Military Cyber Intelligence

Date : 2 maggio 2018

Dopo aver illustrato il concetto di Cyber Intelligence, il suo ruolo ed il suo potenziale nel precedente articolo, ci occuperemo questa volta di analizzare il suo impiego in ambito militare, per trattare poi nei prossimi quello in campo industriale e nel sistema paese.

L'intelligence è una parte fondamentale nelle strategie militari, tanto che di questa tematica si parlava già durante il VI secolo a.C.. Se ne ha evidenza grazie al testo scritto dal generale Sunzi (conosciuto anche come Sun Tzu), intitolato "The Art of War" (nella versione tradotta in lingua italiana, il titolo del libro è "L'arte della guerra").

Il documento non è altro che un trattato di strategie militari, nel quale vengono approfonditi gli aspetti collaterali della guerra e le strategie ad essa annesse. Nel testo viene anche illustrato il ruolo della spia, cioè raccogliere segreti, diffondere disinformazione o cattivi consigli nel campo nemico e se necessario assassinare i funzionari nemici.

Apro una piccola parentesi. La frase "diffondere disinformazione" e la tanto attuale "fake news" vi dicono qualcosa? … Stesso obiettivo perseguito con metodi e tecnologie diverse.

Ora più che mai, le operazioni militari si basano su un'intelligence tempestiva e accurata, informazioni sulle disposizioni di un avversario, la strategia, le tattiche, gli intenti, gli obiettivi, i punti di forza, i punti deboli, ecc. Quest'area ha sempre incluso lo spionaggio e il controspionaggio e oggi include anche la raccolta di informazioni. L'intelligence, con le sue attività di sorveglianza e ricognizione è diventata una componente chiave dell'attuale guerra in tempo reale condotta principalmente usando la rete internet per lanciare attacchi.

Nel campo militare l'obiettivo è quello di sviluppare una cyber intelligence in cui i soldati, già professionisti della pirateria informatica, abbiano anche forti capacità di analisi e un background di base sulle scienze umane in tutte le sue declinazioni.

Per dare una dimostrazione di quanto l'intelligence, e ancora di più la Cyber Intelligence, sia vitale in questo ambito, si cita quanto riportato nel sito delle forze armate britanniche e nello specifico nell'area dedicata all'intelligence:

"Ora più che mai, le operazioni militari si basano su un'intelligence tempestiva e accurata…

…I soldati che operano nell'unità d'intelligence devono essere in grado di valutare e decidere come, perché e in quale situazione devono usare la loro astuzia e la loro intraprendenza per stare un passo avanti al nemico. Essi svolgono un ruolo vitale nei processi decisionali dell'esercito e nella protezione delle sue operazioni da interessi ostili. Nella guerra moderna, la conoscenza è il vero potere". **[1]**

Le attività legate all'intelligence tradizionale, Open Source Intelligence (**OSINT**), Human Intelligence (**HUMINT**) e Signal Intelligence (**SIGINT**) sono componenti essenziali per la Cyber ??Intelligence. A differenza delle informazioni sulle minacce convenzionali, l'intelligenza cibernetica deve funzionare in tempo reale e includere l'intelligenza tecnica (TECHINT) sulle vulnerabilità e l'uso / rilascio di armi cibernetiche. Inoltre la CYBINT deve identificare e monitorare chi sviluppa, vende e utilizza le armi cibernetiche a livello globale.

Ma cosa è L'OSINT e perché è così importante e strategico a livello militare e di difesa?

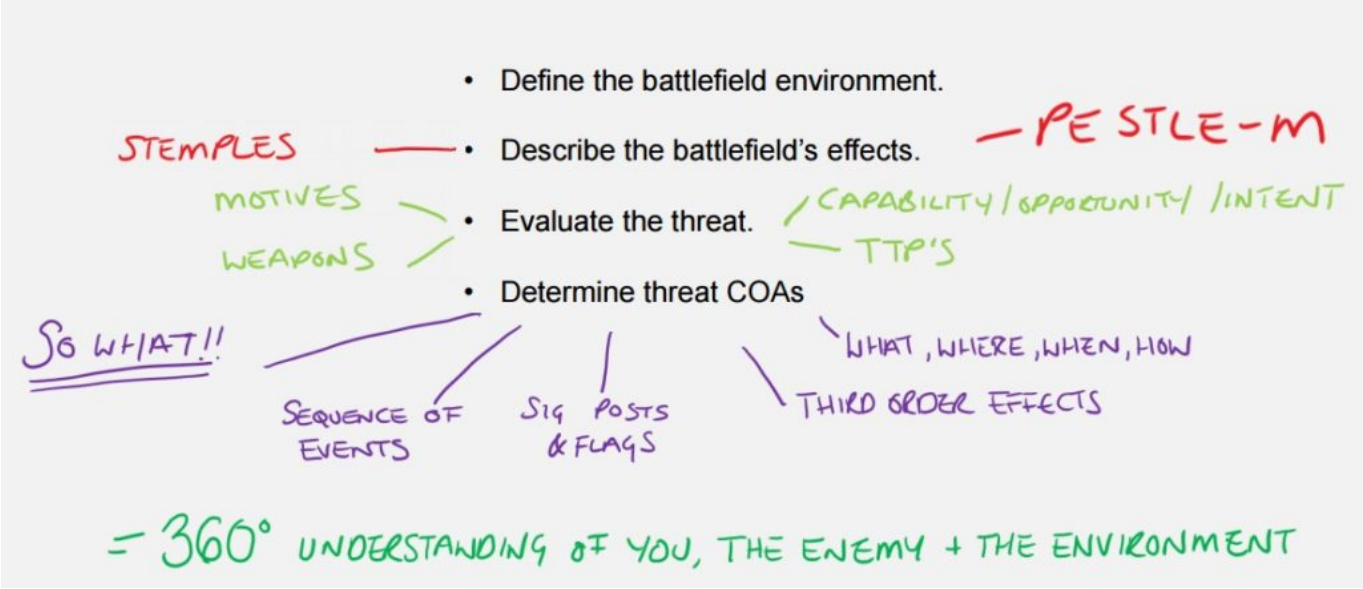
L'OSINT, basandosi su fonti aperte, consente un facile accesso a dati e informazioni permettendo a Script kiddies[2], hacker freelance o sponsorizzati da uno stato di raccogliere enormi quantità di dati per sfruttarli a proprio vantaggio. Analizzando i metadati di file e foto disponibili su siti web e social network si possono ottenere informazioni critiche e tracciare il personale per perseguire obiettivi futuri come attacchi di phishing e cyber spionaggio. Meno tracce e informazioni si espongono, meno conoscenza l'avversario ha di noi.

