE (2019), *Orientamenti etici per un'IA affidabile*, 2019: https://op.europa.eu/it/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-it
- CRANNY-EVANS Samuel (2022) *Fields of silence and broken cycles: Russia's electronic warfare* Global Defence Technology 03.2022 *https://defence.nridigital.com/global_defence_technology_mar22/russia_electronic_warfare*
- CROSS TIM, (2022) *A reality check for the metaverse is coming. Is it really the next big thing? Watch this virtual space*, The Economist, The World Ahead 2023, 14.11.2022 https://www.economist.com/the-world-ahead/2022/11/14/a-reality-check-for-the-metaverse-is-coming
- DE FALCO Marco (2012), *Stuxnet Facts Report. A Technical and Strategic Analysis* NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) Tallin, Estonia 2012 https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf
- DELLA TORRE J. (2022), *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in DI PAOLO G. – PRESSACCO L. (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove e giudizio*, Università degli Studi di Trento, Quaderni della Facoltà di Giurisprudenza, 63, 2022: https://iris.unitn.it/retrieve/handle/11572/361122/598564/IAiris20.12.22.pdf
- EUROPOL (2022), *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*, Publications Office of the European Union, Luxembourg, 2022
- FLORIDI, Luciano (2022), *Metaverse: A Matter of eXperience* (May 27, 2022). Philosophy & Technology September 2022, Scaricabile da SSRN: https://ssrn.com/abstract=4121411
- GALEOTTI M, (2014) *The 'Gerasimov Doctrine' and Russian Non-Linear War, 06.07.2014* https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
- GLENN R., Thoughts on Hybrid Conflict, Small Wars Journal, 2 marzo 2009 https://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf
- JOINT CHIEFS OF STAFF Joint Publication 3-13 2012 (change 1 2014) https://irp.fas.org/doddir/dod/jp3_13.pdf

- JOINT DOCTRINE NOTE 1/18 (2018) *Cyber and Electromagnetic Doctrine* UK Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_Cyber_and_electromagnetic_activities_jdn_1_18.pdf
- KENNY RYAN, (2022) *The Military Metaverse and the Future of Large-Scale Combat Operations*. *New approaches are needed to ensure victory in future operations*. Fairfax Virginia, 2022, AFCEA (Armed Forces Communications and Electronics Association) 1.08.2022 https://www.afcea.org/signal-media/Cyber-edge/military-metaverse-and-future-large-scale-combat-operations
- KOFMAN M., FINK A., GORENBURG D.et al., (2021) *Russian Military Strategy: Core Tenets and Operational Concepts,* CNA's Strategy, Policy, Plans, and Programs Division, Arlington, VA, CNA 2021 https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf
- LEE Lik-Hang, BRAUD Tristan, ZHOU Pengyuan et al. (2021), *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*, Journal of Latex Class Files, Vol. 14, No. 8, September 2021 scaricabile da https://www.researchgate.net/publication/355172308_All_One_Needs_to_Know_about_Metaverse_A_Complete_Survey_on_Technological_Singularity_Virtual_Ecosystem_and_Research_Agenda
- MASCOLO A., (2022) *L'uso dell'Intelligenza Artificiale nel settore pubblico*, in BONTEMPI V. (a cura di), *Lo Stato digitale nel piano nazionale di ripresa e resilienza*, RomaTre Press, 2022: https://romatrepress.uniroma3.it/libro/lo-stato-digitale-nel-piano-nazionale-di-ripresa-e-resilienza/
- MELE S., (2013) *Cyber-weapons: aspetti giuridici e strategici* Roma, Edizioni Machiavelli, 2013 https://www.strategicstudies.it/wp-content/uploads/2013/06/Edizioni-Machiavelli-Cyber-Weapons-Aspetti-Giuridici-e-Strategici-V2.0.pdf
- Ministry of Defence of the Russian Federation *Russian Federation Armed Forces' Information Space Activities Concept https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle*
- MONTI A., (2022) *Musk, Twitter e il potere di comprare il diritto*, in Repubblica.it, 05.05.2022
- NGUYEN Tuong, JUMP Annette, CASEY Danielle Casey, (2023) *Emerging Tech Impact Radar*: *Explore the technologies with the most potential to disrupt,* Gartner Research Stamford, CT, Gartner 2023 *https://www.gartner.com/en/doc/emerging-technologies-and-trends-impact-radar-excerpt*

- PARLAMENTO EUROPEO, (2022) *Risoluzione del 20.10.2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html
- PISANI N. (2021), Intelligenza artificiale e criteri di imputazione della responsabilità penale. Atti digitali del convegno gli stati generali del diritto di internet, Luiss 16-18.12.2021: https://dirittodiinternet.it/wp-content/uploads/2022/01/01-supplemento.pdf
- PISSANIDIS N., ROIGAS H, VEENENDAAL M.(Eas),(2016), *Cyber Power 8th International Conference on Cyber Conflict,* NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) Tallin, Estonia 31 May - 03 June 2016, https://ccdcoe.org/uploads/2018/10/CyCon_2016_book.pdf
- Rapporto *«L'Europa e la società dell'informazione globale. Raccomandazioni al Consiglio europeo*", presentato il 26 maggio 1994, intitolato dal Gruppo di lavoro presieduto da Martin Bangemann, Commissario europeo per le telecomunicazioni: https://op.europa.eu/it/publication-detail/-/publication/31a0bebe-4bc6-4f31-a319-7b7799e45d86
- SALVI G.,(2023) *Attuazione della giurisdizione penale nello spazio virtuale e sicurezza nazionale.* Intervento di apertura dell'anno accademico della Scuola Superiore di Polizia 2022/2023 Roma, 27 ottobre 2022, in Sistema penale: https://www.sistemapenale.it/it/documenti/salvi-intervento-apertura-anno-accademico-scuola-superiore-di-polizia-2022-2023
- SANCHEZ L., MILLER J. (2010), *Hybrid Warfare,* USA Government Accountability Office The Honorable Adam Smith House of Representatives10.09.2010 https://www.gao.gov/assets/gao-10-1036r.pdf
- SHAY Shaul (2021) *Between Kiev and Venice The cognitive warfare and the Biennale of Venice* Vol. 3 No. 2, 2022. Zagreb Security Science Journal https://zagrebsecurityforum.com/Portals/0/SecurityScienceJournal/SSJ%203_2_6%20Between%20Kiev%20and%20Venice.PDF
- STATO MAGGIORE DELLA DIFESA, Ufficio Generale Informazione Difesa (UGID), *Approccio della Difesa alle Operazioni Multidominio,* Edizione 2022. https://www.difesa.it/SMD_/Staff/Sottocapo/UGID/Documents/Concetto_Approccio_Difesa_alle_Operazioni_Multidominio_2022.pdf
- STATO MAGGIORE DELLA DIFESA, Ufficio Generale Informazione Difesa (UGID), *L'impatto delle Emerging & Disruptive Technologies (EDTs) sulla Difesa*, Ufficio Generale Innovazione Difesa, Edizione 2022. https://www.difesa.it/SMD_/Staff/Sottocapo/UGID/Dottrina/Documents/Concetto_Impatto_delle_EDT_sulla_Difesa_Ed_2022.pdf

