Cyberspazio: minacce e fattore umano

Date : 15 marzo 2018

Panorama dei rischi e delle minacce cyber

Nell'annuale **Global Risks Report**[1], il World Economic Forum (WEF) ha rappresentato per il 2018 una realtà carica di spunti interessanti. In particolare, salta agli occhi la rilevanza degli attacchi cyber (**Cyberattacks**), ormai stabilmente presenti nella *top ten* dei rischi globali: si tratta del **terzo rischio** in termini di **probabilità** e il **sesto** in termini di **impatto**, oltre a essere il **primo rischio tecnologico in assoluto**. Per dare un'idea della concorrenza, l'analisi del WEF antepone ai rischi di attacchi cyber solamente quelli relativi a eventi climatici estremi e disastri naturali (in termini di probabilità) e quelli relativi ad armi di distruzione di massa, eventi climatici estremi, disastri naturali, fallimenti dovuti all'adattamento ai cambiamenti climatici e crisi legate alla disponibilità dell'acqua in termini di impatto.

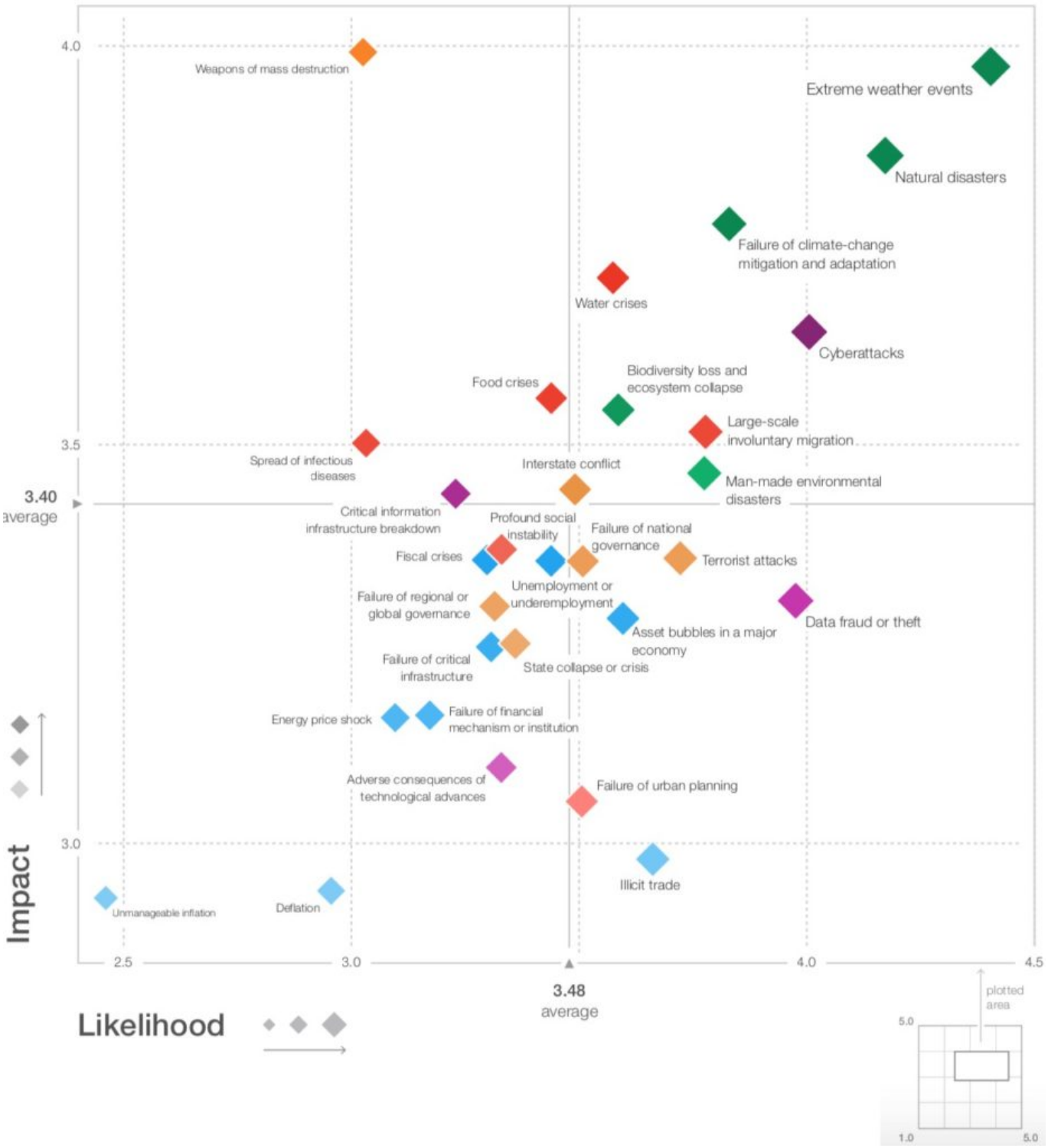

Figura 1 – Global Risks Landscape 2018

Il **rischio globale** è definito nel Report come un “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”.

Restringendo l'analisi al dominio tecnologico, le categorie di rischio più rilevanti sono:

- **conseguenze avverse dell'avanzamento tecnologico**: alcune tecnologie in rapida ascesa quali l'Intelligenza Artificiale, la biologia sintetica e la geo-ingegneria possono causare, in modo intenzionale o meno, danni all'umanità, all'ambiente e all'economia;
- **interruzione delle infrastrutture critiche di comunicazione**: la crescente **cyber dipendenza** (*cyber dependancy*) aumenta la vulnerabilità intrinseca ai disservizi delle infrastrutture critiche di comunicazione (ad esempio reti satellitari e internet) con relativi effetti di discontinuità;
