Rischio Cyber tra incertezza e tecnologia

Author : Andrea Boggio

Date : 6 Febbraio 2019

Introduzione

Il presente articolo sintetizza il *Global Risks Report 2019* del *World Economic Forum (WEF).* La rappresentazione dei rischi globali è, per propria natura, organica e olistica al tempo stesso: le minacce, le probabilità di accadimento e gli impatti degli eventi rischiosi sono parte di un unico ed esteso dominio di analisi. D'altro canto, quando entrano in gioco fattori di rischio tecnologici in generale e *cyber* in particolare, la natura simultaneamente globale e locale degli stessi li rende automaticamente elementi degni della massima attenzione in ogni parte del mondo. Alcuni concetti generali relativi alla **gestione del rischio**, ai più comuni **bias cognitivi** e alla centralità del **fattore umano** sono stati già affrontati nel mio intervento del 2018 "*Cyberspazio: minacce e fattore umano*[1]", cui rimando per eventuali approfondimenti.

Panorama dei Rischi Globali

Come ogni anno il WEF, istituzione internazionale focalizzata sulla collaborazione tra mondo pubblico e privato, ha pubblicato a gennaio il proprio *Global Risks Report*[2]. Nel corso del 2018, anno analizzato all'interno del report, i **rischi macroeconomici** sono saliti alla ribalta: la volatilità dei mercati finanziari è infatti aumentata e il tasso di crescita globale sembra aver raggiunto il proprio picco, con conseguente inizio di dinamiche di discesa previste dal Fondo Monetario Internazionale[3]. Le tensioni geo-politiche e geo-economiche tra le maggiori potenze mondiali rappresentano un punto di attenzione, così come le evidenti frizioni tra la globalizzazione dell'economia mondiale e la crescita di nazionalismi e localismi. I **rischi ambientali** sono percepiti come i maggiori e la **tecnologia** gioca un ruolo sempre più determinante: è diffuso il timore di **frodi sui dati**, di **attacchi cyber** e di un elevato numero di **vulnerabilità tecnologiche** (preoccupano i rischi associati alle *fake news*[4] e al furto di identità digitale[5] così come quelli collegati alla perdita di privacy per aziende e governi). Nel 2018 si sono verificate enormi **violazioni di dati personali (*data* *breach*[6])**, sono state scoperte **gravi vulnerabilità hardware** e la ricerca si è focalizzata sui potenziali **utilizzi dell'Intelligenza Artificiale per ingegnerizzare attacchi cyber** sempre più efficaci; già nel report del 2018 il WEF aveva sottolineato i rischi che gli **attacchi cyber** comportano per le **infrastrutture**

critiche.

