Mediterranean Insecurity

I NUOVI ORIZZONTI DELLA DIFESA CYBER

Amm. Sq. Ferdinando SANFELICE di MONTEFORTE

Un'evoluzione tumultuosa

L'ambiente cibernetico ha compiuto passi da gigante, addirittura inimmaginabili, da quando l'Agenzia di Ricerca Avanzata per Progetti della Difesa USA (DARPA) sperimentò nel 1967 INTERNET, inizialmente chiamato di ARPANET. Il sistema era inteso, all'epoca, solo come un sistema di comunicazione più rapido ed efficace tra gli uffici all'interno del Dipartimento della Difesa, e quindi non richiedeva difese sofisticate per la propria sicurezza, se non quelle perimetrali.

Le Università, coinvolte nel progetto fin dall'inizio, fecero evolvere il sistema, per renderlo utilizzabile su scala sempre maggiore, rendendolo disponibile al grande pubblico. Da quegli anni ad oggi, la strada compiuta da INTERNET è stata tale da connettere, oggi, vari miliardi di persone, istituzioni, aziende e – purtroppo – criminali, singoli o gruppi uniti in apposite organizzazioni. Proprio questi ultimi utenti hanno capito, a un certo punto, che era possibile sfruttare la rete per compiere atti illegali o crimini, senza doversi muovere dalla propria scrivania, e con limitati rischi di essere colti in flagrante.

Dopo i criminali, sono arrivati gli Stati: sono bastati, infatti, pochi anni prima che i governi iniziassero a sfruttare questa facilità di connessione per perseguire i propri

interessi, spesso a scapito di altri Paesi, senza essere scoperti. Per maggiore cautela, spesso, sono state create organizzazioni vicine ai (o dipendenti dai) governi, delegate a compiere veri e propri atti ostili, come lo spionaggio, la disinformazione, l'interferenza sulla politica interna e l'economia altrui e persino il danneggiamento, anche grave, di infrastrutture sensibili. In alcuni casi, come nel caso dell'Estonia nel 2007, intere Nazioni sono state paralizzate da questo tipo di aggressioni.

In definitiva, l'ambiente cibernetico era diventato, negli anni scorsi, un vero e proprio Far West, un territorio senza legge, una situazione resa più agevole da tre fatti:

- come accennato prima, i progettisti di INTERNET, convinti che il sistema fosse esclusivamente per uso interno, non avevano previsto che terzi si intromettessero con fini malevoli, e quindi non avevano avuto cura delle difese antintrusione, al di là di quelle perimetrali;
- l'identità di chi prende iniziative in rete, sia essa un semplice messaggio o un vero e proprio attacco, è lasciata al buon cuore del mittente, per cui esiste da sempre un problema di scoperta dell'identità (e della localizzazione) di quest'ultimo (*Attribution*). Quindi, è stato difficile, fin dall'inizio, avere prove di accusa, valide in un tribunale (nazionale o internazionale), contro chi perpetrava crimini, o peggio, atti di guerra, in rete;
- dopo alcuni anni in cui alcune organizzazioni statuali o internazionali si erano tutelate, utilizzando computer speciali, diversi dai loro equivalenti disponibili al grande pubblico, e quindi difficili da penetrare, per risparmiare sui costi queste organizzazioni decisero di acquistare proprio i computer commerciali e i relativi programmi. Questa prassi, nota come COTS (*Commercial off the Shelf*) ha messo i privati e i criminali alla pari, in termini di mezzi, rispetto alle istituzioni, consentendo ai primi di "bucare" le protezioni, individuando i punti deboli dei sistemi e sfruttandoli a proprio vantaggio.

Di fronte a questa situazione, estremamente sfavorevole, è stato necessario studiare il modo di difendersi dagli intrusi, garantendo agli utenti pubblici e privati una sufficiente sicurezza di comunicazione e, al tempo stesso, la conservazione di dati senza il rischio di una loro perdita.

