« L’economia neoclassica? Una pseudoscienza

Cyber-war: il grande campo di battaglia digitale

di **GIAN PIERO SIROLI** [1]

Negli ultimi anni si sono spalancati gli scenari inquietanti della guerra condotta attraverso tecnologie digitali, nel silenzio quasi totale della stampa. La cyber-war è un dominio bellico che, a causa della sua nascita recente e dell’elevatissima velocità di evoluzione tecnologica, non ha permesso lo sviluppo di una benché minima forma di regolamentazione internazionale. Le armi cibernetiche, che il pubblico ancora conosce pochissimo ma che presto potrebbe subire, danno un’illusione di controllo e di efficienza, ma in realtà presentano notevoli vulnerabilità e sollevano interrogativi etici molto seri, che vanno dai danni collaterali non controllabili alla manipolazione psicologica dei contenuti dei social media e di internet.

Nell’estate del 2010 una notizia compare su alcune riviste e siti specializzati in sicurezza informatica, ma passa inosservata al grande pubblico: descrive un attacco attraverso una apparente vulnerabilità del sistema operativo Windows. A prima vista quasi marginale, solo lentamente e qualche tempo dopo, in seguito ad approfondite analisi di vari esperti e alla discussione pubblica nell’ambito di conferenze specialistiche se ne comprende l’importanza e il significato: si tratta in realtà di una vera e propria azione di sabotaggio dell’impianto nucleare di arricchimento di uranio di Natanz in Iran, compiuto attraverso l’uso di un *worm*, un segmento di codice in grado di riprodursi e propagarsi in rete in modo completamente autonomo e capace di produrre danni “fisici” reali manovrando e lanciando l’attacco dalla dimensione cosiddetta “virtuale” di computer e reti. Stuxnet, questo il nome con cui è ora noto il worm, può essere considerato la prima vera arma cibernetica pubblicamente riconosciuta.

Una nuova forma di arma dunque, ma come si presenta? Stuxnet[2] è un worm specializzato per l’attacco di sistemi di controllo industriale noti con il nome generico di SCADA (Supervisory Control And Data Acquisition) che l’impianto di Natanz utilizza per gestire le apparecchiature di arricchimento. Il worm, attraversando l’infrastruttura Windows nell’ambito del quale è eseguito il software di controllo della centrale, si è propagato fino a raggiungere due particolari e ben precisi microprocessori di basso livello (Programmable Logic Controllers, PLC) prodotti da Siemens, che controllano e regolano fisicamente gli apparati e i processi produttivi; per dare un’idea della complessità, si noti che i PLC sui quale il codice di attacco e’ installato e attivato utilizzano un sistema operativo differente da Windows. In questo modo, manipolando le modalità di funzionamento delle centrifughe di arricchimento di uranio fuori dalle specifiche previste dal costruttore, ne ha provocato il conseguente danneggiamento, mostrando però contemporaneamente al sistema di controllo un apparente corretto funzionamento dell’infrastruttura, allo scopo ai nascondere la sua presenza. Il risultato è stato un progressivo forte deterioramento della funzionalità dell’impianto e quindi della produzione di uranio arricchito. Si stima che in termini di danni

