CESTUDEC-CENTRO STUDI STRATEGICI CARLO DE CRISTOFORIS

PROBLEMI E PROSPETTIVE DEL CYBER TERRORISMO

MARIO AVANTINI

2011

CESTUDEC

Cyber Terrorismo: fenomeno crescente

Il *cyber*-spazio non è più solo lo spazio di diffusione per i mezzi di comunicazione di massa, da quelli tradizionali a quelli a più elevate vocazioni innovative. Esso è piuttosto un nuovo continente, ricco di risorse ma anche di insidie. Di fronte alla crescente militarizzazione di questo spazio, i governi del pianeta – ed in particolare le grandi potenze – sono impegnati in una accelerata competizione. La Russia ha ereditato dall'URSS un sistema, noto con l'acronimo di Sorm-2, in grado di copiare in *backup* ed in tempo reale qualsiasi singolo *bit* che transita nello spazio sovrano russo. La Cina ha attrezzato una rete difensiva nazionale, una sorta di enorme filtro in grado di scremare le informazioni di navigazione su internet considerate dannose, sgradite al governo centrale. Negli anni '60 dello scorso secolo il primato strategico tra USA e URSS si affermava con le missioni spaziali e i satelliti spia; oggi la competizione per la sicurezza si sta spostando rapidamente sulle reti tecnologiche. Non a caso, la relazione annuale presentata nel 2010 al Comitato parlamentare per i servizi di informazione da Dennis Blair, allora direttore della *National Intelligence* americana pone la minaccia cibernetica al primo posto, per la crescita esponenziale della capacità di « rubare, corrompere, danneggiare o distruggere gli *asset* pubblici e privati essenziali per la nazione americana ». Tocca a ciascun Paese, e anche all'Italia, occuparsi di queste minacce che incidono in maniera profonda su qualsiasi attività economica, sociale e istituzionale delle nostre comunità. Chi ha una responsabilità pubblica nei sistemi democratici occidentali dovrà cercare di conciliare in maniera efficace la prevenzione delle minacce con il pieno godimento dei diritti di ciascun cittadino, tra cui rientrano quelli alla riservatezza delle comunicazioni e alla libertà di espressione e di pensiero. I tre elementi costitutivi dello Stato nazionale sono direttamente coinvolti dal potenziale utilizzo per fini criminali delle reti informatiche: l'individuo, il sistema economico e le istituzioni. Nel primo caso, possiamo considerare il criminale virtuale come una versione contemporanea del truffatore *d'antan* e la frode telematica come una diversificazione di portafoglio per i *network* criminali transnazionali, la cui capacità finanziaria è alimentata anche da

questi circuiti. Gli internauti e gli operatori economici sono i bersagli privilegiati di una congerie di criminali dal profilo molto diverso: dai variopinti *hacker*, eroi o anti-eroi della pubblicistica, fino a strutture ben organizzate e aggressive, che originano dalle mafie transnazionali, dalle reti di criminalità finanziaria e anche dalle reti terroristiche. Ma è sul terreno della competizione strategica tra Stati che si gioca la posta più alta, che influirà sui nuovi equilibri internazionali. Concettualmente, occorre acquisire un elemento importante: quei Paesi che definiscono pubblicamente strategie e meccanismi difensivi rispetto alle minacce cibernetiche sono in grado di organizzare in parallelo capacità offensive. Si stanno formando, cioè, dottrine di impiego che sono basate sulla capacità di attaccare un potenziale nemico, di azzerarne le difese e colpirne obiettivi strategici, anche come parte di pianificazioni di attacchi militari, senza che esistano definizioni condivise di questo nuovo spazio di competizione e potenziale contrapposizione strategica. A sua volta, la sicurezza delle infrastrutture informatiche che assicurano il funzionamento delle linee critiche è divenuta una priorità nella ridefinizione della sicurezza nazionale: infrastrutture logistiche e di viabilità, reti elettriche e telefoniche, *pipeline* per il trasporto di idrocarburi, circuiti finanziari sono reti di sensibilità strategica per la vita di un Paese. Non meno sensibili dei comandi satellitari e dei sistemi di controllo del traffico aereo sono le reti e i dialoghi tra macchine che muovono generatori, dighe, ascensori, pompe, treni, piattaforme petrolifere. I *network* informatici e telematici ne rappresentano una metastruttura, una « rete delle reti », il cui danneggiamento può provocare il *black-out* delle operazioni, dalle più elementari a quelle vitali. Un attacco ai nodi sensibili di connessione tra questi *network* può « accecare » parti importanti dei sistemi esistenti. La novità delle minacce legate al *cyber*-spazio è che esse rappresentano un’arma non convenzionale in grado di produrre effetti convenzionali. La minaccia cibernetica ha conosciuto una graduale trasformazione che le ha conferito una dimensione propriamente strategica: ai singoli *hacker* si affiancano da tempo gruppi terroristici e criminali, mentre è più recente la crescente aggressività di attori statuali, i quali combinano posizioni meramente « difensive » –

