“Questa è una minaccia globale, richiede una risposta globale e un’azione rafforzata e coordinata”, ha dichiarato a Davos 2023 Jürgen Stock, segretario generale dell’Organizzazione Internazionale della Polizia Criminale-Interpol.
Negli ultimi anni, l’uso del cyberspazio è cresciuto sempre di più ed è utilizzato come metodo di conflitto sia dai governi che dagli hacker privati.
Il mondo 3D come lo conoscevamo fino ad ora è diventato 4D.

Sono passati quasi quattro anni da quando il cyberspazio è stato riconosciuto come l’ultimo spazio dei conflitti alla stessa stregua di terra, aria e acqua.
Con l’aumento dell’uso di apparecchiature informatiche, esso sta crescendo in maniera accelerata e ha raggiunto negli anni riconosciuti come “pandemia Covid-19” i livelli che ci si aspettava di raggiungere dopo circa 20 anni.
La mancanza di preparazione in termini di infrastrutture e risorse umane per questo fenomeno ha creato le giuste opportunità di hacking e danni a molti livelli.
Secondo i dati dell’anno scorso, gli attacchi informatici DDoS (Distributed Denial of Service) sono aumentati del 79% su base annua.
L’aumento dell’uso della rete e del cosiddetto Internet of Things – IoT ha reso ogni consumatore e non solo le organizzazioni, un bersaglio per l’hackeraggio.
Solo nelle prime tre ore del 15 aprile 2023 risultano 138.000.000 attacchi informatici, mentre i paesi più colpiti sono Mongolia, Nepal, Vietnam, Indonesia, Taiwan.
Istruzione, spazi governativi, e sanità sono i più danneggiati.

Il sistema sanitario risulta così essere progressivamente uno dei più hackerati degli ultimi anni. Gli attacchi consistono sia nel furto di dati sensibili sulla salute dei pazienti sia nel blocco dell’accesso ai programmi che garantiscono il servizio.
Riconoscendo questo crescente problema, l’ENISA – L’Agenzia dell’Unione Europea per la sicurezza informatica nel novembre 2018, ha organizzato in collaborazione con le società mediche europee e i produttori nel campo della sanità elettronica e dei dispositivi medici, il seminario sulla sicurezza informatica in questo campo specifico.
Sulla base delle discussioni e delle questioni evidenziate, nel 2019 è stata riscritta la normativa europea in ambito medico, rafforzando la legge sulla cybersecurity.

Conoscere i dati sanitari importanti di politici o leader è stato utilizzato fin dall’antichità per indirizzare strategie politiche in crisi.
Basti ricordare dall’antichità il caso di Alessandro Magno di Macedonia, e oggi i casi più gettonati di annunci sullo stato di salute di Arafat o di Putin.

Con la progressiva digitalizzazione delle istituzioni sanitarie e il rapido sviluppo della ricerca e dell’utilizzo dei dispositivi in questo campo, diventa sempre più urgente riconoscere e tutelare questa realtà in continua evoluzione.
L’hacking dei dati medici, il collasso del sistema sanitario anche per semplice attacco DDoS

o controllo remoto di dispositivi medici si traduce rapidamente in perdita di vite umane, come nel caso di hacking da parte di organizzazioni o privati, sia come semplice ricatto economico ma che può' diventare rapidamente un "arma" nei conflitti ibridi di oggi.
Si pensi al caso più semplice dell' intervento a distanza nel controllo di un pacemaker cardiaco, di un dispositivo di stimolazione transcranica o di una pompa per insulina; molto semplicemente questi si possono trasformare in un'arma non convenzionale.

L'hacking del sistema sanitario e la perdita di dati è considerato un fallimento della missione critica dell'istituzione.
Anche dopo l'eventuale funzionamento del sistema medico dopo un hacking, rimangono danni a lungo termine: danno d'immagine, danno legale, danno economico.
Se dall'indagine, obbligatoria in questi casi, emergesse che l'ente non ha rispettato quanto previsto dalla normativa sulla cybersecurity, i pazienti i cui dati sono stati violati o chiunque abbia subito un danno dall'evento può chiedere un risarcimento all'ente.

Ricordiamo l'hack globale WannaCry: il 12 maggio 2017, l'attacco informatico WnanaCry si è diffuso in 24 ore a 230.000 computer in tutto il mondo che usavano versioni obsolete del sistema operativo Microsoft Windows XP. Microsoft non aveva rilasciato aggiornamenti di sicurezza per il sistema operativo da aprile 2014, ad eccezione di una patch di emergenza del maggio 2014.
Gli hacker inviarono la richiesta di pagamento in Bitcoin a tutte le persone o istituzioni colpite in questo attacco.
Il danno è stato più devastante per 40 ospedali del Servizio sanitario nazionale (NHS) in Inghilterra e Scozia, con ripercussioni negative sui servizi ai pazienti e costringendo Inghilterra e Scozia a istituire un piano di emergenza governativo nazionale.
Se pensiamo ai richiedenti asilo politico, i dati sanitari personali (i dati personali sulla salute e i dati sullo stato clinico sono considerati tali) sono correlati a dati sensibili (religione, provenienza, convinzioni politiche o stato politico).

