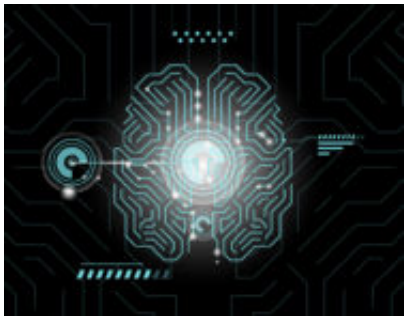
Intelligenza Artificiale - Orientamenti di CyberSecurity nella nuova era delle macchine

Date : 2 febbraio 2018



Premessa

Il presente articolo ha l'obiettivo di effettuare una veloce ricognizione nel *maelstrom* costituito da tecnologie digitali in crescita esponenziale, percezioni di realtà in costante trasformazione e difficoltà di analisi e interpretazione che da queste scaturiscono. Il tentativo di raccontare e dare significato ad alcune *buzzword* è collegato alla prospettiva tipica della mentalità di sicurezza (*Security Mindset*): conoscenza del panorama delle minacce, percezione e analisi del rischio, decisioni informate. Abbiamo bisogno di orientarci all'interno di un ambiente vasto, apparentemente infinito e relativamente nuovo.

Alcune definizioni

Il primo passo è procedere alla definizione di alcuni concetti chiave utili per inquadrare il contesto di riferimento.

Intelligenza Artificiale (**AI)**[1] è un termine ampio, applicabile a qualsiasi tecnica in grado di permettere a una macchina di imitare l'intelligenza umana tramite l'utilizzo della logica, di regole di implicazione (*if … then*), di alberi di decisione e di Machine Learning (incluso il Deep Learning). Il termine è stato coniato da John McCarthy nel 1956 in occasione della Conferenza di Dartmouth, evento che ha segnato la nascita del campo di ricerca. Un'altra "definizione operativa è stata proposta da Alan Turing nel suo articolo "*Computing machinery and intelligence*" (1950): una macchina può essere considerata intelligente se passa il "*Test di Turing*". Il test (o "*Imitation Game*") consiste nel mettere un uomo davanti a un terminale attraverso il quale comunicare con due entità: un altro uomo e un computer. Se la persona che comunica attraverso il terminale non riesce a distinguere fra uomo e macchina, allora il computer ha passato il test".[2]

Machine Learning (ML) è il sottoinsieme dell'AI che include complesse tecniche statistiche che permettono alla macchina di migliorare nell'esecuzione dei propri compiti attraverso l'esperienza. Il Machine Learning può essere *supervisionato* (inferendo una funzione da dati di addestramento opportunamente etichettati) oppure *non supervisionato* (sviluppando e

modificando il modello di comportamento senza avere un modello precedente di riferimento) tramite l'analisi costante dei dati disponibili.

Deep Learning (DL) è il sottoinsieme del ML composto da algoritmi che permettono al software di addestrarsi da solo per eseguire i propri compiti, quali ad esempio il riconoscimento di immagini o del parlato, esponendo reti neurali multistrato a enormi quantità di dati.

