E ci sono ancora degli attrezzi buffi che vorrebbero dare la parola al popolo

Il dominio cyber è oramai ritenuto un elemento fondamentale delle strategie di sicurezza nazionale delle principali potenze. Come ha sottolineato Paolo Mauri su queste colonne, la cyber-warfare sta assumendo un'importanza crescente nel contesto delle strategie di difesa delle principali potenze del pianeta. In questa sede si analizzerà la sicurezza e l'interesse nazionale e il loro legame col dominio cyber in un contesto allargato, in grado di mettere al centro anche le implicazioni economiche e sociali di un efficace gestione dei nuovi paradigmi tecnologici.
Se infatti la cyber-warfare è dominio d'azione riconosciuto come strategico anche dagli Stati Uniti e dalla Nato, la cybersecurity è un paradigma imprescindibile che si lega alla tenuta della sicurezza economica, politica e sociale dei diversi sistemi Paese. In un'epoca come quella globalizzata, in cui la competizione politica e il conflitto, anche coperto, avvengono in ogni dominio, il controllo dei paradigmi su cui viaggia la sicurezza dei dati dalla cui analisi dipendono le scelte degli operatori più rilevanti è fonte di vantaggi competitivi.

Una "cultura di sicurezza" per l'economia
Il tema della guerra economica e dell'intelligence economica acquisiscono sempre più rilevanza: nel contesto della battaglia geopolitica Cina-Usa, ad esempio, assistiamo a un conflitto allo scoperto sui protocolli di sicurezza delle comunicazioni, sulle reti del futuro, sul 5G, i cavi sottomarini e il legame tra "campioni nazionali" della tecnologia e agenzie di intelligence. Tutti domini con cui la cybersecurity si sovrappone in maniera fondamentale. Come insegnano Carlo Jean e Paolo Savona nel loro saggio Intelligence economica, "il ciclo dell'informazione rappresenta sempre più la base delle scelte di ogni sviluppo" politico ed economico; le nuove tecnologie già in circolazione pongono in essere un fattore di moltiplicazione delle opportunità e delle minacce legate alla gestione di questo ciclo; i paradigmi del prossimo futuro, dall'intelligenza artificiale al calcolo quantistico, aumenteranno la sensibilità, la quantità e il valore di input e dati processabili nel sistema, rendendo la loro tutela e la loro protezione un fattore sempre più cruciale.
Il domino cibernetico, per la sua intrinseca vulnerabilità, per la sua pervasività, per l'impunità che concede, è esposto a minacce provenienti da diverse direzioni: la cybersecurity si pone come una scelta non negoziabile per ogni attore che voglia essere protagonista nella società odierna. La fase di pandemia in corso ha esaltato l'importanza della cybersecurity nel contesto civile, come fa notare l'Ispi: in questa fase ci accorgiamo che le nostre società si affidano "sempre di più al dominio cibernetico per la nostra resilienza economica (lo smart working, l'e-commerce, eccetera) e sociale (social networks, insegnamento a distanza, eccetera)". Molto spesso le soluzioni adottate da imprese e enti di fronte alla fase di emergenza non hanno avuto

il punto di forza dell'elaborata complessità e della resistenza ad eventuali attacchi volti a forare banche dati, sistemi informativi, conti bancari e via dicendo.
"Eventuali interruzioni di servizio", dunque, "costano, a noi personalmente ed alla nostra società complessivamente, più caro (come plasticamente dimostrano gli attacchi cibernetici ai danni degli ospedali) e, per converso, gli attacchi cibernetici divengono potenzialmente più vantaggiosi per chi li attua".
Nel contesto italiano, una proficua cultura della sicurezza deve diffondersi anche nel settore delle attività economiche e produttive e non può non passare per un rafforzamento del perimetro di cybersecurity e di consapevolezza delle minacce ibride dell'era presente all'attività delle imprese, sia nel campo operativo che fuori di esso. Di questo avviso è anche Gabriele Suffia, studioso di dinamiche legate al cyber e cultore della materia di Informatica giuridica all'Università degli Studi di Milano, che contattato da Inside Over spiega: "Il tema della protezione delle aziende italiane" sotto il profilo della cybersecurity "si esplicita da un lato nella divulgazione della cultura della sicurezza a livello aziendale", aumentando la consapevolezza per l'utilizzo di prodotti sicuri, e dall'altro nella "tutela dallo spionaggio da attori stranieri come Stati Uniti, Cina Russia". Tutti spiano tutti, aggiunge Suffia, e "poter pubblicare per primo un brevetto e conoscere segreti aziendali ha grande rilevanza".
La reattività sul tema delle minacce cibernetiche è un "termometro" della resistenza di un sistema sotto il profilo della sicurezza economica: non a caso molto spesso il discorso che, in Italia, è portato avanti da istituzioni come il Copasir circa la difesa dell'economia in nome della sicurezza nazionale comprende questa dimensione oltre all'immancabile individuazione del rischio di scalate straniere ai campioni economici nazionali. Senza certezze sul primo fronte, non si può aver percezione delle problematiche insorgenti sul secondo.

Cybersecurity e sharp power

Nel contesto occidentale, oltre che al versante economico, la cybersecurity è stata associata anche alla minaccia proveniente da un altro fronte, quello dell'informazione. Negli Stati Uniti il National Endowement for Democracy ha coniato il termine sharp power per indicare la minaccia ibrida della disinformazione mediatica e informativa condotta da Paesi come Cina, Russia, Iran attraverso lo sfruttamento delle piattaforme telematiche, dei social e di vere e proprie offensive informatiche.
In Italia il tema è stato trattato nel saggio L'era dello sharp power, scritto dal fondatore di "Formiche" Paolo Messa. "La rivoluzione cibernetica", scrive Francesco Bechis nell'introduzione al saggio, "ha cambiato radicalmente le regole del gioco, aprendo un nuovo fronte in cui è difficile distinguere i lupi solitari dalle unità militari dei rispettivi Paesi. le spie in giacca, cravatta e valigetta ventiquattrore hanno lasciato il posto al ben più efficace spionaggio cyber. Il potere d'influenza delle Tv è stato soppiantato dalla penetrazione dei troll nella rete e nei social media". Una versione globalizzata della disinformacija di matrice sovietica, dunque: e un campo d'azione in cui la cybersecurity può giocare un ruolo importante per individuare veri o presunti tentativi di condizionamento esterni. Nella piena consapevolezza che ognuno gioca all'attacco nel territorio del rivale: Paesi come la Cina e la Russia non fanno altro che applicare le lezioni apprese studiando l'utilizzo di social network come Twitter per amplificare messaggi politici durante periodi storici delicati come le Primavere arabe, con il benestare soddisfatto dell'Occidente.

Conclusioni

In definitiva, la cybersecurity e la focalizzazione sul suo sviluppo implicano una decisa “militarizzazione” del perimetro civile della sicurezza nazionale, dato che rafforzarla significa prendere atto della natura ibrida e insidiosa di molte minacce. Un’agenzia di intelligence può sferrare un attacco alla banca dati di una società privata, un gruppo criminale tentare un’azione verso un ente istituzionale o previdenziale, due società finanziarie possono cercare sottobanco di soffiarsi informazioni l’un l’altra. Il perimetro del cyber è il regno dell’indistinto, della competizione di tutti contro tutti: e in un mondo globalizzato che accelera, piuttosto che attenuare, la rivalità tra sistemi-Paesi svilupparne i paradigmi è fondamentale. Per non soccombere nell’agone. Per non restare esclusi dal ciclo dell’informazione che dà linfa vitale alle economie di tutto il mondo.