- STATO MAGGIORE DELLA DIFESA, Centro Innovazione Difesa (CID), *Concetto Scenari Futuri: tendenze ed implicazioni per la Sicurezza e la Difesa*, Edizione 2021 https://www.difesa.it/SMD_/Staff/Sottocapo/UGID/Documents/Concetto_Scenari_Futuri_CSF_versione_Ufficiale_new.pdf
- STOLTON SAMUEL, (2022) *Vestager: Metaverse poses new competition challenges. The EU's digital czar says, 'We should start thinking about it now' when it comes to regulating new digital spaces.* Politico, 18.01.2022, https://www.politico.eu/article/metaverse-new-competition-challenges-margrethe-vestager/
- STUPPLES D., (2015) *The next war wil be an Information war, and we're not ready for it*, The Conversation 26.11.2015: https://theconversation.com/the-next-war-will-be-an-Information-war-and-were-not-ready-for-it-51218
- TOM's HARDWARE (2019) *Facebook può essere una minaccia per le Forze Armate? Un esperimento della NATO lascia a bocca aperta,* Il Fatto Quotidiano,19.02.2019 https://www.ilfattoquotidiano.it/2019/02/19/facebook-puo-essere-una-minaccia-per-le-forze-armate-un-esperimento-della-nato-lascia-a-bocca-aperta/4982410/
- TZU-CHIEH Hung, TZU-WEI Hung,(2022) *How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-DisInformation Wars*, Journal of Global Security Studies, Volume 7, Issue 4, December 2022, https://doi.org/10.1093/jogss/ogac016
- VANORIO Fabio (2021), *Metaverso e Sicurezza Nazionale.Internet 3.0 e Nuovo Ordine Mondiale Digitale* Roma, Edizioni Machiavelli, 2021 paper scaricabile da: https://www.strategicstudies.it/wp-content/uploads/2021/12/Edizioni-Machiavelli-Metaverso-e-Sicurezza-Nazionale.
- VANORIO Fabio (2022), *Metaverse: Implications for Security and Intelligence* NATO Defense College Foundation 2022 Paper scaricabile da: https://www.natofoundation.org/wp-content/uploads/2022/02/NDCF-Paper-Vanorio-110222.pdf
- WARDLE C., DERAKSAN H., (2017) *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe, 23.09.2017 https://edoc.coe.int/en/media/7495-Information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

GLOSSARIO

Questo glossario serve a chiarire i termini specialistici attinenti, i lemmi particolari che ricorrono nel testo di questo studio ed a volte, nonostante siano anglicismi, son già divenuti neologismi piuttosto frequenti nel linguaggio comune.

Non pretende di essere completo né esaustivo bensì di chiarire ed aiutare a comprendere.

AI - *Artificial Intelligence*

Vedasi IA

AR - Augmented Reality

Vedasi Realtà aumentata

Avatar

Alter Ego artificiale tecnologico

Big Tech Firm

Locuzione che si riferisce alle maggiori società nella tecnologia dell'informazione, in particolare le cinque maggiori multinazionali dell'IT: Alphabet (Google), Amazon, Apple, Meta (Facebook) e Microsoft. Queste aziende, altresì indicate come i "Big Five", godono di posizioni dominanti nelle rispettive aree tecnologiche: intelligenza artificiale, *cloud computing*, elettronica di consumo, *e-commerce*, domotica, pubblicità *online*, *social network*, *software* e *streaming* media.

Blockchain

La blockchain è un database condiviso e immutabile, definita come un registro digitale le cui voci sono raggruppate in blocchi concatenati in ordine cronologico la cui integrità è garantita dall'uso della crittografia

Cognitive Warfare

La Cognitive Warfare consiste nell'influenza e manipolazione del processo di decision-making. Basandosi su nuove tecniche delle neuroscienze e dei meccanismi cognitivi, unitamente all'utilizzo dell'Information warfare e della Cyber Warfare, la Cognitive Warfare ha come obiettivo la dimensione cognitiva. Contando sull'intrinseca vulnerabilità della mente umana è volta a minare, influenzare e rivoluzionare punti di vista, idee, convinzioni, opinioni

Criptovaluta

Termine che si riferisce ad una moneta digitale basata sulla crittografia che, a differenza delle monete tradizionali, non esiste in forma fisica e non è controllata né gestita da alcuna banca centrale. Le informazioni sulle transazioni in criptovaluta sono memorizzate in un registro digitale basato sulla tecnologia blockchain. Criptovaluta o criptomoneta è l'italianizzazione del vocabolo inglese *cryptocurrency* che a sua volta è una crasi derivato dei termini inglesi *cryptography* ("crittografia") e *currency* ("valuta").

Cyber Operations (CO)

Le Cyber Operations mirano a creare effetti prima nel Cyberspace e poi nei domini fisici utilizzando e operando nella struttura interconnessa e integrata del Cyberspace. Possono essere utilizzate per scopi militari, politici, economici, sociali e criminali.

Cyberspace

Il Cyberspace è l'ambiente complesso formato da componenti fisici e non fisici, caratterizzati dall'uso di computer e dallo spettro elettromagnetico per archiviare, modificare e scambiare dati utilizzando reti di computer. Il Cyberspace si suddivide in tre livelli *layers*: *physical network, logical network* e *Cyber persona*.

Cyber Warfare

Cyber Warfare è una forma di conflitto che comprende diverse dimensioni concettuali, tra cui la dimensione tecnologica, strategica, legale e umana. In particolare è l'insieme delle operazioni, belliche e non belliche, condotte da un attore al fine di ottenere, distruggere, alterare le informazioni della controparte.

Deep fake

Vocabolo composito da due termini diversi: *deep learning* e *fake*. I deepfake sono media sintetici che sfruttano potenti tecniche di Machine Learning ed Intelligenza Artificiale ed utilizzano reti neurali generative per manipolare o generare contenuti visivi e audio che possono ingannare facilmente. Tali tecniche possono essere utilizzate per creare notizie false.

DT - *Digital Twin*

Vedasi Gemello Digitale

Effetto Proteo

Fenomeno secondo cui il comportamento di un individuo, all'interno di mondi virtuali, viene non soltanto influenzato ma effettivamente modificato dalle caratteristiche del proprio avatar. Quando un individuo ritiene che gli altri si aspettino determinati comportamenti a causa dell'aspetto dei loro avatar, si impegna nell'attuare i comportamenti attesi.