Il problema della difesa

Con il passare degli anni, si è visto che lo studio di sistemi di difesa cibernetica avrebbe dovuto prendere due strade, sempre più divergenti: da un lato, vi era la necessità di contrastare la criminalità informatica (*Cybercrime*), e dall'altro bisognava difendersi da attacchi massicci, ben congegnati e quindi estremamente pericolosi, come quelli condotti o sostenuti da Stati ostili (*Cyberwar*). I normali sistemi di difesa contro il crimine informatico, infatti, erano rapidamente sopraffatti da quest'ultimo tipo di attacco.

Il progresso dei sistemi di difesa è stato lento, anche perché la controparte era in grado di individuare i punti deboli di queste difese, e mettere in atto le misure idonee a superarle o aggirarle. Malgrado ciò, questa nuova versione della lotta tra il cannone e la corazza, ha visto le difese avvantaggiarsi lentamente, sia pure di poco, rispetto alle offensive.

Dalla già citata creazione dei "*firewalls*" (muri di fuoco) agli antivirus, fino ai sistemi anti-*malware*, il progresso è stato continuo; ci si è poi resi conto che i *software*, spesso, contenevano alcuni elementi di vecchia concezione, che aumentavano le vulnerabilità.

Infine, si è avuto cura di assicurare, per le infrastrutture critiche, un minimo di "*Resilienza*" che consentisse loro di funzionare, sia pure al minimo, anche in caso di attacco. In breve, si è visto che "fare pulizia" all'interno dei sistemi informatici era il presupposto fondamentale per poi poter avviare eventuali azioni contro gli attaccanti.

Questo rafforzamento delle difese, insieme con i primi passi avanti nel risolvere il problema della "*Attribuzione*" ha fatto entrare appieno l'ambiente cibernetico nel campo della strategia non solo perché questo ambiente si presta agli attacchi, ma anche per quanto concerne le strategie difensive.

Anche per questo, sia pure con un certo ottimismo, gli specialisti hanno iniziato a parlare di "*Difesa Attiva*" e, sia pure in prospettiva di lungo termine, persino di "*Deterrenza Cibernetica*".

Vediamo cosa dice la strategia teorica, su questi due approcci, e quanto questi possano essere applicabile all'ambiente cibernetico, che – come abbiamo visto – ormai non può più fare a meno della teoria, come ausilio per l'azione. Come osservava uno

studioso, infatti, "*La teoria è descrittiva ed esplicativa, strumento ed organizzazione di una conoscenza sistematica, essa si costruisce l'oggetto-strategia, per svelarne la natura e rendere intelligibile la sua complessità. Normativa, (anche se) con il rischio di ossificarsi nel dogmatismo dottrinale, utilizzando gli elementi del sapere che essa ha costituito, propone agli attori un insieme coerente di metodi di valutazione e di regole di condotta utili; essa offre loro una guida per un'azione che obbedisce alla sua economia specifica*"[1].

Se è ben vero che la teoria costituisce solo un supporto di pensiero, uno spunto di riflessione, e non limita in alcun modo l'inventiva dello stratega, essa è un utile riferimento per ogni campo d'azione che veda due volontà contrapposte l'una di fronte all'altra. E questo, precisamente, è il nostro caso.

La Difesa Attiva

Secondo l'Enciclopedia Treccani, la difesa è "*l'insieme delle mosse intese a consolidare i propri punti deboli o a parare le minacce dell'avversario (per es.,d. attiva, passiva, preventiva)*"[2]. A questa definizione, di carattere generale, si aggiunge un'altra, presa dal linguaggio delle discipline sportive individuali, specie quelle nate per la difesa personale, in cui si definisce la difesa attiva come quell'attività volta a bloccare l'offensiva dell'avversario e utilizzarla a proprio favore.

