Spazio cibernetico: *atout* e vulnerabilità di una nuova dimensione strategica

FRANCESCO PALMAS

Nel marzo nero del 1998, le reti informatiche della Nasa, del Pentagono e di altre agenzie governative, università e centri di ricerca persero negli Usa migliaia di dati sensibili. L'operazione *moonlight maze* fruttò ai russi informazioni riservate su contratti, ricerche scientifiche, tecniche crittografiche e sistemi di pianificazione bellica.

A Mosca vi è un'antica tradizione di guerra digitale: la dottrina militare sovietica includeva già, *illo tempore*, il concetto di ordigno informativo globale, funzione di sistemi avanzati di comando e controllo (C^2), guerra psicologica ed elettronica. I russi considerano molto seriamente la faccenda. Nell'agosto 2008, hanno bombardato la Georgia non solo fisicamente. Rostelecom e Comstar, aziende di telecomunicazioni partecipate dal governo, hanno messo a disposizione il loro *know-how*: il primo a farne le spese è stato il sito della presidenza georgiana, che mostrava un Saakashvili in compagnia di Hitler. L'intento era diversivo; il vero attacco avrebbe di lì a poco paralizzato il traffico dati dei principali dicasteri: dalla Difesa alle Finanze, dagl'Interni agli Esteri, dalla Banca centrale al Consiglio dei Ministri, passando attraverso l'inconsapevole infrastruttura informatica turca. Chi avesse tentato di collegarsi al sito del governo abkhazo in esilio non sarebbe stato più fortunato. Nell'urgenza, il ministero degli Esteri georgiano è stato costretto a ricorrere a un *blog* di una delle piattaforme specializzate di Google. Mentre la presidenza polacca ha offerto ai vertici georgiani il proprio portale, gli analisti del Pentagono si sono affrettati a ridimensionare la portata dell'attacco russo: dal punto di vista militare, i vantaggi sarebbero stati nulli, vista la scarsa informatizzazione georgiana. Tbilisi si è dimostrata tutt'altro che sprovveduta: la sua risposta ha danneggiato i servizi tecnici dell'agenzia di stampa Ria Novosti, inaccessibile per via telematica. Non diversamente è andata a Russia Today: il sito del canale televisivo ha vacillato per oltre mezz'ora, bersagliato da pirati informatici georgiani. Invero la controffensiva di Tbilisi è parsa isolata e mal coordinata, assai meno efficace di quella russa. Lituani ed estoni ne sanno qualcosa. Nel luglio scorso, 300 siti *web* lituani son stati improvvisa-

mente ornati con effigi sovietiche e impossibilitati ad erogare servizi in linea. Poco tempo prima (aprile 2007), gli *hacker* russi avevano puntato i loro strali contro i siti istituzionali estoni, bloccando i contatti *on-line* con oltre duemila interrogazioni al secondo: un attacco in perfetto stile Ddos (*Distributed denial of service*). Muovendo da una serie di computer non presidiati (*zombie*), i *cyber*-guerrieri hanno sferrato un'offensiva coordinata e d'ampio spettro: l'eccesso di traffico dati (*overload*) ha mandato in *tilt* il sistema informatico dell'Hansabank, principale *network* bancario del paese, imponendo l'interruzione dei servizi telematici. Alla Seb Eesti Uhispank, seconda banca estone, non è rimasto che bloccare tutti gli accessi dall'estero. Ondate successive hanno preso di mira *asset* digitali di aziende ed enti pubblici. Il sistema amministrativo si è scoperto tutto ad un tratto vulnerabile: più dell'80% delle dichiarazioni fiscali è fatto in Estonia via internet e del voto elettronico ci si è serviti ampiamente nelle ultime elezioni parlamentari. Internet senza fili è una realtà ovunque, accessibile gratuitamente perfino sugli autobus che scendono lungo il Baltico.

Richiesta dal presidente estone, Toomas Hendrik, la Nato ha inviato un esperto ed incaricato il *Computer incident response capability* di sorvegliare l'evolversi degli attacchi. Il tracciamento del picco di *overload* ha lasciato pochi dubbi: interi gruppi di indirizzi Ip (*netblocks*) additavano la Russia come matrice geografica dell'offensiva. Ma il Cremlino ha subito respinto le accuse, denunciando un complotto e l'uso illegittimo delle coordinate telematiche di organismi istituzionali russi (*spoofing*)[1]. L'ipotesi, almeno teoricamente, non è inverosimile: nel febbraio 1998, il dipartimento della Difesa, a Washington, rilevò una serie d'intrusioni informatiche ostili. In quel periodo, la tensione internazionale con l'Iraq era nuovamente crescente e si temeva che gli attacchi fossero diretti a sottrarre informazioni sui piani d'azione del Pentagono e a minarne i sistemi logistici e di C[2]. Si dette quasi per scontato che a coordinare l'offensiva telematica[2] fosse Baghdad, attraverso suoi agenti ad Abu Dhabi. Rintracciati gli indirizzi fisici da cui muovevano gli attacchi, ufficiali dell'*intelligence* a stelle e strisce fecero irruzione nello stabile sospetto. Ma non trovarono che *server*. Gli *hacker* avevano seminato un falso indizio, comodamente seduti in California[3]. Non erano iracheni, ma semplici adolescenti americani, arrestati poco tempo dopo…

---

[1] Umberto Rapetto, *Superpotenze alla cyberwar*, in «Nova24», supplemento al «Sole24Ore», 4 ottobre 2007, p. 5. Nel gennaio 2008, è stato arrestato Dmitri Galushkevich, studente estone di origini russe, accusato e condannato con sanzione di 1.100 euro per la partecipazione agli attacchi.

[2] Ribattezzata «*solar sunrise*».

[3] James Adams, *Virtual Defense*, in «Foreign Affairs», 2001, n. 3, p. 109.

Incognite e modalità d'attacco

In genere, chi sferra un attacco Ddos necessita di una copiosa rete di computer per paralizzare l'obiettivo[4]. Siti, *host* e computer vulnerabili nella rete sono le prime vittime: gli *hacker* vi installano programmi *ad hoc*, ne annichiliscono l'autonomia (*zombie*) e li cooptano fra le loro fila. In un attacco *standard*, l'impulso iniziale parte dalla postazione elettronica di comando, arriva ad un *master-zombie* e si propaga alla pletora di *slave-zombie* da esso dipendenti. È l'*incipit* dell'offensiva Ddos, che in breve tempo porta al collasso dell''interrogato'. Una variante più dirompente si ha con i *Distributed reflector* dos, attacchi in cui oltre a 'padroni' e 'schiavi' figurano anche 'riflettori', in qualità di moltiplicatori di potenza. Rispetto all'*iter standard*, gli *slave* hanno in questo caso un compito aggiuntivo: ritrasmettere l'indirizzo-bersaglio ai sistemi in rete, per invitarli all'assalto virtuale ed amplificarne la portata.