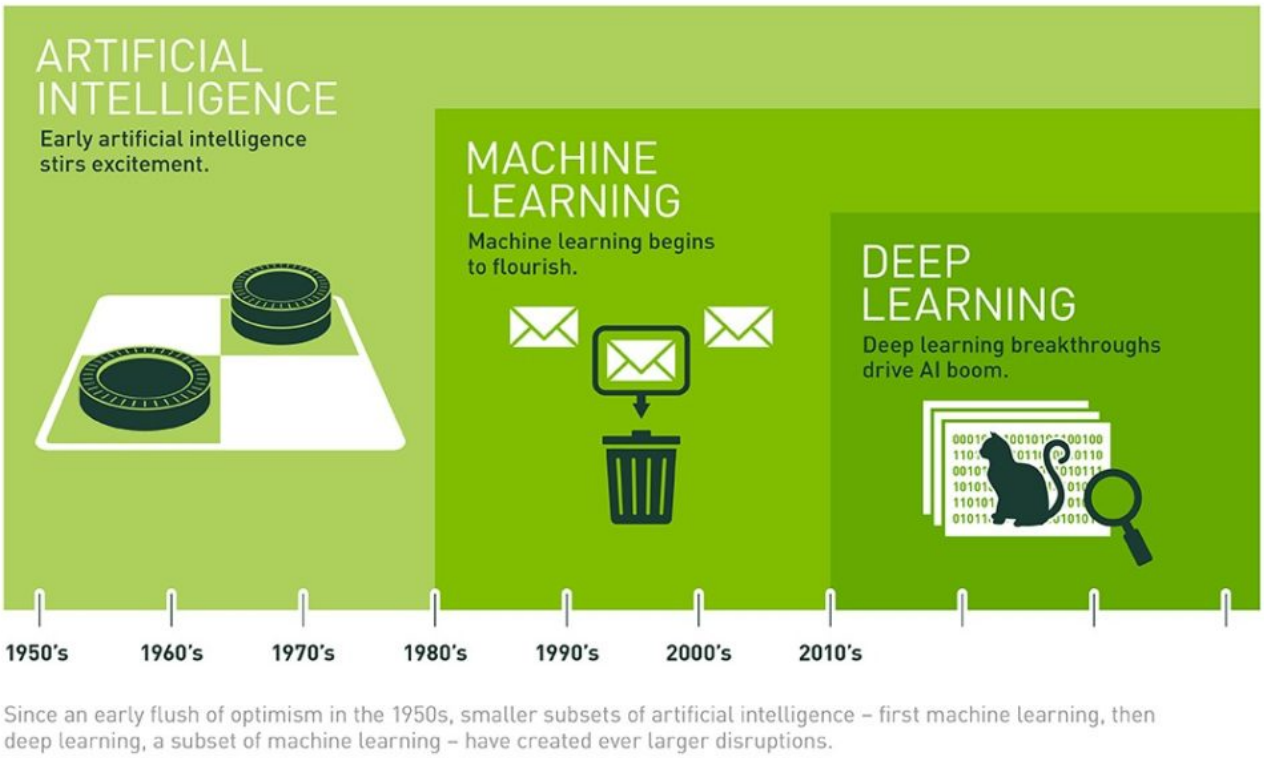


Figura 1 - Intelligenza Artificiale, Machine Learning, Deep Learning**[3]**

Internet of Things (IoT) "è la rete di oggetti fisici che contengono al proprio interno la tecnologia per comunicare, percepire e interagire coi propri stati interni o con l'ambiente esterno"[4]. Il termine è stato introdotto da Kevin Ashton nel 1999 per descrivere un sistema in cui il mondo fisico è connesso ad Internet attraverso dei sensori.

Macchine e Intelligenza

Concluso l'elenco delle definizioni, possiamo cominciare a gettare lo sguardo sulla contemporaneità e su alcuni eventi e processi in atto proprio in questo momento.

Eric Schmidt, CEO di Alphabet (Google), ama raccontare il cambio di paradigma che sta investendo in primis la propria azienda: da *Mobile First* ad *AI First*. Tale cambiamento è particolarmente significativo nella misura in cui Alphabet/Google è, insieme ad Apple, Amazon e

Microsoft, una delle cosiddette “*stack*” (cataste). La definizione di “catasta” appartiene a Bruce Sterling[5] e “indica la strategia di integrazione verticale con cui ognuna delle suddette aziende cerca di controllare la rete, nonché le piattaforme, le applicazioni, i dispositivi fisici e i contenuti presenti sulla rete stessa e grazie a essa connessi”[6]. Google e le altre “*stack*” sono in prima fila nella progettazione e nella realizzazione dei processi di Trasformazione Digitale in cui tutti, volenti o nolenti, siamo totalmente immersi. Bruce Sterling è tra i padri del movimento letterario *Cyberpunk*[7], così come William Gibson, inventore del termine “*Cyberspace”***[8]**, che tanto successo ha avuto nella comunità degli esperti di sicurezza. Il punto di vista tipico della sensibilità artistica - alimentato dalla letteratura *Cyberpunk* così come da capolavori quali *Blade Runner* o *Ghost in the Shell* - può regalarci visioni potenti e anticipare temi di rilevanza sociale, tecnologica, economica e politica: Intelligenza Artificiale, cibernetica e cambiamenti radicali dell’ordine sociale sono alcuni esempi della peculiare capacità artistica di precorrere tempi e spazi. Sempre Eric Schmidt ci informa che quasi tutti i sistemi di conoscenza delle aziende saranno a breve basati su AI e che, in generale, siamo in presenza di una tecnologia *disruptive:* da oggi in poi niente sarà più come prima, l’AI è una pietra miliare che determina un discrimine tra *ex-ante* ed *ex-post***[9]**. Interessante notare che Eric Schmidt è, tra le tante cose, il *Chairman* del *Defense Innovation Board* (*DIB*) del Dipartimento della Difesa degli Stati Uniti: si tratta di un comitato che ha l’obiettivo di mescolare la cultura, l’organizzazione e i processi di innovazione del mercato con il mondo militare. Uno dei primi risultati del DIB è la produzione di “raccomandazioni” al Dipartimento, tra le quali spicca quella relativa alla realizzazione di un istituto dedicato allo studio dell’Intelligenza Artificiale e del Machine Learning: in quest’area il gap tra mercato e mondo militare è evidentemente molto elevato[10]. Un altro spunto di interesse è rappresentato dal ruolo centrale che il World Economic Forum attribuisce a queste tematiche.[11]