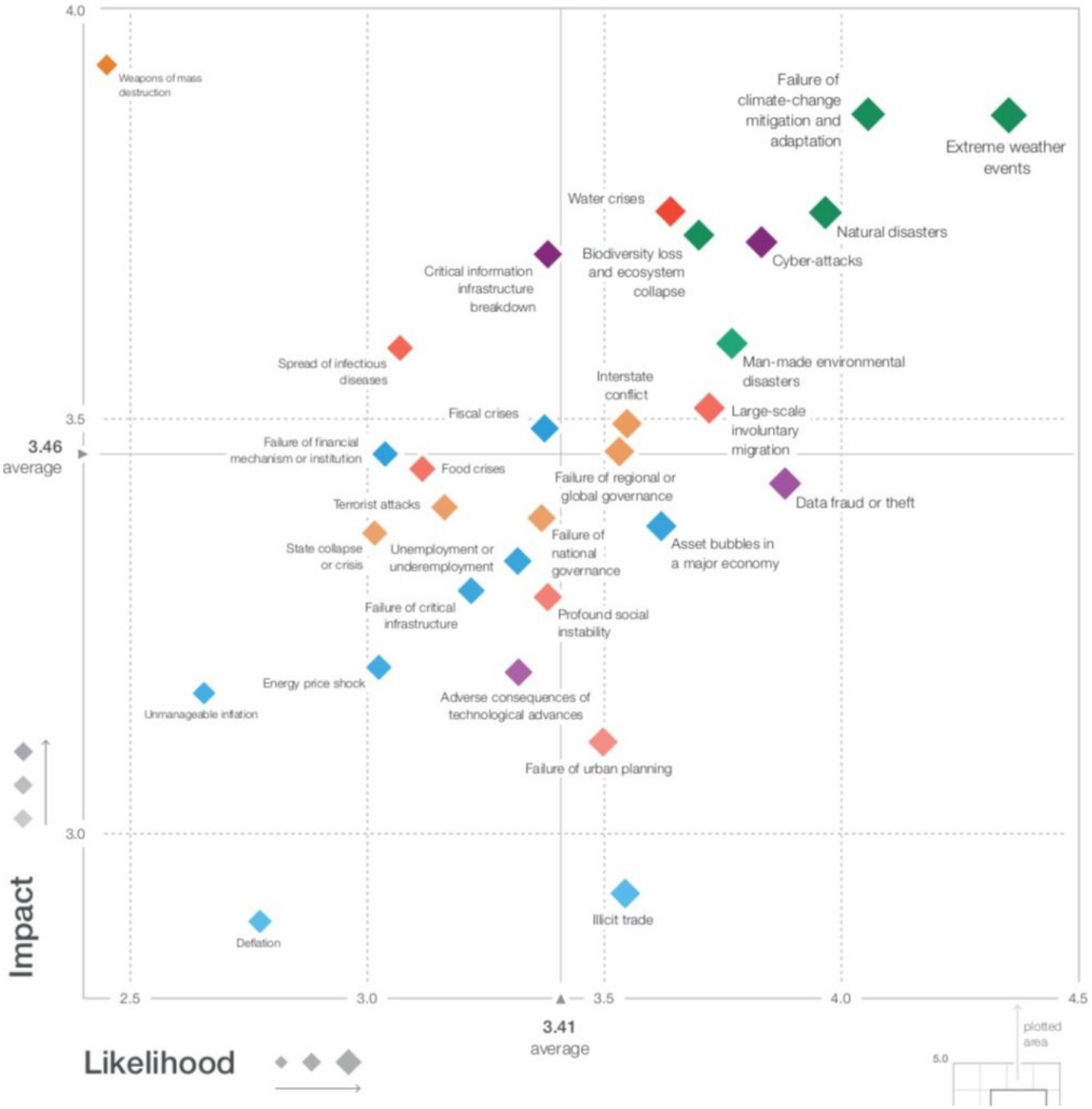

Figura 1 - Global Risks Landscape 2019

Il **lato umano** dei rischi globali è rappresentato dalla proliferazione diffusa di sentimenti di ansia, infelicità e solitudine (si stima che al mondo ci siano almeno 700 milioni di persone affette da problemi di salute mentale). In particolare, le **complesse trasformazioni** – siano esse di natura sociale, tecnologica o collegate al lavoro – determinano un profondo impatto sulle esperienze di vita delle persone: un tema comune è quello relativo allo stress psicologico

collegato al sentimento di mancanza di controllo di fronte all'incertezza.

Altri rischi rilevanti riguardano le **minacce biologiche** e l'**innalzamento del livello dei mari**.

In generale, il report esplora la percezione dei rischi globali nelle loro dimensioni di *vulnerabilità economiche, tensioni geopolitiche, sociali* e *politiche, fragilità ambientali* e *instabilità tecnologiche*.

Rischio tecnologico

La **tecnologia** continua a giocare un ruolo chiave nel dare forma al panorama dei rischi globali ed è una tendenza che ricalca lo schema registrato anche nel 2018, con i **rischi cyber** che di fatto **consolidano la propria posizione predominante (accanto ai rischi ambientali) in termini di impatto e probabilità nel quadrante del panorama dei rischi globali**. Le instabilità tecnologiche sono causate dall'inesorabile e progressiva integrazione delle tecnologie digitali all'interno di ogni aspetto della vita quotidiana, con potenziali effetti dirompenti sulla psicologia e sulle vite delle persone.