Sebbene molti individuino in Russia il paradiso della criminalità informatica, sono invece gli Stati Uniti, Israele e la Cina a primeggiare nel settore[5], seguiti dal Brasile e dai paesi ex-sovietici. Negli anni Novanta, Hu Xiuzhi, direttore della fabbrica militare 7425 di Nanchino, preconizzò che la seconda rivoluzione dell'informazione avrebbe talmente influenzato lo sviluppo della difesa nazionale da sovvertire *modus operandi* ed organizzazione delle forze armate. Un crollo di borsa ben pianificato ed un attacco con virus informatici avrebbero causato non solo incertezze nei tassi di cambio, ma funto da vera e propria arma, come la diffusione su internet di falsità sui *leaders* politici avversari. A Xiuzhi fece eco il maggior generale Dai Qingmin, numero uno della cellula di *Cyber-war* (guerra cibernetica[6]) ed *Info-ops* (operazioni sulle informazioni) dell'Esercito popolare di liberazione (Pla). Tracciando le linee guida del combattimento futuro, il generale indicò nell'attacco ai sistemi cognitivi e di verifica nemici l'*atout* per disarticolarne i comandi. Colpire le reti informatiche avrebbe minato la fiducia dell'avversario, leva decisiva in qualsiasi battaglia. Nelle esercitazioni di Datong, Xian, Xiamen e Shangai, le divisioni di guerra informatica (*Iw Fenduis*) misero in pratica i precetti di Qingmin: spe-

[4] Byard Q. Clemmons, Gary D. Brown, *Targets in Cyberspace, Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction*, in «Military Review», 1999, n. 5, p. 37.

[5] Vi operano *hacker* ufficiali o meno, che gli americani hanno presto etichettato come *Honker Union of China*, *Hacker Union of China* e *China Eagle Union*.

[6] Il termine non è affatto nuovo. Il suo etimo è nella radice greca *kybernan*: dirigere, governare.

rimentarono azioni dimostrative, si ingegnarono a sviluppare e occultare potenti armi di *information warfare*, ad applicare schemi d'inganno e a sfruttare ogni possibilità di sorpresa generata da soluzioni e vulnerabilità tecnologiche. Tattiche non molto diverse da quelle in uso nei principali eserciti occidentali, cui plauderebbe anche il profeta della guerra di movimento, Sun Tzu, se vivente a cavallo tra il XX° ed il XXI° secolo.

Nella primavera 2007, i cinesi hanno dato prova delle loro capacità offensive, incuneandosi negli archivi riservati e nelle comunicazioni governative statunitensi. Sebbene Pechino abbia negato ogni responsabilità, non è stato complicato individuare nelle caserme del Pla le postazioni informatiche dei cecchini digitali[7]. L'incursione avrebbe puntato secondo alcuni a favorire misure draconiane: spingere Washington ad interdire agli utenti cinesi l'accesso ai siti *web* statunitensi. Un tentativo di censura dissimulata, per colpire chi cerca oltremare quella libertà d'opinione inesistente in patria.

Vulnerabilità ed armi digitali

Col diffondersi delle connessioni ad alta velocità e senza fili, più permeabili delle tradizionali, la minaccia Ddos è cresciuta esponenzialmente: arginarla sarà la vera sfida per le architetture che gestiscono e controllano le infrastrutture critiche. Sanità, economia, energia, trasporti, telecomunicazioni, ordine pubblico, difesa e così via hanno infrastrutture di telecomunicazione sempre più interdipendenti, vitali per il funzionamento e la sicurezza di un paese (Cii - *Critical information infrastructures*). Dieci anni fa il loro ordito era ancora segmentato: ciascuna funzionava autonomamente, all'interno di una struttura verticalmente integrata. Oggi le Cii tendono invece a condividere lo spazio cibernetico. Protocolli internet *standard* (Tcp/Ip) presiedono spesso ai processi di controllo strategico[8], un tempo governati da architetture e reti strettamente private[9]. È facile che un guasto ad un nodo finisca col ripercuotersi sugli altri e sia avvertito perfino da utenti remoti.

[7] Già nel 2005, l'operazione *titan rain* aveva permesso ad *hacker* cinesi di penetrare nei sistemi informatici della Nasa, del gigante industriale Lockheed Martin e dei Sandia National Laboratories (Doe), responsabili fra l'altro dei programmi di armi nucleari.

[8] Si tratta delle applicazioni Scada (*Supervisory control and data acquisition*).

[9] Un'inversione di tendenza è rappresentata da Terna che ha affidato ad un modello di 'rete privata' la trasmissione dei dati di controllo sull'esercizio ed il monitoraggio della rete elettrica.

Esistono ovviamente reti quasi impermeabili alle intrusioni esterne. Il *Global command and control system*, elemento fondamentale dell'infrastruttura informatica del Pentagono, dispone di una rete internet privata (Siprnet), come Govnet che trasmette voce e dati prescindendo dalle reti commerciali e pubbliche[10]. Ma non sempre è possibile esulare dall'esterno: per scambiare informazioni e svolgere operazioni commerciali e finanziarie, le Cii devono per forza interconnettersi[11]. Non solo: sarebbe del tutto fantasmagorico un sistema completamente esente da rischio, sia perché procedure troppo restrittive lo renderebbero di difficile utilizzo, sia perché non è possibile prevedere la versatilità degli attacchi esterni ed interni.

Un tempo, a garantire la sicurezza delle informazioni provvedeva l'impenetrabilità dei sistemi: le linee telegrafiche originarie erano state concepite per il solo traffico governativo e militare. Oggi invece degli stessi apparati si servono spesso sia militari che civili o, ancor peggio, a farla da padrone sono le tecnologie commerciali, meno assoggettabili di altre a vincoli e restrizioni all'*export*[12]. In ambito strettamente militare, le medesime informazioni circolano non solo tra i vertici della catena di C^2, ma anche tra le singole piattaforme ed unità combattenti, e vi si può attingere tanto da postazioni convenzionali, quanto da località geograficamente remote[13].

I rischi maggiori per la sicurezza di un sistema discendono proprio dall'ampiezza e dai punti d'accesso e di concentrazione delle sue reti. Milioni di nuovi punti d'ingresso si aggiungono ogni anno, aumentando i rischi di fughe di notizie, di contromisure e di penetrazione da parte del nemico, preludio al fallimento di qualsivoglia operazione.

Negli Usa si parla oggi di ammodernare il sistema di controllo del traffico aereo scommettendo unicamente sul Gps (2010), vulnerabile al disturbo elettromagnetico (*jamming*) ed alla diffusione di coordinate spurie (*spoofing*). La nuova architettura si fonda su sistemi aperti, reti di comunicazione condivise, prodotti *hardware* e *software* commerciali. Il nuovo sistema sarà così meno affidabile del vecchio, somma di più sottosistemi e di reti dedicate difficilmente violabili.

[10] Non diversamente avviene per le italiane Marintranet e Difenet, la cui segretezza è inderogabile.

[11] LUISA FRANCHINA, *Sicurezza delle reti e dell'informazione. La protezione delle infrastrutture critiche informatizzate*, Istituto alti studi per la difesa, 57ª sessione.

[12] Il *Wassenaar Agreement* limita ad esempio l'*export* di *software* crittografici verso alcuni paesi.

[13] Acronimo di comando, controllo, comunicazioni, computer e *intelligence*.