Sulla convenienza della difensiva, rispetto all'offensiva, invece, gli studiosi discutono da quasi due secoli. Da una parte, in effetti, c'è il grande Clausewitz, il quale osservava che "*Lo scopo della difensiva è conservare. Ora, poiché è più facile conservare che guadagnare, ne consegue che, a parità di mezzi, la difensiva è più facile dell'attacco, cioè la difesa è la più forte delle due forme di guerra. La forma difensiva della condotta della guerra non si limita quindi a parare i colpi, ma comprende anche l'abile impiego delle risposte*"[3].

Altri, invece, hanno contestato questa convinzione, asserendo che Clausewitz aveva ragione, parlando della guerra terrestre, ma in ambienti caratterizzati dalla loro

[1] L. PORIER, *Stratégie Théorique. Ed. Economica, 1997.* Vol. I pag. 5.
[2] TRECCANI. *Vocabolario on line.* Voce "Difésa".
[3] C. von CLAUSEWITZ, *Della Guerra.* Ed. Mondadori, 1970, Vol. II pagg. 444, 445.

vastità, come il mare e l'aria, la difesa comporta la dispersione delle forze e introduce, quindi, un fattore di enorme debolezza.

Diceva, a questo proposito, Mahan, che, sul mare, "*difendere significa semplicemente trarre il meglio da una cattiva situazione: cioè non facendo ciò che si vorrebbe fare, ma dando comunque il massimo possibile in base alle circostanze*"[4]. Inutile dire che, per la sua vastità, l'ambiente cibernetico assomiglia molto all'ambiente marittimo.

Tutti gli studiosi, comunque, concordano sul fatto che se si attende passivamente i colpi del nemico, si è comunque votati alla sconfitta. Su questo argomento la Linea Maginot è diventata l'esempio classico dell'inutilità di una difesa passiva. Quindi, anche in una situazione di difensiva strategica, è necessaria l'azione e l'iniziativa, per tenere a bada, guadagnare tempo e logorare l'avversario.

Proprio da queste considerazioni si è diffuso, negli scorsi decenni, anche nel campo della strategia teorica, il termine "*Difesa Attiva*", inteso come approccio da seguire, a fronte di un possibile attacco da parte di forze preponderanti.

Una prima definizione di questo approccio, che si trova nei documenti ufficiali, è che la Difesa Attiva è "*L'impiego di un'azione offensiva limitata e di contrattacchi per negare un'area o una posizione contestata al nemico*"[5].

Questa definizione, purtroppo, non si limita a prevedere reazioni a un attacco nemico, ma apre la porta a una possibile "*Difesa Preventiva*", nello stile della dottrina sovietica durante la Guerra Fredda. La sua applicabilità all'ambiente cibernetico, specie nel contesto europeo, legato ai principi della Carta dell'ONU, appare quindi limitata per motivi politici e giuridici.

Molto più interessante, anche perché oggetto di lunghi anni di elaborazione, è la definizione che viene data dagli studiosi di strategia teorica della Cina, dove la "*Difesa Attiva*" viene considerata, fin dal 1980, come la strategia ufficiale del Paese.

Fino a quella data, la strategia cinese era "*basata sulla preparazione (a contrastare) un attacco da ogni direzione e sull'abbandono della difesa avanzata per*

[4] A.T.MAHAN, *Strategia Navale.* Ed. Forum Relazioni Internazionali, 1997. Vol. II pag. 74.
[5] https//www.//militaryfactory.com

attirare il nemico in profondità. (Bisognava) combattere se possibile vincere, e ritirarsi se ciò non fosse possibile"[6].

Questo approccio, fortemente voluto da Mao Tse Dong, oltre ad assomigliare moltissimo a quanto egli aveva praticato nel corso della pluridecennale guerra civile e nella resistenza all'invasione giapponese, era perfettamente in linea con il pensiero strategico orientale.