ER - *Extended Reality*

Vedasi Realtà estesa

Eye Tracking

L'oculometria (in inglese *eye-tracking* o *gaze-tracking*) riunisce una serie di tecniche per la registrazione dei movimenti oculari. I più comuni *eye-tracker* analizzano le immagini dell'occhio umano registrate da una telecamera per calcolare la direzione dello sguardo.

FT - *Fungible Token*

Token interscambiabili, uguali l'uno all'altro. È il caso, per esempio, delle cryptovalute.

Gaming

Attività ludica accresciuta, potenziata e resa ancor più pervasiva dal punto di vista d'intrattenimento ed esperienziale, tramite ER/RV e Metaverso.

Gemelli digitali

Gemello digitale, ovvero replica perfetta di un oggetto, clone virtuale del soggetto reale.

Tale riproduzione virtuale consente di testare l'oggetto od il suo funzionamento tramite simulazione di utilizzo.

Guerra ibrida

La guerra ibrida è la sfida presentata dalla crescente complessità dei conflitti armati, in cui gli avversari possono combinare più mezzi non militari per neutralizzare la potenza militare convenzionale

Hybrid Warfare

Vedasi Guerra Ibrida

IA - Intelligenza Artificiale

Intelligenza delle macchine che percepisce, sintetizza, deduce informazioni ed agisce razionalmente: il processo che porta il sistema intelligente a risolvere il problema è quello che gli permette di ottenere il miglior risultato atteso date le informazioni a disposizione.

Information Warfare

Uso strategico delle informazioni volto ad influenzare, manipolare, disturbare o distruggere un avversario. L'IW può essere suddiviso in diverse attività ostili, comprese le operazioni di propaganda, la manipolazione dei media, l'uso di disinformazione e altre tattiche simili che prevedono in maniera massiccia l'impiego di tecnologie informatiche.

IoT - Internet Of Things

Espressione che richiama l'interconnessione tra Internet ed oggetti, luoghi ed ambienti fisici; denota un numero sempre crescente di oggetti connessi *online*, con propria identità digitale e conseguente intercomunicazione permettendo la raccolta di nuove masse di dati, nuove conoscenze e forme di conoscenza.

ITC - *Information and Communication Technologies*

La Tecnologia dell'Informazione e della Comunicazione (ICT) è una locuzione più estesa per la tecnologia dell'informazione (IT) che ne mette in evidenzia le comunicazioni unificate, l'integrazione delle telecomunicazioni (linee telefoniche e segnali *wireless*) e dei vari dispositivi di comunicazione (radio, televisione, telefoni cellulari, computer, sistemi satellitari etc.) e dei necessari *software, middleware*, che consentono agli utenti di accedere, archiviare, trasmettere, comprendere e manipolare le informazioni.

Metaverso

Metaverso è il crescente regno digitale che utilizza la Realtà Aumentata, la Realtà Virtuale, la Blockchain, i *social media* ed una vasta serie di altre tecnologie, nella loro combinazione volte alla creazione un mondo virtuale in cui milioni di persone, attraverso il proprio avatar, si connettono e interagiscono in un universo creato nel Cyberspazio.

Minacce ibride

Ampia gamma di mezzi non violenti per colpire le vulnerabilità dell'intera società per minarne funzionamento, unità o volontà dei loro obiettivi, degradando e sovvertendo allo stesso tempo lo

status quo. Strategia attuata per aggiungere gradualmente i propri obiettivi senza innescare risposte decisive, comprese quelle armate

MR - Mixed Reality

Vedasi Realtà Mista

MSF - Metaverse Standard Forum

Luogo per il coordinamento tra le varie organizzazioni di standardizzazione e l'industria, con la missione di promuovere la standardizzazione pragmatica e tempestiva che sarà essenziale per un Metaverso aperto e inclusivo.

NFT - Non-Fungible Token

Un token non fungibile (NFT) è un identificatore digitale univoco che non può essere copiato, sostituito o suddiviso, registrato in una blockchain ed utilizzato per certificare al contempo l'autenticità e la proprietà.

Proteus Effect

Vedasi Effetto Proteo

RA - Realtà Aumentata *(AR - Augmented Reality)*

Possibilità di vedere oggetti, immagini, video, dati numerici o scritti che sono sovrapposti al proprio campo visivo tramite app del proprio smartphone o con specifico visore.

RE - Realtà estesa *(Extended Reality)*

Espressione inerente agli ambienti combinati (reali e virtuali) ed alle interazioni miste uomo-macchina generate dalla tecnologia informatica e dai dispositivi indossabili (es.: visori).

RM - Realtà Mista *(Mixed Reality)*

Stessa situazione che con la AR (vedasi definizione) dunque la possibilità di vedere oggetti, immagini, video, sovrapposti al proprio campo visivo tramite app o con specifico visore ma con l'opportunità di vedere e di manipolare ologrammi, oggetti 3D, gemelli digitali.

RV - Realtà Virtuale *(Virtual Reality)*

Possibilità di ingresso virtuale in una dimensione digitale tramite visore. Possibilità di vedere perfettamente luoghi ed ambienti tramite foto e/o video 3D girati a 360° e/o di entrare, muoversi ed interagire in ambienti iperrealistici di computer grafica

Spatial computing

Con l'avvento delle varie RV - Realtà Virtuale, RA - Realtà Aumentata, RE - Realtà Estesa, RM - Realtà Mista, lo "*spatial computing*" si riferisce alla pratica di utilizzare azioni fisiche (capo e movimenti del corpo, gesti, parole) come input per sistemi multimediali digitali interattivi, con lo spazio fisico 3D percepito come tela per output video, audio e tattili. È strettamente collegato al concetto di ' gemelli digitali '.

VR - Virtual Reality

Vedasi Realtà Virtuale

Web 1.0 (pc e informazione)

Primo paradigma di programmazione web realizzato con pagine HTML i cui contenuti erano modificabili esclusivamente dall'amministratore stesso o dal proprietario del sito web.

A causa di questo tipo di comunicazione, l'interazione tra utente e fornitore di contenuti è sostanzialmente univoca: l'utente può visualizzare i contenuti forniti ma non può modificare lo stato né le informazioni. Da qui il nome: Web statico (Web 1.0)

Web 2.0 (smartphone e social)

Paradigma di programmazione web utilizzato per indicare tutte le applicazioni web che interagiscono attivamente con l'utente, modificando le informazioni mostrate in base alle informazioni generate da quest'ultimo e ricevute dall'*application server*. Proprio per tale caratteristica di *user generated content*, esso si contrappone al precedente web statico o web 1.0.