prodotti alla catena di arricchimento le conseguenze dell'attacco del worm siano state, anche se non equivalenti, comunque paragonabili a un attacco aereo convenzionale.
Il codice sorgente di Stuxnet è estremamente complesso, con caratteristiche che, per il periodo in cui fu scoperto, furono considerate quasi fantascientifiche[3], sia per gli svariati e sofisticati meccanismi di penetrazione, propagazione e occultamento in due differenti ambienti operativi, sia per i meccanismi di comunicazione e autoaggiornamento. La realizzazione di Stuxnet deve sicuramente essere fatta risalire a un numeroso gruppo di esperti in possesso di vaste e approfondite conoscenze informatiche, con risorse economiche e tecnologiche di prim'ordine a disposizione, e che abbia lavorato per un esteso periodo di tempo. Stuxnet è considerato il prodotto di uno o più stati-nazione, sia per la sofisticazione e complessità del progetto ed anche perché nel codice sorgente sono incluse informazioni sensibili probabilmente provenienti da ben informati servizi di intelligence, informazioni che il worm stesso non era in grado di acquisire autonomamente; si presume sia stata un'operazione congiunta USA-Israele[4].
In sostanza Stuxnet rappresenta un modello di worm distruttivo per sistemi SCADA, che potrebbe anche essere replicato, modificato e riutilizzato da parte di aggressori differenti per colpire bersagli diversi da quello originale, riutilizzazione forse già avvenuta; in questo senso si tratterebbe di una tecnologia di attacco forse facilmente proliferante.
E' importante sottolineare che i sistemi SCADA sono utilizzati per il controllo e la gestione di molte grandi infrastrutture civili, quali quelle dedicate alla produzione e distribuzione di energia elettrica, gas, acqua potabile e reflui, nelle industrie di trasporti, di raffinazione, tutti quei sistemi insomma dove un controllo centralizzato di un complesso sistema su scala geografica è fondamentale per la funzionalità globale e il cui malfunzionamento prolungato si traduce in una criticità a livello di sicurezza nazionale dal punto di vista economico, sociale o militare. E' quindi evidente la pericolosità della diffusione e dell'uso di un worm del genere per scopi bellici.
Se si eleva il punto di vista a un livello di astrazione maggiore, risulta evidente come le cosiddette "infrastrutture critiche informatizzate" del tipo di quelle appena citate, indispensabili per il normale funzionamento di una società civile sviluppata, negli ultimi decenni siano diventate sempre più dipendenti dalle tecnologie digitali di informazione e comunicazione, le quali purtroppo risultano intrinsecamente vulnerabili; queste vulnerabilità cibernetiche di computer e reti si sono quindi estese e proiettate sui sistemi infrastrutturali. Il mondo cyber insomma aumenta l'efficienza e le capacità di controllo di complicati processi distribuiti su scala geografica, ma contemporaneamente introduce delle inevitabili vulnerabilità che devono essere prese in considerazione.
In questa ottica, Stuxnet deve quindi essere considerato una cyber-arma a tutti gli effetti e, purtroppo dopo la sua scoperta, negli anni successivi al 2010 è stata individuata tutta una panoplia di armi cibernetiche[5] con meccanismi sempre più sofisticati e con varie funzioni: di ricerca di informazioni, intercettazione di comunicazioni su vasta scala, penetrazione di sistemi sensibili, sabotaggio di diverse infrastrutture. Difficile identificare con precisione gli autori di tutte queste armi cyber, ma si stima che alcune decine di paesi siano attivi ormai da anni nello sviluppo di queste tecnologie.
Non si deve dimenticare che le ICT (Information & Communication Technologies) rappresentano un tipico esempio di tecnologia a doppio uso, civile e militare; gli sviluppi iniziali degli attuali network di comunicazione digitale furono avviati negli anni '70 in ambito militare da DARPA (US Defense Advanced Research Projects Agency) e solamente dopo almeno 10 anni seguì l'evoluzione e il graduale passaggio verso il mondo civile e commerciale, di cui siamo testimoni oggi.
Ma Stuxnet e simili non sono che un elemento della cosiddetta cyber-war. Un aspetto complementare e altrettanto importante della guerra cibernetica è l'attuale tendenza all'estesa digitalizzazione del campo di battaglia, sempre più profondamente radicata nei sistemi e nell'equipaggiamento militare, allo scopo di migliorare l'efficienza operativa integrando piattaforme d'arma, reti di sensori, strutture di comando e intelligence. Tanto per fare un esempio concreto, si stima che per il caccia di ultima generazione F-35 siano state sviluppate circa 10 milioni di linee di codice[6] che gestiscono i vari sistemi di bordo, il controllo del volo, armamenti,

