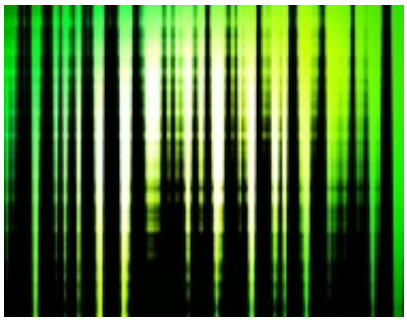
Russia-Ucraina: è guerra informatica

Date : 9 febbraio 2016



Quello che sta succedendo in Ucraina dimostra che la guerra informatica è una realtà nei conflitti moderni

Sono passati ormai cento anni da quando la prima guerra mondiale ha spostato il campo di battaglia nei cieli. Oggi nessuna nazione considera la propria difesa completa senza un'aviazione militare, così come in nessun grave conflitto futuro mancherà una componente informatica.

Vi sono prove che Russia e Ucraina si siano scambiate attacchi informatici durante la crisi a seguito del referendum sulla Crimea ancora in corso. Da alcune notizie apparse sui media abbiamo appreso che durante la votazione i siti web della NATO e dei principali quotidiani ucraini hanno subito attacchi DDoS (Distributed Denial of Service) e che, peggio ancora, successivamente a Mosca sono stati oscurati, alcuni server apparentemente a seguito di una rappresaglia.

Agli osservatori spesso però sfugge che in questi casi si tratta di schermaglie relativamente modeste nel cyber spazio. Sono molto comuni tra gli stati rivali, anche se non sono correlate a ostilità politiche o militari. Rallentare le risorse web di un avversario intasando le reti con traffico spazzatura? E' quasi normale. Nei conflitti informatici contemporanei, ci sono tre livelli, o categorie distinte. Nella crisi Ucraina solo il primo è chiaramente visibile. Non siamo ancora di fronte a una conclamata guerra informatica. Tuttavia, la prospettiva di un'escalation è reale e preoccupante. L'Occidente dovrebbe stare molto attento a quello che succede, perché quanto sta accadendo in Ucraina può benissimo essere preso a modello per i conflitti in corso in tutto il mondo.

Dall'osservazione del caso Ucraina, infatti, possiamo dedurre non solo le funzionalità delle armi informatiche, ma gli obiettivi e le motivazioni che stanno dietro il loro utilizzo.

La prima categoria di una guerra informatica è il livello "business as usual" - attacchi DDoS e intrusioni simili, poco raffinate.

Le interruzioni del servizio dei siti web esercitano sul nemico una pressione non molto rilevante,

ma sono il ceppo più visibile di attacco informatico, poiché chiunque può verificarne il successo: quando la pagina web non si carica, ha funzionato. Queste piccole stoccate sono più o meno continuative; una sorta di spionaggio di tutti i giorni. Durante i conflitti diplomatici o peggio, tuttavia, il numero e la varietà di attacchi aumenta.

Gli attacchi di questo livello in Ucraina presentavano tracce di outsourcing. Come è avvenuto precedentemente nei casi della Russia con l'Estonia e la Georgia, gli attacchi sembrano provenire da mercenari o da "hacker patriottici" protetti dall'alto, cui viene delegato l'atto vero e proprio dell'attacco, piuttosto che dalle forze armate o dall'apparato di intelligence. Questo è preoccupante, perché l'assunzione di hacktivisti offre ai governi la possibilità di negare il proprio coinvolgimento negli attacchi informatici stessi.

Durante la guerra fredda le superpotenze hanno combattuto conflitti a colpi di proxy, facendo ricorso a formazione, investendo denaro e materiale nel teatro degli scontri, come il Vietnam. Assoldare mercenari informatici a contratto è una conseguenza di tale prassi che risale al 21° secolo, anche se ovviamente non è più necessario essere una superpotenza per provocare il caos.

La seconda categoria di conflitto informatico comprende attività di informazione concentrate attraverso Internet, le cosiddette INFOOP. In particolare, le INFOOP si riferiscono a campagne di propaganda e disinformazione che hanno l'intento di spostare o infiammare l'opinione pubblica. Durante la fase di preparazione al voto sulla Crimea, la Russia ha combattuto e vinto una "guerra dell'informazione" sui media tradizionali. Sono state diffuse e riprese interviste pilotate, immagini manipolate e filmati di russi maltrattati a seguito del crescente stato di violenza e insicurezza. Il lato informatico delle INFOOP dà una nuova veste a un fenomeno noto. Gli specialisti di disinformazione possono pompare propaganda classica attraverso siti web di notizie e social media, infiltrandosi nelle comunità online, e rendendo più difficile per la popolazione online distinguere la verità. C'è un lato positivo, però, in questo livello delle INFOOP all'interno del conflitto informatico. Finché le cose rimangono a quel livello, fino a quando la disinformazione è abbondante e la popolazione ha difficoltà a discernere ciò che è vero e ciò che è falso, la crisi non è ancora sfociata in una guerra, reale o virtuale.

Dopo le INFOOPS, infatti, si trova il terzo e più allarmante livello di conflitto informatico: gli attacchi alle infrastrutture critiche, pubbliche e private con l'obiettivo di interrompere o disabilitare i servizi essenziali. Tali attacchi prendono di mira obiettivi che possono includere le reti ATM, i sistemi di ecommerce, le reti energetiche, i segnali stradali e di transito, il controllo del traffico aereo e le linee di comunicazione militari. Se il conflitto Ucraino si intensificasse fino ad arrivare a questo livello, si arriverebbe all'inizio formale di una guerra informatica, insieme alla quale anche la guerra, fisica, sarebbe più probabile. Si tratta della principale conseguenza di attacchi informatici nel modo reale che possiamo ipotizzare e che porterebbe alle ostilità militari.

Gli strumenti di attacco sono anch'essi lo specchio della società che li utilizza. E' logico per una moderna società informatizzata che anche le reti siano considerate campi di battaglia. Tuttavia, c'è ancora molto da fare affinché i governi capiscano i modelli per prevedere le possibili escalation e le conseguenze di una guerra informatica - in particolare, quando è

possibile che un’aggressione superi il confine del mondo virtuale colpendo il mondo reale.

Ecco perché la Crimea, oltre a tutto il dolore e la tensione che racchiude, rappresenta anche un’enorme opportunità. Per poter osservare lo svolgersi di un moderno conflitto informatico in tempo reale, imparando la portata dei danni causati dai potenti attacchi “business as usual”, gli effetti della disinformazione nel cyberspazio, e sperando che non si verifichi un assalto un’infrastruttura di fasetre fino ad arrivare all’utilizzo della violenza militare. C’è da sperare che chi tira i fili di questi attacchi informatici a Mosca e Kiev, oltre a mettere a prova le proprie reciproche capacità informatiche, stia imparando cosa può succedere – e si stia esercitando in particolare sulla virtù della moderazione.

A cura di **Jarno Limnéll**, *Esperto di scienze militari, direttore cyber security, di McAfee parte di Intel Security*

Articolo pubblicato sulla rivista ICT Security – Giugno 2014