Andrew Ng, Computer Scientist esperto di AI con un passato in Google e un presente in Baidu, ci aiuta a capire tramite un’analogia perché queste tecnologie stanno crescendo esponenzialmente: per andare nello spazio abbiamo bisogno di razzi e grandi quantità di carburante. Oggi il razzo è rappresentato da enormi reti neurali supportate da capacità di calcolo elevatissime, mentre il carburante è la quantità immensa di dati a disposizione (*Big Data*).

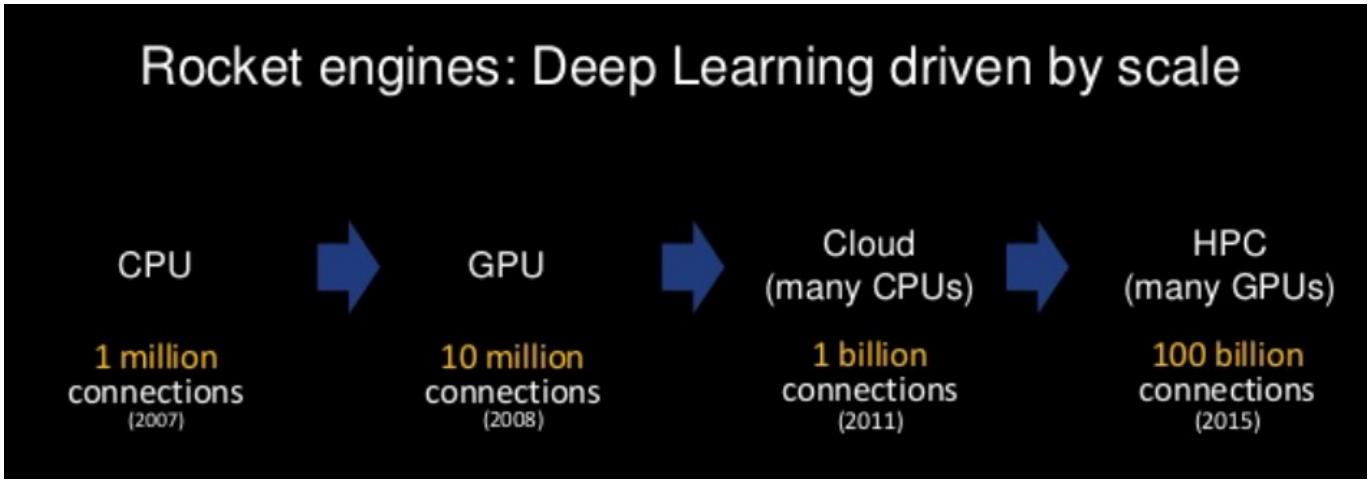


Figura 2 - Deep Learning e scala di calcolo**[12]**

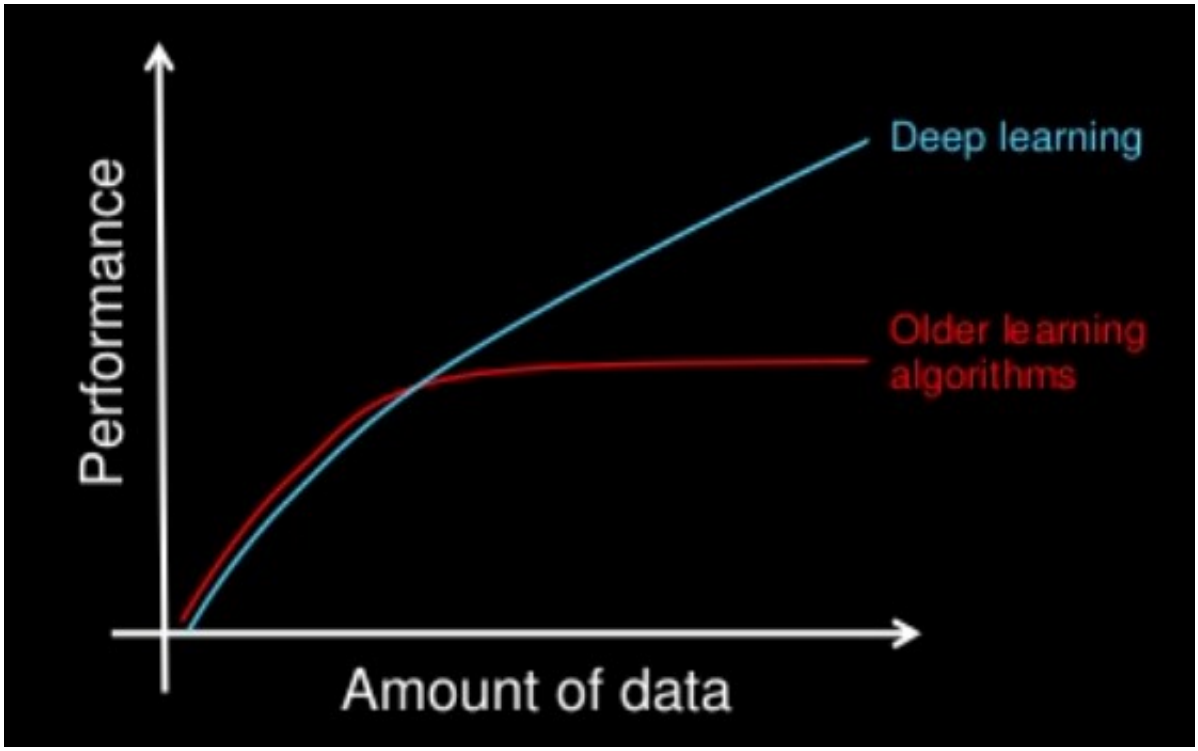


Figura 3 - Prestazioni, quantità di dati e Deep Learning

Quali sono i casi d'uso tipici? sicuramente Immagini, Parole e Comportamento. Il Deep Learning può condurre a scenari di tipo predittivo e dal punto di vista della sicurezza l'interesse immediato ricade nell'analisi del Comportamento: correlare un determinato stato con l'informazione relativa a eventuali minacce. Esclusivamente con le tecnologie prese in considerazione (AI, ML, DL) è possibile processare i *Big Data* generati dalla moltitudine di oggetti connessi in rete. Dal punto di vista della sicurezza, inoltre, la sfida è relativa al fatto che la maggior parte dei dati sono perfettamente "normali" e solo una piccola parte di questi rappresenta una minaccia cyber: si tratta del classico problema di trovare l'ago nel pagliaio e in questo, così come nei compiti di *pattern matching*, AI, ML e DL fanno effettivamente la differenza. Gli