Web 3.0

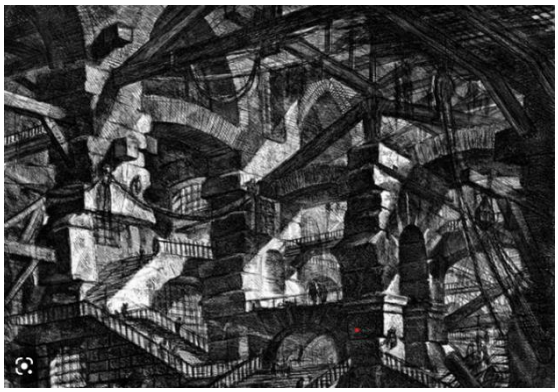
Web 3.0 è una locuzione per indicare una rete informatica in cui tutti i dati sono connessi fra loro le persone interagiscono e comunicano a voce con le macchine (web semantico) ed in cui le macchine processano il contenuto con estrema rapidità.

ALLEGATO

- Giordano Bruno, 1584

"*Io penso a un universo infinito. Stimo infatti cosa indegna della infinita potenza divina che, potendo creare oltre a questo mondo un altro e altri ancora, infiniti, ne avesse prodotto uno solo, finito. Così io ho parlato di infiniti mondi particolari simili alla Terra*"

- G. B. Piranesi - Architettura fantastica – Le carceri di invenzione, 1760



- Giacomo Balla - Iniezione di Futurismo, 1913

- Umberto Boccioni - Forme uniche della continuità nello spazio, 1913

- Giorgio de Chirico, Piazza d’Italia, 1955-56.

- Fortunato Depero - L’aratura, 1926

- Pier Augusto Breccia – Onda Lunga, 2015

ANNESSO - INTERVISTE

A questo Studio vengono aggiunte due diverse interviste, condotte con tre figure rilevanti nel mondo accademico italiano e internazionale.

Entrambe le interviste mirano ad investigare ed a fare luce sui rischi intrinsechi dell'Intelligenza artificiale e del Metaverso: quali rischi e sui relativi impatti cognitivi, culturali, sociali sulla società umana e sulla sicurezza del Paese.

Le interviste sono state condotte con approccio metodologico scientifico ed investigativo e sono ordinate qui di seguito nell'ordine stesso di realizzazione e di evoluzione degli argomenti.

Gli intervistati sono:

1) Paolo Traverso, Direttore del Centro per le Tecnologie dell'Informazione e della Comunicazione della Fondazione Bruno Kessler (FBK-ICT) dal 2008
2) Massimo Leone, Professore Ordinario di Filosofia della Comunicazione, Semiotica della Cultura e Semiotica Visiva presso il Dipartimento di Filosofia e Scienze dell'Educazione dell'Università di Torino, Professore part-time di Semiotica presso il Dipartimento di Lingua e Letteratura Cinese dell'Università di Shanghai, Cina, Membro Associato di Cambridge Digital Humanities, Università di Cambridge.

L'intervista con entrambi si è tenuta il 7 dicembre 2022.

3) Andrea Gaggiolo, Professore Ordinario di Psicologia Generale - Università Cattolica di Milano – e Direttore dell'International Master in User Experience Psychology.

L'intervista si è tenuta il 23 dicembre 2022.

"Intelligenza artificiale e Metaverso: quali impatti cognitivi, culturali, sociali sulla sicurezza del Paese"

intervista con Paolo Traverso e Massimo Leone[135]

Q. Qual'è oggi il quadro del coinvolgimento della IA nell'evoluzione del Metaverso?

R. L'Intelligenza Artificiale è un termine-ombrello per descrivere una serie assai ampia di processi computazionali che simulano i comportamenti intelligenti umani e i loro risultati, concentrandosi di solito su di un tipo d'intelligenza, ossia quella cognitiva, legata al calcolo, alla soluzione razionale di problemi, all'estrazione d'informazione dalla realtà sensoriale, all'elaborazione di dati. Così definita,

[135] *Paolo Traverso è Direttore del Centro per le Tecnologie dell'Informazione e della Comunicazione della Fondazione Bruno Kessler (FBK-ICT) dal 2008. Massimo Leone, è Professore Ordinario di Filosofia della Comunicazione, Semiotica della Cultura e Semiotica Visiva presso il Dipartimento di Filosofia e Scienze dell'Educazione dell'Università di Torino, Professore part-time di Semiotica presso il Dipartimento di Lingua e Letteratura Cinese dell'Università di Shanghai, Cina, Membro Associato di Cambridge Digital Humanities, Università di Cambridge. L'intervista si è tenuta il 7 dicembre 2022.*

l'intelligenza computazionale è presente lungo diverse dimensioni del Metaverso; si possono distinguere tre macro-aree:

- la costruzione di ambienti multi-sensoriali (ma soprattutto visivi) per l'immersione degli utenti, per esempio attraverso l'utilizzo di reti generative avversariali per l'elaborazione di volti "artificiali" foto-realistici o la costruzione combinatoria in tempo reale di scenari visivi che facciano da sfondo e da "mondo" alle interazioni;
- la gestione automatica dei processi d'interazione fra utenti e fra questi e i servizi presenti nel Metaverso, per esempio nel garantirne il continuo adattamento e personalizzazione;
- la simulazione automatica d'istanze di linguaggio nelle interazioni del Metaverso, attraverso i cosiddetti *chatbot*.

Come nel passato con la prima convergenza digitale, che condusse all'incrocio di più media e dispositivi, spesso generando confusione sulla loro definizione, anche quella attuale si manifesta attraverso nuove ibridazioni, che generano fertilizzazioni incrociate fra lo sviluppo dell'IA e quello di altri settori della tecnologia digitale avanzata, come le piattaforme, i sensori, i robots, la grafica digitale.

In buona sostanza, il Metaverso emerge dal connubio fra, da un lato, diverse forme di realtà estesa (aumentata, virtuale, immersiva) e, dall'altro, le piattaforme digitali.

L'IA può essere considerata come il tessuto connettivo di questa ibridazione.

D. Quali effetti positivi e/o negativi potranno verosimilmente ribaltarsi nella società reale?

R. Attualmente è ancora difficile fare previsioni che non siano influenzate da ideologie "apocalittiche" o "integrate"; in fondo, la riflessione sul Metaverso risente ancora molto di un'immaginario fantascientifico dal quale del resto ha tratto il suo stesso nome. Tuttavia si può immaginare che molte delle caratteristiche che, nel bene e nel male, contraddistinguono le relazioni sociali nel "cisverso" saranno riportate in forma digitale più o meno semplificata anche nel Metaverso. Insomma, nonostante quanto possano prospettare le retoriche utopistiche che spesso descrivono il futuro roseo di questa tecnologia, nel Metaverso continueranno a esservi tensioni, conflitti, violenza, sopraffazione, pregiudizi; ma, al contempo, non mancheranno le modalità amichevoli e persino amorevoli di cooperazione, esattamente come avviene nel mondo non-digitale; gli studiosi e le studiose del Metaverso dovranno però concentrarsi sui fattori che ne decreteranno la novità rispetto alla realtà esterna; qui se ne evidenziano solo quattro:

- la necessità di gestire l'identità degli agenti del Metaverso in maniera computazionale, senza riferimento diretto ai corpi degli utenti;
- la necessità di normare il Metaverso probabilmente al di là delle legiferazioni statuali;

- la necessità di monitorare i pregiudizi e i condizionamenti che l'IA inevitabilmente produrrà nella gestione delle interazioni;
- l'effetto dei dati massivi sull'emersione di nuove dimensioni qualitative, per esempio la presenza di una personalizzazione dei servizi che si basi su macrostatistiche molto efficaci, capaci di profilare i soggetti in maniera estremamente precisa e a volte ben al di là dei loro specifici comportamenti individuali.