Minacce alle infrastrutture critiche

Le organizzazioni di sicurezza informatica hanno già lanciato l'allarme: nel prossimo quindicennio, verrà dal terrorismo cibernetico la minaccia principe alla sicurezza occidentale. L'intervallo tra la scoperta di una vulnerabilità sistemica ed un attacco *ad hoc* sta progressivamente riducendosi: nel 64% dei casi, non supera i 12 mesi, e gli *hacker* sono sempre più abili nell'individuare le falle prima che ne sia data comunicazione. Per alcuni analisti, tra virus elettronici ed armi di distruzione di massa (Wmd) non vi sarebbe poi tanta differenza. Difficile contraddirli se si pensi alle conseguenze di un attacco contro il sistema informatico di un grande ospedale, di una centrale nucleare o di un aeroporto. Alterare i *software* di gestione delle linee telefoniche causerebbe danni economici e vittime. Il sistema di segnalazione 7 che sovrintende al traffico telefonico è diffusissimo a livello internazionale. Alle reti che se ne servano basta un pacchetto Ip standard per comunicare fra loro. Le chiamate possono saltare da una rete all'altra grazie all'interconnessione digitale, esponendosi contemporaneamente alle intrusioni informatiche note. Nel 1990, un semplice errore di programma paralizzò per diverse ore il traffico telefonico statunitense. Le ripercussioni si avvertirono in tutti i settori, con perdite per centinaia di milioni di dollari. Alcune persone in difficoltà spirarono per l'impossibilità di comunicare e chiedere soccorso.

Non basta: interrompendo la produzione e la distribuzione di energia elettrica, un attacco digitale avrebbe un effetto domino sui servizi sanitari, emergenziali, comunicativi e gestionali. Dopo la prima guerra del Golfo, i danni alle centrali elettriche irachene causarono almeno settantamila decessi. Sebbene il potenziale elettrico fosse stato allora intaccato da bombardamenti convenzionali, non vi è dubbio che colpire il sistema di gestione informatica delle centrali produrrebbe effetti analoghi: in Iraq, gli ospedali non poterono garantire la continuità delle prestazioni e vi furono problemi sia nella distribuzione che nel trasporto dei farmaci. L'acqua potabile ed irrigua cominciò a scarseggiare.

L'idea di annichilire il sistema elettrico nemico non è affatto nuova: basti pensare alla missione inglese del dirigibile tedesco Zeppelin, durante la prima guerra mondiale. Il vettore cibernetico esalta semmai la possibilità di praticare su vasta scala la teoria[14]. Non stupisca pertanto che Russia e Stati Uniti assimilino ormai gli attacchi cibernetici pletorici alle Wmd e ventilino ogni tanto l'ipotesi di un accordo globale di deterrenza.

[14] Clemmons, Brown, *op. cit.*, p. 43.

Sebbene sia arduo ipotizzare attacchi devastanti a breve termine, le intrusioni illecite in computer e reti stanno aumentando al ritmo annuo del 56%[15]. Vulnerabilità sistemiche emergono di continuo, individuate dal monitoraggio *ad hoc* svolto dalle aziende di *software* e di sicurezza informatica, da ricercatori individuali e purtroppo, assai spesso, da pirati ed organizzazioni criminali.

Worms, virus, cavalli di troia, *logic bombs*, porte-trabocchetto, *spyware*, attacchi Dos, codici o sistemi d'inganno (*malware*), impulsi elettromagnetici[16] ed altri rappresentano armi con cui Stati deboli, non-Stati e perfino attori individuali possono sfidare le potenze militari convenzionali in un teatro digitale a loro congeniale, per colpirne soprattutto la stabilità economica. Senza andare troppo lontano, la guerra cibernetica palestinese è costata alle aziende israeliane un calo dell'8% nel volume delle esportazioni (2001)[17].

Segnali allarmanti giungono anche dai reati di *competitive intelligence* e di spionaggio industriale, subdoli ed in aumento vertiginoso: al centro della scena sono i dati aziendali sensibili, vieppiù nerbo della potenza nazionale[18]. Il sistema di spionaggio elettronico Echelon, prima di degenerare in un apparato Sigint[19] *tout court*, serviva per monitorare i mercati internazionali, anticiparne le mosse e garantirsi manovre finanziarie di successo[20]. Su questo fronte combattono una guerra economica, industriale e strategica anche i sistemisti statunitensi ed europei del comparto bellico. Nel luglio 2003, alcune squadre di ingegneri francesi lamentarono il furto di quattordici computer

[15] Vi sono innumerevoli livelli di guerra cibernetica, tre dei quali indicati come principali: il primo è semplice complemento di un'operazione militare, il secondo si manifesta in *cyber*-attacchi limitati ed il terzo in un'offensiva totale.

[16] Possono essere emessi da 'cannoni' a radiofrequenza o da 'bombe' *ad hoc*, facili da realizzare, economici e pericolosissimi per le memorie dei calcolatori. Vedi Umberto Rapetto, Roberto di Nunzio, *Le nuove guerre. Dalla Cyberwar ai Black Block, dal sabotaggio mediatico a Bin Laden*, Milano, BUR, 2001, p. 97.

[17] Israele è uno dei paesi più informatizzati al mondo con oltre 1 milione di collegamenti internet. Vedi Giles Trendle, *Cyberwar*, in «The World Today», 2002, n. 4, p. 8.

[18] Nella prima metà del 2002, nel solo campo economico-aziendale, si sono registrati più di centottantamila attacchi informatici. L'incremento annuo è dell'ordine del 60%.

[19] La *Signal intelligence* (ricerca informativa elettromagnetica) punta a decifrare le intenzioni operative dell'avversario, intercettandone comunicazioni e collegamenti radio.

[20] Echelon riesce ad intercettare fino a 3 milioni di messaggi al minuto. Ne fruiscono Usa, Canada, Regno Unito, Australia e Nuova Zelanda. L'omologo russo del delatore anglosassone è il Sorm, quello cinese Asiasat-2 e quello europeo Enfopol.

portatili. Guarda caso erano impegnate nei lavori dell'A400M, futuro aereo europeo per il trasporto tattico (Airbus)[21]. Nicolas Sarkozy, allora ministro degli Interni, non sorvolò sulla gravità del fatto. Sebbene non conseguisse prove formali, l'indagine aperta indusse gli esperti dell'*intelligence* economica ad accusare i rivali statunitensi di Airbus: Lockheed Martin e Boeing, produttori del C-130 e del C-17.

Molti virus informatici fungono oggi da semplice arma ricattatoria: non cancellano più le informazioni del disco di turno, ma si limitano ad ingabbiarle con lucchetti crittografici, le cui chiavi sono cedute solo dietro pecunia. Ne sanno qualcosa i responsabili della sicurezza virtuale. Tom Donahue, esperto della Cia, ha indicato nelle centrali elettriche le vittime finora predilette. In un caso almeno, l'aggressione informatica ha messo fuori uso i generatori e provocato *blackout* totali in numerose città. Donahue non ha precisato né dove, né chi vi fosse dietro, ma soltanto ribadito l'obiettivo dell'attacco: taglieggiare i titolari del servizio di pubblica utilità[22].