- **attacchi cyber su larga scala**: attacchi e *malware* diffusi su larga scala causano enormi danni economici, tensioni geopolitiche e aumento della sfiducia nell'utilizzo di internet;
- **incidenti massivi relativi a furto e/o frodi sui dati**: l'appropriazione indebita di dati pubblici e privati avviene ormai a una scala e a un livello di magnitudine totalmente nuove.

Un **trend** è definito come uno schema di lungo periodo attualmente in fase evolutiva ma che potrebbe contribuire ad amplificare i rischi globali e/o ad alterare le relazioni tra essi: tra i trend di tipo tecnologico il più significativo è l'aumento della **cyber dipendenza** determinata dall'interconnessione digitale – in costante crescita - tra persone, cose e organizzazioni.

La rilevanza assegnata dal Report ai rischi cyber è un segno dei tempi e della progressiva dipendenza dell'umanità dalla tecnologia, in particolare dalle *Information & Communications Technology***[2]** (ICT).

A sostegno delle proprie conclusioni, il WEF rappresenta come scenari paradigmatici i casi dei *ransomware* **WannaCry**[3] e **NotPetya**[4] unitamente al trend crescente degli attacchi cyber contro le infrastrutture critiche e i settori industriali strategici. La maggior parte degli attacchi ai sistemi critici e strategici non ha avuto esito positivo, ma la combinazione di isolati attacchi andati a buon fine con una lista crescente di tentativi simili suggerisce che il rischio sia in aumento. Il mondo sempre più interconnesso aumenta la nostra vulnerabilità ad attacchi che non causano semplicemente disservizi isolati e temporanei, ma **shock sistemici radicali e irreversibili**.