comunicazioni, supporto missione, ecc. E questo non è che un singolo sistema d'arma, per quanto particolarmente avanzato e complesso.
La gestione completa del campo di battaglia è sempre più "automatizzata". Forse si può addirittura parlare di un sistema *quasi-real-time* che acquisisce e coordina in modo continuo raccolta, instradamento ed elaborazione di informazioni e dati dai sensori di vario tipo (visuali, infrarossi, magnetici, di movimento ecc) verso gli "shooter" (elicotteri da attacco, bombardieri, caccia) per permettere ai differenti livelli di comando una approfondita consapevolezza situazionale in termini di sorveglianza, acquisizione e neutralizzazione dei bersagli. Con queste tecnologie l'intervallo di tempo dall'identificazione del bersaglio all'attacco si restringe sempre più. Per non parlare poi delle comunicazioni e del controllo remoto dei sistemi autonomi, sia aerei (UAV), che terrestri (UGV) e marini (UUV), che necessitano di una importante infrastruttura di trasmissione dati su scala globale, mantenuta funzionante in zone operative, cioè in condizioni belliche molto avverse. L'uso di questi sistemi si è enormemente espanso nel recente passato: lo dimostra il fatto che nel 2003 gli USA iniziarono le operazioni in Iraq con pochissimi droni (UAV), ma alla fine del 2008 il loro numero superava le 5000 unità; un importante incremento si è avuto anche per gli UGV, inesistenti all'inizio dell'invasione ma che in 5 anni hanno raggiunto i 12000 veicoli. Tra il 2008 e il 2013, il numero di piloti di droni nell'US Air Force è salito da circa 400 a oltre 1,300[7] e dal 2014 si stanno addestrando più piloti di UAV del totale di piloti di bombardieri e caccia. Mentre l'amministrazione G.W. Bush autorizzò circa 50 operazioni antiterrorismo con l'attacco di droni, l'amministrazione Obama ha superato quota 500.[8]
Il grado di autonomia dei sistemi d'arma è in continua estensione, fino a sistemi "fire and forget"[9] con capacità di decisione autonoma nell'acquisizione e neutralizzazione del bersaglio[10], direttamente paragonabili, in ambito informatico, al worm Stuxnet. Tra l'altro, questa evoluzione può porre problemi relativi alle regole di ingaggio (RoE, Rules of Engagement) adottate dai sistemi autonomi (cyber-RoE), in presenza o meno di un umano nel processo decisionale di fare fuoco ("man-out-of-the-loop"); probabilmente si passerà da uno o più piloti per drone, come allo stadio attuale, a un solo pilota che coordina una moltitudine di sistemi autonomi che cooperano tra loro, essendo l'umano eventualmente coadiuvato nelle decisioni da una rete in grado di acquisire dati e auto-apprendere. L'altra faccia della medaglia è che, naturalmente, anche questi sistemi non sono immuni da vulnerabilità intrinseche, potendo subire attacchi sia dallo spazio fisico che dalla dimensione cyber, in termini di disturbo delle comunicazioni o del canale criptato di guida, del segnale GPS di localizzazione, di corruzione dei dati di navigazione, o di iniezione di malware a tutti i livelli. L'uso esteso di questi sistemi d'arma impone quindi una cyber-difesa puntuale delle infrastrutture militari coinvolte. Tra l'altro, in caso di deterioramento e malfunzionamento di uno sciame di droni autonomi, per esempio, quale sarà la catena di responsabilità in caso di danni collaterali, specialmente su umani? Potrà essere compatibile con lo "Jus in Bello", l'insieme delle norme di diritto internazionale che limitano la condotta accettabile dei belligeranti durante una guerra? Si vuole definitivamente conferire a una macchina il potere autonomo di uccidere esseri umani? A questo livello si entra nella discussione di un grande tema etico.
E' evidente come in ambito militare comunque le armi basate sulle ICT costituiscono ormai una parte importante dell'arsenale di attacco e difesa di molte nazioni; in questo settore le attività spaziano dalla ricerca di vulnerabilità sfruttabili per gli attacchi, alla produzione e rivelazione automatica di cyber-armi, network intelligence per l'intercettazione di comunicazioni sensibili e protette, lo sviluppo di software per sistemi autonomi, la difesa dei sistemi SCADA ecc. Da circa una decina di anni a questa parte si possono elencare numerosi eventi[11] interpretabili come tipici esempi di guerra informatica: si va dall'attacco a infrastrutture civili o militari, alla penetrazione e manipolazione di sistemi di difesa aerea, all'intrusione in infrastrutture civili di telecomunicazione, all'intercettazione di video trasmessi da droni durante le operazioni, all'infiltrazione in reti sensibili della difesa di alcuni paesi, fino al sabotaggio di infrastrutture industriali; ciò evidenzia tra l'altro una sorta di accoppiamento, almeno entro certi limiti, tra infrastrutture civili e militari, che deve far riflettere. In certi casi si rischia una sorta di militarizzazione delle infrastrutture civili, sia per scopi