di reazione e contrasto agli attacchi – con quelle che annoverano anche misure controffensive. Per semplificazione analitica ed interpretativa, è possibile suddividere la minaccia derivante dal *cyber*-spazio in quattro principali tipologie:
1) *cyber-crime*: ovvero l'insieme delle minacce poste da organizzazioni criminali nazionali o transnazionali, le quali sfruttano o spazio cibernetico per reati quali la truffa, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali;
2) *cyber terrorism*: ovvero l'utilizzo della rete da parte delle organizzazioni terroristiche, a fini di propaganda, denigrazione o affiliazione. Particolarmente significativo è il caso della *cyber*-propaganda, ovvero della manipolazione delle informazioni veicolate nella rete a fini di denigrazione e delegittimazione politica, discriminazione sociale o personale. Nei casi estremi, si intende ipotizzare l'utilizzo sofisticato della rete internet o dei controlli telematici per mettere fuori uso, da parte di organizzazioni del terrorismo, i gangli di trasmissione critica delle strutture o dei processi che attengono la sicurezza nazionale;
3) *cyber espionage*: ovvero l'insieme delle attività volte a sfruttare le potenzialità della rete per sottrarre segreti industriali a fini di concorrenza sleale (se consumati nel mercato dei brevetti civili) o di superiorità strategica (nel caso di sottrazione di disegni e apparecchiature militari o *dual-use)*;
4) *cyber war*: ovvero lo scenario relativo ad un vero e proprio conflitto tra Nazioni, combattuto attraverso il sistematico abbattimento delle barriere di protezione critica della sicurezza dell'avversario, ovvero attraverso il disturbo o lo « spegnimento » delle reti di comunicazione strategica, e l'integrazione di queste attività con quelle propriamente belliche.
La difficile tracciabilità degli attacchi rende molto complessa la prevenzione della minaccia, se non attraverso adeguati scudi di protezione. Molto spesso, l'offensiva giunge da migliaia di chilometri di distanza ed il *server* che ne scatena il potenziale ha raramente una precisa identità. Vi sono evidenze consolidate dell'interesse di *al-Qaeda* per il *cyber*-terrorismo. Alcuni computer sequestrati alla

rete terroristica hanno fatto trapelare dettagli riguardanti i sistemi di Supervisione e Acquisizione Dati (SCADA) negli Stati Uniti, che controllano l'infrastruttura strategica del Paese, comprese reti elettriche, centrali nucleari, cavi a fibre ottiche, oleodotti e gasdotti, dighe, ferrovie e depositi di acqua. I sistemi SCADA non sono stati creati per essere accessibili da reti esterne, ma molti attualmente sono controllati via internet, cosa che li rende vulnerabili alle intrusioni e agli attacchi informatici. I computer sequestrati ad alcuni appartenenti ad *al- Qaeda* contenevano addirittura gli schemi di una diga negli Stati Uniti, insieme al *software* di ingegneria che abilita gli operatori a simulare un guasto virtuale di dimensioni catastrofiche, con relativa inondazione di aree densamente popolate. Lo sviluppo relativamente recente delle reti digitali globalmente collegate ha inaugurato anche una nuova stagione di spionaggio. Ogni giorno, il Dipartimento della Difesa americano rintraccia circa tre milioni di sonde non autorizzate nei suoi *network*, mentre il Dipartimento di Stato deve fronteggiarne due milioni. Il Dipartimento di polizia di New York registra 70.000 tentativi giornalieri di intrusioni elettroniche. Nel 2007, il Comitato per la Sorveglianza e la Riforma della Pubblica Amministrazione USA ha assegnato al Dipartimento di Stato, a quello della Difesa, a quello del Tesoro e alla Commissione per la Regolamentazione Nucleare un *rating* pari a « F » nella Pagella Federale di sicurezza dei sistemi informatici. Si tratta di uno dei voti più bassi attribuibili. Poche settimane prima, infatti, il sistema informatico della segreteria e del gabinetto del Ministro alla Difesa Robert Gates era stato ripetutamente violato da *hacker* che, secondo le indagini dei servizi di sicurezza, avrebbero avuto supporto logistico e finanziario del governo cinese. Da quella indagine ebbe altresì inizio una analisi più estesa delle minacce legate al *cyber*-spazio provenienti dall'Estremo Oriente. Il risultato è contenuto in un'articolata pubblicazione promossa dallo *US-China Economic and Security Review Commission*, nella quale si individua esplicitamente la crescente competizione tra USA e Cina nella conquista del *cyber*-spazio ed il possibile utilizzo di strumenti informatici per operazioni mirate di sabotaggio o di intromissione nei sistemi americani. La Cina, si afferma, seguirà la strada del *cyber*

