Cyberphobia e fattore umano

di Biagino Costanzo
Dirigente d'Azienda
Docente in Scienze criminologiche per la difesa e la sicurezza
Socio AIPSA

Ormai se ne parla così tanto che si rischia di assuefarsi al tema e restar indietro nella prevenzione e protezione da sempre più sofisticati attacchi malevoli tramite il "web", la "rete".
Nei prossimi anni sul nostro pianeta la popolazione virtuale sarà maggiore di quella reale e la rete sarà sempre più un campo di battaglia, il vero campo di battaglia. L'aumento esponenziale delle connessioni imporrà ai poteri pubblici di approntare strumenti, adeguati per coniugare due valori fondativi della convivenza democratica: la libertà e la sicurezza.(Anche la Commissione Europea si è concentrata con HORIZON 2020, il piu grande Programma di Ricerca e Sviluppo che sia mai stato effettuato dall' Unione Europea, per uno stanziamento di circa 80 miliardi di euro per più capitoli tra cui ICT e appunto la Cybersecurity. Il Programma ha previsto l'investimento immediato di 500 Meuro per avviare progetti diretti con la Commissione n.d.a.)

In tale quadro la cyber intelligence è destinata a rappresentare uno strumento fondamentale. Definirla non è semplice, poiché in essa convivono due elementi che operano con logiche differenti ma che sono destinare ad amalgamarsi per poter garantire la sicurezza di una Repubblica di un Paese e dei suoi cittadini.
Partiamo dalla imprescindibile presenta della Humint, ovvero, l'intelligenza umana; stare sul campo, studiare le aree, approfondire, conoscere, comprendere, interagire, vedere, controllare, analizzare, doti prettamente umane appunto, necessarie per assumere decisioni, e poi lo spazio digitale, popolato da tecnologie sempre più pervasive.
L'argomento è dirompente, se pensiamo ai molteplici convegni e seminari dedicati alla materia o che, per esempio, nella Relazione Annuale al Parlamento del Dipartimento delle Informazioni per la Sicurezza della Repubblica, la parola Cyber è citata ben 86 volte.

In questo primo, quasi, ventennio del nuovo secolo, il cosiddetto «web oscuro» è 500 volte più grande dell'internet visibile; oltre il 75% delle chiamate telefoniche mondiali può essere monitorato; attraverso i like su facebook è possibile scoprire orientamenti sessuali, convinzioni religiose, livelli di reddito e propensioni al consumo, quando, dove e per quanto sei in vacanza; con un semplice click si può destabilizzare una multinazionale, interrompere le trasmissioni di un satellite o manipolare i dati di una consultazione elettorale.

Ormai, come tutti sanno, basta penetrare un firewall (dispositivi software od hardware posti a protezione dei punti di interconnessione eventualmente esistenti tra una rete privata

interna- ad es.una Intranet- , ed una rete pubblica esterna -ad. es. Internet, oppure tra due reti differenti, n.d.a), per produrre rischi concreti, solo alcuni esempi:

- alla Rete elettrica nazionale di un Paese con milioni di cittadini al buio, e senza corrente danni economici per tutti i prodotti deteriorabili ed eventuali possibili rivolte nelle città;
- alla mancanza di fornitura e distribuzione idrica, sabotando le dighe, i serbatoi, gli acquedotti o gli impianti delle fognature che contaminerebbero l'acqua potabile di tutto un Paese o di una zona di esso causando avvelenamento e disidratazione;
- sabotare il traffico aereo causando quindi incidenti e collisioni o qualsiasi altra infrastruttura strategica.

In queste condizioni, più aumenta la presenza delle tecnologie più, paradossalmente, c'è bisogno dell'insostituibile fattore umano per dare un'anima alla sovrabbondanza di dati e disvelare le menzogne della società della disinformazione, delle c.d. fake news, in cui la realtà diventa mera opinione.