Cyberterrorismo

Le reti sono un moltiplicatore di potenza senza uguali per le organizzazioni criminali transnazionali: non solo permettono loro di ampliare dimensione, obiettivi e potere, ma anche di far proseliti, coordinare cellule, comunicare e trasmettere messaggi codificati ovunque, senza quartier generali vulnerabili[23]. Attivisti ed estremisti se ne servono per drenare aiuti: *al-Qaeda* ha una rete globale di finanziamenti, fondata su una pletora di istituzioni benefiche, organizzazioni non governative e finanziarie aduse all'impiego di internet. Sue cellule dispongono di *database* sugli obiettivi da colpire; applicativi *ad hoc* permettono loro di studiare le vulnerabilità delle infrastrutture critiche e simulare l'effetto domino di un determinato attacco[24]. Almeno

[21] Ali Laïdi, *Espionnage économique, arme cachée des grandes puissances*, in «Le monde diplomatique», marzo 2005, http://www.monde-diplomatique.fr/2005/03/LAIDI/12010.

[22] Umberto Rapetto, *Il cyber-racket fa le cose in grande*, in «Nova24», supplemento al «Sole24Ore», 24 gennaio 2008, p. 2.

[23] Steve Coll, Susan B. Glasser, *Terrorists Turn to the Web as Base of Operations*, in «The Washington Post», 7 agosto 2005, edizione *on-line*, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html.

[24] Magnus Ranstorp, "The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation", in Johan Eriksson, Giampiero Giacomello (a cura di), *International Relations and Security in the Digital Age*, London, Routledge, 2007, pp. 17-18, capitolo scaricabile dal sito http://www.fhs.se/upload/Utbildning/Dokument/Publikationer/ISS/Virtual%20Al%20Qaeda%20-%20Ranstorp.pdf.

trentamila siti *web* offrono, talvolta gratuitamente, veri e propri pacchetti per l'attacco informatico[25].

La copertura mediatica che l'Occidente riserva alle offensive elettroniche è oro colato per la strategia propagandistica dei *cyber*-terroristi. Molti gruppi hanno già cooptato tra le loro fila giovani tecnici esperti d'informatica. I *bit* di cui sono armati si servono di vettori assai semplici, economici e disponibili: linee telefoniche e connessioni senza fili, capaci di attentare alla sicurezza nazionale tanto quanto *modi operandi* più rischiosi e costosi.

I pirati cibernetici non hanno confini fisici da oltrepassare, ma solo l'imbarazzo della scelta nelle modalità e negli obiettivi da colpire: possono optare per un accesso non autorizzato (*hacking*) o per una modifica ai software, inserendovi ad esempio dei codici dolosi (*malware*). Oppure possono puntare sull'*hardware*, invalidandolo con la semplice manomissione dei *chip* al silicone. potrebbero servirsi di armi elettroniche tanto per moltiplicare gli effetti di un attacco doloso, quanto per arrecare danni maggiori, ove obiettivo fossero componenti sistemiche cruciali. Pensiamo nuovamente alle infrastrutture critiche: se non funzionanti o distrutte, le capacità di difesa e la sicurezza economica di una nazione sarebbero compromesse al punto tale da esser lecito assimilare un attacco informatico su vasta scala ad un'offensiva contro il centro di gravità strategico[26]. Di questo fanno ormai parte i centri di elaborazione dati e le infrastrutture di comunicazione, le apparecchiature Ict, il personale addetto, i sistemi di controllo, di gestione e di alimentazione, le reti di comunicazione e le loro connessioni geografiche[27].

La storia insegna tuttavia che lungi dall'attaccarla, i terroristi preferiscono servirsi della rete, *medium* prezioso di crescita e propaganda. Agli attentati elettronici preferiscono quelli fisici, dall'effetto certo, dirompente ed immediato. Internet funge piuttosto da campo d'addestramento virtuale. Nel dicembre 2004, un sito islamico militante permetteva ad esempio di scaricare un video che in 26 minuti istruiva i neofiti sull'assemblaggio e l'impiego occulto di esplosivi in attentati suicidi[28].

---

[25] Adams, *op. cit.*, p. 101.

[26] Aa.Vv., *Neutralizzare la guerra cibernetica*, in «Rivista della Nato», 2001, n. 4, p. 17.

[27] Stefano Sciascia, *La protezione delle reti di supporto alle infrastrutture critiche nazionali*, http://w3.uniroma1.it/security2/Eventi/Sciascia.pdf.

[28] Irving Lachow, Courtney Richardson, *Terrorist use of the Internet, The Real Story*, in «Joint Force Quarterly», 2007, n. 45, p. 100.

Politiche preventive

Il crollo dei tre edifici del *World trade center* (Wtc) ha palesato le conseguenze di un attacco fisico ai *network*, l'unico a poter massimizzare gli effetti di un'eventuale offensiva elettronica: in pochi minuti andarono perduti, oltre alle vite umane ed alla tranquillità psicologica di tanti, più di 2.200 circuiti di telecomunicazioni, duecentomila accessi vocali, centomila linee d'affari, 3,6 milioni di database e 10 ripetitori di telefonia mobile. Per non parlare del traffico internet fra Europa e Stati Uniti, bloccato per quasi due giorni a causa del danneggiamento di un cavo dorsale che passava sotto le Torri[29].

Fortunatamente, dopo l'11 settembre, si è galvanizzato un processo *in fieri*, sfociato nell'istituzione di più agenzie di sicurezza informatica, fra cui l'*European network & information security agency* (Enisa-2004). Di stanza a Creta, l'Enisa promuove la sicurezza delle reti e la diffusione di una cultura specifica. Paesi come Austria, Finlandia, Francia, Germania, Italia, Norvegia, Olanda, Regno Unito, Svezia e Svizzera hanno puntellato le difese delle rispettive infrastrutture critiche, studiando sistemi d'allarme preventivo, contromisure e politiche *ad hoc*[30]. La Commissione europea è intervenuta fin dal giugno 2001 per invocare un approccio comunitario al tema. Col quinto programma quadro ha iniziato ad assegnare fondi alla ricerca ed alla cooperazione con gli Usa, patrocinando la nascita della *Eu-Us joint task force on R&D on Cip (Critical infrastructures protection)*. Di più: si è dotata di un libro verde e di un embrione di rete informativa d'allarme (2005)[31]. Ma i problemi son ben lungi dall'essere risolti: molte infrastrutture hanno gestori privati o addirittura stranieri, e non sempre è agevole discernere fra competenze pubbliche, private o internazionali.

A loro volta, anche Nato, G8, Onu ed Ocse si sono attivati. L'organizzazione atlantica ha affidato ad una *road-map* (1997) il compito

[29] Enormi disagi ha causato in Medioriente la rottura recente (febbraio 2008) di due cavi sottomarini in fibra ottica. Vedi Guido Olimpio, *Egitto e Emirati, black out di Internet. Ma chi ha tagliato i cavi sottomarini?*, in «Corriere della Sera», 9 febbraio 2008, edizione *on-line*, http://www.corriere.it/esteri/08_febbraio_09/cavi_internet_olimpio_fa94d9cc-d6f1-11dc-b781-0003ba99c667.shtml.

[30] Gian Piero Siroli, "Strategic Information Warfare: an Introduction", in Aa.Vv., *Cyberwar, Netwar and the Revolution in Military Affairs*, New York, Palgrave Macmillan, 2006, p. 35.

