

Hacking Team, cyberwarfare e il futuro della guerra

di Francesco Piccinelli

01-09-2015

Per quanto chi si riconosce in una tradizione di sinistra prenda molto sul serio l'Articolo 11 della Costituzione, l'ipotesi di conflitti armati resta sempre e comunque attuale. Lo abbiamo scoperto molte volte, dal '48 ad oggi pagando, in alcuni casi, anche un alto tributo di sangue e, purtroppo, rischiamo di scoprirlo altrettante volte, nei prossimi anni, visti il deterioramento delle relazioni internazionali, la crisi finanziaria cinese, il caos ucraino, la nascita di organizzazioni come l'ISIS, il rebus Afghanistan con il progressivo ritiro delle truppe alleate e le tensioni territoriali del Sudest asiatico.

Questo Risiko di grande complessità, nel quale ogni cancelleria è in grado di segnare e segnalare ogni colpo di cannone che cade - come accaduto in Corea recentemente - sta venendo, piano piano, reso ancora più complesso dall'ingresso in forze di tecnologie sempre più sofisticate che mettono in discussione, soprattutto nei paesi democratici, il legame che c'è tra conflitti armati e politica.

Clausewitz, Machiavelli, Paret, Sun Tzu, Jomini: tutti i teorici militari hanno sempre tenuto presente che lo scopo della guerra è politico e che spetta ai politici decidere quando usare le armi e con quali obiettivi. Il problema è che le tecnologie più moderne rendono molto opaco lo scrutinio da parte della leadership politica nei confronti dei militari o - peggio ancora - dei tecnici che lavorano per loro arrivando ad eccessi difficili da giustificare anche partendo da posizioni radicalmente militariste e nazionaliste.

Ciononostante, le operazioni che vengono svolte attraverso nuovi sistemi d'arma e rilevazioni che fanno uso di tecnologie avanzate devono essere sottoposte al segreto più assoluto, per essere portate a termine per due motivi: un'opinione pubblica poco propensa ad accettare perdite in termini di vite umane e uno stato delle relazioni internazionali che - quantomeno - sconsiglia l'uso della forza nella risoluzione di conflitti tra stati delegandolo o a milizie senza insegne (come avrebbero fatto i russi nelle operazioni nell'Ucraina orientale) o ad altri metodi, come le cyber guerre, o, più, propriamente, il cyberwarfare.

Il fenomeno ha visto un'esplosione, negli ultimi anni, con governi di tutto il mondo che hanno usato software e tecnologie sofisticatissime - in alcuni casi con la complicità degli operatori TLC - per sorvegliare cittadini e nemici. Per quanto il sabotaggio rimanga un'ipotesi abbastanza remota e (ad oggi) mai verificata, è indubbio che, in caso di situazioni molto conflittuali, un gruppo di Hacker cinesi potrebbe intrufolarsi nei server di una linea aerea, bloccare il software che distribuisce i piani di volo agli aerei della linea aerea in questione e provocare un danno agli Stati Uniti che potrebbero rivalersi assumendo il controllo - per esempio - di una centrale nucleare o dell'impianto di segnalamento dei treni ad alta velocità cinesi.

Il tutto, in linea teorica, potrebbe tranquillamente passare sotto silenzio, data la sostanziale asimmetria che esiste tra chi gestisce i sistemi che potrebbero essere oggetto di attacco da parte di forze ostili e data la riservatezza che - al momento - esiste sulle attività di cyberwarfare a livello globale.

Per esempio, chi sa cosa combina il NATO Cooperative Cyber Defence Centre of Excellence? Certo, il centro, fondato nel 2009 a Tallin, svolge un'apprezzabile attività di ricerca e di addestramento dei tecnici della NATO per quanto riguarda la guerra digitale. Eppure, sulle attività che la NATO svolge in questo ambito non esiste scrutinio politico e questo non può che generare

qualche dubbio su come il tema viene affrontato, stretti tra una sonnolenta opinione pubblica e la necessità che le operazioni di cyberwarfare si svolgano nella riservatezza più assoluta.