D. Come evolverà l'approccio ai beni materiali e a quelli intangibili che vedono lo stato il massimo attrattore e artefice di coesione nazionale?

R. Questa domanda delinea il perimetro dell'area di riflessione più delicata e al tempo stesso più affascinante rispetto al Metaverso; in un mondo che simula non solo soggetti e oggetti, ma anche una rete sempre più fitta di relazioni fra essi, si pone in effetti la questione di determinare l'identità e la singolarità degli enti che popolano il Metaverso, a cominciare da quelli che svolgono una funzione primaria nella regolazione del rapporto fra individualità nel mondo non-digitale, ossia i corpi. Il Metaverso in realtà trova al proprio esterno enti e corpi che sono già molto digitalizzati, nel senso che la loro esistenza è spesso già legata a procedure d'identificazione digitale. Per lo Stato, per esempio, un individuo non è semplicemente un corpo, ma un corpo tradotto attraverso un codice standardizzato in una serie d'informazioni pertinenti, alcune delle quali confidenziali, ma tutte adesso trasposte in formato digitale. Molti Stati mantengono informazioni anche sulla forma dei corpi, per esempio su quella dei volti, ma pongono comunque limiti alla qualità e quantità d'informazioni che essi possono detenere rispetto all'individuo, per esempio in relazione alla configurazione del suo patrimonio genetico.

Le tecnologie per la gestione dell'identità digitale evolvono di pari passo con la costruzione del Metaverso. Il nodo centrale della questione consiste nel garantire e gestire l'affidabilità dell'intercapedine fra Metaverso e mondo esterno a esso. Il Metaverso infatti è una specie di "*gated community*" digitale la quale ha però continuamente bisogno del "cisverso", da cui importa beni e servizi, oltre che corpi e cose, e al quale offre e vende a sua volta beni e servizi. In che modo le due macro-istituzioni che regolano gli scambi nel mondo non-digitale, ossia il denaro e il diritto, saranno riprodotti e trasformati in quello digitale del Metaverso è materia di dibattito spesso molto ideologico, in quanto il Metaverso in sé, in quanto nuova dimensione tecnologica dello scambio e dell'interazione, non nasce neutro ma con una forte connotazione di decentralizzazione che mal si sposa con ogni tentativo di regolazione centralizzata. Ciò è adesso evidente nell'ambito della riflessione attorno al denaro e alla valuta nel Metaverso, ma lo diventa sempre di più anche in relazione al diritto.

Al momento, la tecnologia blockchain è massicciamente adottata per consentire un buon equilibrio fra operatività e sicurezza dei dati all'interno del Metaverso, per esempio nelle sue transazioni monetarie. Il nodo della questione è far sì che il Metaverso sia al contempo un mondo flessibile e affidabile, ossia concili il principio della libertà individuale con quello della sicurezza. È una conciliazione che molta della riflessione filosofico-politica della modernità persegue come una chimera.

La tecnologia blockchain consente la trasmissione di dati nel tempo (memoria) e nello spazio (comunicazione) senza che essi possano essere modificati (simulazione, frode, menzogna); tuttavia, tale tecnologia si mostra spesso deficitaria nel garantire un'adeguata personalizzazione nell'uso dei dati; elementi intermedi si rendono necessari, come gli *oracles*, per esempio, che recuperano e verificano dati esterni per un loro utilizzo in procedure blockchain.

Si apre comunque un'area molto vasta di ricerca e di formazione sul diritto e sulla finanza del Metaverso, un'area che richiederà un intreccio di competenze finanziarie, giuridiche, e informatiche oggi raramente compresenti. Tutto il mondo degli ETP e degli *smart contracts*, per esempio, ovvero della proiezione del meccanismo blockchain nella gestione dei contratti, sarà estremamente interessante da esplorare e definire nei prossimi anni.

D. Che profili di impatto avrebbe una lusinga di un mondo di tali caratteristiche, connotato da grande astrazione e apparente democratizzazione, rispetto ad una visione delle nuove generazioni sempre più reazionaria rispetto ai precedenti assiomi di realizzazione personale?

R. Vi è senza dubbio una connotazione libertaria in una parte dello sviluppo del Metaverso che lo identifica e sviluppa come un mondo parallelo non necessariamente sregolato, ma regolato secondo principi locali e tecnologici più che globali e giuridici; da un certo punto di vista, si potrebbe sostenere che i giovani imprenditori statunitensi (spesso di adozione) che sviluppano il Metaverso e le sue nuove istituzioni decentralizzate persistano nello spirito di esplorazione individuale e libera delle frontiere che fa parte del mito di fondazione degli Stati Uniti e più in generale di molti Paesi del Nuovo Mondo.

Oggi però sappiamo che forze oscure e spesso violente e distruttrici erano all'opera in quella conquista, la quale generava libertà e affermazione individuale ma spesso anche sopraffazione senza regole. Sicuramente un Far West digitale è oggi un pericolo da scongiurare, a cominciare da una certa moral suasion verso i più giovani, i quali effettivamente dovrebbero comprendere che la creatività e l'agentività personali non sono del tutto inconciliabili con una qualche forma di regolazione; certo è che tale regolazione dovrà avvenire in forme molto diverse rispetto al passato, con una forte componente di tecnologizzazione della dimensione normativa, ma sempre con il rischio che la delega del diritto alla tecnologia celi in realtà anche in questo caso la presenza di forze e pregiudizi nascosti.

Vi è qualcosa di straordinariamente eccitante nel modo in cui giovani menti di tutto il pianeta contribuiscono all'evoluzione del suo corrispettivo digitale, ma c'è anche spesso la sensazione di una certa ingenuità rispetto ai rischi etico-giuridici di tali esperimenti. Tutti gli istituti di ricerca e formazione consolidati possono giocare un ruolo fondamentale in questo processo di nuova regolamentazione delle interazioni digitali, una sorta di cuscinetto fra gli antichi apparati statuali e l'insofferenza delle giovani generazioni rispetto a sistemi di regole centralizzati.

