Il cyberspace e la guerra cibernetica: verso l'e-conflitto

di Roberto Colella

18-09-2016

Le minacce al cyberspace sono parte integrante della quotidianità. Hanno oggi forme diverse, diversi scopi e coinvolgono diversi attori. Professionisti della cyber intelligence, attivisti - o hacktivist, data la dimensione in cui operano -, vere e proprie bande criminali possono acquisire informazioni sensibili, attaccare infrastrutture di vitale importanza per il Paese o la privacy dei singoli cittadini. In questo contesto è il concetto stesso di guerra a cambiare, dando origine a quello che si può definire e-conflitto o guerra cibernetica.

Per questo è necessario acquisire una consapevolezza su questi fenomeni, sulle dinamiche che li caratterizzano, sulle ricadute che possono avere sul singolo e sulla comunità, e sul ruolo che ognuno può giocare per limitare i rischi e, nel peggiore dei casi, le conseguenze.

Cyberweapons

Stefano Mele, professionista di sicurezza, cyber-terrorismo e cyber warfare, nel testo "Cyberweapons - Aspetti giuridici e strategici" definisce giuridicamente una cyber-arma (o cyberweapon) come "un'apparecchiatura, un dispositivo ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica, le sue informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento"

Le cyber weapons offensive possono essere di tre tipi: semplici, moderatamente complesse e complesse, e ciò in funzione della conoscenza ottenuta sui sistemi di controllo dell'obiettivo: nel primo caso si sfrutta direttamente la mancanza di autenticazione; nel secondo si procede preliminarmente a individuare il processo di controllo; e nel terzo il processo stesso viene furtivamente alterato con la conseguenza che il bersaglio non si rende conto del pericolo.1

E dato che molte strutture sono isolate dal vettore Internet, vengono studiate altre soluzioni, fra le quali - a parte le chiavette USB - l'uso di segnali radio per inserire malware in remoto.

L'uso di armi cibernetiche presenta però anche dei delicati problemi. Ad esempio, può essere limitato in zone critiche al fine di evitare danni collaterali a strutture civili (ospedali, etc.) e anche perché un codice distruttivo, tramite tecniche di reverse engineering, può essere rimbalzato contro il mittente.

Cyberspace e guerra cibernetica

Il concetto di cyberweapon è strettamente collegato a quello di cyberspace. Secondo Martin C. Libicki il cyberspace non è altro che un medium virtuale diverso rispetto agli altri domini come la terra, l'acqua, l'aria e lo spazio extra-atmosferico.

Per comprendere la natura ibrida del dominio cibernetico, Libicki rappresenta questa realtà su tre livelli2:

1) Il livello fisico (costituito da elementi "materiali" del cyberspace come cavi a fibra ottica, i satelliti, i router, le antenne.

2) Il livello sintattico in posizione superiore a quello fisico è costituito dalle informazioni e dalle istruzioni che i progettisti e gli utenti danno allo strumento informatico, si tratta di protocolli operativi per mezzo dei quali i computer o le "macchine" interagiscono con le infrastrutture di riferimento. In questo strato si possono verificare operazioni di hacking, ovvero individui outsider che si introducono nel sistema.

3) Il livello semantico rielabora i dati contenuti nelle macchine.

Sotto l'aspetto ambientale il dominio cibernetico si distingue dagli altri ambiti militari. La geografia del cyberspace è molto più mutevole rispetto ad altri ambienti. Le party del cyberspace possono essere attivate con dei semplici click.

Lo spazio cibernetico nel tempo ha cominciato a rimodulare il conflitto stesso. I primi casi di guerra cibernetica hanno coinvolto formazioni irregolari come gli zapatisti del subcomandante Marcos3, ma i casi più emblematici di e-conflittualità sono stati quelli a ridosso del conflitto indo-pakistano per il Kashmir e soprattutto della guerra della Nato contro la Jugoslavia. In quest'ultimo caso, si trattava di una guerra cibernetica che era stata iniziato dai serbi, a cui si erano aggiunti i cinesi dopo il bombardamento dell'ambasciata di Belgrado.

Questa guerra cibernetica aveva visto un massiccio spamming verso i siti del Pentagono e della Nato, un tentativo fallito di penetrare nel sistema operativo del sito della Casa Bianca.

Gli Stati Uniti avevano reagito auspicando attacchi hacker contro i presunti conti su banche estere di Milosevic. In pratica, mentre per lungo tempo l'utilizzo operativo degli e-attacchi era stato riservato agli apparati militari delle grandi e medie potenze, attualmente nell'uso commerciale sono sempre più presenti soggetti irregolari a sostegno di movimenti o gruppi terroristici.

All'inizio del 2001, il Pentagono aveva simulato per la prima volta nella sua storia un conflitto di cinque giorni nello spazio contro una potenza ignota, utilizzando satelliti spia, satelliti killer, raggi laser, missili, scudi spaziali e computer. Dopo quell'esperienza, i generali avevano sentenziato che "la cosa più importante" per la sicurezza dell'impero era la "difesa dei satelliti e dei computer". In particolare, questi ultimi dovevano essere resi impenetrabili. La chiave di tutto, comunque, era la dissuasione e gli Stati Uniti dovevano raggiungere una superiorità militare e tecnologica nello spazio tale da dissuadere chiunque dall'attaccare l'America o i suoi alleati4. In altre parole, l'impero si stava preparando a combattere pure una guerra cibernetica.