[31] Il libro verde è intitolato *Programma europeo per la protezione delle infrastrutture critiche* (Epcip). Un altro acronimo inglese, Ciwin (*Critical infrastructures warning information network*), individua a sua volta la rete informativa d'allarme.

di sensibilizzare al problema e stimolare iniziative di formazione, cooperazione, ricerca e sviluppo. Il gruppo degli 8 paesi più industrializzati ha invece predisposto un vademecum *ad hoc*, indicando strutture e punti di contatto raggiungibili in ognuno dei paesi membri. Quanto all'Onu ed all'Ocse basti citare due documenti ufficiali: *Creazione di una cultura globale sulla sicurezza cibernetica e sulla protezione delle infrastrutture critiche informatizzate* è il titolo della risoluzione n. 58 del 2003, che le Nazioni Unite hanno indirizzato prioritariamente a governi e forze di polizia. Pare invece che con le *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione* (2002), l'Ocse abbia voluto rivolgersi soprattutto ad aziende, operatori ed utenti.

Non è tutto: sia la Nato che l'Ue hanno adottato metodologie *standard* per determinare il grado di affidabilità dei sistemi. Itsec (*Information technology security evaluation criteria*) e *Common criteria* suonano ormai familiari: spetta a loro valutare e certificare prodotti e sistemi Ict[32], fermo restando un margine d'incertezza ineluttabile.

Sovviene a proposito un *case-study* su cui hanno lavorato più volte gli allievi della *National defence university* di Washington: il *chipping*, ovverosia la produzione di *microchip* programmati per guastarsi sincronicamente e paralizzare intere realtà istituzionali. Gran parte della microelettronica è ormai confezionata in Cina: la famosa Legend-Lenovo, cresciuta sotto l'egida dell'Accademia cinese delle scienze e del Pla, ha fagocitato interi settori del colosso Ibm e continua ad avere solidi legami col governo centrale. Di recente ha fornito al dipartimento di Stato americano sedicimila computer, il cui costo, vantaggioso a priori, sarebbe incommensurabile in caso di *chipping*[33].

Rimane tuttavia che il 90% dei sistemi operativi utilizzati in Cina è prodotto da Microsoft e che finora è stata proprio l'azienda di Bill Gates ad adottare metodi truffaldini: d'accordo con la Intel, dotò Windows 98 ed il Pentium di *software* nascosti per accedere ai dati privati dell'utenza[34]. Non basta: negli anni Novanta, la *National security agency* (Nsa) allungò i tentacoli su diverse aziende fornitrici di sistemi crittografici e in particolare sulla Crypto-AG, società svizzera quasi monopolista del ramo, esportatrice in oltre cento paesi. Nel 1997, il governo svedese si accorse che le chiavi di Lotus Notes (Ibm) erano parzialmente in mano all'azienda statunitense: 24 *bit* su 64, suf-

[32] Anche in Italia cerniscono tutti i sistemi e prodotti Ict che trattino informazioni classificate.

[33] Umberto Rapetto, *Sono cinesi i nuovi generali*, in «Nova24», supplemento al «Sole 24Ore», 4 ottobre 2007, p. 5.

[34] Chris Wu, *An Overview of the Research and Development of Information Warfare in China*, in Aa.Vv., *op. cit.*, p. 187.

ficienti a decrittare in pochi secondi i codici segreti dell'utilizzatore. A servirsi del *software* erano all'epoca in tanti: dal ministero tedesco della Difesa a quello francese dell'Istruzione[35] .Chi la fa l'aspetti.

Superpotenze alla guerra cibernetica

Integrare le reti assicura senz'altro vantaggi enormi in termini di efficienza, risparmio e sinergie difensive, ma accresce al tempo stesso la vulnerabilità globale, funzione diretta dell'ampiezza e dell'architettura organizzativa e tecnologica dei *network*. Con 3 milioni di personal computer e dodicimila reti, il Pentagono ha di che preoccuparsi[36].

Nel 2000, un semplice virus (*I love you*) provocò perdite enormi: l'Amministrazione sanitaria per i veterani ricevette 7 milioni di messaggi infetti, la Nasa lamentò il danneggiamento di un migliaio di cartelle digitali ed il dipartimento del Lavoro dovette perdere 2.800 ore nel ripristino dei sistemi. Il danno finale ammontò a svariati miliardi di dollari: l'equivalente di un bombardamento a tappeto su una piccola città americana[37].

È vero: gli Usa contendono all'Impero di mezzo il primato per le attività cibernetiche offensive, ma sono senz'altro primi per quelle difensive (40%). Germania e Sud-Corea seguono a ruota. L'Italia, settima, manca ancora di un'interazione organica fra i Centri per la sicurezza operativa (Soc), causa principe di minori potenzialità e maggiori rischi.

Per fronteggiare le minacce, l'amministrazione statunitense ha emanato da tempo una direttiva *ad hoc*: la Pdd n. 63 del 22 maggio 1998[38], ed attivato presso il Comando supremo il *Joint functional component command network warfare* (Jfcc-Nw), mettendolo alle dipendenze del direttore della Nsa. Obiettivo: agevolare la cooperazione tra i vari organismi impegnati nella difesa delle reti informatiche e nelle attività di guerra telematica, tra cui figura in primissimo piano l'*intelligence* economica. Si tratta di un pericolo tutt'altro che potenziale come conferma un rapporto recente dell'Mi-5 britannico. Il sistema

[35] Frédéric Raynal, Éric Filiol, *Communications chiffrées: et si le ver n'était pas (que) dans la pomme?*, in «Défense Nationale», 2008, n. 5, pp. 83-84.

[36] I sistemi informatici del Pentagono subiscono una media di 60 attacchi quotidiani. Cfr. Dscint Handbook, *Cyber Operations and Cyber Terrorism*, 2005, n. 1, pp. 9-10, 16, http://www.fas.org/irp/threat/terrorism/sup2.pdf.

[37] Adams, *op. cit.*, pp. 106-107.

[38] La direttiva ha portato alla nascita di due agenzie: una, presso l'Fbi, è il Centro per la protezione delle infrastrutture nazionali (Nipc); la seconda, dislocata al dipartimento del Commercio, è l'Ufficio per la sicurezza delle infrastrutture critiche (Ciao).

economico-finanziario è avvisato: le aziende che operano in Cina, e non solo, sono costantemente monitorate dall'esercito popolare, che si serve di internet per sottrarre informazioni confidenziali. Bersaglio principe sono gli archivi elettronici di grandi banche e di studi legali, società di telecomunicazioni e compagnie dell'acqua e dell'elettricità.

Molti eserciti possiedono ormai veri e propri contingenti di truppe cibernetiche e lavorano alacremente allo sviluppo di armi digitali. A parte i soliti noti, figurano nell'elenco Brasile, Francia, India, Iran, Israele, Libia, Pakistan e Regno Unito. Invero, tra i paesi avanzati persistono delle remore ad attacchi cibernetici indiscriminati. Ne andrebbe della fiducia dei consumatori e del pericolo di ritorsioni incontrollabili.