Tra gli altri, ad esempio, lo stratega giapponese Musashi, all'inizio del XVII secolo, era stato estremamente esplicito in proposito, affermando che "*Quando* (il nemico) *vi attacca, rimanete imperturbabili, pur fingendovi deboli. Quando si avvicina, ritraetevi con violenza, quasi voleste spiccare un balzo. Poi, appena lo vedete rilassato, gettatevi addosso a lui*"[7]. Lo studioso, quindi, continuava asserendo che "n*ella strategia è necessario contenere l'assalto del nemico. Dovete comprimere i suoi slanci, e sapervi districare quando egli tenta di afferrarvi. L'espressione "comprimere un cuscino" significa questo*"[8].

In Cina, la strategia di far penetrare il nemico in profondità, prima di colpirlo, man mano che procedeva lo sviluppo economico della Nazione, diventò sempre più oggetto di critiche, specie da parte di chi osservava che cedere città e infrastrutture essenziali, a forza di ritirarsi, significava indebolirsi irreversibilmente.

Non vi era, in queste osservazioni, nulla di rivoluzionario. Infatti, una situazione simile si era verificata nel 1905, durante la guerra russo-giapponese, quando il generale russo Kuropatkin, a capo delle armate zariste, schierate in Manciuria, di fronte all'esercito nipponico, optò per una ritirata strategica, alternata a periodiche battaglie d'arresto, per logorarlo fino al momento in cui avrebbe potuto scatenare la battaglia decisiva.

Il problema di questa strategia fu che, nella ritirata, il generale si ritrovò a dover difendere a oltranza la città di Mukden, snodo principale del ramo della ferrovia transiberiana che collegava la penisola di Liao Tung al resto della Russia, senza il cui possesso la base di Port Artur, sotto assedio, sarebbe rimasta isolata e priva di rifornimenti.

---

[6] M. TAYLOR FRAVEL, *Active Defense.* Ed. Princeton University Press, 2019, pagg. 122-123.
[7] M. MUSASHI, *Il Libro dei Cinque Anelli*, Pillole BUR, 2002, pagg. 69-70;
[8] Ibid. pag. 72.

Memori di questo precedente storico, i generali cinesi cercarono di attenuare l'approccio strategico deciso da Mao, segnalando i pericoli che si correvano con tale strategia – ovvero la perdita di posizioni e infrastrutture critiche - anche se l'imponenza dello schieramento dell'Armata Rossa ai confini cinesi, che nel frattempo era arrivato all'imponente consistenza di 50 Divisioni, non concedeva molte alternative.

Lentamente, dopo che la dirigenza del Partito, sopravvissuta alla Rivoluzione Culturale, trovò di nuovo una compattezza, dopo la morte di Mao e l'arresto della "Banda dei Quattro", fu possibile concepire una nuova strategia, nel presupposto che non ci sarebbe stata una guerra nucleare all'ultimo sangue con l'URSS, bensì solo scontri con armamenti convenzionali, ancorché su grande scala, in linea con quanto attuato dai Sovietici nel 1968, per occupare la Cecoslovacchia.

La nuova strategia, messa a punto grazie a un seminario durato un mese, e approvata dal Capo del Partito nell'autunno del 1980, prevedeva "*una difesa avanzata, basata su una guerra di posizione, integrata da guerra di manovra su piccola scala, per prevenire uno sfondamento strategico e guadagnare tempo per la mobilitazione a livello nazionale"*[9].

Questo approccio strategico imponeva la creazione di "*una rete di posizioni difensive a più strati e in profondità, ognuna delle quali avrebbe dovuto essere distrutta dal nemico*"[10].

Questa rete di capisaldi, posti in modo da fornirsi sostegno reciproco, assomigliava molto, come concezione, a quanto era stato concepito, nel 1918, dal generale Diaz nella difesa della linea del Piave, e che si era rivelata un fattore di successo nella battaglia del Solstizio.