La visione d'insieme dei rischi globali è interessante anche alla luce delle analisi locali: nello specifico, all'interno dell'annuale "*Relazione sulla politica dell'informazione per la sicurezza*" presentata dal Presidente del Consiglio dei Ministri e dal Direttore generale del Dipartimento Informazioni per la Sicurezza (DIS)[5], è possibile trovare spunti e analogie con il Report del WEF. I due principali filoni di minaccia individuati all'interno della relazione sono rappresentati dai *ransomware* (ancora una volta è citato l'esempio di WannaCry) e dalle campagne di influenza mirate a condizionare l'orientamento e il **sentiment** delle opinioni pubbliche, tipicamente previa diffusione online di informazioni trafugate a mezzo di attacchi cyber. Più in generale, "la continua evoluzione del dominio cibernetico (…) nell'ampliare la superficie di attacco, ha parallelamente comportato una pronunciata diversificazione ed un affinamento dei vettori della minaccia. Tattiche, tecniche e procedure si sono caratterizzate, infatti, per diversi livelli di capacita? offensiva: dalla negazione di servizio alla violazione di sistemi ICT, attraverso

operazioni, spesso silenti, finalizzate a compromettere risorse di cui assumere il controllo, cosi? da acquisire i dati in esse contenute".

Il punto di vista della nostra Intelligence diventa molto interessante quando si afferma che nessuno "dubita che molti e significativi saranno gli effetti, **anche sul piano della sicurezza**, degli ulteriori sviluppi che stanno facendo ingresso nella quotidianità di individui, imprese e Stati: dopo *cloud* e *big data* – con il loro corollario di potenzialità e rischi – saranno *l'intelligenza artificiale*, la *robotica* e il cd. *internet delle cose* (IoT) a rivoluzionare i modelli di produzione e le stesse relazioni tra singoli e tra Paesi". Quali sono le categorie delle minacce cyber cui si fa costante riferimento in questi e in altri Report simili? Ne identifichiamo quattro, universalmente riconosciute:

- Il **Cybercrime** si riferisce al generico insieme di attività malevole mosse da intento criminale con finalità di lucro: furto d'identità e di dati confidenziali, frodi informatiche, vendita illegale di informazioni e dati;
- L'**Hacktivism** è la categoria di minacce rappresentata dalla conduzione di attacchi ideologicamente orientati;
- Il **Cyber Espionage** è l'acquisizione impropria di materiale confidenziale;
- **L'Information Warfare** è l'insieme di attività e operazioni condotte nel dominio cyber con lo scopo di conseguire un vantaggio operativo di rilievo militare. Nel 2010 il Pentagono ha riconosciuto il **cyberspazio** come nuovo dominio[6], il quinto dopo mare, terra, aria e spazio. Nel 2016 la NATO, durante il Summit di Varsavia[7], è andata nella stessa direzione.

La visione della distribuzione delle minacce e della tipologia di attacchi cyber globali ci arriva dal prezioso Rapporto Clusit 2017[8] (in attesa di quello del 2018, la cui uscita prevista è successiva alla data di stesura del presente articolo):

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	2H 2016	1H 2017	1H 2017 su 2H 2016	Trend 2016
Cybercrime	170	633	609	526	684	751	377	427	13,26%	↑
Hacktivism	114	368	451	236	209	161	78	46	-41,03%	↓
Espionage / Sabotage	23	29	67	69	96	88	30	68	126,67%	↑
Information Warfare	14	43	25	42	23	50	42	30	-28,57%	↘
TOTALE	469	1.183	1.152	873	1.012	1.050	527	571	+8,35%	↗

