UNIVERSITÀ DI TORINO

Dalla dimensione cyber alle "nuove" intelligenze.
Rischi e sfide per l'Europa

Giuseppe Romeo

ai4ei Artificial Intelligence for European Integration
Jean Monnet Centre of Excellence

CPS CULTURE POLITICA SOCIETÀ

Dalla dimensione cyber alle “nuove” intelligenze.
Rischi e sfide per l’Europa

Giuseppe Romeo
Università di Torino - SUISS e Università del Piemonte Orientale

Artificial Intelligence for European Integration - Jean Monnet Centre of Excellence

Collane@unito.it
Università di Torino

ISBN ebook: 9788875902865
ISBN cartaceo: 9791256001378

Artificial Intelligence for European Integration
Jean Monnet Centre of Excellence

Co-funded by the European Union

Jean Monnet Centre of Excellence
Artificial Intelligence for European Integration
Dalla dimensione cyber alle "nuove" intelligenze. Rischi e sfide per l'Europa

https://www.jmcoe.unito.it
https://www.observatory.unito.it

Graphics and page layout
Silvio Ortolani, SISHO - fotografia & archivi

Ledizioni LediPublishing
Via Antonio Boselli, 10
20136 Milano - Italia
www.ledizioni.it
info@ledizioni.it

Le pagine che seguono vogliono rappresentare non solo un punto di arrivo di un percorso di approfondimento seguito all'interno di «ai4ei» - Artificial Intelligence for European Integration, ma anche una riflessione sull'impatto che la rivoluzione tecnologica del nuovo Millennio ha prodotto e produrrà nelle nostre vite troppo occupate da quotidiani sempre più a termine in anni ogni giorno meno distanti. Un'epoca che vedrà come protagoniste della vicenda umana nuove esperienze, opportunità e minacce digitali e nuove competitive intelligenze entrare sempre di più nel nostro intimo esistenziale. Gli aspetti tecnici sono trattati nella loro centralità nelle relazioni politiche ed economiche del nostro e del prossimo tempo. Le implicazioni giuridiche, che riguardano la disciplina e la regolamentazione dei sistemi digitali quanto dell'Intelligenza Artificiale, i richiami e altri riferimenti normativi sono riferiti ai documenti ufficiali delle Istituzioni dell'Unione europea. Le valutazioni di carattere geopolitico circa le nuove interpretazioni sul progresso delle forme e dei sistemi di digitalizzazione e delle nuove intelligenze nei rapporti di forza tra gli Stati e i protagonisti del nuovo ordine "tecnopolare", e il ruolo dell'UE, descrivono il pensiero dell'Autore. Un pensiero per il quale, per gioco logico-deduttivo, l'Autore ritiene possibile seguire, compatibilmente con le precauzioni del caso, il consiglio di Asimov: quello di iniziare a orientarsi verso un modo di pensare fantascientifico.

In ricordo di Umberto Morelli, interprete, maestro e guida nella Storia delle relazioni internazionali.

A Girolamo Garreffa, fisico prestato alle neuroscienze. Un pensiero senza tempo per un grande ricercatore, un caro amico e umile calabrese.

Giuseppe Romeo

Dalla dimensione cyber alle "nuove" intelligenze. *Rischi e sfide per l'Europa*

Tra mondo cyber e IA. Un nuovo *nomos*

> Ogni ordinamento fondamentale è un ordinamento spaziale. Si definisce una costituzione di un paese o di un continente come il suo ordinamento fondamentale, il suo Nomos. Ora il vero e proprio ordinamento fondamentale si basa, nel suo nucleo essenziale, su determinati limiti e delimitazioni spaziali, su determinate misure e su una determinata distribuzione della terra. All'inizio di ogni grande epoca c'è, pertanto, una grande appropriazione di territorio. In particolare ogni rilevante mutamento e ridefinizione della immagine del mondo sono connessi a mutamenti geopolitici e ad una nuova divisione della terra, ad una nuova appropriazione di territorio.
>
> Carl Schmitt, *Der Nomos Der Erde: Im Volkerrecht Des Jus Publicum Europaeum,* 1950

L'epoca contemporanea si distingue dal passato non solo per la quasi totale dipendenza da sistemi tecnologici, ciò lo è sempre stato in fondo, ma per la velocità e il livello di sostituibilità che proprio tali sistemi hanno assunto rispetto alle capacità dell'uomo. Si tratta di un'epoca nella quale la crescita, la qualità della vita, la sicurezza del nostro quotidiano dipenderà sempre di più dal livello raggiunto dalla tecnologia e dalla tecnica applicata al sistema-Paese o, molto più semplicemente - per le attività di governance come per quelle di impresa - dalla capacità di resilienza. Una capacità, che si risolve nel poter garantire continuità di governo per le prime e di *business continuity* per le seconde. Infatti, crescita e sviluppo economico come la credibilità politica, saranno sempre più subordinati alla forza di non retrocedere sul piano delle conoscenze tecnologiche per difendere un vantaggio competitivo del proprio sistema-Paese.

Ciò che definisce il quadro complessivo del sistema relazionale, infatti, è rappresentato dall'aumento della competizione internazionale, dal vedersi definire ancor più del passato le relazioni politiche ed economiche secondo termini contrattualistici per effetto di una maggiore concorrenza tra gli attori politici ed economici internazionali. Questo significa, in termini concreti, che i

modelli competitivi che segnano il nostro presente, e che inevitabilmente caratterizzeranno il nostro futuro, non potranno che non vedere aumentare tutte quelle attività di acquisizione di informazioni strategiche che verranno processate soprattutto nel cosiddetto «cyberspazio».

Una condizione che non può destare sorpresa se si osserva con obiettività l'evolversi delle conquiste tecnologiche nel mondo e la corsa a superare in qualità il limite raggiunto, facendo sì che l'ordine geopolitico, di fatto definito da una instabilità per differenza di potenza, troverà nel controllo della competizione tecnologica nelle diverse declinazioni possibili (cyber, IA e *Quantum computing*) la soluzione dei conflitti e delle crisi future. E questo, considerato che sia le cosiddette economie che le potenze emergenti investono già da oggi nella capacità di influenza usando le tecnologie digitali e le "nuove" intelligenze. In fondo, non ci sono dubbi che così come ricordato come *Welcome* al Cybersec 2023 in Polonia, il cyberspazio rappresenterà il dominio per i conflitti internazionali che potranno svolgersi sia «al di sotto che al di sopra della soglia della guerra».

D'altra parte, ferma restando una sorta di prospettiva tendente a favorire le aggregazioni tra attori che esprimono e condividono valori e interessi comuni, non vi è dubbio che molti Stati ormai guardano al nuovo mondo come a un'arena troppo affollata. Un'arena nella quale non solo le opportunità sembrano tornare a favorire politiche unilaterali, ma che vede il moltiplicarsi di attori e di spazi che saranno soggetti e oggetti di rivalità. In altri termini, che quella visione cooperativa delle relazioni internazionali che sembrava doversi affermare come modello stabile dell'ordine postbellico si vedrà nuovamente superata da un approccio ancor più competitivo e con tutte le conseguenze che ne deriveranno in termini di attrito.

La struttura stessa del potere si sta trasformando da piramidale a reticolare. Un cambiamento anche di paradigma per il quale gli Stati nazionali, retaggio della pace westfaliana, si vedono erodere le loro prerogative (monopolio della forza e delle informazioni) da nuovi attori sub-nazionali, transnazionali, non-statali o potentati economici capaci di influenzare e modellare i processi decisionali e relazionali. Una conseguenza cui si aggiunge l'esaurirsi delle volontà di condividere politiche monetarie e fiscali tali da poter contenere crisi di sistema, che pongono maggior incertezza sulla possibilità di mettere in campo politiche e interventi anticiclici che imporrebbero sacrifici agli attori che non riusciranno a giocare la partita per imporre una nuova *supremacy*.

Condizioni, le precedenti, che non possono non influenzare anche le scelte geopolitiche di protagonisti determinanti dell'ordine mondiale come gli Stati

Uniti, costretti a fare i conti con la sostenibilità di un aumento o meno della spesa interna rivolta a favorire politiche sociali al netto degli investimenti nel settore della Difesa, della Sicurezza e delle nuove intelligenze. O la Cina che soffre di un calo della competitività internazionale sulla quale, ponendosi alla guida della globalizzazione dei mercati, aveva affidato il proprio futuro come nuova grande potenza mondiale e la Russia costretta a dover fare i conti con un conflitto con l'Ucraina e la necessità di mantenere l'apprezzabilità del rublo quale divisa di riferimento per la comunità eurasiatica. Insomma, si potrebbe dire che Carl Schmitt, probabilmente aveva ben chiaro ciò che sarebbe stato il futuro dell'umanità, segnando non solo un passaggio verso nuove conquiste e nuovi ordini post-eroici, affermando che

> Ogni nuova era e ogni nuova epoca nella convivenza dei popoli si fonda su nuove divisioni spaziali, nuovi recinti e nuovi ordini spaziali della terra[1].

Non ci sono dubbi, al netto delle prospettive all'interno delle quali si vuol ricondurre il pensiero schmittiano, che il nuovo *nomos* della Terra non sarà solo rappresentato dagli spazi che il definito umano potrà rappresentarsi, ma anche da altri luoghi che trasfigurano il limite fisico all'interno di una dimensione se non metafisica sicuramente metaversica. Una dimensione, quest'ultima, nella quale ogni interpretazione della realtà diventa un esercizio di come la percezione del sé e dell'altro possa realizzare nuovi rapporti politici ed economici tra attori sempre più plurali, spostandone la contrattazione su piani e prospettive completamente diverse dal passato, oltre a garantire la possibilità di apprendimento in scenari complessi.

In questo senso, anche la percezione e il significato di un termine come *nomos* può mutare man mano che la sua estrinsecazione si risolverà in più reali, secondo il quanto e il come ogni destinatario vivrà lo spazio nel quale si formeranno e matureranno quelle informazioni attraverso le quali si decideranno le scelte, e i comportamenti, del singolo quanto delle società; queste ultime sempre più interconnesse in sistemi digitali supportati da IA e la cui capacità di qualificare azioni e decisioni saranno progressivamente più evolute rispetto alle capacità umane. O, comunque, deve piegarsi a una nuova visione del mondo così come viene fatto, questa volta, apparire. Infatti, ciò che contraddistingue il mondo di oggi, è la relatività di ogni tentazione assiomatica la quale contraddice la sua essenza per dissolversi nel gioco parallelo tra nuove dimensioni.

[1] C. Schmitt, *Il nomos della terra nel diritto internazionale dello «jus publicum europaeum»*, Adelphi, Milano, 1991; tit. or. *Der Nomos der Erde im Völkerrecht des Jus Publicum Europaeum,* Dunker & Humblot, Berlin, 1988.

ll potenziale della dimensione cyber, quanto quello dell'Intelligenza Artificiale (IA) si manifesta, quindi, in un *nomos* dai pochi ma precisi passaggi e regole che ne determinano anche la qualità come la capillarità delle reti e dei terminali che connettono utente e gestore dei servizi, attraverso architetture interdipendenti e interoperabili, con una integrazione progressiva delle stesse reti e con nuove norme anche di relazione. Insomma, se sino a pochi decenni fa si poteva ancora accettare - pur nel sopraggiungere della tecnologia elettronica divenuta dominante nella produzione come nelle relazioni umane - che la misurazione dello spazio nel quale si risolve l'esistenza umana fosse individuabile determinando l'estensione di un corpo in volume, in superficie (lunghezza, larghezza, altezza o profondità) e l'estensione anche secondo modelli di proporzionalità definiti e definibili in quanto misurabili, oggi non è più così.

Non lo è nelle misurazioni matematiche e neanche nelle certezze geometriche - passando dal determinismo tipico della fisica classica a misurazioni proprie della fisica quantistica - meno che mai nelle relazioni politiche ed economiche e, quindi, nelle scelte di come e in che termini mettere in campo politiche egemoniche spostando le capacità di attacco e di condizionamento sulle società-bersaglio o sull'intimo dell'esistenza. Sulla dimensione non solo misurabile delle capacità economiche e militari, quanto sulla capacità di condizionare comportamenti e scelte manipolando la percezione e la misurazione del reale.

In questo ambiente estremamente e fluidamente complesso, che sposta in avanti i termini del confronto possibile e, quindi, del rischio e della minaccia, trova spazio la necessità di offrire della cybersicurezza, quale necessità di protezione di una comunità, un suo significato che se segue quello della minaccia tradizionale ne sposta in avanti i pericoli definendosi come nuova sfida e come nuova dimensione. Una sfida, nella quale si sommano tutte le aspettative e le angosce di una comunità-bersaglio vista l'intima connessione che la dimensione cyber, nel suo dematerializzare le angosce, realizza rendendo relativi spazi di manovra e distanze.

Certo, ci si potrebbe anche chiedere, a questo punto, se «Il mondo esiste se non lo si guarda?» domanda che Werner Karl Heisenberg si poneva ritenendone la risposta come necessaria per la formulazione di quel principio di indeterminazione che sarebbe diventato paradigma della nuova via quantistica e della relativizzazione ancora più intima del determinismo fisico se non del suo superamento[2]. O, che «la realtà è creata anche dalle nostre domande, ovvero

[2] W.K. Heisenberg, *Über den Anschaulichen Inhalt der Quantentheoretischen Kinematik und Mechanik*. In «Zeitschriftfür Physik», 40-1927, pp. 172-198.

dall'informazione acquisita» dal momento che l'osservazione perturba il fenomeno come descritto da Heisenberg. Ma una risposta efficace a tale interrogativo risiede, ad esempio, nel superare quella frase di Andy Warhol, guru della pop art: «ignoro dove l'artificiale finisce e comincia il reale».

D'altronde, se questo processo evolutivo che connette sempre di più l'esperienza umana alla quantità della tecnologia determina uno spostamento della percezione umana verso nuove possibilità di interpretare il mondo, allora anche nell'ambito delle relazioni politiche in senso lato le dimensioni di un soggetto politico, ad esempio, non sono più considerate prerogativa di forza, ma solo una condizione quantitativa - e non necessariamente solo economica - almeno in termini di gestione di una posizione di egemonia sottesa a una interpretazione qualitativa della stessa idea di forza.

Questo significa che i conti, qualunque sia la versione ideologica e/o dottrinale che si intende perseguire per fissare quali siano gli interessi di una comunità politicamente, socialmente ed economicamente organizzata, si faranno con quella ibridazione del concetto di forza che ridefinisce modi e termini di ogni confronto: politico, economico, militare e culturale. Un confronto, che renderà ancora più diffuse e distribuite sino ai minori livelli di organizzazione sociale quelle complessità e imprevedibilità che regnano sovrane come caratteri non negoziabili dell'esperienza umana, al di là di ogni possibile modalità di ordine delegabile alle sensibilità delle nuove intelligenze.

Torino, 08 dicembre 2023

I. Cybersicurezza.
Una necessità per la nuova sopravvivenza

> Quando il passato è sempre con te, potrebbe anche essere presente; e se è presente, sarà anche futuro.
>
> William Gibson, *Neuromancer*, 1984.

Se oggi si osserva l'evolversi di una geografia relazionale a sovrapposizione progressiva, oltre che di «nuove geografie» si può anche parlare di «nuove topografie» che indicano modi e termini di accesso alla Rete e diventano punto di non ritorno tra chi si inserisce nella corsa al protagonismo mondiale e chi vi rimarrà fuori; tra chi segue vie e percorsi legittimi, e chi persegue un progetto volto a destabilizzare in poco tempo certezze, sicurezze per fini di potenza o di supremazia economica o di semplice dominio criminale. D'altronde, non si può certo non osservare come buona parte della società occidentale si trova ancora oggi confusa di fronte a minacce che dipendono interamente dai nuovi assetti sociali che i cambiamenti relazionali hanno determinato in questi ultimi anni, abbattendo le distanze e riducendo i confini.

Nuove geografie imposte dalla tecnologia ben definite in un saggio del 2016 dal titolo *Connectography*, dove un attento Parag Khanna ridisegnava le nuove mappe del prossimo ordine mondiale[1]. Mappe non solo definite in termini fisico-politici, ma riscritte e reinterpretate facendo sì che alla geografia politica tipica degli Stati si sarebbe sostituita una geografia funzionale. Una descrizione delle relazioni umane che sarebbe stata espressione del grado di interdipendenza o, meglio, delle reti distributive (*supply chains*) che l'interconnessione globale ha creato e sulla quale costruisce giorno dopo giorno una nuova architettura di governance, che riguarda le attività produttive, le interrelazioni tra istituzioni governative, l'accesso o le prestazioni

[1] P. Khanna, *Connectography. Mapping the Future of Global Civilization*, Random House, New York, 2016; trad. it. *Connectograpy. Le mappe del futuro ordine mondiale*, Fazi, Roma, 2016.

di servizi. Una nuova *imago mundi*, che in ridisegna ogni linea di confine rendendola sempre più sottile sia tra le comunità che all'interno delle stesse comunità organizzate. Ma non solo. La relatività dei confini dell'informazione politica, economica e personale rappresenta, parafrasando Khanna, una delle caratteristiche fondamentali delle future relazioni tra Stati, popoli e individui cui si aggiunge una molteplicità di attori non governativi e non convenzionali che supera le barriere fisiche, penetrando nelle coscienze ed esercitando forme di condizionamento del comportamento degli individui, precedentemente affidate a strumenti politici, economici e militari di tipo convenzionale grazie alla connessione globale.

Le società più evolute tecnologicamente, infatti, oggi vivono all'interno di un ecosistema digitale in evoluzione, caratterizzato da un crescente conflitto informatico senza che ci si trovi di fronte a una guerra intesa nel senso tradizionale di pieno e definito confronto militare. Per questo, anche l'aspetto terminologico non è certo trascurabile e per due motivi. Il primo, per configurare al meglio la minaccia e, una volta definita, decidere come affrontarla. Il secondo, per poter individuare comportamenti univoci soprattutto all'interno di coalizioni dove l'aspetto cooperativo relazionale dovrebbe essere decisivo per la qualità della risposta. Perché come ricorda Wyatt Hoffman, già analista e ricercatore senior presso il *Nuclear Policy Program* e la *Cyber Policy Initiative* presso il *Carnegie Endowment for International Peace*, proprio i paesi europei dovrebbero definire il problema da risolvere,

> Poiché una terminologia ambigua crea problemi nel distinguere tra diverse concezioni di strategia[2].

Una sorta di necessità preliminare che non esula da una prospettiva di cybersicurezza ma, al contrario, la definisce man mano che si cerca di completare uno spettro di possibilità di comprensione e di risposta.

In altre parole, ciò vuol dire chiarire preliminarmente - e a fronte di un possibile conflitto informatico prim'ancora che ci si trovi impegnati in una guerra fisicamente *muscolare* - il tipo di attacco, l'impatto sulle comunità-bersaglio, se questo potrà essere espressione di una competizione strategica, se rientra all'interno di una intensificata concorrenza tecnologica globale, se incide sul controllo delle infrastrutture: l'Internet delle *supply chains*, dei mercati internazionali delle telecomunicazioni, delle risorse digitalmente critiche, dei flussi di dati se non sull'innovazione stessa delle tecnologie emergenti.

[2] W. Hoffman, *Is Cyber Strategy Possible?*, in «The Washington Quarterly», 42 (1), 2014 p. 133.

Tuttavia, tale ambiguità dimostra l'esistenza di un vuoto nel pensiero strategico in senso lato, poiché diventa complicato formulare strategie che descrivano in dettaglio come le entità militari e di intelligence dovrebbero avvicinarsi e gestire il nuovo ambiente strategico dematerializzato nella minaccia e, soprattutto, nella condotta. In questo senso, e al netto delle stesse direttive UE, NIS 1 e NIS 2, l'assenza di una univoca visione strategica mette a rischio le società europee e mina la governance democratica, poiché navigare nel nuovo spazio della competizione informatica rappresenta una sfida significativa per la stabilità del continente e per la credibilità della stessa Unione europea. D'altronde, l'innovazione digitale influenza ed è influenzata dalle tensioni geopolitiche mentre, nello stesso tempo, il settore privato esercita un potere significativo per influenzare i risultati in questo ambito.

Le grandi aziende ad alto profilo tecnologico sfidano, infatti, alcune competenze chiave degli Stati nazionali mentre nuovi rischi si presentano all'orizzonte degli eventi per gli Stati includendo non solo un cyberspazio parallelo, ma diventando dipendenti dal paradigma del *first strike* anche nel campo delle capacità cyber e per il cui contenimento Martin C. Libicki, dell'*Institute for National Strategic Studies* e consulente della Rand, nel suo *Cyberdeterrence and Cyberwar*, considera come necessario il preservarsi una capacità di secondo colpo (*second strike*)[3].

L'idea è che, alla fine, una corsa alla supremazia digitale nel cyberspazio determina anche uno o più cyberspazi paralleli dove è la qualità della tecnologia acquisita che farà la differenza pretendendo di riorganizzare le stesse relazioni politiche ed economiche in base al vantaggio raggiunto da un attore rispetto a un altro. Una condizione di competitività che in fondo, e non a caso, rischierebbe di attribuire vantaggi determinanti che potrebbero modificare gli stessi standard internazionali sui quali si muovono le relazioni tra gli attori politici ed economici, la loro stessa stabilità visto che l'interconnessione globale si affida a protocolli condivisi e che difficilmente apprezza slanci in avanti.

Negli ultimi dieci anni, gli studiosi di sicurezza informatica hanno prestato crescente attenzione al modo in cui le ostilità informatiche - siano esse spionaggio, sovversione o disinformazione - che non sono all'altezza delle

[3] Cfr. M.T. Libicki, *Cyberdeterrence and Cyberwar*, Rand, Santa Monica, 2009 p. 127 e ss. Vedasi anche M.B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, Working Paper, Massachusetts Institute of Technology, May 10, 2017.

definizioni legali di conflitto armato e guerra, possano influenzare concetti strategici consolidati come deterrenza, coercizione e offesa, equilibrio[4]. Mentre alcuni autori concordano sul fatto che le forme di ostilità informatiche, accumulate e nel tempo, causano danni significativi alle democrazie liberali, altri non sono d'accordo se rappresentino un'evoluzione o una rivoluzione negli affari strategici[5].

Ad esempio, l'idea stessa di cyberspazio come dimensione definita non sembra rispondere poi così concordemente a una dimensione di per sé molto fluida. In questo senso, si può richiamare quanto già indicato nel 2009 da Libicki per il quale il cyberspazio viene ripartito su tre dimensioni o livelli di comprensione. Il primo, quello fisico, che ha in sé elementi materiali dove ogni attacco può essere gestito e/o inibito attraverso tradizionali operazioni cinetiche condotte sulle architetture informatiche. Il secondo, un livello sintattico, rappresentato dai dati e dalle informazioni assunte, processabili, o da software e linguaggi se non algoritmi necessari per governare le macchine. In questo caso, si tratterebbe di contrastare vere e proprie operazioni di hacking. Vi è, poi, il terzo livello, quello semantico che si spinge anche oltre nella definizione di *cyberweapons,* queste ultime definite quali

> Software e sistemi informatici (IT) che, attraverso le reti ICT, causano effetti distruttivi e non hanno altri usi possibili[6].

[4] E. Gartzke, J.R. Lindsay, *Weaving tangled webs: offense, defense, and deception in cyberspace*, in «Security Studies», 24 (29), 2015 pp. 316-348. J. Jr. Nye, *Deterrence and dissuasion in cyberspace*, in «International Security», 41 (3), 2016/17 pp. 44-71. Vedasi, anche: E.D Borghard, S.W. Lonergan, *The logic of coercion in cyberspace*, in «Security Studies», 26 (3), 2017 pp. 452-481; R. Slayton, *What is the cyber offense-defense balance? Conceptions, causes and assessment*, in «International Security», 41 (3), 2017 pp. 72-109; B. Valeriano, B. Jensen, R. Maness, *Cyber Strategy: the Evolving Character of Cyber Power and Coercion,* Oxford University Press, Oxford 2018; B. Garfinkel, A. Dafoe, *How does the offense-defense balance scale?* In «Journal of Strategic Studie»s, 42 (6), 2019 pp. 736-763.

[5] E. Gartzke, *The myth of cyberwar: bringing war in cyberspace back down to earth*, in «International Security», 38 (2), 2013 pp. 41-73; L. Kello, *The meaning of the cyber revolution: perils to theory and statecraft*, in «Quarterly Journal: International Security», 38 (2), 2013 pp. 7-40; J.R. Lindsay, L. Kello, Lucas, *Correspondence: a cyber disagreement*, in «Quarterly Journal: International Security», 39 (2), 2014 pp. 181-192; W. Hoffman, *Is cyber strategy possible?*, in «The Washington Quarterly» 42 (1), 2014 pp. 131-152.

[6] M.C. Libicki, *Cyberdeterrence and Cyberwarfar*, ...cit.; autore anche di *Cyberspace in Peace and War*, Naval Institute Press, Annapolis, 2021 (2ed). Un articolo interessante che utilizza come consolidato il termine di «cyberweapons» è in I. Bremmer, M. Suleyman, *The AI Power Paradox. Can States Learn to Govern Artificial Intelligence-Before It's Too Late?*, in «Foreign Affairs», August, 2023. Consultabile anche in: https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox.

Un aspetto fondamentale di questa definizione è che i sistemi IT (come il codice informatico) non sono armi autonome, ma richiedono l'incorporazione in un'arma più ampia. Secondo la definizione ristretta, un'arma informatica esisterà solo laddove il software o il sistema IT potrà essere utilizzato unicamente per scopi distruttivi. Una definizione mutuata da quella relativa alle armi chimiche, considerato che è proprio la duplice funzione che definisce il quadro di possibile interpretazione, poiché una definizione così ristretta è coerente con quella adottata dalla comunità internazionale nella Convenzione sulle armi biologiche o a tossine (Biological and Toxin Weapons Convention - BTWC) del 1973 e nella Convenzione sulla proibizione delle armi chimiche (Chemical Weapons Convention - CWC) del 1993.

Entrambi i documenti riguardano, infatti, prodotti che, come molti strumenti informatici, possono avere una duplice funzione. Tuttavia, però, la definizione ristretta si identifica e si qualifica con precisione con l'intento dell'utente. Se esiste qualche ambiguità in termini di destinazione d'uso, lo strumento informatico non sarà considerato un'arma[7]. Le *cyberweapons* sono considerate tali se esse si identificano in uno strumento potenzialmente letale, cioè idoneo a provocare gravi danni a cose, persone, sistemi e strutture; se sono intenzionalmente indirizzate alla distruzione/compromissione di cose o persone (devono avere uno specifico obiettivo); se sono percepite come minaccia effettiva e reale da parte del destinatario.

Come si potrà intuire, dato l'ampio spettro di utilizzo della tecnologia cyber in modi e modalità diverse e imprevedibili, si ridefinisce il quadro della competizione globale, dove la supremazia tecnologica aprirebbe le porte a una nuova corsa verso armamenti di natura diversa, ma altrettanto efficaci nei risultati una volta impiegati. È in questa prospettiva che la stessa strategia dell'«impegno persistente» (*Persistent engagement*) pone gli Stati Uniti molto più avanti dell'Europa; quest'ultima, molto più restìa a mettere in campo strategie di difesa avanzata che richiederebbero una capacità di infiltrarsi preventivamente nelle reti informatiche di altri Stati, ponendo anche in essere tentativi pianificati per condurre attacchi informatici contro obiettivi definiti e impedendo attivamente, e preventivamente, che piani di aggressione possano essere eseguiti[8]. In questo senso, Jason Healey nel suo *The Implications of Persistent (and permanent) Engagement in Cyberspace*, riconosce che

[7] https://ngm.com.au/cyber-weapons-definitions/.

[8] A tal proposito, vedasi: T. Liebetrau, *Cyber conflict short of war: a European strategic vacuum*. In «European Security», vo.31, n.4-2022 pp. 497-516.

> Le forze informatiche sono in costante contatto

e che

> L'impegno persistente è una risposta ragionevole[9].

Healey sostiene che

> Sembra che ci siano molti più modi affinché la nuova strategia possa esacerbare il conflitto informatico piuttosto che smorzarlo[10],

perché la strategia statunitense fa alcune ipotesi fondamentali sul comportamento dell'avversario che potrebbero essere sbagliate.

Ciò significa, che oltre al rischio di interpretazioni errate, ritorsioni ed escalation, abbracciare pubblicamente una strategia che sanziona la rimozione preventiva di server in paesi stranieri può portare a un aumento dello sfruttamento delle vulnerabilità nei software commerciali utilizzati da cittadini, aziende e dalle autorità pubbliche a livello globale[11]. Probabilmente, aumenterebbe l'insicurezza informatica e renderebbe i cittadini e le imprese a livello globale più suscettibili alla criminalità informatica, alla sorveglianza o alle interruzioni dei servizi quotidiani[12].

Questo, però, non vuol dire che i paesi europei dovrebbero adottare ciecamente la strategia americana di impegno persistente e di difesa avanzata (*The Strategy of Persistent Engagement and Defending Forward*).

---

[9] J. Healy, *The implications of persistent (and permanent) engagement in cyberspace*. In «Journal of Cybersecurity», 5 (1), 2019 pp. 1-15. Per la formulazione della necessità strategica di acquisire e mantenere la superiorità nel cyber spazio da parte degli Stati Uniti vedasi anche: US-Cyber Command, *Command Vision for US Cyber Command. Achieve and Maintain Cyberspace Superiority*, 2018, disponibile in https://nsarchive.gwu.edu/sites/default/files/documents/4421219/United-States-Cyber-Command-Achieve-and-Maintain.pdf. E, ancora, *Cyberspace Operations, Joint Chief of Staff,* Joint Publication, June3-12, 2018.

[10] Ivi, p. 2.

[11] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, Oxford University Press, New York 2016. Cfr. anche F. Baiardi, *Il "persistent engagement" nella cyberdifesa Usa: punti di forza, debolezze e sovranità digitale* in «Agenda Digitale», 28 luglio 2022, in https://www.agendadigitale.eu/sicurezza/il-persistent-engagement-nella-cyber-difesa-usa-punti-di-forza-debolezze-e-sovranita-digitale/.

[12] Gli episodi di criminalità informatica stanno aumentando in tutta Europa in termini sia di quantità che di sofisticazione. Una tendenza destinata a crescere in futuro, visto che si prevede che 22 miliardi circa di dispositivi in tutto il mondo saranno collegati all'Internet delle cose entro il 2024. Vedasi anche, A. Klimburg, *Mixed signals: a flawed approach to cyber deterrence*, in «Survival», 62 (1), 2020 pp. 107-130; J.T. Jacobsen, *Cyber offense in NATO: challenges and opportunities*, in «International Affairs», 97 (3), 2021, pp. 703-720.

Ma di certo società, governi, imprese e individui dovranno essere consapevoli che nell'essere sempre più dipendenti dall'ambiente digitale, diventano, così, sempre più vulnerabili all'uso improprio di quell'ambiente. Un rischio che è ormai una sorta di condizione propria di un nuovo modello neo-global di relazioni politiche ed economiche che nel declinare il senso dell'internazionalizzazione, non si ripiega su se stesso, ma si ridefinisce in un modello postmoderno del significato delle diversità e delle competitività. In questo senso, la sicurezza informatica non può, allora, avere limiti di prospettiva, ma deve andare ben al di là degli stessi confini di una comunità.

Considerando le minacce possibili, per Rich Baich, esperto in *cybersecurity*, queste in ambiente cyber si possono dividere nelle seguenti opzioni: *cybercrime*, quale condotta criminosa, caratterizzata dall'abuso di componenti della tecnologia dell'informazione sia sottoforma di hardware che di software ovviamente per finalità illecite di lucro; *cyberspionaggio* dove i pirati informatici pongono in essere attacchi informatici su commissione di governi e grandi aziende con lo scopo di poter entrare in possesso di dati riservati; guerra cibernetica (o *cyberwarfare*) dove gli attori principali sono gli Stati e non solo questi, e dove l'obiettivo principale è quello di indebolire l'avversario attraverso propaganda e/o disinformazione, o attaccando i suoi sistemi informatici, le infrastrutture, o le aziende strategiche; *cybernuisance*, cioè l'attacco condotto contro i server di imprese o organizzazioni per motivi etici, facendo comparire sul sito delle vittime dei messaggi a contenuto politico o sociale tipico di movimenti antagonisti o di radicalismi di vario genere, politici o, ad esempio, anche religiosi[13].

Difendersi nel cyberspazio. «Tallinn Manual» e dintorni

La galassia delle possibili minacce non si esaurisce in modi e tempi definiti o anche solo definibili. Oggi c'è molto di più della semplice vulnerabilità dei sistemi. Oltre alla protezione da perdite finanziarie, danni fisici, ecc., alla sicurezza informatica si richiede di garantire e orientare gli sforzi per massimizzare i benefici, poiché la sicurezza del cyberspazio è tanto

[13] Cfr. https://findbug.io/the-4-types-of-cybersecurity-threats-and-a-formula-to-fight-them/ *The four types of threats*. La formula interpretativa è: Risk = vulnerabilities x threat x asset value. Anche in: https://cybersecuritysymposium.charlotte.edu/speaker/rich-baich/.

tecnologica quanto commerciale e strategica; tanto internazionale quanto regionale, nazionale e personale; e tanto una questione di pericolo e vulnerabilità quanto un'opportunità di crescita sociale, economica e culturale[14]. Tutto questo, è sufficiente per trasformare il cyberspazio nel nuovo dominio delle sfide del futuro, nella competizione non solo politica, ma anche economica e nel quale matureranno e si declineranno le politiche di crescita di una società.

Eppure, mentre questa nuova dimensione assume maggiore importanza per le strategie di sicurezza governative, non esiste ancora oggi una definizione univoca e generalmente condivisa del termine cyberspazio. Una possibile definizione potrebbe essere quella che definisce il cyberspazio come quel dominio dove

> Ogni aspetto della vita di relazione, sia esso sociale, economico e politico se non culturale dipende da una rete interdipendente di infrastrutture informatiche che nel loro insieme definiscono il cosiddetto «cyberspazio»[15].

Una dimensione, la precedente, nuova nel modo di percepire spazio e tempo e che altera le stesse grandezze fisiche modificandole e adattandole a processi di elaborazione, subordinandole a condizioni di accesso, di uso di dati e di informazioni o espressione di governance sociali ed economi-

[14] P. Cornish (ed.*), The Oxford Handbook of Cyber Security Get access Arrow*, Oxford University Press, Oxford, 2021.

[15] Vi sono altre definizioni che maturano negli ambienti governativi o all'interno di alleanze. Ad esempio, la Germania definisce il cyberspazio come «lo spazio virtuale di tutti i sistemi IT a esso collegati in termini di dati a livello globale. La piattaforma base del cyberspazio è Internet considerato quale strumento universale e accessibile al pubblico, rete di collegamento e di trasporto che può essere integrato e ulteriormente ampliato in qualsiasi numero di reti dati aggiuntive». Cfr. Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011. Disponibile in: http://www.cio.bund.de/SharedDocs/Publikationen/DE/StrategischeTh emen/css_engl_download.pdf;jsessionid=5B6636607CB58EFBB61431566F7E5B15.2_cid334?_blob=publicationFile (p.14). Così in Department of Defense, *Dictionary of Military Terms*: http://www.dtic.mil/doctrine/dod_dictionary/. Più edulcorata quella offerta dall'International Telecommunications Union (ITU) che ricorre al cosiddetto «ambiente cibernetico» nel quale sono compresi utenti, reti, dispositivi, software, processi, informazioni in archiviazione o in transito, applicazioni, servizi e sistemi che possono essere connessi direttamente o indirettamente alle reti. Vedasi International Telecommunication Union, *Series X: Data networks, open system communications and security: overview of cybersecurity*, 2008. Consultabile in: http://www.itu.int/net/ITUR/asp/terminology-definition.asp?lang=en&rlink={3E2AC1A2-9D18-4235-80B6-7946B3266788}. Così anche in: F.D. Kramer, S. Starr, L.K. Wentz *Cyberpower and National Security: Policy Recommendations for a Strategic Framework, in Cyberpower and National Security,* National Defense University Press, Washington (D.C.), 2009.

che completamente automatizzate. Gli Stati Uniti, dal canto loro, ritengono che si tratti di un

> Dominio globale all'interno dell'ambiente informativo costituito dalle reti interdipendenti di informazione, da infrastrutture tecnologiche e dati residenti, compreso Internet, da reti di telecomunicazioni, sistemi informatici embedded-responsabili e responsabili del trattamento.

Vi è anche la definizione ad esso attribuita nel «Tallinn Manual 2.0» per la quale il cyberspazio è da intendersi come

> L'ambiente formato da componenti fisici e non fisici, caratterizzati dall'uso del computer e dello spettro elettromagnetico, per immagazzinare, modificare e scambiare dati mediante reti informatiche[16].

Creato sotto la supervisione di Michael N. Schmitt, preside del Dipartimento di Diritto Internazionale presso lo U.S. Naval War College oltre che già membro del George C. Marshall, Centro Europeo per gli studi sulla sicurezza, il Tallinn Manual rappresenta il primo tentativo di dare organicità a una serie di norme e misure possibili nell'ambito di attacchi, quindi di condotte aggressive, portate ai sistemi di governance e alle architetture digitali delle nazioni NATO. Il «Tallinn Manual», definito come necessario per dare un quadro complessivo e possibilmente normativo per quanto possibile non essendo il prodotto di una istituzione internazionale su pari mandato, è stato promosso dal NATO-Cooperative Cyber Defence Centre of Excellence (CCDCOE) istituito nella capitale estone ritenendo che un attacco cyber avrebbe potuto legittimare l'applicazione dell'articolo 5 del trattato dell'Atlantico del Nord giustificando il ricorso alla difesa collettiva di uno Stato-parte aggredito.

Lo scopo di tale Manuale era quello di offrire un quadro normativo possibilmente organico, derivato per analogia, in materia di cyberspazio e *cyberwarfare*. Pubblicato in una prima edizione nel 2013, un aggiornamento verrà poi offerto tre anni dopo presentandosi come un *corpus juris* senza carattere vincolante ma utile nell'essere una sorta di Testo Unico e, dove possibile, indicando le norme che disciplinano i conflitti tradizionali con la loro possibile applicazione agli attacchi cyber. La ricerca di analogie, di sintesi interpretative e di possibilità applicative ne fanno una pubblicazione di riferimento in un vuoto legislativo esistente nel diritto internazio-

[16] Cfr. M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, New York, 2017. Consultabile anche in: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379#search (p.278).

nale che si affida all'applicazione per analogia delle norme in vigore per i conflitti cosiddetti fisici. Composto nella versione 2.0 del 2016 il Manuale comprende quattro sezioni per un totale di 154 *rules*.

La prima sezione del Manuale indica i principi fondamentali di diritto internazionale relativamente alla tutela della sovranità, alla giurisdizione e responsabilità statale per quanto applicabili alla disciplina del cyberspazio. La seconda, si articola tra *rules* che riguardano come si possono regolare e garantire la tutela dei diritti umani, le relazioni diplomatiche, il diritto aeronautico e del mare in senso lato definite nel cyberspazio, quanto l'applicabilità delle norme di diritto internazionale relativamente all'uso legittimo della forza piuttosto che alla gestione delle crisi internazionali.

Un Manuale che nasce a ridosso di un attacco condotto contro asset bancari e non solo estoni nel 2007 e attribuito alla Russia. Si trattò di un primo e vero uso in termini di *cyberwarfare* di un Distributed Denial of Service (DDoS)[17]. Il risultato ottenuto fu il collasso del sistema bancario, di molti servizi governativi, di alcune società e dei media. Un attacco che determinò un problema giuridico a premessa e un dilemma operativo dettato dal ritenere o meno un attacco informatico alle infrastrutture critiche di un Paese Nato riconducibile all'interno delle previsioni ex art. 5 del trattato dell'Atlantico del Nord. Una questione risolta in senso positivo al vertice Nato di Madrid del 28-30 giugno 2022 e confermata durante la Nato Cyber Defence Pledge Conference tenutasi a Roma il 9 e 10 novembre dello stesso anno. Conferenza, quest'ultima, nella quale si ribadiva che gli alleati, nel riaffermare il mandato difensivo della Nato, si sono impegnati a impiegare l'intera gamma di capacità per scoraggiare, difendere e contrastare attivamente l'intero spettro delle minacce informatiche in ogni momento, anche considerando risposte collettive ritenendo fondamentale la necessità di cooperare in materia di cybersicurezza e sottolineando che

> Il cyberspazio non è uno spazio libero e dunque i diritti fondamentali, le leggi e le sue applicazioni valgono online come offline.

La definizione di armi informatiche

A questo punto si pone l'interrogativo se *malware* (*malicious software*) e altre formule di interazione digitale, finalizzate a sovvertire una gover-

[17] «Distributed Denial of Service» (DDoS). Attacco condotto attraverso una serie di richieste fittizie di dati e informazioni alle quali il sistema non riesce a rispondere e non risponde neanche alle richieste legittime.

nance nei vari aspetti possibili, siano classificabili come vere e proprie armi informatiche. Un quesito che in ragione degli effetti ottenibili sulla stabilità di una comunità politicamente organizzata, sovrana e indipendente vede ancora una volta il Manuale di Tallinn definirle *cyberweapons*. Per il Nato - Cooperative Cyber Defence Centre of Excellence, la definizione non è univoca e formalmente definita. Il Tallinn Manual versione 2.0 indica, infatti, come arma informatica un

> Mezzo di guerra informatica utilizzato, progettato o destinato a essere utilizzato per causare lesioni o morte di persone o danni o distruzione di oggetti.

Il Manuale di Tallinn offre anche la definizione di «attacco informatico» come

> Un'operazione informatica, offensiva o difensiva, che si prevede ragionevolmente possa causare lesioni o morte a persone o danni o distruzione di oggetti.

Ma non solo. Vengono anche evidenziate due caratteristiche degne di nota al fine di definirne meglio il perimetro interpretativo. In primo luogo, il riferimento ad atti di violenza nell'articolo 49 del I Protocollo Aggiuntivo è stato interpretato come se non limitasse la portata di un attacco alle attività che rilasciano forza cinetica. In secondo luogo, ciò che costituisce un attacco informatico è rappresentato dalle conseguenze delle operazioni informatiche. Il gruppo internazionale di esperti che ha elaborato il Manuale ha convenuto, infatti, che l'esistenza di un «danno consequenziale» derivante dall'operazione informatica qualificherebbe l'operazione stessa come un attacco laddove la nozione di «danno consequenziale»

> Comprende qualsiasi danno consequenziale, distruzione, lesione o morte ragionevolmente prevedibili[18].

Tale interpretazione non è stata ritenuta sufficiente a qualificare la sola consequenzialità come un elemento essenziale per configurarne la norma vietata affermando che il danno o la distruzione non soddisfa la soglia del danno consequenziale che costituisce un attacco[19].

---

[18] «...encompasses any reasonably foreseeable consequential damage, destruction, injury, or death...».

[19] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 p. 106.

È un pò lo stesso dilemma che riguarderà le cosiddette «Armi autonome» (*Lethal Autonomous Weapons Systems* - LAWS), che determineranno il passaggio alla nuova rivoluzione negli affari militari e che porrà delle condizioni necessarie di riflessione sulle validità delle norme sui conflitti armati, sulla legittimità dei sistemi d'arma a controllo IA e, soprattutto, sulla responsabilità di chi vi ricorrerà e di come e a quale costo di vite umane e di danni collaterali. A tal proposito i termini stessi di produzione e uso di LAWs sono oggi posti sul terreno del confronto poiché, in termini di disciplina circa la produzione e l'uso delle LAWs, ben poco si è fatto e raggiunto circa la limitazione e la responsabilità nell'uso[20]. La qualità principale delle LAWs è quella di abbattere la sfera emozionale, perché in queste non vi è paura né si pongono scrupoli morali, ed è proprio in questa versione della nuova *warfare* che il vero obiettivo nelle nuove condotte sarà proprio quello di superare il limite emozionale[21].

Attacchi in Rete

Gli attacchi cibernetici si manifestano con caratteri peculiari che li distinguono dalle condotte cinetiche tradizionali. Imprevedibilità, immediatezza, intangibilità degli obiettivi, mezzi/sistemi considerati come veri e proprie *cyberweapons* oltre che del danno, non necessariamente fisico, rappresentano insieme alla difficoltà di individuazione della sorgente i caratteri più singolari e le difficoltà più significative per porre in essere efficaci misure di allarme, contenimento e risposta[22]. Ciò richiede, infatti, la necessità di definire un perimetro necessario nel quale poter ricondurre tali comportamenti nell'ambito dell'applicazione del diritto internazionale. La possibilità di nascondere o dissimulare l'identità della sorgente

[20] A. Kane, *Lethal Autonomous Weapons Systems: can the international community agree on an approach?* Vienna Center for Disarmament and Non-Proliferation, May 28, 2018. https://vcdnp.org/lethal-autonomous-weapons-systems-can-the-international-community-agree-on-an-approach/. Anche Congressional Research Service, *Defense Primer. US Policy on Lethal Autonomous Weapon Systems*. Così in https://crsreports.congress.gov/product/pdf/IF/IF11150.

[21] F. Farruggia (a cura di), *Dai droni alle armi autonome. Lasciare l'Apocalisse alle macchine?* Franco Angeli, Milano, 2023. Interessanti anche i contributi presenti a riguardo come *War at Hyperspeed, Autonomous robots and swarms will change the nature of warfare*, in «The Economist», *The Future of War*, «Special Report» pp. 13-15 e, nello stesso «Special Report», *Man and Machine. AI-empowerd robots pose entirely new dangers, possibly of an existential kind*, pp.15-16.

[22] *Ibidem.*

dell'attacco o del luogo da cui esso viene lanciato, o di non poter definire a priori e in termini concreti l'entità del danno, rappresentano i limiti, ma anche la necessità di individuare una responsabilità oggettiva e soggettiva all'attacco condotto. Volendo ricondurre tali atti all'interno delle previsioni di cui all'art.2 p. 4 dello Statuto delle Nazioni Unite, si potrebbe convenire con una chiave interpretativa per la quale

> Qualora un attacco cibernetico, direttamente o indirettamente, provochi una conseguenza fisica, cioè una distruzione, dispersione, deterioramento o inservibilità totale o parziale di cose mobili o immobili, ovvero una lesione o la perdita di vite umane, costituisce un uso della forza[23].

Il problema di definire l'ambito possibile di applicabilità delle previsioni dello Statuto delle Nazioni Unite in caso di aggressione cibernetica - riconducendone la legittimità giuridica nel novero delle previsioni del diritto internazionale - richiederebbe di valutare se l'art.51 della stessa Carta possa trovare una sua collocazione ed esprimere una propria efficacia dal momento in cui l'articolo stesso, quale eccezione in discrimine al divieto dell'uso della forza ex art.2 p. 4, indica la possibilità di agire in legittima difesa. Ciò, però, richiederebbe anche di definire se e in che modo il perimetro giuridico di applicabilità dell'art.51 possa ricomprendere al suo interno un attacco cyber considerato che, a supporto, vi è la più stretta configurazione dell'agire digitalmente rispetto alla più ampia nozione di uso della forza.

È evidente, in ogni caso, che per integrare la scriminante dell'uso legittimo della forza in risposta a un attacco cyber si tratterebbe di poter innanzitutto determinare la gravità dell'azione intrapresa, i tempi di condotta e le conseguenze, il nesso causale tra azione e danno, la misurabilità del danno arrecato, la qualificazione del soggetto agente come Stato e la sua responsabilità nell'aver violato la sovranità di un altro Stato e quale destinatario delle norme di diritto internazionale. Sia il Manuale di Tallinn che le posizioni assunte dalla stessa Alleanza Atlantica dopo il Vertice di Madrid del giugno 2022, tendono a ritenere idonee le condizioni precedenti a qualificare la fattispecie ex art. 51 legittimante l'autodifesa in caso di attacco cyber visto che tali attacchi, se producono danni fisici alla sopravvivenza fisica ed economica di uno Stato sovrano, integrerebbero perfettamente le condizioni necessarie per l'uso legittimo della forza.

[23] www.sicurezzanazionale.gov.it.

Vulnerabilità ad ampio spettro

Le prossime sfide si giocheranno su più piani man mano che si eleverà il livello di governance ma dove ogni piano, però, vedrà interconnettersi e condividersi informazioni attraverso le quali dipenderà la sicurezza fisica oltre che economica di una società. Lo stesso concetto di *cybervulnerability* non è certo limitato e limitabile a forme definite di minacce. La configurazione di un software aggressivo, o il modificarsi di questo da parte di chi condurrà un attacco informatico, sarà sempre espressione del livello e della qualità delle conoscenze tecnologiche messe in campo da una società per conseguire gli obiettivi di sicurezza informatica, riservatezza, integrità e disponibilità, che, senza un'opportuna strategia a difesa, possono tutti o in parte essere compromessi.

Per questo diventa necessario tener conto dei rischi potenziali cui l'architettura digitale potrebbe incorrere oltre a considerare procedure utili a prevenire, se non rendere minime, le conseguenze di una minaccia improvvisa, assicurando la sicurezza e la funzionalità di ogni assetto di governance dello Stato-bersaglio. Così come, si tratterebbe anche di ridurre le vulnerabilità organizzative attraverso l'adozione di misure utili a contrastare possibili *malware* permettendo la continuità della gestione di servizi attraverso modalità di controllo sia fisiche che tecniche derivanti dagli applicativi scelti a protezione. Per questo, la sicurezza non potrà non considerare come ambiti di verifica il controllo degli accessi (personale autorizzato e procedure); l'utilizzo di soli strumenti certificati (per evitare contaminazioni esterne); norme chiare dirette a disciplinare l'organizzazione delle procedure di sicurezza con l'attribuzione di ruoli specifici al personale coerentemente con le funzioni, e responsabilità, devolute; controlli periodici di sicurezza e verifiche sull'affidabilità degli strumenti utilizzati.

Tuttavia, deve essere chiaro che nonostante gli apprestamenti in difesa, comprendere lo spazio nel quale la minaccia cyber si svolge non è agevole, poiché tale minaccia contiene e supera le altre dimensioni nel presentarsi come una costante prossimità al quotidiano da parte di un potenziale avversario. Una prossimità per la quale ogni volontà di delimitarne i perimetri rappresenta una difficoltà non trascurabile, mentre nell'universo cyber lo spazio si contrae e si diluisce secondo tempi scanditi da chi conduce l'attacco, dal momento che può essere condotto da un altrove possibile e colpire in più punti. Se volessimo utilizzare un linguaggio mili-

tare si potrebbe affermare che non vi sono modi per delimitare un possibile campo di battaglia in termini fisici se ci si trova di fronte a un conflitto virtuale. Chi conduce l'attacco, in altre parole, dispone sempre di un vantaggio iniziale. D'altronde, in un attacco cyber non vi è alcuna tridimensionalità riferibile a una condotta ortodossa così considerata in termini tradizionali, considerato che gli spazi si dilatano o restringono in relazione agli obiettivi di chi conduce l'attacco e alle capacità di scoperta, contenimento e risposta del soggetto-bersaglio.

Ecco, allora, che per il Department of Defense statunitense un attacco informatico può essere generalmente definito come

> Un atto ostile condotto attraverso l'uso di computer o sulle reti o verso sistemi correlati, e destinato a perturbare e/o distruggere le risorse critiche di un avversario[24].

Ovviamente, un attacco informatico, sia esso concreto o in forma di minaccia, non è solo diretto contro le risorse, ma anche contro le infrastrutture critiche, in termini di governance, i processi come i servizi. L'obiettivo è quello di rendere inutilizzabili totalmente o parzialmente, almeno, le infrastrutture di Comando e Controllo (C2) di una comunità politica o di un competitor. In questo senso, l'allargamento del dominio cyber non rappresenterebbe altro che una dilatazione dello spettro cognitivo, dove la sfida sarà determinata dalla conquista delle informazioni ritenute più utili, ad esempio, per condurre operazioni di manipolazione dell'opinione pubblica, profilandone il *sentiment* attraverso operazioni di *social engineering*. Ovvero, ancora, nel condurre veri e propri attacchi diretti a realizzare una strategia di disinformazione quale comunicazione diretta a incidere sulle percezioni ricorrendo alla falsificazione totale, alla selezione e alla distorsione dei fatti per narrare storie alternative funzionali a un obiettivo.