Nelle menti dei generali cinesi, in caso di aggressione, una volta guadagnato il tempo necessario per mobilitare il Paese, mediante un'azione ritardatrice, sarebbe stato possibile "*combinare la difesa delle linee interne strategiche con offensive per linee esterne, per creare una situazione di stallo. Infine, se la forza d'invasione si fosse sufficientemente indebolita, sarebbe stato possibile all'Esercito di Liberazione Popolare passare a una controffensiva strategica*"[11].

[9] M. TAYLOR FRAVEL. Op. cit. pag. 141-142.
[1010] Ibid, pag. 142.
[11] Ibid.

In definitiva, la "*Difesa Attiva"* così come concepita dai generali cinesi, si basava su alcuni elementi-chiave, e precisamente:

- Difesa avanzata (*Forward-edge defense*) in cui la rete di capisaldi dislocati in profondità, sarebbe stata sostenuta da una notevole potenza di fuoco. Per questo, l'Esercito ha "*messo in campo un numero crescente di missili balistici e di crociera, con gittate elevate e capacità di guida di precisione, intesi a respingere un'avanzata nemica fin dal primo approccio"*[12]. A tal fine, le capacità di operazioni multi-arma e interforze, da parte dell'Esercito Popolare di Liberazione furono ritenute fondamentali;
- Controllo Efficace (*Effective Control*) che presuppone il confronto e la distruzione dei sistemi avversari "*acquisendo il dominio in tre campi: informazione, spazio e aria, con il dominio dell'informazione ritenuto un prerequisito per acquisire la superiorità negli altri campi"*[13]. In questo ambito il cyber, la guerra elettronica, lo spazio e le operazioni psicologiche dovevano giocare un ruolo fondamentale.

Quindi, mentre la strategia di "*Difesa Attiva*" nella sua versione iniziale, si limitava a concepire una guerra di attrito prolungata, per respingere un invasore, prima di scatenare una controffensiva, nelle successive elaborazioni della strategia di "*Difesa Attiva*" è spuntato, in questi ultimi anni, un terzo elemento, denominato "*Guerra Localizzata*", che prevede la possibilità di un'azione "*localizzata geograficamente, lungo la periferia della Cina e limitata come scopo, durata e mezzi*"[14].

Per evitare che un Paese vicino provochi una guerra in grado di scatenare una reazione a catena, i generali cinesi hanno pensato che l'unico modo fosse quello di stroncare il pericolo sul nascere con "*la rapida applicazione della forza per conseguire gli obiettivi operativi e imporre una veloce risoluzione del conflitto"*[15].

Inutile dire che questo terzo elemento alludeva ai conflitti che la Cina ha avuto con l'India nel 1962 e con il Vietnam nel 1979, oltre a giustificare una possibile azione

[12] T. A. ORNELAS, *China's active defense military strategy.* Marines Corps Gazette, October 2021, pag. 58.
[13] Ibid.
[14] Ibid, pag. 59.
[15] Ibid.

punitiva nei confronti di Taiwan, impresa, peraltro, ben più complessa e ardua, rispetto alle prime due.

Possibili applicazioni all'ambiente cibernetico

Passando dall'ambiente operativo reale a quello cibernetico, è possibile notare che i primi due elementi della "*Difesa Attiva"* concepiti dagli strateghi cinesi possono trovare corrispondenza in una rete difensiva, in parte fissa e in parte mobile, in grado di prevedere una prima reazione automatica fin dall'inizio a un attacco massiccio, anche senza l'ambizione di sventarlo *in toto*, già nella sua fase iniziale.

Lo scopo di questa prima reazione è di guadagnare tempo, in modo da avere modo di dispiegare capacità di localizzazione e di reazione maggiori, contro i sistemi dai quali è partito l'attacco. Contro individui, come gli hacker e gli attivisti che compiono atti ostili contro singoli individui, piccole ditte e/o infrastrutture minori è sufficiente una difesa a livello locale, anche se gli attuali sistemi di difesa, come gli antivirus, gli anti-malware e le predisposizioni per assicurare la resilienza delle infrastrutture, non sono sempre sufficienti e andranno integrati.