Figura 2 - Tipologia e distribuzione degli attaccanti

Gestione del rischio

L'idea di rischio e quella complementare di sicurezza hanno finito per dominare l'orizzonte culturale e l'agenda del dibattito pubblico e politico delle società occidentali: gli attributi di invisibilità, immaterialità e imprevedibilità hanno reso evidente l'inadeguatezza della visione convenzionale del rischio come prodotto della probabilità di un evento avverso moltiplicata per il danno conseguente. Nel corso del tempo sono state elaborate numerose teorie all'interno di discipline eterogenee: dall'apocalisse della modernità (Beck) al carattere di riflessività (Giddens), dalla prospettiva della *governamentalità* (Focault) agli aspetti sociali dei processi decisionali e della comunicazione (Luhmann), dagli studi culturali (Douglas) all'approccio psicometrico (Tversky e Kahneman) fino alla amplificazione sociale del rischio[9]. L'approccio ingegneristico al rischio (Knight) lo rappresenta come incertezza calcolabile sulla base del principio del razionalismo economico e della logica formale. Tale approccio si fonda sul paradigma dell'*agente razionale* che, a tutti gli effetti, sembra in crisi profonda: se l'incertezza, l'imprevedibilità e l'imponderabilità definiscono le specificità del rischio, si può assumere che queste vengano ridotte ma mai del tutto eliminate. Normalmente, in effetti, la gestione del rischio inizia proprio così: tramite l'identificazione e la stima della probabilità e dell'impatto di una data minaccia possiamo decidere se un rischio rientra nei nostri limiti di tolleranza e come reagire riducendo la nostra esposizione ad esso. Il **fallimento** durante questo processo è **frequente**: nuove tecnologie e progressi nella scienza dei dati hanno aumentato la capacità di identificare trend, valutare rischi e generare avvertimenti iniziali. In questa dinamica è necessario comprendere al meglio le ragioni per le quali le persone sono più propense a reagire a certi rischi ignorandone altri. **L'elemento comportamentale è cruciale** per gestire in modo efficace i rischi – sia per riconoscerli sia per tradurre tale conoscenza in azioni efficaci.

Semplificando molto, il nostro modo di pensare in quanto esseri umani prevede due sistemi cognitivi (sistema impulsivo e sistema riflessivo), ognuno dotato di caratteristiche peculiari[10]:

Sistema impulsivo	**Sistema riflessivo**
Incontrollato	Controllato
Spontaneo	Meditato
Associativo	Deduttivo
Rapido	Lento
Inconsapevole	Consapevole
Abile	Ligio alle regole

Come esseri umani siamo naturalmente portati a operare continuamente scelte e, allo scopo di facilitarci la vita, mettiamo in campo una serie di regole pratiche molto utili ma che possono condurre a distorsioni sistematiche (**euristiche** e **bias cognitivi**). Tversky e Kahneman hanno sviluppato questo concetto individuando tre euristiche frutto dell'interazione tra sistema impulsivo e sistema riflessivo (*Ancoraggio, Disponibilità* e *Rappresentatività*)[11]; altro "errore" cognitivo tipico è l'*ottimismo irragionevole*, che conduce all'assunzione inutile e pericolosa di rischi. Le persone odiano perdere e i loro sistemi impulsivi in questi casi spesso hanno reazioni emotive forti. L'avversione alle perdite porta alla generazione dell'*inerzia*, rappresentabile come un forte attaccamento verso ciò che già si possiede, portandoci a non fare cambiamenti anche

quando tali cambiamenti sarebbero nel nostro interesse. Un’altra causa di inerzia è la tendenza a privilegiare la situazione nella quale già viviamo (bias dello *status quo*).

Il nostro cervello fa alcuni scherzi che fanno apparire alcuni rischi diversi da quello che sono nella realtà. Essere consapevoli di questi elementi permette a chi deve decidere di modulare le proprie azioni e prevenire crisi o mitigare eventuali danni. In situazioni deliberative i bias di ancoraggio e di conferma possono distorcere le percezioni, portandoci ad assegnare un peso maggiore a informazioni e viste presentate in precedenza. Queste distorsioni possono essere compensate modificando i processi decisionali e accertandosi che ci siano diverse voci intorno al tavolo, incoraggiando il dibattito strutturato e il dissenso costruttivo. In altre parole, il rischio di considerare una gamma di punti di vista che rafforzano le scelte già intraprese è elevato.

Uno degli errori cognitivi più pervasivi è il *bias di disponibilità*, che induce coloro che prendono decisioni ad appoggiarsi su esempi ed evidenze che vengono subito in mente: tale processo conduce l’attenzione delle persone verso eventi emotivamente significativi, lontano da eventi più probabili e ad alto impatto. Quando i membri di un gruppo decisionale sono troppo omogenei possono insorgere ostacoli alla loro capacità di riconoscere e reagire al rischio in modo appropriato. Troppa poca **diversità** può enfatizzare il *bias di conferma* e rendere più difficile per gli individui il semplice fatto di parlare dei rischi per paura di perdere il consenso acquisito. Spesso le organizzazioni agiscono con fermezza per contrastare il rischio solamente quando una violazione significativa, quale una catastrofe, un evento di *hacking* o un *data breach* conclamato le obbliga a farlo.