In genere definite come *Information Operation* (IO), si tratta di azioni messe in campo per usare e gestire informazioni attraverso l'uso della propaganda per ottenere vantaggi competitivi, utilizzando la diffusione di informazioni per promuovere alternative di governance attraverso la disinformazione e la sua influenza non solo nei mercati finanziari globali, ma anche cercando di affermare la non legittimità di una leadership minan-

[24] US. Department of Defense Cybersecurity, *Resource and Reference Guide*, February 28, 2022. Consultabile in: https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf.

done la sua credibilità. Non è un caso che a tal proposito Clint Watts, del Alliance For Securing Democracy & Foreign Policy Research Institute della George Washington University ha definito come «Advanced Persistent Manipulators» quelle realtà *cyber* che dispongono di adeguate risorse per condurre

> Un attacco esteso, sofisticato, multipiattaforma e multimediale su un obiettivo specifico[25],

ricorrendo a campagne di influenza online con le operazioni trasferite nel quotidiano di una comunità-bersaglio, attraverso il perseguimento di propri traguardi e obiettivi informativi per un periodo prolungato; superando la chiusura degli account e i time-out della piattaforma attaccata; impiegando combinazioni di tecniche di influenza sia nel mondo reale che in quello virtuale. O, ancora, operando su tutte le piattaforme di social media utilizzando le caratteristiche di ciascuna di esse per raggiungere i propri obiettivi, disponendo di risorse sufficienti per formare o assumere i migliori talenti e sviluppare o acquistare la migliore tecnologia; sfruttando, aggregando e analizzando i dati degli utenti per condurre una efficace profilazione dell'utente/client e sviluppando tattiche e tecniche adattive che evitino i termini di servizio della piattaforma e i controlli predefiniti dalla stessa; conoscendo, operando e controllandone i contenuti[26].

È evidente che simili operazioni, possibili e ad ampio spettro, possono presentarsi mediante la costruzione di notizie false che si caratterizzano per l'uso delle reti social - cui si ricorre con la creazione di falsi account – e che si risolvono come dei veri e propri «falsi amplificatori», sfruttando l'effetto *bandwagoning* che ne deriva, utile per influenzare e dirigere il *sentiment* dell'opinione pubblica su un dato evento o su un certo consenso. Ricorrere a tali strumenti sul piano tattico significa inondare i media in termini di ridondanza progressiva di più narrazioni e, quindi, interpretazioni e spiegazioni di un dato evento confondendo il formarsi di una opinione condivisa, promuovendo false letture della realtà, ponendo in discussione la credibilità di un avversario politico o di un competitor economico, essere utili distrattori per l'opinione pubblica in momenti di particolare crisi di consenso o di fragilità della tenuta interna di una comunità

[25] C. Watts, *Alliance for Securing Democracy & Foreign Policy Institute*. Così in https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/.

[26] https://securingdemocracy.gmfus.org/wp-content/uploads/2019/02/APM-Clint-1.pdf.

politicamente organizzata. O, anche, creare movimenti di protesta attraverso l'uso di gruppi di contropotere o di controinformazione costruiti *ad hoc* veicolandone il messaggio nell'universo digitale.

Insomma, si tratta di un panorama complesso, che viene ricondotto all'interno di una nuova configurazione delle minacce che riguardano la formazione dell'opinione pubblica e del consenso come le *Cyber-Enabled Information Warfare and Information Operations* (CyIOs) il cui target è definito dalla volontà di far perdere di credibilità ai candidati durante le consultazioni elettorali, manipolare il consenso con la costruzione di notizie false che mirino a delegittimare il risultato politico e, in questo modo, attaccare la fiducia nelle istituzioni[27]. Tutto questo, ricorrendo a società di *trolling-as-a-service* per aggregare i dati sul pubblico e diffondere messaggi mirati e spesso non autentici. O, ancora, per condizionare scelte politiche in campo economico e non solo a vantaggio di chi detiene il potere di accesso alle informazioni critiche, magari utilizzando anche strumenti, e piattaforme, di uso comune come, ad esempio, ricorrendo a una semplice class-room su Google o su altre piattaforme, registrandosi e condividendo informazioni con un hacker.

[27] H. Lin, J. Kerr, *On Cyber-Enabled Information Warfare and Information Operations* pp. 251-272. In P. Cornish (ed.) *The Oxford Handbook of Cyber Security Get Access Arrow*, Oxford University Press, Oxford, 2021. Anche se il focus del volume è orientato verso la tenuta degli Stati Uniti quale potenza globale, è interessante, come si sottolinea, che gli avversari degli Stati Uniti si rivolgono sempre più a metodi asimmetrici per affrontare i conflitti. In tale contributo, si afferma una riflessione interessante per la quale l'idea delle operazioni di guerra e influenza dell'informazione (IWIO-*Information Warfare & Influence Operations*) abilitate dal cyber debbano essere viste come una forma di conflitto o confronto cui gli Stati Uniti, e le democrazie liberali più in generale, sono particolarmente vulnerabili. Per IWIO, in particolare, si intende un uso deliberato di informazioni contro un avversario per confondere, fuorviare e influenzare le scelte e le decisioni prese a difesa. In questo senso, si può dire che le IWIO siano da ricondurre all'interno di attività ostili tra parti i cui interessi si sovrappongono se non siano in pieno conflitto. Tuttavia, per il diritto internazionale, una condotta espressa in termini di IWIO non necessariamente avrebbe in sé tutti gli elementi necessari per definirsi, e quindi qualificarsi, come guerra nel senso compiuto e giuridicamente definibile. Ciò nonostante, le operazioni IWIO, rappresentano di certo forme di condotta che mirano a intervenire sulla manipolazione delle informazioni e sulla formazione di un'opinione pubblica attraverso l'uso delle tecnologie comunicative. È evidente che condotte IWIO intraprese sul piano cyber permettono di utilizzare a proprio vantaggio l'elevata connettività, una bassa latenza, alti gradi di anonimato, l'insensibilità alla distanza e ai confini nazionali.

Dalla «Zona Grigia» al Quinto Dominio

I precedenti possono essere considerati tutti aspetti che si accompagnano e si sommano, in una prospettiva più ampia, a una nuova versione del confronto che vede nel campo delle relazioni internazionali, l'affermarsi di uno spazio di confronto definito come «Zona Grigia» (*Gray Zone*) nel quale si decidono iniziative diplomatiche che mettono in campo processi decisionali e perseguono obiettivi non necessariamente, apertamente, militari. Infatti, la compulsività della competizione geopolitica tra le potenze rivali nella loro corsa a ritagliarsi o espandere le proprie aree di influenza, si stanno manifestando sempre più in uno spazio che va ben oltre la diplomazia e al di fuori della guerra convenzionale, definito, appunto, Zona Grigia. Un aspetto chiave delle sfide nella Zona Grigia è che dovrebbero essere sufficientemente ambigue da lasciare gli stessi targets incerti su come rispondere[28].

A tal proposito, il Comando delle Operazioni Speciali degli Stati Uniti ha coniato una definizione di «Gray Zone» intendendola come spazio di

> Interazioni competitive tra e all'interno di attori statali e non statali che si collocano tra il tradizionale dualismo guerra e pace[29].

Un elemento chiave delle operazioni all'interno della Zona Grigia è che esse rimangano al di sotto della soglia di un attacco, che potrebbe avere una risposta militare convenzionale legittima (*jus ad bellum*). Il concetto stesso di Zona Grigia non è nuovo ed è stato spesso utilizzato in passato come strategia militare nelle guerre per procura o surrogate, quanto nei conflitti a bassa intensità e nella sponsorizzazione di attori non statali[30].

---

[28] Cfr. *Shades of grey. The use of constructive ambiguity.* In «The Economist», *The Future of War*, Special Report, January 27, 2018 p.8 e ss.

[29] «…competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality».

[30] B.R. Prakash, *The Gray Zone - Targeting the Power Grids*, April 6, 2021, Consultabile in https://dras.in/the-grey-zone-targeting-the-power-grids/. Sull'argomento vedasi anche: T. Dobbs, G. Fallon, S. Fouhy, *Gray Zone. The Forge (Report),* Australian Defence College, September 9, 2020; P. Kapusta, *The Gray Zone* (pdf), in: www.soc.mil. United States Special Operations Command, e *Challenging the Gray Zone,* in: www.law.upenn.edu. University of Pennsylvania Law School, February 18, 2021. L.J Morris, M.J. Mazarr, J.W. Hornung, S. Pezard, A. Binnendijk, M Kepe, *Gaining competitive advantage in the Gray Zone* (pdf), in: www.rand.org. RAND, February 18, 2021. J. H. Matisek, *Shades of Gray deterrence: issues of fighting in the Gray Zone*, in «Journal of Strategic Security» vol. 10, n. 3, 2017, pp. 1-26. Così, anche: D. Carment, D. Belo, *Gray-zone conflict management: theory, evidence, and challenges*, in «European, Middle Easter & African Affairs», Summer 2020 n.2 pp. 21-41 e www.airuniversity.af.edu.

La sua rideterminazione si giustifica nel ritenere che sia tra gli Stati che tra le élite politiche è la consapevolezza che il *cyber-power* e la sua applicazione nella Zona Grigia ha il potenziale per sconvolgere l'equilibrio più ampio del potere tra gli Stati Uniti e i suoi alleati da un lato, e Cina e Russia dall'altro. Al di là di questo ampio consenso, non c'è molto accordo su come questo sia sostenibile visto che la concorrenza tecnologica può essere valutata o misurata in termini di potere; una situazione aggravata dalla frequente comparsa di nuove tecnologie (come nano chip, chip a base di carbonio, architetture *cloud*, calcolo quantistico, Intelligenza Artificiale, autonomi sistemi d'arma e robot militari).

Attacchi informatici, notizie false, disinformazione, sovversione delle istituzioni democratiche e distruzione della coesione sociale rappresentano i nuovi obiettivi da conseguire in questo campo di battaglia della Zona Grigia e vengono sempre più ricercati per creare spazi nuovi e radicali per la sua espansione[31]. In questo senso, l'idea che possa affermarsi anche una cosiddetta «Gray-Zone Warfare» (GZW) diventa, così, uno dei prodotti delle trasformazioni e dell'uso della dimensione cyber e dei software che si trasformano o sono trasformabili, in veri e propri sistemi d'arma in senso lato. Con le operazioni GZW si crede, ad esempio, di evitare un possibile conflitto ma in realtà il vero risultato che si ottiene è quello di creare un *bias* cognitivo per il quale, al contrario, proprio nella Zona Grigia si acquisiscono le informazioni utili o si apprestano le decisioni per condurre al conflitto.

D'altra parte, anche Nathan Freier, professore di studi sulla sicurezza nazionale presso lo Strategic Studies Institute dell'U.S. Army War College, non lesina nel suo *The Darker Shade of Grey: A New War Different Any Other* di sottolineare come quasi tutte le strategie della Zona Grigia includono combinazioni uniche di metodi ostili all'interno e attraverso strumenti di potere, domini tradizionali (aria, terra, mare, spazio) e spazi competitivi fortemente contestati (ad esempio, spettro elettromagnetico o cyberspazio). Sottolinea, inoltre, che gli avversari della Zona Grigia rappresentano una minaccia in quanto il carattere dei loro metodi competitivi promette risultati bellici anche senza ricorrere alla provocazione militare. Ciò dimostra quanto nella Zona Grigia, strategie e approcci conflittuali

> Si trovano tra guerra e pace "classiche", tra motivazioni e metodi legittimi e illegittimi, tra condizioni e norme universali, tra ordine e anarchia[32].

[31] *Ibidem*

[32] «Lie between "classic" war and peace, legitimate and illegitimate motives and methods, universal conditions and norms, order and anarchy». Così, N. Freier, *The Darker Shade of Gray: A New War Unlike Any Other*, Center for Strategic & International Studies, July 27, 2018. Consultabile in https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other.

In questo quadro, proprio il controllo di una *Virtual Humint* può diventare la vera cartina di tornasole sulla capacità di affrontare e contenere, se non rispondere e capovolgere a proprio favore, una minaccia cyber gestendo l'intero complesso OHST, ovvero, le *Osint-Humint-Sigint-Techint* dirigendo l'attenzione verso orizzonti *open source* che sempre di più offrono, seppur sovrapponendo informazioni spesso ridondanti, ampi spazi di ricerca di informazioni utili a garantire la sicurezza di una nazione quanto la tutela di patrimoni di know how fortemente competitivi se si dispone di capacità di verificare la correlazione delle più coerenti e di maggior interesse[33].

Ecco, quindi, che ritenendo che la sfida sarà quella di determinare un quadro di razionalità comportamentale - quasi un *behaviorismo* digitale connesso magari a un organismo senziente nel prossimo futuro - definire la dimensione nella quale si svolgeranno le azioni degli attori politici ed economici diventerà una necessità di metodo oltre che un obbligo di conoscenza.

Ciò significa, allora, che in una versione e visione multi-dominio dello svolgersi della attività umane, il cyberspazio coniugato con forme di IA evoluta sul piano quantistico, rappresenterà la nuova frontiera dove si espanderanno le capacità, non solo umane, per agire nell'interesse delle comunità nelle quali ogni diversità culturale si riorganizzerà in termini politici e si confronterà con le proprie esigenze economiche secondo aspettative e necessità di garantirsi crescita e sopravvivenza fisica. In questo senso, il «Quinto Dominio» rappresenta già oggi, in una definizione ormai largamente condivisa - pur con qualche eccezione che lo ricondurrebbe in un substrato generale ancorché sub-strutturato, dei quattro tradizionali domini - una dimensione che per Daniel T. Kuehl è rappresentata da

> Un dominio globale all'interno dell'ambiente informatico il cui carattere distintivo e unico è caratterizzato da un uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare, e sfrut-

[33] Interessante il volume di Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World*, nel quale si sottolineava come l'universo open source nel campo della ricerca e acquisizione delle migliori informazioni che possono riguardare la sicurezza di uno Stato o degli asset produttivi sia quello non solo più ricco, ma, scegliendo opportunamente, quello che contiene le informazioni di maggior interesse per la sicurezza fisica ed economica di uno Stato. Cfr. R.D. Steele, *On Intelligence: Spies and Secrecy in an Open World*, AFCEA International Press, Fairfax, 2000.

tare le informazioni attraverso sistemi interdipendenti e interconnessi che utilizzano le tecnologie delle informazioni e delle comunicazioni[34].

Una delle caratteristiche del Quinto Dominio è certamente la sua trasversalità nel condurre azioni aggressive su obiettivi di vario livello di importanza e prescindendo dalla loro collocazione geografica. Mutuando dall'esperienza militare si può dire che la stessa *Information Warfare* (IW) si presenta come una sorta di strumento preliminare alla condotta di un possibile attacco capace di superare ogni confine fisico nel momento in cui si può penetrare l'intimo della governance dello Stato-bersaglio. È evidente che un'operazione di IW ha, sia nel caso di condotta militare che non-militare, lo scopo di definire e sancire la superiorità informazionale per ottenere una posizione di vantaggio tattico/strategico o comunque di *supremacy*.

Un carattere sottolineato da Libicki per il quale l'IW si declina sia in *Command and Control Warfare* (C2W) che come *Intelligence-based Warfare* (IBW). Ovvero, nella condotta di operazioni fondate sull'acquisizione di informazioni utili a conseguire sia obiettivi simultanei che di progettare e/o proteggere i propri sistemi destinati al controllo delle informazioni manipolando quelli avversari; *Electronic Warfare* (EW); *Psychological Warfare* (PSYOP); *Hacker Warfare* (HW); *Economic Information Warfare* (EIW) e guerra cibernetica quale sintesi delle precedenti sono solo alcune delle traduzioni operative circa le possibilità di condotta[35].

In questa prospettiva, il cyberspazio, visto come una «Quinta/o Dimensione/Dominio» della conflittualità, aggiungendosi a quanto lo sono terra, mare, aria e spazio, nel comprendere reti e infrastrutture di informazione e telecomunicazione, dati che le supportano e sistemi informatici, processori e dispositivi di controllo, si presenta come un ambiente che dematerializza la fisicità umana e così fu posto all'attenzione del grande pubblico da Bruce Bethke già nel suo racconto *Cyberpunk* del 1983[36]. Termine, «cyberpunk», che verrà poi riutilizzato anche da William Ford Gibson in *Neuromancer* del 1984 il quale, lo riconduceva all'interno di una

[34] Così Daniel T. Kuehl, *From Cyberspace to Cyber-power: Defining the Problem, in Cyberpower and National Security*, in F.D. Kramer, S.H. Starr, L.K. Wentz, *Cyberpower and National Security, ...*cit. pp. 26-28.

[35] M.T. Libicki, *Operational Cyberwar*. In *Cyberdeterrence and Cyberwar, ...*cit. pp. 139-142.

[36] B. Bethke, *Cyberpunk,* in «Amazing Science Fiction Stories», vol. 57, n.4, November 1983 o W.F. Gibson, *Neuromancer,* Ace, New York, 1984; trad. it. *Neuromante,* Editrice Nord, Milano, 1986.

condizione di allucinazione consensuale o, successivamente, attraverso le recenti nozioni di cyberspazio come regno per la costruzione di comunità virtuali, creando una matrice globale di menti e/o rafforzando i legami spirituali delle persone in tutto il mondo[37].

Minacce e cyberdipendenza

Come ricordavano John Arquilla e David Ronfeldt già nel 1999, vi è ormai una tendenza a vedere il cyberspazio come qualcosa di più che un prodotto della tecnologia[38]. In questo senso, il cyberspazio si presenta come un ambiente nel quale dai settori di produzione, manifatturiero o dei servizi, e oggi anche politico se si guarda alla gestione delle informazioni a supporto delle decisioni, soprattutto nel campo delle ICT si risolvono, in termini di automazione dei processi, fasi di negoziazione, di acquisto o di fornitura attraverso lo scambio di dati tra l'utente e il fornitore, tra il produttore e il consumatore, tra l'erogatore di servizi e il beneficiario, tra pubblica amministrazione e cittadino. La realtà digitale è, quindi, parte di un quotidiano che si svolge attraverso l'uso di *device* ormai sempre più smart e che rappresentano un *digital bridge* tra l'utente e il mondo con il quale esso interagisce a complessità diverse, ma tutte integrate tra di loro (SmartTv, Smartphone/Tablet, Smarthome, Smartcar, Smartwork ecc.).

Se, quindi, uno dei caratteri che contraddistingue il cyberspazio è dato dalla pervasività dei dispositivi e dei sistemi che lo definiscono quale nuovo luogo di relazioni sempre più intime, va da sé che l'ulteriore passo è dotarsi di una definizione anche della minaccia che in tale dimensione può presentarsi. Il concetto stesso di *cyber threat* diventa, quindi, centrale in una nuova coscienza della sicurezza di una comunità organizzata, sia essa politica che economica nelle sue diverse forme. La galassia delle *cyber threats*, infatti, può essere definita come la sommatoria di diversi tipi di minacce: *cyber-crime*, *cyber-terrorism*, *cyber-espionage*, *cyberwar*. D'altra parte, l'insidiosità di una *cyber threat* è rappresentata, sia in termini di cyber-

[37] W.F. Gibson, *Count Zero*, Victor Gollancz Ltd., London, 1986; trad. it. *Giù nel cyberspazio*, Mondadori, Milano, 1990.

[38] *Recognition of the Noosphere*. In J. Arquilla, D.F. Ronfeldt, *The Emergence of Noopolitik: Toward and American Information Strategy*, Rand & Co., National Defense Research Institute, Santa Monica, 1999 pp. 7-26. Vedasi anche *Cyberwar is Coming!* Rand & Co., National Defense Research Institute, Santa Monica, 1993 e, *Looking Ahead: Preparing For Information-Age Conflict*, in *In Athena Camp's: Preparing for Conflict in the Information Age,* Rand & Co. National Defense Research Institute. Santa Monica, 1997 p. 439 e ss.

sicurezza che di *cyberwarfare*, nel superare i limiti spaziali e temporali, permettendo una continua, costante condotta di attacchi localizzabili in ogni altrove rispetto alla comunità-bersaglio. Attacchi, caratterizzati da immediatezza e imprevedibilità e che possono anche sommarsi a condotte di vere e proprie operazioni militari di cui ne definiscono l'ibridazione di un conflitto combattuto sia sul campo di battaglia fisico che nella dimensione digitale. Per questo, una minaccia cyber viene definita, più o meno concordemente, come

> Un'azione concepita, organizzata e condotta per inabilitare i processi o per acquisire dati in maniera fraudolenta per vantaggi illeciti. Ovvero, essa si manifesta attraverso tecniche di aggressione con intrusione e manipolazione dei sistemi digitali di uno Stato o di imprese o assetti pubblici e sociali.

In fondo, ogni azione condotta contro una comunità-bersaglio ogni giorno più dipendente dai processi di digitalizzazione del proprio quotidiano e interdipendente nelle relazioni politiche ed economiche provoca sempre una serie di effetti concatenati, iniziando da quelli che sono diretti e immediati, come l'inibizione di accesso ai servizi più semplici e ricorrenti e proseguendo con effetti più complessi e differenti nel tempo rispetto a quanto prestabilito in fase concettuale. In verità, si può dire, quindi, che nel campo della cybersicurezza si avrà a che fare con dottrine che non sono di per sé stabili, ma particolarmente flessibili; ovvero, capaci di adattarsi in progressione alle condizioni di risposta se si tratta di chi attacca.

Si tratta di condizioni che non hanno limiti di frontiera e se si volge lo sguardo ai cosiddetti Paesi economicamente emergenti, ad esempio, anche il loro essere competitor nell'era cyber sembra dipendere proprio dalle capacità di attacco esprimibili da comunità di *hackers* in luoghi dove si definiscono vere e proprie scuole criminali di *hacking* che riescono a utilizzare ogni *hack* disponibile in rete, formati se non sostenuti attraverso tutorial e/o tutor finanziati da associazioni criminali se non terroristiche[39]. Se a questo si aggiunge che anche formule sempre più innovative ritenute più sicure come quelle riconosciute come Air gap, ovvero che permettono di aumentare il livello di sicurezza di una LAN evitando qualunque tipo di contatto con

[39] «ZeroFox», ad esempio, ha rilevato una minaccia condotta da cybercriminali nigeriani che sfruttando le funzionalità di messaggistica multipiattaforma integrate in Facebook e Messenger, hanno dato luogo a un'attività di truffa manipolando i sistemi di messaggistica diretta. Vedasi: https://www.zerofox.com/blog/cross-platform-messaging-social-media-scam/.

Internet siano di fatto vulnerabili, si comprende di come l'evoluzione della minaccia sposta il rischio in avanti riducendo i confini della stessa definizione di *cyberwarfare*, ovvero non riconducendola solo sul piano militare[40].

Ecco, perché, l'idea di fondo è che il differenziale strategico in fase di condotta difensiva risiederà tutto nella rapidità dell'adattamento tattico alle condizioni di aggressione che dovranno essere, per questo, determinate in progressione per dare la possibilità che l'obiettivo ultimo di un attacco cyber non si realizzi: cioè, la paralisi dell'avversario e la conquista del dominio del quotidiano altrui.

Lo stesso abbattimento della dimensione spazio-temporale e l'accesso sempre più diffuso perché quotidianamente necessario all'*Information Technology* più semplice e più redditizia, nel consentire il dialogo a distanza e l'azione, per certi versi, ha determinato non solo una rivoluzione modificando e aprendo a nuovi schemi comportamentali l'individuo, ma ha riorganizzato in relazione all'impatto esponenziale della tecnologia digitale anche i rapporti di forza.

Rapporti non più necessariamente rappresentati dalla capacità di conquistare fisicamente uno spazio, di qualunque natura esso sia, quanto di dominarlo, gestirlo se non di governarlo secondo gli interessi dell'attore che aggredisce una comunità-bersaglio. Da ciò ne deriva che tre sono sicuramente i caratteri che contraddistinguono, e rendono particolarmente insidiosa, una minaccia cyber alla sicurezza di una comunità organizzata: la particolare capacità di abbattere ogni limite temporale e spaziale nel suo definirsi; il fare dell'imprevedibilità il fattore di potenza principale; il considerare l'ubiquità un elemento critico per il contrasto a una minaccia cyber.

Questo, perché, il cyberspazio è in sé uno spazio di rischio dematerializzato ma non de-intimizzato: tutt'altro. Esso si esprime attraverso una umanizzazione dello spazio digitale considerato che la popolazione social è ormai aumentata a tal punto da creare un universo informazionale e re-

[40] I pirati informatici sono ormai in grado di realizzare sistemi sempre più capaci di penetrare architetture di sicurezza anche con dispositivi semplici. Infatti, se sino a ieri era necessario introdursi quanto meno nella struttura che ospitava la rete «air gap», oggi è possibile hackerare anche a distanza sfruttando rilevatori di calore, antenne per gli ultrasuoni o per le onde radio e addirittura dei droni. L'uso dei droni si è rivelato funzionale a condurre attacchi soprattutto da parte dei cosiddetti «droni jacking». Droni, questi, capaci di condurre un attacco informatico il cui scopo è quello di prendere il controllo del dispositivo della vittima esprimendo una maggior letalità rispetto a un comune *malware*, penetrando all'interno degli stessi processi produttivi e definendo, in questo modo, e in maniera ottimale, una vera e propria attività di *cyber-espionage*.

lazionale parallelo a quello della realtà fisica dove piattaforme come Facebook, Instagram, Linkedin o dell'e-commerce come E-bay, Amazon e simili dimostrano quanto la sfida geopolitica si sia spostata sulla capacità di raggiungere, e assicurarsi nel tempo, una *digital supremacy* che potrà essere solo governata, ma non più evitata se non subita.

Lo stesso sistema internazionale, al di là della sua configurazione tradizionale come luogo in cui si confrontano gli Stati nazione, si presenta come una sorta di campo gravitazionale nel quale si sviluppano, si sommano o si sovrappongono relazioni sociali, politiche ed economiche tra le unità politiche che lo compongono non più necessariamente formali, ovvero necessariamente istituzionalizzate. In questo senso, il sistema internazionale può essere considerato, nuovamente, come una sorta di campo di forza competitivo, dinamico, non statico, alla ricerca di un ordine, se non di un equilibrio, definito dal ruolo e dalle capacità che il progresso tecnologico offre a ogni singola parte organizzata, politicamente ed economicamente. Un campo di forza nel quale esercitare una propria azione sia essa rivolta a garantirsi la sopravvivenza fisica, quindi politica, che economica o a esercitare, in questa prospettiva, e in ragione di interessi definiti e ritenuti vitali, condizioni di egemonia a risorse e capacità date. Capacità valutate secondo le seguenti categorie: strategia e dottrina; governance, comando e controllo; capacità fondamentali di cyber-intelligence; potenziamento e dipendenza informatica; sicurezza informatica e resilienza; leadership globale negli affari del cyberspazio; capacità informatica offensiva.

È evidente, quindi, che in questa prospettiva, il sistema internazionale determina anche l'*habitus* degli attori poiché se cambia il campo di forza, l'ambiente competitivo e le regole stesse della competizione, muta anche l'*habitus* dei protagonisti. Tutto questo perché il «campo del confronto», accettando la definizione di Pierre Bourdieu, rappresenta quella sfera del vivere sociale internazionale che si qualifica attraverso proprie regole creando un network di relazioni tra Stati e individui, che non necessariamente occupano uguali posizioni o sono portatori di altrettanto condivisi interessi[41]. Le dimensioni di un soggetto politico, ad esempio, non sono più considerate prerogativa di forza, ma solo una condizione quantitativa - e non necessariamente solo economica o anche militare - almeno in termini di gestione di una posizione di egemonia dal momento, e nel campo

[41] P. Bourdieu, *Capitale simbolico e classi sociali*, «Polis», n. 3-2012.

della IA ciò farà tutta la differenza del caso, che sarà sempre più valido il *first mover advantage*[42].

Ecco perché, dal vertice di Ginevra del 2003 sino a quello di Tunisi del 16 ottobre 2005 a oggi non vi sono dubbi che molti passaggi sono stati fatti, anche se lentamente, per trovare una soluzione comune tra gli Stati circa una governance internazionale del Web che superi e tenga conto del nuovo ambiente creatosi nel campo di forza degli Stati tecnologicamente più competitivi, quasi come si trattasse di un sistema parallelo di relazioni nelle quali n-attori si muovono secondo schemi e interessi che aggregano, o dividono o che riaggregano volta per volta, quasi a suggellare uno spazio a più strati. Tuttavia, resta un dato di fatto che ancora oggi la governance di Internet sia una sorta di tabù nonostante si tratterebbe di riprendere quel confronto che vorrebbe affidare alle Nazioni Unite il controllo internazionale della Rete sottraendone il monopolio agli Stati Uniti, o favorendo il consolidarsi di una cooperazione intergovernativa e una volontà degli Stati di garantire non solo un libero accesso, ma di eliminare gli ostacoli di censura politica.

Ciononostante, numeri e analisi si moltiplicano e demoltiplicano nelle diverse fasi delle relazioni politiche o nelle contrattazioni economiche e pongono la qualità della *cyber-intelligence* come una capacità strategica necessaria per valutare tendenze o affinare e raffinare dati considerati fondamentali per poter condurre politiche, o azioni, rivolte a garantire competitività in un caso o sicurezza nell'altro. Lo stesso controllo dei *data-mining* e l'elaborazione in tempi rapidi delle informazioni sottese per ricondurle all'interno di un quadro coerente non è più solo un lusso, ma una necessità. D'altra parte, come si ricorda nella comunità digitale, i dati non sono mai muti se si sa porre loro le domande giuste. Una considerazione fondamentale se non, si potrebbe affermare, un paradigma alla base delle ragioni algoritmiche di gestione dei big data e, soprattutto, la ragione se non la consapevolezza del sé di una Intelligenza Artificiale.

[42] «First mover advantage» (vantaggio della prima mossa). Si riferisce al vantaggio di cui gode una impresa come conseguenza del suo ingresso anticipato in un nuovo mercato. Sebbene il termine suggerisca che un ingresso anticipato sia auspicabile, i vantaggi di aprire la strada a un nuovo mercato sono spesso controbilanciati da svantaggi. La questione se sia probabile un «vantaggio della prima mossa» in un qualsiasi contesto specifico dipende dalle caratteristiche del mercato emergente e dell'impresa che entra. Da M. Augier, D.J. Teece (eds), *Palgrave Encyclopedia of Strategic Management,* Palgrave-MacMillan, London, 2018.

Insomma, è evidente che la qualità delle capacità algoritmiche già definite nell'universo cyber, prim'ancora che all'interno di un modello di IA, è tutta riconducibile alla possibilità di trovare quelle correlazioni tra dati diversi poiché provenienti da fonti altrettanto diverse. *Data-mining* e *knowledge extraction* rappresentano due modi necessari per poter non solo disporre di nuove conoscenze aggregando dati ma, soprattutto, di scegliere azioni e politiche più adeguate per condizionare i comportamenti degli individui attraverso operazioni di *profiling* mutuate dal modello economico e trasferibili anche sul piano della condotta di attività di *cyberwarfare*.

La Rete è divenuta, quindi, una nuova mappa che cambia continuamente anche le dimensioni degli interessi e altrettanto richiede nuove forme di lettura poiché essa è un'estensione necessaria dell'esistenza di interi sistemi, inserendosi in forme e con conseguenze diverse nella vita materiale di ciascun soggetto politico-sociale, sia esso organizzato in comunità o semplice individuo. Se questo è il risultato della nuova configurazione di un sistema di governance sempre più orizzontale piuttosto che verticale, assenza di geo-specificità e difficoltà di individuazione dell'origine e provenienza della minaccia, dimostrano quanto un'aggressione cyber possa essere la migliore forma per piegare a costi contenuti la volontà dell'avversario al di là delle sue dimensioni fisiche.

Difficilmente identificabile e chiaramente riconducibile a soggetti criminali specifici, a matrici politico-ideologiche o a Stati e a organizzazioni politiche istituzionalizzate o, ancora, a forme ibride che mettono insieme più combinazioni tra quelle indicate, la sicurezza si risolve nella necessità di riuscire a disporre di modelli di previsione, di governo del rischio o, meglio, dell'imprevisto valutato, quest'ultimo, nella sua immanenza e nella sua capacità di modificare in tempi rapidi ogni certezza, ogni abitudine. In fondo, ogni forma di autorità si poggia su una idea di governo originaria che riguarda non solo l'autorità in quanto tale, se così riconosciuta perché imposta attraverso regole condivise o dalla forza, ma anche su quella accettata inconsapevolmente magari manipolando le coscienze e ridefinendo i caratteri del consenso.

L'*habitus* non fa il monaco? Vulnerabilità e conquista dell'intimo digitale

La rivoluzione cyber ha modificato molti assunti. Ad esempio, è estremamente fuorviante poter credere che un mondo socialmente organizza-

to possa ancora essere rappresentato da un universo di presupposizioni, cioè scontato per coloro che vi appartengono o investito di valore per chi ne vuol far parte. La possibilità di introdursi nell'intimo delle coscienze e la volontà di porre in essere modalità e termini di governo del consenso rende la minaccia cyber quella potenzialmente più adatta a superare ogni barriera creata a garantire una sorta di fidelizzazione nel tempo a un governo, a una leadership. Certo, la possibilità di difendersi di fronte a una minaccia che si articola nell'uso dell'IT non è certo semplice.

Ma la *policy* alla base di ogni possibile strategia di difesa dovrebbe essere quella di realizzare una sorta di sintesi tra oggettivismo e soggettivismo; ovvero, tra strutture a difesa e azioni possibili. In fondo, uno degli obiettivi di una minaccia cyber nell'uso delle IT in una condotta di IW è certamente quello di modificare, nel breve periodo o anche nel medio-lungo termine, in ragione degli obiettivi che chi aggredisce si prefigge, proprio l'*habitus* della comunità bersaglio. Quell'*habitus* interpretato come l'insieme di predisposizioni, schemi di pensiero e comportamentali, frutto di condizionamenti sociali, che definisce, mediandole quando possibile, le scelte dei singoli individui e, in termini geopolitici, quelli degli Stati.

Prodotto della storia, l'*habitus* è anche un «produttore di storia» visto che genera pratiche individuali e collettive conformemente agli schemi generali della storia. Bourdieu, infatti, inquadra l'*habitus* all'interno di una prospettiva costruttivista visto che l'*habitus* è il prodotto di determinate strutture sociali che possono essere rafforzate o trasformate una volta che gli individui e gli Stati definiscono le loro scelte in termini di interessi[43]. Se si volesse definire anche il nuovo mondo della digitalizzazione della quotidianità, si potrebbe anche attribuire ai nuovi processi relazionali una sorta di dimensione egotica che supera il passaggio dall'*homo rudens* all'*homo faber* per giungere a una versione ridisegnata in termini di capacità di osservazione, apprendimento e di azione mediata da nuove categorie attraverso e all'interno delle quali esprimere una nuova umanità nelle sue diverse relazioni, culturali, politiche o economiche che siano. Dalle comunità di destino alle comunità creative, alla possibilità di potersi esercitare anche in abilità predittive, magari potendo contare su intelligenze collettive cooperative e su nuove opportunità offerte dai computer quantistici, il segno del tempo sembra quello di voler far diventare l'uomo una periferia di una macchina.

[43] P. Bourdieu, *Capitale simbolico e classi sociali* ...cit.

Se si osserva la realtà dei videogiochi, ad esempio, diventa difficile comprendere se è l'uomo la periferia del gioco o il contrario, se è la consolle la periferia attraverso la quale l'uomo interpreta se stesso e agisce in un mondo che spesso segue la realtà alla ricerca di uno *stargate* per giungere a una ulteriore nuova *gateland*. Ma fermandosi al *cyberland*, di certo non si può non considerare che anche i processi che connettono i quotidiani di ogni individuo si trasformano, nel frattempo, in potenziali portali, piccole vie di accesso a informazioni che, come si vedrà, nell'Internet of Things (IoT) o «Internet delle cose», come la domotica, maturano nell'intimo di ogni utente finale.

Infatti, le vulnerabilità - intese come mal funzionamenti, configurazioni sbagliate o semplicemente errori presenti in un sistema che lo espongono a dei rischi - vengono considerate come specie di «piccole crepe» che un attore utilizza per infiltrarsi; spesso esistono proprio nei dispositivi e sistemi IoT che sono al di fuori dal controllo informatico o delle procedure di sicurezza sottraendosi, in questo modo, a ogni possibile monitoraggio e diventano ottime superfici di attacco. Cioè, creazione di uno spazio che gli attori della minaccia possono utilizzare per le loro azioni offensive[44]. In questo senso, ci sono due modalità di azione riferite a due diverse esigenze di intervento. La prima, che vede la richiesta di individuare quali siano le possibilità di violare un sistema IT cercando di comprendere sino a quale punto una minaccia possa comprometterne il funzionamento (*Penetration test*, cioè simulazione di un attacco hacker). Il secondo, è cercare di individuare quali e quante possibilità di violare un sistema/architettura IT vi possono essere a condizioni date, con una valutazione delle possibilità di rischio e delle capacità di resilienza e di risposta (*vulnerability assessment*).

Due modalità, le precedenti, che dimostrano quanto la resilienza informatica equivalga alla resilienza amministrativa o aziendale ed è evidente quanto in ogni settore della vita quotidiana tutto questo possa interessare una dimensione pubblica piuttosto che privata. Ecco, perché, un accordo

[44] In genere si definiscono tre tipi di vulnerabilità informatiche. La prima, rappresentata dalla vulnerabilità di un software, chiamata anche «bug software». Si tratta di cattivi funzionamenti o di errori di *script* del software che possono presentarsi all'interno di un codice, in una configurazione o determinarsi anche nel processo di installazione. Un software malfunzionante può dare corso sia a un'azione diretta verso l'esterno che verso l'interno presentando una vulnerabilità. La seconda, è la vulnerabilità dei protocolli. Cioè, di possibili spazi non definiti in termini di sicurezza e relativi alle procedure di comunicazione tra le tecnologie che sono presenti e definiscono l'architettura del sistema informatico. Vi è poi la terza, ovvero la vulnerabilità hardware. In questo caso, si tratta di un pericolo che deriva dal malfunzionamento di ogni parte del sistema.

generale per garantire i servizi e limitare i danni non può non imporre comportamenti adeguati nell'uso quanto individuare responsabilità verso i produttori e i fornitori di supporti cyber determinando poche eccezioni di diligenza. D'altronde, non esistendo un «rischio zero», la sicurezza digitale ha un suo costo visto che negli ultimi anni, al di là dei diversi rapporti sul tema, come il «Rapporto Clusit» del 2023, si osserva come dal 2018, per gli attacchi rilevati tra il primo semestre 2018 e il primo semestre 2023 la crescita è stata dell'86% (745 a 1.382) con una media mensile di attacchi definiti gravi passata da 124 a 230 tenuto conto che il Rapporto considera solo gli attacchi che hanno non solo determinato dei danni ma che sono noti; ovvero, con un impatto sistemico in diversi aspetti della società, della politica, dell'economia e della geopolitica[45]. L'aumento degli attacchi informatici rispetto al passato ha dimostrato un certo mantenimento della tendenza a una sorta di spostamento in avanti delle capacità criminali di ridefinire azioni e nuovi profili di illecito avvicinando realtà criminali diverse, ma accomunate da medesimi disegni criminosi.

Inoltre, il conflitto russo-ucraino ha dimostrato come non esistano elementi di discontinuità nella necessità di definire strategie di sicurezza considerato che l'attacco alle infrastrutture di governance digitali rappresenta una minaccia definita in sé, e non solo per tipologia e soggetto che aggredisce. Strategie, che dovrebbero mirare a mutuare processi e procedure tipiche della condotta difensiva e che oggi ricorrono anche a cosiddetti *honeypot* (vasi di miele) quali sistemi informatici esca, capaci, cioè, di rendere un obiettivo attraente per le operazioni di guerra informatica o per condotte criminali[46].

[45] In particolare, e circa la crisi russo-ucraina, per gli autori del Rapporto sin dal 2022 «Il conflitto tra Russia e Ucraina ha messo in campo strumenti cyber-offensivi altamente sofisticati a supporto di attività di *cyber-intelligence* e di *cyber-warfare*». Ciò farebbe ritenere che «questo processo sia difficilmente reversibile e che in prospettiva potrebbe causare conseguenze di inaudita gravità, ponendo l'Italia e l'Europa sulla soglia di una guerra cibernetica globale». Il Rapporto del 2023 è consultabile/disponibile su file:///C:/Users/Admin/Downloads/Rapporto_Clusit_aggiornamento_10-2023_web.pdf

[46] «Honeypot», letteralmente «vaso o barattolo di miele». Si tratta di un hardware o di un software adibito il primo, e creato il secondo, a prestarsi come esca per proteggere una rete da attacchi esterni. In genere si tratta di un PC o di un sito o di un indirizzo IP che apparentemente è parte della Rete e, altrettanto apparentemente, sembra disporre e/o processare informazioni appetibili per un attacco hacker ma che, al contrario, è isolato dalla Rete stessa. Lo scopo di un *honeypot* non è solo quello di attirare gli attacchi deviandone il corso dalla Rete principale, ma anche quello di dare dati utili circa la natura e la frequenza degli attacchi subiti. L'unico, e non poco importante, rischio è rappresentato dalla possibilità che essi possano condurre a ingressi non protetti ma connessi con la Rete principale.

La stessa Unione europea, dei prossimi anni, trovandosi al centro della nuova competizione mondiale per la supremazia tecnologica dovrà fare i conti con scenari di guerra cibernetica globale, poiché più di un terzo degli attacchi ha impatto critico e più di un quarto colpisce il continente europeo. Attacchi che sono aumentati non solo quantitativamente e qualitativamente, ma sono condotti indiscriminatamente dal momento che l'aumento si definisce all'interno dei cosiddetti *multiple targets*; ovvero, nel colpire obiettivi non più specifici ma differenziati considerando, ovviamente, l'interdipendenza di governance informatica che soprassiede a ogni singola utility o a ogni singola gestione di commodity[47]. La crisi russo-ucraina, al di là delle operazioni militari sul terreno, gioca un ruolo fondamentale nel presentarsi come una sorta di banco di prova di uso di strumenti e capacità *cyber-offensive*, sommati alla condotta delle operazioni tradizionali con una sempre maggiore centralità attribuita alle attività di *cyber-intelligence*, *cyber-espionage* e di *cyberwarfare*.

Una crisi che pone, semmai ve ne fosse necessità, quanto e in che misura il ricorso alle capacità cyber per influenzarne la condotta di operazioni sul campo, come per condizionarne l'andamento di una crisi in senso lato, sia ormai da considerarsi un processo non reversibile tenuto conto dell'alto livello di interdipendenza raggiunto attraverso la digitalizzazione non solo dei processi produttivi e di governance, ma del quotidiano in sé.

Alcune minacce che vanno per la maggiore

È evidente, quindi, che le infrastrutture critiche e i sistemi digitali che ne governano i processi diventeranno sempre di più i bersagli preferiti e meno costosi da raggiungere in caso di attacco informatico condotto da attori governativi e non solo. Gli stessi cybercriminali non colpiscono più in maniera indifferenziata e indiscriminata obiettivi multipli, ma indirizzano la loro azione a target ben definiti tra obiettivi governativi/militari, obiettivi informatici, banche, sanità, istruzione e trasporti.

D'altra parte, se la dimensione cyber si caratterizza per essere uno spazio dove le regole sono fissate da regolarità logiche algoritmicamente definite, è evidente che il non riscontrare per tempo una determinata regolarità significa fare i conti con l'indeterminatezza di una possibile condot-

[47] «Utility»: società normalmente quotate in borsa che erogano/forniscono servizi di pubblica utilità come energia, acqua, telecomunicazioni, ecc. «Commodity»: materie prime, la cui offerta sul mercato non presenta differenze qualitative.

ta che di fatto può sottendere una volontà aggressiva con serie difficoltà per chi si appresta a difesa nell'approntare risposte adeguate all'attacco in corso. Questo fa sì che diversi software possono essere armi riconoscibili non solo nelle modalità di processo, ma negli scopi di condotta come veri e propri sistemi d'arma (*cyberweapon*)[48].

Tra le minacce più diffuse i *malware* come Flame, Mirai, Wiper, gli *spyware* come Pegasus, utilizzato spesso non solo per catturare dei criminali, ma anche per silenziare attivisti, giornalisti e dissidenti politici. Quest'ultimo, nato come arma digitale in favore delle forze dell'ordine, è stato utilizzato in modo tale da violare i diritti umani e attualmente è compreso nella lista nera dei software non ammissibili negli Stati Uniti proprio per la caratteristica di consentire la violazione della privacy di un individuo. E cosa dire del più famoso Stuxnet? Un *malware selettivo*, ma anche un *worm* capace di autoreplicarsi all'interno di una rete il cui primo riconosciuto uso viene riferito all'attacco condotto nel 2010 alla centrale nucleare di Natanz, in Iran che disabilitò le turbine. Un *malware*, Stuxnet, considerato come una delle prime manifestazioni di *cyberwarfare* cui ricorsero asseritamente gli Stati Uniti e Israele conto l'Iran[49]. Ma anche Great Cannon, un *denial-of-service* lanciato su siti web il cui scopo è quello di condurre un attacco *man-in-the-middle* (uomo nel mezzo) dove si trasmette una comunicazione manipolata da terzi senza che ciò emerga lasciando alle parti la certezza della genuinità della sorgente. E, poi, Acidrain, un *malware wiper* capace di mettere in crisi la catena di approvvigionamento più significativa e che si è affidato a Viasat sia nella gestione degli impianti energetici che dei servizi di comunicazione europei. A questi si aggiunge, ma solo a titolo esempli-

[48] N. Ebner, *Cyber Space, Cyber Attack and Cyber Weapons. A Contribution to the Terminology*. IFSH – Institute for Peace Research and Security Policy at the University of Hamburg, October 2015 pp. 1-10.

[49] Si trattò di un'operazione condotta contro una centrale nucleare iraniana attraverso l'uso di un *malware* capace di selezionare solo sistemi con determinate caratteristiche e funzioni con lo scopo di creare danni di inibizione delle attività del sistema attaccato, ma non pregiudicando altre parti dell'architettura. Fu condotto utilizzando una chiavetta contenente il *malware*, per cui pur con un semplice ingresso in uno dei computer della centrale l'obiettivo sarebbe stato conseguito. Nel caso specifico, la completa inibizione del funzionamento delle turbine della centrale e, quindi, il rallentamento del programma nucleare di Teheran. A scoprire l'attacco e il *malware* fu Sergey Ulasen. Cfr. *The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight*. Così in https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/. Vedasi anche *A cyber-missile aimed at Iran?*, in «The Economist», September 24, 2010. Consultabile in https://www.economist.com/babbage/2010/09/24/a-cyber-missile-aimed-at-iran-.

ficativo, un *malware* distruttivo chiamato WhisperGate fatto penetrare nei sistemi di diverse organizzazioni governative, no profit e dello spazio dell'Information Technology, che ha aperto la strada a nuove forme di violazione di spazi fisici dettati non solo dalla persona ma dalla fisicità dei dati e dei servizi a essa collegati. Un *malware* che si comporta da *ransomware* ma senza avere le caratteristiche del riscatto di ritorno, poiché l'accesso ai dati viene reso definitivamente indisponibile.

Così come, per citare uno dei casi più interessanti ormai di spostamento sul piano digitale del confronto, nel giugno 2017 il servizio di intelligence militare russo, il GRU, sembrò lanciare una delle ormai periodiche operazioni di attacco informatico a infrastrutture di comunicazione e non solo di Kiev. L'attacco, denominato NotPeya non andò in porto ma, nello stesso tempo, spostò il suo campo di attacco per protocolli digitali simili su un fronte completamente diverso colpendo le capacità di funzionamento di alcune società occidentali e non solo, causando danni per 10 miliardi di dollari. Maersk, ad esempio, non riuscì a condurre le proprie attività di trasporto marittimo, mentre Merck, società farmaceutica, avrebbe vinto una causa di risarcimento assicurativo nel gennaio 2022 per 1,4 miliardi di dollari per coprire le perdite dovute all'attacco di NotPetya[50]. Tutto questo, ha dimostrato come un attacco cyber non sempre segue calcoli predefiniti ma potrebbe, in virtù del riconoscimento di protocolli simili, mutare l'obiettivo di attacco. In questo senso, infatti, NotPeya si è diffuso attraverso le reti di distribuzione globali[51]. O, anche Wannacry (o WanaCrypt0r 2.0), un *worm* autoreplicante, versione *malware* del *troyan* Cryptolocker del 2013, che ha operato come un *ransomware* e che ha criptato i file presenti su PC che utilizzavano il sistema operativo Microsoft-Windo-

[50] Non bisogna dimenticare, a tal proposito, che quasi il 90% del commercio mondiale si svolge lungo le rotte marittime. Ogni attività di hackeraggio condotta sui sistemi di gestione delle rotte tramite GPS e sulle comunicazioni digitali tra navi e compagnie può dare luogo a danni rilevanti se non distruggere asset societari ben definiti. Come ricorda «Kaspersky», forzando le chiavi dei terminali dei container, i criminali possono portare al crollo del ciclo degli approvvigionamenti nazionali o regionali di un determinato paese, sia di merci che di energia. Cfr. https://www.kaspersky.it/blog/maritime-cyber-security/6098/.

[51] A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world,* in «Wired» August 22, 2018. Così in https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Cfr. anche: *Cyber Capabilities and National Power: A Net Assessment*, The International Institute for Strategic Studies, London, 2019 p.1 e ss.

ws nell'autunno del 2017, subordinando la decrittazione al pagamento di un riscatto in bitcoin da parte degli utenti colpiti. Un attacco al più noto sistema operativo attribuito verosimilmente a hacker riconducibili alla Corea del Nord[52].

Il salto di qualità. Le APT

Se ci si sposta sul campo delle cosiddette «Advanced Persistent Threat» (ATP), "minacce persistenti avanzate" si potrà notare come una minaccia concreta rappresentata da avversari che presentano un livello di alta qualità e capacità tecnica sia un ulteriore anello nel definire una condotta di attacco su più scenari. Le APT possono rappresentare non solo organizzazioni strutturate, ma anche Stati sovrani che affidano a tali comunità, precostituite informalmente o anche istituzionalizzate, il compito di condurre attacchi anche su larga scala e nel tempo con più vettori, sugli asset sensibili, economici o anche militari, verso le comunità-bersaglio. Attacchi condotti su obiettivi specifici, silenziosamente, e prolungati nel tempo ricorrendo a *malware*, *tools* offensivi e altro. Lo stesso acronimo, APT, può essere meglio precisato proprio nei termini di identificazione. Una «minaccia avanzata» è tale perché essa esprime competenze elevate, dispone di risorse tecnologiche ed economiche importanti e può ricorrere non solo a software liberi ma anche autoprodotti e, per questo, più complessi da individuare e contrastare[53].

Per raccogliere informazioni sui propri obiettivi una APT potrebbe servirsi di *tool*, ovvero di *utility* destinate a interagire con l'utente e anche installabili in default come applicativi, utilizzate per l'analisi, la configurazione, l'ottimizzazione e/o la manutenzione del computer. Le operazioni condotte da gruppi APT indicano che gli attacchi al settore finanziario sono

[52] Un attacco al più noto sistema operativo attribuito verosimilmente a hacker riconducibili alla Corea del Nord. Cfr. *Offensiva hacker su scala mondiale: PC in ostaggio in 150 Paesi*. Cfr. www.corrierecomunicazioni.it, 19 dicembre 2017.