Hacktivists e attacchi Ddos

In queste guerre parallele una menzione speciale meritano gli hacktivisti (combinazione di "attivismo e "hacking") israeliani. Il primo caso di e-ostilità ha riguardato un Ddos che aveva messo fuori uso per una settimana o più il sito ufficiale Hizbullah. Gli israeliani avevano inviato attraverso il provider America On Line migliaia di e-mail, alcune delle quali con un virus. Si erano dati da fare per contattare gli hacker più esperti e avevano creato un sito per "search and destroy" i siti arabi. Da lì era possibile organizzare gli attacchi, e scaricare strumenti per attacchi Dos user-friendly, cioè di

utilizzo facile per i principianti. C'era poi una chat room con vari link, un sito civetta per attrarre potenziali lettori del sito Hizbullah ufficiale e perfino un sito trappola che prometteva di scaricare il necessario per gli e-attacchi contro Israele, ma che in realtà metteva fuori uso il pc dell'incauto hacktivista5.

Il Ddos in generale consiste in una tipologia di attacco nel quale gli hacker attivano un numero elevatissimo di false richieste di servizio, provenienti in contemporanea da più macchine e rivolte al medesimo server, consumando le risorse di sistema e di rete del fornitore del servizio. In questo modo le strutture informatiche dell'azienda, dell'ente o del provider "affogano letteralmente sotto le richieste incessanti, poiché non più in grado di erogare i servizi per i quali sono preposte, risultando quindi irraggiungibile.

In diverse occasioni alcuni dei network provider coinvolti hanno dichiarato di essere stati sommersi da oltre 1 Gigabyte al secondo di traffico. In realtà, il più delle volte, questo tipo di attacco occulta un ben più serio pericolo: il controllo totale del/dei sistema/i sotto attacco da parte dell'hacker, il quale trasforma il sistema nel così detto "zombie" al proprio servizio, anch'esso pronto a sferrare attacchi su nuove direttrici di rete.

Il primo (e il più abusato) prodotto di DoS che ha acquisito notorietà è stato lo Smurf Attack che tutt'oggi è in grado di paralizzare reti con tecnologie non aggiornate (generalmente piccole/medie aziende e ISP locali). In seguito è stato utilizzato The LowDown, conosciuto anche come Network Saturation Attack o Bandwidth Consumption Attack: un nuovo attacco DoS in grado di inondare un network con un numero impressionante di pacchetti. I router e i server che subiscono l'attacco, nel tentativo di gestire correttamente il traffico, subiscono un eccessivo carico di lavoro a causa del quale interrompono la propria funzionalità. Ovviamente l'eccesso di traffico ostile rende impossibile anche il traffico lecito (posta, web, file transfer ecc.) bloccando intere reti in pochi minuti.

La generazione successiva, attualmente impiegata, è appunto quella degli attacchi di tipo Distributed Denial of Service (DDoS) e Distributed Reflection Denial of Service (DRDoS).

Spingendo all'eccesso l'idea del network saturation attack, il DDoS ripete lo stesso approccio utilizzando però diversi punti d'ingresso contemporanei: in questo modo un cracker (un individuo in grado di effettuare azioni di crash di sistemi telematici, alterandone il codice di funzionamento) è in grado di mettere in ginocchio sistemi più grandi che sarebbero indifferenti a un singolo flood.

Per effettuare questo genere di operazione si deve poter installare un proprio agente sui sistemi da cui si vuole scatenare l'attacco stesso.

È quindi una tecnica che viene preparata per tempo, attrezzandosi con un pool di macchine compromesse da poter scagliare contro il sistema vittima. Il DRDoS consiste invece nell'attuazione di un DDoS con ulteriore moltiplicazione delle fonti di attacco. Ciò avviene mediante il reclutamento di server operanti su larga banda (ISP Server o DSL Bandwith Server) innescati da delle SYN request (richieste di connessione).6

Le frontiere della guerra cibernetica

L'ultima frontiera della cyber war è oggi la cyber repressione.

Una guerra cibernetica è in realtà vasta e complessa, e non si limita ad azioni di hacking. Alcuni attacchi hanno ramificazioni molto profonde basti vedere quello che è successo in Siria.Appare chiaro quindi che nell'era dei bit i DDoS rappresentano un'arma importante.

Inoltre facendo uso della terminologia militare, a proposito dei targeted attacks si parla, infatti, di advanced persistent threats, APT, intese a minacciare o addirittura ad aggredire entità economiche precise.

Le APT, infatti, si differenziano dai tradizionali attacchi di massa perché sono progettate appositamente per colpire obiettivi precisi e sono dotate di strumenti appropriati per azioni pianificate, anche se non fulminee ma lente.

Ciò dimostra la preparazione e gli obiettivi ambiziosi a cui punta chi attua un'APT prevede la competenza non di semplici hacker, ma di entità ben più importanti.