In parte ciò avviene perché gli umani tendono a ignorare la probabilità che gli scenari peggiori si verifichino realmente, cosa che può renderci cechi dinnanzi a pericoli ovvi.

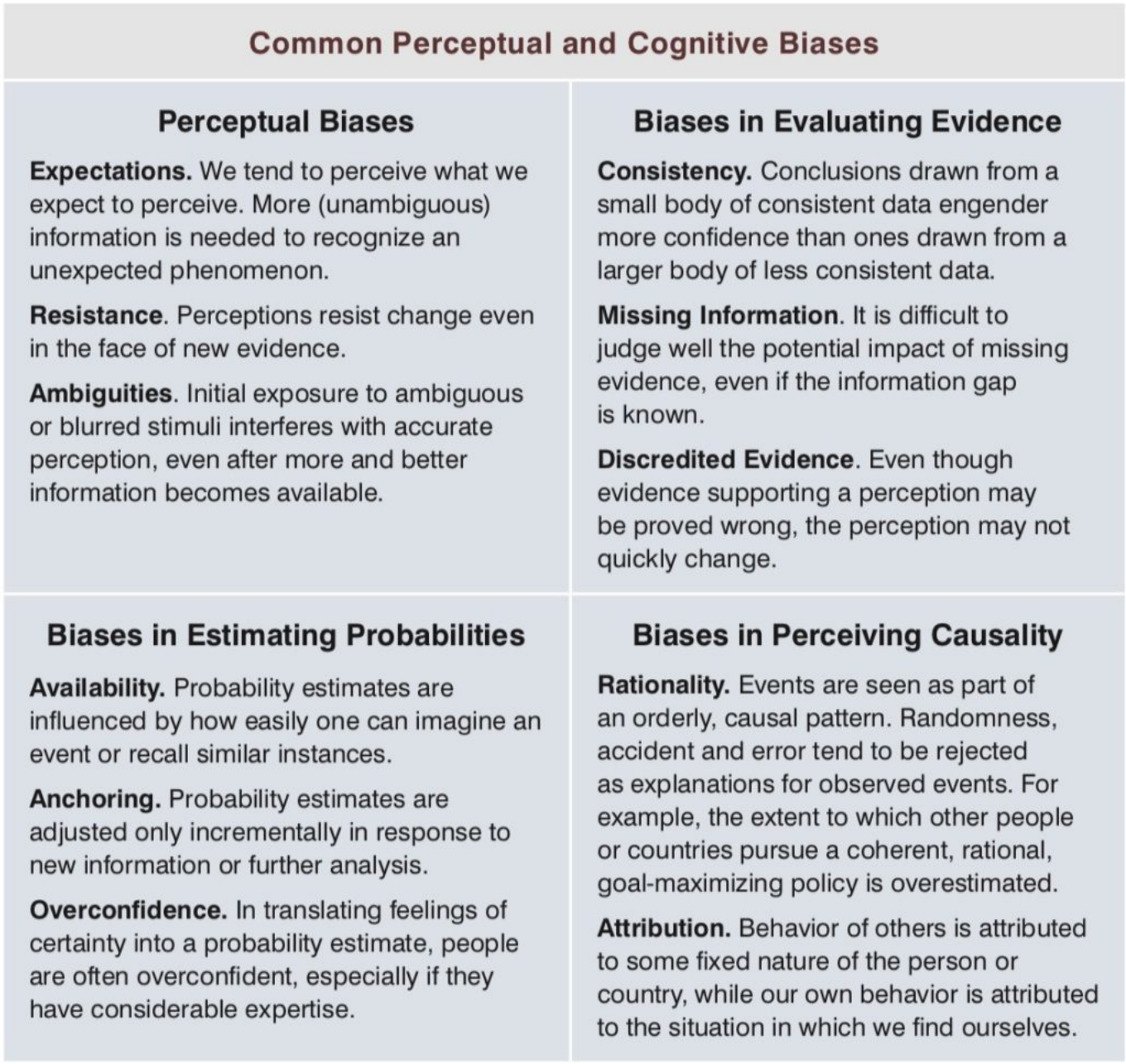

Figura 3 - Comuni bias cognitivi e percettivi[12]

