L’Italia tra dominio cibernetico e geopolitica ibrida

Author : Andrea Chiappetta

Date : 15 Luglio 2020

Quando si parla di sicurezza, il pensiero va subito alla protezione delle nostre case, famiglie, attività, comunità. Su questo fronte le forze dell’ordine, tutte, sono impegnate quotidianamente. Tuttavia è necessario aumentare risorse e strumenti in mano alle autorità, occorre un piano di formazione che preveda anche la creazione di corpi specializzati che si occupino direttamente di prevenzione e difesa.

Alle strategie per tutelare il cittadino sul piano della sicurezza fisica si devono affiancare misure efficaci sul piano cibernetico, non meno pericoloso e insidioso; come cittadini, rappresentanti del mondo imprenditoriale e Pubblica Amministrazione dobbiamo essere pronti a **monitorare e proteggere il nostro mondo digitale**, che durante la pandemia ha visto sicuramente una forte capacità di adattamento e trasformazione, ma serve un piano, una strategia seria e ragionata.

Nel passato abbiamo avuto idee che non potevamo immaginare, né realizzare a causa della mancanza degli strumenti tecnologici; oggi la potenza di calcolo e il basso costo rendono tali strumenti estremamente più accessibili e questo riscriverà il concetto di crittografia e altro, aprendo il mondo a nuove sfide connesse al calcolo quantistico.

Le contromisure da intraprendere devono essere pensate in **ottica stratificata** (*“layered defence”*): solo l’adozione coordinata di misure comportamentali (i.e. cambio frequente di password complesse, backup regolare dei dati, aggiornamento sistematico degli strumenti di sicurezza, consapevolezza nei confronti del phishing e delle tecniche di *Social Engineering*, utilizzo consapevole dei social, …) e tecnologiche (i.e. utilizzo di firewall, antivirus, VPN…) può condurre a una corretta postura di sicurezza.

Questa la strategia che ognuno di noi può perseguire per far fronte a minacce sempre più crescenti e complesse: in **un futuro che è gia qui**, l’utilizzo di nuovi vettori di attacco quali il cyberspazio, le tecnologie avanzate di droni, canali organizzati di disinformazione costituiranno sempre più una minaccia al sistema paese e alle sue principali componenti: infrastrutture critiche, tessuto produttivo, sistemi elettorali.

Lo sviluppo e la crescente adozione di tecnologie IoT e AI aumenteranno sensibilmente la superficie d’attacco e getteranno le basi di una **nuova generazione di *malware* adattivi** e di

tecniche avanzate di *spoofing* d'identità; gli attacchi *ransomware* saranno sempre più sofisticati e mirati, le accresciute capacità e disponibilità di algoritmi di AI saranno strumento nelle mani di organizzazioni criminali per lo sviluppo e l'esecuzione di sofisticati attacchi di *Aocial Engineering* e, in sinergia con le recenti tecnologie *Big Data*, per l'elaborazione e commercializzazione sul mercato nero di informazioni riservate e sensibili come segreti di stato, brevetti e dati di natura sanitaria e socio politica dei cittadini.

La difesa ed il presidio del cyberspazio devono entrare nel nostro modo di vivere, esattamente come l'avvento delle automobili ha reso naturale guardare a destra e a sinistra prima di attraversare una strada trafficata.

Tenere sotto controllo i nostri dispositivi, aggiornarne i software, conoscere le nostre eventuali vulnerabilità, sono azioni che devono far parte di un **processo continuo di gestione del rischio informatico**. E ancora, se si allarga l'orizzonte, pensare a un cambiamento culturale profondo che parta dalle fondamenta: educazione – dunque scuola - e coinvolgimento di giovani imprese nello strutturarsi sempre di più come *cyberguardian* del prossimo futuro, perché la trattazione di questo argomento non può prescindere dal coinvolgimento attivo delle Istituzioni: solo attraverso una seria campagna di sensibilizzazione e consapevolezza mirata a tutte le fasce sociali, si possono gettare le fondamenta di quel substrato necessario a motivare e invogliare le nuove generazioni a intraprendere un percorso di studi legato al mondo della cybersecurity.

Un importante passo in tal senso è stato fatto con l'attuazione della Direttiva europea NIS, come con il DL Cyber che definisce un perimetro di sicurezza nazionale cibernetica; siamo sulla buona strada ma non possiamo fermarci, la sicurezza informatica è dinamica - non statica - e il processo amministrativo burocratico non sostiene un rapido adeguamento, rischiando di lasciare "aree scoperte" o scelte rinviate per troppo tempo.

Solo un forte sinergia tra mondo pubblico e privato, con il puntuale coinvolgimento degli atenei, può colmare un tema cruciale, ovvero quello di affrontare l'elevato ***skill shortage*** per far fronte alle crescenti richieste e quindi alla necessità di avere figure professionali qualificate.

Ma non solo formazione; risulta a mio avviso aumentare la presenza, in seno ai consigli di amministrazione di società che operano in settori rilevanti, di membri che abbiano la capacità di comprendere meglio la posizione dell'organizzazione sullo stato della sicurezza informatica, in quanto essa è uno dei temi su cui si concentra l'attenzione dei top manager e quindi trasferire tematiche complesse all'intero *board* per prendere le scelte migliori volte a garantire la sicurezza *in primis* dell'azienda, dei clienti, dei piccoli e grandi investitori. Tema che negli Stati Uniti è affrontato con molta enfasi.

Il cyberspazio è diventato uno degli aspetti più importanti di una società, di uno stato e di una vita individuale a seguito di rapidi sviluppi e dell'applicazione della tecnologia dell'informazione in modo estensivo. Presenta un elevato numero di potenziali sfide e rischi, oltre alla sua convenienza. Molti paesi che hanno fatto progressi nella tecnologia dell'informazione e della comunicazione hanno escogitato strategie e politiche per il cyberspazio, come la creazione di corpi militari specializzati e l'istituzione di unità e dipartimenti specifici, finanche alla creazione

di specifici ministeri (UK, Australia, Giappone etc).

La geopolitica, in special modo in questo contesto, è un fattore cruciale per comprendere, spiegare e prevedere la condotta internazionale dei paesi. Dal punto di vista del cyberspazio, occorre comprendere le influenze geopolitiche per fronteggiare e in taluni casi prevedere le gravi minacce che corrono in rete. Un'analisi delle operazioni informatiche negli ultimi dieci anni mostra **una chiara connessione tra motivazioni geopolitiche e campagne informatiche** sponsorizzate da Stati il cui obiettivo era duplice: sabotare e acquisire conoscenza. La geopolitica moderna deve essere combinata con la tradizionale raccolta di informazioni sulle minacce per aiutare le aziende e stati a determinare come, dove e quando rischiano di ottenere attacchi da parti esterne, coniugando quindi gli aspetti digitali ad aprendo alla geopolitica ibrida.

Su di noi grava la grande responsabilità di decodificare la realtà di oggi, coglierne le opportunità e lavorare seriamente per impostare una strategia di crescita sostenibile, economica, sociale ed etica; le scelte che prendiamo e che dovranno essere prese nell’immediato futuro, detteranno le condizioni di vita di quella che sarà l'Italia di domani, quella che non vediamo e che dobbiamo necessariamente tutelare.

L’Italia ha tutte le carte per avere un ruolo centrale nelle sfide “connesse” al dominio cibernetico: dobbiamo puntare a essere *leader* e non *follower*.

Articolo a cura di **Andrea Chiappetta**