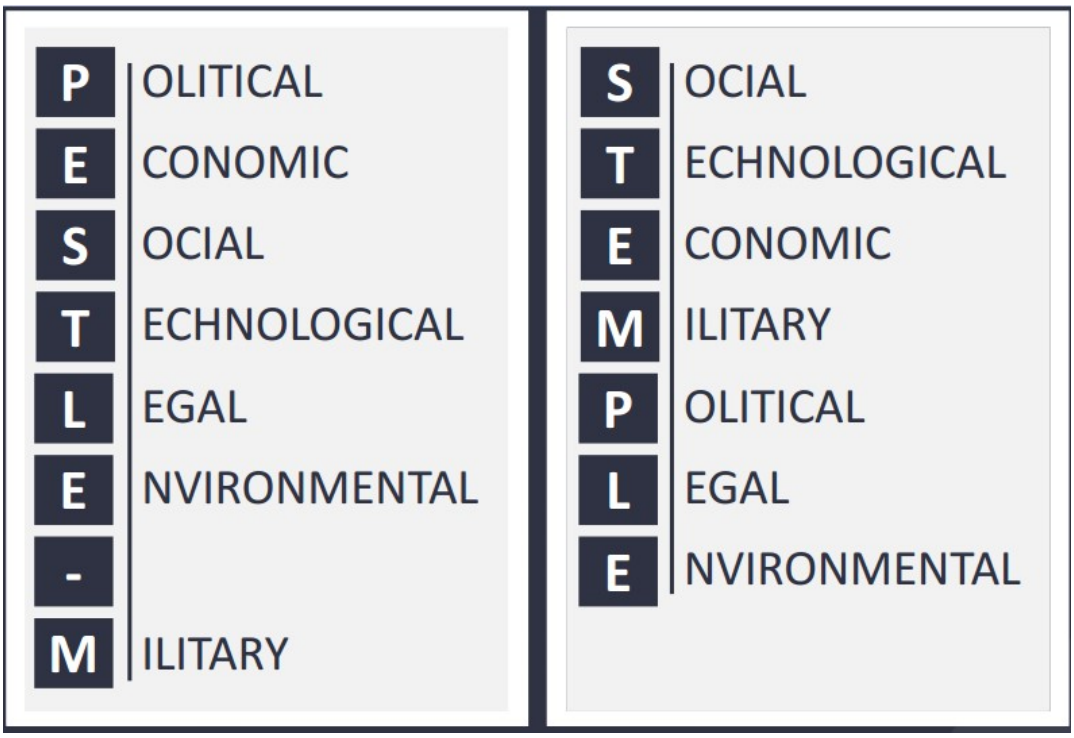
Le armi cibernetiche possono essere definite "la corsa agli armamenti 2.0". Queste stanno diventando l'obiettivo primario per ogni nazione in quanto possono essere usate in modo silente per attaccare un altro stato causando ingenti danni o disagi. La parte più drammatica di quanto appena detto riguarda la quasi impossibilità di attribuire con certezza un attacco ad una specifica nazione, in quanto il cyberspazio non ha confini geografici e i metodi per offuscare le tracce sono innumerevoli. Potenziali errori nell'identificazione della nazione attaccante o la perdita inaspettata del controllo di un'arma cibernetica che si diffonde sulle reti di paesi che non sono obiettivo dell'attacco, potrebbero coinvolgere nuovi attori nel conflitto allargandolo innumerevolmente. Questa situazione di confusione potrebbe potenzialmente sfociare in un ricorso alla forza militare convenzionale.