La storia racconta che quando i serbi manomisero il sito della Nato, gli americani evitarono di fare altrettanto con i conti bancari di Milosevic. Sebbene il presidente Clinton avesse ordinato di affiancare bombardamenti informatici a quelli aerei, il Congresso si oppose, paventando pericolose conseguenze per il futuro. Il dipartimento della Giustizia manifestò più di un dubbio sulla legittimità della rappresaglia elettronica, così come in passato si era opposto ad attacchi informatici contro i serbo-bosniaci. Gli ex-jugoslavi non rinunciarono invece all'arma digitale. Duemila messaggi elettronici inondarono, saturandoli, i *server* di posta dell'Alleanza atlantica (*mail bombing*)[39]. Nel campo, i balcanici non erano certo dei neofiti: nel 1998, avevano già colpito in Svizzera, obnubilando il sito che ospitava «La voce del Kosovo», organo d'informazione dell'etnia albanese.

Contromisure

Esistono ovviamente dei baluardi agli attacchi elettronici: dall'irrobustimento alla ridondanza dei sistemi, dalle federazioni di reti al traffico multiprotocollo, dagli strumenti di *backup* alle sequenze di recupero. Saranno inoltre disponibili sistemi per la correlazione fra minacce, vulnerabilità ed *asset* da proteggere, che permetteranno di determinarne il livello di criticità. Sistemi prototipici simuleranno le modalità di diffusione di un *malware* in un'infrastruttura di rete complessa, riducendo non solo i tempi di reazione e di esposizione al rischio, ma vigilando al contempo sull'obsolescenza tecnologica. Secondo alcuni analisti, bisognerebbe allentare il legame simbiotico fra reti ed equiripartirle geograficamente, per avere più barriere fisiche. Di massima utilità sarebbe diversificare i sistemi operativi con cui i

[39] La Nato dovette fronteggiare anche attacchi Ddos, sferrati da *hactivist* internazionali che protestavano contro i bombardamenti.

network funzionano, così da scoraggiare le intrusioni e rendere più ardue le incursioni dei *cyber*-terroristi.

Rimane tuttavia il paradosso di tali e tante vulnerabilità. Internet era stata concepita durante la guerra fredda come sistema di comunicazione inespugnabile: l'idea del Pentagono era di plasmare un *medium* resiliente ad un attacco atomico, che desse alle autorità politico-militari sopravvissute la possibilità di comunicare e contrattaccare. Nel 1968, l'Arpa (*Advanced research project agency*), agenzia di ricerca e sviluppo della difesa[40], lanciò il progetto Arpanet che, nel giro di pochi anni, avrebbe portato gli Usa a disporre di una fitta rete di computer interconnessi in tempo reale. Anche il mondo accademico contribuì agli studi, beneficiando di fondi pubblici e di squadre di ricerca validissime. In una di queste lavorò Vinton Cerf che, ancora studente a Los Angeles, concepì l'architettura di un modo di comunicare rivoluzionario: tra il 1973 ed il 1978, Cerf sviluppò e collaudò con Robert Kahn i protocolli di comunicazione Tcp/Ip, fondamento dell'internet attuale[41].

Oggi, il sistema è talmente vulnerabile che alcuni non nascondono il timore di una Pearl Harbor digitale. Sebbene molti siano scettici, la Casa Bianca comincia a premunirsi. Richard Clarke, nominato dal presidente Bush consigliere speciale per la sicurezza cibernetica, ha dipinto un quadro tutt'altro che idilliaco: il sistema industriale americano si prepari. Il problema non è sapere se un tracollo stile 11 settembre avverrà o meno, ma quando.

Rivoluzione informatica e negli affari militari

In caso di conflitto tra potenze maggiori, la *cyber-war* esploderebbe in tutta la sua virulenza[42]. Nella nuova rivoluzione militare (Rma), l'informazione ha importanza basilare, sia a livello politico-strategico, che operativo e tattico. L'evoluzione e l'integrazione dei sensori terrestri, aerei e spaziali dovrebbe permettere di penetrare la 'nebbia della battaglia', rendendo lo scenario operativo più intelleggibile[43]. Nel complesso metasistema è l'informatica a giocare un ruolo fondamentale. Dalla potenza di calcolo dipende infatti la capacità di

[40] Oggi Darpa.

[41] Furono poi i fisici Tim Berners-Lee e Robert Cailliau, ricercatori al Cern di Ginevra, ad ideare il sistema ipertesto del *World wide web* (1983).

[42] James A. Lewis, *Between the Us and China: the Dynamics of Military Space*, p. 4, http://www.ifri.org/files/politique_etrangere/Lewis_gb.pdf.

[43] Lo scenario operativo include una superficie convenzionale di 100mila km^2 circa (lato 320 km).

sfruttamento della mole d'informazioni trasmesse dai sensori: satelliti d'osservazione terrestre e di sorveglianza elettronica, sistemi Awacs e Jstars[44], altrimenti sottoimpiegati. In Kosovo, effettivi 10 volte inferiori a quelli schierati nell'operazione *Desert Storm* hanno utilizzato un volume d'informazioni 3 volte maggiore. Sistemi civili son stati integrati nei dispositivi militari, moltiplicando le capacità di trasmissione, soprattutto spaziali[45]. È stato il trionfo del concetto C^{4}Istar, che tende a sostituire l'ormai classico C^{3}I[46], fondendo le varie funzioni in un «sistema di sistemi», secondo la definizione dell'ammiraglio Owens[47].

Sia chiaro: la rivoluzione dell'informazione non è solo fusione di dati in tempo reale. Le sue applicazioni militari sono molteplici e si traducono in armi più precise, sensori più numerosi, apertura a sistemi intelligenti e così via. In Afghanistan, piattaforme aeree e forze di terra son state collegate fra loro e con quartier generali distanti migliaia di chilometri. Ricognitori non pilotati (Uav) erano equipaggiati con missili e collegamenti diretti sia con le forze di terra che con i comandi di teatro. Bombardieri a lungo raggio ricevevano l'aggiornamento di compiti ed obiettivi durante il volo di rotta. Per la prima volta, sia i comandanti sul campo di battaglia che l'alto comando di Tampa disponevano di dati in tempo reale sull'evoluzione dei combattimenti.

Come se non bastasse, 9 giorni prima dell'operazione *Iraqi Freedom*, la difesa statunitense attivò un nuovo sistema di comunicazione satellitare che federava fra loro le varie componenti di forza armata, il Pentagono, la Casa Bianca, il dipartimento di Stato ed il Comando spaziale. Oltre 100 satelliti militari supportarono lo sforzo bellico, garantendo una capacità di trasmissione 10 volte superiore a quella registrata in *Desert Storm*[48]. La crescita è stata impressionante: l'Uav *Global Hawk* assorbe da solo 5.100 *megabits* al secondo, il quintuplo

[44] Il primo è acronimo di *Airborne early warning and control* (sistema di sorveglianza radar e controllo in volo); il secondo di *Joint surveillance target attack radar system*. Si tratta in entrambi i casi di velivoli radar assai sofisticati. Il Jstars ad esempio è in grado di rilevare e localizzare un carro armato distante oltre 150 km.

[45] Alla fine degli anni Novanta, il Pentagono spendeva già il 20% del suo bilancio (54 miliardi di dollari) in architetture C^{4}Istar.