[53] Interessante il documento denominato *Apt1 Exposing One of China's Cyber* realizzato da Mandiant Intelligence Center per il quale Apt1 era definita una campagna pluriennale di spionaggio informatico condotta su scala aziendale. Per Mandiant, Apt1 rappresentava allora uno dei più prolifici in termini di quantità di informazioni rubate, quindi uno dei più attivi nel settore delle «Espionage Units». Per il Report vi erano prove incontrovertibili che collegavano APT1 al 3° dipartimento del dipartimento di stato maggiore generale (GSD) del 2° ufficio dell'Esercito popolare di liberazione (PLA) cinese. In particolare, Apt1 si configurava con oltre 40 famiglie di *malware* APT1. Il Report è consultabile in: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf?_gl=1*1agmtit*_up*MQ..*_ga*MTY2NzA1ODEyMS4xNjk3MjY2NTYz*_ga_X6642ZTDJ7*MTY5NzI2NjU2My4xLjAuMTY5NzI2NjU2My4wLjAuMA.

spesso motivati dallo spionaggio ed è per questo che la loro funzione è eseguire l'impostazione e/o il monitoraggio o altre operazioni amministrative di dispositivi, sistemi operativi, hardware o altri software dedicati. D'altronde, una APT è «persistente» perché, al di là dei vantaggi immediati che non sono lo scopo, l'obiettivo è quello di essere presente nei sistemi attaccati il tempo necessario per poter acquisire il maggior numero di informazioni ritenute utili per condurre a buon fine l'operazione e/o per massimizzare il risultato predefinito e/o imporre il maggior danno possibile alla comunità/istituzione o sistema-bersaglio[54].

Le APT sono sempre caratterizzate da un'ampia mutevolezza, sono controllate da remoto da soggetti fisici la cui capacità di sfuggire ai tentativi di difesa risiede nell'adottare le migliori soluzioni per rendere complessa la loro attività o nella dissimulazione stessa nell'attacco condotto. Il contrasto a tali minacce risiede, pertanto, nel disporre di sistemi di scoperta; cioè, di individuazione del pericolo, del tipo e della provenienza. Per guadagnare tempo nel tentativo di identificarne proprio la provenienza, si può ricorrere a una distribuzione in remoto di team incaricati della scoperta e della risposta frammentando, in questo modo, le capacità di attacco. Anche effettuare delle contro-ricognizioni diventa necessario per vincere un confronto con una APT.

D'altronde, in questo ambito non si ha a che fare con semplici operazioni di hackeraggio, ma con attacchi strutturati condotti da avversari più avanzati che, come visto, possono far capo a Stati nazionali o a gruppi terroristici con livelli di competenza e risorse altamente sofisticati che cercano di stabilire punti d'appoggio permanenti nelle infrastrutture digitali delle istituzioni avversarie. Tra i più prolifici e avanzati si è distinto Apt28, noto anche come Sofacy; cioè, un gruppo organizzato probabilmente sotto egida russa che ha condotto attacchi cyber progressivi contro obiettivi militari e istituzionali con capacità di sfruttare al meglio gli «Zero-day»[55];

[54] Cfr. National Institute of Standards and Technology, *Managing Information Security Risk Organization, Mission, and Information System View. Information Security*, US-Department of Commerce, 2011 p.16 e ss.

[55] Per «Zero-day», si intende una vulnerabilità di sicurezza che non è nota allo sviluppatore o al produttore di un software. Uno Zero-day può individuare anche un particolare programma, chiamato *exploit* che usa le vulnerabilità non note al fine di eseguire anche solo parzialmente azioni che normalmente non sarebbero permesse dal software. La definizione di Zero-day è così attribuita dal momento che sono passati zero-giorni da quando la vulnerabilità è nota allo sviluppatore che ha avuto, a sua volta, zero-giorni per provvedere a definire una possibile patch. In genere si fa riferimento a «vulnerabilità Zero-day» allorquando un cracker prova a individuarle per ottenere un accesso abusivo al sistema informatico o provocare danni o perdite di dati.

in altre parole, sostituendo in tempi ristretti i *malware* scoperti con nuovi *malware*[56].

Remediation & Recovery

Gli attacchi rappresentano ormai un universo-mondo che si manifesta su piattaforme che si sovrappongono se non si interfacciano tra di loro. Si pensi a *SymStealer*, un *malware* realizzato per sfruttare una ben

[56] Se si volesse fare un elenco delle possibilità di software a difesa si possono elencare i seguenti; *Bloodhound*, uno strumento di intelligence sulla rete, che viene utilizzato per mappare e visualizzare le relazioni tra gli account e i computer. Uno strumento di analisi delle relazioni che visualizza graficamente le relazioni di privilegio all'interno di una rete. Oppure *Burp Suite*, un set di strumenti per il *testing* della sicurezza delle applicazioni web, che include uno scanner di vulnerabilità, un *proxy* per il traffico web e uno strumento per l'intrusione manuale. Si può aggiungere *Cobalt Strike,* quale piattaforma di test delle vulnerabilità e di simulazione degli attacchi, spesso utilizzata per il *Penetration testing* e per l'addestramento delle squadre di sicurezza informatica o, anche *Core Impact*. Quest'ultimo è un framework di *Penetration testing* che aiuta a identificare, valutare e gestire le vulnerabilità della rete e delle applicazioni. Vi è poi *Covenant*, altro framework di post-exploitation, C2 (Command-and-Control), che fornisce funzionalità di gestione remota per l'esecuzione di comandi su macchine compromesse; *Crackmapexec*, strumento di *Penetration testing* che automatizza la scansione e l'esecuzione di attacchi contro le reti Windows; *Impacket*, cioè una collezione di strumenti *Python* per l'interazione di rete, inclusa la manipolazione di pacchetti di rete e la gestione di protocolli di rete; *PowerShell Empire*, framework di post-exploitation che consente di mantenere l'accesso a un sistema compromesso, automatizzando alcune attività di gestione e controllo e che utilizza *PowerShell* per eseguire attività di persistenza e controllo su una macchina compromessa; *Male-winrm*, script di *PowerShell*, che facilita l'accesso remoto a una macchina Windows tramite WinRM (Windows Remote Management); *Metasploit Pro*, noto framework anche questo di *Penetration testing* che offre una vasta gamma di strumenti per individuare, sfruttare e convalidare le vulnerabilità di un sistema; *Mimikatz*, un *tool* per il recupero di password e l'esecuzione di attacchi basati su *pass-the-hash*, *pass-the-ticket* e *mimikatz*; *Powerview,* strumento di raccolta di informazioni all'interno di un dominio Active Directory utilizzando *PowerShell*; *PrintSpoofer,* che sfrutta una vulnerabilità di Windows per ottenere privilegi di sistema utilizzando il servizio di stampa; *Responder*, uno strumento che sfrutta le vulnerabilità nei protocolli di autenticazione di rete per ottenere le credenziali degli utenti; *Rubeus*, *tool* di hacking basato su *Kerberos* che consente di eseguire attacchi di *pass-the-ticket* e di gestire i token di accesso; *SharpHound,* modulo di *BloodHound* scritto nel codice sorgente C# che raccoglie informazioni sul dominio per l'analisi delle relazioni; *SQLmap* è uno strumento specializzato per il *Penetration testing* di applicazioni web che utilizzano database SQL, aiutando a individuare e sfruttare le vulnerabilità riferite alle query SQL -«Structured Query Language». I comandi SQL non sono altro che istruzioni utilizzate per comunicare con un database al fine di eseguire attività, funzioni e query con dei dati. I comandi di SQL possono essere utilizzati per cercare nel database e per svolgere altre funzioni come creare o eliminare tabelle, e aggiungere o modificare dati.

precisa e riconosciuta vulnerabilità su Google Chrome (definita come CVE- Common Vulnerabilities and Exposures-2022-3656) che ha visto come vittime circa 2,5 miliardi di utenti di Google Chrome e/o di browser su Chromium, versione *open source* del più noto browser, che ha permesso il furto di file sensibili, come portafogli crittografici e credenziali del provider di servizi cloud attraverso collegamenti simbolici con i quali creare nuovi siti web e nuove chiavi crittografiche come se si trattasse di un rispristino del sito originario. Come si comprende, una delle sfide principali di questi e dei prossimi anni è quella di pensare che la tecnologia non risolverà sempre tutto.

Affidarsi, infatti, solo alle capacità di risposta di sistemi tecnologici, per quanto avanzati essi possono e potranno essere, escludendo l'intervento umano esporrebbe più di quanto non si possa pensare a rischi di attacchi che tecnologicamente si potrebbero replicare e controreplicare. Per questo, riconoscere e, quindi, poi accettare che tutte le difese possano essere superate è una condizione necessaria se non vitale per mettere in campo una strategia di contenimento di minacce che si costruiscono, e si autodefiniscono, nel tempo in ragione dei sistemi che si vogliono colpire e delle barriere che si vorrebbero superare.

In questo ambito, si inserisce anche il concetto di *cyber-resilience*; cioè, quella capacità di adattarsi allo stress o alle avversità permettendo al sistema di tornare a un punto di ripristino ad attacco subito e contenuto. Il raggiungimento della resilienza informatica richiede, però, un deciso dominio del proprio cyberspazio e una consapevolezza delle capacità di risposta del sistema[57].

Cioè, favorire il formarsi di una consapevolezza sulla necessità di predisporre capacità di *Remediation & Recovery* visto che i tempi di individuazione e risposta sono fondamentali per limitare i danni e poter reagire, se non prevenire, un prossimo attacco in maniera adeguata. È evidente che una volta definita e messa in campo la risposta alla minaccia, indagare sulla natura diventa un'operazione per la quale più velocemente si rileva e si risponde a un incidente, più è probabile che si potrà contenere il danno e prevenire un attacco simile in futuro.

Le azioni che possono essere condotte si possono indicare come: *reimage systems* (cioè, se possibile, il ripristino dei backup); patch o sistemi

[57] A tal proposito, World Economic Forum, *Global Cybersecurity Outlook 2022*, Insight Report, January 2022 pp. 26-27.

di aggiornamento (come le applicazioni o gli aggiornamenti del sistema operativo); riconfigurare l'accesso al sistema (rimozioni di account, reimpostazione della password); riconfigurazione dell'accesso alla rete; rivedere le capacità di monitoraggio su server e altre risorse; convalidare le procedure di applicazione delle patch e altri controlli di sicurezza eseguendo scansioni delle vulnerabilità della rete.

Tuttavia, è sin troppo chiaro che gli obiettivi di una strategia di sicurezza devono essere tali da permettere una caccia alle minacce in modo efficiente ed efficace; quindi, una previsione delle minacce, un esame efficiente delle cause degli attacchi, migliorare l'architettura di sicurezza, monitorare i comportamenti di sicurezza interessati e gestire i risultati falsi positivi da parte dei sistemi di rilevamento basati su regole predefinite prima e durante la gestione degli attacchi. In questo senso, una *policy*, se non una vera e propria strategia di sicurezza, non può che definire il proprio campo di azione ponendosi delle priorità fondamentali che, in un certo senso, possono essere ricondotte a individuare quegli eventi che potrebbero avere un impatto maggiore sulle operazioni di governance, sia essa istituzionale che economica in senso lato, produttiva e/o finanziaria.

Questo richiede una valutazione *a priori* di quali siano i sistemi considerati fondamentali per il funzionamento dell'architettura di governance, quali siano i sistemi fondamentali per assicurare la continuità delle attività quotidiane, quali altri sistemi e architetture digitali, siano essi dispositivi nel primo caso e reti nel secondo, siano da ritenersi critici, dove e in che misura vengono memorizzati e/o archiviati dati e informazioni ritenuti strategici se non vitali.

Accorgimenti, se non vere e proprie regole di tutela giustificate dal fatto che la crescita della digitalizzazione aumenta lo spettro delle possibilità di minaccia e le vulnerabilità dei dispositivi che nell'uso quotidiano sono dei terminali utili all'accesso delle più diverse richieste. È evidente, allora, che quanto in conclusione riporta il *Global Cybersecurity Outlook 2022* reso disponibile dal World Economic Forum Centre for Cybersecurity, la spinta anche verso un maggior ricorso all'IA nei settori più disparati dell'attività umana, da quella produttiva a quella economica a quella di sussistenza e di sicurezza e difesa, farà sì che, come si vedrà nella parte finale, anche il mondo della sicurezza informatica non sarà più lo stesso.

Intermediari sold-out?

Un altro aspetto, che va di pari passo con il decentramento che l'architettura digitale consente in chiave di governance, è l'inutilità di una intermediazione dimostrata dall'abbattimento delle distanze tra il livello politico-strategico e quello tattico, ovvero quotidiano. In questa prospettiva, non si deve tralasciare la nuova frontiera della tecnologia a blocchi, meglio nota come *blockchain*. Cioè, quella catena di registri che si muove su una rete di nodi attraverso i quali si gestiscono assetti finanziari, e non solo, senza ricorrere alle procedure fisiche di *banking* ma affidandosi a una rete aperta la cui sicurezza si fonda su una serie di consensi progressivi che l'utente rilascia nel corso delle operazioni. Nata soprattutto per gestire il mondo delle criptovalute, la tecnologia *blockchain* potrebbe però presto costituire una risorsa per organizzare processi di governance amministrativa che favorisca livelli di decentralizzazione, semplificandone il funzionamento.

Un processo di decentralizzazione immateriale che dovrebbe permettere una registrazione distribuita delle informazioni tra più nodi per il controllo di coerenza da parte del gestore della piattaforma. È evidente che la tracciabilità e la possibilità di ricostruire i diversi passaggi che caratterizzano un tale processo rappresentano un aspetto importante per garantire il controllo e la verifica delle operazioni informatiche. Ma costituisce anche il momento più delicato dell'intero processo nel corso del quale l'esistenza di un *bug* informatico potrebbe compromettere tali operazioni (transazioni finanziarie, atti amministrativi ecc.) o modificarne i termini e i contenuti.

Un altro aspetto, che va di pari passo con il decentramento, è proprio, come visto, l'inutilità di una intermediazione. Su questo piano, la possibilità stessa offerta dalle nuove tecnologie *blockchain* - nelle quali si colloca anche l'idea del ricorso a un «Metaverso» nelle transazioni bancarie o nei processi amministrativi o, ancora, nelle fasi di contrattazione/negoziazione - ne rappresenta, sempre meno, un aspetto potenziale[58]. D'altra parte,

[58] Il termine «Metaverso» fa la sua prima apparizione nel romanzo di fantascienza *Snow Crash* del 1992 scritto da Neal Stephenson, autore del movimento cyberpunk. Metaverso è, quindi, null'altro che una combinazione tra meta e universo. Lo sviluppo del Metaverso è quasi sempre legato al progresso tecnologico relativamente alla realtà virtuale e alla maggior possibilità di immersione che il sistema offre. A tal proposito, vedasi N. Stephenson, *Snow Crash*, Bantam Doubleday Dell Publishing Group Inc, New York, 2000.

ciò non è più un'ipotesi, ma una realtà all'interno della quale si definiranno rapporti giuridici oltre che relazionali considerato che il «Metaverso» si definisce come un'ipotetica interazione di Internet, un unico mondo virtuale universale e immersivo che coniuga realtà virtuale con una cosiddetta «realtà aumentata». Secondo uno studio condotto da JP Morgan il Metaverso rappresenterà una delle sfide dei prossimi anni visto che al suo interno saranno presenti quasi tutti i settori delle attività economiche, nel quale la contrattazione assumerà una propria validità e dove mondo cyber e IA coesisteranno in termini complementari e non interdipendenti.

L'aver previsto, ad esempio, un centro commerciale virtuale denominato *Decentraland*, strutturato su una *blockchain* di Ethereum, vedrebbe l'utente negoziare attraverso un proprio Avatar che nell'interagire in *Decentraland*, può porre in essere negozi giuridici legalmente validi ed efficaci. In *Opportunities in the Metaverse*, si dimostra come il Metaverso assumerà una propria centralità nei rapporti bancari e nelle negoziazioni grazie a una economia decentralizzata che, attraverso l'interoperabilità, potrebbe sbloccare immense opportunità economiche, per cui i beni e i servizi digitali non sarebbero più vincolati a una singola piattaforma o brand. Secondo il «Report», di J.P. Morgan, il vantaggio del Metaverso, rispetto a Second Life[59] o a Roblox[60] risiederebbe nell'assenza di una struttura proprietaria mentre, al contrario, proprio il suo carattere di ambiente decentralizzato, lo porrebbe come il luogo nel quale la gestione della virtualità delle relazioni è affidata, e garantita, da una community di gestori, che ricorrono a una o più DAO (Digital Autonomous Organization)[61]. Questo, dimostra quanto il mondo che si presenta alla nostra percezione fisica e misurabile in termini tradizionali si spinge ormai verso nuovi mondi digitali che modificheranno non solo il rapporto tra promotore e utente, ma anche i rapporti di lavoro laddove le grandi società investiranno, e sposte-

[59] Entrato sul mercato nel 2003, «Second Life» è un simulatore di un mondo virtuale che presenta avatar tridimensionali profilati per ogni utente e spazi e pensati per le più diverse attività sociali. Si potrebbe considerare come una sorta di simulatore di vita antesignano della tecnologia metaversica.

[60] «Roblox» si presenta come un universo virtuale definitivo che consente di creare, condividere esperienze con altri utenti oltre a essere una piattaforma attraverso la quale creare videogiochi con un proprio programma di grafica tridimensionale.

[61] https://youmark.it/ym-interactive/jp-morgan-apre-una-filiale-nel-metaverso-e-presenta-il-report-opportunities-in-the-metaverse-dove-illustra-luci-e-ombre-di-un-affare-valutato-un-biliardo-di-dollari/. Per un Virtual Tour, vedasi in JP Morgan's Onyx Lounge. In *Decantraland*: https://www.youtube.com/watch?v=54zs_mbUa1I.

ranno nel prossimo futuro, le operazioni nel Metaverso facendo del lavoro da remoto una condizione e non una eccezione[62].

Tale punto di vista, offrirebbe una visione del mondo che risolve la fisicità nell'abbattimento delle barriere spazio-temporali dei processi di governance, andando oltre rispetto a quella «visione da vicino» - una sorta di «mirror vision», espressione coniata da David Gelernter, professore alla Yale University, e autore di *Mirror Worlds* del 1991 - in cui si dimostrerebbe come l'idea di rete si sviluppi nel quotidiano, trasfigurando i paradigmi della nuova società in nuovi termini organizzativi e/o di relazione[63].

[62] In un interessante articolo dal titolo *Tech Trends 2022: Incontriamoci nel Metaverso*, viene indicato come e in che misura il cosiddetto «Continuum del Metaverso» sia già presente in nuove tecnologie che non potranno che riorganizzare le attività produttive, di offerta e di distribuzione delle aziende costrette, per gli autori dell'articolo, a dover modificare i propri processi attraverso l'adozione di strategie idonee a descrivere un mondo nel quale la dimensione fisica e quella virtuale si incontrano su piattaforme diverse e il cui successo «dipenderà dalla capacità di navigarle tutte per raggiungere i clienti, i partner e le proprie persone». Così in https://www.accenture.com/it-it/insights/technology/technology-trends-2022, 16 marzo 2022.

[63] *Building Mirror Worlds*, in D. Gelernter, *Mirror Worlds: or the Day Software Puts the Universe in a Shoebox… How it Will Happen and What it Will Mean,* Oxford University Press, Oxford, 1993, pp. 179-212.

II. Il «dilemma della sicurezza»

> Immagino che qualcuno potrebbe dire: «Perché non mi lasciate da solo? Non voglio far parte della vostra Internet, della vostra civiltà tecnologica, o della vostra società in rete! Voglio solo vivere la mia vita!». Bene, se questa è la vostra posizione, ho delle brutte notizie per voi. Se non vi occuperete delle reti, in ogni caso saranno le reti ad occuparsi di voi. Se avete intenzione di vivere nella società, in questa epoca e in questo posto, dovrete fare i conti con la società in rete. Perché viviamo nella Galassia Internet.
>
> Manuel Castells, *Galassia Internet*, 2001

In questa articolata nuova complessità dei prossimi anni, la cybersicurezza sicuramente risponde a pieno al «dilemma della sicurezza»; ovvero, quel dilemma che si risolve nel soddisfare quel paradigma per il quale la sicurezza è composta, in proporzioni variabili, tanto dalla protezione della sopravvivenza nazionale, intesa questa nei suoi significati fisici, politici ed economici, quanto dal perseguimento dei fini di politica estera; cioè dell'interesse nazionale. L'idea stessa che si possa raggiungere il massimo profitto con il minor rischio possibile, valorizzando capacità previsionali adeguate per qualità delle informazioni acquisite, fanno sì che la stessa Information Warfare (IW) e la Cyber Warfare (CW) si definiscano come due complementari paradigmi strategici che si completano sia nella condotta di superficie che in profondità.

Joshua Cooper Ramo, nel suo *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It* è molto chiaro laddove offre quale chiave interpretativa il fatto che non avendo scelte nel vivere in una società del rischio, la pace profonda (deep peace) nascerebbe solo e soltanto dalla consapevolezza che sia necessario controllare le forze che agiscono in profondità, all'interno di comunità sempre più complesse[1]. Se per Ulrich Beck la società del rischio è un prodotto della postmodernità,

[1] J. Cooper Ramo, *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*, Little Brown & Co., New York, 2009; trad. it., *Il secolo imprevedibile. Perché il nuovo disordine mondiale richiede una rivoluzione del pensiero*, Elliot, Roma, 2009.

per Cooper Ramo il rischio è rappresentato dall'ubiquità della minaccia unita alla sua invisibilità e alla certezza che essa si sarebbe potuta manifestare senza alcun elemento o forma di preavviso. Insomma, un prodotto tipico di un Black Swan così definito per l'essere un evento creduto imprevedibile, con un grande impatto e, dopo il fatto, in genere magari ridurne la portata cercando una spiegazione che lo faccia sembrare meno casuale e più prevedibile di quanto non fosse. Una scelta affascinante, ma non troppo[2].

Cooper Ramo, a tal proposito, propone il concetto di sicurezza profonda (deep security) ritenendo che ciò possa rappresentare una consapevole presa di coscienza per poter agire contro, così come definiti da Beck,

> I protagonisti informali delle relazioni internazionali, quali gli sviluppatori del Web, i terroristi e gli speculatori della finanza internazionale[3].

L'uso della Information Warfare, o, se si vuole, lo spostamento sul piano di una Digital Warfare in senso lato determina, infatti, uno shift a pieno campo sui servizi critici poiché se è vero che Internet favorisce l'abbattimento dei costi del quotidiano, esso lo fa anche nell'aumentare la capacità di penetrazione e di condizionamento degli asset sui quali si costruisce e si svolge quel quotidiano la cui continuità è il fine ultimo della sicurezza di una comunità politicamente ed economicamente organizzata. Aumento della vulnerabilità delle reti di approvvigionamento dell'energia, definizione e autonomia di governance secondo un modello C5I (Comando, Controllo, Comunicazioni, Computer, Cyber e Informazioni), comunicazioni in tempo reale sono ambiti nei quali si risolve il dilemma della sicurezza, ma anche gli spazi in cui l'avversario studia conseguenze e impatto degli attacchi. Ciò significa che, alla fine, la protezione del quotidiano, in termini di garanzia della sicurezza si risolve in una sorta di continue «lessons learned».

In questa prospettiva, le migliori performances high tech si pongono come un sostegno alla governance delle reti tecnologiche di supporto e ciò riguarda i centri decisionali, le commodity, le utility e ogni infrastruttura critica «intrinsecamente» interdipendente. Tutto questo, fa comprendere perché negli ultimi anni sia mutata l'idea di vulnerabilità, ponendosi come aspetto multidimensionale quanto richiedendo nuove formule di adde-

[2] A tal proposito vedasi, N.N. Taleb, *The Black Swan. The Impact of the Highly Improbable*, Penguin, New York, 2008; trad. it. *Il cigno nero. Come l'improbabile governa la nostra vita,* Saggiatore, Milano, 2023.

[3] U. Beck, *Risk Society: Towards a New Modernity*, Sage Publications, New York, 1992.

stramento informatico, capacità di acquisire know how strategico necessario per un efficace controllo del cyberspazio attraverso strategie *full spectrum dominance*. E si comprende anche perché la minaccia muta e nella sua non linearità pone a confronto dimensioni e protagonisti diversi per qualità e per obiettivi, mentre la stessa idea di forza, come visto, si rimodula attraverso un processo di ibridazione il cui epilogo, ad esempio, è che l'idea stessa che il soldato, quindi lo Stato, ne abbia ancora il monopolio si trasforma in un assunto non più realisticamente difendibile. Infatti, il campo di battaglia si sposta, per fisiologica ricerca del risultato più immediato, nelle aree dove più significativamente insistono i nodi di connessione delle strutture politiche, economiche e sociali che governano e supportano la vita di una nazione, di una comunità politicamente organizzata, di un'economia.

Cooper Ramo va ancora oltre. Sulla ricerca in IA ritiene che sarà impossibile condurla in maniera efficace e competitiva senza disporre o, meglio, far parte, di una connessione al sistema globale. La possibilità di gestire da remoto molti se non moltissimi aspetti del quotidiano come della governance attraverso forme di cloud computing, o ricorrendo allo smart working se non affidandosi alla blockchain per poi approdare alle opportunità che saranno offerte dall'Intelligenza Artificiale - il cui primo passo si può individuare nelle opportunità e nelle soluzioni che la domotica già offre all'utente - amplieranno il campo delle applicazioni IA[4].

Anzi, lo stesso incremento del ricorso al cosiddetto cloud computing - cioè a quella rete che permette tra vari dispositivi di connettere l'utente con il fornitore creando una vera e propria nuvola informatica nella quale si processano informazioni e ordini su piattaforme condivise - realizzerà un legame diretto tra periferie e centro, tra l'individuo remoto e un'architettura di strutture centrali che garantisce, o dovrebbe garantire, che in una condizione *peer to peer* delle relazioni si possa anche definire un quadro di soddisfazione e di fidelizzazione dell'utente/consumatore creando una sorta di interazioni mediate dalla tecnologia, magari giungendo a rideterminare la profilazione in una identità tecnologica per ogni utente/consumatore.

Un fenomeno che già accade nella formazione a distanza o nel lavoro da remoto, o smart working, laddove la dematerializzazione fisica del lavoratore può lasciare il dubbio di dove e in che misura l'altrove informa-

[4] J. Cooper Ramo, *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*, ...cit. p. 263 e ss.

zionale possa essere condiviso con altra concorrenza sfuggendo dal dominio del dante causa proprio il controllo del lavoratore nonostante l'esistenza di soluzioni informatiche che controllano e verificano il livello di attenzione del lavoratore, le altre connessioni aperte dai processi o dallo stesso lavoratore/operatore.

Insomma, quello che si osserva oggi nel mondo digitale, quale premessa evolutiva verso una dimensione IA di governo dei processi e delle quotidianità, è il formarsi di una visione di conoscenza ancora più avanzata rispetto a ieri. Una conoscenza che si immergerà nel transumano delle procedure e dei supporti che saranno offerti proprio dall'Intelligenza Artificiale, per la quale i processi digitali non saranno altro che i veicoli di acquisizione e uso delle informazioni da parte delle grandezze algoritmiche. Questo non rappresenterà altro che la conseguenza del principale obiettivo raggiunto dalla rivoluzione e dalla ricerca se non dalla conquista della leadership digitale. Ovvero, l'abbattimento del carattere carismatico del decisore, perché una IA può guidare da remoto il consenso mediando, in un ecosistema costantemente connesso, se stessa attraverso i dispositivi ritenuti più idonei al risultato: conquistare e indirizzare, in questo modo, le stesse emozioni delle masse.

D'altronde, se i sistemi tecnologici sono anche una produzione sociale e se la produzione sociale è modellata dalla cultura, anche la Rete, il mondo cyber e l'IA non fanno e non faranno eccezioni. La cultura di chi produce reti ne plasma il mezzo. Ecco, allora, che se la realtà che osserviamo oggi è che le relazioni politiche ed economiche saranno sempre di più ricondotte nel campo degli algoritmi, allora gusti e propensioni, scelte e decisioni saranno affidate alle valutazioni algoritmiche delle tendenze. Questo vuol dire che anche le operazioni di cyber-espionage muteranno di pelle, agganciando la loro condotta e affidando il loro successo proprio alla capacità di conoscere quel know how sensibile che è alla base della competitività se non della propria credibilità o di quella del proprio competitor. Infatti, il vero vantaggio competitivo illecito risiede tutto nel saper acquisire know-how dai sistemi IT dei proprietari/titolari per rimpiazzarlo su nuovi mercati ricorrendo all'anonimato. In questo senso, lo stesso Manuale di Tallinn definisce il cyber-espionage come

> Un atto intrapreso clandestinamente o con l'inganno che utilizza le capacità informatiche per raccogliere - o tentare di raccogliere - le informazioni con l'intenzione di comunicarle alla parte avversa.

Insomma, che si tratti di spionaggio industriale messo in campo *as-a-service* da gruppi strutturati di cui è stata ritenuta probabile - alla luce sia delle ingenti risorse dispiegate, sia della selezione dei target, quasi sempre funzionale al conseguimento di obiettivi strategici e geopolitici - la matrice statuale, la vulnerabilità di ogni processo umano, di ogni attività sia essa di governance che di distribuzione di informazioni su piattaforme e architetture che sovraintendono al quotidiano sarà rappresentata dal fatto che, parlando di una nazione, questa sarà vista nel suo insieme di dato politico e/o di aggregato economico-produttivo[5].

Attaccare senza far rumore

Si comprende quindi, come, sia che si tratti di operazioni di *cyber-espionage* ma anche di altre attività condotte sul piano informazionale, ciò che rende vulnerabile una piattaforma di governance, politica e/o economica è che attraverso una puntuale e ben definita profilazione si costruisce un consenso legittimante. Ciò vuol dire che l'obiettivo principale nel quadro di definire e garantire la sicurezza dell'utente nella scelta, nell'acquisto di un bene o nell'uso di un servizio presuppone la capacità delle istituzioni di governance di dominare le tendenze e, ciò, richiede il dominio del web dal momento che la Rete, come intermediario necessario, fornisce un canale di comunicazione orizzontale nell'ambito, in particolare, della e-governance. Questo dimostra il perché il rischio di attacchi alla sicurezza delle infrastrutture e alle architetture di governance, infatti, è direttamente proporzionale al grado di dipendenza tecnologica delle reti di comunicazione e scambio dati, i sistemi sono sempre più vulnerabili alle loro periferie che non al centro e, ovviamente, le possibilità di penetrazione sono illimitate.

In questo senso, gli stessi attacchi condotti da gruppi cyber come Legion e Killnet rimodulano la loro capacità di penetrazione attraverso di-

[5] È evidente che ogni operazione di difesa non può essere portata a termine se non si riducono i danni dell'attacco e se non si dispone di un adeguato livello di resilienza e di risposta minima, e ciò richiede quello che viene definito un livello adeguato di valutazione del rischio (*risk assessment*). In questo caso, infatti non si tratta solo di poter stabilire una efficace *Identity and Access Management Policy*, quanto di porre in essere tutte quelle misure e quegli accorgimenti che dovrebbero gestire e conservare i dati all'interno di un «perimetro di sicurezza» di un network di difesa con l'uso di firewall efficaci, crittografia dei dati e restrizioni all'utilizzo di Internet. Aspetti, questi, che non possono prescindere da un altrettanto adeguato livello di addestramento e di educazione dei dipendenti, di far maturare una consapevolezza del rischio e del loro essere gli attori principali nel sistema di sicurezza dell'organizzazione.

verse procedure di attacco quali i *Denial of Service* (DoS) o *Distribuited Denial of Service* (DDoS). In entrambi i casi, lo scopo è quello di far giungere al sistema una serie di richieste fittizie di dati e informazioni cui il sistema non riesce a rispondere e non risponde neanche alle richieste legittime. Le procedure adottate sono tali da distribuire tale attività su più dispositivi attraverso operazioni di *defacing* (o *defacement*), come attacchi condotti in maniera mirata su pagine di siti destinate al pubblico con l'intenzione di promuovere contenuti e, quindi, informazioni, utili a chi a vario titolo ha interesse a modificare una opinione, una percezione o una propensione.

Tra le tante possibilità di condotta di operazioni di cyber attacco ne vengono indicate in maniera molto articolata le più frequenti. Si possono così definire come cyberspionaggio, web vandalismo, propaganda, acquisizione di dati riservati, distribuzione di equipaggiamenti/attrezzatura, attacchi alle infrastrutture critiche, hardware contraffatto e/o compromesso, furto e/o distruzione dell'hardware. Una serie di rischi cui si aggiungono quelli più diretti alle capacità di gestione di dati e di uso come gli attacchi *ransomware*. Ovvero, come visto, azioni condotte per acquisire in maniera illecita e criptare tutti i file di un'azienda e che permettono ai cyber-criminali di richiedere un riscatto per sbloccare l'operatività della vittima e non divulgare i dati sottratti.

A questi si aggiunge il *phishing*, uno dei più comuni attacchi che consiste in una truffa telematica il cui scopo è quello di impossessarsi di informazioni, dati, codici ingannando l'utente; in genere, le modalità di attacco sono individuabili in messaggi di posta elettronica dal contenuto ingannevole. Vi è poi il cosiddetto «uomo nel mezzo» (*man-in-the-middle*), come visto, un attacco cyber condotto attraverso la manipolazione della comunicazione tra due parti che ritengono non solo di comunicare direttamente tra di loro, ma considerano l'oggetto trasmesso assolutamente credibile. È evidente che lo scopo è quello di impossessarsi, modificare, compromettere delle informazioni scambiate dalle parti senza che queste ultime siano consapevoli dell'intrusione di una terza parte la quale, in relazione al fine da perseguire, può sostituirsi a una delle due.

Tra i cosiddetti attacchi *ransomware* si può ricordare quello del 28 novembre 2016 condotto contro la metropolitana di San Francisco. Attacco che ha messo in crisi la metropolitana provocando gravi danni. Infatti, in due giorni consecutivi, i sistemi di controllo dei *gate* di accesso ai treni sono saltati, restando aperti a chiunque, anche senza un valido titolo di

viaggio. Si trattava del primo episodio che ha letteralmente messo in luce una delle possibili e più frequenti minacce il cui bersaglio possono essere proprio quelle Smart City sulle quali il nuovo modello di urbanizzazione tenderà a orientarsi nei prossimi anni. Quanto accaduto a San Francisco infatti, dimostrò già pochi anni fa come il prevedere innovazioni a un livello così ampio di digitalizzazione e *remote control* di servizi non vale a nulla se non vengono integrate adeguate misure di sicurezza. A questo caso di studio può aggiungersi anche l'attacco del 22 marzo 2018, alla città di Atlanta. Un attacco *ransomware* durato cinque giorni che ha colpito i sistemi informatici della corte di giustizia, dell'amministrazione comunale e dei centri per l'impiego.

Circa la qualità e dimensione di chi attacca in *Can Cyber Attacks Prevent Wars?,* Gunnar Westberg ritiene che dominare lo spazio cyber non sempre definisce capacità di esprimere una politica assertiva in virtù delle proporzioni di un attore rispetto a un altro[6]. Una guerra informatica, infatti, potrebbe anche essere un modo per una nazione più piccola di evitare un attacco militare da parte di un avversario superiore in termini di grandezze fisiche e disponibilità militari. Questo perché, ad esempio, un avversario di minor dimensioni potrebbe comunque decidere di condurre un attacco informatico ricorrendo segretamente a risorse utili sul piano della conoscenza e penetrabilità delle reti, per condurre un attacco più forte da siti collocati al di fuori del paese. Intendendo con questo *out of country*, posizioni da remoto la cui ubiquità possibile confonderebbe non poco le capacità dello Stato sottoposto ad attacco di poter individuare, per tempo, la direzione e la paternità della minaccia per poter efficacemente rispondere.

Tutto questo, fa capire come una *cyberwarfare* si porrebbe come una sorta di «equalizzatore» di potenza poiché offre opportunità anche al presunto perdente che ha possibilità di reagire, tenuto conto che uno dei più grandi vantaggi assicurati dalla guerra informatica è quello di essere multidirezionale; cioè, di non far individuare, almeno nelle fasi iniziali, la provenienza dell'attacco.

Sicurezza senza guadagno

I progressi nelle tecnologie di rete non distinguono, infatti, tra risorse fisiche e digitali; tra umanizzabili nei processi e controlli delle procedure

[6] G. Westberg, *Can Cyber Attacks Prevent Wars?* In J.M. Ramírez, L.A. García Segura (eds), *Cyberspace: Risks and Benefits for Society, Security and Development,* Springer, New York - London, 2017 pp. 275-279.

per quanto automatizzabili, considerandole entrambe quali risorse collocate su una rete[7]. Come si potrà facilmente riscontrare nelle esperienze del nostro quotidiano, molte organizzazioni hanno provveduto a installare reti elettroniche per ragioni di efficienza. Dalla posta elettronica ad altre applicazioni di rete è evidente che si possono realizzare importanti guadagni di efficienza e ciò è più che sufficiente per dimostrare una sorta di ineluttabilità della trasformazione di buona parte del quotidiano in un vissuto digitale del quale lo stesso Metaverso ne è la più recente ma non definitiva frontiera di ciò che sarà nel prossimo futuro la società delle reti distributive.

D'altronde, il passaggio dal primo livello dell'uso funzionale dell'informatica a supporto delle necessità individuali al secondo livello, ovvero all'attribuzione di capacità di governance in senso lato, non poteva che determinare cambiamenti comportamentali e organizzativi decisivi e, con essi trasformare anche i termini, i modi e gli strumenti con i quali sarebbero state e saranno affrontate e risolte le relazioni future in vari ambiti e nei diversi domini. La stessa intera gamma di *pay off* sarà sempre di più espressione e risultato di come e in che modo le tecnologie informazionali influenzeranno lo stile di vita delle persone come i comportamenti degli Stati e degli attori delle relazioni internazionali[8].

Nel 2013, Thomas Rid fece proprie tutte queste osservazioni nel suo *Cyber War Will Not Take Place*[9]. Volume nel quale affermava che le capacità informatiche non sono come i missili. Queste, infatti, non distruggono direttamente nulla e, pertanto, gli attacchi informatici raramente, se non mai, uccidono o feriscono fisicamente qualcuno. Esse sottendono un primo e fondamentale effetto: raccogliere informazioni tramite spionaggio, influenzare i risultati elettorali attraverso la sovversione o interrompere ogni vantaggio avversario attraverso il sabotaggio. Ma anche il sabotaggio informatico è un risultato indiretto. Insomma, negli stessi teatri di guerra un'operazione informatica potrebbe avere un impatto sul campo di battaglia, non ricorrendo a sistemi d'arma tradizionali, ma interrompendo la logistica, intervenendo sulle capacità di alimentazione dello sforzo o sull'approvvigionamento e questo vuol dire ridurre lo sforzo avversario se

[7] R.F. Weigley, *War and the paradox of technology*, in «International Security», Fall 1989, pp. 192-202.
[8] L. Sproull, S. Kiesler, *Connections: New Ways of Working in the Networked Organization,* MIT Press, Cambridge, 1991 pp.15-16.
[9] T. Rid, *Cyber War Will Not Take Place*, C. Hurst & Co. Publishers Ltd, London, 2013.

non proprio inibirlo con effetti direttamente misurabili sia sul piano militare che politico. Una possibilità, questa, non da escludere al netto di ogni ipotesi di escalation e facilmente adattabili a condizioni di *non-war*.

Infatti, trasferendoci sul piano non militare ma altrettanto competitivo come quello politico-economico, una metodologia utilizzata è quella di creare un *tracker* che ha attrattività, una tecnologia usata per monitorare l'attività online e ciò rappresenta la minaccia più diffusa alla privacy, consentendo l'accumulo lento, costante e implacabile di dati relativamente banali su come ogni individuo vive la propria vita online: cronologia di navigazione, utilizzo delle applicazioni, acquisti di dati ecc. In questo, ogni forma di attacco si trasforma nella definizione di cosiddetti *spy event* che non possono non essere oggetto di monitoraggio e di valutazione delle ragioni della condotta e degli obiettivi che si intendono perseguire.

Ecco, allora, che se si sommano le capacità possibili offerte dalla qualità cyber è più che evidente che la minaccia futura sulla sicurezza correrà lungo assi strategici che si muoveranno in ambienti dematerializzati poiché più facilmente aggredibili e utili a rendere sempre più intima la minaccia e il senso del pericolo, distribuendo un alone di sofferenza non solo sulla comunità in quanto tale, ma individuo per individuo, trasformando ogni dispositivo in un portale per penetrare l'intima sicurezza di ognuno di noi. Si definirebbe, in questo senso, una sorta di correlazione quantica in termini di strategie possibili dove il garantire ambiti ottimali di cybersicurezza è affidato alla possibilità di dominare lo spazio digitale con sistemi di sorveglianza ad alta sensibilità di verifica degli input realizzati per nascondere i veri scopi della richiesta, per poter penetrare in quel *gateland* che permette l'accesso al quotidiano della comunità-bersaglio e degli individui che ne fanno parte.

Muoversi sulla Rete significa, allora, avere chiari i vari livelli di stratificazione nella quale questa si articola. Ovvero, in quel passaggio dal cosiddetto *Surface web* nel quale si gioca e risolve l'accesso ai servizi di rete tra portali, piattaforme social e siti oltre a offerte di informazioni in open source, all'e-commerce e prodotti multimediali. Questi ultimi, in particolare, capaci di produrre sul piano emozionale risultati di particolare valore strategico in termini di gestione dell'intimo individuale e collettivo. D'altra parte, gli stessi influencer ormai recitano e bene ruoli che possono essere anche decisivi nella condotta di un attacco cyber o solo per poter ottenere una esfiltrazione di dati.

A questi si aggiunge però quel Deep Web caratterizzato da risorse informative che non sono indicizzate dai normali motori di ricerca, nel quale l'accesso si perfeziona ulteriormente discriminando, e qualificando, capacità di accesso ulteriori ma, anche, maggior condivisione di informazioni sensibili. E, in questo caso, si può approdare al Net-banking piuttosto che ai Research Paper, ai Medical Records, ai Private Forums, ai Private Networks e Hidden Wiki (una sorta di enciclopedia per pochi intimi raggiungibile attraverso Tor by-passandone i controlli, affidando al Deep Web le transazioni più imbarazzanti se non illecite possibili). Ma non basta. Vi è poi una ulteriore raffinazione delle possibilità di navigazione in un Dark Web dove i siti sono raggiungibili, ma solo attraverso l'uso di software dedicati e dove le IP sono rese anonime. Una parte del web nella quale attraverso portali ad accesso definito come Tor[10], operano tutte quelle realtà al limite delle condizioni di *facing* necessarie per verificare la legittimità non solo delle informazioni, ma delle operazioni condotte.

Mettersi al sicuro

Un aspetto interessante, in questa prospettiva, è rappresentato dalle reti «BotNet» che producono notizie volte a demolire una notizia presente nel web che necessita di piattaforme IA. In modo particolare, una *botnet* si presenta come una delle minacce più significative. *Botnet*, infatti, è una rete composta da dispositivi gestiti da remoto e infettati da *malware*. La pericolosità risiede nell'invisibilità in quanto gli utenti/possessori potrebbero non rendersi conto dell'infezione. Si tratta, in particolare, di reti complesse grazie alle quali le organizzazioni criminali che dispongono di *botmaster* sviluppano continuamente modi innovativi per reclutare nuove vittime nelle loro reti e monetizzarle.

Nella sua configurazione più semplice una *botnet* può essere definita come un gruppo di computer infettati da *malware* e che consente al suo controller (o master) di assumere una certa misura di controllo sulla macchina/e infetta/e (*shell*). Ogni *botnet*, viene utilizzata per eseguire una se-

[10] «Tor» (The Onion Router) non è altro che un software ad accesso libero, così reso disponibile con licenza BSD 3-Clause, che consente una web-navigazione del tutto anonima. Tor garantisce una non facile tracciatura o profilazione dell'attività svolta sia dall'utente in Internet, sia da parte di società commerciali che da parte di soggetti potenzialmente ostili. Tor è disponibile sia per sistemi Linux che Windows piuttosto che Android o anche MacOS.

rie di attività illecite all'insaputa della vittima. Una volta infettato dal *malware botnet*, il computer diventa un «morto che cammina e senza cervello», pronto a eseguire gli ordini del suo padrone. Le difficoltà a definire come e in che modo opera una *botnet* è rappresentata dall'incapacità di poter attribuire se non nell'immediato almeno in tempi ragionevoli dalla scoperta, una identità a coloro che operano nelle reti *botnet*, perché sono così diffuse ma, soprattutto, individuare quali siano i motivi reconditi del loro uso oltre alla necessità di poter determinare in che modo gli aggressori creano e distribuiscono una rete *botnet* e, ancora, come poter scoprire se un terminale è parte o meno di una rete *botnet*.

Tuttavia, gli attacchi *botnet* più frequenti sono condotti proprio attraverso attacchi DDoS (Distributed Denial of Service). Cioè, attraverso attacchi informatici il cui obiettivo è quello di ostacolare l'accesso a determinati siti web o a server. Una volta infettato il computer o il dispositivo, agendo mediante *malware* o intaccandone la sicurezza, esso è potenzialmente in grado di arrecare danni in quanto idoneo a diffondere il *malware*. A differenza del primo, questi tipi di attacchi sono riconoscibili in quanto il sistema risulta notevolmente rallentato poiché proprio nell'ambito di un attacco DDoS, come visto nelle pagine precedenti, lo scopo sotteso è quello di indirizzare una quantità di traffico così elevata su un server web da sovraccaricarlo e da non poter rispondere alle richieste legittime. Una tecnica comune consiste nel lanciare un attacco molto breve per estorcere protezione in cambio del non condurre un altro attacco più ampio.

Una delle minacce più pericolose del nuovo secolo rimane ancorata alla possibilità di manipolare l'opinione pubblica, a condizionarne e dirigerne il consenso attraverso strategie comunicative di falsa propaganda; ovvero, alla diffusione di informazioni false. Infatti, non per nulla, tra gli obiettivi di una *cyberwarfare* vi è la possibilità di manipolazione delle percezioni dell'avversario, sia esso Stato o comunità-bersaglio, attaccando i sistemi decisionali e rendendo inutilizzabili informazioni e processi per rallentare l'eventuale risposta e avere tempo per massimizzare il *pay off* prefigurato.

In questo senso, e adottando una cultura della consapevolezza diffusa, sia negli ambienti di protezione strategica che riguardano le istituzioni, per l'Unione europea piuttosto che le singole nazioni-partner che le imprese, il riconoscere e, quindi, accettare che tutte le difese possano essere superate è una condizione necessaria da porre a premessa di ogni *policy* e di ogni capacità di pianificazione di risposta alle minacce. Si tratta di una

predisposizione vitale, utile a realizzare una strategia di contenimento di minacce che si costruiscono e autodefiniscono nel tempo in ragione dei sistemi che si vogliono colpire e delle barriere che si vorrebbero superare.

È chiaro che poter disporre di una resilienza informatica richiede, però, un deciso e preciso dominio del proprio cyberspazio e una consapevolezza delle capacità di risposta del sistema, perché garantire una libertà di azione all'interno del cyberspazio rappresenta una condizione necessaria per condurre operazioni e attività commerciali intraprese da qualsiasi organizzazione istituzionale e/o privata.

D'altronde, è evidente che la possibilità di contenere un attacco, di resistere e di riuscire a rispondere prima che raggiunga l'obiettivo di compromettere la sopravvivenza di una architettura/rete di governance, risiede nel predisporre opportune misure e contromisure a difesa come gli antivirus, la cui capacità di rilevare, bloccare e rimuovere virus informatici da dispositivi infetti deve essere sempre più rapida nel tempo, aggiornandosi costantemente nella rilevazione della minaccia e nel contrasto alla stessa. Ciò, tenuto conto che il tempo di scoperta e di risposta rappresenta la vera sfida sull'utilità di tali software che, in genere, si è dimostrato solo parzialmente efficace.

Proprio per questo si ricorre ad altri strumenti come la crittografia, utilizzata anche nelle piattaforme social, la quale dovrebbe garantire riservatezza e sicurezza delle informazioni scambiate con chiavi crittografiche - definite da stringhe alfanumeriche idonee poi alla decodificazione - anche queste aggiornate in tempi utili ad anticipare e, quindi, inibire nuove minacce. Vi è poi il tradizionale ma fondamentale *backup*, cioè il produrre periodicamente copie di sicurezza di un insieme di dati o di un file su un supporto esterno al server, precauzione fondamentale per un'operazione di *disaster recovery*.

Vi sono poi strumenti di scoperta come l'*honeypot*, cioè ricorrere a un elemento periferico della rete cui si attribuisce il compito di essere un terminale-esca. Una possibilità utile a operazioni di scoperta di eventuali minacce e che prescinde dalla protezione dell'hardware o del software, permettendo di poter far sì che il tempo sia una risorsa a favore della difesa e non dell'attacco, riuscendo a individuare informazioni idonee a identificare nuove minacce e modalità di condotta di un eventuale attacco cyber. Seguono anche i citati *Penetration test*, utili nelle valutazioni della sicurezza di architetture/sistemi-rete aziendali e/o di governance in senso lato.

Tutto questo, richiede un'analisi condotta sia passivamente che attivamente per individuare i possibili punti di vulnerabilità o di accesso e/o difetti tecnici di hardware e software che potrebbero favorire la contaminazione di parte o dell'intera rete. Si aggiungono a questi, i sistemi di autenticazione circa l'identità dell'utente, la genuinità (attendibilità) delle informazioni e delle fonti/sorgenti. Tali sistemi possono ricorrere alla scansione dei tratti fisiologici dei soggetti come le impronte digitali e vocali, sistemi di riconoscimento del volto, iride ecc. Sistemi che se favoriscono da un lato una velocità nell'accesso si prestano, però, a un alto rischio di alterazione o di replica.

In un quadro di interdipendenza che sottende le relazioni contemporanee, l'ulteriore sfida si sposta anche sulla capacità di cooperazione tra pubblico e privato e sull'esistenza di una consapevolezza del rischio considerato che non sono pochi i casi nei quali il furto del cosiddetto IP critico, cui si riferisce anche la proprietà intellettuale e non solo la persona, può essere in corso da anni senza che l'utente sia a conoscenza di essere stato hackerato. Una soluzione, in questo caso, potrebbe essere rappresentata dal disporre di una potente piattaforma dati e/o utilizzando un super motore di correlazione, per identificare e valutare in modo proattivo attività insolite o sospette e rispondere rapidamente se capaci di individuare, per tempo, potenziali vulnerabilità.

Virtuali, e non troppo private

Nel poter verificare da dove e in che termini una minaccia può raggiungere un *gate*, e penetrare in uno spazio pubblico condiviso in una politica di sicurezza dell'architettura digitale di una nazione, non si possono trascurare le «Virtual Private Network» (VPN). Cioè, quelle reti virtuali private che in linea di massima dovrebbero garantire le migliori condizioni di protezione di dati ma che, in realtà - permettendo il collegamento tra il privato che crea un proprio network e una rete specifica, aziendale o pubblica, superando anche le barriere nazionali con una possibilità di sfuggire a operazioni di monitoring come avviene nell'acquisto di prodotti, beni o servizi in contesti geografici, e mercati quindi, extra UE - possono rappresentare le migliori condizioni per penetrare uno spazio protetto. D'altra parte, la possibilità di implementare una VPN è riconosciuta a quasi tutti i sistemi operativi più diffusi, e in genere si usano le VPN per consentire il collegamento dell'utente da remoto alla rete con la quale dialoga per motivi di lavoro o per altri motivi che attendono al proprio quotidiano.

Ciò comporta, però, che nel definire un *tunnel proxy* tra la rete aziendale o del concessionario di servizi e la propria connessione individuale, si possono scambiare dati la cui direzione può essere diversa da quella ritenuta adeguata dal sistema. Infatti, con una connessione VPN ci si può collegare da un client (utilizzatore, sia hardware che software) come se si fosse fisicamente, attraverso un cavo di rete o un intramezzo wireless, cablati. La sicurezza del sistema è assicurata dal fatto che se l'utente ha il servizio VPN attivato, tutte le sue richieste transitano dai server aziendali, come se la connessione fosse effettuata in locale, ottenendo pertanto l'accesso ai servizi riservati. Ciò non eviterebbe che un adeguato processo di hacking non riesca a superare le protezioni identificandosi come client e inserendosi nella rete, nonostante le procedure di sicurezza messe in campo. Ovviamente, anche in questo caso si possono individuare limiti e pericoli delle VPN.

Posto che lo scopo di una VPN è che i server sui quali essa è attestata garantiscono conservazione e tutela di dati attraverso un *tunnelling* crittografato gestito da un hacker (quanto da un governo o da un provider), attraverso una VPN si può modificare anche un IP. Ma non solo. L'utente, ad esempio potrà trovarsi anche sottoposto alle condizioni del gestore il quale potrà decidere se crittografare la connessione o meno in ragione del livello di sicurezza che ritiene più adeguato a tutela del servizio fornito o dei dati di cui si permette l'accesso. È anche vero, però, che l'utente di una VPN può decidere di affidarsi a un server non necessariamente aziendale in ragione dell'uso che ne intenderà fare. La sicurezza per il gestore, che si svolge sulle reti definite Intranet, dovrebbe essere assicurata dalla limitazione degli accessi o dall'interdizione per il possessore di una VPN di poter accedere a siti non autorizzati dallo stesso gestore.