Ad esempio, tralasciando quelle già note, (dalle scie chimiche, ai chip inseriti nei nostri cervelli a ns insaputa, al finto attentato alle Torri Gemelle, al falso allunaggio) tra le fake intrise di complottismo siamo arrivati a metter in dubbio l'attentato di Manchester di qualche settimana fa o anche la morte per di un bimbo per otite causa cura omeopatica somministrata da un medico (??) e con genitori consenzienti, ma forse per alcuni webbologi, notizia orchestrata dalle lobby degli produttori di antibiotici (sigh..). Qui la realtà supera la più ironica fantasia del personaggio mirabile inventato da Crozza nei suoi spettacoli, "Napalm 51" !
Fa paura che si creda che attraverso la rete si è al centro dell'Universo, aver convinzione di esser tuttologi. Non vi è cognizione che in realtà, si ignori del tutto il mondo reale, perché persi in quella solitudine che pregna la stanza da dove clicchi, è illusorio credere di far parte di grandi comunità, di avere migliaia di "amici" di godere quando si hanno tanti like e andare, letteralmente in depressione, quando si hanno i tanti, desiderati, clik "mi piace". Tutto questo non è reale e tutto questo porta dipendenza.

In merito è davvero molto interessante analizzare l'articolo pubblicato sul Corsera lo scorso 19 giugno dalla filosofa italiana Adriana Cavarero, docente di Filosofia politica all'università di Verona, dal titolo "La post-verità, da Platone fino a Trump..", dove si evince che i governanti diventano popolari sfruttando il pregiudizio e l'ignoranza, ma questo, appunto è da sempre, e la colpa, chiaramente, non è di certo solo dei governanti, ma di chi evita il sacrificio di conoscere, informarsi sul serio, studiare, capire!
Nell'articolo emerge che gli " Oxford Dictionaries hanno eletto «post verità» parola internazionale dell'anno 2016, a seguito del controverso referendum sulla «Brexit» e dell'elezione presidenziale americana ugualmente contestata, che

hanno contribuito a diffondere questo termine tanto nei mass media che nel gergo politico. Il dizionario definisce «post-verità» come «in rapporto o contestuale a circostanze in cui i fatti oggettivi sono meno influenti nel plasmare l'opinione pubblica rispetto alla leva esercitata sulle emozioni e sulle credenze personali». Il prefisso «post», in questo caso, non significa «successivo», ma anzi denota un'atmosfera in cui la verità è irrilevante e prevalgono le credenze radicate nelle emozioni."

Stiamo vivendo insomma un periodo pericolosissimo a livello di tenuta collettiva, è un mutamento epocale e sottovalutare la cosa o pensare che, in fondo, "ne abbiamo già visto di tutti i colori", può risultare, questa volta, devastante.
I social network, da apprezzabile grande intuizione si sono trasformati, per i più, incubatori di stupidita di massa, e non lo diciamo certo in pochi, negli ultimi giorni si è aggiunto addirittura Evan Williams co-fondatore di Twitter che ha affermato come "Internet si sia rotto", che " le persone usano Facebook non solo per offendere ma anche per mostrare suicidi, risse o assassini, in tempo reale. Twitter è un tale alveare di abusi che sembra impossibile smettere e, ancora, che le false notizie, create per ideologia o per profitto, sono sconvolgenti.
Sono quindi divenuti ormai veri e propri strumenti per invadere il web di, tante menzogne che portano a rimettere in discussione, acclarate conquiste scientifiche come i vaccini, oppure dubitare della veridicità di notizie storiche, o alimentare il complottismo tout court su ogni cosa, o immergersi nelle menti di giovanissimi tanto che, notizia di poche settimane fa, sta prendendo piede una cosa aberrante, per dirla con un eufemismo, in rete esiste il gioco della "Blue whale" la Balena blu, dove devi rispettare 50 regole dettate da "un tutor" che on line ti ordina punto per punto cosa fare fino ad arrivare al punto 50, la " vittoriosa meta" ovvero suicidarsi dal palazzo più alto che si possa trovare e, cosa ancora più scioccante farsi filmare mentre lo fai.
Siamo alla follia, alla distrazione totale da parte di società civile, genitori, educatori, qui si passa dalla materia psicologica a cambio epocale degli usi e costumi del genere umano.
Bisogna non solo perseguire chi ha creato questo abominio, chi lo distribuisce in rete e anche chi filma il tutto (complice per istigazione al suicidio) e parliamo di centinaia di ragazzine e ragazzini, non solo in Russia,dove tutto è nato, ma purtroppo, come qualsiasi cosa viene messa in rete, diviene globale, ma fare un ragionamento davvero più profondo sull'abisso al quale l'uomo si è affacciato e, con disarmante superficialità, sta per precipitare definitivamente.