I concetti di trasparenza, proporzionalità e non proliferazione potrebbero essere ricodificati per scopi informatici. E forse le armi informatiche potrebbero essere collettivamente vietate, alla stessa stregua delle armi nucleari, chimiche e biologiche.

Proprio per la criticità che le cyber armi stanno assumendo oggigiorno, si sta cercando di regolamentarne il loro uso. Nel report "The Global Risks Report" [3] rilasciato qualche settimana prima dell'evento, tenutosi a Davos in Svizzera, si ipotizza in un prossimo futuro di vietare collettivamente l'uso delle "armi cibernetiche" alla stregua delle armi nucleari, chimiche e biologiche.

Rob Dartnall, Cyber Intelligence Director/CEO of Security Alliance, definisce l'intelligence da applicare al campo di battaglia in 4 punti[4]:

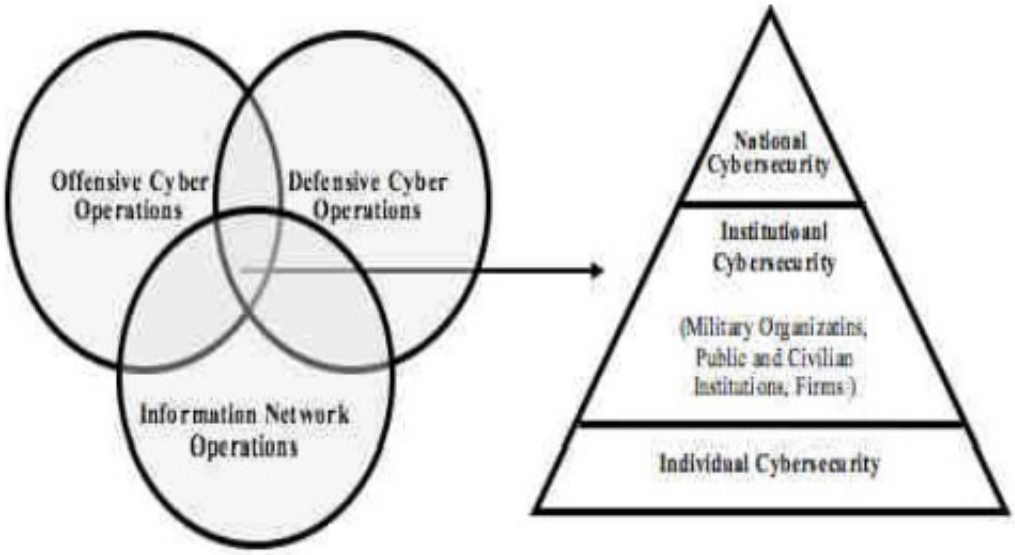




Le guerre ad oggi non vengono più combattute via terra o via mare, ma principalmente in un nuovo campo di battaglia definito "**cyberspazio**". Pertanto non si parlerà più di azioni militari ma di "azioni militari nel cyberspazio".

Queste, dette anche Cyberspace Operation, sono divise in tre macro aree:

- Operazioni Cyber Difensive
- Operazioni Cyber Offensive
- Operazioni di Raccolta Informazioni



Le tre macro aree che compongono le Cyberspace Operation devono essere integrate all'interno di un modello organizzativo più complesso che mira alla "protezione del sistema paese". Questo modello può essere riassunto in grafico piramidale, dove nella parte più alta troviamo la "Sicurezza Nazionale", alla base la cybersecurity di ogni singolo elemento del sistema paese (aziende e cittadini) e al centro tutti gli organismi militari, pubblici e privati che hanno un focus specifico sulle tematiche di cybersecurity.

Ad oggi, se si vuole realizzare un piano valido di Sicurezza Nazionale, bisogna costruire un sistema di "**Information Sharing**" che permetta la condivisione di informazioni tra tutti gli attori di primaria importanza per una nazione (infrastrutture critiche, il settore tecnologico e l'intelligence militare).

Verso la tematica di Sicurezza Nazionale si sono mosse la NATO con il "**National Cyber Security Framework Manual**"[5], l'UE con la "**Riforma per la Cyber Security**"[6] e l'Italia sviluppando il suo piano di sicurezza nazionale[7].

La tematica della cyber intelligence come strumento cardine per la Sicurezza Nazionale verrà trattata in modo dettagliato in un specifico articolo ad essa dedicato.

Note

- [1] https://www.army.mod.uk/who-we-are/corps-regiments-and-units/intelligence-corps/
- [2] https://it.wikipedia.org/wiki/Script_kiddie
- [3] WEF - The Global Risks Report 2018 - 13th Edition (https://www.weforum.org/reports/the-global-risks-report-2018)
- [4] https://www.sans.org/summit-archives/file/summit-archive-1517245731.pdf
- COA = Course(s) of Action
- [5] https://ccdcoe.org/multimedia/national-cyber-security-framework-manual.html
- [6] http://www.consilium.europa.eu/en/policies/cyber-security/

- [7] https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pubblicato-il-nuovo-piano-nazionale-cyber.html

A cura di: **Giuseppe Brando**