Attacchi cyber e protocolli di *cybersecurity* inefficienti hanno portato a violazioni massive di dati personali nel 2018. Il più grande *data breach* si è verificato in India, dove il database governativo delle Identità Digitali, Aadhaar[7], ha subito numerosi attacchi e violazioni con la potenziale compromissione di 1.1 miliardi di cittadini registrati. Durante il mese di Gennaio è stato riferito che i *cyber criminali* stavano vendendo l'accesso temporaneo al database (10 minuti al prezzo di 500 rupie). In altri casi eclatanti, violazioni di dati personali hanno riguardato 150 milioni di utenti dell'app *MyFitnessPal*[8] e oltre 50 milioni di utenti Facebook[9].

Il 2018 ha registrato anche impatti negativi dovuti ai **disservizi cloud**: condizioni ambientali particolarmente avverse hanno determinato, per esempio, periodi prolungati caratterizzati da alte temperature (Microsoft)[10], venti e pioggia dei *Noreaster*[11] di Marzo (AWS, Equinix)[12]e fulmini (Microsoft). Questi eventi sottolineano il collegamento tra le catastrofi naturali e il rischio cyber all'interno dei Data Center.

La minaccia rappresentata dagli attacchi cyber alle **infrastrutture critiche** implica impatti economici assoluti. Un esempio della magnitudine dei disservizi tali attacchi possono provocare è la campagna *ransomware*[13] condotta a Marzo contro la città di Atlanta: l'erogazione dei principali servizi ai cittadini si è interrotta dopo che i computer municipali sono stati compromessi*[14]*.

Le vulnerabilità cyber possono arrivare da direzioni inattese, come risulta evidente dalle minacce di *Meltdown*[15] e *Spectre*[16], che coinvolgono **debolezze hardware** e non software. Potenzialmente, si tratta di minacce che riguardano ogni processore Intel prodotto negli ultimi 10 anni. Il 2018 ha ulteriormente evidenziato che gli attacchi cyber sono un rischio per le infrastrutture critiche: nel mese di Luglio il governo degli Stati Uniti ha dichiarato che gli hacker avevano ottenuto accesso alle *control room*[17] di alcune aziende nazionali fornitrici di servizi di pubblica utilità. La potenziale vulnerabilità dell'infrastruttura tecnologica critica è diventata sempre più un problema di sicurezza nazionale.

L’**Intelligenza Artificiale (IA)** sta diventando sofisticata e capace di amplificare i rischi esistenti: in particolare, l’*Internet of Things* (IoT) connette miliardi di dispositivi. IBM ha segnalato un malware basato su Intelligenza Artificiale capace di nascondere una minaccia ben nota – *WannaCry*[18] – all’interno di un’applicazione di videoconferenza, attivandola solo in caso di riconoscimento del volto degli obiettivi dell’attacco[19]. Innovazioni simili si stanno verificando anche in altri campi (è possibile per un agente di minaccia usare l’IA nella biologia sintetica per creare nuovi micro-organismi patogeni). L’IA può anche riconoscere, rispondere e manipolare le emozioni umane e giocare un ruolo fondamentale nelle camere dell’eco[20] dei *social media* e delle *fake news* (una ricerca ha dimostrato che su 126.000 *tweet* analizzati la maggior parte di essi conteneva fake news e informazioni non vere[21]).

Altro rischio tecnologico è rappresentato, paradossalmente, dall’avanzamento del *quantum computing*[22], le cui capacità di calcolo *monstre* rendono obsolete le basi dell’attuale crittografia digitale, in particolare degli algoritmi a chiave pubblica. Un’eventuale *debacle* della crittografia a chiave pubblica trascinerebbe nel baratro le fondamenta stesse della *vita digitale* insieme ai propri elementi costitutivi quali autenticazione, riservatezza, integrità, fiducia e identità.