È evidente che la pericolosità di accessi indesiderati risiede nella gestione dei protocolli di tunneling soprattutto quando si permette a un protocollo straniero di essere usato su una rete che naturalmente non lo supporta. In materia di sicurezza è vero che il tunneling *Secure Shell* permette di oltrepassare i firewall che proibiscono determinati servizi Internet, sempre che siano permesse connessioni in uscita. Ma è altrettanto vero che proprio la possibilità di aggirare i firewall in uscita, utilizzando protocolli riconosciuti come autentici, rischia di far accedere una minaccia all'interno di sistemi o di definire e superare la protezione crittografica della comunicazione.

Al di là delle varie protezioni che una VPN dovrebbe avere, va da sé che i moltiplicatori di sicurezza si identificano in protocolli che dovrebbero permettere l'autenticazione e, in alcuni, casi la crittografia della rete. Poiché i tunnel hanno un ingresso e una uscita e viceversa, chi gestisce/amministra/utilizza uno dei due *gate* deve aver stabilito con l'altra parte le condizioni e le regole di accesso. L'obiettivo è quello di evitare compromissioni ma, in particolar modo, intrusioni nel percorso VPN sfruttando proprio i protocolli di sicurezza e l'ingresso nel tunnel proxy. Questo, per evitare la minaccia più frequente indentificata in un cosiddetto *replay-attack*. Cioè, un attacco condotto sulla rete diretto a impossessarsi di credenziali di autenticazione comunicate per replicarle in maniera fraudolenta. Oggi, tuttavia, le tecnologie e le tecniche difensive tradizionali affrontano il 99% delle minacce informatiche anche solo ricorrendo a sensori tradizionali, software e antivirus.

Cose di casa. L'Internet of Things

Per combattere minacce informatiche sempre più avanzate Timothy Paul Coderre, Chief Strategy Officer-CSO di Arc4dia[11], ritiene che il nuovo campo di confronto non è solo quello delle infrastrutture critiche degli Stati, ma anche il cosiddetto «Internet of Things» (IoT) o «Internet delle cose». Cioè minacce condotte sui dispositivi che gestiscono le *smart things* nel tentativo di penetrare, usandole come teste di ponte (*pivoting*), per conquistare spazio nelle reti principali di gestione dei dati attraverso le quali raggiungere i sistemi centrali.

Il campo delle «Internet of Things», (o *Web of Things*), non è altro che rappresentato dall'universo di *smart object* che dai *device* personali si sposta sulla domotica e su altre attività o "cose" digitali. La principale fetta di questo mercato sembra essere rappresentata dalle applicazioni di Smart Metering (i contatori intelligenti installati presso le utenze domestiche), dalle Smart Car, nella Domotica o Smart Home, o nelle Industrial IoT[12]. Gli aggressori, infatti. sfrutteranno sempre di più i servizi offerti e i processi dei dispositivi intelligenti[13]. Un aspetto, quest'ultimo, che era stato ben evidenziato sin dal Vertice Nato di Varsavia del 8 e 9 luglio 2016.

[11] https://arc4dia.com/.

[12] Cfr. A. Tumino, *Mercato IoT: quanto vale l'Internet of Things in Italia*. In https://blog.osservatori.net/it_it/mercato-iot-in-italia, 11 aprile 2019.

[13] T.P. Coderre, *Battling Today's Most Advanced Cyber Threats*, in *Strengthening Peace and Security*, Nato Summit 2016, Warsaw, Atlantic Treaty Association, Global Media Partners, 2016 p. 85.

Infatti, dal 2015, in ambito NATO, ad esempio, si era dato il via a una collaborazione nel settore privato con lo sviluppo di una «Malware Information Sharing Platform» (MISP)[14]. Ovvero, un'ampia interazione diretta con l'industria e workshop di progetti di difesa intelligente. Inoltre, sempre nel 2015, anno dell'avvio di tali progetti e di maggior sensibilità verso la cybersecurity, circa 65 rappresentanti dell'industria hanno partecipato alla «NATO Cyber Coalition». Un'idea di collaborazione operativa con lo scopo di approfondire le procedure e garantire un rapido coordinamento sia a livello operativo che strategico attraverso scenari realistici in modo che l'Alleanza, nel suo insieme, fosse preparata in caso di crisi da attacco informatico. Da allora, il Centro di eccellenza per la difesa informatica della NATO di Tallinn, in Estonia, organizza un'esercitazione annuale, *Locked Shields*, per rappresentanti delle nazioni alleate e partner.

Per Coderre, le vulnerabilità spesso esistono proprio nei dispositivi e sistemi IoT che sono al di fuori dal controllo informatico o delle procedure di sicurezza sottraendosi, in questo modo, a ogni possibile monitoraggio. Si pensi agli impianti di condizionamento, la gestione elettronica degli accessi o alle diverse possibilità offerte dalla domotica. Un campo, quello delle IoT, estremamente sensibile dove i vari *device* rappresentano ottime porte di accesso a dati e informazioni che si inseriscono dal quotidiano privato alla dimensione pubblica delle relazioni sociali e politiche oltre che economiche. Anche lo stesso apprendimento automatico (*Machine Learning* - ML) e l'Intelligenza Artificiale potranno essere utilizzati in modo improprio per ascoltare su dispositivi connessi come Smart TV e altoparlanti, per curiosare nelle conversazioni, personali e aziendali, che possono fornire materiale per estorsioni o spionaggio aziendale[15]. Alle IoT si sommano anche gli attacchi all'Industrial Internet of Things (IIoT) messi in campo da attori statali o da attori esterni i cui obiettivi sono rappresentati dai servizi di pubblica utilità alle fonti energetiche e alle industrie manifatturiere.

Per fronteggiare simili vulnerabilità, la maggior parte delle organizzazioni hanno tradizionalmente usato come perimetro del sistema di difesa

[14] J. Wiseman, S. Michell, *Strengthning Peace and Security,* Warsaw, Nato Summit, 2016.
[15] In *The converged future ushers in old and new attacks and techniques that expose information technology (IT) and operational technology (OT) assets*, https://www.trendmicro.com/vinfo/ph/security/research-and-analysis/predictions/2020. Vedasi anche: *The New Norm. Trend Micro Security Predictions for 2020*. Paper disponibile in https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf.

i firewall aggiungendo, di volta in volta, livelli ulteriori di sicurezza in ragione dell'evoluzione della minaccia. Però è anche vero, che pur dovendo affrontare una minaccia sempre più complessa, un firewall che si implementa ogni volta alla fine perde di efficacia. L'idea sarebbe quella di poter disporre di soluzioni firewall di nuova generazione capaci di realizzare, all'interno di un ben definito perimetro di sicurezza, una rete che andrebbe dal cloud ai dispositivi mobili attraverso i quali si accede ai servizi e se ne garantisca la difesa, permettendo di proteggere in maniera integrata server di posta, server web, l'infrastruttura wireless. Ciò richiede però, come visto, nuovi concetti di firewall che abbandonino la loro natura di difesa passiva, riconfigurandosi in sistemi attivi con capacità di acquisire informazioni utili per assicurarsi un rapido adeguamento alle minacce indicate, perché ogni attacco hacker tende a essere sempre più sofisticato e sincronizzato, senza dover rispondere a particolari condizioni fisiche di collocazione spaziale.

La stessa economia del cloud e lo studio dei costi e dei benefici del *Cloud computing* rappresentano ambiti di particolare interesse e vulnerabilità da un punto di vista di tutela di una erogazione di servizi effettuata attraverso Internet e su richiesta di un utente finale da parte di un fornitore[16]. E anche su questo, la necessità di definirne i modi e i termini di protezione segna una ulteriore sfida alla tenuta di un'architettura complessiva di sistemi di dati necessari alla crescita economica o al funzionamento di sistemi di governance.

[16] Il «Cloud computing», letteralmente "nuvola informatica" o "servizi nella nuvola", indica un'erogazione di servizi offerti su richiesta da un fornitore a un utente finale attraverso la rete internet e che si risolve, ad esempio, nell'archiviazione, l'elaborazione o la trasmissione dati, permessa da una rete di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. Cfr. anche: P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, NIST, Special Publication, September 2011.

III. L'Unione europea e le norme sulla cybersicurezza. Semplificare la complessità

> Nella battaglia per l'unità europea è stata ed è tuttora necessaria una «concentrazione di pensiero e di volontà per cogliere le occasioni favorevoli quando si presentano, per affrontare le disfatte quando arrivano, per decidere di continuare quando è necessario».
>
> Altiero Spinelli, *L'Europa non cade dal cielo*, 1960

L'aspetto più sensibile nella definizione di come può essere messa in campo una strategia di sicurezza digitale non può non considerare l'impatto giuridico che le nuove relazioni, i processi, le contrattazioni e la gestione in senso lato dei dati e del patrimonio informazionale di un utente presentano. Questo, non solo perché lo spettro delle relazioni umane si sposta su piattaforme e ambiti non più necessariamente fisici, ma perché la rapidità dei processi implica una fiducia sulla legittimità di scelte, azioni e risultati decisi e conseguiti da un altrove non solo fisico.

Come visto nelle pagine precedenti, infatti, imprevedibilità e complessità rappresentano i due caratteri contraddistintivi dell'era cyber e lo saranno ancor di più se si fa riferimento alle cosiddette tecnologie rivoluzionarie come l'Intelligenza Artificiale. In questo nuovo mondo che corre velocemente e che riduce i confini non solo fisici ma umani, lo sforzo principale degli Stati e dell'Unione europea è rivolto a creare condizioni condivise di sicurezza fissando norme che, pur tenendo conto degli interessi dei singoli Stati membri, siano adeguate a costruire nel tempo un'unica architettura di governance e, quindi, prevedere condivise procedure di difesa e di risposta agli attacchi del futuro.

Già con il Regolamento (UE) n. 2016/679 del 27 aprile 2016, (*General Data Protection Regulation* - GDPR) relativo alla protezione dei dati ci si poneva il problema di come tutelare la disponibilità, l'autenticità, l'integrità e riservatezza dei dati personali. Al di là delle norme di garanzia, ciò che era interessante era dato dalla previsione nel Regolamento del «principio di accountability» (art.22) quale principio di «responsabilizzazione» per il quale il titolare del trattamento dei dati, ovvero, colui che ne ha legittima-

mente la disponibilità, deve adottare comportamenti proattivi e attività dimostrabili, finalizzati al rispetto della normativa contenuta nel Regolamento stesso. Ma non solo. L'art.25 chiarisce che la sicurezza deve essere prevista secondo una privacy «by design»; ovvero, sin dalla fase di progettazione di un modello di gestione di dati e/o informazioni sensibili. Per questo, le misure di sicurezza «by design» non possono che derivare che da un'attenta valutazione del rischio (approccio *risk based*).

In altre parole, i dati personali devono essere trattati, secondo un'architettura predefinita, in maniera necessaria e sufficiente per le finalità previste e limitatamente al periodo ritenuto necessario per i fini autorizzati ed evitando un eccesso di ricorso ai dati al di fuori di motivazioni specificatamente indicate (*privacy by default*). Inoltre, a chiudere il «perimetro della sicurezza», vi era la necessità di garantire una continuità operativa che, ancorché non direttamente prevista ex art. 32 del Regolamento, si desume dal fatto che, per l'articolo citato, al titolare del trattamento e della custodia dei dati veniva e viene attribuita la responsabilità per il solo fatto di dover provvedere a mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, implementando una vera strategia di continuità operativa, periodicamente testata in modo da poterne dimostrare l'efficacia.

Se questo riguarda la tutela dei dati come prima consapevolezza dell'importanza dei processi informazionali nella governance digitale che avrebbe caratterizzato il nuovo secolo, di certo non poteva non consolidarsi negli ultimi anni una certa sensibilità verso la cybersicurezza. Nel 2016, infatti, veniva emanata la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 (o Direttiva NIS 1 – Network and Information Systems) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi; ovvero, sulla sicurezza delle reti e dei sistemi informativi dell'Unione[1]. Lo scopo era quello di dare contenuto

[1] https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf. Recepita in Italia con il Decreto Legislativo 18 maggio 2018, n. 65 *Attuazione della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*, (18G00092) (GU Serie Generale n.132 del 09-06-2018). Il Decreto ha anche previsto l'istituzione, presso la Presidenza del Consiglio dei Ministri, di un unico Computer Security Incident Response Team, detto CSIRT Italia, al quale venivano assegnati compiti e funzioni dei precedenti CERT-Nazionale (CERT-N) e CERT-Pubblica Amministrazione (CERT-PA). L'8 agosto 2019, con un DPCM ad hoc, *Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team* è stato costituito il CSIRT Italia presso il Dipartimento Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri con la parziale trasformazione del CERT-PA in CERT-AgID. CSIRT Italia è ora confluito nella Agenzia per la Cybersicurezza Nazionale - ACN.

alla EU's-*Cybersecurity Strategy for the Digital Decade*[2], ridefinendo i termini attraverso i quali garantire non solo la tutela del trattamento e della conservazione dei dati, quanto definire modi e termini di risposta agli attacchi ritenendo ormai la resilienza uno dei paradigmi fondamentali di ogni strategia di *cybersecurity*.

Raggiungere un elevato grado di sicurezza dei sistemi informativi e delle reti richiede a ogni operatore dei servizi digitali (DSP) obblighi nel mettere in campo misure di sicurezza idonee, stabilendo adeguate condizioni per garantire la continuità dei servizi organizzando la migliore risposta possibile. Infatti, il nucleo centrale della Direttiva e, quindi, della strategia UE, ieri come oggi, è rappresentato dall'attribuire alla resilienza delle reti e delle cosiddette infrastrutture critiche un ruolo fondamentale per garantire una tenuta delle infrastrutture digitali da eventuali attacchi ai propri sistemi di governance quanto di contribuire, in tal misura, a rendere credibile, rafforzandola, la stessa leadership UE sia in materia di normativa che di standard di sicurezza rivolta al cyberspazio. La stessa Direttiva prevedeva, altrettanto, la cooperazione internazionale e affermava che l'Unione promuoveva la creazione di un cyberspazio globale, aperto, stabile e sicuro disciplinato da un ordinamento giuridico adeguato che salvaguardi diritti umani, libertà fondamentali e assetti democratici.

In tali termini, sarà così che tra il 9 e il 10 giugno 2016, nell'ambito del Consiglio Giustizia e Affari Interni, i ministri della Giustizia dell'UE nel discutere su come migliorare la giustizia penale nel cyberspazio per combattere le attività criminali adottavano due conclusioni che stabilivano delle misure pratiche per incrementare la cooperazione, nonché un calendario per ulteriori azioni relative sia al miglioramento della giustizia penale nel cyberspazio che della rete giudiziaria europea per il contrasto alla criminalità informatica[3]. Un anno dopo, il 24 ottobre 2017 veniva concordato un ulteriore piano d'azione per la sicurezza informatica. In particolare, il Consiglio conveniva di istituire un piano d'azione per la riforma della cybersicurezza dell'Unione europea considerando che la sicurezza online rappresenta una condizione essenziale per i cittadini e le imprese europee.

[2] High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade*, Brussels, 16.12.2020, in: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[3] https://www.consilium.europa.eu/en/press/press-releases/2016/06/09/criminal-activities-cyberspace/.

In particolare, le misure definite a livello intergovernativo sancivano la razionalizzazione delle procedure di assistenza giudiziaria reciproca e, ove applicabile, di mutuo riconoscimento relativamente al cyberspazio grazie all'uso di moduli e strumenti elettronici standardizzati, il miglioramento della cooperazione con i fornitori di servizi attraverso lo sviluppo di un quadro comune (es. uso di moduli e strumenti perfettamente allineati) per richiedere specifiche categorie di dati e l'avvio di un processo di riflessione su possibili criteri di collegamento per la competenza esecutiva nel cyberspazio.

Successivamente, il 20 dicembre 2017, le istituzioni dell'Unione europea, Commissione compresa, si sono dimostrate particolarmente sensibili nel ritenere necessario il dover rafforzare la cooperazione in materia di contrasto agli attacchi informatici. In questo ambito, ne è scaturito un accordo che istituiva una squadra permanente di risposta alle emergenze informatiche, una squadra di pronto intervento informatico per le istituzioni, gli organi e le agenzie dell'UE come CERT-UE. Struttura, quest'ultima, che avrebbe servito tutte le istituzioni, gli organi e le altre agenzie dell'Unione. Lo scopo di CERT-EU era ed è quello di garantire la migliore e più efficace e coordinata risposta dell'Unione agli attacchi informatici contro le sue istituzioni. Tuttavia, la rilevanza degli assetti digitali e le vulnerabilità definibili nell'arco di tempi molto ristretti fecero sì che il 16 aprile 2018, circa le attività informatiche dannose, il Consiglio nelle conclusioni sottolineasse quanto l'importanza di un cyberspazio globale, aperto, libero, stabile e sicuro in cui si applichino pienamente i diritti umani, le libertà fondamentali e lo Stato di diritto fosse la condizione necessaria per un mondo più sicuro[4].

Un Cybersecurity Act

Il problema diventava, però, come dare spazio e definire un *Cybersecurity Act* idoneo a soddisfare il paradigma cooperativo per offrire maggior efficacia alla risposta in caso di attacco informatico, di razionalizzazione dei costi e di migliore distribuzione delle capacità di difesa.

In questa prospettiva, il 13 settembre 2018, sempre il Consiglio avrebbe avviato dei negoziati con il Parlamento europeo con l'obiettivo di rag-

[4] Documento 7925/18 del 16 aprile 2018. Page 78. 77. 173. *Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza*. Documento di riflessione, marzo 2019. Consultabile in: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_IT.pdf.

giungere un accordo sul *Cybersecurity Act* entro la fine di quell'anno. L'orientamento generale su questa proposta era già stato raggiunto l'8 giugno. Il *Cybersecurity Act* avrebbe dovuto avere come scopo quello di migliorare la resilienza informatica ricorrendo a un livello di certificazione UE per prodotti, servizi e processi ICT. La consapevolezza di dover dare corso a un quadro comune di sostegno, oltre che di disciplina nel campo della sicurezza dello spazio digitale europeo, avrebbe fatto sì che a distanza di pochi mesi, sempre il Consiglio, il 18 ottobre 2018, chiedesse idonee misure per realizzare una credibile cybersicurezza nell'Unione visto che i leader europei auspicavano un ulteriore rafforzamento della deterrenza, della resilienza e della risposta dell'Unione alle minacce ibride, informatiche, chimiche, biologiche, radiologiche e nucleari (CBRN). Una richiesta, la precedente, favorita, suo malgrado, dagli attacchi informatici subiti dell'Olanda nello stesso anno ai danni dell'Organizzazione per la proibizione delle armi chimiche (Organisation for the Prohibition of Chemical Weapons-OPCW) all'Aia[5].

Il 19 novembre 2018, in materia di difesa informatica, il Consiglio aggiornava nuovamente il quadro politico perché l'Unione riteneva non più dilazionabile nel tempo la necessità di dover rafforzare la propria capacità di resilienza, questa volta promuovendo non solo la cooperazione tra Stati membri, ma anche tra il mondo militare e quello civile; ovvero, tra quello della Difesa e quello della Sicurezza. Alla fine, in particolare, il 19 dicembre 2018 gli ambasciatori presso l'Unione approvarono la proposta di regolamento.

Si trattava di un passo decisivo, seppur avvenuto nella frammentazione degli istituti e delle normative che avrebbero dovuto assicurare al meglio una certificazione di sicurezza informatica a livello europeo e consolidare un'agenzia europea permanente per la sicurezza informatica. Già il 10 dicembre 2018 la presidenza del Consiglio e il Parlamento europeo avevano raggiunto un accordo provvisorio sul *Cybersecurity Act*. Giunto a tale traguardo, il 13 marzo 2019 si poneva il problema di come mettere in comune le competenze in materia di cybersicurezza.

Dal canto suo, il Consiglio avviò nuovi negoziati con il Parlamento europeo. Gli ambasciatori presso l'UE conferivano nel frattempo alla presidenza del Consiglio il mandato di avviare i colloqui con il Parlamento europeo sulla condivisione delle competenze in materia di sicurezza digitale. I negoziati

[5] https://www.consilium.europa.eu/en/meetings/european-council/2018/10/18/.

si sarebbero concentrati, in particolare, su due iniziative. La prima, nell'istituire una base di conoscenze attraverso il Centro Europeo Industriale, Tecnologico e di Ricerca sulla cybersicurezza. La seconda, nel creare una rete di centri nazionali di coordinamento. Il 9 aprile 2019, il Consiglio adottava il regolamento, il *Cybersecurity Act*, che introduceva un modello di sistemi di certificazione a livello UE, un'Agenzia europea per la sicurezza informatica, che sarebbe subentrata all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione pur mantenendone l'acronimo ENISA.

Definita la cornice di sicurezza, e individuato l'ente di vigilanza e garanzia, l'idea di definire un quadro complessivo di difesa in campo digitale, e di porre norme a riguardo di un'Europa sempre più cyber-resiliente, la si individuerà nel Regolamento (UE) 2019/881 del Parlamento e del Consiglio del 17 aprile 2019 relativo proprio alla nuova ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione per le tecnologie dell'informazione e della comunicazione, che abrogava il Regolamento (UE) n. 526/2013 («Regolamento sulla cybersicurezza»). Entrando in vigore il nuovo Regolamento, si spostava in avanti il perimetro della sicurezza istituendo una nuova figura di valutazione e certificazione.

Gli obiettivi del nuovo *Cybersecurity Act* sono ben definibili in una necessaria visione comune circa la sicurezza informatica dei prodotti ITC e dei servizi digitali, nell'attribuire maggiore enfasi all'ENISA rafforzandone il ruolo guida e infondendo maggior fiducia nei consumatori nel mercato europeo[6]. Ciò che si sarebbe aggiunto sarebbe stato l'aver previsto anche un quadro sanzionatorio a livello UE. Infatti, il 17 maggio 2019 il Consiglio prevedeva la possibilità di imporre sanzioni mirate volte a scoraggiare e contrastare gli attacchi informatici che costituiscono una minaccia esterna per l'Unione europea e/o per gli Stati membri. Per la prima volta, insomma, si prevedeva un quadro sanzionatorio con la possibilità di comminare sanzioni a persone o entità responsabili di attacchi informatici o tentati attacchi informatici, che forniscono sostegno finanziario, tecnico o materiale per tali attacchi o che sono altrimenti coinvolte e che prevedono sia un divieto per le persone che viaggiano verso l'Unione che un congelamento dei beni di persone sia fisiche che giuridiche.

[6] La nuova Agenzia dell'UE per la cybersicurezza si basa sulle strutture del suo predecessore, l'Agenzia europea per la sicurezza delle reti e dell'informazione, ma ha un ruolo rafforzato e un mandato permanente. Il compito affidato è quello di sostenere gli Stati membri, le istituzioni dell'UE e altre parti interessate nella gestione degli attacchi informatici.

Tutto questo, dimostra come l'Unione europea si preparava e prepara a voler essere più resistente e a rispondere agli attacchi informatici dotandosi di un regime sanzionatorio idoneo a scoraggiare e rispondere agli attacchi informatici che costituiscono una minaccia esterna per l'Unione e/o i suoi Stati membri. Un quadro sanzionatorio che si sarebbe applicato e si applica anche agli attacchi informatici contro Stati terzi o organizzazioni internazionali, in cui le misure restrittive sono considerate necessarie per raggiungere gli obiettivi della politica estera e di sicurezza comune nelle sue diverse declinazioni (anche se si sarebbe dovuto attendere il 30 luglio 2020 per vedere imposte, per la prima volta da parte dell'UE, sanzioni contro gli attacchi informatici).

Il 9 giugno 2020, il Consiglio, ancora una volta, adottava delle conclusioni con le quali si affrontavano un'ampia gamma di questioni legate all'attuazione della strategia digitale dell'Unione europea[7]. Mentre, nell'ottobre del 2020, i leader dell'Unione chiedevano e ottenevano la convocazione di un Consiglio straordinario, il 1° e il 2 ottobre, dedicato al rafforzamento delle capacità per *Un futuro digitale per l'Europa* necessarie per: proteggersi dalle minacce informatiche; provvedere a un ambiente di comunicazione sicuro, soprattutto attraverso la crittografia quantistica; garantire l'accesso ai dati a fini giudiziari e di contrasto. In questo ambito, uno degli aspetti ritenuti strategicamente importanti era rappresentato dalla promozione della cyber-resilienza da inserire come parte fondamentale di un'adeguata strategia UE in materia di cybersicurezza.

Infatti, nel dicembre 2020, la Commissione europea e il servizio europeo per l'azione esterna (SEAE) presentavano una nuova strategia per la sicurezza digitale i cui obiettivi dovevano essere quelli di offrire uno standard di resilienza elevato e idoneo a garantire i cittadini e le imprese europee nel poter contare sull'erogazione dei servizi e sul funzionamento degli strumenti digitali da ritenersi affidabili e, in particolar modo, attendibili. In tal senso, il successivo 22 marzo 2021 il Consiglio adottava, altresì,

[7] Il testo evidenzia l'impatto della trasformazione digitale sulla lotta alla pandemia e il suo ruolo fondamentale nella ripresa post-COVID-19. In relazione alla sicurezza informatica, poiché le minacce e i crimini informatici stanno aumentando in numero e sofisticatezza, i ministri dell'Unione europea intendono migliorare le capacità di risposta dell'UE e a salvaguardare l'integrità, la sicurezza e la resilienza delle infrastrutture digitali, delle reti e dei servizi di comunicazione. L'Unione sostiene, inoltre, la necessità di un approccio coordinato per mitigare i rischi legati alla sicurezza informatica e garantire una diffusione sicura del 5G.

conclusioni sulla strategia in materia di cybersicurezza, sottolineando che essa è essenziale per costruire un'Europa resiliente, verde e digitale. A tal proposito, i ministri dell'UE stabilivano, in questo modo, che l'obiettivo fondamentale da raggiungere era rappresentato dall'autonomia strategica pur mantenendo nel contempo un'economia aperta.

Competere in cybersicurezza

Proprio in tale ambito, sarebbe stato definito quel «Percorso per il decennio digitale» quale programma strategico dell'Unione per favorire la trasformazione digitale, individuandone gli obiettivi, i traguardi digitali specifici da raggiungere entro il 2030. Il programma, infatti, che colloca al primo posto competenze e istruzione digitali, è articolato intorno a quattro settori: competenze, imprese, pubblica amministrazione e infrastrutture[8].

Ma proprio per le competenze, il programma definisce anche come intensificare la cyber-difesa attraverso formule e politiche di cooperazione che coinvolgono l'Agenzia Europea per la Difesa (AED), l'Agenzia dell'UE per la Cybersicurezza (ENISA) ed Europol collocandole all'interno della strategia di sicurezza dell'Unione adottata dalla Commissione europea e il Servizio Europeo per l'Azione Esterna già dal dicembre 2020.

Per l'Unione e per gli Stati membri, infatti, l'obiettivo di una cybersicurezza e cyberdifesa credibili è quello, come visto, di promuovere un cyberspazio aperto, libero, stabile e sicuro. Uno spazio digitale nel quale sia i diritti umani, che le libertà fondamentali quanto lo Stato di diritto trovino rispetto e garanzia a favore della stabilità delle comunità, della loro crescita economica, della ricchezza e dell'integrità e solidità delle istituzioni libere e democratiche che contraddistinguono l'Unione e ogni Stato membro. Per fare questo, l'Unione europea si avvale, nel poter condurre con successo gli sforzi diretti verso una maggior sicurezza digitale, di un pacchetto di strumenti della diplomazia informatica che si risolve in quella «Diplomazia digitale» dell'UE all'interno e per mezzo della quale il Consiglio concorda un approccio europeo più concertato alle sfide poste dalle nuove tecnologie digitali, dal momento che

[8] https://www.consilium.europa.eu/it/policies/a-digital-future-for-europe/. Vedasi anche *Europe's Digital Decade*: *Digital Targets for 2030*, in https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it.

> Le tecnologie digitali hanno portato nuove opportunità e nuovi rischi nelle vite dei cittadini dell'UE e delle persone in tutto il mondo,

perché

> Sono diventate anche parametri competitivi fondamentali che possono modificare gli equilibri geopolitici di potere[9].

Anzi, in questo senso si ritiene che la stessa diplomazia digitale sia un aspetto fondamentale per attribuire successo a quella *Global Gateway Strategy* per la quale connessioni sostenibili e affidabili funzionano per le persone e il pianeta, aiutano ad affrontare le sfide globali più urgenti, dalla lotta al cambiamento climatico, al miglioramento dei sistemi sanitari e al rafforzamento della competitività e della sicurezza delle catene di approvvigionamento globali[10].

Un altro aspetto affrontato dal Consiglio in materia di cybersicurezza è rappresentato dall'approvazione il 2 dicembre 2020 di conclusioni nelle quali, riconoscendo il crescente utilizzo di prodotti di consumo e dispositivi industriali connessi a Internet - e i relativi nuovi rischi per la vita privata, la sicurezza delle informazioni e la sicurezza informatica - si sottolineava l'importanza di valutare la necessità di definire una sorta di legislazione orizzontale a lungo termine per affrontare tutti gli aspetti pertinenti della cybersicurezza dei cosiddetti «dispositivi connessi» quali disponibilità, integrità e riservatezza. I «dispositivi connessi», comprese le macchine, i sensori e le reti che compongono l'Internet delle cose (IoT), infatti, saranno quelli che, nel quadro di una sicurezza intesa come valore, assumeranno un ruolo chiave nel definire il futuro digitale dell'Europa, così come la loro stessa sicurezza.

In virtù di tale consapevolezza, l'11 dicembre 2020 il Consiglio e il Parlamento europeo raggiungevano un accordo provvisorio su una proposta rivolta a istituire il Centro Europeo di Competenza industriale, Tecnologica e di Ricerca sulla Cybersicurezza ivi compresa una rete di centri nazionali di coordinamento. Lo scopo di tale nuova architettura era ed è quello di proteggere il mercato unico digitale nei settori dell'e-commerce, della mobilità intelligente e, ovviamente, dell'Internet delle cose.

[9] https://www.consilium.europa.eu/it/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/.

[10] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en.

Una necessità ritenuta fondamentale per aumentare l'autonomia dell'Unione nel settore della sicurezza informatica. Uno strumento ritenuto indispensabile e non rinviabile per sostenere quella strategia per la cybersicurezza che ha lo scopo di garantire un Internet globale e aperto, offrendo nel contempo un meccanismo di salvaguardia, non solo per garantire la sicurezza, ma anche per proteggere i valori europei e i diritti fondamentali di tutti che si possono declinare come resilienza, sovranità tecnologica e leadership.

E, proprio su tale traccia, il Centro Europeo di Competenza Industriale, Tecnologica e di Ricerca sulla Cybersicurezza diventa il depositario della responsabilità di migliorare il coordinamento della ricerca e dell'innovazione. Il Cybersecurity Competence Center con sede a Bucarest, infatti, avrebbe ottenuto il via libera dal Consiglio il 20 aprile 2021. L'UE si riteneva così pronta a rafforzare la sicurezza di Internet e di altre reti e sistemi informativi critici istituendo tale Centro con lo scopo, in particolare, di razionalizzare e dare unicità di indirizzo agli investimenti nella ricerca, nella tecnologia e nello sviluppo industriale sulla cybersicurezza. Il nuovo organismo, avrebbe dovuto gestire i finanziamenti legati alla sicurezza informatica provenienti dai programmi «Orizzonte Europa» e «Europa digitale» (DIGITAL-Europe Program)[11].

Altro aspetto interessante, fu la necessità espressa dal Consiglio il 15 dicembre 2020, di rafforzare la resilienza per contrastare le minacce ibride, compresa la disinformazione osservando che le nuove tecnologie e le crisi offrono agli attori ostili grandi occasioni e opportunità per espandere le proprie attività di interferenza con la governance dell'Unione e degli

[11] «Orizzonte Europa» è il programma quadro di ricerca e innovazione (R&I) dell'Unione europea per il periodo 2021-2027. L'obiettivo del programma «è rafforzare la base scientifica e tecnologica dell'UE, anche sviluppando soluzioni per affrontare priorità strategiche come le transizioni verde e digitale. Il programma contribuisce inoltre al conseguimento degli obiettivi di sviluppo sostenibile e rafforza la competitività e la crescita. Costituisce l'iniziativa di punta dell'UE a sostegno della R&I, dall'ideazione al mercato». Le dotazioni di Orizzonte Europa ammontano a 95,5 miliardi di euro, di cui 5,4 miliardi di euro provenienti da «Next Generation EU». Il programma integra i finanziamenti nazionali e regionali in R&I. «Orizzonte Europa» è la continuazione del precedente programma «Orizzonte 2020» dell'UE. Così in https://www.consilium.europa.eu/it/policies/horizon-europe/. «Europa Digitale» (DIGITAL Europe Program) è un programma di finanziamento rivolto a promuovere la tecnologia digitale all'interno delle imprese, ai cittadini e alle pubbliche amministrazioni. Cfr.: https://digital-strategy.ec.europa.eu/it/activities/digital-programme.

Stati membri, oltre che incidere sul quotidiano di ogni cittadino europeo. D'altronde, come riconosciuto dal Consiglio, la stessa esperienza pandemica ha dimostrato quanto e in che misura sia l'Unione europea nel suo insieme che gli Stati membri singolarmente considerati fossero e siano vulnerabili alle minacce ibride. Minacce, queste ultime, che ricorrono alla diffusione della disinformazione, delle interferenze manipolative e che richiedono misure condivise di contrasto alle attività informatiche dannose ricorrendo ad approcci globali che implichino una cooperazione e un coordinamento efficaci.

In questa prospettiva, il 22 marzo 2021, sempre il Consiglio avrebbe adottato delle conclusioni sulla strategia dell'Unione per il cosiddetto «Decennio digitale». Una strategia già presentata dalla Commissione europea e dall'Alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza nel dicembre 2020 e che descriveva e disegnava un quadro d'azione dell'Unione rivolto a proteggere i cittadini e le imprese dalle minacce informatiche, promuovere sistemi di informazione sicuri e un mondo globale e aperto in un cyberspazio libero e sicuro.

D'altronde, i dispositivi connessi - compresi i macchinari, i sensori e le reti che costituiscono l'Internet delle cose (IoT) - e la loro sicurezza come si è visto, svolgeranno un ruolo chiave nel plasmare ulteriormente il futuro digitale dell'Europa e per questo, sin dal dicembre 2020, il Consiglio ha adottato conclusioni in cui si riconoscono l'utilizzo crescente di prodotti di largo consumo e dispositivi industriali connessi a Internet e i relativi nuovi rischi per la vita privata, la sicurezza delle informazioni. Le conclusioni, ancora una volta, individuano le priorità in termini di sicurezza digitale mettendo al centro, ad esempio, non solo la necessità di rafforzare la competitività globale del settore dell'Internet delle cose, ma anche la garanzia di poter contare in ogni momento, e ad attacco dato, sui più elevati standard di sicurezza, protezione e resilienza.

Cybercrime e dintorni

Tutte queste sfide per il Consiglio richiedono un rafforzamento della capacità di compiere scelte autonome nel settore della cybersicurezza, con l'obiettivo di rendere più forte e credibile la leadership digitale e le capacità strategiche dell'UE. Anche nel campo della lotta al cybercrime e, in particolar modo, contro i reati di abusi su minori, Consiglio e Parlamento europeo il 29 aprile 2021 concludevano un accordo su misure temporanee,

ma necessarie, in materia di contrasto ai reati relativi all'abuso sessuale di minori, con provvedimenti mirati a controllare i sistemi di messaggistica al fine di individuare, e contrastare, le modalità di adescamento attraverso il web. Conclusioni non solo di indirizzo perché si sarebbe aggiunto, nel frattempo, il Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio del 14 luglio 2021 relativo a una deroga temporanea a talune disposizioni della Direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero, per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori.

Ferme restando le iniziative nel campo della sicurezza sul cybercrime, il Consiglio Trasporti, Telecomunicazioni ed Energia il 3 dicembre 2021, concordando la sua posizione sulla nuova Direttiva sulla cybersicurezza, affermava la necessità che maturasse un approccio generale sulle misure per un elevato livello comune di sicurezza informatica in tutta l'UE nell'ambito di quella che sarebbe stata la Direttiva NIS 2.

Lo scopo della nuova versione della NIS era quello di migliorare, ulteriormente, la resilienza e la qualità di risposta agli incidenti sia nel settore pubblico che in quello privato e nell'Unione nel suo insieme, cercando di eliminare le divergenze nei requisiti di sicurezza informatica e nell'attuazione nei diversi Stati membri e a rafforzare la sicurezza e la resilienza nello spazio digitale dell'UE. Certo, lo sforzo normativo non sarebbe stato semplice non solo perché si trattava di raccordare legislazioni nazionali, seppure emanate nell'ordine di una comune *policy* definita dalla Direttiva precedente. Ma perché, la frammentazione delle normative nazionali che tentavano di restare al passo con l'evoluzione delle minacce avrebbe richiesto, e in buona misura richiederebbe ancora oggi, una razionalizzazione dell'assetto giuridico europeo magari attraverso un Regolamento nel quale ogni aspetto che rientri nella cybersicurezza trovi una disciplina organica nel presente e prontamente aggiornabile in ogni sua parte nel futuro prossimo.

Anche in questo caso, il settore del cybercrime si pone come amplificatore di necessità. Infatti, era ed è evidente che una strategia di cybersicurezza non può non tener conto dell'evoluzione del crimine organizzato non solo negli interessi da perseguire, ma di come perseguirli nel tempo con norme adeguate, condivise e organiche. Una necessità di unità di normazione e di applicazione che deve considerare quanto la criminalità in-

formatica rappresenti un ambito nel quale il modus operandi si caratterizza per una fluidità intrinseca, interpretabile in diversi modi dal momento che il crimine non potrà che essere sempre più digitale nei suoi diversi aspetti. Ciò significa che - dal ricorrere a *malware* per poter controllare device personali per sottrarre dati o comprometterne l'uso, o per distribuire contenuti illegali o diffondere notizie false, vendere beni illeciti o promuovere comportamenti illeciti che vedono come vittima i minori - l'idea che il cyberspazio sia la dimensione della minaccia futura rappresenta la vera sfida dei prossimi anni e che diventerà una costante per ogni *policy* posta a premessa di una strategia comune.

Proprio in tale prospettiva, Europol ha istituito un Centro europeo per la lotta alla criminalità informatica specializzato quale supporto ai membri dell'Unione per poter indagare al meglio i reati sommersi in rete e disarticolare le organizzazioni criminali responsabili. A favorire questo, interviene, infatti, lo European Multidisciplinary Platform Against Criminal Threats (EMPACT), quale strumento per identificare, definire ed affrontare le principali minacce poste all'Unione dalla criminalità organizzata e dalle forme gravi di criminalità internazionale superando, così, l'EU-*Policy Cycle* del 2010 (Ciclo politico dell'UE per la criminalità organizzata e le forme gravi di criminalità internazionale) strutturato nel garantire, in un ciclo distribuito su quattro anni, continuità ed efficacia nella lotta contro le forme gravi di criminalità internazionale e organizzata[12].

Resistenza resiliente

Insomma, che la sfida della cybersicurezza si giochi tutta nella capacità di esprimere una credibile e efficace resilienza informatica è cosa ormai ben definita, come campo prioritario da disciplinare e settore nel quale indirizzare gli sforzi non solo normativi, ma anche finanziari per poter offrire prodotti con elementi digitali più sicuri[13]. A tal proposito e circa la sicurezza dei prodotti informatici, la Commissione aveva già presentato il 15 settembre 2022 una proposta di Regolamento (*European Cyber Resilience Act*) circa i requisiti orizzontali di sicurezza digitale per i prodotti

[12] Vedasi anche, https://www.interno.gov.it/it/ministero/osservatori-commissioni-e-centri-coordinamento/european-multidisciplinary-platform-against-criminal-threats-empact.

[13] La Commissione ha indicato in 5.5 trilioni di euro nel 2023 l'ammontare dei profitti che il cybercrime otterrà a condizioni date di difesa e resilienza.

con elementi digitali. Una proposta a modifica del Regolamento (UE) 2019/1020[14]. Per la Commissione, i prodotti hardware e software sono sempre più soggetti ad attacchi informatici con una stima di danni calcolati già allora in 5.500 miliardi di euro.

Per la Commissione, infatti, i problemi presentati da tali prodotti non sottoposti preventivamente a un controllo sulla sicurezza del software ivi allocato o anche esterno sono rappresentati da

> Un basso livello di cybersicurezza, testimoniato da vulnerabilità diffuse,

e

> Dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per porvi rimedio e da una insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori, che impediscono loro di scegliere prodotti con proprietà di cybersicurezza adeguate o di utilizzarli in modo sicuro.

Per la Commissione, ancora,

> In un ambiente connesso un incidente di cybersicurezza in un prodotto può pregiudicare una intera organizzazione o una intera catena di approvvigionamento, spesso propagandosi attraverso le frontiere del mercato interno nel giro di pochi minuti,

rappresentando, in questo modo, un elemento perturbatore delle transazioni economiche e/o commerciali sino a potersi trasformare in una minaccia letale[15].

A tale proposta, il 18 aprile 2023, la Commissione europea ha fatto seguire una ulteriore proposta di Regolamento, l'EU-*Cyber Solidarity Act*, per migliorare la preparazione, l'individuazione e la risposta agli incidenti di sicurezza informatica nell'Unione[16]. Il documento ha lo scopo di perfezionare le capacità dell'Ue di individuare, prepararsi e rispondere a minacce

[14] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0454&qid=1667215475863&from=EN.

[15] La Commissione, all'interno del preambolo della proposta di Regolamento, non lesinava di indicare alcuni esempi di attacchi informatici condotti su vasta scala. In particolare vengono citati il *worm ransomware* WannaCry, che ha sfruttato una vulnerabilità di Windows, colpendo, nel 2017, 200.000 computer in 150 paesi e provocando danni per miliardi di dollari e l'attacco alla catena di approvvigionamento di Kaseya VSA. Un attacco condotto con un software di amministrazione di rete di Kaseya per attaccare oltre 1000 imprese e costringendo una catena di supermercati a chiudere tutti i suoi 500 negozi in Svezia, cui si aggiungerebbero i numerosi attacchi condotti ai danni delle applicazioni bancarie per rubare denaro a consumatori ignari.

[16] https://www.eu-cyber-solidarity-act.com/.

e attacchi alla sicurezza informatica su larga scala. La proposta così presentata dalla Commissione prevede una sorta di «scudo europeo» composto da centri operativi per la cybersicurezza e rivolto a realizzare un'architettura di centri operativi interconnessi prevedendo un meccanismo globale di emergenza per migliorare la posizione informatica dell'Unione europea[17]. Il documento prevede un meccanismo di emergenza informatica destinato a garantire il miglioramento della preparazione e della risposta agli incidenti di sicurezza informatica, sostenendo azioni di preparazione attraverso il testing di operatori in settori cruciali come la finanza, l'energia e la sanità per individuare *bug* che potrebbero renderle vulnerabili alle minacce informatiche.

A ciò segue la creazione di una riserva di cybersicurezza dell'Unione europea rappresentata da servizi di risposta agli incidenti offerti da fornitori di servizi privati di fiducia, attivabili su richiesta degli Stati membri o delle istituzioni, degli organi o delle agenzie dell'Unione, per affrontare questioni significative o incidenti di sicurezza informatica su larga scala. Il meccanismo prevede, ovviamente e coerentemente con la *policy* di creare una risposta univoca e determinante ad attacchi che coinvolgono asset europei e degli Stati membri, una mutua assistenza che vede sostenere lo Stato membro che offre assistenza reciproca a un altro Stato membro colpito da un attacco alla propria sicurezza informatica. A completare tale «scudo difensivo» (*cyber shield*) la Commissione, nella proposta di Regolamento, introduce anche un ulteriore meccanismo di revisione degli incidenti di sicurezza informatica per valutare ed esaminare specifici casi[18].

[17] Lo «Scudo informatico europeo» (*cyber shield*) sarà composto da «Centri operativi di sicurezza» (SOC) in tutta l'UE, riuniti in diverse piattaforme SOC multinazionali, realizzate con il supporto del «Programma Europa Digitale» (DEP) per integrare i finanziamenti nazionali. Il «Cyber Shield» avrà il compito di migliorare il rilevamento, l'analisi e la risposta alle minacce informatiche. Questi SOC utilizzeranno tecnologie avanzate come l'Intelligenza Artificiale e l'analisi dei dati per rilevare e condividere avvisi su tali minacce con le autorità oltre confine. Consentiranno una risposta più tempestiva ed efficiente alle principali minacce. Durante una prima fase, avviata nel novembre 2022, sono stati selezionati tre consorzi di centri operativi di sicurezza (SOC) nell'ambito del programma «Europa Digitale» (DIGITAL-EU).

[18] Il Meccanismo di revisione degli incidenti di sicurezza informatica opererebbe su richiesta della Commissione o delle autorità nazionali (attraverso la rete EU-CyCLONe o CSIRT). L'Agenzia dell'UE per la cybersicurezza (ENISA) sarà responsabile dell'esame di specifici incidenti significativi o su larga scala e dovrebbe fornire una relazione che includa lezioni apprese e, se del caso, raccomandazioni per migliorare la risposta informatica dell'Unione.

NIS 1 e …2

Al netto delle misure prese dall'Unione, si comprende che al centro della strategia di contenimento, contrasto e reazione nei vari ambiti di decisione viene a collocarsi il valore della capacità di resilienza esprimibile rappresentando, questa, il vero fattore-guida per realizzare un cyberspazio comune caratterizzato da una cyberdifesa credibile non solo delle infrastrutture, ma di ogni patrimonio informativo e informazionale che riguarda l'UE, gli Stati membri e i cittadini dell'Unione. Non per nulla il concetto di resilienza si ripropone in molti documenti dell'Unione come, ad esempio, l'EU-*Ministers United in Strengthening Cyber Resilience in the EU* dell'8 marzo 2022, o il *Digital Operational Resilience Act* (DORA), accordo provvisorio dell'11 maggio 2022. Un documento, quest'ultimo, attraverso il quale si pongono norme ritenute necessarie per garantire che il settore finanziario in Europa sia in grado di mantenere operazioni resilienti seppur di fronte a gravi interruzioni operative.

Lo scopo del DORA, infatti, è quello di creare un quadro normativo sulla resilienza operativa digitale in base al quale tutte le aziende devono assicurarsi di poter resistere, rispondere e riprendersi da tutti i tipi di interruzioni e minacce legate all'ICT. All'adozione del DORA, segue il 13 maggio il documento *Rafforzare la cyber sicurezza e la resilienza dell'UE* quale accordo comune sulla Direttiva NIS 2, oltre ai provvedimenti del Consiglio orientati a prorogare il regime sanzionatorio nei confronti degli attacchi informatici del 16 maggio e un successivo accordo del 23 maggio in materia di cyberspazio. Un accordo, il cui scopo è quello di rafforzare la cybersicurezza dello spazio dell'Unione e prevenire attacchi informatici soprattutto a fronte della nuova crisi russo-ucraina e che faceva seguito a una riunione informale organizzata dalla presidenza francese del Consiglio l'8 e il 9 marzo 2022. Riunione nel corso della quale, ancora una volta, i ministri dell'Unione responsabili delle telecomunicazioni e degli affari digitali, ponevano sul tavolo di lavoro i modi per rafforzare e accelerare il ritmo della cooperazione europea nel settore della sicurezza informatica, a seguito dell'aumento dei livelli di minaccia informatica, aggravati dalla situazione in Ucraina e dal rischio di incidenti anche all'interno della stessa UE.

Il risultato sarebbe stato una richiesta di maggiore informazione sui rischi che minacciano le reti e le infrastrutture di comunicazione europee e raccomandazioni su come rafforzare la loro resilienza crisi durante. Insomma, è evidente che l'obiettivo sempre più stringente nei termini e nei

tempi, così come definito il 13 maggio 2022, doveva essere quello di rafforzare la sicurezza e la resilienza digitale a livello UE. Un obiettivo che giustifica oggi il superamento della vecchia normativa NIS 1 per giungere alla nuova Direttiva NIS 2. In questo senso, come visto, il Consiglio e il Parlamento europeo hanno raggiunto un accordo provvisorio sulle misure per garantire un elevato standard comune di sicurezza informatica in tutta l'Unione, per migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti sia del settore pubblico che di quello privato e dell'Unione nel suo insieme.

Una volta adottata, la nuova Direttiva, denominata NIS 2, che avrebbe sostituito la NIS 1 sulla sicurezza dalle reti e dai sistemi informativi, avrebbe offerto un nuovo impianto normativo a riguardo che dovrebbe garantire una gestione e una cooperazione più forte circa la prevenzione e il contenimento dei rischi e degli incidenti. Così come, nell'approvare una proroga di ulteriori tre anni al regime sanzionatorio in materia di attacchi informatici, il Consiglio nel maggio 2022 decideva di voler rafforzare ulteriormente la sicurezza digitale dell'UE e prevenire gli attacchi informatici approvando delle conclusioni sullo sviluppo della postura informatica dell'Unione, che riguardavano la forza complessiva di tutela e la resilienza rispetto alle minacce informatiche.

Era evidente che le conclusioni derivavano da diversi provvedimenti e politiche dell'Unione, tra cui, in particolare la «EU-*Strategic Compass*» come il «Piano d'Azione dell'UE» per rafforzare la politica di sicurezza e difesa entro il 2030. Tuttavia, la crisi russo-ucraina apertasi dalla fine del febbraio 2022 ha fatto sì che il 21 giugno 2022 il Consiglio adottasse delle conclusioni questa volta rivolte a permettere all'UE di dare una risposta coordinata a possibili campagne di cyber-aggressione. Nel contesto della crisi russo-ucraina, e in seguito all'approvazione della EU-*Strategic Compass* da parte del Consiglio europeo del precedente 24 e 25 marzo, il Consiglio dell'UE ha ribadito nelle sue conclusioni l'importanza di sviluppare un pacchetto di strumenti ibridi. Questo pacchetto di strumenti introduceva una risposta coordinata alle minacce e alle campagne ibride che avrebbero potuto colpire l'Unione europea e i suoi partner. Riuniva tutti gli attori, le politiche e gli strumenti adeguati e utili a contrastare l'impatto delle minacce ibride in modo più coordinato e, quindi, più efficace.

Da parte sua il Consiglio, nella sua veste di organo intergovernativo, ha comunque ribadito che la responsabilità di contrastare le minacce ibride

rimaneva a capo degli Stati membri, anche se non ha mancato di ricordare che le decisioni su una risposta coordinata dell'Unione a una minaccia ibrida hanno come scopo finale quello di proteggere la democrazia e il diritto internazionale, oltre che garantire nel tempo il raggiungimento degli obiettivi dell'Unione. Per questo, ogni risposta dovrà essere proporzionata a ogni minaccia e dovrà essere sostenuta da una consapevolezza della situazione, valutare le condizioni di crisi e il contesto, rispettare il diritto internazionale e proteggere i diritti e le libertà fondamentali.

Anche l'universo dei social, come quello dell'e-commerce rappresentava un altro ambito nel quale l'Unione cercava una propria sicurezza digitale. Così, il 19 ottobre 2022, infatti, veniva approvato il *Digital Service Act* (DSA), Regolamento (UE) 2022/2065, entrato in vigore il 25 agosto 2023, relativo a un mercato unico dei servizi digitali e che modificava anche i contenuti della Direttiva 2000/31/CE[19]. Il Regolamento, rappresenta una nuova versione in materia di servizi intermediari di trasmissione o memorizzazione dell'informazione (piattaforme, motori di ricerca, hosting) offerti a destinatari situati in Unione europea.