[46] C^{3}I è acronimo di comando, controllo, comunicazione e *intelligence*, mentre C^{4}Istar sta per comando, controllo, comunicazione, computer, *intelligence*, sorveglianza, acquisizione obiettivi e ricognizione.

[47] Ex vice-presidente dello Stato maggiore interforze, l'ammiraglio ha avuto un ruolo cruciale nel promuovere e diffondere i principi della Rma in seno alle forze armate statunitensi.

[48] Gli Usa hanno più di 200 satelliti militari operativi, il decuplo degli europei. Spendono nel settore il 90% del totale mondiale, contro il 4% dei secondi.

dell'ampiezza di banda complessivamente disponibile durante la prima guerra del Golfo. Non basta: le ultime missioni insegnano che, dal 2010, occorreranno almeno 16 *gigabits* al secondo per soddisfare le esigenze di trasmissione delle forze armate statunitensi[49]. L'uso dei satelliti commerciali si è già imposto per ragioni di bilancio: i droni statunitensi trasmettono per lo più sulla frequenza Ku, servendosi di operatori commerciali come Intelsat ed Ses Global. Informazioni altamente confidenziali circolano, cifrate, sugli stessi satelliti che permettono di telefonare dall'Africa rurale[50]. Satelliti commerciali nazionali e non, come Ikonos, QuickBird, Orbview e Spot[51], affiancano nell'osservazione terrestre sistemi militari propriamente detti (Lacrosse, KeyHole).

Per l'ex capo di Stato maggiore dell'aeronautica militare statunitense, generale Fogelman, dominare lo spettro informativo è oggi preludio alla vittoria quanto lo era in passato l'occupazione di un territorio o la supremazia aerea. Al manuale classico sulle operazioni (Fm 100-5) se ne affianca così un altro sulla guerra informativa (Fm 100-6).

Fin dalle prime fasi del conflitto, vengono sferrati attacchi simultanei sull'intera profondità del campo di battaglia: un'offensiva in cui si fanno convergere contro i centri nevralgici dell'avversario (C^3I) armi digitali e munizionamento di precisione, sia aria-terra che superficie-superficie (*cruise*), prodromo all'annichilimento definitivo. Obiettivo è conoscere tutto del nemico, decapitarlo ed immobilizzarlo, senza lasciargli carpire nulla né del proprio dispositivo, né delle proprie capacità ed intenzioni. Sarebbe così possibile sbaragliarlo con il fuoco, privandolo di qualsiasi possibilità di reazione (*full spectrum dominance*)[52].

All'osservatore attento non sarà sfuggito che nei primi giorni delle operazioni nella ex-Jugoslavia, in Iraq ed in Afghanistan, le forze occidentali si sono concentrate nell'ingannare e bombardare i sistemi di rilevamento nemici, le centrali telefoniche, i ponti radio, i centri

[49] Limiti di banda hanno impedito che in Afghanistan si impiegassero simultaneamente più di 4 degli 8 Uav disponibili. Tecniche laser permetteranno tuttavia di valicare i limiti attuali. Vedi DAVID WEBB, «Missile Defence – The First Steps Towards War in Space?», in AA.VV., *op. cit.*, p. 83.

[50] RODOLPHE PARIS, *Marine et télécommunications par satellite: dualité civile et militaire*, in «Défense nationale», 2003, n. 6, p. 190.

[51] Sebbene meno celebrata di altre, l'azienda francese Spot e la sua costellazione di 5 satelliti per l'osservazione ottica detengono il 75% del mercato mondiale dell'immagine spaziale in risoluzione media (2-5 metri).

[52] Evoluzione del principio *global reach*, il dominio assoluto dello spazio elettromagnetico testimonia della pervicacia statunitense nel conservare una superiorità militare schiacciante su qualsiasi avversario.

nodali in fibra ottica e le linee coassiali per le comunicazioni. Questa è guerra cibernetica.

Pentagono e principali agenzie d'*intelligence* americane[53] hanno convogliato da tempo gran parte delle attività di ricerca e sviluppo nazionali verso un sistema di difesa integrata aria-spazio, deputato a garantir loro il predominio in entrambe le dimensioni[54]. Insieme al *cyber*-spazio, la stratosfera è infatti un moltiplicatore irrinunciabile di potenza politica, militare, economica e comunicativa: tutte le operazioni *net*-centriche dipendono dal controllo della dimensione aerospaziale. Le reti informatiche stesse iniziano dai sensori, i cui collegamenti sono assicurati in gran parte da assetti aerei o satellitari. Non per caso, gli Stati Uniti sono pronti a rigettare qualsiasi accordo internazionale sugli armamenti che interferisca con i loro progetti di dominio spaziale. Di più: la nuova *National space policy* (2006) si arroga il diritto di negare l'accesso alla quarta dimensione a chiunque non si uniformi agli interessi americani[55].

Washington ricava oggi il 70% delle sue informazioni strategiche dalle piattaforme spaziali, gran parte delle quali dedicate alle comunicazioni della marina militare; 90% della sua *intelligence* ha matrice satellitare[56], il che non sempre è un bene se si pensi agli errori (?) grossolani commessi nelle guerre balcaniche contro l'ambasciata cinese a Belgrado e più convogli di rifugiati[57].

Conclusioni

Lo sviluppo crescente di armi antisatellite (Asat)[58] e di tecniche di depistaggio e camuffamento dei sensori rischia di trasformare la dipendenza dallo spazio, cibernetico o meno, in un vero e proprio tallone d'Achille[59]. Poco convincenti sono le prove cui è stata finora

[53] Hanno un *budget* di 43,5 miliardi di dollari.

[54] Alain Dupas, *Il piano americano per il dominio del cosmo*, in «Limes», 2004, n. 5, pp. 53-54.

[55] Marco Valsania, *Bush: spazio proibito ai nemici dell'America*, in «Il Sole24ore», 19 ottobre 2006, p. 7.

[56] Giancarlo Elia Valori, *Geopolitica dello spazio, Potere e ricchezza nel futuro del pianeta*, Milano, Rizzoli, 2006, p. 63.

[57] *Hactivist* filo-cinesi risposero con una protesta elettronica di massa, attaccando i siti governativi statunitensi.

[58] Veicoli ad energia cinetica, laser posti a terra, disturbatori (*jammers*) satellitari, armi ad impulso elettromagnetico, minimissili antisatellite e così via.

