Cyberwar

Se al posto dei cannoni la guerra si fa coi computer

I rapporti di forza internazionali si giocano ormai sullo scacchiere cibernetico
Un esercito di specialisti tecnologici e di hacker al centro degli equilibri futuri

NELLA STANZA DEI BOTTONI Le grandi potenze mondiali hanno capito che il futuro delle relazioni internazionali si giocherà anche attraverso le strategie cibernetiche. I reparti speciali addestrati alle guerre informatiche sono quindi in grande espansione e gli investimenti in quel settore continuano ad aumentare.

Meno cannoni, navi, aerei e missili ma più computer, hacker e virus informatici. Complice anche la crisi finanziaria molti tra i Paesi che rivestono un rilevante ruolo militare stanno tagliando i budget assegnati alla Difesa riducendo arsenali e organici in tutti i settori tranne quello della guerra informatica. L'ultimo esempio in tal senso giunge da Londra, alle prese con una spending review che sta riducendo ai minimi termini la consistenza delle sue forze militari ma prevede massicci investimenti nella guerra cibernetica. Non solo in termini difensivi, cioè per proteggere le reti informatiche nazionali (civili e militari) dai virus e dagli attacchi lanciati dal «nemico» ma anche in termini offensivi, sviluppando cioè la capacità di paralizzare le reti informatiche degli avversari. «Costruire le difese digitali non è sufficiente, come in altri campi della guerra serve un deterrente. La Gran Bretagna si doterà di strumenti per il contrattacco nel cyberspazio e, se necessario, per lanciare a sua volta attacchi» ha detto senza mezzi termini il ministro della Difesa, Phil Hammond, ricordando che nel 2012 sono state bloccate 400 mila minacce informatiche dirette contro reti sensibili del Regno Unito. Secondo fonti governative l'anno scorso il 93% delle grandi società e il 76% delle piccole aziende britanniche hanno subito intrusioni informatiche. Come hanno già fatto cinesi, russi, israeliani e statunitensi anche i britannici contano di arruolare nel nuovo reparto per la cyberwar militari specializzati e «talenti» provenienti dal mondo civile.

GIANANDREA GAIANI

Il primo assaggio di cyberwar su vasta scala si verificò durante la crisi tra Mosca e Tallinn nel 2007 quando un attacco condotto da server situati in Russia paralizzò per un mese le reti informatiche estoni che gestivano il Governo, il Parlamento, banche, ministeri, giornali e radio-televisioni. Un black out attuato con un «click» (che Mosca replicò l'anno successivo contro la Georgia) aggirando le deboli difese delle reti informatiche dell'Estonia che fino a pochi anni prima sarebbe stato ottenibile solo con una guerra convenzionale impiegando migliaia di tonnellate di bombe e provocando migliaia di morti. L'impatto di quell'evento dimostrò come in un'era in cui i conflitti convenzionali diventano sempre più impropribili per ragioni legate ai costi da sostenere e all'impatto negativo sull'opinione pubblica, la cyberwar sta diventando l'arma prioritaria per colpire le capacità strategiche di un Paese senza sparare un solo colpo. Non è un caso che la NATO abbia istituito proprio a Tallinn il suo Centro di eccellenza sulla cyberwar (Cyber Defence Centre of Excellence) nel quale decine di esperti elaborano strategie e dottrina per la guerra informatica. Se il recente caso di Edward Snowden ha confermato come il controllo delle reti informatiche e in generale delle telecomunicazioni consentano agli Stati Uniti e ai loro alleati anglosassoni operazioni di spionaggio a livello globale non va dimenticato che la Cina è forse il Paese che ha messo meglio a frutto le capacità cyber tese a sottrarre segreti militari e industriali arruolando migliaia di hacker «patrioti» e istituendo speciali unità militari già impiegate in massicce intrusioni nelle reti informatiche di Taiwan, Giappone e Stati Uniti.