La lezione dello scandalo Hacking Team

Per quanto lo spazio cibernetico sia virtuale, quando diventa un campo di battaglia ha bisogno - anche lui - di armi. Le armi che vengono utilizzate assomigliano molto a delle formule magiche: sono righe e righe di codice che vengono scritte da una élite di programmatori che è in grado di costruire software che sono in grado di entrare dentro a device come tablet, pc, smartphome e - da qui - entrare dentro a server e rubare le informazioni che questi contengono.

Come ha riportato la cronaca degli ultimi mesi, una delle aziende più sofisticate del settore era la milanese Hacking Team che, dai suoi uffici di Via della Moscova, trattava con i governi di mezzo mondo i propri software di intrusione e di sorveglianza di massa. E lo faceva a chiunque, letteralmente, anche se i governi in questione non erano esattamente democrazie compiute.

La pubblicazione delle mail - a cura di WikiLeaks - ha permesso di accedere a un mondo degno di un romanzo di spionaggio fantascientifico: software, governi, spie, inchieste giornalistiche. In altre parole, gli ingredienti per una spy story in diretta dal futuro. Una spy story particolarmente sinistra perché, mentre i software di Hacking Team finivano negli inventari delle forze di sicurezza di mezzo mondo, tutto questo accadeva senza che nessuno potesse effettuare il minimo scrutinio.

In fondo, il software è facilissimo da distribuire: basta una connessione Internet ed è tutto a posto, lo scrutinio da parte delle autorità è ridotto al minimo. Non solo. A volte, sembra che le autorità non capiscano un accidente di quello che società come Hacking Team fanno.

In una delle mail che sono state pubblicate da WikiLeaks è evidente: uno dei soci va a Roma per discutere di un'inchiesta giornalistica su Hacking Team da parte de "L'Espresso" e se ne va incassando un attestato di stima da parte dei dirigenti ministeriali che ha incontrato esprimendo fastidio e disprezzo per la giornalista che ha osato ficcare il naso in una materia che non deve essere toccata dai non addetti ai lavori.

Questa allergia nei confronti dello scrutinio da parte della società è un atteggiamento tipico della comunità tecnologica italiana. Infatti, all'inchiesta del "The New York Times" dedicata alle condizioni di lavoro di Amazon è stata contestata in Italia con argomenti che poco avevano a che fare con il rispetto della dignità del lavoro.

Tuttavia, tutti gli attori sulla scena pubblica dovrebbero essere sottoposti ad una qualche forma di scrutinio, sia esso legale, tecnico o politico. Infatti, a questa necessità di scrutinio sulle attività delle software house che si occupano di sorveglianza di massa e cyberwarfare hanno (molto parzialmente) risposto le istituzioni internazionali estendendo ai software realizzati da Hacking Team all'interno dell'Accordo di Wassenaar, gettando nello sconforto la comunità hacker, ma chiarendo in termini giuridico internazionali che anche questi software sono armi a tutti gli effetti la cui compravendita deve essere regolata.

Le difficoltà oggettive del controllo e la posta in gioco

Ne abbiamo parlato all'inizio dell'articolo: il mondo digitale, oltre una certa soglia, è difficilissimo da

controllare. Eppure, il mondo digitale si sta configurando come l'unico terreno sul quale le grandi potenze possono scontrarsi davvero.

In fondo - è un leitmotiv abbastanza diffuso negli ultimi anni - i conflitti armati su vasta scala sono virtualmente impossibili per colpa della (o grazie alla) presenza, negli arsenali, di armi atomiche in grado di distruggere N volte la vita sulla terra. Non solo: combattere guerre è diventato molto costoso. Non è come nel '39 quando aerei molto belli, ma decisamente rudimentali, potevano essere costruiti in pochi giorni.

Oggi, lo scenario è molto diverso. Pilotare un moderno aereo da guerra richiede competenze incredibili, difficili da rimpiazzare in caso un pilota venga ucciso, e - soprattutto - il costo unitario per ogni macchina è dell'ordine delle decine di milioni di euro. Per esempio, un Eurofighter costa 69 milioni di euro, senza contare armamenti e carburante.

Davanti a queste cifre, è evidente come nessuno abbia voglia di combattere direttamente una guerra. Ecco che si cercano escamotage tecnologici: i droni, certo, ma anche il cyberwarfare. Sofisticato, costoso ma - per ora - abbastanza sicuro in termini di perdite di vite umane.