di difesa che per la semplice utilizzazione, rischiando gravi danni collaterali nel settore civile in caso di attacco.
Le problematiche di difesa militare si sovrappongono pesantemente alla dinamiche economiche nel settore civile privato. Non bisogna dimenticare inoltre che l'ampio spettro delle ICT riveste grande importanza anche come supporto alle operazioni militari convenzionali: le forze armate USA fanno affidamento su tecnologie informatiche a ogni livello, dalla logistica, al comando e controllo, posizionamento e guida dei sistemi d'arma[12]. Stuxnet è stato il primo raggio di luce a illuminare questo vasto ed oscuro mondo, ma quello che si intravvede e' solo la punta dell'iceberg.
Per affrontare questo dominio in modo coerente e integrato, gli USA nel 2014 hanno creato il Cyber Comando unificato (CYBERCOM), di fatto un riconoscimento formale della rilevanza militare dello spazio cibernetico. Si tratta del comando centralizzato delle operazioni svolte nello cyber-space dalle quattro forze armate USA, comando che coordina e conduce lo spettro completo delle operazioni militari in questo dominio e protegge contemporaneamente le reti della difesa USA. Dal 2010 la NATO organizza periodiche esercitazioni di guerra digitale, "Locked Shields"[13], con team di reazione rapida in tempo reale di difesa di reti e sistemi (inclusi SCADA).
Ci si può fare una idea, seppur vaga, della proliferazione e penetrazione delle infrastrutture militari nelle reti mondiali anche civili, attraverso l'affaire *NSA-leaks*: alla fine del 2013 *Der Spiegel*[14] esce con una serie di articoli basati sulle rivelazioni di E. Snowden, ex collaboratore della National Security Agency USA, che descrivono un vastissimo sistema di sorveglianza globale con estese capacità di intercettazione (di servers, desktop, computer portatili, dispositivi di rete, firewalls, telefoni fissi e mobili, sistemi SCADA ecc) messo in opera da una speciale unità dell'NSA e associato a un vero e proprio arsenale software di sofisticate tecniche di penetrazione a tutti i livelli[15]. Naturalmente gli USA non sono l'unico paese con attività del genere: ad esempio anche l'agenzia di intelligence britannica (GCHQ) ha sviluppato strumenti simili, anzi alcuni di questi hanno come bersagli i "contenuti" veicolati dalla rete, e non solo le infrastrutture tecnologiche. In UK è stato infatti finanziato un importante programma di ricerche per analizzare il futuro della cyber-war, incluse tecnologie emergenti relative a social media e tecniche psicologiche, con intercettazione bidirezionale di messaggistica in tempo reale, la modifica dei risultati di sondaggi online in rete o l'amplificazione di selezionati messaggi, normalmente video, su popolari siti web. Il risultato di tale attività, in gergo Operazioni Psicologiche (PSYOPS), è la manipolazione mediatica a livello sociale della percezione degli utenti della rete. Questo contesto è denominato "Information Warfare", in alternativa (e in parte sovrapposizione) a "Cyber Warfare", quest'ultimo riferendosi a una visione più limitata al lato tecnologico. Esempi concreti di azioni tipiche di Information Warfare sono il supporto a gruppi dissidenti di determinati paesi, l'uso e la manipolazione di media di massa e social media in rete (tra cui Wikileaks e NSALeaks), azioni di informazione e disinformazione nonché campagne di reclutamento. E' interessante notare come molte operazioni di Information Warfare hanno luogo in una fase non bellica o pre-bellica.
Ma ritorniamo alla guerra informatica in senso più stretto e cerchiamo di descriverne alcune delle caratteristiche intrinseche, ricordando però che su molti di questi temi è aperta un'attiva discussione internazionale. Va innanzi tutto rilevato che il dominio cyber, dal punto di vista bellico, è considerato un dominio autonomo, in confronto ai domini bellici operativi tradizionali di terra, mare, aria e spazio; inoltre questi tradizionali domini bellici sono essi stessi in fase di digitalizzazione più o meno avanzata. La prima delle caratteristiche intrinseche della "dimensione" cyber, che differisce da tutti gli altri "spazi" bellici, è che si tratta di una dimensione artificiale, creata dall'uomo, la cui stessa "topologia" (cioè la geografia dello spazio cibernetico) è altamente volatile, tanto che regioni intere dello spazio cyber possono apparire o scomparire a comando, o sotto attacco (fisico o digitale). In altre parole, le operazioni belliche modificano la topologia stessa dello spazio in cui vengono condotte.
Le armi cyber possiedono un altissimo grado di mobilità e velocità di propagazione in rete, oltre a una formidabile capacità di fuoco (cioè di attacco digitale), un elevatissimo grado di automazione sia dell'arma stessa che dei sistemi di comando e controllo. E' opinione diffusa che questo nuovo