Saper "usare" il web è divenuto ormai la vera priorità. Non esiste più privacy in generale. Basta pensare che ormai basta una piccola webcam cinese da dieci euro o uno smartwactch o un piccolo monitor per svegliare i nostri bambini in culla, oppure la bambola Cayla, che in Germania poteva "spiare" i bambini, guardare, registrare a insaputa dei genitori, sapere. Questa tipologia di bambola è dotata di un microfono bluetooth che si collega agli smartphone intorno ad essa anche a diversi metri di distanza, quindi qualsiasi male intenzionato può ascoltare, ma anche parlare con i bambini.

Ormai è corsa a proteggersi da eventuali “intrusioni” come per esempio i più paranoici mettono il nastro adesivo sulla webcam del proprio laptop, usano lenzuoli scuri per coprire la tastiera quando digitano le password, chiedono a tutti gli ospiti di chiudere gli smartphone nel forno a microonde.
A Washington nel 2015 i genitori, preoccupati del loro bimbo di tre anni che affermava di “sentire voci” nella notte, lo hanno portato dallo psicologo e scoperto che uno dei baby monitor (quelli per controllare i bambini), tra i piu venduti negli States, era hackerabile e delle persone erano entrate realmente nel sistema e parlavano con il bambino.
Ma si può vivere cosi? Semplicemente inquietante.

Intanto continuano gli attacchi di Ddos, tipica aggressione informatica contro l’Internet delle cose, negli USA la Federal Trade Commission, l’agenzia che si occupa dei consumatori, ha accusato il produttore di Smart tv Vizio di registrare gli utenti mentre si sta tranquillamente in salotto. Analoghe accuse erano emerse per prodotti Samsung e Lg. E in Inghilterra, anche a seguito dei reiterati attentati terroristici, la premier Theresa May, durante le sedute di Governo ha bandito gli smartwatch, è sempre piu probabile che potrebbero essere usati dagli hacker come microfoni per ascoltare le conversazioni. Gli IoT, ovvero gli oggetti collegati a Internet, rischiano di essere i televisori-telecamere sempre accesi, giorno e notte senza alcuna possibilità di spegnerle.
Allora, è forse tempo di fermarsi, Istituzioni, Governi, Associazioni, Imprese devono comprendere che è tempo di rimettere nel giusti binari, il progresso e la globalizzazione. Un salto di qualità che deve saper superare la mera convenienza del momento e avere una visione di futuro.

Nell’era delle tecnologie, dunque, c’è sempre maggiore bisogno dell’intelligenza umana, poiché gli algoritmi non sempre hanno ragione e anzi a volte possono risultare fuorvianti.
Si tratta di stimolare una nuova consapevolezza e alimentare una nuova davvero non più rimandabile “cultura della sicurezza”, anche sacrificando un po’ della nostra privacy (d'altronde fanno sorridere coloro che si appellano alla propria privacy e poi postano sui social di tutto anche le cose più intime della loro vita pur sapendo che una volta in rete il tutto diventa pubblico e prelevabile….), o aver la pazienza di fare un po’ più di coda per i sacrosanti controlli, tutto per proteggere e rafforzare la democrazia, contrastare la criminalità organizzata, il terrorismo islamico, i foreign fighters, e anche il terrorismo rappresentato da frange anarchiche interne che possono saldarsi con quello internazionale e far loro da “manovalanza”, fornendo al contempo le maggiori garanzie possibili a quel bene sempre più raro rappresentato dalla nostra riservatezza.