Eppure, quanto succede tra i server delle forze di sicurezza di mezzo mondo non è secondario, data la sensibilità delle informazioni che contengono e data la problematicità delle relazioni internazionali, in questa particolare contingenza storica.

Infatti, come vedremo, iniziative di cyberwarfare hanno provocato già oggi danni economicamente - e strategicamente - rilevanti che gli strateghi dei paesi occidentali non possono più fare a meno di considerare.

Cina, terrorismo e lupi solitari: che confusione

Per quanto contestato, strapagato e - probabilmente - obsoleto, negli anni in cui il ritardo del programma F-35 era quasi accettabile, una tegola incredibile si abbatté sul consorzio multinazionale che lo sostiene: la Cina, con un attacco mirato, ha rubato i segreti di software e struttura dell'aereo, costringendo la Lockheed Martin e la BAE Systems a riscrivere il software dell'aereo e riprogettare alcune altre sue parti.

L'hack è stato un gravissimo campanello d'allarme per le forze armate occidentali, se non altro perché ha evidenziato una grande vulnerabilità dei programmi occidentali nei confronti di forze organizzate. E' pur vero che mettere quelle informazioni all'interno di server che usano protocolli Internet non è stata una buona idea. Ma tant'è: i contribuenti di paesi che vanno dagli USA al Regno Unito all'Italia hanno pagato a caro prezzo l'imperizia dei propri fornitori.

Il risultato, oltre allo smacco subito, è stato che i programmi pensati da Pechino in risposta ai caccia di quinta generazione americani ha beneficiato della tecnologia che è stata rubata, azzerando il vantaggio strategico che avere quei sistemi d'arma avrebbe in caso di guerra obbligando USA e partner a inventarsi qualcos'altro per rimettere le cose, quantomeno, in pareggio.

Il dramma, però, è che a sfuggire al controllo sono anche le azioni di criminali e di singoli, in alcuni casi che - però - sono in grado di danneggiare moltissimo non solo i governi, ma anche i privati. E' vero che la fuga di contatti di Ashley Madison e della conseguente esposizione di nomi e cognomi di

persone che cercavano incontri extraconiugali è un atto più criminale che terroristico, mancando il fine politico. Eppure, si moltiplicano gli allarmi in questo senso.

In effetti, non è difficile ipotizzare che un gruppo terrorista abbia interesse a violare i server di qualche istituzione esponendone, per esempio, i dati, mettendo a rischio la vita di chi ci lavora. Già, ma con quali software, visto che quelli di Hacking Team non sono reperibili sul mercato legale?

In questo caso, viene in aiuto l'open source. GitHub è pieno di software di hacking. Esiste, persino, una distribuzione di Linux dedicata a questo. Certo, tra l'attività di hacking di basso livello e quella fatta dalle forze di sicurezza di stati sovrani c'è una differenza che non deve essere sottovalutata. Eppure, data l'architettura open di questi software, chi può, in sincerità, scommettere che non verranno modificati e migliorati per adattarli alle esigenze e alle necessità di gruppi terroristici?

La domanda non è peregrina ed è un altro fattore di cui prendere coscienza, se si vuole capire come verranno combattute le guerre di domani nel cyberspazio, dove, più che in un universo settecentesco fatto di eserciti professionali, viviamo in un Vietnam nel quale non si capisce un accidente, con il rischio che - a farne le spese - siano le libertà dei cittadini, grazie alle tecniche di sorveglianza di massa che, in teoria, dovrebbero limitare le attività terroristiche o di spionaggio da parte di potenze straniere.

Questo scenario molto complesso è scoraggiante. Le minacce sono talmente tante che non si può non fidarsi dei tecnici e dei militari. Tuttavia, Clausewitz non è cambiato, ed è ancora lì ad insegnarci che, venendo meno il fine politico del conflitto armato, si entra in una dinamica di "guerra assoluta", di scontro fine a se stesso che, però, a molti tecnici piace nella stessa misura in cui al Generale Cadorna piaceva mandare al macello i nostri soldati contro le mitragliatrici austroungariche.