D. Le esperienze vissute negli spazi digitali possono essere usate come palestre di allenamento per il reale? Quale sconvolgimento potrebbe portare questo nella nostra vita emotiva?
R. Sviluppo degli avatar nel Metaverso e il loro collegamento a sistemi di piattaforma regolati da intelligenza artificiale avrà senza dubbio un impatto sulla dimensione emotiva degli individui e delle società, ma con differenze a seconda delle categorie sociali e delle culture di appartenenza. Non bisogna infatti dimenticare che, per il momento, solo una percentuale piuttosto ristretta della popolazione dei Paesi tecnologicamente avanzati ha accesso a questo tipo d'infrastruttura digitale. In ogni modo, è plausibile ritenere che questo nuovo assetto simulato darà luogo a nuovi processi emotivi guidati dal Metaverso, che s'innesteranno però su modalità d'interazione emotiva già esistenti. Sono già in corso per esempio molti esperimenti che consentano agli utenti di "vedersi" nel Metaverso, di analizzare i propri atteggiamenti e comportamenti dall'esterno, o di scambiare, in una seduta psicanalitica, i ruoli del paziente e dell'analista; è assai probabile che gli individui le cui capacità sensoriali, cognitive, e motorie sono condizionate da situazioni di deficit potranno accedere a nuove possibilità, le quali andranno però regolate e normate anche con l'aiuto di specialisti affinché non generino situazioni pregiudizievoli per l'integrità mentale dei soggetti.

D. Quali nuovi rischi per la sicurezza del Paese si prospettano e andrebbero affrontati?
R. I rischi sono quelli collegati al fatto che dati, attività, e interazioni sensibili vengano affidati a un universo digitale; questi sono tuttavia pericoli che si conoscono già da tempo e che già da tempo vengono affrontati da specialisti nel settore, i quali partecipano dal lato della sicurezza e del controllo a questa corsa esponenziale fra sistemi di vigilanza e sistemi di *hackeraggio*.
Un Metaverso totalmente impermeabile a possibili intromissioni e manomissioni non può esistere, perché ne andrebbe della flessibilità e della ricchezza delle interazioni che vi hanno luogo; tuttavia, è indubbio che particolare cura dovrà essere posta da tutti quegli enti e soggetti la cui esposizione nel Metaverso possa essere bersaglio di attacchi da parte di agenzie ostili e perniciose, siano esse quelle di Stati nemici o di individui e gruppi che operano con l'obbiettivo di lucrare sulla destabilizzazione del sistema informatico.

Vi è però da considerare anche un rischio più di lungo periodo, che è quello non tecnologico ma digitale legato alla possibile disaffezione dei soggetti, soprattutto quelli delle ultime generazioni, nei confronti dell'idea stessa di Paese. Quest'idea è del resto legata a uno sviluppo storico molto lungo e abbastanza recente, il quale però potrebbe essere scavalcato da processi culturali che leghino sempre meno la definizione dell'identità al luogo in cui si è nati e cresciuti, e dove si hanno le proprie relazioni "reali", e sempre più a contesti virtuali ove si svolgono le proprie attività professionali, ludiche, sentimentali.
Immaginando che un numero crescente di attività umane vengano trasposte nel Metaverso, non è da escludere che ciò conduca a un progressivo scardinamento dell'idea tradizionale di Paese, ma anche, per converso, all'emersione di nuovi nazionalismi digitali, che cerchino invece di creare percorsi di affermazione identitaria anche nella simulazione digitale in rete.

D. Che cosa si intende per 'sicurezza dell'individuo' nel mondo digitale/Metaverso?
R. La sicurezza dell'individuo nel Metaverso è tripartita; si tratta di difendere il passaggio d'informazioni dal mondo reale a quello digitale; di proteggere l'elaborazione di questi dati all'interno stesso del Metaverso; e il passaggio d'informazione dal Metaverso al mondo reale. Questa tripartizione è complicata dal fatto che la separazione fra mondo "reale" e mondo "digitale" è vieppiù messa in discussione da incroci molteplici e ambigui. Non molti anni fa, per esempio, la comunità di un giocatore digitale del Metaverso, avendo appreso la notizia della scomparsa di costui nel mondo "reale", aveva deciso d'interrompere i giochi per rendergli omaggio con un funerale "virtuale" nel Metaverso stesso; un nemico del gruppo però ne approfittò, sterminando gli avatar durante il corteo funebre. In questo come in molti altri esempi, una comunità creatasi nel Metaverso ma ancorata a corpi esterni a esso, che muoiono, soffrono, e provano empatia, compie azioni anch'esse digitali le quali, guidate da sentimenti "reali", ha poi ricadute sulla stessa realtà digitale, spesso con conseguenze gravi. Numerosi altri esempi di tali complesse ibridazioni riguardano l'acquisto di beni e servizi reali nel Metaverso, così come l'attribuzione di valore reale a un artefatto digitale (per esempio negli NFT artistici).

D. I sistemi di persuasione di masse potrebbero essere notevolmente più efficaci. Si prospettano rischi per le democrazie?
R. Occorre valutare i rischi delle nuove tecnologie insieme con i loro benefici, senza cedere ai proclami utopici delle imprese commerciali ma neppure cedendo a un pessimismo distopico orwelliano. È ragionevole ipotizzare che, come in tutte le svolte tecnologiche, anche questa sarà interpretata da alcuni in maniera radicale, come un'occasione per separarsi dalla realtà e vivere una fuga digitale da essa. Per la maggior parte degli individui, tuttavia, si sperimenteranno percorsi

piuttosto personali e di solito moderati d'inserimento di questi nuovi dispositivi e delle relative pratiche all'interno del tessuto di esperienze mediali quotidiano, il quale del resto è in perenne evoluzione e di solito non elimina mai del tutto esperienze tecnologiche più tradizionali ma le integra in questo *bouquet* di vecchio e di nuovo, con livelli più o meno alti d'investimento corporale. Chi avrebbe detto, dieci anni fa, che non ci saremmo mai staccati dal nostro cellulare, o che andare al cinema sarebbe diventato un'esperienza retrò da abbinare alla fruizione dei contenuti *on demand* delle piattaforme globali? Si può prevedere che un numero crescente d'individui passerà un numero anch'esso crescente di ore con un *headset* attorno al capo, svolgendo attività che saranno dapprima puramente ludiche, ma che un giorno non lontano potrebbero coinvolgere molte altre attività. Un giovane ricercatore universitario potrebbe in effetti avere l'esperienza e persino la pratica di un insegnamento nel Metaverso nel prossimo decennio, con una modificazione sostanziale della geografia ma anche della geopolitica della cultura.