La necessità di dotarsi di un Regolamento di questa portata, preliminarmente all'introduzione della NIS 2, è stata determinata dal fatto di dover porre in essere norme e modalità utili a contrastare i contenuti illeciti presenti sulle diverse piattaforme non solo di e-commerce, ma anche sul piano della lotta alla disinformazione. Gli obblighi derivanti per le piattaforme digitali sono contenuti in cinque capitoli, ognuno dei quali tende a individuare i destinatari, le relative responsabilità ed esenzioni, il quadro di cooperazione tra la Commissione e le Autorità nazionali.

Tra gli obblighi previsti si possono elencare quello di trasparenza, il prevedere meccanismi utili a segnalare da parte dell'utenza ai prestatori di servizi la presenza di informazioni dai contenuti illegali e, a fronte di ciò, l'obbligo del titolare delle pagine web di porre le limitazioni/restrizioni che dovranno essere chiaramente specificate circa la loro visibilità e la loro possibile rimozione nel caso, appunto, di segnalazione da parte dell'utente/destinatario. A questi si aggiungono la sospensione e/o limitazione anche dei relativi pagamenti, se non la cessazione del servizio fornito o la chiusura dell'account del destinatario, l'obbligo di indicare la prevista moderazione delle pagine purché ciò sia motivato e contestabile da parte dell'utenza.

[19] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065&from=EN.

Inoltre, per quanto riguarda la profilazione, è fatto obbligo di segnalare la possibilità offerta all'utente di accettare o negare la profilazione.

In ogni caso, l'aspetto singolare del DSA è il prevedere una eccezione, o esenzione se si vuole, dalla responsabilità condizionale per la quale, qual ora sia reso noto un contenuto illegale ospitato sulla piattaforma a insaputa del gestore, questi non ne è responsabile se non nella misura in cui, una volta nota l'illiceità dell'informazione, non provveda alla sua eliminazione. Tuttavia, ben due giorni prima, il 17 ottobre, il Consiglio avrebbe adottato delle conclusioni anche sulla sicurezza della catena di approvvigionamento delle tecnologie dell'informazione e della comunicazione (TIC) dell'Unione. Altro aspetto sensibile se non determinante, circa la ricerca di un'autonomia strategica in campo digitale dell'UE che sarebbe confluito nella Direttiva NIS 2.

In questo senso, le conclusioni affrontavano, in particolare, le dipendenze nelle catene di approvvigionamento delle TIC. Il Consiglio, infatti, chiedeva adeguamenti ai quadri di controllo degli appalti pubblici o degli investimenti esteri diretti, compresi i criteri di selezione relativi alla sicurezza informatica. In tale prospettiva, proprio gli Stati membri avevano già chiesto alla Commissione di pubblicare delle linee guida per incoraggiare le amministrazioni aggiudicatrici a porre la dovuta attenzione alle pratiche di sicurezza informatica nel campo degli appalti e dei subappalti di servizi.

Le conclusioni dell'ottobre 2022 hanno avuto il merito di individuare una nuova disciplina organica che si occupasse di sicurezza della catena di approvvigionamento delle TlC, della revisione della Direttiva sulla sicurezza delle reti informatiche che sarebbe confluita nella nuova Direttiva NIS 2, prevedendo nuovi schemi di certificazione; il tutto, rivolto a definire una nuova proposta di regolamento sulla resilienza informatica.

Così, prima di giungere all'adozione della nuova Direttiva sulla cybersicurezza e la resilienza NIS 2, il 14 dicembre 2022 sarebbe stata emanata la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza recante la modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abrogava, appunto, la Direttiva (UE) 2016/1148. Rispetto alla NIS 1, la nuova Direttiva pone l'attenzione ancora una volta, ma con più assertività nelle previsioni, sulla resilienza delle entità critiche che coprono un'ampia gamma di settori nel tentativo di superare ambiti interpretativi nazionali troppo ristretti. Ambiti, ritenuti poco inclini a definirsi

in un quadro strategico di risposta e di provvedimenti che dovrebbero implementarsi in un regime europeo.

Se per certi versi entrambe le Direttive tendono a porre in essere misure idonee ad affrontare rischi presenti e futuri, online o offline, la NIS 2 riduce l'autonomia degli Stati nel tentativo di ricondurre la risposta su una unica capacità di difesa affinché in caso di attacchi cibernetici dovuti alla criminalità o ai disastri naturali, si possa reagire, ogni Stato membro, in maniera coerente e, soprattutto, complementare. Inoltre, la NIS 2 tende a sopperire al fatto che con la precedente Direttiva, vi fosse una quasi assente condivisione delle informazioni per affrontare le crisi in modo congiunto, oltre a porre un termine di notifica di 24 ore dal verificarsi di incidenti o sospetti di attacchi per definire una risposta comune adeguata.

La NIS 2, inoltre, sottrae agli Stati membri il compito di identificare i cosiddetti «operatori di servizi essenziali» (OSE) che saranno, e sono, al contrario e per coerenza con la *policy* cui si ispira la Direttiva, determinati da quest'ultima[20]. Ciò vuol dire, attribuire capacità di gestione e di risposta condivise secondo profili e strategie univoche. Strategie idonee, soprattutto, ad abbattere i tempi di scoperta, definizione e risposta a una minaccia cyber, aumentando a proprio favore le capacità di governo degli ambiti pubblici e privati più sensibili per una comunità, quali le amministrazioni pubbliche, laboratori di ricerca, trasporti e reti energetiche, con lo scopo non solo di poter disporre di uno scudo adeguato ma, in particolare, di rendere le architetture digitali il più impermeabili possibili a mi-

[20] La normativa italiana di recepimento definisce molto precisamente cosa si intende per soggetto che svolge funzioni essenziali. L'essenzialità è rappresentata dal fatto che l'operatore svolge una «funzione essenziale» dello Stato perché l'ordinamento gli ha attribuito compiti e funzioni tali da dover assicurare la continuità dell'azione di governo e degli organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti. In questo senso, un soggetto, pubblico o privato, presta un «servizio essenziale» per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, laddove ponga in essere attività che siano strumentali all'esercizio di funzioni essenziali dello Stato; necessarie per l'esercizio e il godimento dei diritti fondamentali; necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; di ricerca e relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale. Vedasi il Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, *Regolamento in materia di perimetro di sicurezza nazionale. Disposizioni attuative.*

nacce sempre più complesse e veloci[21]. L'art.21, ad esempio, individua i soggetti obbligati fissandone in maniera chiara la responsabilità di dover provvedere a mettere in campo misure e iniziative adeguate in termini operativi e proporzionate al livello di sicurezza e interesse sotteso.

Altra novità della Direttiva NIS 2 è che essa indica anche alcune misure che possono essere prese per prevenire una minaccia come il ricorrere a politiche di analisi dei rischi e di sicurezza dei sistemi informatici; alla gestione degli incidenti; a garantire la continuità operativa, la gestione del backup di ripristino in caso di evento disastroso; la sicurezza della catena di approvvigionamento, compresi gli aspetti riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; strategie e procedure per valutare l'efficacia delle misure di gestione dei

[21] La Direttiva NIS 2 si applica sia ai fornitori di servizi cosiddetti essenziali che dei servizi digitali. Per «servizi essenziali» si individuano: le società di produzione e di distribuzione di energia; i servizi sanitari; i trasporti; le infrastrutture di comunicazione elettronica; i servizi bancari e finanziari, la grande distribuzione alimentare ecc. Per «servizi digitali» si indicano i seguenti: le piattaforme di e-commerce; i motori di ricerca; il *cloud computing*; la gestione dei servizi ICT, della pubblica amministrazione e dello spazio. Tuttavia, la Direttiva NIS 2 introduce anche «altri settori critici» quali i servizi postali e di corriere; la gestione dei rifiuti; la fabbricazione, la produzione e la distribuzione di sostanze chimiche; la produzione, la trasformazione e la distribuzione di alimenti; la fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro; la fabbricazione di computer e prodotti di elettronica e ottica; la fabbricazione di apparecchiature elettriche; la fabbricazione di macchinari e apparecchiature non classificati altrove; la fabbricazione di autoveicoli, rimorchi e semirimorchi; la fabbricazione di altri specifici mezzi di trasporto; i fornitori di servizi digitali; le organizzazioni di ricerca. La Direttiva, inoltre, stabilisce altri nuovi criteri circa gli attori deputati a realizzare il perimetro di sicurezza entro il quale garantire la funzionalità delle infrastrutture critiche. Ad esempio, una delle novità introdotte è la «dimensione del soggetto» quale destinatario della normativa e parte chiamata in causa nella definizione delle strategie e nella messa in campo dei provvedimenti necessari ad assicurare il miglior standard di sicurezza e la migliore capacità di resilienza e risposta. Per la NIS 2, infatti, sono interessati e, quindi, destinatari di norme quei soggetti, pubblici o privati, che ricondotti all'interno delle tipologie ad "alta criticità" o "altri settori critici", prestino i loro servizi o svolgano le loro attività all'interno dell'Unione; siano considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superino i massimali per le medie imprese di cui al paragrafo 1 del medesimo articolo. A questi, si aggiungono anche i fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica offerti al pubblico, i fornitori di servizi di registrazione dei nomi di dominio, alcuni enti della pubblica amministrazione e altri soggetti definiti come "critici" dalla stessa Direttiva (UE).

rischi di sicurezza informatica. Così anche le *best practices* di sicurezza informatica di base e formazione; *policy* e procedure relative all'uso della crittografia; sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione dei varchi attivi; uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno[22].

[22] Il quadro normativo italiano in materia di cybersicurezza ha trovato la sua prima formulazione nel Decreto Legge 21 settembre 2019 n. 105 *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, poi convertito con Legge 18 novembre 2019, n. 133. Un Decreto che sin dall'inizio dimostrava come si trattasse di dover urgentemente aprire un percorso normativo che rivedesse le norme del passato e che si articolava in numerose fonti normative che si sono susseguite fino a oggi. Così, contribuendo a delineare un quadro normativo piuttosto frammentario che richiedeva un necessario intervento di razionalizzazione a beneficio, anzitutto, dei soggetti destinatari di tali previsioni normative. In questo senso, la definizione di un «Perimetro di Sicurezza Nazionale» rappresentava una presa di coscienza sull'importanza di delimitare i confini entro i quali l'interesse del Paese viene messo in gioco e all'interno dei quali impedire se non la penetrazione quanto meno la contaminazione delle infrastrutture digitali. L'articolo 1 del D.L. 21 settembre 2019, n. 105 nell'istituire il «Perimetro di Sicurezza Nazionale Cibernetica», per la prima volta dichiarava l'urgenza e la necessità di assicurare un livello elevato di sicurezza di reti, sistemi informativi e servizi informatici dei soggetti pubblici e privati dai quali dipendono tutte le funzioni di governance dello Stato e le attività di prestazioni di servizi essenziali per poter garantire nel tempo l'erogazione di questi in campo civile, amministrativo, politico, economico e sociale, il cui pregiudizio si trasforma in un pregiudizio per la sicurezza nazionale. Una condizione di necessità ed urgenza definitasi poi con l'istituzione della Agenzia Nazionale per la Cybersicurezza (ANC). Il «Perimetro di Sicurezza Nazionale Cibernetica» prevedeva ben cinque decreti di attuazione attraverso i quali risolvere in senso compiuto il problema della sicurezza nazionale disciplinando i vari aspetti che ne identificano la sua specificità. Il primo, il DPCM n. 131 del 2020 con il quale si definiscono metodi e criteri per l'identificazione di enti e asset parte del Perimetro di Sicurezza Nazionale Cibernetica. Per il decreto, i destinatari del PSNC sono da identificarsi nei soggetti che esercitano una funzione essenziale dello Stato o i soggetti che prestano un servizio essenziale per gli interessi dello Stato «la cui compromissione comporterebbe un problema serio per la sicurezza nazionale». Al precedente è seguito il DPCM 81/2021, con i nuovi obblighi di notifica degli incidenti al CSIRT nazionale (Computer Security Incident Response Team) istituito all'interno della Agenzia Nazionale per la Cybersicurezza, poi il DPCM del 15 giugno 2021 che, assieme al DPR 5 febbraio 2021, n. 54 (cioè, al regolamento recante attuazione dell'articolo 1, comma 6, della Legge "Perimetro") individua le modalità e le procedure relative al funzionamento del Centro di Valutazione e Certificazione Nazionale (CVCN). Seguiva, il DPCM 18 Maggio 2022 n. 92, Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa.

Tutto questo, alla fine, per creare un piano di gestione degli incidenti definendo un *Data Breach Recovery Plan* utile a gestire «incidenti significativi» ovvero,

> Un incidente che ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; o un evento che si è ripercosso sulle strutture di governance o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli[23].

Di certo la crisi russo-ucraina ha fatto da acceleratore sul dover disporre di una visione d'insieme degli attori protagonisti e delle procedure da attuare per garantire la sopravvivenza delle reti sulle quali queste si muovono. A ciò risponde la creazione del Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTS), attribuito al coordinamento lettone e messo in campo come progetto nell'ambito della Cooperazione Strutturata Permanente dell'UE (Permanent Structured Cooperation - PESCO). Insomma, è evidente come si cerchi di creare, attraverso una sinergia favorita da norme di indirizzo comuni, una sorta di «perimetro di sicurezza europeo» ormai ritenuto necessario per accrescere la cyber-resilienza, per combattere la criminalità informatica, rafforzare la diplomazia informatica, intensificare la cyberdifesa, promuovere la ricerca e l'innovazione e, quindi, proteggere le infrastrutture critiche come i trasporti, l'energia, la sanità e la finanza. Ma, ovviamente non tutto si esaurisce con l'adozione della NIS 2.

Il 23 maggio 2023, considerando il cyberspazio come un campo di competizione strategica, i rischi per la sicurezza e la difesa dell'Unione sembravano aumentare di fronte a momenti di crescenti tensioni geopolitiche e alla sempre più ineluttabile dipendenza dalle tecnologie digitali. Il Consiglio, circa la difesa informatica, ha richiamato nuovamente gli Stati membri affinché rafforzino ulteriormente la loro resilienza di fronte alle minacce informatiche, aumentino la sicurezza e la difesa informatica con-

[23] La Direttiva NIS 2 prevede, a tal proposito, un preallarme entro 24 ore da quando si è venuti a conoscenza dell'incidente; una notifica entro 72 ore dalla conoscenza dell'incidente, che aggiorni - se necessario - le informazioni del preallarme; una relazione finale entro un mese dalla trasmissione della notifica, il cui contenuto minimo sarà dettagliato dal legislatore dello Stato membro in fase di recepimento. In caso di minaccia il Data Breach Recovery Plan deve contenere l'indicazione del responsabile della sicurezza informatica; la definizione dei ruoli e delle responsabilità del personale coinvolto nella gestione degli incidenti; la definizione delle procedure da seguire in caso di Data Breach.

tro comportamenti dannosi e atti di aggressione nel cyberspazio. In questo senso, il 26 giugno 2023 il Consiglio dell'UE e il Parlamento europeo, infatti, hanno raggiunto un accordo provvisorio su un quadro comune per la sicurezza informatica delle istituzioni, degli organi e degli organismi dell'Unione europea rivolto a rafforzare il ruolo e le funzioni del CERT-UE. L'accordo dovrebbe contribuire a migliorare la loro resilienza e le capacità di risposta agli incidenti e garantire standard e cooperazione comuni.

Lo scopo dell'accordo provvisorio era, ed è, quello di finalizzarlo a livello tecnico come proposta di Regolamento per poi essere inviato agli ambasciatori presso l'UE per conferma. Una volta confermato sia dal Consiglio che dal Parlamento, entrambe le istituzioni lo avrebbero dovuto adottare formalmente. Nel luglio 2023 i rappresentanti degli Stati membri (COREPER) hanno poi raggiunto una posizione comune sulla proposta legislativa relativa ai cosiddetti «requisiti orizzontali» di cybersicurezza per i prodotti con elementi digitali (proposta di Regolamento sulla resilienza informatica). Le nuove norme proposte mirano a garantire che i prodotti con componenti digitali, come fotocamere domestiche connesse, frigoriferi intelligenti, TV e giocattoli, siano sicuri prima di entrare nel mercato unico dell'UE[24].

Un «Cyber Polygon» per l'UE?

Con l'ulteriore accelerazione della digitalizzazione globale, il mondo sta diventando sempre più interconnesso. Si creano ormai nell'altrove digitale veri e propri ecosistemi dove paesi, aziende e individui stanno approfittando della rapida diffusione di Internet e dei dispositivi intelligenti. In questo contesto, basta un solo anello vulnerabile per far crollare una intera architettura digitale di governance proprio come un effetto domino. Per il World Economic Forum (WEF), un approccio sicuro allo sviluppo digitale oggi determinerà il futuro dell'umanità per i decenni a venire.

In questa prospettiva da qualche anno a questa parte proprio su iniziativa del WEF si è organizzato un «Cyber Polygon». Ovvero, un evento unico sulla sicurezza informatica proposto in una formula *combined* mettendo insieme, infatti, la più grande formazione tecnica al mondo per i team aziendali e una conferenza online con alti funzionari di organizzazioni internazionali e aziende leader. Ogni anno, l'esercitazione vede riunirsi

[24] http://documenti.camera.it/leg19/dossier/pdf/ES027.pdf.

un'ampia gamma di aziende globali e strutture governative, mentre lo *streaming live* riunisce milioni di spettatori da tutto il mondo.

Gli obiettivi strategici di Cyber Polygon sono quelli di: favorire una consapevolezza e una capacità di valutazione pubblica e privata alle diverse forme organizzative sulla propria capacità di resilienza informatica; scambiare le migliori pratiche e portando risultati concreti e di interesse per la comunità globale; sviluppare le competenze dei team nel respingere gli attacchi informatici; espandere la conoscenza pratica degli specialisti tecnici; coinvolgere il management delle organizzazioni e delle società internazionali nel dialogo sulla sicurezza informatica, sensibilizzandone l'opinione pubblica[25].

Non ci sono dubbi, infatti, che colpire le cosiddette *supply chains*, ovvero le catene di approvvigionamento che permettono di portare sul mercato un prodotto o rendere disponibile un servizio, rappresenta uno degli obiettivi preferiti sia che si tratti di attacchi *ransomware* da *cybercrime* che propriamente riconducibili ad attività di *cyberwarfare*. Ciò significa che la tendenza globale verso lo sviluppo di ecosistemi all'interno della comunità imprenditoriale non può non dirigersi verso le vulnerabilità possibili delle *supply chains* e tutto ciò richiederà non solo capacità di prevenzione e contrasto ma, soprattutto, di riduzione del rischio o dei danni qual ora l'attacco si fosse già manifestato.

La domanda che sembra essere la più interessante allora è quella posta da Bernard Marr su «Forbes» del 6 febbraio 2023: *Cyber Apocalypse 2023: Is The World Heading for a "Catastrophic" Event?*[26] Infatti, il meeting annuale del 2023 del World Economic Forum, si è concluso a Davos, in Svizzera, con una previsione inquietante da parte di una delle voci più autorevoli. Nel corso di una presentazione del rapporto *Global Cybersecurity Outlook 2023*, l'amministratore delegato del forum Jeremy Jurgens ha rivelato che il 93% degli intervistati ritiene che un evento catastrofico di sicurezza informatica sia probabile nei prossimi due anni. Infatti, per il Rapporto, la criminalità informatica entro il 2025 dovrebbe costare all'economia mondiale circa 10,5 trilioni di dollari all'anno, in aumento rispetto ai 3 trilioni di dollari del 2015 secondo «Cybersecurity Ventures»[27].

[25] «Cyber Polygon» rientrava in una iniziativa di BI.ZONE sino al 2021 (visto che la società ha sede a Mosca) supportata dal World Economic Forum Center for Cybersecurity.

[26] https://www.forbes.com/sites/bernardmarr/2023/02/06/cyber-apocalypse-2023-is-the-world-heading-for-a-catastrophic-event/.

[27] https://cybersecurityventures.com/cybersecurity-almanac-2023/

D'altra parte, solo nelle possibilità offerte dalla rete di poter mettere in campo operazioni di *cyberlaundering*, ovvero di riciclaggio di denaro proveniente da attività illecite, si comprende perché la capacità di operare sulle diverse piattaforme permette di accelerare le operazioni di collocazione di capitali in tempi rapidi, ostacolandone la tracciabilità. Insomma, se si volessero contestualizzare tali cifre si potrebbe dire, come rilevato dallo stesso Report, che il *cybercrime* varrebbe da solo ben il terzo PIL più grande al mondo dopo Stati Uniti e Cina. È evidente che i fattori determinanti una simile crescita del volume d'affari da parte delle organizzazioni di *cybercrime* sia dovuto alla progressiva digitalizzazione delle società e ai cambiamenti nelle abitudini che sottendono ormai una digitalizzazione del quotidiano, oltre a condizioni di instabilità politica e le diverse e distribuite aree di crisi che favoriscono utili condizioni di recessione economica internazionale[28]. Tra le minacce più rilevanti sottolineate dal Rapporto del WEF del 2023 vi sarebbe una minaccia *mutante*. Ovvero, una minaccia che potrebbe assumere la forma di un virus abilitato dall'Intelligenza Artificiale che si trasforma mentre infetta vari sistemi e organizzazioni per eludere i sistemi di difesa o addirittura il rilevamento[29].

[28] S. Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, in «Special Report». *Cyberwarfare In The C-Suite*. Consultabile in: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.

[29] T. Newcombe, *A Catastrophic Mutating Event Will Strike the World in 2 Years, Report Says*, January25,2023,inhttps://www.popularmechanics.com/technology/security/a42660926/global-catastrophic-mutating-event-coming-in-2-years/.

IV. Il tempo dell'Intelligenza Artificiale

> Semplificherà le cose per il lettore se spiegherò prima le mie convinzioni in merito. La domanda originale "Possono pensare le macchine?" Credo sia troppo priva di significato per meritare una discussione. Tuttavia, credo che alla fine del secolo l'uso delle parole e l'opinione generale colta saranno cambiati a tal punto che si potrà parlare di macchine pensanti senza aspettarsi di essere contraddetti.
>
> Alan M. Turing, *Computing machinery and intelligence.* In «Mind», A Quarterly Review of Psychology and Philosophy, October 1950

In *The AI Power Paradox Can States Learn to Govern Artificial Intelligence - Before It's Too Late?* Pubblicato in «Foreign Affairs» nell'agosto 2023, Ian Bremmer e Mustafa Suleyman sottolineavano come nel 2035, l'Intelligenza Artificiale (IA) sarà ovunque e, per questo, si chiedevano, se gli Stati possono imparare a governarla prima che sia troppo tardi. Per gli autori, infatti, se solo un anno fa un simile scenario sarebbe sembrato frutto di una previsione ottimistica almeno nei tempi, oggi sembra quasi inevitabile. I sistemi di Intelligenza Artificiale Generativa, infatti,

> Possono già scrivere in modo più chiaro e persuasivo della maggior parte degli esseri umani e possono produrre immagini, opere d'arte e persino codici informatici originali basati su semplici istruzioni linguistiche.

Per gli autori, insomma,

> L'Intelligenza Artificiale generativa è solo la punta dell'iceberg. Il suo arrivo segna un momento di Big Bang, l'inizio di una rivoluzione tecnologica che cambierà il mondo e rimodellerà la politica, le economie e le società.

Insomma, ancora,

> Come le ondate tecnologiche del passato l'Intelligenza Artificiale abbinerà una crescita e opportunità straordinarie a disagi e rischi immensi. Ma

[1] Cfr. I. Bremmer, M. Suleyman, *The AI Power Paradox. Can States Learn to Govern Artificial Intelligence-Before It's Too Late?* ...cit.

a differenza delle ondate precedenti, avvierà anche un cambiamento epocale nella struttura e nell'equilibrio del potere globale poiché minaccia lo status degli stati-nazione come principali attori geopolitici del mondo.

Questo significa che i modelli geopolitici di ieri, definiti nell'ordine di potenza e di sovranità politica ed economica esprimibile, non saranno più gli stessi visto che verranno riorganizzati secondo nuovi paradigmi dove l'idea stessa di supremazia verrà ritagliata per differenza dal capitale di conoscenze e di possibilità tecnologiche esercitabili da un attore che non necessariamente si identificherà in uno Stato. Sovranità e Intelligenza Artificiale si confronteranno per caratterizzare un ordine emergente «tecnopolare», dove le Technology Companies potranno esercitare nei loro domini quel tipo di potere un tempo riservato agli Stati-nazione. Per Bremmer e Suleyman, i sistemi di Intelligenza Artificiale gestiranno ospedali, compagnie aeree e si combatteranno tra loro nelle aule di tribunale[2]. La produttività raggiungerà livelli senza precedenti e innumerevoli aziende precedentemente inimmaginabili si saranno sviluppate, nel frattempo, a una velocità vertiginosa, generando immensi progressi nel benessere. Nuovi prodotti, cure e innovazioni arriveranno quotidianamente sul mercato, mentre la scienza e la tecnologia entreranno in azione. Ma non soltanto questo.

Per il «Rapporto» McKinsey sarà il futuro dell'Intelligenza Artificiale Generativa (*Generative AI*), che descriverà algoritmi che potranno essere utilizzati per creare nuovi contenuti, tra cui audio, codici, immagini, testo, simulazioni e video[3]. Ciò renderà le relazioni nel cyber-sistema-mondo sempre più imprevedibili e, allo stesso tempo, quest'ultimo più fragile mentre soggetti non formali, siano essi gruppi antagonisti o organizzazioni terroristiche o criminali, troveranno nuovi modi per minacciare le società con armi informatiche intelligenti e in evoluzione mentre il top management rischierà di trovarsi ai margini della sfida.

---

[2] *Ibidem.*

[3] «Generative Artificial Intelligence describes algorithms (such as ChatGPT) that can be used to create new content, including audio, code, images, text, simulations, and videos. Recent breakthroughs in the field have the potential to drastically change the way we approach content creation». https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai.

Crescita, opportunità e ...pericoli

Come avvenuto in ogni passaggio della storia segnato dall'evoluzione tecnologica, toccherà all'Intelligenza Artificiale abbinare crescita e opportunità straordinarie a rischi e pericoli con una differenza rispetto al passato: che essa, l'IA, nell'avviare un cambiamento nella struttura e nell'equilibrio del potere globale, poiché metterà in discussione anche lo status degli Stati-nazione come principali protagonisti geopolitici del mondo, farà aumentare il quadro complessivo degli attori delle relazioni politiche ed economiche mondiali.

Un risultato che non è certo fuori luogo se si pensa a come negli ultimi anni del secolo scorso e nei primi anni del nuovo Millennio, il paradigma tecnologico sia mutato radicalmente e con esso i rapporti di forza, quindi quelli di potenza in ragione del differenziale tecnologico a disposizione di un attore piuttosto che un altro. Infatti, nell'ambito delle grandi imprese che guidano la IT non vi sono dubbi che esse abbiano assunto un ruolo determinante nel gestire e dirigere le scelte politiche e non solo degli Stati nelle quali hanno sede le Corporate, o nei Paesi nei quali si realizza e si distribuisce la produzione. In questo senso, si sono creati dei veri e propri nuovi attori geopolitici digitali che superano gli Stati in termini di capitali e nel definire anche i confini in materia di offerta della produzione tecnologica, di qualità e di gestione dell'accesso alle materie prime.

Di fronte a tale fotografia del futuro prossimo, si può dire che uno dei veri problemi sarà che l'Intelligenza Artificiale non farà altro che dilatare ulteriormente questi nuovi spazi dal momento che la dimensione cyber, ovvero la digitalizzazione del quotidiano, sarà gestita se non controllata proprio da risorse IA. Un aspetto che porterà a dover riconfigurare ogni rapporto tra uomo e dispositivo e tra dispositivo e IA. Infatti, l'Intelligenza Artificiale si presenterà come un acceleratore di opportunità, ma anche di problemi collegati alla gestione del limite dell'agire e dal considerare che ogni sua azione andrà ben oltre il mondo digitale, invadendo la sfera politica e, attraverso questa, dominando l'intimo di una comunità e degli individui che la compongono.

In questa prospettiva si possono individuare quattro configurazioni di Intelligenza Artificiale suddivisi in macchine puramente reattive, macchine con capacità di memoria, sistemi con una propria coscienza, sistemi dotati di una propria autoconsapevolezza. Ciò dimostra, ai vari livelli di capacità evolutive dimostrate, che ogni sistema IA è in grado di compren-

dere un discorso, imparare, pianificare, risolvere problemi, ragionare, percepire, maneggiare e spostare oggetti. E, ancora non basta[4].

La complessità della tecnologia e la velocità del suo progresso renderanno quasi impossibile per i governi emanare norme pertinenti a un ritmo ragionevole e ciò rappresenterà una vera preoccupazione per il futuro. D'altronde, non ci sono dubbi che la semplificazione dei processi e la necessità di ridurre la complessità del mondo fisico nella sua governance abbia trovato, nella digitalizzazione progressiva delle attività quotidiane, una sorta di strumento attraverso il quale rendere più rapidi i tempi, migliori e più economiche le risposte. In questo, l'ulteriore passaggio all'Intelligenza Artificiale rappresenta la nuova sfida verso una capacità di performare ancora di più la produzione oltre che le relazioni attraverso una sorta di mediazione tecnologica delle attività umane. Si dimostra, così, non solo l'avvio di una nuova rivoluzione tecnologica, ma anche la formazione di una coscienza robotica che, per quanto semplificata, possa riuscire a essere più empatica muovendosi e proponendosi in questo modo verso l'elemento umano, cercando di raggiungere risultati tali che possano permettere non solo di spiegare i processi, ma di interagire con gli esseri umani.

Insomma, quello che viene chiamato l'*inner speech* diventa, quindi, la vera cartina di tornasole sulla possibilità di poter disporre di una IA al servizio dell'uomo e non, invece il contrario. L'esistenza di un possibile dialogo interiore significa riconoscere a una IA la capacità di valutare il contesto e ciò determina l'adozione di un'architettura cognitiva che renderà l'Intelligenza Artificiale complementare e senza attribuire a essa posizioni esclusive nella vita complessa di una comunità umana quanto del singolo individuo. In altre parole, si tratta di raggiungere nella definizione e nella realizzazione di IA nei vari campi, un'adeguata interazione con l'essere umano e una migliore immagine antropomorfa tale da realizzare un clima di fiducia tra uomo/utente e IA.

[4] Esistono tre tipi di IA: Intelligenza Artificiale Limitata (Artificial Narrow Intelligence - ANI), Intelligenza Artificiale Generale (Artificial General Intelligence - AGI) e Superintelligenza Artificiale (Artificial Super Intelligence - ASI). L'Intelligenza Artificiale Limitata (ANI) è considerata come una IA debole dal momento che non va oltre una ristretta capacità di impiego come nel riconoscimento vocale o nell'automazione nell'ambito dell'automotive; l'Intelligenza Artificiale Generale (AGI) è considerata come una Intelligenza forte poiché essa definisce modalità di comprensione e di azione paragonabili a quelle proprie dell'intelligenza umana; la Superintelligenza Artificiale (ASI) a oggi non disponibile, rappresenta l'epilogo della IA nel momento in cui la macchina in sé è giunta ormai al livello successivo: il superamento dell'intelligenza umana.

Interazioni senza scrupoli

Certo, non è semplice credere di poter definire in termini di perfetta simmetria il rapporto uomo/IA pur seguendo le note «Leggi di Asimov» dotando di una saggezza artificiale una IA nella misura in cui questa possa assumere in sé una capacità di discrimine per la quale, di fronte a una data situazione complessa, essa possa mettere in campo, scegliendoli, una serie di comportamenti eticamente adeguati e privi di danno per l'utente e per i destinatari delle azioni condotte e dei risultati ottenuti[5]. D'altronde, non vi sono dubbi che le interazioni con l'universo-mondo cyber si autoprodurranno grazie a un'architettura ampiamente condivisa in quella realtà virtuale definita dal Metaverso dove si risolve un'assistenza puntuale di una realtà virtuale a interazione immediata tra i processi, il gestore e l'utente rappresentato da un proprio avatar.

Una condizione, la precedente, che abbatte le ultime barriere fisiche e geografiche dove, rispetto alla sperimentata interazione offerta dai social per mezzo della mediazione algoritmica, si aggiunge una ulteriore dimensione e dove, grazie a tale protagonismo per differenza, si sperimenteranno abilità che altrimenti non sarebbero sperimentabili, per ragioni di distanza se non di elaborazione dei dati in tempi, fisicamente, ristretti. In altre parole, Metaverso e IA forniranno una realtà metavirtuale offrendo alternative al quotidiano, creando l'illusione che proiettando risultati sulla coscienza questi possano soddisfare aspettative che non sarebbero conseguibili i primi e attese le seconde in una dimensione perfettamente, fisicamente, reale.

Non per nulla la stessa Commissione Europea ha definito una policy strategica «Web 4.0 e i mondi virtuali» ritenendo di dover iniziare a porsi l'interrogativo di come guidare la prossima transizione tecnologica assicurandosi un ambiente digitale aperto e sicuro per i cittadini dell'Unione europea. Un obiettivo ambizioso, che vede nel cosiddetto Web 4.0 una nuova versione di interconnettività fondata sulla convergenza delle tecnologie cosiddette immersive, dell'Internet delle cose (IoT), della *blockchain* e dell'Intelligenza Artificiale, all'interno di ambienti che permetteranno

[5] Le «leggi di Asimov» o della robotica: 1. Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno; 2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge; 3. Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge. Cfr. I. Asimov, *Io, robot*, Mondadori, Milano, 1950.

esperienze intuitive e immersive. Ovvero, in grado di creare un linkage tra il mondo fisico e quello digitale perfettamente simmetrico.

D'altronde, secondo le stime elaborate dalla Commissione Ue, il mercato globale dei mondi virtuali crescerà da 27 miliardi di euro già nel 2022 a oltre 800 miliardi di euro entro il 2030, aprendo a circa 860.000 nuovi posti di lavoro.

> Il Web 4.0 e i mondi virtuali porteranno benefici per la salute, contribuiranno alla transizione verde e anticiperanno meglio i disastri naturali. Ma dobbiamo mettere le persone al centro e modellarle secondo i nostri diritti e principi digitali dell'UE, per affrontare i rischi relativi alla privacy o alla disinformazione. Vogliamo assicurarci che il Web 4.0 diventi un ambiente digitale aperto, sicuro, affidabile, equo e inclusivo per tutti[6].

È evidente che la sfida del futuro si sposterà sul piano dell'acquisizione e dell'utilizzo dei Big Data che saranno sempre di più raccolti in maniera significativa e in tempi sempre più brevi e in grande quantità con l'accortezza che la raccolta sia sempre meno ridondante, operando tra dati strutturati e dati destrutturati affinché si possano offrire a ogni Machine Learning, ad esempio, informazioni sempre più coerenti sui gusti, profilazioni progressive e sempre più precise, e sulle necessità nel campo dei servizi.

Ciò dimostra come il passaggio a una sorta di società del *dataismo* è una delle conseguenze dell'evoluzione dei processi di governo in senso lato delle relazioni umane e del privato, per le quali i dati diventano preziosi nel poter condurre analisi comportamentali nei diversi settori che vanno dal consenso politico alle produzioni commerciali, alle transazioni economiche sino ai rapporti privati in termini contrattualistici ma anche sociali.

In fondo, comprendere il *sentiment* dell'altro significa poter disporre di informazioni utili proprio nel momento in cui si tratta di decidere un'azione politica, una scelta di offerta economica di un prodotto o il migliore investimento possibile guardando l'andamento dei mercati e prevedendo le intenzioni degli investitori nelle diverse piazze. È quindi evidente, che la stessa valutazione delle qualità della persona sono affidate alle tracce lasciate sui Big Data in termini di credibilità, affidabilità, e ciò pone ampi problemi di carattere etico e di tutela giuridica della sfera privata per il singolo o di protezione delle informazioni vitali per un'azienda o per uno Stato.

[6] La strategia sul Metaverso dell'Unione Europea. In «Osservatorio Metaverso», 17 luglio 2023. In https://osservatoriometaverso.it/la-strategia-sul-metaverso-dellunione-europea/.

Sul piano delle relazioni umane, l'IA tenderà ad alterare la percezione di sé e delle relazioni sociali visto che queste dipenderanno da condizioni psicologiche e difficoltà relazionali che non potranno essere facilmente rese come schematiche regolarità. In questo senso, un eccessivo e deregolamentato ricorso all'Intelligenza Artificiale quale supporto, se non sostituto alle scelte e alla profilazione delle relazioni stesse potrebbe danneggiare le relazioni umane poiché favorirebbe situazioni di fragilità psicologica. Questo, dal momento che una IA social nell'essere presente, disponibile, tenderà a essere sempre e comunque confermativa. Ciò significa, che un uso indiscriminato di tali supporti/piattaforme rischierà di dare ancora più spazio a comportamenti di ritiro sociale riconducibili alla «sindrome di Hikikomori».

Coscienze algoritmiche

A quanto visto, si aggiungerebbe anche il problema della cosiddetta «discriminazione algoritmica» per la quale si tratterebbe di attribuire un senso etico alla definizione degli algoritmi, affinché si possa superare quel dubbio che si risolve nella risposta alla domanda fondamentale che qualunque sviluppatore dovrebbe porsi: sino a quando un algoritmo può dare risposte utili, coerenti non solo con i dati acquisiti, ma con lo scopo a esso attribuito? Gli algoritmi, infatti, funzionano su assi crescenti di dati e con modalità di calcolo *in* e *out* per cui se l'algoritmo trova regolarità di dati, pur se non inseriti dallo sviluppatore, può usarli lo stesso. Come si vede, non si può certo non affermare che l'aumento di *bias* statistici pone ancora una volta il problema di chi controlla i dati tenuto conto che l'uomo è un insieme di dati che sono sparsi in rete e, quindi, reperibili e utilizzabili e, soprattutto, aggregabili in *cluster* temporanei sui quali l'algoritmo vi lavora per definire, o cercare, regolarità. Il rischio, se trasferito sul campo politico, è che gli algoritmi possono decidere chi è *in* e chi è *out*.

È sin troppo chiaro, allora, che in una dimensione IA evitare le discriminazioni risponde a un senso etico necessario non essendo attribuibile alle ragioni sottese all'uso di una IA la possibilità di derogare a diritti e garanzie proprie della civiltà giuridica, evitando rischi di alienazione se non di totale assenza e abbandono della propria personalità fisica oltre che giuridica. Ma, ancor di più, è altrettanto necessario evitare possibilità di autoprogrammazione di una IA; cioè, della possibilità che vi siano regolarità tali da giustificare se non indurre una Intelligenza Artificiale a ride-

finire obiettivi e azioni rispetto a quanto programmato. Per evitare questo rischio sarà necessario far sì che l'educazione e le capacità di programmazione seguano di pari passo l'evoluzione tecnologica per scongiurare l'incubo che in un domani possibile una IA possa superare l'uomo.

In questa sfida a metà strada tra il consolidamento della rivoluzione digitale e l'avvio di un nuovo quadro sinergico che dalla Quinta possa spostarci vero una Sesta dimensione, entrano in gioco altri due scenari che aprono a sviluppi nuovi di uso della tecnologia come la cosiddetta «cognitive war» (guerra cognitiva) e il rischio che la manipolazione delle capacità umane di autovalutazione dei processi e delle azioni definisca un quadro manipolatorio tipico di un nuovo *Manchurian Candidate*, prima romanzato da Richard Condon, contemporaneo per qualche anno di Aldous Huxley, e poi proposto cinematograficamente nel 2004[7]. Una versione non nuova di una sfida già aperta in passato e che oggi supera il livello della riservatezza per approdare alla ricerca di nuove opportunità di egemonizzare l'avversario in futuro[8]. Una sfida che si ricolloca sul campo della cosiddetta *wetware*; cioè, di quella possibile connessione tra capacità cognitive e elaborative umane e software che ricerca il miglior moltiplicatore delle possibilità cognitive e di azione tendenti ad aumentare la capacità logiche e computazionali della mente umana.

Per questo, la «guerra cognitiva», ovvero la possibilità di condizionare direttamente le scelte e le azioni di ogni attore non è certo un lusso da fantascienza o da libri di fantapolitica, ma una realtà che coinvolge ogni

[7] A tal proposito, R. Condon, *Manchurian Candidate*, MacGraw-Hill Book Company Inc, New York, 1959.

[8] Un'ipotesi non remota oggi, dove il miglioramento delle capacità prestazionali del soldato, l'idea di impianti sottocutanei per facilitare prestazioni cognitive e percettive, oltre che gestire quel remoto psicologico che lascia spazio a emozioni non richieste sembra essere l'obiettivo del futuro. La creazione di un non luogo nel quale tracciamento, geolocalizzazione, controllo della forza e capacità di dosarne l'uso o di dirigerne gli effetti sono solo alcuni dei particolari fattori di potenza che si vuole mettere in conto, rivoluzionando il modello militare, non disumanizzandolo, per adesso, ma portandolo su un piano di transizione tra l'oggi e l'oggi di domani. Un modello utile a ridurre i costi e a massimizzare i risultati. Alla fine si potrebbe dire che saremo testimoni di un'idea di «guerra non guerra» (War not War - WnW), o del non conflitto per la quale anche la distinzione tra ciò che è convenzionale (*conventional warfare*) e ciò che non lo è (*unconventional warfare*) decadrebbe considerando che è la ragione della forza, in termini di affermazione di una volontà, che determinerà la differenza in un conflitto dove ogni procedura di comando e controllo, se non anche di pianificazione, si dematerializzerà in uno spazio a sua volta disumanizzato e nel quale opereranno più attori e magari a dirigerne l'azione vi sarà una IA.

livello di sicurezza creando un modello di governo dell'agire umano nella consapevolezza che ogni dispositivo digitale e ogni possibilità IA offerta non sarà altro che una ulteriore estensione di capacità sensoriali già di per sé messe in campo con la rivoluzione digitale.

Insomma, che si tratti di approdare a una implementazione tra motori di ricerca e che si possa vivere attraverso una Matrix quotidiana, attribuendo alla realtà metaversica un significato di concreto e legittimo spazio di relazione, non è certo distante quale epilogo evolutivo della dimensione cyber che lascia spazio a una versione replicata e poi replicante dell'essere umano. D'altra parte, la sfida sul piano cognitivo delle capacità umane amplificate o, semmai anche, ridotte per atrofizzazione dei processi mentali, rimane tutta nella sfida della interconnessione dei cervelli con il risultato di omologarne le risposte, di preconfezionarne i comportamenti a condizioni, e informazioni, date.

Peter Sloterdijk fu preciso il 13 maggio del 2007 quando a Udine esordì con la seguente riflessione per la quale

> Sembra inevitabile associare la globalizzazione al tema della comunicazione. Indipendentemente dal mezzo considerato, essa avrebbe due caratteristiche essenziali: velocità e onnipervasività. Il mondo sarebbe globale in quanto nulla sfuggirebbe a una interconnessione rapida e capace di mettere in contatto luoghi e persone distanti.

Ma proprio lo spostamento da una società di conoscenza verticale orientata alla verità a una orizzontale, diretta verso la verità omologante, rappresenterebbe la cifra distintiva del percorso di digitalizzazione dei processi di conoscenza e ciò comporterebbe che

> Il privilegio dell'orizzontalità a scapito della verticalità e sarebbe del tutto irrilevante da quale fonte provenga questo o quel contenuto informativo, ciò che conta è la proliferazione di un gioco di scambi virtualmente illimitato la cui posta è data dal puro atto di parteciparvi[9].

Si potrebbe anche dire che secondo Sloterdijk le azioni collettive potrebbero cancellare quell'io individuale sul quale si fa la differenza tra capacità di conoscenza e omologazione.

La conseguenza, che rende sempre più urgente dotarsi di una consapevolezza della necessità di un nuovo paradigma della sicurezza, è che i conflitti e i non-conflitti del futuro saranno lunghi e cruenti, ma non per il

[9] Cfr. P. Sloterdijk, *La costruzione telematica del reale*. Stralcio della conferenza tenuta a Udine all'interno della manifestazione Vicino/Lontano del 13 maggio 2007.

numero di vittime sul campo. Ma per le vittime sociali degli attacchi ai sistemi di relazione, politici, economici, sociali e agli stili di vita essi si manifesteranno in molteplici forme e in luoghi diversi, disegnando un versante creativo dell'*Information Age*. L'idea della sicurezza, quindi, si sposta sulla possibilità di individuare e contrastare le azioni di agenti intelligenti considerati quali agenti autonomi, algoritmi capaci di scegliere autonomamente le informazioni di interesse per raggiungere uno scopo definito dall'utilizzatore.

Ogni competitor, e ogni minaccia, si presenterà ricercando il modo più efficace e produttivo possibile con una visione indistinta di un avversario multidimensionale. Un avversario non necessariamente statualizzato, che non si manifesterà chiaramente, ma che potrà colpire in tutto lo spettro delle strutture fisiche o artificiali che sostengono la vita di una comunità politica o economica, o agire sui valori e le certezze morali, oltre che materiali, che ne garantiscono la coesione, per le quali sono le condizioni provocate che vanno gestite e dirette verso l'obiettivo, e non solo quelle predefinite.

Il dominio del cyberspazio, insomma, non si esaurirà solo nella dimensione digitale, ma si completerà nell'implementarsi con la stessa Intelligenza Artificiale. Uno scenario sin troppo chiaro che richiede un'attenzione costante verso l'evoluzione dei sistemi e dei software considerato che la forza muterà sempre di più secondo lo strumento di persuasione prescelto, assumendo capacità artificiali di riprodurre processi e decisioni quali momenti di conquista dell'intima coscienza dell'avversario, oltre che di manipolazione dei suoi bisogni. È, questa, una riflessione, un monito non da poco se si guarda alla rapidità dei cambiamenti nelle relazioni umane, politiche ed economiche di oggi che riducono le distanze con la percezione del dubbio di cosa possa riservare il futuro.

Realizzare un quadro sostenibile di cybersicurezza ad ampio spettro rappresenta un paradigma fondamentale, visto che la velocità dell'accesso alle migliori informazioni sull'avversario e la rapidità del processo di elaborazione detteranno le regole e i tempi di difesa dalle prossime minacce. Un aspetto che se ricondotto sul piano della tecnologia al servizio dell'industria militare diventerebbe un inequivocabile, se non imperituro, monito. Una *Revolution in Military Affairs* (RMA) ma rivolta, questa volta, a favore di una sorta di guerra permanente giocata su piani diversi, dove la forza assume una poliedricità senza precedenti riducendo la distanza tra ciò che è

di interesse militare piuttosto che civile in termini di sicurezza e difesa. Così, ad esempio, in materia di Intelligenza Artificiale sarà il grado di autonomia consentito l'aspetto nel quale si risolverà il paradosso transumano, dove la singolarità sarà data dal se e dal come etica e morale saranno valori superabili proprio nell'uso dell'IA in operazioni volte a garantire sicurezza e/o difesa di una comunità e delle sue architetture di governance.

Se un sistema autonomo opera in uno spazio troppo riservato e affidato solo al controllo di chi vi ricorre, diventa evidente che in nome dell'interesse o de «il fine giustifica i mezzi», la macchina verrebbe lasciata libera di operare ben oltre il limite sostenibile in termini di morale ed etica; aspetti, questi ultimi, compressi se non sacrificati dal raggiungimento dello scopo finale. In altre parole, se la linea dell'umanamente accettabile dovesse essere superata, ciò non farebbe venir meno l'impiego della migliore formula di attacco, ma costringerebbe l'avversario a giocare al rialzo pur di vincere lasciando altrettanta autonomia alle sue creature.

Nulla sarebbe più certo circa il futuro della guerra di come la tecnologia modellerà i conflitti e le relazioni politiche e condizionerà la lotta per una supremazia. Niente è più sicuro oggi del fatto che le possibilità tecnologiche modelleranno sempre di più la lotta per il potere invadendo ogni aspetto, ogni spazio residuale della vita dell'umanità. In altre parole, non si può certo non affermare che software e hardware possono essere anche interpretati come veri e propri sistemi d'arma al punto tale da poter modificare o modellare secondo le regole del più forte, ovvero del più capace e di colui che dispone della migliore tecnologia a supporto, le stesse relazioni internazionali.

E questo, perché la singolarità espressa non si risolve solo nell'effetto destabilizzante dovuto all'aggressione dell'intimo-organizzativo o dell'intimo vissuto di una comunità quanto dall'essere, le armi digitali, molto più semplicemente economiche, facilmente approvvigionabili e che non determinano gravi danni per colui che ne fa uso.

Oggi, non vi sono dubbi che integrare IA con il dominio cyber rappresenti una nuova e ben più pericolosa, perché più invasiva, minaccia quale possibilità di trovarsi di fronte a una sorta di attacco combinato. Questo significa che diventerà sempre più necessario, e in tempi brevi, riuscire ad analizzare e migliorare la posizione di sicurezza informatica di un'organizzazione poiché questa richiederà sempre di più capacità superiori al semplice intervento umano. Se ciò è vero, è altrettanto vero il contrario te-

nuto conto che l'Intelligenza Artificiale rappresenterà, oltre una minaccia, anche il futuro della sicurezza informatica. L'Intelligenza Artificiale, infatti, è ormai non solo una forma di tecnologia, ma una filosofia tecnologica in costante evoluzione e in costante progressione nella conquista di spazi sempre più ampi di applicazione. I sistemi informatici, quindi, possono apprendere, ragionare e agire utilizzando l'Intelligenza Artificiale per processare sempre più ampi set di Big Data raccolti dai vari sensori e non solo sulle piattaforme digitali.

L'universo digitale, insomma, sembra dilatare le capacità di governo delle informazioni replicando o permettendo che si replichino procedure metaumane il che richiederà nuove frontiere di sfida dove, se le tecnologie attuali minacciano la sicurezza informatica dell'organizzazione, le procedure messe in campo solo nell'ambito della sicurezza digitale rischieranno di fallire se i controlli di vulnerabilità alla difesa non si combineranno con la forza dell'Intelligenza Artificiale applicata alla sicurezza informatica.

D'altra parte, le organizzazioni che si affideranno a un digitale gestito da una IA potranno disporre di *insight* più rapidi; ovvero, vedranno accelerare i flussi di lavoro delle *machine learning* con una capacità di generare automaticamente informazioni dettagliate sui dati, quindi tempi di risposta più rapidi. Ciò dimostra già oggi come l'Intelligenza Artificiale per la sicurezza informatica sembra essere un'opportunità, perché l'IA può elaborare grandi quantità di dati potendo affidarsi a un'automazione della progettazione di algoritmi di apprendimento in grado di rilevare un'ampia gamma di rischi per la sicurezza informatica come e-mail di spam, siti Web pericolosi, programmi di terze parti e files condivisi.

IA: sfida in corso d'opera

L'integrazione dell'Intelligenza Artificiale con la sicurezza informatica richiede una sorta di *comprehensive approach* cui non si potrà rinunciare presentandosi come l'approccio più efficace per rilevare e rispondere agli attacchi in tempo reale. Infatti, l'Intelligenza Artificiale potrà monitorare l'intero sistema per rilevare eventuali pericoli e, a differenza degli esseri umani, l'IA potrà "vedere" i rischi in anticipo semplificando, in questo modo, le procedure di cybersicurezza. Nel tempo, l'Intelligenza Artificiale acquisisce, infatti, più conoscenze e sfrutta tale *intelligenza* per migliorare la sicurezza della rete nel tempo apprendendo il comportamento di una rete aziendale utilizzando l'apprendimento automatico e il *deep learning*.

Potrà rilevare modelli nella rete e raggrupparli cercando eventuali differenze, deviazioni logiche o individuando vere e proprie vulnerabilità prima che il sistema inizi a elaborare le informazioni necessarie o individuare problemi di sicurezza rispetto alla norma prima di agire. Infatti, le reti neurali artificiali possono contribuire a migliorare la sicurezza in futuro apprendendo modelli nel tempo e, in questo modo, verificare eventuali minacce con caratteristiche identiche a quelle documentate che verranno identificate tempestivamente e bloccate.

Tutto questo, perché l'Intelligenza Artificiale apprende costantemente, rendendo più difficile per gli hacker superarla in astuzia; si potrebbe dire che la vera singolarità dell'IA applicata alla cybersicurezza non è altro che la migliore gestione delle vulnerabilità perché diventerà più semplice. La gestione delle vulnerabilità, infatti, è fondamentale per la sicurezza della rete poiché affrontare minacce diverse significa rilevarle, identificarle e prevenirle. In questo senso, l'Intelligenza Artificiale potrà consentire di esaminare i sistemi molto più rapidamente migliorandone significativamente le capacità di risoluzione dei problemi. Aiuterà le aziende a concentrarsi su compiti cruciali di sicurezza identificando i punti deboli nei sistemi informatici e nelle proprie reti. Consentirà, in poche parole, la gestione tempestiva delle vulnerabilità e il funzionamento sicuro dei sistemi aziendali.