dominio artificiale sia intrinsecamente orientato all'offesa, favorisce cioè l'attacco preventivo sulla difesa, quindi destabilizzante dal punto di vista strategico.
Il cyber-dominio è inoltre profondamente asimmetrico, sia in termini degli attori in gioco (statali o non statali, mercenari, con maggiori o minori risorse), ma anche in termini di dipendenza e vulnerabilità infrastrutturale, nonché dei relativi costi di protezione. Diversamente dai domini bellici convenzionali, il problema dell'attribuzione di un attacco cibernetico può essere tecnicamente molto complicato o giungere con forte ritardo sull'evento, in modo da essere strategicamente quasi inutilizzabile.
Un quesito importante a cui dare risposta è il seguente: quando un attacco cibernetico può essere definito "atto di guerra"? In termini di diritto alla difesa (*jus ad bellum*) l'argomento può essere importante. Altre domande meritano un'analisi: per quali scopi la cyber-war può essere considerata più efficace? Per operazioni di intelligence, sabotaggio, attacchi di tipo guerriglia limitati in tempo e spazio, oppure su infrastrutture globali? Lo sviluppo di questo dominio porterà vantaggi a breve o lungo termine, aumentando o riducendo la stabilità globale? Potrà essere un'occasione per alcuni paesi, più o meno tecnologicamente avanzati, per riposizionarsi militarmente a livello internazionale sfruttando le caratteristiche di asimmetria? Queste e molte altre domande sono attualmente in discussione nel contesto internazionale e le risposte sono tutt'altro che definite.
Quello cyber è un dominio bellico che, proprio a causa della sua nascita recente e dell'elevatissima velocità di evoluzione tecnologica, non ha permesso lo sviluppo di una qualche forma di regolamentazione internazionale, a differenza degli altri domini bellici, sempre ammesso che ciò sia possibile nel contesto specifico in discussione.
Non ci sono dubbi che tutti i futuri conflitti armati avranno una dimensione cibernetica di livello variabile, attualmente difficile da valutare nella sua interezza e complessità, ma per i quali molti paesi si stanno attrezzando[16]. La guerra condotta nel cyber-space è un dominio vasto e interdisciplinare, e certamente gli aspetti tecnici non sono che una parte limitata della visione complessiva, che dovrà includere una visione socio-politica e anche economica, a livello internazionale, e che probabilmente richiederà lo sviluppo di nuovi approcci e una nuova appropriata terminologia per affrontare l'argomento.
Il mondo digitale ormai è qui con noi e ci resterà a lungo, nel bene e nel male, è quindi importante promuovere una attenta riflessione sul ruolo e i rischi di queste nuove tecnologie. C'è una responsabilità nei confronti della società che tecnici e scienziati in particolare, ma non solo loro, anche militari e decisori politici, devono assumere per promuovere uno sviluppo coerente ai principi di stabilità e di sicurezza globale, nonché di stabilite convenzioni internazionali che regolano il comportamento durante i conflitti. E sarà importante ricordare queste parole di Albert Einstein: "Non possiamo risolvere i problemi usando lo stesso modo di pensare che abbiamo usato per crearli".