D. Gli spazi digitali superano i confini geografici e geopolitici: chi li governa e ci sarà un confine nazionale nel Metaverso? Che ipotesi ci possono essere?
R. Sarà difficile determinare confini nazionali nel Metaverso, se non in relazione ai suoi appigli fisici e indessicali, come del resto già avviene per le piattaforme digitali. Normare questo contesto sarà molto arduo, non tanto in astratto, ma perché è di solito considerata sterile quella riflessione giuridica che deve esulare dall'applicazione della legge. Far applicare la legge nel Metaverso richiederà però tecnologie diverse da quelle attuali, le quali tuttavia dovranno non essere invasive se l'ideologia di libertà che connota lo sviluppo di questa infrastruttura dovrà essere preservata. A questo proposito bisognerebbe ricordare che culture giuridiche diverse abbracciano l'innovazione tecnologica libertaria con più o meno entusiasmo. L'Europa non ha la stessa cultura giuridica del Primo Emendamento che hanno gli USA, e dovrà dunque ingegnarsi molto di più per adattare una tecnologia sostanzialmente nata e sviluppatasi al di là dell'Atlantico alla sensibilità etico-giuridica del Vecchio Continente. In questo ambito, istituzioni con la testa tecnologica pienamente nell'Occidente più avanzato, e principalmente negli USA, ma con il cuore in Europa, e anzi in Italia, come FBK, per esempio, potranno giocare un ruolo essenziale nel calibrare le nuove proposte tecnologiche globali secondo assetti valoriali legati al territorio, al Paese, e alle sue culture e tradizioni.

Metaverso: rischi ed impatti sulla società

intervista con Andrea Gaggiolo[136]

D. Qual'è oggi il quadro del coinvolgimento degli studi accademici del suo settore nell'evoluzione del Metaverso e delle tecnologie disruptive/immersive?

R. Il concetto di Metaverso, ovvero, l'idea di uno spazio virtuale condiviso in cui le persone possono interagire e comunicare tra loro e una vasta gamma di media digitali - ha conseguito una crescente attenzione da parte della comunità accademica negli ultimi anni. Il Metaverso è stato da alcuni osservatori descritto come una potenziale evoluzione futura di Internet, in cui le persone possono interagire tra loro e con oggetti e ambienti virtuali attraverso un medium spazializzato. Esiste una quantità crescente di studi accademici che si stanno focalizzando sul Metaverso e sui suoi potenziali impatti sulla società, la cultura e l'economia. Tuttavia, è utile premettere che, come settore di studio, la ricerca scientifica sulla realtà virtuale e della realtà aumentata non è nuovo, esistendo da almeno sessant'anni a livello accademico. Dall'altro lato, è indubbio che tali ricerche abbiano recentemente ricevuto nuovo impulso in virtù delle significative risorse economiche (nell'ordine di svariati miliardi di dollari) che sono state investite nell'ultimo lustro da grandi *player* tecnologici internazionali per lo sviluppo commerciale del Metaverso, tra cui rientrano, in primis gli investimenti dell'azienda Meta (ex Facebook).

Alcune delle principali aree di studio accademiche sul Metaverso includono la progettazione e lo sviluppo di mondi virtuali e comunità online, gli impatti sociali e psicologici della realtà virtuale e degli ambienti immersivi, il potenziale del Metaverso come piattaforma per il training, la formazione e l'intrattenimento e le questioni etiche e legali che circondano il Metaverso. Una delle principali sfide che devono affrontare i ricercatori in questo campo è la mancanza di una chiara definizione del Metaverso e di come differisca da altri ambienti virtuali, come videogiochi o piattaforme di social media. È inoltre in corso anche un dibattito sulla misura in cui il Metaverso sarà in grado di replicare il mondo fisico e le interazioni sociali che si verificano al suo interno. Nel complesso, lo studio scientifico del Metaverso è un campo in rapida evoluzione, e resta da vedere come si svilupperà e quale sarà il suo impatto finale sulla società.

D. Dalla sua prospettiva, quali effetti positivi applicativi e/o negativi potranno verosimilmente ribaltarsi nella società reale?

R. Il Metaverso ha il potenziale di avere sia effetti positivi che negativi sulla società. Un potenziale effetto positivo del Metaverso è che esso rappresenta una sorta di "meta-medium", ovvero di una

[136] *Andrea Gaggiolo è Professore Ordinario di Psicologia Generale - Università Cattolica di Milano – e Direttore dell'International Master in User Experience Psychology. L'intervista si è tenuta il 23 dicembre 2022*.

piattaforma virtuale omnicanale che consentirà alle persone di connettersi in uno spazio tridimensionale condiviso e formare comunità complesse e sincrone.

Il Metaverso rappresenta soprattutto un'interfaccia di comunicazione avanzata, che consente alle persone di interagire in modo naturale a distanza. Ad esempio, una squadra di progettisti che opera nelle sedi decentrate di un'azienda può utilizzare uno spazio simulato condiviso per collaborare alla soluzione di un problema. In campo medico, la Realtà Virtuale sta dimostrando un eccellente potenziale, con applicazioni nell'ambito della riabilitazione neurologica e nella psicoterapia. Questa tecnologia sta conoscendo una crescente diffusione anche nell'industria dell'*entertainment*, dove, oltre al settore dei videogiochi, essa trova applicazioni nella cinematografia, nei parchi tematici e nei musei. I social network, l'e-commerce, l'educazione, lo sport, sono solo alcune delle ulteriori aree che i mondi virtuali promettono di rivoluzionare.

Tuttavia, ci sono anche potenziali effetti negativi del Metaverso che vanno presi in considerazione. Una preoccupazione centrale è che il Metaverso potrebbe contribuire all'isolamento e alla disconnessione sociale, poiché le persone potrebbero trascorrere più tempo in ambienti virtuali e meno tempo a interagire con gli altri nel mondo fisico. In particolare, non sono ancora note le potenziali implicazioni per la salute mentale dell'immersione prolungata – per ore o addirittura per giorni – in un ambiente virtuale, che potrebbe condurre a sintomi associati al disturbo di depersonalizzazione/derealizzazione, una condizione mentale caratterizzata da frequenti disgregazioni del senso di sé e del mondo.

Il Metaverso potrebbe anche aggravare le disuguaglianze sociali esistenti, poiché l'accesso e la partecipazione al Metaverso potrebbero essere limitati per alcune persone a causa di barriere tecnologiche, economiche o educative. Inoltre, il Metaverso potrebbe sollevare una serie di questioni etiche e legali, come preoccupazioni per la *privacy*, i diritti di proprietà intellettuale e la regolamentazione delle attività e delle interazioni virtuali.

D. Quali profili di impatto psicologico/cognitivo rileva nelle esperienze vissute negli spazi virtuali che sarebbero degni di attenzione per il nostro sistema della Difesa?