[59] Paul-Ivan de Saint German, *Analyse de la notion de «Gap» - Le 'Gap' transatlantique*, «Frs», 2002, n. 27, p. 6, http://www.frstrategie.org/barreFRS/publications_ colloques/rech_doc/Telechargements/rechdoc27.doc.

sottoposta la Rma per sanzionarne il successo definitivo[60]: nelle guerre del Golfo, le capacità irachene son state ampiamente sopravvalutate, per ragioni politiche. Le truppe irachene e la guardia repubblicana erano poco addestrate e demotivate già prima dell'attacco alleato con tecniche d'*information warfare*. Di più: hanno evitato lo sconto diretto. Nonostante i *raid* aerei avessero distrutto i sistemi di Tlc più avanzati, da quelli satellitari, a quelli a microonde e via cavo, Saddam Hussein continuò a servirsi di corrieri per inviare ordini alle batterie missilistiche Scud. Nella prima guerra erano rimasti attivi collegamenti sufficienti a richiamare le truppe dal Kuwait e a ridispiegarle secondo il nuovo scenario. Annichilire i sistemi avversari di C^2 non è stato affatto semplice. I militari americani hanno capito in seguito che gli iracheni, persi i sistemi militari, si erano serviti delle reti commerciali e dell'internet *standard* per l'instradamento ed il recupero delle avarie, a conferma che il reindirizzamento dinamico funziona. Nella seconda guerra, il fragilissimo esercito nemico è riuscito a disturbare i satelliti per le telecomunicazioni, l'osservazione ottica e perfino il Gps che impartisce le coordinate del bersaglio alle armi aeree di caduta[61]. Non è poco: gli Stati Uniti schieravano oltre centomila ricevitori Gps e più di 6.600 bombe a radionavigazione (Jdams), 80% del totale[62].

Vi è da chiedersi che cosa sarebbe potuto accadere contro nemici più consistenti. Il teatro d'operazioni, desertico e privo d'ostacoli, non poteva che sublimare il ruolo della potenza aerea e meccanizzata. Il feldmaresciallo Rommel l'avrebbe intuito già nel 1942, forte delle esperienze in Nordafrica.

Piegare la ex-Jugoslavia non è stato altrettanto semplice: concepita come operazione rapida, la campagna *Allied Force* si è protratta per più di due mesi, ottenendo un risultato più deludente di quanto non fosse stato già negoziato a Rambouillet. Il terreno aspro, compartimentato e spesso coperto da nubi ostacolò i compiti dei sensori e dell'intelligence elettronica. Rientranze naturali offrirono ottimi ripari ad un difensore abilissimo nel perfezionare con l'arte i vantaggi offerti dalla natura.

---

[60] Ron Tira, *The Limitations of Standoff Firepower-Based Operations: On Standoff Warfare, Maneuver, and Decision*, «Inss», marzo 2007, n. 89, pp. 47-48, http://www. tau.ac.il/jcss/memoranda/memo89.en.pdf.

[61] Ferdinando Sguerri, *Defensive Counterspace*, in «Rivista Aeronautica», 2007, n. 1, p. 131.

[62] Una crescita impressionante se si pensa che il munizionamento a guida Gps non superava il 5-10% nella prima guerra del Golfo, raggiungeva appena il 35% in Kosovo ed il 70% in Afghanistan.

I radar per la difesa aerea furono occultati ed un intenso fuoco di sbarramento costrinse i velivoli alleati ad altitudini superiori ai quindicimila piedi. Inutile dire che identificare ed attaccare le artiglierie mobili serbe divenne missione assai gravosa. Gli ex-jugoslavi ingannarono i sistemi di rilevamento avversari con un acume tattico da far invidia: «*gens virum truncis et duro robore nata*»[63], potremmo dire con Virgilio. Ai ricognitori erano esposti bersagli reali, ai bombardieri obiettivi falsi. Veicoli civili furono massicciamente impiegati insieme a vettori militari ben camuffati. Al sorvolo dei ricognitori nemici, radar e sistemi d'allerta arrestavano le unità terrestri per impedire il tracciamento dei bersagli in movimento[64]. Nei trentottomila *raid* aerei, gli alleati non distrussero più di 50-200 obiettivi mobili serbi, vale a dire il 5-20% delle forze regolari nemiche, bottino assai magro per 78 giorni di combattimenti[65].

La vittoria finale arrivò più che dalle proprietà taumaturgiche della Rma, dall'enorme disparità fra belligeranti[66]. Difficilmente, combattenti abili e coraggiosi si lasciano demoralizzare da bombardamenti aerei massicci: la resistenza degli afgani agli invasori sovietici avrebbe dovuto essere un monito per gli Stati Uniti[67]. La storia militare racconta di unità capaci di combattere senza collegamento alcuno con i quartier generali. In Normandia (1944), le forze tedesche si ritrovarono spesso senza radio. Grazie al grado di addestramento, alla dottrina d'impiego e all'eccellente comando tattico, resistettero per quasi 2 mesi ad un avversario numericamente assai superiore, capitolando più per il logorio che per la mancanza di comunicazioni.

Lungi dall'essere un vantaggio, l'eccesso d'informazioni, può talvolta nuocere alla fluidità della catena di C^2. Niente garantisce che l'autorità di vertice, lontana dal teatro operativo, sia in grado d'interpretarne lo scenario così accuratamente come gli attori principali[68].

---

[63] «Una stirpe nata dai tronchi e dalle dure querce». Per gli antichi, le popolazioni autoctone nascevano dai tronchi degli alberi e, similmente a questi, avevano nella durezza la loro caratteristica principale. Vedi Publio Virgilio Marone, *Eneide*, libro VIII, verso 250.

[64] Tira, *op. cit.*, p. 48.

[65] In compenso, la Nato distrusse le infrastrutture del Paese e 500 falsi bersagli...

[66] Mackubin Thomas Owens, *Technology, the RMA, and Future War*, in «Strategic Review», 1998, n. 2, p. 68. Lo smacco d'Israele nella seconda guerra libanese conferma i limiti della Rma.

[67] Hervé Coutau-Bégarie, *Traité de stratégie*, Paris, Œconomica, 1999, pp. 473-474, 476.

[68] Alain De Neve, Joseph Henrotin, *La Network-Centric Warfare: de son développement à Iraqi Freedom*, in «Stratégique», 2006, n. 86-87, p. 65.

Quando il telegrafo fece irruzione sul campo di battaglia, nella seconda metà del XIX° secolo, determinò non poche frizioni tra classe politica e vertici militari. Sfruttando le possibilità di comunicazione e d'informazione offerte dal nuovo *medium*, i *leaders* politici interferirono in più di un'occasione nella condotta delle operazioni. Stesso discorso potrebbe esser fatto per le reti informatiche odierne che accrescono, *bello durante*, l'incisività del decisore politico, sia a livello strategico che tattico.

Eserciti iper-tecnologici, sebbene imbattibili sulla carta, possono rivelarsi del tutto inadatti allo scenario del XXI° secolo, soprattutto ove adottino condotte strategiche definite in funzione non degli obiettivi ma delle capacità militari, confondendo le une con gli altri[69]. Gli Usa si sono accorti in Iraq che la ridondanza di sensori ed altri orpelli è destabilizzante per il soldato: dopo aver investito milioni di dollari nel progetto *Land Warrior*, questo si è rivelato sostanzialmente inutile, a riprova che la tecnologia è solo un mezzo, non un fine, e può servire gli interessi della sicurezza nazionale solo se sussunta in uno schema strategico capace di discriminare esattamente il tipo di minaccia.

[69] ÉTIENNE DE DURAND, *Quel format d'armée pour la France?*, in «Politique Étrangère», 2007, n. 4, p. 731; ANDREA LOCATELLI, *Le false promesse della rivoluzione negli affari militari*, Centro argentino di studi internazionali, novembre 2006, pp. 18-19, www.caei.com.ar/es/programas/teoria/26.pdf.