Nella ricerca di una *supremacy* in IA bisogna anche considerare che il tempo è un fattore strategico fondamentale, vista la rapidità con la quale mutano i processi di acquisizione di tecnologie sempre più avanzate nelle sfere del *mind control*, della robotica e della biotecnologia. Tuttavia, credere che l'Intelligenza Artificiale possa risolvere ogni problema strategico in futuro può essere una bella e ottimistica speranza. Ma, a tal proposito, si dovrebbe considerare che ogni sistema autonomo cercherà di giungere alla massima possibilità esprimibile di apprendimento della macchina, alla massima capacità di elaborazione di informazioni per rispondere, superando le possibilità umane, alle diverse minacce multidimensionali: ad esempio, gli attacchi informatici, il lancio di missili ipersonici o la guerra elettronica, oltre a diventare essenziale, se non insostituibile, nei processi di gestione ed elaborazione di grandi volumi di dati. Il vero problema, infatti, sarà come conciliare la direzione umana dei sistemi e la filosofia dell'IA affidata a sequenze che rispondono proprio al paradigma «Osservare-Orientare-Decidere-Agire» (*Observing-Orient-*

Decide-Act; OODA), con una conseguenza immediata: che il vantaggio sarà ottenuto sul campo della sicurezza e della difesa da chi disporrà dei migliori «algorithmic warfare»[10].

Bisogna dire che la sfida IA si presenterà anche come una corsa progressiva al miglioramento delle performances dei sistemi e dei processi che li governano sia in fase di sviluppo/progettazione che in fase di produzione. Questo significa che la corsa all'egemonia tecnologica, in assenza di un quadro cooperativo sarà l'aspetto dominante dei prossimi anni. Una realtà che si dimostra e contiene in sé le ragioni di una evoluzione dei sistemi e delle intelligenze a supporto delle attività umane che potrà solo raggiungere traguardi successivi di qualità e di sempre migliori abilità performanti. Una condizione che si può già notare nei confronti dell'Intelligenza Artificiale applicata all'apprendimento automatico se ci spostiamo sul piano quantistico (*Quantum Machine Learning* - QML), dove la migliore performance è data dal punto di incontro tra le capacità predittive tipiche delle ML (*Machine Learning*) con le possibilità di calcolo quantistico che tenderanno a migliorare gli algoritmi.

La stessa sfida tra Open AI con la sua ChatGPT e la chatbot, ovvero la chat conversazionale Bard di Google si risolve nel confronto tra le qualità generaliste di ChatGPT, e la capacità di Bard di offrire risposte mirate, più specifiche e, quindi, più aderenti al tipo di richiesta ricevuta[11]. Questo significa, per Bard, disporre di algoritmi capaci di tradurre in termini di particolare aderenza i contenuti, fornendo supporto ad attività di ricerca o anche alle decisioni di governance mentre ChatGPT si presenta ancorata a un modello conversazionale complesso ma, proprio per questo, limitato a offrire risposte generaliste seppur caratterizzate da un'apprezzabile coerenza. Ma anche le competenze linguistiche di Bard superano ChatGPT utilizzando un vocabolario di più di 40 lingue, il che rende, al momento, la *chatbot* del browser più famoso del mondo particolarmente versatile a superare ogni possibile ostacolo dettato dalle differenze tra comunità di

[10] P. Layton, *Algorithmic Warfare Applying Artificial Intelligence to Warfighting*, Air Power Development Center, Canberra, 2018.

[11] Chat GPT (Chat-Generative Pre-trained Transformer) risponde ai dati in possesso ma, soprattutto, risponde secondo le loro qualità. Essa risponde all'abilità di generare testi coerenti conversando e accettando input di testo, ricorrendo a un sistema probabilistico per indovinare e comporre frasi che hanno comunque un loro significato logico e dove si cerca di dare risposte a un problema complesso pur non disponendo, sino a oggi, di una propria consapevolezza.

ricercatori o operatori economici internazionali quali utenti le cui decisioni provocano effetti in campi e settori più vasti.

Come si potrà intuire, l'idea è che si possa affermare una sorta di imperialismo digitale tale da determinare una nuova corsa all'egemonia geopolitica questa volta attraverso l'uso dell'IA quale fattore determinante la supremazia tecnologica. Il capovolgimento delle relazioni di forza dovute alle capacità economiche esprimibili nel controllo dei mercati e delle rotte commerciali - che erano alla base delle teorie continentaliste di Halford Mackinder e l'idea dell'*Isola-mondo* (o *Heartland*) piuttosto che talassocratiche proprie della prospettiva di Alfred Thayer Mahan o di Nicholas John Spykman e la sua *Rimland* - sembrano oggi rideterminare ogni relazione spaziale riconducendone il significato in un altrove tecnologico nel quale il dominio della migliore IA esprimibile rappresenta il fattore di potenza più significativo e assertivo schierabile in un confronto competitivo[12]. D'altronde, non vi sono dubbi che ogni possibile nuova visione strategica si risolve in una prospettiva geopolitica che tende a mettere al centro di una politica di potenza il proprio differenziale tecnologico in termini di deterrenza e in una prospettiva economica rappresentata dalla qualità della tecnologia e dal differenziale di innovazione esprimibile rispetto ai propri competitor[13]. L'idea che si possano affermare degli imperi tecnologici non è nuova e, se lo è, lo è soltanto se la si vuole osservare sul piano di una realtà complessa dove la fisicità della tecnologia strutturale lascia lo spazio a una «geopolitica liquida», per prendere in prestito un termine caro a Zygmunt Bauman, per la quale è la digitalizzazione del controllo dei processi politici ed economici a fare la differenza.

La stessa digitalizzazione progressiva dei processi, d'altronde, ha alterato i rapporti di forza fisici per traghettare ogni possibilità di dominio all'interno di qualità di governance fortemente sostenute dalla migliore tecnologia esprimibile in termini di semplificazione dei processi e di ra-

[12] A.T. Mahan, *The Future in Relation to American Naval Power*. In «Harper Monthly Magazine», 1895. Ovvero, *The Interest of American in Sea Power, Present and Future*. Boston, 1898; H. Mackinder, *The Geographical Pivot of History*, Royal Geographical Society, London, 1904; N.J. Spykman, *The Geography of the Peace*, Harcourt, Brace and Company, New York, 1944.

[13] A tal proposito vedasi anche D. Breznit, *Innovation in Reals Places. Strategies for Prosperity in an Unforgiving World*, Oxford University Press, New York 2021.

[14] Così in Z. Bauman, *Modernità liquida*, Laterza, Bari-Roma, 2011; tit. or. *Liquid Modernity*, Polity Press, Cambridge, 2000. Anche, E. Di Nolfo, *Dagli imperi militari agli imperi tecnologici. La politica internazionale dal XX secolo a oggi*, Laterza, Bari-Roma, 2013.

pidità delle decisioni che pone in stretta relazione le grandi multinazionali e le potenze di ieri.

D'altra parte, se sino a ieri erano le materie prime e il mercato dell'energia, oltre che la supremazia militare nei sistemi d'arma nucleari, gli obiettivi da conquistare e controllare per assumere una posizione egemonica nelle relazioni internazionali, è del tutto evidente che oggi la determinante di una politica di potenza si sposta sul campo dell'egemonia tecnologica e, in particolare, nella supremazia nella corsa alla migliore qualità di IA esprimibile anche nel campo della tecnologia quantistica.

È del tutto evidente che si tratta di una sfida cui l'Unione europea non può rinunciare salvo il rischio di pagare il prezzo di una marginalità le cui distanze saranno sempre più difficili da colmare di fronte ad attori che assumeranno posizioni di vantaggio nell'uso e nel controllo dell'Intelligenza Artificiale e delle materie prime e del know how alla base del suo sviluppo. Le iniziative europee dovranno, quindi tener conto di dover anticipare gli eventi evitando di cadere nella trappola di un colonialismo digitale che tende a rendere subalterna ogni possibile concorrenza nel settore.

D'altronde, e senza cadere nella retorica o nel sensazionalismo, Nicolas Miailhe si poneva un interrogativo necessario e interessante nel suo *The Geopolitics of Artificial Intelligence: the Return of Empires?* del 2018 allorquando a premessa osserva che da Putin piuttosto che Elon Musk con il suo Optimus di seconda generazione - nella sua predizione di una nuova guerra mondiale per la supremazia tecnologica - la consapevolezza che la conquista delle migliori possibilità di IA rappresenti paradigma delle relazioni internazionali, politiche ed economiche del prossimo domani è una certezza difficile da contestare[15]. Le ragioni di tali riflessioni sono tutte frutto del convincimento che sarà impossibile arrestare il progresso nel campo dell'Intelligenza Artificiale considerato che il raggiungimento e la disponibilità delle migliori performances si trasforma in un fattore di potenza non trascurabile sia nelle relazioni economiche che politico-strategiche, ponendosi al vertice della piramide delle qualità necessarie per poter esprimere una politica di potenza di nuovo tipo. Infatti, non solo l'Intelligenza Artificiale determinerà nuovi rapporti di forza. ma modificherà anche ambiti spaziali considerati fondamentali per definire nuove geografie e nuovi linguaggi geopolitici attraverso relazioni politiche, eco-

[15] N. Miailhe, *The Geopolitics of Artificial Intelligence: the Return of Empires?* In «Politique étrangère» n. 3 - 2018, pp. 105-117.

nomiche e strategico-militari non necessariamente definibili come in passato solo ricorrendo ai criteri della prossimità o contiguità spaziale.

L'Intelligenza Artificiale si sta sviluppando rapidamente e sta diventando un vero e proprio strumento di potere. Ciò vale tanto per l'hard power (applicazioni militari) quanto per il soft power (impatto economico, influenza politica e culturale, ecc.). Gli Stati Uniti e la Cina dominano il mercato e impongono il loro potere mentre l'Europa, in ritardo, per Miailhe, cerca di rispondere dotandosi di una propria *Digital Strategy* cui si accompagna uno sforzo decisivo nel dotarsi di un proprio ordinamento giuridico a riguardo. In fondo, credere che non vi sia il rischio che altre potenze possano mutuare la postura di Pechino definita dalla cosiddetta *wolf warrior diplomacy* sostenendola proprio grazie alla supremazia tecnologica è di certo una superficialità che la stessa Unione europea non dovrebbe permettersi[16]. In fondo, non ci sono particolari dubbi sul fatto che nel campo della competizione nel campo della IA non si possa ridefinire una sorta di Guerra Fredda 2.0 come ipotizzato in più sedi ma che, nella sostanza, ogni visione e ogni comportamento assunto nel rilancio della competizione tecnologica riconduce ogni previsione possibile, a condizioni geopolitiche date, a una nuova polarizzazione tecnologica[17].

In questa rideterminazione dei rapporti di potenza e dell'esercizio di una supremazia sempre più tecnologica anche lo spazio sul quale si esercita il potere egemonico subisce una sua riorganizzazione. Il nuovo terreno di conquista è uno spazio fisicamente dematerializzato nel quale esercitare il potere effettivo di un impero, quello spazio digitale caratterizzato dalla rete di nodi che si pone come una rete neurale artificiale di una o più comunità connesse con l'unica fonte di potere e detentrice del controllo digitale.

Ecco, perché, nel riscrivere le condizioni del modello relazionale del futuro prossimo non solo Miailhe riprende e restituisce forza al ruolo degli attori non-Stato ma dotati di alto potere di influenza come le Multina-

[16] «Wolf warrior diplomacy» (letteralmente, la «diplomazia del lupo guerriero»). Definita durante l'era di Xi Jinping, si caratterizza per una particolare assertività che Pechino tende ad affermare negli ultimi decenni ponendosi come attore competitivo e superando, nella visione di Xi, la visione di Deng Xiao Ping più orientata a risolvere ogni iniziativa diplomatica all'interno di relazioni cooperative utili a ridurre condizioni/cause di controversie. Cfr. *Europe, U.S. should say "no" to China's "wolf-warrior" diplomacy - EU envoy,* «Reuters» December 10, 2020.

[17] Interessante se non illuminante l'esteso articolo di E. Morozov, *Guerre Froide 2.0. Histoire Secrète de l'Intelligence Artificielle*, in «Le Monde Diplomatique», Mai 2023.

tional Corporations (MNCs) scrivendo di colonialismo digitale, ma attribuisce loro modalità adattive alle esperienze storiche imperiali nel momento in cui queste tendono non solo a controllare i mercati delle materie prime e garantirsi capacità di produzione, ma puntano a concentrare la propria influenza assumendo ruoli e determinando comportamenti dovuti alle loro decisioni più assertivi di quanto richiesto allo Stato tradizionale conquistando la supremazia tecnologica[18].

Per Miailhe il colonialismo digitale si estrinseca in un controllo dei software utilizzati dalla Corporation, l'uso di *Server as a Service* (SaaS), un controllo dell'hardware e un controllo del network. Ciò significa violare il principio della *net-neutrality*. Le MNCs si occupano di tecnologia digitale perché ciò garantisce loro di poter esercitare un dominio sulle funzioni critiche nell'ecosistema tecnologico. Si sommano così profitti ricavati dalla proprietà intellettuale e dall'accesso alle infrastrutture e, potenzialmente, si garantiscono anche grandi capacità di sorveglianza esercitando un controllo sul flusso di informazioni, ad esempio, nella divulgazione di notizie o di servizi in streaming o sulle attività sociali, come i social network e lo scambio culturale.

In questo ambito, l'Europa dovrebbe porsi come attrice fondamentale nell'impedire che si possa non solo determinare una sorta di possibile colonialismo digitale e, quindi, tecnologico, ma anche porre in essere norme e favorire comportamenti tali da evitare che si formino derive unilaterali in totale disaccordo con la politica a sostegno di relazioni cooperative e multilaterali come affermato al Summit di Londra del novembre 2023, dove il motivo centrale è stato rappresentato dalla volontà di mettere in campo tutte quelle iniziative utili a favorire una distribuzione equa di potere e di responsabilità in materia di governance dell'IA; cioè, una volontà di agire (*Pledge action*).

E, questo, avrebbe poco da spartire con una versione a senso unico per la quale uno Stato, quale attore principale delle relazioni internazionali, dovrebbe porsi come potenza tecnologica al di sopra degli altri partner dal momento che solo una superiorità tecnologica potrà affrancarlo dalle scelte e dalle conseguenze di un colonialismo tecnologico cui si sarà costretti a rideterminare anche il significato di sovranità, visto che al vincitore della competizione sarà garantita l'egemonia globale. Si comprende, allora, come lo sforzo dell'Unione europea di dotarsi di una propria stra-

[18] *Ibidem*.

tegia nel campo dell'Intelligenza Artificiale e di nuove norme che ne disciplinino la produzione e l'uso oltre la sicurezza, è dettato coerentemente con i principi sovranazionali per i quali è l'interesse del cittadino europeo a essere collocato al centro di ogni iniziativa. In questo senso un obiettivo fondamentale e coerente con il principio della distribuzione dei vantaggi è quello di evitare casi di concentrazione di potere economico e politico nei sempre più definiti e aggregati board delle grandi multinazionali che si occupano di IA.

V. L'Ue e le nuove "Intelligenze"

> A volte sono proprio le persone che nessuno immagina a fare cose che nessuno può immaginare.
> Alan M. Turing

È necessario, preliminarmente, precisare che non vi è un'unica definizione di Intelligenza Artificiale il che fa sì che il semplice termine "Intelligenza Artificiale" sia ricondotto a un'interpretazione generalista dal momento che per IA si intenderebbe l'insieme delle applicazioni informatiche che, al di là della diversità delle tecniche adottate, presentano capacità che comunemente e abitualmente sono associate o riconducibili ad attività proprie dell'intelligenza umana. Stuart Russel, coautore di *Artificial Intelligence: A Modern Approach*, definisce l'Intelligenza Artificiale come

> Lo studio dei metodi per far sì che i computer si comportino in modo intelligente.

Per Russel, l'Intelligenza Artificiale include compiti come l'apprendimento, il ragionamento, la pianificazione, la percezione, la comprensione del linguaggio e la robotica[1].

Tuttavia, il Parlamento europeo il 3 marzo 2023 ha adottato una definizione di IA simile a quella dell'OCSE per la quale per IA si intende

> Un sistema basato su macchine progettato per funzionare con diversi livelli di autonomia e che può, per obiettivi espliciti o impliciti, generare output come previsioni, raccomandazioni o decisioni che influenzano ambienti fisici o virtuali.

Con il Vertice di Londra del 1-2 novembre 2023, il cosiddetto AI-*Safety Summit*, superando ogni definizione, sul tavolo delle discussioni si è posto un altro problema: l'impatto e il ruolo che l'Intelligenza Artificiale, nelle sue diverse e complesse declinazioni, assumerà nei prossimi anni. Di certo, le preoccupazioni non si sommano solo alla sostituzione progressiva di

[1] S. Russel, P. Norvig, *Artificial Intelligence: A Modern Approach*, Pearson Education Limited, London, 2021.

funzioni umane di conoscenza e di decisione ma, in particolare, segnano il confine tra ciò che è dominio dell'uomo razionale quale essere vivente e l'uomo-sistema, espressione, nella sua esistenza, di una evoluzione tecnologica che ne amplifica le capacità nel dominio dello spazio fisico nel quale agisce, considerato nella trasfigurazione di capacità affidate a entità senzienti con particolari qualità di elaborazione di informazioni e di messa in opera di comportamenti.

È evidente che le preoccupazioni siano soprattutto fondate e da ricercarsi nella capacità di dominare una simile sfida evolutiva che sembra porsi quasi come un incubo per leadership che soffrono di una capacità limitata di percezione del ruolo dell'Intelligenza Artificiale e dei necessari limiti da definire. Una preoccupazione non di poco conto al di là della sincerità dei 28 paesi firmatari più l'Unione europea, della «Dichiarazione di Bletchley Park», luogo emblematicamente simbolico come scelta per aver visto prendere il suo corso quella macchina decodificatrice di Enigma che avrebbe traghettato il suo ideatore, Alan Mathison Turing, verso la nuova era informatica[2].

Una preoccupazione che, dopo il «processo AI di Hiroshima» - un forum dedicato all'armonizzazione della governance dell'IA nel maggio 2023 in ambito G7 - ha messo in chiaro, almeno nelle intenzioni, la necessità che siano i governi, - ammesso che si possano trovare dei punti in comune a riguardo e che gli obiettivi politici ed economici siano ispirati a una sincera volontà di cooperazione e sinergia reciproca - e non le aziende, a proteggere le persone dai pericoli dell'Intelligenza Artificiale. Pericoli non ben definiti e non ben definibili che non si presentano solo nella disumanizzazione dei processi ma nell'uso non etico, si potrebbe anche dire non pacifico, dell'IA. Non per nulla, la Dichiarazione si apre sottolineando a premessa che

> L'Intelligenza Artificiale presenta enormi opportunità globali: ha il potenziale per trasformare e migliorare il benessere umano, la pace e la prospe-

[2] I Paesi partecipanti: Australia, Brasile, Canada, Cile, Cina, Unione Europea, Francia, Germania, India, Indonesia, Irlanda, Israele, Italia, Giappone, Kenya, Regno dell'Arabia Saudita, Paesi Bassi, Nigeria, Filippine, Repubblica di Corea, Ruanda, Singapore, Spagna, Svizzera, Turchia, Ucraina, Emirati Arabi Uniti, Regno Unito di Gran Bretagna e Irlanda del Nord. Stati Uniti d'America. Al vertice hanno preso parte società quali Anthropic, Google DeepMind, Microsoft, Meta e xAI, OpenAI oltre a Ursula von der Leyen quale presidente della Commissione UE, Kamala Harris vicepresidente degli Stati Uniti e il segretario generale delle Nazioni Unite António Guterres.

rità. Per realizzare ciò, affermiamo che, per il bene di tutti, l'Intelligenza Artificiale dovrebbe essere progettata, sviluppata, implementata e utilizzata in modo sicuro, in modo tale da essere incentrata sull'uomo, affidabile e responsabile. Accogliamo con favore gli sforzi compiuti finora dalla comunità internazionale per cooperare sull'Intelligenza Artificiale per promuovere la crescita economica inclusiva, lo sviluppo sostenibile e l'innovazione, per proteggere i diritti umani e le libertà fondamentali e per promuovere la fiducia del pubblico nei sistemi di Intelligenza Artificiale per realizzare appieno il loro potenziale[3].

L'aspetto cooperativo diventa, pertanto, fondamentale e in questa prospettiva si colloca anche l'azione dell'Unione europea. In questo senso, in una prospettiva di maggior cooperazione e per dare un senso di unità all'azione da condurre sia in termini nazionali che internazionali, per affrontare i rischi derivanti da un uso non controllato della Intelligenza Artificiale, gli obiettivi posti nel vertice di Londra sono stati individuati nell'/nel

- identificare i rischi per la sicurezza dell'IA di interesse condiviso, costruire una comprensione scientifica condivisa e basata sull'evidenza di questi rischi e sostenere tale comprensione mentre le capacità continuano ad aumentare, nel contesto di un approccio globale più ampio alla comprensione dell'impatto dell'IA nelle nostre società;
- costruire rispettive politiche basate sul rischio in tutti i nostri paesi per garantire la sicurezza alla luce di tali rischi, collaborando in modo appropriato e riconoscendo che i nostri approcci possono differire in base alle circostanze nazionali e ai quadri giuridici applicabili. Ciò include, oltre a una maggiore trasparenza da parte degli attori privati che sviluppano capacità di Intelligenza Artificiale di frontiera, parametri di valutazione adeguati, strumenti per test di sicurezza e lo sviluppo di capacità del settore pubblico e della ricerca scientifica pertinenti.

L'idea, secondo le volontà racchiuse nella Dichiarazione di Bletchley Park, è proprio quella di favorire lo sviluppo di una rete di collaborazione

[3] *The Bletchley Declaration by Countries Attending the AI Safety Summit*, London, 1-2 November 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023. Sul rapporto tra algoritmi e diritti umani, vedasi *Algorithms and Human Rights. Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular algorithms) and Possible Regulatory Implications,* Council of Europe Study, 2018. Consultabile in https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

e di cooperazione che sia capace di promuovere e governare i progressi e le applicazioni della IA attraverso politiche inclusive a livello internazionale nel campo della ricerca scientifica sulla sicurezza dell'Intelligenza Artificiale e tali da poter integrare programmi e iniziative di raccordo multilaterale, plurilaterale e bilaterale promuovendo, nel frattempo, forum internazionali che possano concretizzare quel potenziale positivo di trasformazione che è riconosciuto all'IA.

In questo senso, l'attenzione si rivolge a una sorta di patto con gli sviluppatori ai quali si richiede di definire preliminarmente capacità e rischi sottesi alle novità IA che verranno proposte soprattutto nel campo della guida autonoma, della medicina, della sicurezza nazionale. Per i partecipanti governativi i test dovranno essere condotti da ben definite terze parti indipendenti, dovranno essere trasparenti e accessibili al pubblico. Lo scopo, ovviamente di tale preliminare sinergia, dovrebbe essere quello di identificare, valutare i rischi e porre e/o suggerire modi e termini per limitarne i danni possibili nella gestione.

D'altra parte, al netto delle critiche che possono riguardare diversi punti di vista sull'argomento, dettati da ragioni di governance politica sui rischi piuttosto che sugli interessi delle grandi compagnie che si occuperanno di offrire le migliori soluzioni di IA nel prossimo futuro, è fuori discussione che l'Intelligenza Artificiale non sia pericolosa se non nel suo utilizzo condotto al di fuori di una regolamentazione specifica. Una regolamentazione che sia in grado di tenere il problema della gestione umana delle competenze artificiali senza cadere in una prospettiva distopica ed emergenziale che possa creare difficoltà all'azione politica o alle scelte economiche e di sicurezza, piuttosto che nell'offerta di servizi di pubblica utilità o nella gestione delle reti energetiche o dei sistemi di produzione. Una regolamentazione idonea nel garantire una sicurezza tale da concretizzare le capacità di indirizzo e di controllo delle attività di una IA, ancorché generativa, nella misura in cui si debba riuscire a evitare possibili fantasmi da supercomputer senzienti realizzati su reti neurali grazie alle quali l'Intelligenza Artificiale potrebbe prendere il sopravvento[4].

D'altronde, coerentemente con quanto indicato dall'OCSE, le tecnologie di apprendimento automatico rappresenteranno gli strumenti prin-

[4] A tal proposito, vedasi: A.D. Signorelli, *Cos'è lo "scenario Terminator" che fa venire gli incubi al papà di ChatGPT*. In «Wired» 28 marzo 2023. Consultabile in https://www.wired.it/article/chatgpt-openai-sam-altman-scenario-terminator-lungotermismo/.

cipali per modellare e scegliere le informazioni online. Moderazione e credibilità dei contenuti sono spesso il risultato di una procedura automatizzata, con algoritmi e IA che decidono quali contenuti debbano essere rimossi o a chi andrebbero. Ma esiste anche il rischio concreto che tali tecnologie abbiano un impatto negativo sulle libertà fondamentali ed è questo che giustifica tutta l'architettura della proposta giuridica di disciplina dell'Intelligenza Artificiale che si fonda su un *risk-based approach*[5].

In questo senso, il Parlamento europeo ha individuato i vari livelli di rischio qualificandone la portata e l'impatto sulla possibilità di sviluppare o meno progetti di IA. Le regole proposte, e che dovranno tradursi in un Regolamento dedicato, saranno confezionate in maniera tale da tener conto del livello di rischio. Un parametro fondamentale, quest'ultimo, cui si riconduce la responsabilità degli sviluppatori/produttori e utilizzatori oltre che il relativo regime sanzionatorio e ciò vale anche per le cosiddette IA Generative come ChatGPT. In quest'ultimo caso, a fare la differenza è la trasparenza dei processi e delle informazioni fornite su input dell'utente[6].

[5] https://www.osce.org/fom/ai-free-speech.

[6] «Rischio inaccettabile» laddove i sistemi di Intelligenza Artificiale siano da considerarsi come una vera e propria minaccia per l'utente. La proposta prevede tra questi la manipolazione cognitivo-comportamentale di persone o specifici gruppi vulnerabili. Ad esempio: giocattoli ad attivazione vocale che incoraggiano comportamenti pericolosi nei bambini; punteggi sociali: ovvero, classificazione delle persone in base al comportamento, allo stato socioeconomico o alle caratteristiche personali; sistemi di identificazione biometrica in tempo reale e remota, come il riconoscimento facciale. Tuttavia, sono ammesse alcune eccezioni. Relativamente ai sistemi di identificazione biometrica remota, in cui l'identificazione avviene dopo un ritardo significativo, si potranno utilizzare ma solo se autorizzati e ritenuti necessari per perseguire reati gravi, e solo previa autorizzazione dell'autorità giudiziaria. «Alto rischio»; ovvero, quando i sistemi di IA influiscono negativamente sulla sicurezza o sui diritti fondamentali. Essi sono suddivisi in due categorie. La prima, riguarda i sistemi di Intelligenza Artificiale utilizzati nei prodotti che rientrano nella legislazione sulla sicurezza dei prodotti dell'UE: giocattoli, aviazione, automobili, dispositivi medici e ascensori. La seconda, riguarda i sistemi di IA rientranti in otto ambiti specifici che dovranno essere registrati in un database UE. E, cioè: identificazione biometrica e categorizzazione delle persone fisiche; gestione e funzionamento delle infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso e godimento dei servizi privati essenziali e dei servizi e benefici pubblici; esecuzione di provvedimenti legislativi; gestione delle migrazioni, del diritto d'asilo e il controllo delle frontiere; assistenza nell'interpretazione giuridica e nell'applicazione della legge. «Rischio limitato»: riguarda i sistemi di IA che dovrebbero rispettare requisiti minimi di trasparenza che consentirebbero agli utenti di prendere decisioni consapevolmente sulla base di informazioni ufficiali. Dopo aver inte-

Rischi intelligenti

Così come i vantaggi sembrano essere sicuramente molti, il Parlamento ha messo in guardia anche sulle minacce e i rischi soprattutto in materia di Intelligenza Artificiale[7]. Così, un eccessivo se non un vero e proprio abuso nel ricorrere a sistemi IA o il determinare una vera e propria dipendenza può essere problematico dal momento che investire in applicazioni di Intelligenza Artificiale che si rivelano non utili, o applicare l'Intelligenza Artificiale in compiti per i quali non è adatta. Per esempio utilizzandola per spiegare questioni sociali complesse senza eccessiva dipendenza dall'IA, possono essere interpretate come potenziali rischi dovuti a un minor controllo esercitato sui risultati messi in campo senza considerare la garanzia dei diritti e di non discriminazione, oltre che la sicurezza nei confronti dell'utilizzatore. Anche un minor ricorso a sistemi di IA si trasformerebbe in una pericolosa minaccia alla competitività dell'Unione europea nei diversi settori strategicamente fondamentali quali quello economico, nel porre in discussione la condotta delle politiche relative alla realizzazione del *Green Deal* dell'Unione europea, oltre che significare la perdita di vantaggio competitivo rispetto ad altre parti del mondo, la stagnazione economica e minori possibilità di crescita e di miglior qualità della vita per i cittadini europei.

Il sottoutilizzo potrebbe derivare dalla sfiducia del pubblico e delle imprese nell'Intelligenza Artificiale, da infrastrutture inadeguate, mancanza di iniziativa, scarsi investimenti o, poiché l'apprendimento automatico

ragito con le applicazioni, l'utente può decidere se desidera continuare a utilizzarle. Gli utenti dovrebbero essere informati quando interagiscono con l'Intelligenza Artificiale. Ciò include i sistemi di Intelligenza Artificiale che generano o manipolano contenuti di immagini, audio o video, ad esempio i *deepfake*. Tutti i sistemi di IA ad alto rischio saranno valutati prima di essere immessi sul mercato e anche durante tutto il loro ciclo di vita. Per le IA Generative come ChatGPT, si tratta di rispettare requisiti di trasparenza rivelando che il contenuto è stato generato da una Intelligenza Artificiale, progettando il modello in modo da impedire la generazione di contenuti illegali, pubblicando riepiloghi dei dati con diritti d'autore utilizzati per l'addestramento. Cfr. EU-*AI Act: first regulation on artificial intelligence,* 14-06-2023, consultabile in https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?at_campaign=20226. Vedasi anche: European Commission, *A European Approach to Artificial Intelligence,* https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

[7] https://www.europarl.europa.eu/news/en/headlines/priorities/artificial-intelligence-in-the-eu/20200918STO87404/artificial-intelligence-threats-and-opportunities.

dell'Intelligenza Artificiale dipende dai dati, da mercati digitali frammentati. Certo, una delle più importanti sfide sarà rappresentata dall'individuare le responsabilità dei danni provocati da un device o da un servizio gestito/fornito da una Intelligenza Artificiale e questo richiede l'elaborazione di un quadro normativo europeo che non lasci spazio a interpretazioni nell'individuare quale responsabile lo sviluppatore, il produttore, o lo stesso utente. È evidente che la migliore garanzia di qualità, a fronte delle grandi opportunità di guadagno che derivano dall'investire in IA, non può non trovare nel produttore una delle principali figure responsabili in caso di danni, tenuto conto che una possibile esenzione si trasformerebbe in una scarsa attenzione nella produzione di qualità di sistemi IA affidabili e verso i quali indirizzare la fiducia dell'utente/consumatore.

È altrettanto evidente che il ricorso a sistemi IA nei processi di governance pone anche seri interrogativi su come e in che misura si possano manipolare i dati, dal momento che una distorsione delle informazioni rischia di estromettere dai processi logici di un algoritmo anche dati fondamentali per ottenere risultati importanti o, al contrario, definire giudizi strutturalmente non aderenti con la realtà. D'altra parte, il rischio di *mathwashing*, cioè un «lavaggio matematico» quale risultante di una procedura solo apparentemente neutra ma che, in realtà, è arbitraria, è sempre possibile[8]. Tra gli ulteriori rischi definiti nel quadro UE vi è il fatto che l'Intelligenza Artificiale potrebbe portare a decisioni influenzate dai dati sull'etnia, sul sesso, sull'età al momento dell'assunzione o del licenziamento, dell'offerta di prestiti o persino in procedimenti penali. Ovvero, se non preliminarmente orientata sui diritti non negoziabili ne comprimibili, potrebbe porre a rischio quel principio di non discriminazione che è un fondamento dell'architettura etica europea così come porre a rischio il diritto alla privacy e alla protezione dei dati nel caso in cui fosse utilizzata da apparecchiature per il riconoscimento facciale o per il tracciamento e la profilazione online degli individui.

[8] «Mathwashing» cioè, «Lavaggio matematico». Processo tipico della logica algoritmica in genere è funzionale a imporre politiche di egemonia culturale attraverso il ricorso a un algoritmo che riconosce opinioni umane strutturate in forma matematica. Opinioni che, nei fatti, tendono a riproporre delle cosiddette precomprensioni dei progettisti e/o le serie storiche prese come riferimento. Il risultato è legare il futuro al passato facendo sì che correlazioni contingenti siano percepite come pseudo-relazioni di causa-effetto. C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin, New York, 2017.

Se il web non è uno spazio democratico di certo sistemi di Intelligenza Artificiale potrebbero creare delle camere di risonanza online offrendo solo i contenuti che una persona intende mostrare o divulgare, invece di creare un ambiente idoneo per un dibattito pubblico pluralistico, ugualmente accessibile e inclusivo. Così come, una IA potrebbe essere utilizzata per confezionare video, audio e immagini falsi ma estremamente realistici; veri e propri *deepfake*, dai quali possono derivare rischi finanziari, danneggiare la reputazione e mettere alla prova il processo decisionale. Tutto ciò potrebbe portare alla separazione e alla polarizzazione nella sfera pubblica e, anche, alla manipolazione del consenso, così come danneggiare la libertà di riunione e di protesta, poiché potrebbe tracciare e profilare individui legati a determinate convinzioni o azioni.

Anche sul lavoro i rischi non mancherebbero. Se la digitalizzazione di procedure e processi lavorativi ha determinato una contrazione degli stock occupati è certo che un ricorso alla IA comporterà se non una nuova contrazione, certamente un cambiamento della qualità occupazionale, il che significa che essa potrà creare posti di lavoro migliori purché l'istruzione e la formazione siano capaci di offrire una forza lavoro qualificata. A ciò si aggiungerebbe anche il pericolo che un accumulo di informazioni concentrate su un unico soggetto dominante in una data attività di produzione e/o offerta possano determinare delle distorsioni della concorrenza, dal momento che le aziende con maggiori e migliori informazioni potrebbero ottenere un vantaggio eliminando dal mercato i propri competitor.

Inoltre, sottolineato il fatto che l'Europa è sprovvista di una rete sociale e di vere e proprie catene industriali, soprattutto per quanto riguarda i semiconduttori e microprocessori, questo significa che guardando le due *cloud economy* più importanti come Cina e Stati Uniti, l'economia globale si stia spostando verso una economia immateriale. E chi si sposta su questo piano si sposta su un universo parallelo dove Stati Uniti e Cina rappresentano le uniche voci che possono determinare nuove relazioni di forza giustificate dall'essere le uniche a produrre processori e semiconduttori per le tecnologie digitali, IA e quantistiche.

In una prospettiva ancora più concreta, ciò suggerisce una visione sincera del futuro prossimo dove anche il linguaggio, visto relativamente al

«prompting»[9], diventerà sempre più centrale nel considerare la possibilità che l'utente possa ricevere la risposta migliore in relazione alla qualità della domanda posta dall'utente stesso a una Intelligenza Artificiale. Infatti, più il linguaggio utilizzato sarà preciso e più l'IA darà un responso migliore. Un aspetto che varrà anche per la programmazione. In questo senso Open AI ha dato la possibilità di create delle GPTs. Ovvero, pagando un *quid* si può utilizzare già da oggi una GPT4 e con il linguaggio naturale, pur parlando con dei criteri, si puoi riprogrammare l'IA per farla diventare specializzata in qualcosa che interessa l'utente. Si può insegnare a rispondere in un certo modo e a determinati stimoli, insegnare concetti tecnici specifici che all'IA mancano realizzando, così, una vera e propria Intelligenza Artificiale creata dall'utente per essere al suo servizio[10].

[9] «Response Prompting Procedures». Si tratta di procedure di suggerimento della risposta mutuate da strategie sistematiche utilizzate per aumentare la probabilità di risposta corretta nel mondo umano offrendo opportunità di rinforzo positivo e fornendo e rimuovendo man mano i suggerimenti dati. La risposta viene così sollecitata in ragione delle informazioni ricevute e veicolata a essere la miglior risposta possibile. Così come nella formazione umana, si tratta di trasferire il controllo dello stimolo dal prompt allo stimolo discriminativo desiderato.

[10] In realtà la corsa alle versioni di IA generative è già iniziata e la concorrenza tra Google, Open Ai e la cinese Baidu, l'alter ego di Google, sembra già aver conquistato il palcoscenico del confronto. Nella corsa ad acquisire capacità in materia di IA generativa, vista come l'offerta più immediata a supporto di attività umane quotidiane Google non è stato a guardare il corso di Chat GPT4 di Open Ai e ha proposto Gemini ritenendo che la nuova offerta rappresenti un passo ancora più in avanti rispetto a ChatGPT4 dove al linguaggio naturale che sostiene l'elaborazione di testi nelle varie forme e lingue si aggiungono abilità ad ampio spettro della nuova IA di Google. Questo, poiché si aggiungono abilità multimodali e multimediali che ampliano il campo di azione con lo scopo di far sì che Gemini possa comprendere e combinare diversi tipi di informazioni. Uno dei vantaggi di Gemini sarebbe quello che rispetto a GPT4 di Open AI, che non è in grado di eseguire operazioni matematiche, il modello offerto da Google è anche più avanzato nella matematica e nella codifica specializzata. Per gli sviluppatori/creatori di Google, Gemini non solo raggiunge nella versione Ultra «prestazioni all'avanguardia» in 30 dei 32 benchmark accademici cui è stato affidato lo sviluppo di modelli linguistici di grandi dimensioni ma, altrettanto, il punteggio ottenuto in un test di *Massive Multitask Language Understanding* (MMLU) è stato pari al 90% superando, come comunicato da Google, le prestazioni di un esperto essere umano. In, sostanza, alle competenze testuali e linguistiche associa la creazione di video correlati e altri prodotti multimediali riconducibili al risultato richiesto. Vedasi: https://it.cointelegraph.com/news/how-to-try-google-new-ai-model-gemini-chatbot. Anche la società cinese Baidu ha presentato nell'autunno del 2023 una nuova versione di Ernie AI 4.0. Lo scopo è il confronto con GPT4 di Open Ai, rispetto alla quale per la società cinese, Ernie presenta migliori capacità di comprendere, generare, ragionare e memorizzare. In questo senso, Ernie, a detta della società cinese, si è dimostrata capace di ela-

Questo, rimetterebbe al centro l'importanza dell'istruzione considerata come capacità degli utenti, delle persone di elaborare un linguaggio comprensibile, chiaro e razionale senza il quale l'Intelligenza Artificiale non può capire qual è l'istruzione data e lo scopo da raggiungere. In questo modo, si recupererebbe la qualità del linguaggio e dei suoi contenuti visto che il linguaggio naturale presenta caratteristiche di chiarezza e razionalità utili nel processo IA. Inoltre, altro elemento, *last but not least*, l'Intelligenza Artificiale vista come una possibile super-entità senziente non potrà fare a meno che vedere man mano moltiplicarsi le proprie abilità attraverso l'aumento delle capacità di calcolo. Capacità che saranno direttamente proporzionali alla disponibilità di energia per i computer quantistici che saranno alla base e a supporto delle nuove capacità IA e che richiederanno l'individuazione delle migliori fonti di energia e una revisione dei termini e delle modalità di accesso e di distribuzione e un nuovo sforzo verso il rilancio della fusione nucleare e/o delle mini centrali; strutture, queste ultime, di produzione di energia grazie a reattori piccoli e modulari[11]. Una questione, quella energetica, che non solo rilancia i termini di competizione ma che, per certi versi, rappresenta uno strumento a favore della tutela dell'umano come ultimo gestore di una IA poiché se è l'uomo il detentore del controllo dell'offerta, ogni possibile super-intelligenza non potrebbe avere il sopravvento.

EU-Artificial Intelligence Act

La Commissione europea nell'aprile del 2021 aveva già presentato una propria proposta per definire in maniera chiara un primo quadro normativo all'interno del quale ricondurre la disciplina in materia di Intelligenza Artificiale. L'obiettivo, come ricordato sin dalla proposta, era quello di

borare un video promo relativamente a un'auto sportiva disponendo solo di alcune limitate informazioni di testo (un prompt di testo). Ma non solo. Sempre per gli sviluppatori/creatori di Ernie 4.0, l'aggiornata versione cinese di GPT si è dimostrata capace a risolvere problemi complessi di geometria oltre che rivelarsi adattiva a modificare racconti fantasy o completarli se forniti a testo incompleto o, ancora, a portare avanti ricerche accademiche, riassumere informazioni creando documenti, producendo slideshow e presentazioni. Così in: https://tech.everyeye.it/notizie/chatgpt-cinese-ernie-potente-gpt-4-parola-baidu-677954.html.

[11] *Nucleare: Cingolani insiste: «Va studiata una nuova generazione di mini-reattori»*. In https://www.e-gazette.it/sezione/elettricita/nucleare-cingolani-insiste-va-studiata-nuova-generazione-mini-reattori.

offrire una regolamentazione orizzontale, armonizzata, in materia di Intelligenza Artificiale concentrandosi soprattutto sull'utilizzo specifico di tali sistemi e sui rischi a essa associati[12]. In particolare, nel voler offrire un quadro normativo organico in materia di IA, la Commissione riteneva che il futuro quadro normativo sull'Intelligenza Artificiale avrebbe dovuto raggiungere i seguenti obiettivi specifici:

- garantire che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente sui diritti fondamentali e i valori dell'Unione;
- garantire la certezza giuridica per facilitare gli investimenti e l'innovazione nel campo dell'Intelligenza Artificiale;
- migliorare la governance e l'efficace applicazione della normativa vigente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico per applicazioni di IA legali, sicure e affidabili e prevenire la frammentazione del mercato[13].

La stessa Commissione si proponeva di formulare anche una definizione tecnologicamente neutrale dei sistemi di IA nel diritto dell'Unione stabilendone, in questo modo, una classificazione con requisiti e obblighi diversi adattati, come visto, su un «approccio basato sul rischio» (*risk-based approach*). La valutazione del rischio di impatto sui valori, sulle garanzie e, soprattutto, sui diritti fondamentali dell'Unione evitando, soprattutto, casi di discriminazione o intervenendo sulla libertà di espressione oltre che sulla sicurezza dei cittadini europei e dell'Unione stessa quale attore politico ed economico dovrebbe rappresentare anche in futuro il discrimine sulla possibilità di accesso al mercato continentale da parte di tecnologie IA non direttamente prodotte nello spazio UE.

Iniziativa presa coerentemente con quanto già indicato nel «Libro Bianco» sull'Intelligenza Artificiale del 2020 quale approccio europeo in-

[12] *Regulation of the European Parliament and of the Council Layimg Down Harmonized Rules on Artificial Intelligence (Artficial Intelligence Act) and Amending Certain Union Legislative Acts*. Consultabile in, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[13] *Regulation of the European Parliament and of the Council Layimg Down Harmonized Rules on Artificial Intelligence (Artficial Intelligence Act) and Amending Certain Union Legislative Acts. Explanatory Memorandum*. In, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206. Vedasi anche l'Annesso alla proposta, https://artificialintelligenceact.eu/annexes/.

centrato sull'eccellenza e sulla fiducia[14]. In questo caso le premesse rappresentano le volontà a monte di ogni successiva e possibile regolamentazione considerato che, in un contesto estremamente competitivo delle relazioni globali, un solido approccio europeo viene ritenuto necessario per ottenere il massimo possibile dalle opportunità offerte dall'Intelligenza Artificiale e affrontare le sfide che essa porrà. In questo senso, la Commissione si riteneva determinata a promuovere il progresso scientifico e a preservare i progressi tecnologici dell'Unione europea e garantire che le nuove tecnologie fossero al servizio di tutti gli europei per migliorarne la vita quotidiana nel rispetto dei loro diritti.

Anche il Report dal titolo *Orientamenti etici per un'IA affidabile* redatto dal Gruppo indipendente di esperti sull'Intelligenza Artificiale istituito dalla Commissione europea nel giugno 2018, ha indicato delle linee guida da seguire proponendo un articolato documento nel quale non solo si collocava al centro delle valutazioni il carattere di affidabilità della IA ma, in particolare, si definiva in maniera chiara cosa si intendeva, e si intende, per «affidabilità» (*trustworthy*) e quali dovevano essere le ragioni per le quali la governance dei processi IA rappresenta la vera sfida del domani al netto dei vantaggio che comunque essa potrà apportare nel quotidiano dei cittadini europei[15].

Una sfida che sull'affidabilità aveva già visto, sempre nel 2018, i Paesi OCSE confrontarsi sul tema e indicare anche cinque principi cui l'Intelligenza Artificiale avrebbe dovuto soddisfare per essere ritenuta un acceleratore della crescita e del miglioramento della qualità della vita dell'uomo. Ovvero:

1. portare beneficio a favore delle persone e del pianeta, stimolando la crescita inclusiva, lo sviluppo sostenibile e il benessere;
2. i sistemi di IA andrebbero progettati in modo da rispettare lo stato di diritto, i diritti umani, i valori democratici e la diversità e dovrebbero includere salvaguardie appropriate per garantire una società giusta ed equa, ad esempio consentendo, se necessario, l'intervento umano;
3. ci dovrebbe essere trasparenza e divulgazione responsabile intorno ai si-

[14] *White Paper On Artificial Intelligence - A European approach to excellence and trust*, Bruxelles 19.02.2020. Consultabile in, https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf. F.

[15] High-Level Expert Group on Artificial Intelligence, *Set up by the European Commission Policy and Investment Recommendations for Trustworthy AI*, Gruppo Indipendente di esperti ad alto livello sull'Intelligenza Artificiale. file:///C:/Users/Admin/Downloads/ethics_guidelines_for_trustworthy_ai-it_87FEA6D2-977E-4064-0532C4315EB55247_60430.pdf.

stemi di Intelligenza Artificiale, per garantire che le persone comprendano tutto ciò che è collegato al loro utilizzo e possano sfruttare al meglio i loro risultati;
4. i sistemi di IA devono funzionare in modo solido e sicuro, per tutta la durata delle loro applicazioni, e i potenziali rischi vanno continuamente valutati e gestiti;
5. le organizzazioni e gli individui che sviluppano, utilizzano o gestiscono sistemi di IA dovrebbero essere ritenuti responsabili del loro corretto funzionamento, in linea con questi principi e linee guida[16].

In questo senso, alla base dell'affidabilità di una IA ci sarebbero altri quattro principi fondamentali: il rispetto dell'autonomia umana, la prevenzione dei danni, l'equità, l'esplicabilità. Ma la sfida si giocherà anche nel valutare come e a quali costi ogni IA sarà coerente nel suo agire con la necessità di tutelare i diritti fondamentali visti e interpretati come titolarità non negoziabili né superabili di diritti morali e giuridici riconosciuti al cittadino europeo e posti alla base del funzionamento dell'Unione euro-

[16] Il Parlamento europeo, in particolare, nell'ottobre 2020 aveva già adottato delle risoluzioni riguardanti l'IA ponendo al centro di ognuna di esse etica, responsabilità, diritto d'autore. Nel 2021 sono poi seguite le risoluzioni sull'IA in materia di cooperazione nel diritto penale, istruzione, cultura e audiovisivo. In quel periodo, il Parlamento stesso in materia di etica dell'Intelligenza Artificiale, della robotica e delle tecnologie a essa correlate ha specificamente raccomandato alla Commissione di proporre un'azione legislativa per sfruttare le opportunità e i vantaggi dell'Intelligenza Artificiale, ma anche per garantire la protezione dei principi etici. La risoluzione includeva, in tale senso, un testo della proposta legislativa di regolamento. La proposta del Parlamento veniva presentata nel rispetto dei principi di legalità, sussidiarietà e proporzionalità. E' seguendo queste indicazioni che la Commissione ha proposto un quadro normativo sull'intelligenza artificiale cui affidare il raggiungimento dei seguenti obiettivi: garantire che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente sui diritti fondamentali e i valori dell'Unione; garantire la certezza giuridica per agevolare gli investimenti e l'innovazione nel campo dell'Intelligenza Artificiale; rafforzare la governance e l'effettiva applicazione della normativa esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA; agevolare lo sviluppo di un mercato unico per applicazioni di IA legittime, sicure e affidabili e prevenire la frammentazione del mercato. *European Parliament resolution of 20 October 2020 on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012(INL); *European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence*, 2020/2014(INL); *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies,* 2020/2015(INI); *European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, 2020/2016(INI).

pea. Ciò richiede la volontà di stabilire comuni principi etici di utilizzo, dove il criterio dell'affidabilità rappresenta il vero centro del confronto e la cartina di tornasole sulla qualità dell'Intelligenza Artificiale e sulla garanzia delle funzioni svolte. Realizzare una IA affidabile, insomma, significa definire modalità e termini di esercizio del controllo umano, garantire l'affidabilità tecnica e la sicurezza come la qualità della resilienza in caso di attacchi, il definire un piano di emergenza, garantire la riservatezza e la governance dei dati; cioè, il rispetto della qualità, dell'integrità e delle autorizzazioni all'accesso e uso dei dati.

A ciò si unisce la trasparenza dell'azione condotta compresa la tracciabilità ma, soprattutto, la tutela delle diversità e, quindi, l'affermazione e la difesa del principio di non discriminazione ed equità ivi comprese la prevenzione di distorsioni inique, l'accessibilità e la progettazione universale, e la partecipazione dei portatori di interessi a ogni iniziativa etica in materia di Intelligenza Artificiale. Tutto questo, oltre che includendo ogni azione relativa alla governance dell'IA e del suo impiego all'interno delle politiche di sostenibilità e rispetto ambientale, valutando anche l'impatto sociale e la difesa degli assetti, e dei valori, democratici. In quest'ultimo caso si affermerebbe il principio di responsabilità (*accountability*) visto come necessità di definire e garantire nel tempo la verificabilità e la riduzione al minimo degli effetti negativi e la loro segnalazione[17].

In altre parole, così come enunciato nel Report del Gruppo Indipendente di esperti, l'affidabilità di una IA, considerata come funzionale a offrire di se stessa un positivo impatto in Europa, dovrebbe trovare un'accettazione diffusa di un codice etico universale che riconosca all'Intelligenza Artificiale la capacità di dare potere e proteggere gli esseri umani e la società, aumentandone la conoscenza e la consapevolezza attraverso il suo uso, proteggere l'integrità degli esseri umani, della società e dell'ambiente promuovendo anche un approccio IA sulle attività lavorative e produttive. L'idea stessa di «non lasciare nessuno indietro» dovrebbe rappresentare il paradigma della missione IA cui si intende affidare le sorti di una umanità qualitativamente, si spera, più consapevole.

Ciò però, vuol dire anche dover mettere a punto sistemi e procedute necessari a monitorare l'impatto sociale dell'Intelligenza Artificiale, tra-

[17] M. Kritikos, *Artificial Intelligence ante portas: Legal & ethical reflections*, European Parliament,2019,inhttps://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634427/EPRS_BRI(2019)634427_EN.pdf.

sformando, quindi, anche il settore privato europeo, promuovendo l'adozione della tecnologia e dei servizi di IA in tutti i settori in Europa, ampliando le soluzioni IA che favoriscono l'innovazione e la distribuzione/trasferimento della tecnologia relativa. Ma non solo. Si riconosce anche la necessità di istituire partenariati pubblico-privato per promuovere ecosistemi funzionali se non di settore di Intelligenza Artificiale, attribuendo al settore pubblico europeo il ruolo di rappresentare un catalizzatore/promotore di crescita e di innovazione sostenibile, fornendo servizi realizzati attraverso il ricorso all'IA al cui centro vi deve essere il cittadino europeo. Ciò richiede, però, un approccio innovativo alla governance vista, questa volta, come una piattaforma di decisioni e di guida.