Secondo i dati dell'IOM (Organizzazione internazionale per le migrazioni) il numero di migranti è triplicato rispetto al 1970 e la rotta migratoria balcanica sta diventando sempre più importante in questo fenomeno.
I richiedenti asilo spesso lasciano i loro Paesi per convinzioni politiche, religiose o per fuggire ad organizzazioni terroristiche nel loro Paese di origine. Riporto l'esempio di tante giovani donne soprattutto eritree, che negli ultimi anni hanno chiesto asilo in Europa dopo essere riuscite a sfuggire dai terroristi di Al Shabaab/Harakat al-Shabab al-Moudjahidin, "il movimento dei giovani combattenti".
In questi casi, i dati sanitari comprendono anche dati anagrafici, religiosi, ideologici, familiari, ecc. che è necessario conoscere per curare al meglio il paziente dal trauma subito. Il servizio sanitario, nel caso dei centri per richiedenti asilo, diventa così un duplice bersaglio, sia di hacker "comuni" nel furto di dati, ma anche di hacker istituzionali dei

luoghi da cui questi pazienti sono partiti, o di organizzazioni terroristiche .

Esistono cinque principi per una solida cultura della sicurezza informatica:

1. trasparenza;
2. riconoscimento della responsabilità delle azioni che si compiono;
3. adeguata conoscenza del sistema;
4. conformità della programmazione informatica della società dove si opera con gli aspetti legali richiesti nel campo pertinente e con le procedure richieste;
5. conoscere i canali di comunicazione formali di un incidente informatico.

In termini legali, qualsiasi settore, società, servizio, incluso quello medico, è soggetto alle leggi locali e alle convenzioni sottoscritte.
La legge europea sulla sicurezza informatica è una parte specifica dell'ultima versione del GDPR (regolamento generale sulla protezione dei dati), adattata nel 2020.
Anche la Svizzera, che non fa parte dell'Unione Europea, ha firmato l'accordo con l'UE e si adegua a questa legge in particolare per quanto riguarda i dispositivi medici.

Il GDPR obbliga il servizio medico ad avere un responsabile della protezione dei dati (DPO). La mancanza di tale figura e la mancata attuazione di leggi specifiche in materia, comportano gravi conseguenze legali per i servizi sanitari, come sopra descritto.

Negli Stati Uniti, l'Health Insurance Portability and Accountability Act (HIPAA) richiede che tutte le informazioni sanitarie dei pazienti siano protette utilizzando tecniche di crittografia. La globalizzazione ha portato con sé anche lo spostamento di molti servizi sanitari al di fuori del rispettivo paese; ad esempio una società statunitense può aprire una filiale sanitaria all'estero o nell'UE. Fino ad ora, ci sono stati molti malintesi nella giurisdizione riguardante questo campo e che si sono tradotte per queste società in problematiche legali in termini di legalità informatica, non essendo chiaro a quale giurisdizione dovrebbero dovevano essere soggette. Gli ultimi anni hanno fortemente sottolineato l'importanza della chiarezza legislativa a riguardo.
Il Centro statunitense per gli studi strategici e internazionali ha sostenuto nel rapporto intitolato "A Human Capital Crisis in Cybersecurity" che il governo degli Stati Uniti aveva accesso solo al 3-10% dei professionisti della sicurezza informatica di cui aveva bisogno.

È innanzitutto imperativo che le organizzazioni dispongano in primis di una chiara gestione dell'identità e degli accessi (IAM). Secondo un sondaggio di Centrify su "Privileged Access Management in the Modern Threatscape", il 74% delle violazioni della sicurezza dei dati informatici inizia con "l'uso improprio di credenziali privilegiate" (Centrify Corporation,

2019).

Anche gli aspetti psicologici sono da tenere in considerazione nell' approccio alla cibernetica; paura di qualcosa che non possiamo vedere o toccare.
La paura è un aspetto biologico, naturale ed innata, che fa parte delle emozioni primarie di difesa, quindi non è nulla di negativo finché noi stessi non la rendiamo patologica.
Concentrandosi sugli aspetti che caratterizzano l'essere umano insieme agli scimpanzé (Human 2008, M.S. Cazzaniga, p. 84), la progettualità distruttiva e violenta è un aspetto che ci distingue dagli altri esseri viventi.

Conoscere questa caratteristica porta come risultato accettabile il fatto che se creo qualcosa, qualcun'altro cercherà di rubarla o distruggerlo.
La conoscenza di questi fenomeni implica una collaborazione interfunzionale tra competenze; come può un informatico o un ingegnere informatico costruire un dispositivo di stimolazione transcranica se non sa perché un medico ne ha bisogno, e come può un medico sfruttare al meglio le potenzialità che l'informatica offre se non ha le conoscenze necessarie? Come in altri campi, condividere conoscenze e confrontarsi crea una sorta di "incrocio genico" per far nascere qualcosa di nuovo, stimoli diversi aumentano la creatività.

Partendo dalle conoscenze e dai bisogni in continua evoluzione come ho descritto sopra, i Paesi dell'UE e non solo, hanno da tempo istituito dipartimenti di Medical Intelligence (MEDINT); negli USA, NCMI – National Center for Medical Intelligence.

L'articolo è estrapolato da "Cyber Intelligence and Cyber Terrorism in Medical Field" – Balkan Cybersecurity Days (Ohrid, maggio 2023); relatrice dott. med Emanuela Dyrmishi, spec. Psicofarmacologia, spec. Relazioni transculturali, analista in rischio economico, geopolitica e intelligence, form. Terrorismo e conflitti ibridi, spec. Gestione della sicurezza informatica, spec. Progettazione economica europea e internazionalizzazione.