Nel giugno 2010, il malware "Stuxnet" è divenuto pubblico, qualcosa come una "bomba digitale a penetrazione" che attaccava il programma nucleare iraniano.

Durante la crisi del Kosovo la NATO ha subito i primi seri casi di guerra cibernetica. Questo ha portato al blocco per molti giorni degli account di posta elettronica dell'Alleanza per i visitatori esterni, e alla ripetuta distruzione del sito web della NATO.

Inoltre nel 2008, uno dei più seri attacchi è stato lanciato contro i sistemi computeristici militari USA. Attraverso una semplice penna USB collegata a un pc portatile del sistema militare in una base militare in Medio Oriente, la spia è penetrata inosservata tanto nei sistemi classificati che in quelli non classificati. Ciò ha mostrato cosa voleva dire avere una testa di ponte digitale, da cui migliaia di file erano stati trasferiti a server sotto controllo straniero.

Stuxnet ha mostrato il potenziale rischio di malware che colpisce i sistemi computeristici fondamentali che gestiscono l'approvvigionamento energetico

Si sono verificati dei massicci attacchi ai siti web governativi e ai server in Georgia durante il conflitto Georgia-Russia, rendendo concreto il termine di guerra cibernetica. Queste azioni non hanno prodotto subito un danno fisico. Hanno indebolito il governo georgiano durante una fase critica del conflitto. Hanno pure influito sulla sua capacità di comunicare con un'opinione pubblica nazionale e mondiale assai scossa.

Come se tali rapporti non fossero già abbastanza minacciosi, il bruco Stuxnet, apparso nel 2010, ha evidenziato un ulteriore salto qualitativo nelle capacità distruttive della guerra cibernetica. Nell'estate 2010, si sparse la notizia che circa 45.000 sistemi di controllo industriale della Siemens su scala mondiale erano stati infettati da un virus trojan specifico che poteva manipolare i processi tecnici fondamentali per gli impianti di energia nucleare in Iran.

Molto simile alla struttura modulare di Stuxent è stata quella di Gauss, un esempio di malware progettato per colpire una precisa infrastruttura, ovvero quella bancaria, limitandosi all'area geografica del Libano. Scopo principale quello del cyberspionaggio bancario.

I malware Stuxnet, Duku, Flame e Gauss, secondo l'uso internazionale, sono definiti "cyber

weapons", ma - a rigore - solo Stuxnet, finora, ha dimostrato di avere capacità letali.

Duku, Flame e anche Gauss, pur rassomigliando per certi aspetti a Stuxnet, tanto è vero che gli Stati che li hanno prodotti sono quasi certamente gli stessi, hanno avuto finalità spionistiche, attivandosi per rubare informazioni, talora prevalentemente specifiche e su determinate regioni del mondo, propedeutiche a possibili successivi attacchi di guerra cibernetica.

Secondo il Dipartimento di Difesa degli Stati Uniti le cyber operation possono essere distinte in tre categorie differenti: a) computer network attack CNA ; b) computer network exploitation CNE ; c) computer network defence CND7.

Le CNA comprendono tutte quelle operazioni "finalizzate a disturbare, negare, degradare, distruggere le informazioni contenute all'interno di computer o reti di computer, o i computer e le reti stesse".

Le CNE sono quelle operazioni di intelligence "atte a permettere la raccolta di dati da una rete o un sistema informativo automatizzato di un obiettivo o di un avversario".

Le CND, infine, si riferiscono alle "azioni intraprese per proteggere, monitorare, analizzare, rilevare e rispondere alle attività non autorizzate nei sistemi informativi del Ministero della Difesa e nelle reti informatiche".

E' bene tenere a mente che, a rigore, solo le CNA, e tra queste solo quelle che costituiscono una minaccia o un uso della forza, potrebbero dare vita a una guerra cibernetica vera e propria.

1# D. Peterson, "Offensive Cyber Weapons - Construction, Development, and Employment", in "The Journal of Strategic Studies", febbraio, 2013.

2# Cfr al riguardo M.C. Libicki, "Cyberdeterrence and Cyberwarfare", RAND, Santa Monica, California 2009.

3# Cfr. al riguardo D. Ronfeldt - A. Martinez, "A Comment of the Zapatista "Netwar"", in J. Arquilla -D. Ronfeldt , (a cura di), op. cit., pp. 369-391.

4# E. Caretto, "Anno 2017, guerra Usa-Cina", in "Corriere della Sera", 30/1/2001, p. 14.

5# A. Sema, "E-Strategie per E-Conflitti: il caso Israele" in «Limes 2001» Quaderni speciali, I signori della rete.

6# M.A. Vatis, "Cyber Attacks During the War on Terrorism: A Perspective Analysis" - Istitute for Security Technology Studies, Dartmouth College - 2001. Si veda anche F. Corona - "Web Intelligence", dispense corso Techno-Intelligence del Master in Sicurezza e Intelligence (MAINS) Link Campus Università di Malta - Roma, 2004.

7# E. Greco, "Cyberwar e Cybersecurity" Istituto di Ricerche Internazionali Archivio Disarmo (IRIAD) SIS - 11/2014.