Secondo fonti citate dal Financial Times, nel 2007 i cinesi sarebbero riusciti a penetrare il computer di Robert Gates, allora segretario alla Difesa e da allora hanno tentato più volte di carpire dagli archivi informatici del Pentagono e delle aziende del settore militare i segreti dei più sofisticati sistemi d'arma statunitensi (vedi box in basso).

Scontri sulla Rete

I confini delle cyberwar vanno però ben al di là del mondo degli 007 per assumere la dignità di una vera e propria capacità bellica. Paradossalmente solo i Paesi del terzo mondo, ancora lontani dalla piena digitalizzazione, sono relativamente immuni da attacchi portati con virus informatici mentre nei Paesi avanzati si punta ormai alla «cyber guerra preventiva», cioè ad autorizzare azioni di attacco contro nemici reali o potenziali perché tutti gli esperti concordano nel ritenere che l'attacco informatico sia molto più semplice e gestibile della cyber difesa dalla sterminata distesa di reti informatiche. Insomma se il fronte da presidiare è troppo esteso la migliore difesa è l'attacco. Fonti statunitensi e britanniche riferiscono di migliaia di attacchi condotti ogni giorno contro le reti informatiche, il National Cyber Bureau di Tel Aviv ha denunciato decine di migliaia di attacchi quotidiani alle reti israeliane condotti soprattutto dagli hacker di Hamas e della Jihad islamica. Gerusalemme ha istituito il suo Cyber Command potenziando il reparto militare di intelligence elettronica «Unit 8200» spendendo quest'anno in questo settore ben 537 milioni di euro. Investimenti giustificati non solo dai successi conseguiti in difesa ma soprattutto dall'aver ritardato lo sviluppo del programma atomico iraniano grazie al virus Stuxnet, sviluppato insieme agli statunitensi che nel 2010 mandò in tilt gran parte delle centrifughe utilizzate da Teheran per arricchire il suo uranio. Negli Stati Uniti, a fronte di una consistente riduzione di organici in tutte le forze armate, viene potenziato il Cyber Command, posto alle dirette dipendenze dello Strategic Command col compito di proteggere gli oltre 15.000 computer che fanno capo alla rete del Pentagono in 4.000 basi, uffici e installazioni sparsi per una novantina di Paesi. Nei prossimi anni il Cyber Command quintuplicherà le forze da 900 a 4.900 addetti suddividendole in tre divisioni: le «national mission forces» per difendere i sistemi informatici e le reti civili, le «combat mission forces» per pianificare e attuare attacchi informatici e le «cyber protection forces», che dovranno rafforzare il sistema di difesa delle reti militari. Il moltiplicarsi degli attacchi informatici e i rischi per la sicurezza nazionale (strategica ed economica) emersi recentemente con il caso Snowden hanno indotto molti Paesi a correre ai ripari istituendo specifici comandi militari e centri di coordinamento tra la Difesa e le infrastrutture civili. Nel maggio scorso il Consiglio federale ha approvato la «Strategia nazionale per la protezione della Svizzera contro i cyber rischi» incaricando il Dipartimento federale delle finanze dell'attuazione della strategia in collaborazione con l'Amministrazione federale, i Cantoni e l'economia entro il 2017 e di costituire a questo scopo un organo di coordinamento. Non tutti gli attacchi informatici sono definibili episodi di guerra cibernetica. Ad esempio i dati riguardanti l'Italia resi noti dal rapporto Clusit riferiscono un aumento del 254 per cento degli attacchi informatici nel 2012 rispetto all'anno precedente ma di questi il 54% erano legati ad azioni criminose , il 31 % ad attivismo politico e il 6% a cyberwar e spionaggio mentre per il 9% dei casi non è stato possibile stabilire l'origine. Del resto sul fronte cibernetico il confine tra crimine e azione di guerra è molto labile. Il professor Richard B. Andres del National War College sottolinea il crescente impiego da parte dei Governi di «milizie irregolari» invece di unità militari per le incursioni informatiche. «È una tecnica che i Paesi aggressori stanno usando sempre di più per colpire gli Stati Uniti e altre nazioni» costituendo bande autonome di hacker senza credenziali ufficiali che possano agire senza far ricadere la responsabilità sui Governi.