Il lato umano

Il report del WEF dedica una sezione al **lato umano dei rischi globali** partendo da alcuni dati estremamente interessanti: per molte persone questo è un mondo sempre più ansioso, infelice e solitario. Il sentimento di rabbia cresce e l'empatia sembra essere in declino in ogni area analizzata (sociale, tecnologica e lavorativa). Lo stress psicologico è legato a una sensazione di **mancanza di controllo** di fronte all'**incertezza**: i dati dell'Organizzazione Mondiale della Sanità (OMS) suggeriscono che la depressione e i disturbi d'ansia sono aumentati rispettivamente del 54% e del 42% tra il 1990 e il 2013[23]. In uno studio recente[24], la **tecnologia** è stata citata come **una delle principali cause di solitudine e isolamento sociale** dal 58% degli intervistati negli Stati Uniti e dal 50% nel Regno Unito. Il cambiamento tecnologico è sempre una fonte di stress, ma l'attuale ondata di trasformazione, cui spesso viene dato il nome di **Quarta Rivoluzione** Industriale[25], tende a sfumare ulteriormente la linea di demarcazione tra “umano” e “tecnologico”.

L'**automazione** ha permesso a un enorme numero di lavoratori di risalire la catena del valore e sfuggire a compiti monotoni e pericolosi, ma già nel 1959 l’OMS aveva notato segnali di effetti psicologici allarmanti unitamente alle possibili minacce insite nelle dinamiche stesse dell'automazione[26]. La tecnologia rende più facile per i datori di lavoro l’esercizio di forme di controllo e monitoraggio dei lavoratori: l’aumento notevole delle *capability di sorveglianza* contribuisce a creare diffidenza e condizioni difficili per lo sviluppo del *trust*[27] tra *Labour* e *Capital*. I cambiamenti più ampi nella **struttura del lavoro** sono un'ulteriore fonte di potenziale stress: la sicurezza e la stabilità del lavoro sono in declino in molte economie avanzate, con una crescita degli utili lenta o stagnante e un'espansione meno prevedibile della *gig economy*[28].

Panopticon digitale[29]

La biometria*[30]* sta facendo progressi esponenziali: le tecnologie che ieri erano fantascienza plasmano oggi la realtà di miliardi di persone. Riconoscimenti facciali[31], analisi della deambulazione[32], assistenti digitali, *affective computing***[33]**, microchip, lettura labiale digitale, sensori di impronte digitali: mentre queste e altre tecnologie proliferano, ci spostiamo in un mondo in cui tutto di noi viene catturato, immagazzinato e sottoposto ad analisi operate da algoritmi di Intelligenza Artificiale. Ciò rende possibili servizi pubblici e privati sempre più individualizzati, ma anche nuove forme di persuasione mirata. Se gli esseri umani sono sempre più sostituiti da macchine in processi decisionali cruciali, il risultato può portare non solo a una maggiore efficienza, ma anche a una maggiore rigidità sociale. La politica globale si espone a rischi di derive autoritarie, facilitate in un mondo caratterizzato da **visibilità** e **tracciabilità** totali. Molte società stanno già lottando per bilanciare le minacce alla privacy, alla fiducia e all'autonomia contro le promesse di maggiore sicurezza, efficienza e novità.

Mentre l'intreccio della tecnologia con la vita umana si rafforza, è probabile che l'***affective computing*** - l'uso di algoritmi in grado di leggere le emozioni umane predicendo le nostre risposte emotive - diventi sempre più **prevalente**. Col tempo, l'avvento di *woebot*[34] e strumenti simili basati sull'IA potrebbe modificare radicalmente le modalità di erogazione delle terapie psicologiche, in modo similare a quanto sta avvenendo nel mondo dei dispositivi indossabili[35] (monitor cardiaci, contapassi, etc). Eventuali conseguenze negative prodotte da algoritmi emotivamente intelligenti, causate sia accidentalmente sia intenzionalmente, potrebbero essere profonde.

Conclusioni

In generale, il sociologo Charles Perrow[36] ha identificato due aspetti dei sistemi che li rendono vulnerabili ai fallimenti imprevisti: **complessità** e **accoppiamento forte**. Un sistema complesso è simile a una rete elaborata con molte parti intimamente connesse a gran parte di ciò che accade, mentre un sistema strettamente accoppiato presenta poco spazio e scarso margine di errore. Quando qualcosa va storto in un sistema complesso, i problemi iniziano a spuntare ovunque ed è difficile capire cosa sta succedendo. Un accoppiamento forte significa che i problemi emergenti si trasformano rapidamente in situazioni fuori controllo e anche piccoli errori possono precipitare in crolli e fallimenti epocali.