R. L'evoluzione del Metaverso dovrebbe portare nel giro di qualche anno alla nascita di una sorta di "metamedium" – l'*interrealtà* – nella quale l'esperienza fisica tende ad ibridarsi con quella digitale (o "Confluenza Uomo-Macchina"). Questo avverrà grazie allo sviluppo di interfacce in grado di leggere, interpretare e persino predire i nostri stati cognitivi/emotivi, che consentiranno ai dati di fluire in modo bidirezionale - dal mondo fisico a quello virtuale, e viceversa. L'emergere dell'interrealtà estenderà in modo indefinito la gamma di esperienze (e relative alterazioni) che sarà possibile creare utilizzando la Realtà Virtuale e Aumentata.

La crescente convergenza tra le tecnologie simulative avanzate, le neurotecnologie (come la *brain*-stimulation e il *neurofeedback*) e gli strumenti di intelligenza artificiale sta ponendo le condizioni, nel breve-medio termine (5-10 anni), dello sviluppo di strumenti di trasformazione e alterazione della sfera cognitiva e comportamentale di enorme potenziale.

La realtà virtuale è uno strumento tecnologico che simula la realtà, la nostra mente è un sistema biologico che ha lo stesso obiettivo: simulare la realtà per riuscire a prevedere opportunità e minacce. E questo rende la realtà virtuale una tecnologia "trasformativa" in grado di modificare le sensazioni, le emozioni, gli atteggiamenti e perfino l'identità dei suoi utenti.

Tale potenziale trasformativo è ulteriormente sostenuto e continuamente alimentato dalle nuove scoperte delle neuroscienze cognitive e cliniche, e dalla disponibilità di una tecnologia di simulazione che genera sensazioni sempre più realistiche. Ne sono esempio eloquente le ricerche sul cosiddetto "effetto Proteus" e sulla possibilità di modulare l'attività cerebrale mentre si è immersi in un mondo virtuale. I risultati di questi studi rappresentano solo i primi passi verso lo sviluppo di alterazioni sempre più profonde della psiche umana. Il "doppio utilizzo" della Realtà Virtuale, ovvero il fatto che questa tecnologia possa essere applicata anche per scopi diversi rispetto a quelli per cui è stata progettata - ad esempio per manipolare la volontà, alterare l'identità, estorcere informazioni, o perfino per perpetrare torture psicologiche, creando esperienze virtuali in grado di indurre forti emozioni negative se non traumatiche. Queste applicazioni sono oltremodo realistiche in quanto le tecnologie virtuali e le neuro-tecnologie sono utilizzate con ottima efficacia per il trattamento di complesse patologie psichiche e per la neuroriabilitazione. Le potenzialità psico-trasformative della Realtà Virtuale rendono questa tecnologia particolarmente soggetta ad utilizzi strumentali a fini persuasivi. Si tratta di una prospettiva che certamente ci deve interrogare rispetto a quali misure preventive occorre adottare per prevenire eventuali azioni offensive basate su questi sofisticati dispositivi.

D. Il Metaverso prospetta nuovi spazi *off-limits* dove sperimentare ciò che non è possibile sperimentare nel mondo fisico. Sul piano psicologico e cognitivo, quanta informazione/innovazione può la mente umana reggere e sostenere?

R. In generale, il sovraccarico cognitivo può verificarsi quando le risorse cognitive di un individuo, come l'attenzione e la memoria, vengono superate dalle esigenze del compito o dell'ambiente. Nel contesto della realtà virtuale e aumentata (VR/AR), il sovraccarico cognitivo può verificarsi quando le informazioni e gli stimoli presentati attraverso l'AR superano la capacità di un individuo di elaborarli e integrarli in modo efficace. Ad esempio, in uno spazio virtuale la logica della "realtà" può essere totalmente sovvertita: come se si trattasse di uno spazio onirico o immaginativo, in una simulazione è possibile andare a ritroso nel tempo, duplicare o moltiplicare la propria identità, e

alterare le leggi della fisica. Questa violazione degli schemi può costituire una sorgente di esperienze potenzialmente destabilizzanti.

Ulteriori rischi di sovraccarico cognitivo associati alle tecnologie simulative avanzate includono: (i) Sovraccarico di informazioni: la VR/AR può presentare una grande quantità di informazioni e stimoli complessi e dinamici, che possono portare a un sovraccarico cognitivo, in quanto possono essere richiesti alti livelli di risorse attenzionali per elaborare e integrare gli elementi virtuali e fisici dell'ambiente; (ii) Richieste di memoria a breve termine: la VR/AR può anche porre richieste sulle risorse di memoria di lavoro ("*working memory*") di un individuo, poiché potrebbe essere necessario ricordare una grande quantità di informazioni sia dall'ambiente virtuale che da quello fisico; (iii) Richieste di attività complesse: le attività VR/AR complesse o che richiedono un alto livello di elaborazione cognitiva possono anche aumentare il rischio di sovraccarico cognitivo. Per mitigare i rischi di sovraccarico informazionale, è importante progettare le esperienze virtuali rispettando i principi dell'ergonomia cognitiva, limitando la quantità di informazioni presentate, presentando indicazioni e istruzioni chiare e consentendo alle persone di controllare le modalità con cui interagiscono con l'ambiente simulato.

Oltre al sovraccarico cognitivo, esistono diversi fattori di sistema sia dai sistemi *hardware* VR che dai sistemi operativi che possono causare o aumentare malessere psicofisico, la cosiddetta "*Cybersickness*". Si tratta di una forma di cinetosi che si verifica quando si è immersi in un ambiente generato dal computer come la realtà virtuale. Essa dipende da un conflitto tra il sistema visivo e quello vestibolare. Nei vertebrati, il sistema vestibolare è una componente dell'orecchio interno, e nella maggior parte dei mammiferi, compreso l'uomo, esso rappresenta il sistema sensoriale che fornisce il contributo principale al senso di equilibrio e all'orientamento spaziale, allo scopo di coordinare il movimento con l'equilibrio. Il sistema vestibolare rileva la posizione del corpo nello spazio in relazione alla forza gravitazionale e individua se la testa è in posizione eretta (verticalità), se è flessa, estesa o capovolta, e permette la percezione d'improvvisi cambiamenti di direzione o di velocità del movimento. Per questa ragione, quando durante una simulazione virtuale il movimento rappresentato nel campo visivo dell'utente non corrisponde perfettamente al movimento rilevato dal nostro senso vestibolare, possono verificarsi sintomi spiacevoli, che includono: disorientamento, fastidio oculomotorio (ad es. affaticamento degli occhi) e nausea. Gli utenti possono anche provare, anche se in misura molto meno frequente, sensazioni di vertigine e mancanza di coordinazione dopo una sessione virtuale immersiva.

Nota sull'IRAD[137]

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

[137] http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pagine/default.aspx


9 791255 150701