IL CASO

QUEI «FALCHI» CINESI COSÌ SIMILI AI «FULMINI» AMERICANI

«Una percentuale schiacciante di attacchi informatici contro aziende, agenzie governative e organizzazioni statunitensi provengono da un edificio per uffici alla periferia di Shanghai, che è collegato all'Esercito Popolare di Liberazione cinese». Il rapporto stilato dalla società Mandiant, contractor del Governo di Washington in materia di sicurezza informatica, attribuisce gran parte degli attacchi cyber agli hacker al soldo del Governo cinese che avrebbero rubato enormi quantità di informazioni dalle reti informatiche americane. Nel «bottino» vi sarebbero anche molti segreti militari legati soprattutto alla propulsione dei velivoli a decollo corto e atterraggio verticale e alle tecnologie stealth che rendono i velivoli meno visibili ai radar. Nel 2009 il Wall Street Journal riferì che pirati informatici erano riusciti a impossessarsi di molti dati relativi all'F-35 «Fulmine», il cacciabombardiere di Lockheed Martin destinato a equipaggiare le forze aeree USA e alleate. Il Pentagono smentì la notizia e Lockheed Martin ammise solo il tentativo di penetrare le difese informatiche della società, tentativi che vennero definiti «continui». Nel maggio di quest'anno un rapporto preparato per i vertici del Pentagono dagli esperti del Defense Science Board ha confermato intrusioni di hacker soprattutto nelle reti di società contraenti o subcontraenti del Dipartimento della difesa che avrebbero sottratto informazioni circa molti sistemi d'arma, dai velivoli F-35 ed F-18 ai missili antimissile Thaad, dal sistema radar e missilistico navale Aegis alle navi Littoral Combat Ship (LCS), dagli elicotteri Black Hawk ai convertiplani Osprey MV-22. Pechino ha respinto le accuse ma i risultati del cyber spionaggio cominciano a «vedersi». Le ultime corvette «invisibili» cinesi pare utilizzino soluzioni e tecnologie «mutuate» dalle LCS americane così come i nuovi aerei invisibili (sviluppati anche in versione ad atterraggio verticale) J-31 «Falcone» sembrano avere davvero molto in comune con gli F-35. Così i cinesi «si sono risparmiati 25 anni di ricerca e sviluppo» ha affermato un alto ufficiale americano protetto dall'anonimato. GG

DI COSA SI TRATTA

LA DEFINIZIONE

Spesso sui media si sente parlare di cyber armi o di cyber attacchi senza che queste terminologie vengano adeguatamente spiegate lasciando così che vengano avvolte da un alone misterioso e vagamente fantascientifico. Come ci spiega Stefano Mele, da noi intervistato nella pagina accanto, è invece importante anche da un punto di vista del diritto internazionale, che venga definito che cosa è realmente una cyber arma. Si tratta, ci spiega l'esperto, di «un'apparecchiatura, un dispositivo ovvero un qualsiasi insieme di istruzioni informatiche utilizzato all'interno di un conflitto tra attori, statali e non, al fine di procurare anche indirettamente un danno fisico a cose o persone, ovvero di danneggiare in maniera diretta i sistemi informativi di un obiettivo critico nazionale del soggetto attaccato».

LE CARATTERISTICHE

Ne conseguono così alcuni elementi tipici delle cyberwar che possiamo tentare di sintetizzare così: «l'obiettivo, deve essere mirato e, pertanto, l'apparecchiatura, il dispositivo ovvero qualsiasi insieme di istruzioni informatiche non devono essere stati creati con lo scopo di avere la massima diffusione, come accade per i generici malware; i sistemi informativi colpiti devono essere qualificabili come un obiettivo critico nazionale del soggetto attaccato; l'obiettivo dev'essere di penetrare attivamente e con finalità malevole i sistemi informativi del bersaglio (non quindi di creare un semplice disservizio); i sistemi informativi dell'obiettivo devono essere protetti e infine, perché si possa parlare di cyberwar, si devono creare danni fisicamente tangibili o significativamente rilevabili».