algoritmi e le reti neurali di DeepInstict promettono di proteggere "istintivamente" le nostre informazioni di valore: impossibile non apprezzare l'accostamento di una caratteristica tipicamente animale e umana (l'istinto) a un software di Intelligenza Artificiale[13].

Mondo virtuale e mondo reale

L'immersione nella realtà è un'esperienza quotidiana: velocità e pervasività della comunicazione globale, così come le tecnologie digitali, sono parte integrante delle nostre vite. I confini tra mondo virtuale e mondo reale sfumano progressivamente e uno degli effetti più interessanti è che "nella dimensione virtuale non c'è più né soggetto né oggetto ma entrambi diventano elementi interattivi"[14]. Soggetto e oggetto, umanità e cose: interazione tra soggetto e oggetto nel mondo virtuale e nel mondo reale.

Un punto di vista estremamente interessante è, come spesso accade, quello che Bruce Schneier ha espresso all'RSA Conference del 2017[15]: secondo Schneier, già nel 2011 Marc Anderssen sosteneva che il software si stava "mangiando il mondo"[16] e tutto stava (e sta) diventando un computer. Il sillogismo – scontato ma non privo di fondatezza - è che se tutto diventa computer allora la sicurezza dei computer diventa la sicurezza di tutto. Questa idea determina almeno un paio di riflessioni interessanti:

1. il corpo di conoscenze tipico della sicurezza informatica sarà applicabile e applicato a tutto;
2. le restrizioni fisiche saranno applicabili al mondo virtuale.