Per raggiungere tali obiettivi, la proposta presentava un approccio normativo definito orizzontale, considerato equilibrato e proporzionato alle possibilità nei vari settori dell'esperienza politica, culturale, economica e sociale dell'Intelligenza Artificiale oltre che all'impatto sul quotidiano dei cittadini europei. Un quadro giuridico idoneo a rispettare i requisiti minimi necessari per affrontare i rischi e i problemi legati all'IA, senza limitare o ostacolare indebitamente lo sviluppo tecnologico o aumentare in altro modo in modo sproporzionato i costi di immissione. L'obiettivo, raggiunto nei termini di accordo conegoziato il 9 dicembre 2023 tra Parlamento e Consiglio, dovrà armonizzare le norme del Regolamento.

La base giuridica della proposta del 2021 e che sopravvive oggi è in primo luogo l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), che prevede l'adozione di misure volte a garantire l'instaurazione e il funzionamento del mercato interno. Inoltre, la natura dell'IA, che spesso si basa su dati ampi e diversificati e che può essere incorporata in qualsiasi prodotto o servizio che circola liberamente nel mercato interno, richiede che gli obiettivi della proposta, e da dicembre del Regolamento che sarà, non possono essere raggiunti efficacemente dai soli Stati membri. Il che significa che l'armonizzazione definita nell'accordo del 9 dicembre doveva risolvere il rischio che un mosaico emergente di norme nazionali potenzialmente divergenti potesse ostacolare il formarsi di una disciplina organica tenuto conto che la tutela del principio di sussidiarietà, anche in questo ambito, non ammette spinte in avanti degli Stati membri quasi a ritenere la disciplina della IA, o di alcuni suoi aspetti, come competenza esclusiva o rientrante nell'ambito degli affari interni sottratti alle materie UE.

Anche in questo caso, la norma di riferimento è da individuarsi nel citato art.114 TFUE visto che si tratta di evitare una ulteriore frammentazione del mercato unico in quadri nazionali "potenzialmente contraddittori" che impediscono la libera circolazione di beni e servizi che ricorreranno all'IA. Questo perché, come ricordato, solo un quadro normativo europeo armonizzato condiviso e soprattutto chiaro rivolto a comunicare una IA affidabile potrà garantire condizioni di parità e proteggerà tutte le persone, rafforzando al contempo la competitività e la base industriale dell'Europa nel settore dell'Intelligenza Artificiale.

Ambizioni intelligenti

Ed è così, che dal 14 giugno 2023, giorno in cui il Parlamento europeo approvava il progetto dell'EU-*AI Act* - tappa fondamentale che ha anticipato ciò che sarà il futuro delle nuove possibilità offerte dall'Intelligenza Artificiale sia in termini di impatto sui cittadini che in materia di governance – si giunge al 9 dicembre 2023, data nella quale si è raggiunto un accordo tra Parlamento e Consiglio UE per la legge sull'Intelligenza Artificiale definita da Thierry Breton, commissario europeo per il mercato interno, «Momento storico». Momento così definito ritenendo che con l'EU-*AI Act* l'Unione europea prova a porsi alla guida della disciplina in materia di IA rispetto al resto del mondo proponendo, e dotandosi, entro il 2024 della prima legislazione organica in materia di uso e limitazioni della IA che ha lo scopo di fissare standard di produzione, disciplina e limitazioni a garanzia dei diritti fondamentali del cittadino europeo.

Lo stesso EU-*AI Act* è il prodotto, nella sua forma di regolamento, del rapporto tra sviluppatori/produttori e utenza, tra governance e destinatari delle scelte politiche, di un quadro di valori condiviso secondo una nuova visione del mondo che non sarà di certo meno competitiva del passato, ma solo più distributiva nelle possibilità/capacità di influenzare le scelte e determinare, in questo modo, la scala gerarchica della credibilità di un soggetto geopolitico. Non ci sono dubbi, quindi, che l'Unione tenti di giocare una propria carta piegando sui propri valori l'uso della tecnologia da IA comprendendo sin da oggi che la sfida nell'essere protagonista nel sistema internazionale - reso sempre più multilaterale nella sua distribuzione del potere - non si giocherà nel mettere in campo politiche di potenza dettate da ambizioni egemoniche su larga scala, ma sulla capacità anche di piccoli ma significativi attori di disporre di una diversa e più alta

qualità di tecnologia IA disponibile per influenzare i mercati, per offrire servizi, per gestire il quotidiano, poiché

> L'approccio dell'UE all'Intelligenza Artificiale è incentrato sull'eccellenza e sulla fiducia, con l'obiettivo di rafforzare la ricerca e la capacità industriale, garantendo nel contempo la sicurezza e i diritti fondamentali[18].

Richiamando tra le diverse iniziative prese dalle istituzioni europee, sicuramente *Shaping Europe's digital future The digital transition should work for all, putting people first and opening new opportunities for business. Digital solutions are also key to fighting climate change and achieving the green transition* e il suo *First report on the State of the Digital Decade calls for collective action to shape the digital transition*[19] rappresentavano e rappresentano due delle migliori premesse per fissare, sin dal 2020, gli obiettivi cui l'UE si sarebbe dovuta ispirare nel gestire una transizione non semplice nel passaggio ulteriore dal solo campo cyber all'interdipendenza fisiologica dello spazio Cyber+IA. Non vi sono dubbi che l'obiettivo, coerentemente con un rinnovato spirito dei trattati sia quello, anche in questa fase di rivoluzione copernicana delle relazioni politiche ed economiche tra gli Stati dettata dalla transizione digitale e dall'avvento dell'IA, di far sì che al centro del cambiamento vi siano le persone al primo posto.

«Plasmare il futuro digitale dell'Europa» non può, allora, che rappresentare un paradigma strategico di ogni elaborazione politica e giuridica che tenda a definire il ruolo della transizione digitale e dell'Intelligenza Artificiale e le norme che ne disciplineranno l'uso, coerentemente con l'architettura di principi e diritti sulla quale si è costruita sino a oggi l'UE e sulla quale si dovranno innestare i prossimi pilastri di governance complessiva.

Insomma, per il Parlamento europeo e per la Commissione, la transizione digitale dovrebbe funzionare per tutti, mettendo le persone al primo posto e aprendo nuove opportunità per le imprese. Le soluzioni digitali sono fondamentali anche per combattere il cambiamento climatico e realizzare la transizione verde[20]. In questa prospettiva *2030. Digital Deca-*

[18] https://digital-strategy.ec.europa.eu/it/policies/european-approach-artificial-intelligence.

[19] *2030. Digital Decade*. In https://digital-strategy.ec.europa.eu/en/news/first-report-state-digital-decade-calls-collective-action-shape-digital-transition.

[20] «Plasmare il futuro digitale» dell'Europa è una prima relazione sullo stato del decennio digitale che chiede un'azione collettiva per plasmare la transizione digitale. In https://digital-strategy.ec.europa.eu/it.

de individua i pilastri posti alla base di un tale approccio europeo e posti a fondamento della EU-*Digital Compass* cui si affida il compito di promuoverne non solo le opportunità, ma anche costruire un rapporto di fiducia nell'agenda digitale europea e nella sfida verso la IA: un'economia digitale, giusta e competitiva; una società aperta, democratica e sostenibile in un'Europa sovrana e competitiva (*Europe as a global leader*)[21].

Se la premessa del Regolamento in materia di IA è che la tecnologia è al servizio delle persone, questo vuol dire perseguire un'adeguata strategia che promuova nuove competenze digitali per ogni cittadino europeo, oltre che garantire la protezione dalle cyberminacce e rassicurare che ogni progresso nell'ambito della IA sarà rivolto a conquistare la fiducia del cittadino europeo, nel suo interesse e nel pieno rispetto dei diritti fondamentali a esso riconosciuti in ambito UE. Nuovi orizzonti di impresa sia in termini di capacità di produzione che di nuovi rapporti di lavoro, tecnologie affidabili nella misura in cui esse favoriscono la dignità del lavoro e del lavoratore semplificandone le funzioni, migliorandone la qualità e la sicurezza dal momento che i processi più a rischio di infortuni potranno essere affidati all'Intelligenza Artificiale oltre ad aprire nuove posizioni lavorative, man mano che le industrie guidate dall'IA cresceranno e cambieranno, sono solo alcuni dei risultati cui si guarda verso una IA tale da favorire un'economia vivace e sostenibile all'interno di una società aperta e democratica. Una economia propria di una Unione europea competitiva e tale da permettere il costituirsi di vivaci comunità di start-up, sostenendo gli sforzi anche delle piccole imprese innovative e in rapida crescita, permettendo un accesso semplificato ai finanziamenti.

Una economia che non rinuncia a essere garante della miglior lealtà e qualità della concorrenza tra le aziende europee. La stessa idea di porre l'Europa in una posizione leader nella transizione digitale e nelle applicazioni dell'IA determina anche le ragioni per realizzare, attraverso le nuove tecnologie, una società sempre più aperta, democratica e sostenibile. Così come, anche la transizione green si modella sulla transizione digitale assumendo l'ambizione di coniugare qualità della produzione e dell'offerta tecnologica con l'obiettivo di far diventare l'Europa climaticamente neutrale entro il 2050, riducendo le emissioni di carbonio anche nel settore digitale.

[21] https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade e anche, file:///C:/Users/Admin/Downloads/Italy_1F3YVDl61gqVi5zTDOAeAW3U8_98653.pdf.

A ciò si aggiunge la volontà di offrire ai cittadini europei un potere di controllo diffuso sulla qualità dei servizi digitali e IA garantendo, nel contempo, una sempre più puntale protezione dei dati personali come, ad esempio, nel creare uno «spazio europeo dei dati sanitari» necessari per la ricerca e per una nuova diagnostica e per cure puntuali cui si aggiungerebbe anche la lotta alla disinformazione online cercando di promuovere contenuti mediatici che siano non solo diversificati ma, soprattutto, affidabili. Per la EU-*Digital Compass*, l'Intelligenza Artificiale potrebbe certamente essere utilizzata per la prevenzione della criminalità e nel governo del sistema di giustizia penale, considerato che grandi volumi di dati potrebbero essere elaborati più rapidamente, i rischi di fuga dei prigionieri potrebbero essere valutati in modo più accurato, la criminalità o persino gli attacchi terroristici potrebbero essere previsti e prevenuti.

In questo senso i contenuti del Regolamento in materia di IA avviato sulla strada di una disciplina organica nei prossimi mesi del 2024, e che una volta definito e approvato entrerà in vigore nei due anni successivi, definiscono la possibilità di concludere accordi di salvaguardia sull'Intelligenza Artificiale per scopi generali, la limitazione all'utilizzo di sistemi di identificazione biometrica da parte delle forze dell'ordine, vengono posti divieti di *social scoring* e di uso dell'Intelligenza Artificiale per manipolare o sfruttare le vulnerabilità degli utenti, si ribadisce il diritto dei consumatori di presentare reclami e ricevere spiegazioni significative e si pongono sanzioni da 35 milioni di euro o del 7% del fatturato globale a 7,5 milioni o 1,5% del fatturato per le imprese/gestori IA che contravvengono alle previsioni normative.

Tutto questo, coerentemente con i presupposti già in discussione nei lavori dei mesi precedenti per i quali l'idea principale è quella di regolamentare la produzione, l'uso dell'Intelligenza Artificiale, nelle sue diverse forme e architetture applicative, in base alla capacità di quest'ultima di causare danni alla società seguendo un approccio *risk-based*. Ovvero, maggiore è il rischio, più severe sono le regole. Inoltre, viene creato all'interno della Commissione un Ufficio IA con il compito di supervisore per quanto riguarda gli sviluppi dell'IA, la promozione di standard qualitativi e test di conformità, oltre che organo di valutazione sulla applicazione delle norme in materia di IA negli Stati membri. A questo, si aggiunge un Comitato IA composto dai rappresentanti degli Stati membri quale organo di coordinamento e consultivo cui si affida il compito di verificare l'attuazione del

Regolamento, oltre a prevedere un Forum consultivo con carattere e funzioni prevalentemente tecniche.

Ovviamente, in ambito UE si ritiene che trattandosi della prima proposta legislativa di questo tipo a livello globale, essa potrebbe rappresentare uno standard globale per la regolamentazione dell'Intelligenza Artificiale anche in altri Paesi se non ispirare una normativa internazionale a riguardo partendo proprio, come ricorda il Consiglio in una nota ufficiale del 9 dicembre 2023, dall'approccio europeo alla regolamentazione tecnologica sulla scena mondiale[22].

E non è un caso, che nel garantire il miglior uso e accesso alle tecnologie IA, o se si vuole proprio l' «affidabilità» (*trustworthy*), il progetto di Regolamento approvato nel dicembre 2023 da Parlamento e Consiglio, oltre a definire le modalità di uso quale acceleratore della competitività economica e di accesso a miglior qualità di servizi, al di là delle finalità di giustizia, si distingue per essere il primo provvedimento organico che pone dei limiti e delle sanzioni a usi non conformi allo spirito dei trattati della IA.

Tra gli usi vietati vi sono il riconoscimento e la potenziale minaccia ai diritti dei cittadini e alla democrazia rappresentata da alcune applicazioni dell'Intelligenza Artificiale. Tra questi in particolare: i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili (es. convinzioni politiche, religiose, filosofiche, orientamento sessuale, razza); la raccolta non mirata di immagini facciali da Internet o filmati CCTV per creare database di riconoscimento facciale; il riconoscimento delle emozioni sul posto di lavoro e nelle istituzioni educative; il punteggio sociale basato sul comportamento sociale o sulle caratteristiche personali; i sistemi di intelligenza artificiale che manipolano il comportamento umano per aggirare il loro libero arbitrio; i sistemi IA utilizzabili per sfruttare le vulnerabilità delle persone (a causa della loro età, disabilità, situazione sociale o economica)[23].

Uno dei terreni più accidentati, comunque, è rappresentato dalle misure biometriche e dal cosiddetto «riconoscimento facciale» (RBI - Remote Biometric Identification). A tal riguardo l'accordo tra Parlamento e Consiglio si è risolto nel concordare una serie di garanzie ed eccezioni circa l'uso dei sistemi di identificazione biometrica in spazi accessibili al pubblico per sco-

[22] *Artificial Intelligence Act: Council and Parliament strike a deal on the first rules for AI in the world*. Così in https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/.

[23] https://www.europarl.europa.eu/news/it/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

pi di contrasto ad attività criminali, previa autorizzazione giudiziaria e per elenchi di reati rigorosamente definiti. Per il cosiddetto RBI «post-remoto», vi si potrà ricorrere ma solo per la ricerca mirata di una persona condannata o sospettata di aver commesso un reato grave. Per il RBI «in tempo reale», i limiti al suo utilizzo sono ricondotti a precise condizioni di tempo, luogo, per la ricerca mirata delle vittime (sequestro, tratta, sfruttamento sessuale), prevenzione di una minaccia terroristica specifica e attuale, o la localizzazione o l'identificazione di una persona sospettata di aver commesso uno dei reati specifici menzionati nel Regolamento (terrorismo, tratta, sfruttamento sessuale, omicidio, rapimento, stupro, rapina a mano armata, partecipazione a un'organizzazione criminale, reati ambientali).

In ogni caso, nelle previsioni e garanzie e nella disciplina vi è racchiusa un'ambiziosa volontà diretta a proteggere la sovranità digitale dell'Unione e sfruttare i suoi strumenti e poteri normativi per definire regole e standard globali in un momento di forte corsa verso la supremazia tecnologica di Cina e Stati Uniti *in primis*. Per questo, oltre al chiarimento di come e in che termini opererebbe il principio della sussidiarietà, l'altro principio definito con chiarezza sin dal 2021 è quello della proporzionalità. Per il Parlamento, la proposta della Commissione, ridefinita e fatta propria dall'accordo tra Parlamento e Consiglio del 9 dicembre, fa riferimento a norme già presenti adattandole, per quanto possibile e proporzionalmente in linea con gli obiettivi prefissati, con quella che sarà l'esperienza dell'IA vista come necessaria oltre che ineluttabile, funzionale a migliorare la qualità della vita dei cittadini europei e garantire maggior competitività all'UE. Obiettivi di sopravvivenza politica ancorati a migliori performance di governance per garantire nel tempo i migliori risultati seguendo un approccio basato sul rischio che impone oneri normativi solo quando è probabile che un sistema di IA presenti rischi elevati per i diritti fondamentali e la sicurezza[24].

[24] Per altri sistemi di IA non ad alto rischio vengono imposti solo obblighi di trasparenza molto limitati, ad esempio in termini di fornitura di informazioni per segnalare l'uso di un sistema di IA quando interagisce con gli esseri umani. Per i sistemi di IA ad alto rischio, i requisiti di dati di alta qualità, documentazione e tracciabilità, trasparenza, supervisione umana, accuratezza e robustezza sono strettamente necessari per mitigare i rischi per i diritti fondamentali e la sicurezza posti dall'IA e che non sono coperti da altre norme esistenti. Le norme armonizzate e gli strumenti di supporto e di orientamento aiuteranno i fornitori e gli utenti a conformarsi ai requisiti stabiliti dalla proposta e a ridurre al minimo i costi. I costi sostenuti dagli operatori saranno proporzionati agli obiettivi raggiunti e ai benefici economici e reputazionali che gli operatori potranno aspettarsi da questa proposta.

Ciò, però, significherebbe far maturare anche una consapevolezza sulla necessità di sviluppare e sostenere infrastrutture di sicurezza informatica specifiche per l'Intelligenza Artificiale, promuovendo la formazione di competenze adeguate in materia, oltre che rivedere anche i sistemi e i modelli educativi nelle diverse fasi riconoscendo e premiando le migliori capacità nel ricorrere all'IA. A tal proposito, l'azione dell'Unione dovrebbe anche guardare a un miglior riposizionamento delle donne nell'ambito della ricerca scientifica e qualificare la forza lavoro, oltre che definire un quadro giuridico unitario già messo in pratica con l'EU-*AI Act*. A ciò segue la necessità di individuare un quadro giuridico chiaro a tutela dell'uso dell'IA e della protezione del know how sotteso oltre che promuovere la ricerca di finanziamenti adeguati per migliorarne la qualità e la sicurezza[25].

Una necessità e una opportunità che trovano la loro copertura giuridica negli articoli 114 e 149 del TFUE. In questa prospettiva emersa anche al richiamato Summit di Londra sull'Intelligenza Artificiale del novembre 2023, gli aspetti sui quali l'azione dell'UE in materia di IA dovrebbe concentrarsi non sono pochi. Si tratterà di permettere di realizzare dati e infrastrutture per l'Intelligenza Artificiale negli Stati membri, sviluppando iniziative di gestione e condivisione dei dati etiche e legalmente conformi in ambito UE. Anche in questo caso, il Summit di Londra ha assunto una sua chiara valenza proprio nel rappresentare un primo e non trascurabile momento rivolto a sostenere nel tempo le leadership e le rispettive governance nello sviluppo di IA.

Insomma, EU-*AI Act* a parte, è evidente che la sfida raccolta si inserisce in una necessità di governare sin dall'inizio un processo irreversibile nel quale uomo e tecnologia seguono i passi della storia, diventando creatori e destinatari di una evoluzione esistenziale che rende sempre più sovrapponibili ricerca scientifica, diritti e sentimenti di una umanità alla continua sfida con la complessità dell'esistente e con le ragioni della sopravvivenza sia essa politica che economica e non solo.

Una nuova disciplina, quella del EU-*AI Act* che dovrebbe rientrare in una visione di un'Europa protagonista in un modello relazionale sempre più competitivo dove la posta in gioco è la supremazia tecnologica. «Un'Europa sovrana e competitiva» si pone, oggi, come una condizione non negoziabile non solo per assicurare la sopravvivenza di un disegno di sempre maggior integrazione, ma per attribuire all'UE un ruolo neces-

[25] M. Kritikos, *Artificial Intelligence ante portas: Legal & ethical reflections,* ...cit.

sariamente almeno da comprimario e non da periferia del mondo, cercando di riconfermarsi quale modello globale per l'economia digitale, sostenendo le economie ancora non perfettamente allineate nel passaggio al digitale, sviluppando standard digitali e promuovendoli a livello internazionale.

VI. La sfida corre sul "quanto" [1]

> Noi siamo il prodotto delle fluttuazioni quantistiche presenti nell'universo primordiale. Chi fosse religioso potrebbe dire che davvero Dio gioca a dadi.
>
> Stephen Hawking e Leonard Mlodinow,
> *Il grande disegno*, 2011.

Tra dimensione cyber e progresso verso l'Intelligenza Artificiale, la corsa alla supremazia tecnologica rideclinata in supremazia quantistica non risparmierà nuove frontiere e non si lascerà intimidire da scrupoli di carattere etico. Nel campo delle IA sembra ormai evidente che la chiave di volta del passaggio da un'era classica a una nuova modernità risiederà nel come e in che modo l'umanità nelle sue diverse forme di espressione riuscirà a superare problemi sempre più complessi, avvalendosi di nuovi supporti ai processi razionali di analisi e deduzione.

In questa prospettiva, il superamento delle vecchie macchine hardware fondate sulla fisicità degli elementi porterebbe a una migliore elaborazione di sistemi IA con capacità di processare dati complessi, aggregati o meno, che avvicinerebbero ogni sistema artificiale al modello umano di elaborazione, aggregazione, scorporo, sistemazione e assunzione logica. In quest'ot-

[1] Il «Quanto» definito nella fisica detta quantistica secondo l'approccio di Max Planck che cercò di trovare una correlazione (*entanglement*) per giustificare i relativi risultati sperimentali che introducevano la teoria dell'emissione elettromagnetica di un corpo nero. Al di là delle prove di laboratorio condotte attraverso oscillatori armonici elettricamente carichi, il «quanto» viene definito come un elemento su scala microscopica capace di assorbire e di emettere radiazioni proprie di una definita frequenza (nel caso sperimentale, coincidente con la frequenza dell'oscillatore). Per Planck, l'energia meccanica totale di ogni oscillatore poteva essere espressa, misurata, solo con valori che fossero multipli interi di una quantità piccola ma finita (e non infinitesima), un «quantum», e pari al prodotto della frequenza "ν", propria dell'oscillatore e di una costante "h" uguale per tutti gli oscillatori, la cosiddetta «costante di Planck» e che è presente in tutte le teorie quantistiche (pari a 6,6·10–34 J·s.). Cfr. voce *Quanto*, In Enciclopedia Treccani; anche in: https://www.treccani.it/enciclopedia/quanto/.

tica, il *Quantum computing* (o calcolo quantistico) rappresenta la nuova ulteriore corsa verso la supremazia quantistica dettata dal riuscire a superare il determinismo (visto come misurabilità in termini matematici dei fenomeni naturali) e sfruttare le tecnologie offerte dalla fisica quantistica. In poche parole, è la complessità e la sua soluzione nelle diverse circostanze che definisce in sé la necessità di superare i computer tradizionali per approdare ai computer quantistici, gli unici a permettere una maggior velocità di calcolo a fronte di una sempre maggior quantità di dati da dover processare.

Tutto questo, perché gli algoritmi quantistici creano spazi a n-dimensioni e n-combinazioni nei quali si definiscono i diversi modelli possibili suggeriti dalle correlazioni dei dati processati, fornendo le diverse e più adeguate soluzioni per un problema complesso. Ciò definisce una qualità fondamentale della dimensione quantistica e di una IA quantistica rappresentata dal poter contare sul *Quantum entanglement*. Ovvero, sulla correlazione quantistica. Cioè su quel legame che si ottiene tra due o più elementi che presentano qualità/proprietà o contengono informazioni correlate e che controintuitivamente vengono assunte anche a distanza come parti di una informazione complessivamente, in un tempo dato, definita[2].

[2] Il «Quantum entanglement» (o correlazione quantistica). Si tratta di un fenomeno e di un enigma allo stesso tempo tipico della fisica quantistica che si risolverebbe nel cosiddetto «paradosso di Einstein, Podolsky e Rosen». Nel 1935 Albert Einstein, Boris Podolsky e Nathan Rosen scrissero un articolo dal titolo *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?* conosciuto anche come «The EPR Paper» dalle iniziali degli autori. In questo saggio lo stesso Einstein, superando un certo scetticismo della prima ora verso l'approccio quantistico, e ragionando «controintuitivamente» rispetto all'approccio tipico della meccanica classica e di una prospettiva deterministica, ancorché ricondotta all'interno della teoria della relatività, sosteneva che non solo la teoria quanto-meccanica del mondo era da considerarsi vera, ma che da queste osservazioni doveva anche derivare il paradossale risultato definito nella possibile relazione di particelle che possono, anche senza aver mai condiviso un sistema, e a informazioni date, correlarsi riconoscendo un comune dato informazionale per il quale il mutamento dell'una avrebbe comportato anche un pari mutamento dell'altra al di là della distanza intercorrente tra le stesse. Questo nuovo spostamento in avanti rispetto alla relatività ristretta formulata anni prima, fece sì che Einstein mutasse l'opinione per la quale, in una precedente lettera a Max Born, scriveva che «Non potrò mai credere che Dio giochi a dadi con l'Universo». Vedasi, A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*, in «Phisycal Review», v.47, May 15, 1935 pp.777-780, consultabile in https://cds.cern.ch/record/405662/files/PhysRev.47.777.pdf. Vedasi anche: D. Aczel Amir, *Entanglement: The Greatest Mystery in Physics,* Basic Books, New York, 2002; trad. it. *Entanglement. Il più grande mistero della fisica*, Raffaelo Cortina, Milano, 2004.

In *Convergence: Artificial Intelligence and Quantum Computing*: *Social, Economic, and Policy Impacts*, Greg Viggiano si indica come sia ormai necessario prepararsi per l'imminente convergenza tra Intelligenza Artificiale e Informatica Quantistica[3]. Una convergenza, attraverso la quale si realizzeranno nuovi mondi nel campo dell'economia globale e dell'ordine geopolitico che sarà. Proprio in questa prospettiva non si può credere che non si sia già oggi affermata una geopolitica digitale le cui determinanti sono rappresentate dal come e in che misura si possano esprimere qualità di governance, oltre che di applicazioni quotidiane, attraverso sistemi IA senza una necessaria disciplina condivisa tra le nazioni.

In verità, bisogna riconoscere che l'Unione europea soffre di un certo ritardo nel condure politiche di sviluppo nel settore del *Quantum computing* e questo rischiando di doversi ritrovare dipendente dalle scelte operate da altri attori geopolitici. È anche vero che nel 2018 l'Unione europea con la *Quantum Computer Flagship* ha cercato di rimettersi al passo accettando la sfida ormai avanzata, tra Cina e Stati Uniti in maniera particolare, verso la ricerca quantistica diretta a migliorare, se non aumentare in termini esponenziali, le capacità computazionali delle nuove macchine. A ciò si è unita anche la *Quantum Technologies Flagship* che si è posta e si pone, oggi, come un'ambiziosa iniziativa di ricerca rivolta a favorire processi di innovazione nel lungo periodo facendo sì che l'Unione europea sia protagonista della cosiddetta seconda rivoluzione quantistica. Una rivoluzione che si affida a una consapevolezza: che l'innovazione sia il vero e irrinunciabile campo competitivo della nuova contrattazione internazionale il cui scopo, mutuato dalle applicazioni nei processi di produzione e distribuzione, colloca al centro le qualità delle leadership oltre che le propensioni e le intenzioni che non sono solo rilavanti da un punto di vista economico, ma che contengono e sottendono scopi politicamente rilevanti nella formazione del consenso o nel determinare la legittimità e la credibilità di una leadership. Una sorta di DARQ-power (*Distributed Ledger*, *AI*, *Extended Reality*, *Quantum Computing*) trasfigurato in una dimensione politica.

Si realizza, così, quella rivoluzione che poggia sull'interrelazione tra tecnologia, modelli e sistemi quantistici che proprio dall'interrelazione tra particelle, quanti di informazione (qubit), permette di creare legami, meglio «correlazioni», a distanza (*entanglement*). In altre parole, traducen-

[3] G. Viggiano (ed), *Convergence: Artificial Intelligence and Quantum Computing*: *Social, Economic, and Policy Impacts*, John Wiley & Sons Inc, Hoboken, 2022.

do sul piano pratico, la possibile complementarità tra *Quantum computing* e IA di certo permetterebbe di poter offrire, all'IA, informazioni sempre più dettagliate rispetto a quelle di partenza potendo non solo processare un maggior numero di dati, ma potendosi affidare alla correlazione di dati acquisiti dove ogni qubit processato è il risultato della misura di un altro qubit e così via al di là delle distanze e delle fonti. Si raggiungerebbe, in sostanza un'architettura di elaborazione dati simile a quella umana e aggiornabile man mano che sempre più dati verranno a essere acquisiti e processati correlazionalmente.

L'*entanglement*, infatti, unitamente alla sovrapposizione, rappresenta il cuore del funzionamento del computer quantistico dal momento che, molto semplicemente, senza l'*entanglement*, non si potrebbero correlare i dati con le informazioni di volta in volta ricevute[4]. È evidente che le possibilità aperte dalla tecnologia quantistica e dalla IA determineranno una nuova corsa verso la supremazia tecnologica la quale imporrà anche questioni di sovranità della ricerca e una ricollocazione delle attività economiche a essa collegate con una necessità di *decoupling* che determinerà nuove possibili competizioni e attriti tra le potenze in gioco, in particolar modo tra Cina e Stati Uniti. D'altronde, non vi sono dubbi, e ciò rappresenta un termine di confronto per l'Europa ma anche per gli Stati Uniti che la Cina in materia di Intelligenza Artificiale abbia raggiunto risultati importanti superando la soglia della sola IA generativa.

Tuttavia, il forte legame con la tecnologia cinese, soprattutto nel campo dell'apprendimento e dell'automazione dei processi, diventa oggi una condizione importante per l'Unione europea soprattutto nell'ottica di difendere una propria autonomia attraverso la quale raggiungere risultati di egemonia tecnologica; cioè, dimostrare di possedere i migliori *net-assessment capacitivi*, al netto di una minima se necessaria e sostenibile, interdipendenza con il proprio alter ego geopolitico[5]. E, questo, nella consapevolezza che Cina e Stati Uniti non rifuggono da possibili accordi per dividersi il quanto

[4] L'iniziativa «Quantum Technologies Flagship» ha lo scopo di sostenere la ricerca in un arco temporale definito in 10 anni. Il bilancio previsto è di un miliardo di euro. Cfr. Commissione europea, *Plasmare il futuro digitale dell'Europa.Tecnologia quantistica Flagship*. In https://digital-strategy.ec.europa.eu/it/policies/quantum-technologies-flagship. Vedasi anche *Shaping Europe's digital future, Quantum Flagship: a major boost for European Quantum Research*, July 11, 2019.

[5] J. Bateman, *US-China Technological "Decoupling". A Strategy and Policy Framework*. Carnegie Endowment for International Peace, April 25, 2023.

di supremazia esercitabile sui mezzi di produzione delle tecnologie che servono per strutturare il nuovo mondo. Una strategia che sottende l'obiettivo di deindustrializzare i possibili competitor per dominare il mercato high tech di domani.

Lo stesso Kai-Fu Lee in *AI Superpowers: China, Silicon Valley, and the New World Order* non lesina anche di lanciare un proprio monito per il quale a causa di tali sviluppi senza precedenti nell'Intelligenza Artificiale, cambiamenti significativi avverranno molto prima di quanto ci si potrà aspettare. Infatti, mentre la competizione sull'Intelligenza Artificiale tra Stati Uniti e Cina inizia a correre su piani di particolare competizione, si auspica che gli Stati Uniti e la Cina possano accettare e riconoscere le grandi responsabilità che derivano da un significativo potere tecnologico, perché la stessa IA non potrà non modificare anche i rapporti di lavoro. Argomento, quest'ultimo, con il quale l'Unione di domani sarà costretta a fare i conti per non subire le conseguenze di un progressivo depauperamento delle capacità economiche e produttive e rassegnarsi a una condizione di dipendenza, di colonialismo tecnologico[6].

Insomma, tecnologie quantistiche e Intelligenza Artificiale determineranno nuove implicazioni geopolitiche e nuovi equilibri, maggiori velocità di elaborazione dati e di gestione delle attività umane fornendo in tempi brevi le migliori soluzioni per problemi complessi di governance pubblica o privata, nel campo politico come in quello economico e dei servizi, ad esempio, offrendo una delle prestazioni più critiche: quella di riuscire a inserirsi nei processi di produzione e di governo attraverso capacità crittografiche o di decrittazione. Anzi, proprio la distribuzione a chiave quantistica (*Quantum key distribution* - QKD) rappresenta uno dei vantaggi fondamentali nell'assicurare comunicazioni sicure e tutela di know how considerato che per garantire comunicazioni sicure, si abilitano le due parti a produrre e condividere una chiave segreta casuale, valida solo tra le stesse parti e che potranno usare per cifrare e decifrare i loro messaggi[7]. Già alcuni

[6] A tal proposito, vedasi: L. Kai-Fu, *Al Superpowers: China, Silicon Valley, and the New World Order*, Mariner Books, Boston, 2021.

[7] Come ricordava l'International Institute for Strategic Studies già nel 2019 «Il campo della scienza dell'informazione quantistica sta dando origine a molteplici nuove applicazioni legate alla difesa che sono spesso raggruppate sotto l'unico soprannome di "quantistico", ma che meritano una considerazione indipendente. La distribuzione delle chiavi quantistiche (QKD), la crittoanalisi quantistica e il rilevamento quantistico, infatti, influenzeranno in maniera significativa la sicurezza strategica in modi diversi. Ad esempio,

anni fa, al 4° Forum europeo sulla sicurezza informatica, Cybersec Summit 2018, tenutosi a Cracovia in Polonia, fu ben sottolineato il rischio che nazioni tecnologicamente più capaci con tecnologie quantistiche maggiormente performanti potrebbero imporre obblighi di trasparenza delle comunicazioni ai propri competitor mentre si avvalgono a loro tutela e/o vantaggio delle migliori QKD disponibili.

D'altronde, velocità e volume computazionale di un processore definito come quantità di operazioni logiche eseguibili prima, unite alle capacità di elaborare sequenze crittografate delinea molto bene quali siano i punti di forza di una superiorità quantistica e quanto peserà il gap tecnologico esprimibile in termini di competitività non solo economica, ma anche politica. Questo, aumentando la velocità di comprensione di un fenomeno e la velocità di risposta con tutto ciò che ne deriva in termini di sicurezza nazionale, laddove la sicurezza delle linee di comunicazione, quanto la penetrabilità delle stesse, faranno tutta la differenza del mondo.

La tecnologia non è certo un campo neutrale alle dinamiche geopolitiche. Al contrario, essa rappresenta un acceleratore delle possibilità di affermazione di egemonie costruite sulle migliori disponibilità di nuovi sistemi a supporto del confronto economico come di quello militare. Lo stesso concetto di «forza soverchiante», definito da Winston Churchill in tempi diversi presenta però una sua validità ancora oggi anche se la supremazia tecnologica era già ben definita come fattore di potenza nella corsa alla supremazia nucleare, allo stesso modo, e in termini più invasivi e solo apparentemente meno distruttivi, essa si propone come condizione ancora più efficace per la supremazia tecnologica nel campo della dimensione cyber-quantistica e della IA acquisendo un livello di penetrabilità delle comunità al momento mai raggiunto.

Al netto dei dati tecnici di funzionamento dei componenti dei computer quantistici, da un punto di vista di impatto sulla vita quotidiana, è sin troppo evidente, ormai, che la complementarità tra Intelligenza Artificiale e nuova dimensione cyber, declinata in termini quantistici, porrà il

la QKD offre ai difensori un vantaggio a breve termine per proteggere le loro comunicazioni, mentre la crittoanalisi quantistica è una capacità intrinsecamente offensiva, sebbene stia maturando a un ritmo più lento. L'informatica quantistica generalizzata offrirà molte altre possibilità, ma in questa fase sono troppo incerte per consentire un'analisi concertata dei loro effetti di secondo ordine». *The Military Balance 2019*, February 2019 pp. 18-20, Publisher: IISS https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/quantum-computing-and-defence.

problema di come controllare nuovi sistemi IA fortemente generalistici; cioè, capaci di processare dati al di fuori di specifici compiti attraverso nuove logiche algoritmiche capaci di autodefinire regolarità tra dati prescindendo dal compito definito assegnato. In poche parole, Intelligenze Artificiali che si traducono quali metaorganismi/entità senzienti approssimandosi alle capacità umane. È anche vero, però, in uno scenario positivo, ma vincolato alla formazione di una coscienza universale maturata all'interno di convenzioni internazionali realizzate ad hoc, che una computazione quantistica può anche assicurare una parità di vantaggio competitivo nella misura in cui la tecnologia *Quantum computing* sia resa disponibile sui mercati garantendone un accesso allargato ed equamente distribuibile. Ciò significa, in altri termini, che pari condizioni di accesso renderanno meno rischioso l'affermarsi di posizioni di *supremacy* nelle relazioni economiche, sociali e politiche tra gli Stati/soggetti utilizzatori.

Interessante anche l'aspetto militare che meriterebbe una trattazione a parte circa le opportunità che si aprirebbero nell'adozione di sistemi quantistici. In questo ambito la cosiddetta Scienza dell'informazione quantistica (*Quantum Information Scienze* - QSI) rappresenta il terreno di confronto sul piano della capacità di applicare la migliore comprensione del mondo subatomico, quello quantistico, rappresentato, come ben descritto in N*ational Strategic Overview for Quantum Information Science* da tecnologie che includono al loro interno non solo la microelettronica dei semiconduttori, ma anche il sistema di posizionamento globale (GPS) o la risonanza magnetica (MRI) quali sistemi significativi ormai di ogni architettura relativa alla difesa dell'infrastruttura economica o della difesa nazionale[8]. In questo senso, non solo si tratta di definire termini e limiti di proliferazione, ma anche termini e modi per realizzare una cooperazione che garantisca pari qualità nel gioco delle opportunità.

D'altronde, non ne fa un mistero neanche l'Istituto Internazionale di Studi Strategici laddove ricordava, già qualche anno fa, quanto e in che misura l'integrazione delle tecnologie quantistiche rappresentasse già uno dei progressi più attesi per le forze armate e non solo nei processi di elaborazione delle informazioni e comunicazioni e nel supporto alle decisioni, quanto alle capacità e rapidità di scoperta di sistemi d'arma, vettori e portatori di minaccia nelle diverse dimensioni e ambienti, da quelli

8 https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

terrestri a quelli sottomarini sino a rendere obsolete le stesse tecnologie *stealth* di ultima generazione[9].

Gli Stati Uniti, dal canto loro, di certo non perderanno tempo nel condurre una politica orientata verso la supremazia quantistica alla stessa stregua di Cina e Russia e del Regno Unito, quest'ultimo orientato con un proprio programma a creare una comunità coerente di tecnologia quantistica governativa, industriale e accademica. Insomma, come si può notare, non si tratta solo del volume di finanziamenti messi in campo, ma della possibilità se non della consapevolezza che disporre della migliore tecnologia per definire in termini di processo informazionale le migliori scelte nel campo economico come politico e politico-strategico rappresentano la nuova frontiera delle politiche di potenza. Dalle capacità di rilevamento e scoperta alle comunicazioni e alla loro sicurezza, alla guerra in altre dimensioni la tecnologia quantistica è a ragione ritenuta una tecnologia trasformativa. Un aspetto non secondario se si accetta il fatto che la sfida, come si vedrà, nel campo del *Quantum computing* sarà di riuscire a correlazionare informazioni che sembrano sfuggire alle capacità logico-deduttive umane dimostrando, al contrario, una propria correlazionalità.

Proprio di fronte a simili nuove traiettorie, che collocheranno al centro di ogni scelta il differenziale tecnologico esprimibile, l'Unione europea ha cercato di mettere un primo punto proprio con la EU-*Quantum-technologies Flagship*. Un programma articolato su quattro principali aree della tecnologia quantistica: comunicazione, calcolo, simulazione e rilevamento.

Una necessità che l'Unione europea dovrebbe considerare se la sovranità tecnologica rivisitata in chiave quantistica può avere un senso di fronte alla troppo semplice subordinazione nell'affidarsi a tecnologie prodotte altrove credendo che abbattendo i costi della ricerca, e fruendo delle altrui eccellenze, ciò possa garantire nel tempo una competitività che prima o poi farà conti con il principale fornitore di tecnologia. Probabilmente, ponendosi in quest'ottica, non è di certo fuori luogo ribadire e rinnovare la validità delle due norme fondamentali del libero mercato che ne garantiscono anche un'autoregolamentazione da porre alla base di una disciplina dei mercati relativi allo scambio di tecnologie quantistiche: quella dell'applicazione nelle forniture della regola della nazione più favorita, e nella di-

[9] *The Military Balance 2019*, February 2019 pp. 18-20. Publisher: IISS. Vedasi in: https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/quantum-computing-and-defence.

stribuzione degli acquisti, quella della reciprocità. In questo modo si favorirebbe un necessario livellamento tra le possibilità/opportunità, ma anche una migliore distribuzione qualitativa tra le parti.

Il QFS tra mito e possibilità

Senza cadere nelle tentazioni o nel fascino di singolari teorie è evidente che l'evolversi del *Quantum Computing* non potrà che avere anche degli effetti significativi nel rimodulare le operazioni sui mercati azionari come in quelli finanziari. In un certo senso, si potrebbe anche valutare come e in che misura il *Quantum Financial System* (QFS) possa sostituirsi allo SWIFT (Society for Worldwide Interbank Financial Telecommunication), in un momento nel quale le sanzioni rappresentano l'arma ritenuta più percorribile per condizionare le scelte di un attore evitando il confronto diretto. In un certo senso, il *Quantum Financial System* è un nuovo sistema finanziario che alcuni ritengono potrebbe rivaleggiare con il sistema SWIFT in futuro ed eliminare la corruzione, l'usura e la manipolazione all'interno del sistema bancario. In ogni caso è importante notare che il sistema finanziario quantistico non si basa su alcuna tecnologia o infrastruttura riconosciuta o pubblicamente nota.

Inoltre, non esistono prove verificabili a sostegno dell'esistenza o dell'implementazione di un tale sistema. In teoria il QFS è un sistema finanziario teorico che dovrebbe competere con il sistema bancario esistente affrontando, e risolvendo, problemi come la corruzione e la manipolazione nel settore finanziario. Per i promotori del QFS, questo utilizzerebbe l'Intelligenza Artificiale e l'informatica quantistica per rivoluzionare le transazioni finanziarie ed eliminare la necessità di sistemi tradizionali come SWIFT. In questo senso, la sfida viene riportata sulla possibilità di resistere ai tentativi di violazione della crittografia da parte dei computer quantistici, che potrebbero ridefinire la sicurezza dei dati nel mondo digitale. Per i promotori delle criptovalute e di una nuova dimensione della gestione dei portafogli, il QFS offrirebbe diversi vantaggi grazie alla più ampia capacità di calcolo, a un'analisi avanzata dei dati, una maggiore sicurezza, l'ottimizzazione del portafoglio.

Ovviamente, un QFS si avvarrebbe di una IA che si sostituirebbe alle banche, gestendo direttamente i portafogli senza ricorrere a intermediazioni per le transazioni, potendo contare sulla possibilità di sfuggire ai tentativi dei computer quantistici di penetrare all'interno delle forme di crit-

tografia utilizzate in campo digitale. Che si tratti però di una possibilità congetturata ma non realizzata, resta il fatto che il processo di conversione in valute digitali da parte delle Banche centrali è ormai avviato. Tuttavia è indubbio che, al di là della realizzazione di QFS, di certo è che l'integrazione delle tecnologie quantistiche nelle scelte finanziarie avrà il potenziale per cambiare il modo in cui funzioneranno i prossimi sistemi finanziari.

Maggiore capacità computazionale, elaborazione di algoritmi a velocità superiori rispetto alle architetture informatiche e agli algoritmi tradizionali permetteranno di processare quantità di dati tali da determinare le migliori scelte per gli investimenti avvalendosi di analisi del rischio maggiormente puntuali per fare la migliore scelta, al miglior rendimento e al minor rischio possibile. D'altra parte, gli algoritmi quantistici di apprendimento automatico possono contribuire, elaborando una maggior quantità di dati correlandone il significato in relazione al risultato da conseguire; a migliorare, ad esempio, la stessa lotta alle frodi finanziarie oltre che offrire le migliori previsioni di mercato per i prodotti che si intenderanno allocare secondo tendenze e opportunità. Sicuramente la crittografia quantistica permetterà una maggior sicurezza delle informazioni sensibili, riducendo il rischio di attacchi informatici o di sottrazione di dati dovuti ad accessi non autorizzati attraverso operazioni di *phishing*.

Il futuro?
Un continuo presente

> È il cambiamento, il cambiamento continuo, il cambiamento inevitabile, che è il fattore dominante nella società odierna. Nessuna decisione sensata può essere più compiuta senza tenere conto non solo del mondo come è ora, ma di come sarà [...]. Questo, a sua volta, significa che i nostri uomini di stato, i nostri imprenditori, i nostri uomini comuni, devono orientarsi verso un modo di pensare fantascientifico.
>
> Isaac Asimov, *My Own View*,
> The Encyclopedia of Science Fiction, 1978.

Come visto nelle pagine precedenti, l'obiettivo di ogni vera e propria dottrina di difesa e reazione a un attacco cyber non può prescindere sia in termini di *policy* che di strategia conseguente dal realizzare un modello di resilienza per affrontare quelli che vengono definiti shock globali. D'altronde, non è certo fuorviante ritenere che una delle priorità dei prossimi anni sarà di individuare il modo nel quale l'ecosistema digitale si interseca con il contesto internazionale in materia di sicurezza, concorrenza economica e affari militari. Per questo sarà sul come affrontare e risolvere le condizioni di crisi diffusa determinate da incertezze maturate e/o indotte a vario titolo sui mercati, come sugli assetti politici e geopolitici, sulla loro frequenza, che si definirà una nuova leadership tecnologica. Una leadership solo apparentemente orizzontale ma verticale nei fatti e nelle ambizioni, capace di anticipare eventi la cui gravità non giustificherebbe comportamenti di sottovalutazione dettati dal considerarli troppo complessi per affrontarli in termini preventivi. L'incertezza, infatti, non può giustificare una inazione.

Cadere nella trappola del *Black Swan* di fatto rappresenta un rischio da evitare attraverso la capacità di porre in essere strategie per identificare e iniziare ad affrontare eventi estremi incerti, con l'elaborazione di un ragionevole caso di peggiore scenario. Questo significa che i governi do-

vranno essere preparati ad accettare un certo livello di rischio e ad affrontare una indesiderata eventualità. Credere che la sola regolamentazione in materia di cybersicurezza possa garantire ampi margini di serenità è una convinzione velleitaria in un mondo, quello cyber, governato dalla imprevedibilità della minaccia e dalla complessità dei processi nei quali questa si inserisce.

Costruire modelli di resilienza per garantire la tenuta dei sistemi critici in caso di attacco, prevedendo una capacità di riserva adeguata, significa non solo garantire la sopravvivenza fisica dell'infrastruttura-bersaglio, quanto riuscire a diluire gli effetti negativi derivanti da attacchi la cui provenienza non è immediatamente identificabile, assicurandosi capacità di risposta e almeno sufficienti a limitare i danni. A tal proposito, diventano sempre più necessarie politiche pubbliche e buone strategie idonee a gestire gli eventi dei prossimi anni. L'Unione europea e i suoi membri dovranno essere pronti ad agire ad ampio spettro sulle minacce possibili provenienti da un altrove non individuabile in tempo reale. Questo richiede il dover definire una *policy* comune, mettere in campo una strategia che veda la partecipazione di ogni attore istituzionale, governativo e non governativo, una collaborazione civili-militari dettata dal fatto che la minaccia cyber non è una minaccia che si pone limiti di aggressione e dove l'obiettivo civile apparentemente può anche trasformarsi in obiettivo militare. Ciò presuppone anche la capacità di poter continuare nel tempo ad affidarsi a modalità di allerta precoce che possono essere definite solo attraverso la maturazione di una consapevolezza della situazione nazionale e dei rischi che possono provenire da minacce esterne, ma anche interne con il loro propagarsi rapidamente incidendo sugli interessi nazionali. Ma non basta.

Diventa necessario anche tener conto di un altro aspetto importante rappresentato dalla cosiddetta «situational awareness» considerata come la conoscenza e la percezione delle vulnerabilità; ovvero, delle attività minacciose, dei rischi cui possono essere esposte le architetture digitali oltre agli impatti e come questi possono influire sul normale e corretto funzionamento e sulla sicurezza delle infrastrutture digitali come di un'organizzazione che si muove nel cyberspazio. Un approccio che tenderebbe a limitare il concetto di *brinkmanship*, ovvero del «rischio calcolato», ma che aggiunge, al contrario, una consapevolezza del rischio e dei danni possibili guardando in termini globali (*global information awareness*) secondo pro-

spettive diverse e multidimensionali, ma convergenti nell'assicurare sicurezza. È evidente che un'analisi e una successiva consapevolezza situazionale va di pari passo con una capacità di dotarsi di un dominio informazionale adeguato a proteggere le funzioni affidate a una infrastruttura digitale. Significa riuscire a dotarsi di capacità di gestione dei processi decisionali multidominio; cioè, tali da essere in grado, in qualunque momento, di ben valutare la situazione contingente rispondendo adeguatamente alle possibili minacce.

Per questo, condividere, ricevere, integrare le fonti di informazione dei partner nella valutazione del rischio rappresenta il presupposto fondamentale di ogni strategia di risposta a una *cyber threat* ma, soprattutto, la precondizione per potersi garantire una sicurezza credibile che si identifica nella resilienza esprimibile e che preveda anche adeguate contromisure. Ma tutto questo potrebbe non essere ancora sufficiente. Vi è anche una resilienza sociale necessaria e che fa la differenza nella tenuta di una comunità politicamente e economicamente organizzata, e che si riferisce alla capacità di questa di adattarsi a possibili condizioni avverse e ripristinare un senso di normalità da uno shock esterno.

È evidente che, anche nella Quinta come, sorprendentemente anche nella Sesta dimensione metaversica, il tempo resterà una risorsa strategica e la sua gestione un paradigma fondamentale nel successo di una pianificazione a difesa di minacce dematerializzate. Infatti, tanto più si dilatano i tempi di risposta e meno rapidamente la comunità-bersaglio potrà recuperare completamente la sua capacità se non la sua sovranità, nel caso di minaccia alla esistenza della stessa, sia in senso economico che politico. Come si potrà intuire, tutto questo non lascia spazi di immunità dal rischio e suggerisce che promuovere una cultura della resilienza significa anche dare priorità alle componenti più vulnerabili della società, siano esse architetture di governance che soggetti che soffrono di non adeguate capacità psico-fisiche o che non godono di adeguate condizioni economiche di sussistenza o di partecipazione alla vita civile. Condizioni e soggetti la cui vulnerabilità può essere l'oggetto di attacco per creare instabilità sociale. In altri termini, si tratta di sostenere politiche e provvedimenti tali da rafforzare quegli anelli deboli della comunità che si presentano come dei pericolosi *gate*, dei portali di accesso dai quali, una volta penetrati nell'intimità della società, diventa difficile arginare minacce il cui profilo operativo è quello di allargare la propria azione su più obiettivi.

Nel 1978 il Presidente francese Valery Giscard d'Estaing, nel rivolgere una lettera al proprio Ispettore generale delle finanze sottolineava come

> Les dévelopment des applications de l'informatique est un factor de transformation de l'organisation économique et sociale et du mode de vie: il convient que notre société soit en mesure, à la fois, de le promouvoir et de le maîtriser, pour le mettre au service de la démocratie et du developpement humain[1].

L'Ispettore generale delle finanze, nel rispondere al Presidente, a sua volta scrisse che,

> La réflexion sur l'informatique et la société renforce la convinction que l'équilibre des civilisations modernes repose sur une alchimie difficile: le dosage entre un exercice de plus en plus vigoreux, même s'il doit être mieux cantonné, des pouvoirs régaliens de l'Etat, et une exubérance croissante de la société civile. L'informatique, pour le meilieur ou pour le pire, sera un ingrédient majeur de ce dosage[2].