L'INTERVISTA STEFANO MELE

«Ma contro Assad le armi informatiche servono a poco»

L'analisi dell'esperto di studi strategici

MATTEO AIRAGHI

Uno scenario in cui molti intravedono i prodromi di una guerra cibernetica è quello siriano. Ne abbiamo parlato con l'avvocato Stefano Mele, coordinatore dell'Osservatorio «InfoWarfare e Tecnologie emergenti» dell'Istituto Italiano di Studi Strategici Niccolò Machiavelli, tra i massimi esperti a livello europeo di cyber guerre e del ruolo del cyber spazio nel contesto dei conflitti armati.

Dottor Mele, innanzitutto una considerazione di carattere generale, che ruolo stanno assumendo le tecnologie informatiche nell'ambito dei conflitti militari contemporanei e perché?

«Le tecnologie informatiche oggigiorno governano in maniera trasversale e completa i ritmi della nostra vita e le modalità di gestione di tutte le nostre infrastrutture statali, sia in ambito civile che militare, siano esse sensibili o meno. Comunicazioni, trasporti, lo sviluppo e il benessere economico, così come l'approvvigionamento elettrico, idrico e di beni, sono solo alcuni dei principali esempi di ambienti dove le tecnologie svolgono ormai un ruolo predominante e imprescindibile. La possibilità di danneggiare o anche solo disattivare temporaneamente i sistemi informativi di una nazione attraverso un cyber attacco rappresenta oggi una (nuova) minaccia di primaria importanza capace di colpire in qualsiasi momento, da qualsiasi parte del mondo e, soprattutto, con una altissima probabilità per chi attacca di restare completamente anonimo ed impunito».

La situazione siriana, ad uno sguardo superficiale, sembrerebbe prestarsi particolarmente a questo tipo di attacchi, perché lei è invece scettico al riguardo?

«In prima battuta, a differenza dei Paesi occidentali, l'intero tessuto sociale siriano, così come le sue infrastrutture militari, godono di un livello di permeazione delle tecnologie informatiche medio-basso. Com'è facile immaginare, anche solo questo elemento costituisce un primo e rilevante ostacolo ad un possibile cyber attacco su vasta scala o comunque ad un attacco informatico da cui scaturiscano effetti considerevoli in ambito di sicurezza nazionale.

Peraltro, l'estrema sofisticazione e personalizzazione richiesta ad una cyber arma per colpire ogni singolo e specifico obiettivo sensibile, nonché l'alto potenziale di danno che queste devono portare con sé, comportano per la loro realizzazione un notevole quantitativo di risorse economiche, di tempo e di forza lavoro altamente specializzata, così come di un rilevante lavoro da parte del comparto intelligence. Tutti elementi incompatibili allo stato attuale con le esigenze e le tempistiche del conflitto siriano.

Infine, anche in caso di un cyber attacco da parte degli Stati Uniti, Bashar al-Assad avrebbe in mano una carta difensiva di impareggiabile efficacia, tipica esclusivamente dei regimi dittatoriali o delle oligarchie, ovvero disconnettere istantaneamente l'intero territorio siriano dalla rete Internet, facendo immediatamente cessare ogni effetto dell'attacco».

Ma il cyber spazio può anche fungere da semplice supporto alle operazioni militari «tradizionali». Ci sono precedenti in questo senso e con quali esiti?

«Al di là delle fanfare mediatiche e delle (più che legittime) necessità promozionali delle aziende, il ruolo principale attualmente ricoperto dal cyber spazio in un'ottica di sicurezza nazionale è esattamente quello di agevolare attacchi militari tradizionali.»

Pertanto, alla luce di quanto detto finora, ad Obama non resta altra chance se non quella di sfruttare le eventuali debolezze dei sistemi informatici della difesa siriana (quasi tutti di provenienza russa) proprio per agevolare attacchi fisici tradizionali, disabilitando, ad esempio, i sistemi di controllo dello spazio aereo al fine di facilitare gli attacchi missilistici e/o gli eventuali successivi bombardamenti aerei.