Troppo spesso i vari comitati e consigli di amministrazione approcciano l'analisi del rischio come elemento isolato e come lista da spuntare. Pensiamo a un impiegato che manda all'aria ogni piano di cyber security cliccando inavvertitamente su un messaggio email di *phishing* perché non è stato fatto abbastanza per trasferire dal vertice alla base dell'organizzazione la consapevolezza dei rischi associati a un comportamento del genere. Per prevenire questo tipo di violazione, la gestione del rischio ha bisogno di uscire dal proprio silos e diventare **parte organica** della gestione delle operazioni, del budget e dei progetti. Le organizzazioni devono migliorare nell'educazione dei dipendenti relativamente alla consapevolezza dei rischi, ma devono anche assicurare che le loro culture incoraggino i dipendenti a sentirsi liberi di parlare ed essere presi sul serio.

Visioni possibili…

Il romanzo *Cyberstorm*[13] di Matthew Mather, ambientato principalmente a New York, delinea con precisione uno scenario complesso determinato dall'indisponibilità prolungata nel tempo delle ICT in concomitanza di un evento atmosferico estremo. Senza rovinare l'esperienza della lettura del libro, basti sapere che entrano in gioco le infrastrutture critiche, le *fake news* e la manipolazione dell'informazione, forme di resistenza umana realizzate tramite l'utilizzo creativo della tecnologia (*l'hacking* nel senso più nobile del termine), cyber terroristi, *hacktivist* e tensioni geopolitiche globali. *Cyberstorm* è un esempio perfetto di *ripple effect* o effetto domino: cosa succederebbe se le infrastrutture di comunicazione smettessero di funzionare? cosa significherebbe non disporre improvvisamente di elettricità e acqua corrente? cosa accadrebbe immediatamente dopo negli ospedali? diminuendo la disponibilità di acqua e cibo e con esse i livelli complessivi di igiene, con quale velocità si trasmetterebbero eventuali malattie? e se le condizioni ambientali a contorno fossero particolarmente critiche (grande freddo o grande caldo)? come si comporterebbe l'essere umano privato degli elementi tecnologici che contribuiscono a definirne il livello di civiltà?

La visione di Mather non è né esagerata né apocalittica: tanto più una società si affida alle ICT per la propria prosperità, tanto più tendono a crescere la superficie complessiva di attacco e le vulnerabilità cui la società si espone. La conoscenza delle minacce e la gestione del rischio cyber sono essenziali, alla stregua della consapevolezza dei limiti connaturati all'essere umano: ogni architettura di protezione, declinata nelle proprie componenti tecnico-organizzative e nelle capacità operative, deve necessariamente mettere al centro il **fattore umano**[14].

Note

- [1] https://www.weforum.org/reports/the-global-risks-report-2018
- [2] https://en.wikipedia.org/wiki/Information_and_communications_technology
- [3] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- [4] https://en.wikipedia.org/wiki/Petya_(malware)
- [5] http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf
- [6] https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
- [7] https://www.nato.int/cps/en/natohq/official_texts_133169.htm
- [8] https://clusit.it/rapporto-clusit/
- [9] https://www.letture.org/rischio-e-comunicazione-teorie-modelli-problemi-andrea-cerase/
- [10] https://it.wikipedia.org/wiki/Nudge
- [11] http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf
- [12] http://www.analysis.org/structured-analytic-techniques.pdf
- [13] https://en.wikipedia.org/wiki/Cyberstorm_(novel)
- [14] https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

A cura di: **Andrea Boggio**