Il campo da gioco sembra diventare, letteralmente, il mondo intero. Pensiamo all'Internet of Things (IoT), alle "*cose*" che si parlano tra loro: Sensori, Smart, Attuatori. Questo scenario crea una Internet che sente, pensa e agisce: ci troviamo dinnanzi alla classica definizione di Robot. Stiamo costruendo un Robot distribuito, privo di cervello centrale e nemmeno progettato a monte: sta semplicemente avvenendo, sulla scorta di una profezia che si auto-avvera. Le cose intelligenti agiscono fisicamente e direttamente nel mondo reale, quindi gli effetti di tali azioni diventano reali e rilevanti per l'umanità. Dal punto di vista della sicurezza delle informazioni le minacce più rilevanti non riguardano la dimensione di Confidenzialità, bensì quelle di Disponibilità e Integrità. Siamo sempre più preoccupati di minacce quali la manipolazione dell'Informazione (*fake news*, attacco all'Integrità) o i DDoS (attacco alla Disponibilità) e tutto ciò è vita reale. L'impatto reale di attacchi informatici più o meno probabili pone un problema di sicurezza fisica: immaginiamo cosa può succedere alterando le normali funzionalità di un dispositivo connesso come un Peacemaker o disabilitando da remoto i freni di un'automobile (oggi un'automobile è un insieme di computer con elementi meccanici), per non parlare di sistemi SCADA e di Infrastrutture Critiche. Come si può recepire la sicurezza all'interno dell'Internet of Things? Ci sono tante linee-guida che suggeriscono cosa fare, ma i produttori delle "cose" ne tengono conto? I dispositivi a basso costo (ad esempio tanti router per le connessioni domestiche, oppure sistemi di videosorveglianza domestica) non sono toccati dai processi di messa in sicurezza del software e *patching* di eventuali vulnerabilità. Molti dispositivi non possono nemmeno essere *patchati*. Alcune dinamiche di mercato, quali il tasso di CHURN, possono generare buoni livelli di sicurezza, come nel caso degli *smartphone*, ma non funziona così per i dispositivi a basso costo. Le problematiche evidenziate da Schneier assumono contorni sconcertanti di fronte ai tassi di crescita stimati dei dispositivi IoT: si parla di circa 10 miliardi di oggetti connessi entro il 2020[17]. La possibilità di utilizzare dispositivi (soprattutto quelli a basso costo) vulnerabili come vettori di attacco genera un aumento eccezionale della superficie d'attacco complessiva. Molto pragmaticamente, Schneier suggerisce di disconnettere da Internet i sistemi critici e di mettere insieme tecnologia e politica per creare regole che tengano conto dei nuovi rischi di sicurezza cui siamo oggi esposti.

Percezione, Realtà e Decisione

Il mondo (virtuale e reale) accelera la propria trasformazione mettendo in discussione concetti fondamentali quali identità, relazione e sistemi di valore. Come individui siamo chiamati continuamente a operare scelte e molte di queste hanno a che fare con la nostra sicurezza (fisica e virtuale). La sicurezza è ciò che si definisce un *trade-off*: la domanda corretta non è se

fare o non fare una determinata cosa ci renda più sicuri, ma se ne valga la pena. A rendere complicata ogni scelta concorre il fatto che rispondiamo alla sensazione della sicurezza e non alla realtà: spesso realtà e sensazione coincidono, ma non sempre. La fallacia del processo decisionale sconta anche il problema del bias cognitivo (Kahneman e Tversky)[18]. Ancora Schneier ci segnala almeno 4 bias cognitivi tipici legati alla percezione della sicurezza[19]:

- tendiamo a esagerare rischi rari e spettacolari e minimizziamo quelli comuni (abbiamo paura dell'aereo più di quanta nel abbiamo nel guidare la nostra automobile, anche se tutte le evidenze statistiche ci dicono che l'aereo è più sicuro dell'automobile);
- l'ignoto viene percepito come più rischioso del familiare (le persone temono il rapimento di un proprio caro da parte di estranei ma è molto più facile che ciò avvenga per mano di persone conosciute);
- i rischi personificati sono percepiti come maggiori dei rischi anonimi (sapere chi era Bin Laden e che esisteva ha determinato una percezione di rischio maggiore che non saperlo);
- le persone sottovalutano i rischi nelle situazioni che controllano, mentre li sopravvalutano nelle situazioni che non possono controllare (il terrorismo genera elevata percezione di rischio perché non è nel nostro controllo, fumare o fare immersioni determina una percezione minore in quanto attività sotto il nostro controllo).