Nulla di nuovo per il Governo americano, che nel marzo del 2011, in occasione della predisposizione dei piani di attacco contro la Libia, valutò in maniera molto concreta la possibilità di colpire e disabilitare attraverso un cyber attacco alcuni obiettivi sensibili e i sistemi di difesa aerea del Governo di Gheddafi, commissionando uno specifico studio sulle infrastrutture tecnologiche libiche ad un gruppo di 21 esperti del settore a livello internazionale (il dottor Mele ha fatto parte di questo gruppo di esperti, *Ndr*).

Un'ulteriore opzione – meno «ovvia» – potrebbe essere quella di colpire i conti bancari detenuti da Bashar al-Assad e dagli altri leader siriani, al fine di prosciugarli o comunque alterarne la capienza, tagliando così una parte – sicuramente consistente – delle risorse economiche del regime a supporto del conflitto.

Anche questa opzione non risulta totalmente nuova. Gli americani ci pensarono già per colpire Saddam Hussein e Slobodan Milosevic. Nessuno di questi attacchi, tuttavia, almeno per quanto è dato sapere da fonti pubbliche, alla fine fu mai posto realmente in essere per paura delle ovvie ricadute nel campo del diritto internazionale e per evitare di creare un precedente storico. I tempi però, oggigiorno, potrebbero essere maturi».

In che modo, allora, il regime di Bashar Assad potrebbe difendersi e reagire ad una cyber guerra scatenata dagli Stati Uniti?

«Nel settore della cyber security, quando si pensa alla Siria, la mente corre immediatamente al gruppo di attivisti denominato Syrian Electronic Army. Nel merito, questo gruppo – attualmente tra i più attivi e pericolosi sulla scena dei cosiddetti hacktivist – non è nuovo ad attacchi contro obiettivi americani e solo negli ultimi mesi si è caratterizzato per numerose operazioni di hacktivism e di social engineering. In ambito strettamente governativo e di Forze Armate, invece, la Siria non è ancora capace di mettere in campo reali capacità di cyber warfare, dovendo necessariamente affidarsi, almeno in questo settore, esclusivamente al potenziale di attacco di eventuali alleati».

Che ruolo, allora, potrebbero giocare gli alleati di Assad, Russia e Iran in testa, in questa guerra tecnologica. Da cosa devono guardarsi in particolare gli Stati Uniti e le altre potenze occidentali?

«Pensando ad un possibile attacco e/o contrattacco, decisamente più preoccupante è la possibilità da parte della Siria di attirare dalla sua parte alleati ben più solidi e preparati ad un vero e proprio scontro attraverso il cyberspazio, capaci di rappresentare una discreta minaccia anche in un'ottica di cyber warfare. È il caso della Russia, che già da tempo ha sviluppato eccellenti capacità soprattutto nei settori della cyber intelligence e del cybercrime e che, di conseguenza, potrebbe decidere di colpire – in maniera più o meno evidente – obiettivi americani non governativi di prima fascia (come grandi società private e multinazionali, magari anche vicine al comparto Difesa). Ma questo è anche il caso dell'Iran, uno dei principali e più solidi alleati della Siria, che ha investito ingenti somme di denaro nella creazione di unità militari specificatamente addestrate alle attività di cyber warfare. Per quanto lo scenario tracciato sia abbastanza semplice e lineare, non è detto, infine, che anche chi oggi si oppone all'utilizzo delle armi chimiche da parte del Governo di Bashar al Assad, in caso di scoppio di un conflitto reale, potrebbe decidere di appoggiare – anche in maniera occulta – le azioni del Governo siriano, protestando contro l'interventismo degli Stati Uniti. Ciò potrebbe essere fatto, qualora le capacità lo permettano, ovviamente anche attraverso un attacco informatico».

La carta del dittatore

In caso di cyber attacco Assad potrebbe difendersi semplicemente disconnettendo la Siria da Internet