NOTE

[1] Ricercatore al Dipartimento di Fisica e Astronomia, Università' di Bologna, INFN e CERN. Ha insegnato Tecnologie dell'informazione e sicurezza internazionale presso l'Università di Pisa fin dal 1999 e Computer and network security all'Università di Bologna. Ha partecipato e contribuito a vari meeting sull'argomento presso la sede ONU di Ginevra, scrive articoli e tiene regolarmente conferenze su cyber-war. Partecipa all'attività del Movimento Pugwash (insignito del premio Nobel per la pace nel 1995) ed è co-coordinatore del Gruppo di Lavoro su "Disarmament, conflict resolution, and new weapons technology". Nel 2016 ha tenuto due lezioni al CERN su cyber-weapons https://indico.cern.ch/event/438525/] e cyber-war http://indico.cern.ch/event/438526/].

[2] Per un report tecnico dettagliato si veda "W32.Stuxnet Dossier" N.Falliere, L.O Murchu, E.Chienhttp://www.symantec.com/content/en/us/en...

[3] Il worm contiene ben quattro vulnerabilità del tipo "0-day" (al tempo sconosciute e quindi sfruttabili in tutti i sistemi), si auto-aggiorna attraverso meccanismi peer-to-peer, utilizza rootkit per nascondere la propria presenza a livello di Windows ma anche di PLC (una tecnica mai osservata

prima nell'ecosistema cibernetico), usa certificati digitali trafugati per impedire la rivelazione da parte dei sistemi di difesa, e contiene sofisticate tecniche contro il reverse-engineering.

[4] "Obama Order Sped Up Wave of Cyberattacks Against Iran", New York Times 2012, http://www.nytimes.com/2012/06/01/world/...

[5] Per i lettori interessati a cercare ulteriori informazioni, citiamo alcuni nomi: Duqu, Flame, Gauss, Shamoon, Red October.

[6] "F-35 Joint Strike Fighter benefits from modern software testing, quality assurance", Military Aerospace 2013, http://www.militaryaerospace.com/article...

[7] "Wired for War? Robots and Military Doctrine" P.W. Singer, JFQ, 2009, http://intelros.ru/pdf/jfq_52/21.pdf

[8] "Obama's Embrace of Drone Strikes Will Be a Lasting Legacy", New York Times, 2016, http://www.nytimes.com/roomfordebate/201...

[9] In gergo militare si definisce così un'arma che una volta lanciata ricerca e acquisisce il bersaglio in modo completamente autonomo, senza guida esterna dopo il rilascio.

[10] Al contrario del UAV Predator, pilotato attraverso un link satellitare, il Global Hawk opera virtualmente in modo completamente autonomo, esclusi decollo e atterraggio, navigando via GPS e trasferendo informazioni alla base con collegamento diretto e continuo.

[11] Per una lista puramente indicative si veda http://www.infoplease.com/world/events/c...

[12] Su dipendenza e vulnerabilità si veda "Cyber Warfare: Just How Vulnerable is the U.S. Military?", Real Clear Defense 2016 http://www.realcleardefense.com/articles...

[13] Locked Shields 2016, https://ccdcoe.org/locked-shields-2016.h...

[14] "Inside TAO: Documents Reveal Top NSA Hacking Unit", Der Spiegel 2013, http://www.spiegel.de/international/worl...

[15] Si stima che il tempo medio che intercorre tra l'infiltrazione informatica in un sistema e la scoperta dell'attacco perpetrato, vari da tre a otto mesi, a seconda della sofisticazione dell'attacco. Gli strumenti di NSA sono rimasti nascosti per anni, non rivelati dai sistemi di difesa, prima dell'annuncio pubblico.

[16] Si veda "The DoD Cyber Strategy", US DoD 2015, http://www.defense.gov/Portals/1/feature...

(28 giugno 2016)

Tag:cyber-war, droni, guerra informatica, Information Warfare, Stuxnet