Il modello sviluppato da Perrow all'epoca (primi anni 80) era riferito ai pochi sistemi complessi e fortemente accoppiati di quei tempi: centrali nucleari, sistemi di allarme missilistico e missioni di esplorazione spaziale. Da allora, tuttavia, un'enorme quantità di complessità è stata aggiunta al nostro mondo – sempre più dipendente da tecnologie digitali, a volte intrinsecamente fragili, per il proprio funzionamento e per la propria prosperità - e la possibilità che piccoli problemi possano innescare catene di eventi che portano a enormi fallimenti è assolutamente concreta.

La rappresentazione dei rischi globali del WEF non deve essere interpretata come descrizione apocalittica di eventi escatologici che conducono inevitabilmente a scenari di distruzione di massa (anche se, obiettivamente, la definizione di *rischio globale* del WEF va in questa direzione: "*evento o condizione incerta che, nel caso in cui effettivamente si verificasse, potrebbe causare un significativo impatto negativo per diversi paesi o industrie nei 10 anni successivi*"). D'altronde, non è possibile gestire il rischio e proteggere un *asset* (sia esso

materiale o immateriale) senza valutare la probabilità e l'impatto delle minacce che lo mettono a repentaglio, esplorando ogni esito in tutte le sue conseguenze, anche le più estreme.

Dal punto di vista della comunità cyber è fondamentale concentrare gli sforzi e le capacità sulla dimensione tecnologica dei rischi globali, in particolare sulla loro caratterizzazione cyber, ma è imprescindibile inquadrarli all'interno di una visione analitica organica e multidimensionale.

- [1] https://www.ictsecuritymagazine.com/articoli/cyberspazio-minacce-e-fattore-umano/
- [2] https://www.weforum.org/reports/the-global-risks-report-2019
- [3] https://it.wikipedia.org/wiki/Fondo_Monetario_Internazionale
- [4] https://it.wikipedia.org/wiki/Fake_news
- [5] https://it.wikipedia.org/wiki/Furto_d%27identità
- [6] https://en.wikipedia.org/wiki/Data_breach
- [7] https://www.bbc.com/news/world-asia-india-42575443
- [8] https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/
- [9] https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/
- [10] https://rcpmag.com/articles/2018/09/04/microsoft-cloud-outage-datacenter.aspx
- [11] https://it.wikipedia.org/wiki/Noreaster
- [12] https://www.crn.com/slide-shows/security/300107391/the-10-biggest-cloud-outages-of-2018-so-far.htm
- [13] https://it.wikipedia.org/wiki/Ransomware
- [14] https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html
- [15] https://it.wikipedia.org/wiki/Meltdown_(vulnerabilità_di_sicurezza)
- [16] https://it.wikipedia.org/wiki/Spectre_(vulnerabilità_di_sicurezza)
- [17] https://en.wikipedia.org/wiki/Control_room
- [18] https://it.wikipedia.org/wiki/WannaCry
- [19] https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/
- [20] https://it.wikipedia.org/wiki/Camera_dell%27eco
- [21] https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/
- [22] https://it.wikipedia.org/wiki/Computer_quantistico
- [23] https://www.who.int/mental_health/policy/services/essentialpackage1v7/en/
- [24] http://files.kff.org/attachment/Report-Loneliness-and-Social-Isolation-in-the-United-States-the-United-Kingdom-and-Japan-An-International-Survey
- [25] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution
- [26] https://apps.who.int/iris/handle/10665/40448
- [27] https://it.wikipedia.org/wiki/Trust
- [28] https://it.wikipedia.org/wiki/Precariato#Gig_economy
- [29] https://it.wikipedia.org/wiki/Panopticon

- [30] https://it.wikipedia.org/wiki/Biometria
- [31] https://en.wikipedia.org/wiki/Facial_recognition_system
- [32] https://en.wikipedia.org/wiki/Gait_analysis
- [33] https://it.wikipedia.org/wiki/Affective_computing
- [34] https://woebot.io
- [35] https://en.wikipedia.org/wiki/Wearable_technology
- [36] https://it.wikipedia.org/wiki/Charles_Perrow

Articolo a cura di **Andrea Boggio**