Ci sono altri bias cognitivi che influenzano la nostra percezione del rischio, come l'euristica della disponibilità, ossia stimare la probabilità di un evento sulla base della facilità con cui siamo in grado di pensare agli esempi relativi, oppure il bias di conferma[20] che ci porta ad accettare i dati che confermano le nostre convinzioni respingendo quelli che le contraddicono. Questi bias agiscono da filtro tra noi e la realtà e il risultato è che sensazione e realtà vanno fuori fase, diventano diversi. Si può determinare un falso senso di sicurezza o un falso senso di insicurezza. In un mondo complesso i modelli sono necessari per capire il rischio: il modello è una rappresentazione intelligente della realtà, seppur limitato. I modelli possono derivare da molte cose e possono cambiare, non sono statici ma dinamici e alla fine diventano invisibili. Nel mondo tecnologico non abbiamo esperienza per giudicare i modelli e dipendiamo da altri: se le sensazioni e la realtà tendono a combaciare, facciamo scelte migliori sulla sicurezza.

Conclusioni

Nonostante la tentazione di cedere a scenari distopici alla Orwell, composti da dispositivi tecnologici di controllo e repressione ultra-evoluti e predittivi (come descritti da Philip K. Dick in "*The Minority Report*" e oggi venduti come servizi nel mondo reale, per esempio, da PredPol[21]) o da Intelligenze Artificiali in conflitto con l'umanità sotto ogni punto di vista (come nella trilogia di *Matrix*, nella serie dei vari *Terminator* e nelle visioni eccezionali di Asimov), appare necessario il tentativo di comprendere le dinamiche di innovazione tecnologica in atto, cogliendone caratteristiche e potenzialità, valutando pro e contro e conducendo un'analisi costi-benefici. Dal punto di vista della CyberSecurity la superficie di attacco aumenta esponenzialmente, i vettori di attacco idem e la complessità esplode. Di contro, l'utilizzo di tecnologie di AI, ML e DL aumenta la visibilità e la capacità di reagire velocemente e in maniera efficiente alle minacce emergenti. L'automazione delle analisi di sicurezza può ridurre lo stress degli analisti umani, che sono soliti trattare grandi quantità di dati non connessi tra loro generati

da sorgenti disparate. L’automazione integrata nel normale flusso di lavoro aiuterà gli analisti umani a focalizzarsi sulle attività a valore, quali il miglioramento della gestione del rischio, lo sviluppo sicuro, il contenimento attivo delle minacce e altro ancora. Probabilmente la protezione delle informazioni rimarrà, almeno nel medio periodo, un compito tipicamente umano che sarà necessariamente coadiuvato, in misura crescente, da *capability* tecnologiche sempre più intelligenti e capaci di gestire quantità inimmaginabili di dati: del resto, nel mondo vasto e infinito della rete l’unico orientamento possibile sembra essere quello della collaborazione tra umanità e macchine.

Note

- [1] http://fortune.com/ai-artificial-intelligence-deep-machine-learning/
- [2] http://leganerd.com/2015/07/17/breve-storia-dellintelligenza-artificiale/
- [3] https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/
- [4] https://www.gartner.com/it-glossary/internet-of-things/
- [5] https://people.well.com/conf/inkwell.vue/topics/487/Bruce-Sterling-Jon-Lebkowsky-Sta-page01.html
- [6] http://www.einaudi.it/libri/libro/adam-greenfield/tecnologie-radicali/978880623634
- [7] https://archive.org/details/cyberpunk-antologia-di-testi-politici
- [8] https://en.wikipedia.org/wiki/Cyberspace
- [9] https://www.youtube.com/watch?v=oWH1wZhiL6A
- [10] https://www.defense.gov/News/Article/Article/1353822/defense-innovation-board-chair-recommendations-making-an-impact/
- [11] https://www.weforum.org/agenda/archive/artificial-intelligence-and-robotics/
- [12] https://www.slideshare.net/ExtractConf/andrew-ng-chief-scientist-at-baidu
- [13] http://www.deepinstinct.com
- [14] http://www.mediamente.rai.it/home/bibliote/intervis/b/baudrillard.htm
- [15] https://www.youtube.com/watch?v=b05ksqy9F7k
- [16] https://www.wsj.com/articles/SB10001424053111903480904576512250915629460
- [17] https://www.gartner.com/newsroom/id/3598917
- [18] http://people.hss.caltech.edu/~camerer/Ec101/JudgementUncertainty.pdf
- [19] https://www.youtube.com/watch?v=wQJC2MMB8nA
- [20] https://en.wikipedia.org/wiki/Wason_selection_task
- [21] http://www.predpol.com

A cura di: **Andrea Boggio**