Oggi, l'Unione europea ha di fronte a se una scommessa con il suo futuro che dovrebbe guardare soprattutto al garantire una nuova figura di cittadino europeo che non si esaurisca solo nel definirlo un destinatario, quanto un dominus della *noosphera* che lo avvolgerà sempre di più nei prossimi anni e che con l'evoluzione ulteriore del cyberspazio sarà costretto a condividere il ruolo di attore con l'Intelligenza Artificiale e le opportunità che saranno offerte dai computer e relative applicazioni quantistiche.

L'idea di rideterminare il rapporto tra macchina e utente non rappresenterà solo uno scopo etico, ma strategicamente necessario se l'Europa vorrà non solo procedere a una integrazione reale e concreta perché condivisa, ma affidare la propria sicurezza a ogni cittadino che si sentirà responsabile del proprio e dell'altrui futuro. Per fare questo, si dovrebbe far sì che la cosiddetta «Società in Rete» eviti che essa, la società, sia sprovvista di conoscenza e consapevolezza tecnica evitando che i cittadini siano solo destinatari di profilazioni manipolabili per finalità di consenso politico o commerciale. Si tratterà di rendere i cittadini della Rete cittadini europei, dove il senso di libertà deve essere coniugato con un principio di

[1] Lettera di Valéry Giscard d' Estaing a M. Simon Nora, Ispettore Generale delle Finanze, Parigi, 20 dicembre 1976. In S. Nora, A. Minc, *L'information de la société. Rapport à M. le Président de la Republique*. La Documentation française, Paris, 1978.
[2] *Ibidem*.

responsabilità. Si dovrebbe riuscire a far sì che l'idea di una possibile democratizzazione della Rete sia un valore fondamentale della nuova Europa e non una utopia così considerata se prevarrà ancora una volta una dimensione tecnocratica dell'UE che farà perdere di significato a quella cittadinanza europea che si risolve nell'abbattimento dei confini e nella velocità delle scelte e delle azioni comuni operate e condotte nell'interesse comune.

Non per nulla Jaron Lanier nel suo *Maoismo digitale. I pericoli del nuovo collettivismo online* si chiedeva

> Cosa impedisce a una massa online di persone anonime ma connesse di trasformarsi improvvisamente in una folla cattiva, proprio come le masse di persone hanno più e più volte nella storia di ogni cultura umana? È sorprendente che i dettagli nella progettazione del software online possano far emergere potenziali così diversi nel comportamento umano. È tempo di pensare a quel potere su base morale[3].

Il vero problema dei prossimi anni è riuscire a evitare di raggiungere quel punto di non ritorno, quell'orizzonte degli eventi o, meglio, «orizzonte della scomparsa» come definito da Jean Baudrillard per il quale raggiunto un livello di manipolazione possibile dell'evento e della sua narrazione diventa poi difficile riuscire a definire le nostre esistenze se non al di fuori di quella realtà virtuale cui si attribuisce un significato esistenziale, per il singolo, e di governance, per le strutture politiche all'interno delle quali si perde l'idea stessa di realtà. In questo processo di *acting-out*, come descritto da Baudrillard, si consumerebbe la fine dell'umanità pensante e il suo pieno affidarsi alle capacità digitali e metaumane dell'Intelligenza Artificiale in un mondo nel quale l'iperrealtà dominerebbe ogni nostra espressione vitale e definirebbe il nostro quotidiano secondo una nostra percezione costruita su sentimenti veicolati da volontà altrui[4].

Probabilmente l'idea del futuro racchiude non solo la necessità di dare un ordine possibilmente condiviso al caos determinato dalla ridondanza delle informazioni e dei dispositivi, ma ricordando George Charles Beresford, più noto come Herbert George Wells, già autore di *A Tale of the Twentieth Century* e di *A Vision of the Past*, pubblicati entrambi nel 1887, per il quale le nuove conquiste tecnologiche, la via sempre più rapida verso

[3] J. Lanier, *Maoismo digitale. I pericoli del nuovo collettivismo online,* Edge Foundation, Inc. 29 maggio 2006, revisione seriale. 33 (1): 45–53. doi: 10.1016 /j.serrev.2006.11.002.
[4] J. Baudrillard, *La scomparsa della realtà*, Fausto Lupetti, Bologna, 2009 p. 21 e ss.

la conoscenza e il ridursi dei confini materiali e immateriali per effetto dei progressi nei trasporti e nella comunicazione farebbero sì che

> Le idee, le considerazioni assumono più efficacia di qualunque personalità, e più forza dell'interesse partigiano. Reso noto a tutti, il progetto comune può essere difeso contro ogni stravolgimento e tradimento. Può essere elaborato con fermezza e su una base molto ampia, senza che il suo sviluppo sia ostacolato da malintesi personali, locali o di parte[5].

Lo stesso Cooper Ramo nel suo *Seven Sense: Power, Fortune, and Survivor in the Age of Networks* non lascia dubbi sui progressi delle reti ormai entrate nella vita di ogni individuo costruendo vere e proprie architetture esistenziali, dove a ogni struttura e a ogni dispositivo corrispondono regole e sentimenti d'uso, una nuova sensibilità ai ritmi progressivi della storia cui faceva riferimento Nietzsche, ripreso dallo stesso Cooper Ramo[6]. Una sorta di necessità di sopravvivere all'accelerazione della storia dettata dal progresso tecnologico che fa sì che l'asticella del nuovo uomo si sposti su un «settimo senso» attraverso il quale la conoscenza, le relazioni e le interrelazioni si muovono su un universo quotidiano costantemente connesso. Un universo quotidiano, dove i processi neurali alla fine si accompagnano a necessari surrogati tecnologici che ne moltiplicano le capacità rendendo l'uomo autore e destinatario delle sue creature e delle semplificazioni che la logica dei processi elaborativi di informazioni complesse determina e conduce ai risultati dal momento che, proprio nei sistemi complessi, il potere viene definito in termini di concentrazione piuttosto che di distribuzione.

[5] Tutte le organizzazioni operano su quello che è noto come il limite del caos. È uno spazio di transizione tra ordine e disordine, una regione di instabilità limitata, dove le forze sia progressiste che conservatrici combattono per il controllo. Un manager può avere una strategia triennale e il protocollo, i team e i dipartimenti in atto per realizzarla, ma realizzare tale strategia significa affrontare innumerevoli eventi dirompenti; l'ingresso di un nuovo concorrente nel mercato, un cambiamento nel comportamento dei consumatori – persino, forse, il desiderio stesso del manager di ritirarsi in un tranquillo villaggio di campagna. G.C. Beresford, più noto come Herbert George Wells, fu autore di *The Past and Present of the Human Race* nel 1893, una sorta di romanzo distopico e di fantascienza e aprendo le porte a un catastrofismo che riporterebbe il mondo alle sue regole iniziali e di *The Time Machine* (1895) e, soprattutto di *The War of the Worlds* (1896); così citato in E.L. Bernays, *Propaganda. Dalla manipolazione dell'opinione pubblica in democrazia*, Fausto Lupetti, Bologna, 2008 pp. 28-29; tit. or. *Propaganda*, Horace Liveright Publication, New York, 1928.

[6] J. Cooper Ramo, *Seven Sense: Power, Fortune, and Survivor in the Age of Networks*, Little Brown & Co., New York, 2016.

Per Cooper Ramo, il potere è quindi, oggi, concentrato nelle mani di chi controlla i *gate* poiché attraverso questi si esercita il controllo sullo spazio che l'autore chiama *gateland* e, ovviamente, la creazione di un *gate* non sarebbe altro che una fisiologica conseguenza della connessione che capovolge anche i termini di relazione sociale se non politica con una relativizzazione di istituti che sino a ieri sembravano comunque non negoziabili come la cittadinanza[7].

Ma il cyberspazio si caratterizzerà anche per disporre di un livello virtuale di Intelligenza Artificiale che è alla base della gestione delle reti connesse e interdipendenti. Un aspetto che fa sì che Peter Singer, spingendosi oltre e ponendosi a metà strada tra transumanesimo ed etica non lesinava di individuare nei processi futuri legati allo sviluppo delle possibilità AI i veri moltiplicatori di forza per le nuove frontiere sulle quali si muoveranno gli attori internazionali, se ancora tale dimensione, quella internazionale, potrà avere un significato[8].

Se la geopolitica della rete rappresenta, infatti, il livello ulteriore di sfida, di certo esiste oggi, come vedremo, una New-noopolitik che si propone quale visione di conoscenza ancora più avanzata rispetto a ieri[9]. Una conoscenza che si immergerà nel transumano delle procedure e dei sup-

[6] *Gateland*, ivi.

[8] P. Singer, *One World: The Ethics of Globalization*, Yale University Press, New Haven, 2003; trad.it. *One World. L'etica della globalizzazione,* Einaudi, Torino, 2003.

[9] «Noosphere». Termine coniato dal teologo e scienziato francese Pierre Teilhard de Chardin nel 1925 e diffuso in pubblicazioni postume tra gli anni '50 e '60 del Novecento. Teilhard credeva nella necessità di una noosfera espansiva e basata sull'etica. Per Teilhard, nello stesso mondo proposto da Julian Sorell Huxley, la noosfera è una rete di pensiero vivente. P.T. De Chardin, *Le phénomène humain*, Le Seuil, Paris, 1955 pp. 287 e ss.; e *L'avenir de l'homme*, Seuil, Paris, 1959 pp. 175 e ss. Per Arquilla e Ronfeldt la «Noopolitik» è vista come come una geopolitica della rete. Un modello che si estende dal cyberspazio all'infosfera (*infosphere*). Quest'ultima quale coagulo di tutte le reti di comunicazione, database e fonti di informazioni del mondo ricondotte in una vasta, intrecciata ed eterogenea architettura di interscambio digitale. Un modello/rete che riunisce tutte le persone e tutta la conoscenza in un unico luogo, e che nel mondo civile include spesso trasmissioni, stampa e altri media (*mediasphere*); mentre nel mondo militare l'Infosfera può includere sistemi di comando, controllo, comunicazione, intelligence, sorveglianza e ricognizione, i sistemi elettronici dell'ambiente di informazione militare sopra e intorno a un possibile campo di battaglia. Si tratterebbe, insomma, di un processo di riorganizzazione di ogni aspetto informazionale che porterebbe alla cosiddetta noosfera globale (*global noosphere*). Così, in J. Arquilla, D.F. Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy,* Rand & Co. National Defense Research Institute, Santa Monica, 2000 pp. 7-8.

porti che saranno offerti dall'Intelligenza Artificiale. Si tratterà di avere a che fare con un ecosistema nuovo e dove qualunque operazione, militare, di terrorismo, o di bio-attacco, potrà essere condotta da remoto. E, proprio in questa prospettiva, il transumanesimo trova il suo spazio non rappresentando altro che il superamento dell'uomo con la possibilità di trascendere i limiti della condizione umana affidandone il destino a un'Intelligenza Artificiale.

Si tratterebbe, in sostanza, di un potenziamento tecnico delle capacità mediante la tecnologia, rivolto a ridurre il campo emozionale aumentando le capacità di risposta. Ma se così fosse, e probabilmente così sarà, allora potremmo essere testimoni di un passaggio dalla società tecnicista alla società tecnocratica, quasi formalizzando una nuova interpretazione esistenziale dettata da sostituti dell'umanità. Günther Anders, nel suo *Die Antiquiertheit des Menschen: Über die Seele im Zeitalter der Zzweiten Industriellen Refevolution*, (*L'uomo è antiquato*)[10], o Martin Heidegger nella sua *Die Technik und die Kehre*[11], (*La questione della tecnica*), o ancora, Ernst Jünger in *Der Waldgang* con il suo paradosso della società tecnicista, avevano già considerano l'uomo quale vittima del suo stesso sapere, superato nella sua condizione da ciò l'uomo stesso crea. Anzi, tra queste, quella di Jünger si dimostra come una percezione molto chiara presentandosi con una visione proto-transumana, che lo renderà famoso per la sua disarmante evidenza dettata dal ritenere, nel suo *Trattato del ribelle* che

> Der Mensch befindet sich in einer großen Maschine, die zu seiner Vernichtung ersonnen ist.

Ovvero,

> Laddove la macchina fa la sua apparizione, la lotta dell'uomo contro di essa appare senza speranza;

o più semplicemente

> L'uomo è in una grande macchina progettata per la sua distruzione[12].

---

[10] G. Anders (al secolo Günther Stern), *Die Antiquiertheit des Menschen: Über die Seele im Zeitalter der Zzweiten Industriellen Revolution,* C.H. Beck, München, 1956. Trad.it. *L'uomo è antiquato,* Il Saggiatore, Milano, 1963.

[11] M. Heidegger**,** *Die Technik und die Kehre*, Klett-Cotta. Stuttgart, 1962; trad. it. *La questione della tecnica.* In *Saggi e discorsi*, Mursia, Milano, 1976.

[12] E. Jünger, *Der Waldgang*, Klostermann. Frankfurt am Mein, 1951.

Se l'idea è che la sfida nelle sue diverse declinazioni di egemonia tecnologica alla stregua di una qualsiasi corsa a una *supremacy* possa essere intesa come una *discovery* progressiva di forza e potenza, rimarrà sempre una costante il fatto che la tecnologia supererà le barriere mobili dell'umanamente possibile, sino a manifestare la sua stessa potenza, abbattendo ogni giorno di più quella distanza critica tra l'infinitamente grande e l'intimamente piccolo.

Lo stesso Henry Kissinger, insieme a Eric Schmidt e Daniel Huttenlocher non ha perso occasione in un recente saggio di spostare l'attenzione sul ruolo che in futuro avrà l'IA nel definire non solo le relazioni umane nei diversi settori dell'esistenza, ma nel sostenere anche se non suggerire scelte politiche a riguardo. Per gli autori de *The Age of AI: and Our Human Future*, l'Intelligenza Artificiale ha imparato a vincere a scacchi facendo mosse che i grandi maestri umani non avevano mai concepito, così come anche nel campo biomedico, una IA ha scoperto nuovi farmaci e nuove cure analizzando processi molecolari non compresi dai ricercatori, e anche nel campo militare jet pilotati/guidati da IA raggiungono capacità di combattimento superiori a quelle dei piloti meglio addestrati. Tutto questo, dimostra come l'Intelligenza Artificiale diventerà un fattore di cambiamento determinante per gli assetti sociali, economici e, ovviamente, politici[13].

In questa prospettiva di sovrapposizione, allora, tra confini fisici sempre più ridotti e dematerializzazione delle certezze del singolo come delle modalità di governance, l'idea è che l'universo cyber nelle sue prossime declinazioni dovute all'implementazione della e con l'Intelligenza Artificiale e tecnologie quantistiche sarà il nuovo terreno di confronto tra la capacità dell'umana coscienza di definirne i limiti e il rischio di un prevalere di una coscienza algoritmica propria dell'Intelligenza Artificiale. E, questo, in quella corsa esponenziale verso una sempre più profilata raccolta dati che aumenterà la capacità di apprendimento degli hardware e delle intelligenze artificiali che regolano già oggi i primi, e ancor di più le seconde, molti processi decisionali nei media selezionando per l'uomo quali eventi sono notiziabili e quali no.

Insomma, l'idea è che proprio nell'Intelligenza Artificiale, nell'apprendimento automatico, nelle analisi robotiche e nell'uso dei big data che si

[13] H.A. Kissinger, E. Schmidt, D. Huttenlocher, *L'era dell'Intelligenza Artificiale. Il futuro dell'identità umana*, Mondadori, Milano 2023. Tit or. *The Age of AI and Our Human Future*, Little Brown & Co, Boston, 2022.

devono cercare quegli ingredienti attraverso i quali verranno prodotti sistemi o affinati processi e armi con vari gradi di autonomia: dalla possibilità di lavorare sotto la supervisione umana al pensare per se stessi e al raggiungere obiettivi predefiniti. D'altra parte, affidarsi a un sistema IA dovrebbe rispondere a migliorare i tempi decisionali poiché il sistema dotato di una propria elaborazione dovrebbe permettere un processo decisionale rapido, una elevata eterogeneità e/o miglior gestione del volume di dati, evitare comunicazioni intermittenti, tener conto dell'elevata complessità dell'azione coordinata e del pericolo sotteso alla condotta della stessa missione e, se fosse, della elevata persistenza e resistenza dell'avversario[14].

Tuttavia, è anche vero che credere che l'Intelligenza Artificiale possa risolvere ogni problema strategico in futuro può essere una bella e ottimistica speranza. Ma si dovrebbe tener conto, però, che ogni sistema autonomo cercherà di giungere alla massima possibilità esprimibile di apprendimento della macchina, alla massima capacità di elaborazione di informazioni per rispondere, superando le possibilità umane, alle diverse minacce multidimensionali: dalla competizione e gestione dei mercati e delle economie delle singole nazioni, ai processi politici di governo sino ad attacchi informatici a guida IA.

Il rischio, come ricorda ormai una pubblicistica precauzionale, è che in un futuro sempre più metaumano, subordinato all'impero della logica algoritmica, si rischia di vedere sfuggire dal controllo umano decisioni prese e rese efficaci, quindi applicabili, in un altrove intelligente di cui la parte cyber ne è solo l'esatto veicolo di estrinsecazione sul campo e valutazione sulle qualità della cosiddetta Intelligenza Artificiale Generativa.

Per Cooper Ramo, il connubio uomo-macchina - sia esso strettamente orientato a gestire e orientare informazioni in campo digitale quanto la interdipendenza con nuove formule di IA - determinerebbe non solo una minor propensione delle leadership a mettersi in gioco individualmente, quanto richiederebbe una miglior qualità del cittadino. Quest'ultimo, unico e definitivo attore per poter far fronte a una deriva tecnologica usando quel senso di umanità che non risiede solo nella dittatura delle competenze, ma che di certo non può essere rinvenuto in coscienze algoritmiche per quanto evolute queste potranno essere[15].

[14] Defense Science Board, *Autonomy,* Report DoD, «Office of Security Review», giugno 2016 pp. 1-98.
[15] *Citizens!* In, J. Cooper Ramo, *Seven Sense: Power, Fortune, and Survivor in the Age of Networks*, ...cit. pp. 276-308

Non vi sono dubbi che le nuove tecnologie e la stessa Intelligenza Artificiale troveranno spazio anche nei processi educativi con lo scopo di migliorare la capacità di apprendimento, semplificandone i processi ma, si spera, non discriminando le fonti e le interpretazioni contestualizzate alle età, alle esperienze e alle tradizioni culturali. Se così non fosse, si comprende quanto il rischio di veder disattese le conquiste più importanti nell'ambito delle garanzie dei diritti fondamentali degli individui, come delle comunità, rischierebbe di fare del mondo un luogo di omologazione progressiva. Un abbattimento delle differenze che non risponderebbe a una migliore crescita, ma a un appiattimento verso forme di dominio che si affermerebbero nella standardizzazione dei comportamenti, ovviamente rendendo l'idea stessa di libertà piegabile e misurabile nella misura in cui si sarebbe liberi solo e soltanto se si risponde a quell'etica dominante cui l'Intelligenza Artificiale si ispirerebbe.

Bisogno fondamentale alla stessa stregua dell'alimentazione e della casa, l'educazione contribuisce alla stabilità sociale, incoraggia la crescita economica a lungo termine e aiuta ognuno a migliorare le proprie condizioni di vita. Ancora impermeabile alle nuove tecnologie sin dall'inizio del 2010, l'educazione è ormai sotto i riflettori dell'high tech e i fornitori si affollano di fronte alle possibilità quasi illimitate che l'Intelligenza Artificiale può offrire loro. Imparare meglio è forse meno traumatico di quanto potrebbe sembrare[16].

Così come, ad esempio, si può immaginare l'uso dell'IA nel decidere e misurare il rendimento del lavoratore, o anche solo decidere come e in che modo valutare la necessità del lavoratore assunto in base alle valutazioni affidate a un algoritmo gestendo lavori soprattutto temporanei e rientranti nella cosiddetta *gig economy*. Ovvero, rientranti in un modello economico prestazionale fondato sul cosiddetto «lavoro a chiamata», quindi occasionale e temporaneo, e non sulle prestazioni lavorative stabili e continuative, caratterizzate, ovviamente, da maggiori garanzie contrattuali e competenze definite. La ricerca e la gestione di tali assunzioni viene già oggi affidata a sistemi IA i quali sono ritenuti più efficaci e efficienti, e meno influenzabili, del personale umano e, in questa prospettiva di *algorithmic management*, si inserisce la necessità di valutare volta per volta le necessità e di offrire servizi secondo modalità standard[17]. In fondo, la stessa realtà economica

[16] R. Genet, *Edtech: les nouvelles technologies au service de l'éducation*. In «Mayonéz» n.7, avril 2002 p.10

[17] Cfr. S. O'Connor, *When your boss is an algorithm*. In «Financial Times», September 8, 2016.

che deriva da una piattaforma di rete è quella di andare ben oltre i vantaggi delle economie di scala per le quali, al di là del miglior prezzo di un bene o servizio vantaggioso per il fruitore/consumatore si aggiunge la qualità/efficienza di quanto prodotto.

Eppure, sull'interazione tra poteri e reti Niall Ferguson in *La piazza e la torre. Le reti, le gerarchie e la lotta per il potere. Una storia globale,* dimostra come nell'arco abbastanza ampio la storia dell'umanità sia in fondo la storia di modelli di vita e di governance, politica ed economica, e di modelli culturali influenzati dalla costruzione di reti, dai mutamenti gerarchici nell'ordine internazionale per gli Stati, economico per gli attori finanziari e sociale per gli individui. Reti, dove la tecnologia ha assunto il ruolo di guida nel capovolgere modelli o nell'offrire alternative anche percettive sino a giungere alla rivoluzione digitale che ha aperto nuove frontiere sociali, creando quel nuovo cittadino digitalmente transumante definito «netizen» la cui illusione è quella di considerare democratico il modello relazionale offerto dal web[18].

Ferguson sottolinea quanto il fermarsi a considerare acriticamente positivo il modello gerarchico offerto dalle piattaforme di rete apre le porte a ogni eccesso e pericolo, dalla violenza terroristica alla manipolazione delle coscienze per cui solo l'ordine gerarchico, alla fine determinerebbe le migliori condizioni per garantire un equilibro geopolitico dal momento che «la lezione della storia è che affidarsi alle reti per governare il mondo è una ricetta perfetta per l'anarchia». Un avvertimento che potrebbe lasciare sorpresi coloro che credono in un approccio più realisticamente cooperativo se non ingenuamente non competitivo. Ray Dalio, nella parte finale del suo *I Principi per affrontare il nuovo ordine mondiale*. *Dal trionfo alla caduta delle nazioni* offre alcune indicazioni per affrontare le sfide del futuro prossimo cercando di descrivere ciò che andrebbe inteso come futuro e, in particolare, il rapporto del futuro con l'esistenza umana. Ovvero, quel legame tra la conoscenza dell'esperienza e ciò che sarà dopo il presente vissuto come un futuro che sposta la sua linea volta per volta.

Il sapere come i cambiamenti avvenuti in ogni epoca e determinati dalle diverse rivoluzioni non solo politiche o religiose o culturali ma anche, se

[18] Il termine «netizen» è ben espresso in N. Ferguson, *The False Prophecy of Hyperconnection: How to Survive the Networked Age*. In «Foreign Affairs», vol. 96, n. 5-2017, pp. 68-79. Vedasi anche, *La piazza e la torre. Le reti, le gerarchie e la lotta per il potere. Una storia globale.* Mondadori, Milano, 2018; tit. or. *The Square and the Tower. Networks, Hierarchies and the Struggle for Global Power*, Penguin, London, 2018.

non, soprattutto economiche e tecnologiche non lasciano dubbi sul fatto che quanto avvenuto possa ripetersi con modalità nuove ma attraverso processi simili e, quindi, già vissuti. Per Dalio,

> Per affrontare il futuro bisogna 1) riconoscere e adattarsi agli eventi, anche se non li si può prevedere; 2) collocare le probabilità degli eventi futuri; 3) saperne abbastanza sulle probabilità future per riuscire a tutelarsi da eventi inaspettati, anche se non si riesca a farlo perfettamente[19].

Alla fine è altrettanto vero che esiste un problema di incongruità tra le norme di uso delle piattaforme di rete per l'utente e per la community e le norme tradizionali ponendo seri problemi sul rispetto non solo di norme e prassi deontologiche, ma degli stessi diritti del singolo laddove i privilegi di partecipazione sono dettati dal gestore della piattaforma stessa. In questo senso e non solo, l'Unione europea deve evitare di trovarsi dipendente da piattaforme di rete collocate in altri luoghi che hanno precise se non condizionanti caratteristiche geopolitiche che possano limitare la libertà di azione dell'UE, la sua competitività o comprimere i diritti dei propri cittadini. Il vero problema è che l'UE non ha a oggi proprie piattaforme di rete globali come invece accade negli Stati Uniti piuttosto che in Cina o anche in Russia. In fondo, gli Stati e le leadership saranno costretti a dover agire in aree di possibile convergenza caratterizzate dall'intersezione tra molti nuovi mondi in cui gestiranno realtà fisiche e virtuali e realizzando shift geopolitici da una prospettiva globale a un'altra in ragione degli interessi delle potenze tecnologiche che si affermeranno.

Infatti, al di là delle possibilità che si giunga in tempi rapidi a una definizione di un EU-*Quantum Chips Act,* cui si affiderebbe lo scopo di tutelare gli interessi europei sul fronte della sovranità tecnologica è evidente la consapevolezza dell'Unione europea di cercare di affrancarsi man mano dalla dipendenza da risorse e componentistica altrui; cioè, da Paesi extra-UE fornitori di materie prime e semiconduttori necessari per la transizione digitale. Questo significa definire come poter creare un apparato industriale europeo capace di poter fornire tecnologie quantistiche. Una scelta obbligata, che sottende che una sfida geopolitica determinante per il futuro della sovranità tecnologica continentale risiederà nella capacità di riu-

[19] R. Dalio, *I Principi per affrontare il nuovo ordine mondiale. Dal trionfo alla caduta delle nazioni,* Hoepli, Milano, 2022 p. 451 e ss., tit. or. *Principles for Dealing with the Changing World Order: Why Nations Succeed and Fail*, Avid Reader Press / Simon & Schuster, New York, 2021.

scire per l'UE a fare la differenza tra le ambizioni egemoniche in campo digitale e dell'IA di Stati Uniti e Cina, se non delle Global Company che agiscono con capacità e capitali superiori al Pil di molti Stati evitando, in questo modo, il declassamento economico dell'intera Unione.

Kissinger, Schmidt e Huttenlocher in *L'era dell'Intelligenza Artificiale. Il futuro dell'identità umana*, avvertono di come

> L'Europa si trova di fronte alla necessità di scegliere se agire da alleata dell'una o dell'altra parte in ogni principale sfera tecnologica - dirigendone l'evoluzione attraverso una relazione speciale - oppure come ago della bilancia.

La *policy* europea, allora, non potrà che essere diretta a trovare un compromesso sostenibile, sul piano giuridico dei trattati quanto dei principi a essi sottesi, sullo sviluppo economico e il sostegno alle società europee che si occupano di IA perché,

> L'Intelligenza Artificiale trascende già la percezione umana, in un certo senso attraverso la composizione cronologica o il viaggio nel tempo: alimentata da algoritmi e potenza computazionale, analizza e impara attraverso processi per completare i quali la mente umana avrebbe bisogno di decenni se non di secoli[20].

Se è così, l'uso della Intelligenza Artificiale permetterà anche di poter raggiungere risultati a un livello di complessità e di soluzione nei diversi settori dell'esperienza dell'esistenza umana, ma dovrà anche dotarsi di una etica condivisa dell'Intelligenza Artificiale, nella progettazione e nell'uso. Ciò vuol dire che l'era che si approssima è ormai definibile come post-digitale per un verso e neo-neo-digitale se si considera il digitale non più un elemento distintivo ma la condizione sine qua non per raccogliere ulteriori sfide che si trasferiranno nella competizione in materia di IA.

Concludendo, plasmare il futuro con comuni principi e norme circa l'uso di sistemi IA diventerà una condizione quasi esistenziale, considerato che affidarsi all'Intelligenza Artificiale senza tener conto degli effetti e senza un'etica potrebbe trascinare l'umanità intera verso un orizzonte degli eventi devastante in termini di sopravvivenza. Il risultato è che ogni sforzo normativo dovrebbe andare nella direzione di porre limiti e autorizzazioni all'uso di sistemi IA tenuto conto che, al di là dei dati forniti con algoritmi tradizionali o nella versione quantistica, quindi demoltiplicati

[20] H.A. Kissinger, E. Schmidt, D. Huttenlocher, *L'era dell'Intelligenza Artificiale. Il futuro dell'identità umana*, ...cit. p.184 e ss.

nelle capacità di elaborazione delle informazioni, ogni informazione - per quanto dettagliatamente fornita per raggiungere un determinato risultato - può, una IA, di fronte a istruzioni non date per situazioni non definite, processarle o agire cercando proprie nuove regolarità sfuggendo, in questo modo, al controllo umano con tutte le immaginabili ...e non immaginabili conseguenze.

Una condizione per la quale sembrerà che il vero pericolo del nuovo tempo sia la possibilità che si possa penetrare l'intimo umano per connetterlo a nuovi mondi paralleli rendendolo, così, parte di una serie interminabile di infiniti a termine.

Aczel Amir D., *Entanglement: The Greatest Mystery in Physics,* Basic Books, New York, 2002; trad. it. *Entanglement. Il più grande mistero della fisica*, Raffaelo Cortina, Milano, 2004.

Anders G. (al secolo Günther Stern), *Die Antiquiertheit des Menschen: Über die Seele im Zeitalter der Zzweiten Industriellen Revolution,* C.H. Beck, München, 1956; trad. it. *L'uomo è antiquato*, Il Saggiatore, Milano, 1963.

Arquilla J., Ronfeldt D.F. *Cyberwar is Coming!* Rand & Co. National Defense Research Institute, Santa Monica, 1993.

Arquilla J., Ronfeldt D.F., *The Emergence of Noopolitik: Toward and American Information Strategy*, Rand & Co., National Defense Research Institute, Santa Monica, 1999.

Arquilla J., Ronfeldt D., *Networks and Netwar. The Future of Terror, Crime, and Militancy*, Rand & Co., National Defense Research Institute, Santa Monica, 2001.

Augier M., Teece D.J. (eds), *Palgrave Encyclopedia of Strategic Management*, Palgrave-MacMillan, London, 2018.

Baiardi F., *Il "persistent engagement" nella cyberdifesa Usa: punti di forza, debolezze e sovranità digitale.* In «Agenda Digitale», 28 luglio 2022. In https://www.agendadigitale.eu/sicurezza/il-persistent-engagement-nella-cyberdifesa-usa-punti-di-forza-debolezze-e-sovranita-digitale/.

Bateman J., *US-China Technological "Decoupling". A Strategy and Policy Framework*, Carnegie Endowment for International Peace, April 25, 2023.

Baudrillard J., *La scomparsa della realtà*, Fausto Lupetti, Bologna, 2009.

Bauman Z., *Modernità liquida*, Laterza, Bari-Roma, 2011; tit. or. *Liquid Modernity*, Polity Press, Cambridge, 2000.

Beck U., *Risk Society: Towards a New Modernity*, Sage Publications, New York, 1992.

Belo D., Carment D., *Grey-Zone Conflict: Implications for Conflict Management*. www.cgai.ca. CGAI, February 24, 2021.

Beresford G.C. (H.G. Wells), *A Tale of the Twentieth Century*. In « The Science School Journal», May 1887.

Beresford G.C. (H.G. Wells), *The Time Machine*. In «The National Observer», 17 March - 23 June, 1894.

Beresford G.C. (H.G. Wells), *The War of the Worlds*, William Heinemann, London, 1898.

Bernays E.L., *Propaganda,* Horace Liveright Publication, New York, 1928; trad. it. *Propaganda. Dalla manipolazione dell'opinione pubblica in democrazia,* Fausto Lupetti, Bologna, 2008.

Bethke B., *Cyberpunk*. In «Amazing Science Fiction Stories», vol. 57, n.4, November 1983.

Borghard E.D, Lonergan S.W., *The logic of coercion in cyberspace*. In «Security Studies», 26 (3), 2017.

Both, M., Partsch K.J. (eds.), *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, Leida, 1982.

Bourdieu P., *Capitale simbolico e classi sociali*, «Polis», n. 3/2012.

Breznit D., *Innovation in Reals Places. Strategies for Prosperity in an Unforgiving World*, Oxford University Press, New York, 2021.

Buchanan B., *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, Oxford University Press, New York, 2016.

Carment D., Belo D., *Gray-zone Conflict Management: Theory, Evidence, and Challenges*. In «European, Middle Easter & African Affairs», Summer 2020 n. 2; anche in: www.airuniversity.af.edu. Air Force University.

Chan E., *Escalating Clarity without Fighting: Countering Gray Zone Warfare against Taiwan*. In «The Global Taiwan Institute», June 21, 2021.

Cornish P. (ed), *The Oxford Handbook of Cyber Security Get access Arrow*, Oxford University Press, Oxford, 2021.

Chien-Pang L., Kui-Hsiang W., Lim, E., *Taiwan coast guard ships add new livery to distinguish them from China's*. In «Focus Taiwan»; www.focustaiwan.tw, February 17, 2021.

Clarke R.A., Knake R. K., *Cyber War. The Next Threat to National Security and What to do About It*, HapperCollins Publishers, New York, 2010.

Coderre T.P., *Battling Today's Most Advanced Cyber Threats*. In *Strengthening Peace and Security,* Nato Summit 2016, Warsaw, Atlantic Treaty Association, Global Media Partners, 2016.

Command Vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 2018.

Command Vision for US Cyber Command, *Cyberspace Operations, Joint Chief of Staff,* Joint Publication, June 3-12, 2018.

Condon R., *Manchurian Candidate*, MacGraw-Hill Book Company Inc, New York, 1959.

Cooper Ramo J., *Seven Sense: Power, Fortune, and Survivor in the Age of Networks*, Little Brown & Co., New York, 2016.

Cooper Ramo J., *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*, Little Brown & Co., New York, 2009; trad. it., *Il secolo imprevedibile. Perché il nuovo disordine mondiale richiede una rivoluzione del pensiero*, Elliot, Roma, 2009.

Cornish P. (ed.*), The Oxford Handbook of Cyber Security Get access Arrow*, Oxford University Press, New York, 2021.

Dalio R.*, I principi per affrontare il nuovo ordine mondiale. Dal trionfo alla caduta delle nazioni,* Hoepli, Milano, 2022, tit. or. *Principles for Dealing with the Changing World Order: Why Nations Succeed and Fail*, Avid Reader Press/Simon & Schuster, New York, 2021.

De Chardin P.T., *Le phénomène humain*, Le Seuil, Paris, 1955.

De Chardin P.T., *L'avenir de l'homme*, Le Seuil, Paris, 1959.

Di Nolfo E., *Dagli imperi militari agli imperi tecnologici. La politica internazionale dal XX secolo a oggi*, Laterza, Bari-Roma, 2013.

Denig E., Van Der Meiden A., *Relations A Geography of Public Trends*, Springer, Berlin, 1985.

Denmark A.M., Mulvenon J. (ed.), *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security, January 2010, Washington DC.

Dobbs T., Fallon G., Fouhy S., *Gray Zone. The Forge (Report),* Australian Defence College, September 9, 2020.

Ebner N.*, Cyber Space, Cyber Attack and Cyber Weapons. A Contribution to the Terminology*. IFSH - Institute for Peace Research and Security Policy at the University of Hamburgf, October 2015.

Efrony Y. S., *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice.* In «The American Journal of International Law», vol. 112, n. 4, 2018.

Einstein A., Podolsky B., Rosen N., *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*. In «Phisycal Review», v.47, May 15, 1935.

Farruggia F. (a cura di), *Dai droni alle armi autonome. Lasciare l'Apocalisse alle macchine?* Franco Angeli, Milano, 2023.

Ferguson N., *The Square and the Tower.Networks, Hierarchies and the Struggle for Global Power*, Penguin, London, 2018; trad. it. *La piazza e la torre. Le reti, le gerarchie e la lotta per il potere. Una storia globale*. Mondadori, Milano, 2018.

Freier N., *The Darker Shade of Gray: A New War Unlike Any Other*, Center for Strategic & International Studies, July 27, 2018.

Garfinkel B., Dafoe A., *How does the offense-defense balance scale?* In «Journal of Strategic Studies», 42 (6) 2019.

Gartzke E., *The myth of cyberwar: bringing war in cyberspace back down to earth*. In «International Security», 38 (2), 2013.

Gazula M.B., *Cyber Warfare Conflict Analysis and Case Studies*, Working Paper, Massachusetts Institute of Technology May 10, 2017.

Gelernter D., *Mirror Worlds. Or the Day Software Puts the Universe in a Shoebox.. .How It Will Happen and What It Will Mean*, Oxford University Press, Oxford, 1993.

Gibson W.F., *Neuromancer,* Ace, New York, 1984; trad. it. *Neuromante,* Editrice Nord, Milano, 1986.

Gibson W.F., *Count Zero*, Victor Gollancz Ltd., London, 1986; trad. it. *Giù nel cyberspazio*, Mondadori, Milano, 1990.

Graham D., *Cyber Threats and the Law of War'*. In «Journal of National Security Law & Policy» n. 87- 2010.

Healy J., *The implications of persistent (and permanent) engagement in cyberspace*. In «Journal of Cybersecurity», 5 (1), 2019.

Heidegger M.W.**,** *Die Technik und die Kehre*, Klett-Cotta. Stuttgart, 1962; trad. it. *La questione della tecnica.* In *Saggi e discorsi*, Mursia, Milano, 1976.

Hoffman F., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington 2007.

Hoffman F., Mattis J.M., *Future Wars: The Rise of Hybrid Wars,* 132. In «Proceedings Magazine», November 2005 Vol. 132/11/1.

Hoffman W., *Is Cyber Strategy Possible?* In «The Washington quarterly», 42 (1), 2014.

International Institute of Strategic Studies, *Global Trends. Paradox of Progress*, London, 2017.

International Institute of Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment*, London, 2019.

Jacobsen J.T., *Cyber offense in NATO: challenges and opportunities*. In «International Affairs», 97 (3) 2021.

Jacobsen J.T., Klimburg A., *Mixed signals: a flawed approach to cyber deterrence*. In «Survival», 62 (1) 2020.

Jünger E., *Der Waldgang*, Klostermann, Frankfurt am Mein, 1951.

Kai-Fu L., *Al Superpowers: China, Silicon Valley, and the New World Order*, Mariner Books, Boston, 2021.

Kapusta P., *The Gray Zone* (pdf), in: www.soc.mil. United States Special Operations Command, e *Challenging the Gray Zone*, in: www.law.upenn.edu. University of Pennsylvania Law School, February 18, 2021.

Kello L., *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*. «Quarterly Journal: International Security», 38 (2) 2013.

Kelsey J., *Hacking into International Humanitarian Law: the Principles of Distinction and Neutrality in the Age of Cyber Warfare*. In «Michigan Law Review» 1427, 2008.

Kessler O., Werner W., *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*. In «Leiden Journal of International Law», vol. 26, no. 4, 2013.

Khanna P., *Connectography. Mapping the Future of Global Civilization*, Random House, New York, 2016; trad. it. *Connectograpy, Le mappe del futuro ordine mondiale*, Fazi, Roma, 2016.

Kissinger H.A., Schmidt E., Huttenlocher D., *The Age of AI and Our Human Future*, Little Brown & Co, Boston, 2022; trad. it. *L'era dell'Intelligenza Artificiale. Il futuro dell'identità umana,* Mondadori, Milano, 2023.

Klimburg A., *Mixed signals: a flawed approach to cyber deterrence*. In «Survival», 62 (1), 2020.

Korolev A., *Political and Economic Security in Eurasia: English School Perspective*. In Sahakyan M. (ed), *China and Eurasian Powers in a Multipolar World Order 2.0, Security, Diplomacy, Economy and Cyberspace*, Routledge, London, 2023.

Kramer F.D., Starr S., Wentz L.K., *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*. In *Cyberpower and National Security,* National Defense University Press, Washington (D.C.) 2009.

Kuehl D.T., *From Cyberspace to Cyber-power: Defining the Problem*. In *Cyberpower and National Security,* National Defense University Press, Washington, D.C. 2009.

Layton P., *Algorithmic Warfare Applying Artificial Intelligence to Warfighting*, Canberra, Air Power Development Centre, 2018.

Lee Y., Lague D., Blanchard B., *China launches "gray-zone" warfare to subdue Taiwan*. www.reuters.com. «Reuters». February 18, 2021.

Libicki M.C., *Cyberdeterrence and Cyberwarfar*, Rand Corp, Santa Monica, 2009.

Libicki M.C., *Cyberspace in Peace and War*, Naval Institute Press, Annapolis, 2021.

Liebetrau T., *Cyber conflict short of war: an European strategic vacuum*. In «European Security», v.31, 2022.

Lin H., Kerr J., *On Cyber-Enabled Information Warfare and Information Operations*. In P. Cornish (ed.), *The Oxford Handbook of Cyber Security Get access Arrow*, Oxford University Press, Oxford, 2021.

Lindsay J.R., Kello L., *Correspondence: a cyber disagreement*. In «International Security», 39 (2) 2014.

Mackinder H., *The Geographical Pivot of History*, Royal Geographical Society, London, 1904.

Mahan A.T., *The Interest of American in Sea Power, Present and Future*. Boston, 1898.

Matisek J. H., *Shades of Gray Deterrence: Issues of Fighting in the Gray Zone*. In «Journal of Strategic Security», vol. 10, n. 3, 2017.

Mell P., Grance T., *The NIST Definition of Cloud Computing,* NIST, Special Publication, September 2011.

Morgan S., *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. In «Special Report»: *Cyberwarfare In The C-Suite*. Consultabile in: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.

Morris L.J., Mazarr M.J., Hornung J.W., Pezard S., Binnendijk A., Kepe M., *Gaining Competitive Advantage in the Gray Zone* (pdf) in: www.rand.org. RAND, February 18, 2021.

National Institute of Standards and Technology, *Managing Information Security Risk Organization, Mission, and Information System View. Information Security*, US-Department of Commerce, 2011.

Nora S., Minc A., *L'information de la société. Rapport à M. le Président de la Republique*, La Documentation française, Paris, 1978.

O'Neil C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin, New York, 2017.

Nye J. Jr., *Deterrence and dissuasion in cyberspace*. In «International Security», 41 (3), 2016/17.

Ramírez J.M., García Segura L.A. (eds), *Cyberspace: Risks and Benefits for Society, Security and Development,* Springer, New York - London, 2017.

Rattray G.J., *Strategic Warfare in Cyberspace*, MIT Press, Cambridge, 2001.

Rid T., *Cyber War Will Not Take Place*, C. Hurst & Co. Publishers Ltd, London, 2013.

Romeo G., Giordano F.M., *Cybersecurity. Aspetti di sistema e traiettorie in movimento*. In Giordano F.M., Caraffini P. (a cura di), *L'Unione europea nel XXI secolo. Profili e prospettive dell'integrazione europea*. In «De Europe», Special Issue, 2023-2024.

Russel S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson Education Limited, London, 2021.

Sahakyan M. (ed), *China and Eurasian Powers in a Multipolar World Order 2.0, Security, Diplomacy, Economy and Cyberspace*, Routledge, London, 2023.

Schmitt M.N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013.

Schmitt C., *Der nomos der erde im Völkerrecht des Jus Publicum Europaeum,* Dunker & Humblot, Berlin, 1988; trad. it. *Il nomos della terra nel diritto internazionale dello «jus publicum europaeum»*, Adelphi, Milano, 1991.

Schmitt M.N., *Cyber Operations and the Jus in Bello: Key Issues*. In «International Law Studies» v.87, 2011.

Schmitt M.N., *Essays on Law and War at the Fault Lines*, Asser Press, The Hague, 2012.

Schmitt M.N., *Classification of Cyber Conflict*. In «Journal or Conflict & Security Law» 17(2), 2012.

Schmitt M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017.

Shackelford S., *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. In «Berkeley Journal of International Law» v. 192, 2012.

Singer P., *One World: The Ethics of Globalization*, Yale University Press, New Haven, 2003; trad. it. *One World. L'etica della globalizzazione,* Einaudi, Torino, 2003.

Slayton R., *What is the cyber offense-defense balance? Conceptions, causes and assessment*. In «International Security», 41 (3), 2017.

Sproull L., Kiesler S., *Connections: New Ways of Working in the Networked Organization,* MIT Press, Cambridge, 1991.

Spykman N.J., *The Geography of the Peace*, New York, Harcourt, Brace and Company, 1944.

Steele R.D, *On Intelligence: Spies and Secrecy in an Open World*, AFCEA International Press, Fairfax, 2000.

Stephenson N., *Snow Crash,* Bantam Spectra, New York, 1992.

Stoker D., Whiteside C., *Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking*. In «Naval War College Review». 73 (1), Winter 2020.

Su-Wei W., Chin J., *Embrace innovation, admiral says*. In «Taipei Times» (www.taipeitimes.com), June 17, 2023.

Talbot J., *The Tallinn Manual 2.0: Highlights and Insights*. In «Georgetown Journal of International Law», vol.48, 2017.

Taleb N.N., *The Black Swan. The Impact of the Highly Improbable*, Penguin, New York, 2008; trad. it., *Il cigno nero. Come l'improbabile governa la nostra vita,* Saggiatore, Milano, 2023.

The White House, *The National Strategy to Secure Cyberspace*, Washington DC, 2003.

US-Cyber Command, *Command Vision for US Cyber Command. Achieve and Maintain Cyberspace Superiority*, 2018. Consultabile in https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

US-Department of Defense, *Cybersecurity. Resource and Reference Guide*, February 28, 2022.

Valeriano B., Jensen B., Maness R., *Cyber Strategy: the Evolving Character of Cyber Power and Coercion,* Oxford University Press, Oxford, 2018.

Viggiano G.(ed.), *Convergence: Artificial Intelligence and Quantum Computing*: *Social, Economic, and Policy Impacts*, John Wiley & Sons Inc, Hoboken, 2022.

Von Heinegg W.H., *Chapter 1: The Tallinn Manual and International Cyber Security Law*, in «Yearbook of International Humanitarian Law», vol. 15, 2012.

Weigley R.F., *War and the Paradox of Technology*. In «International Security», 1989.

Westberg G., *Can Cyber Attacks Prevent Wars?* In Ramírez J.M., García Segura L.A. (eds), *Cyberspace: risks and benefits for society, security and development,* Springer, New York - London, 2017.

Wiseman J., Michell S., *Strengthning Peace and Security Warsaw*, Nato Summit, Varsavia, 2016.

World Economic Forum, *Global Cybersecurity Outlook 2022*, Insight Report, January 2022.

Ringraziamenti

Alla fine di questo percorso ringrazio coloro che ne hanno sostenuto lo sforzo e stimolato la realizzazione di questa sintesi a metà strada tra una guida sul futuribile e uno sguardo ancorato al presente. Ringrazio, quindi, Paolo Caraffini e Filippo Maria Giordano per avermi assegnato tale tema inserendomi nel progetto «ai4ei». Ringrazio Elisabetta Tarasco per la pazienza nella verifica dell'editing, Silvio Ortolani per l'impaginazione e la veste grafica, Francesco Cuzzi Brancacci per le osservazioni tecniche che mi hanno orientato in un universo digitale sempre più affollato da soluzioni che influenzeranno il nostro quotidiano nei prossimi anni. Ringrazio Roberto Gay che da molto tempo segue con sincera amicizia quanto scrivo. Tuttavia, ciò che in questi anni ha contraddistinto il mio percorso accademico è dovuto alla fiducia di Umberto Morelli cui questo lavoro è dedicato in apertura al suo ricordo, a chiusura di un'attività da Lui voluta e portata avanti oltre la sofferenza, come «Artificial Intelligence for European Integration» - ai4ei - Jean Monnet Centre of Excellence e «NoFear4 Europe Chair» (NoFEUr) dell'Università di Torino.

L'autore

Giuseppe Romeo

Analista politico, giornalista pubblicista e accademico. Calabrese, ha frequentato l'Accademia Militare di Modena e la Scuola Ufficiali Carabinieri. Laureato in Giurisprudenza, Scienze Politiche e Scienze Strategiche ha tenuto, a vario titolo, lezioni e seminari in diverse università italiane in *Diritto dell'Unione europea*, *Storia dei trattati e politica internazionale*, *Sociologia delle relazioni internazionali*, *Analisi della politica estera*, *Storia delle relazioni internazionali*, *Relazioni internazionali*, *Studi strategici*. E' docente a contratto di *Relazioni internazionali* presso il Dipartimento di Giurisprudenza e Scienze politiche, Economiche e Sociali dell'Università del Piemonte Orientale, sede di Alessandria; di *Storia delle relazioni internazionali* (con approfondimento sulla *Politica estera della Russia e degli Stati Uniti*) e di *Storia politica dell'integrazione europea* (cui è affidato un percorso di approfondimento sulla *Difesa Europea*) presso la Scuola Universitaria Interdipartimentale di Scienze Strategiche, Università di Torino/Comando per la Formazione e Scuola di Applicazione dell'Esercito. Alle precedenti collaborazioni universitarie, si aggiungono quelle in *Storia contemporanea* e in *Contemporary History and Media History* presso la Link University di Roma. È autore di circa 150 contributi pubblicati a vario titolo su Riviste scientifiche e divulgative su argomenti di politica della difesa e di relazioni internazionali. Tra le ultime monografie pubblicate in qualità di autore e altri contributi su curatele, si segnalano, in particolare: *Da Vienna a Parigi. Gli ultimi giri di valzer. La Grande Guerra, la Conferenza di pace e l'ordine mondiale. Storia di un'Europa sconfitta* (2021); *Una Nazione incompiuta. L'Italia: dal sistema dei partiti alla crisi della democrazia* (2022). *Guerre Ibride. I volti nuovi del conflitto* (2022); *La Nato dopo la Nato. Perché l'Alleanza rischierà di implodere* (2023).

Il sostegno della Commissione europea alla produzione di questa pubblicazione non costituisce un'approvazione del contenuto, che riflette esclusivamente il punto di vista degli autori, e la Commissione non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni ivi contenute.

Stampato nel mese di aprile 2024 da BDPrint - The Factory (Roma)

Jean Monnet Centre of Excellence
Artificial Intelligence for European Integration

https://www.jmcoe.unito.it
https://www.observatory.unito.it

Dalla dimensione cyber alle “nuove” intelligenze
Rischi e sfide per l’Europa

Giuseppe Romeo

L’ormai quasi totale dipendenza da sistemi tecnologici digitali, la velocità e il livello di sostituibilità che proprio tali possibilità/opportunità hanno assunto rispetto alle capacità dell’uomo si risolvono nella continua evoluzione delle conquiste nella dimensione Cyber e nel campo della AI. Per questo, la corsa a superare in qualità il modo con cui le informazioni verranno processate riposiziona i termini di potenza ancorandoli alla conquista della superiorità tecnologica nelle diverse declinazioni possibili: Cyber, AI e Quantum Computing. Ciò attribuisce un significato decisivo al paradigma della “sovranità tecnologica”, unica garanzia di indipendenza se non di sopravvivenza politica ed economica di un attore-Stato. L’Unione europea, di fronte alle “nuove Intelligenze”, ha cercato nel vertice di Londra del novembre 2023, AI-Safety Summit, di provare a superare ogni definizione mettendo sul tavolo delle discussioni un altro problema: l’impatto e il ruolo che l’Intelligenza Artificiale, nelle sue diverse e complesse manifestazioni, assumerà nei prossimi anni. Una preoccupazione non di poco conto condivisa dai 28 paesi firmatari più l’Unione europea e contenuta nella «Dichiarazione di Bletchley Park». L’ordine geopolitico e geoeconomico, ancora una volta definito da nuove instabilità per differenza di potenza e capacità, troverà nel controllo della produzione e dell’accesso a tecnologie sempre di più extra-dimensionali, la ragione quanto la soluzione dei conflitti e delle crisi future in un modello relazionale decisamente tecnopolare. Un modello, quest’ultimo, nel quale l’Europa del domani dovrà decidere con quali politiche e con quali strumenti, giuridici, economici e tecnologici, vorrà giocare il proprio destino.

€ 39,00

9 791256 001378