Le cose si complicano, inevitabilmente, a livello di "Guerra Cibernetica", dato che sarà necessario controllare le vie di accesso a livello nazionale, predisponendo sistemi di filtraggio che rallentino, se non blocchino, l'azione avversaria. L'esempio già citato della rete di capisaldi, che si appoggiano mutuamente, come quella ideata dal Maresciallo Diaz per respingere l'offensiva austriaca del Solstizio 1918, appare da imitare, anche se richiede uno sforzo infrastrutturale e organizzativo notevole.

La seconda fase, quella della controffensiva, potrà iniziare, una volta che saranno evitati danni maggiori ai nostri sistemi. Inutile dire che questa seconda fase presuppone una capacità che non tutte le Nazioni potranno possedere, autonomamente. Specie in caso di un attacco massiccio, l'azione della controffensiva sarà efficace solo se partirà da più Nazioni, in modo concertato, e con una capacità di individuare la fonte dell'attacco (*attribution*) ben superiore a quella attuale. Bisogna, infatti, guardarsi dallo scatenare un "*Effetto Polifemo*", colpendo alla cieca, con il rischio di danneggiare chi non sia stato l'autore di un atto di guerra cibernetica.

A questo punto entrano inevitabilmente in campo Organizzazioni in grado di agire a livello internazionale, come la NATO e l'UE, anche se è ancora presto affinché queste riescano a dotarsi di sistemi così potenti da effettuare una controffensiva efficace, colpendo i punti vulnerabili dell'avversario, anche se sarà necessario rimanere nell'ambito cibernetico: nessuno, infatti, giustificherebbe azioni di altro tipo, specie quelle che prevedono l'uso di sistemi d'arma convenzionali.

A maggior ragione, intensificare la controffensiva fino al punto di privare il nemico della capacità offensiva, è un tipo di azione che, oltre a prevedere una capacità di individuazione dell'attore che ha perpetrato l'aggressione, impone un coordinamento tra più Nazioni, pena la sua inefficacia.

Questo, per noi Europei, significa dover organizzarsi in modo da poter ricorrere al supporto degli altri Membri dell'Unione o agli alleati della NATO. Sul piano giuridico, infatti, un attacco cibernetico potrebbe essere considerato un *casus belli* solo in attacchi particolarmente gravi. Però, la controffensiva, atto pienamente giustificato in questi casi, sarebbe possibile solo laddove l'aggressore venisse identificato con certezza, cosa ancora difficile da conseguire.

Per questi motivi, anche se si comincia a pensare ad una controffensiva con armi convenzionali anche per taluni attacchi cyber, è ancora giocoforza ricorrere solo a risposte simmetriche e limitate.

In definitiva, dovranno, naturalmente, essere predisposti piani e sistemi di "*Difesa Attiva*" in campo cibernetico, da parte delle Organizzazioni Internazionali di cui facciamo parte, oltre a predisporre piani nazionali, comunque indispensabili per affrontare le prime fasi di un attacco.

Se già la "*Difesa Attiva",* per essere efficace, richiede uno sforzo a livello multinazionale, potenziare i sistemi di protezione fino al punto di esercitare una "*Deterrenza Cibernetica"*, o quantomeno una "*Dissuasione Cibernetica*" è un'impresa ancora più complessa, il cui conseguimento appare ancora lontano nel tempo.

In ogni caso, poiché lo sfruttamento dell'ambiente cibernetico per compiere atti ostili sta diventando sempre più frequente, per effetto della crescente tensione internazionale, prepararsi, quando si è ancora in tempo, è un dovere. La strada è lunga, ma va percorsa, passo dopo passo, per garantire un livello di sicurezza che, oggi, non ci è ancora dato possedere.