Cosa fare per orientarsi in questo scenario: diritto ed etica

Come abbiamo lungamente messo in evidenza nei paragrafi precedenti, la guerra cibernetica pone sfide senza precedenti. Come sempre, quando la tecnologia trasforma uno scenario, non si sa bene quali pesci prendere. In effetti, il cyberwarfare è una cosa così invisibile e così sofisticata che aspettarsi - allo stato attuale - un efficace scrutinio politico da parte dei politici è un'ipotesi semplicemente peregrina. Eppure, però, è necessario che i politici rimettano a ficcare il naso in quello che accade nei data-center delle loro forze armate, cercando di capire se sia giusto o meno utilizzare quel tipo di armi.

Poniamo che, per esempio, un team di hacker cinesi dell'Unità 61398, trovi la sua strada attraverso i sistemi informatici di una centrale nucleare giapponese, provocando, deliberatamente una fusione del nocciolo. Come potrebbe, il governo giapponese, dimostrare davanti all'opinione pubblica che quanto successo è un'operazione di guerra? Non potrebbe e i cinesi avrebbero buon gioco a definire le ipotesi giapponesi una provocazione.

Il problema, ovviamente, è a monte. E, per quanto debole, il diritto internazionale può offrire e già offre delle soluzioni interessanti. In fondo, per quanto si continuano a usare - per esempio - le bombe a grappolo, queste sono state molto limitate, nel loro uso, negli ultimi 30 anni. E' vero che Israele le ha usate (almeno) nell'operazione "Piombo Fuso" in diretta tv colpendo anche civili. Ma comunque, per quanto esecrabile, è stato un utilizzo che ha trovato pochi altri riscontri, in giro per il mondo.

Lo stesso si può dire per le armi chimiche. Per quanto ISIS e il regime siriano di Al-Asad ne abbiano fatto un uso più o meno sistematico, si può sostenere che, ad oggi, è molto raro vedere l'utilizzo di gas tossici come armi. E questo è un indubbio successo della comunità internazionale, per non parlare di quanto accaduto con le mine antiuomo che, per quanto siano - ancora - diffusissime in giro per il mondo, non vengono più usate in modo così diffuso come quando accaduto, per esempio, nei Balcani.

Il successo più grande del controllo delle armi, a livello mondiale, però, probabilmente, è il Trattato di Non Proliferazione Nucleare che, per quanto non sia stato firmato da Paesi come India, Pakistan e Israele, ha permesso un'effettiva limitazione della proliferazione nucleare, con un gruppo molto ristretto di stati che le ha sviluppate e le ha messe nei propri arsenali.

A verificare il Trattato di Non Proliferazione Nucleare, c'è l'AIEA, l'Agenzia Internazionale per l'Energia Atomica che - per quanto sia un vaso di coccio in mezzo a tanti vasi di ferro - ha un ruolo di primo piano ogni volta che un paese minaccia di intraprendere un programma nucleare con fini bellici.

Visto il parziale successo di questa agenzia, potrebbe essere utile crearne una simile dedicata al cyberwarfare che cerchi di limitarlo, vigilando sulle attività di guerra cibernetica che si svolgono sulle infrastrutture digitali mondiali, inclusi satelliti e dorsali oceaniche. Evidentemente, esiste il rischio che questa agenzia si trasformi in un baluardo della sorveglianza di massa, ma un trattato ben bilanciato che la fondi non è un'utopia. Bisogna, però, che i governi riscoprano una cosa che, spesso, in guerra viene dimenticata, ovvero l'etica.

Per quanto la guerra e i conflitti armati siano esecrabili, i pianificatori politici devono chiedersi quando è giusto farvi ricorso e che cosa sia morale fare. Per questo, servono politici nazionali sensibili e consapevoli di quanto succeda loro intorno. E' - quindi - ovvio e necessario che le università, i partiti e le istituzioni dove i politici si formano comincino a porre seriamente il tema di come la tecnologia modifica - spesso irreversibilmente - la nostra società, non rifiutandone la complessità, ma accogliendola e dominandola.

E' una strada in salita e non è detto che, a settembre 2015, non sia già tardi per una svolta di questo tipo. Tuttavia, la posta in palio è troppo alta per ignorare questa sfida che è cruciale se vogliamo che la politica abbia un ruolo, in futuro.

Vuoi leggere l'anteprima del numero due di Pandora? Scarica il PDF

Vuoi aderire e abbonarti a Pandora? Le informazioni qui