spionaggio con particolare determinazione, sia attraverso agenzie governative sia sponsorizzando altre organizzazioni che si stanno impegnando in questo tipo di « pirateria » internazionale. Il Pentagono ritiene che gli *hacker* militari cinesi abbiano compilato piani dettagliati per il sabotaggio delle infrastrutture di comunicazione militare USA; nella primavera del 2009, il *Wall Street Journal* ha riportato la notizia secondo cui parti del programma militare *Joint Strike Fighter* (JSF), il più costoso programma della storia per la creazione di un nuovo caccia, per un valore complessivo di più di 40 miliardi di dollari, erano state intaccate da *hacker*-spia cinesi. Nel 2007, l'Amministrazione Bush ha investito 17 miliardi di dollari nella *Comprehensive Initiative on Cybersecurity*, che ha identificato e segnalato le vulnerabilità esistenti. Poco dopo l'inizio del suo mandato, il presidente Obama ha dichiarato che la sicurezza cibernetica sarebbe stata considerata elemento strategico di sicurezza nazionale, procedendo poi alla nomina di un Coordinatore nazionale delle attività *(cyber-zar)*, che opera alla Casa Bianca in raccordo con il *National Security Council*. Il Segretario Generale della *International Telecommunications Unit* dell'ONU, Hamadoun Toure, ha invocato l'urgenza di un accordo internazionale per prevenire la possibilità di una guerra informatica tra grandi potenze, i cui effetti sono stati definiti « più devastanti di uno *tsunami* »; contemporaneamente, sulla base di uno studio commissionato dal *World Economic Forum* di Ginevra, è emerso come almeno 20 Paesi del mondo abbiano già sviluppato capacità sofisticate per avviare un conflitto su larga scala utilizzando gli strumenti informatici. Nell'enfatizzare la capillarità della rete informatica mondiale – di cui internet è solo l'espressione più nota –, non possono essere sottovalutate le possibili implicazioni derivanti dall'utilizzo distorto e dalla manipolazione dei contenuti informativi a fini di propaganda politica, discriminazione o denigrazione personale e professionale, creazione di consenso attraverso la distruzione della reputazione dell'avversario. La rete come « arma politica » ed evoluzione dei più tradizionali strumenti di propaganda richiede una particolare attenzione da parte di chi è chiamato a regolare, negli spazi di discussione, confronto e dibattito *online*, messaggi e contenuti che

richiedono, innanzitutto, la piena assunzione di responsabilità da parte degli utenti. Queste variabili producono, a loro volta, una serie di criticità nell'elaborazione di strategie difensive:
• rendendo indispensabile un approccio sistemico. Una politica di difesa cibernetica comprensiva, riguardando tutti i settori della società, presuppone necessariamente uno stretto coordinamento fra i diversi soggetti, dalle agenzie governative competenti alle imprese che gestiscono infrastrutture critiche, fino ai singoli cittadini, in termini di « educazione » alla sicurezza informatica. Uno fra i problemi di un simile coordinamento « pubblico-privato », al di là dei pur significativi aspetti tecnici e logistici, consiste nell'imporre al settore privato la subordinazione degli interessi particolari a quelli generali. Ad esempio, in un rapporto del *Congressional Research Service* statunitense, ci si interroga circa l'opportunità di obbligare le compagnie informatiche a dare immediata notizia al *Department of Homeland Security* (DHS) di eventuali vulnerabilità riscontrate nei propri prodotti;
• rendendo necessario il superamento, sul piano metodologico, della divaricazione fra ambito militare e civile. Il linguaggio utilizzato per descriverne i concetti chiave è spesso derivato dal settore della difesa (« aggressione », « minaccia », « attacco », ecc.), ma le minacce informatiche riguardano in egual misura anche le infrastrutture civili. Inoltre, alcune tipologie di attacchi informatici toccano necessariamente le competenze di organismi civili di sicurezza e di polizia, come avviene, ad esempio, per le truffe elettroniche e il furto d'identità; altre, quali l'intrusione dall'estero in una banca dati governativa classificata, attengono evidentemente agli organi preposti alla difesa del Paese. Questo aspetto ostacola notevolmente un efficace coordinamento internazionale a difesa delle infrastrutture informatiche poiché influenza la definizione stessa di minaccia cibernetica, sempre fortemente modellata dalle specifiche sensibilità di ogni singolo Paese ed attore. Così, ad esempio, la « *Cyber Security Strategy* », recentemente pubblicata dal Governo australiano, pone un forte accento sull'aspetto « micro » della minaccia (truffe informatiche, *privacy*, furti d'identità, mentre dalla documentazione statunitense traspare l'ormai consolidata

tendenza di Washington a mettere in primo piano la dimensione strategico – militare e quella terroristica;
• generando un dibattito giuridico-istituzionale, in particolare negli USA, sulla suddivisione delle responsabilità della difesa informatica, a livello statale, fra Esecutivo e Legislativo. La discussione chiama fortemente in causa la funzione regolatoria dell'organo legiferante, specialmente a causa dei dilemmi che solleva in materia di rispetto della *privacy* delle comunicazioni. Tuttavia, essa risente di un interrogativo più profondo circa l'importanza della dimensione operativa della minaccia cibernetica. L'istituzione di un *Cyber Command* presso il Pentagono, forte di quasi 90.000 uomini e con capacità tecnologiche all'avanguardia, è l'eloquente conferma della decisione di considerare il *cyber*-spazio un nuovo fronte militare. Oltre a interrogarsi sulla possibilità di un futuro *cyber*-attacco terroristico catastrofico, il dibattito sulla materia negli USA ha toccato anche l'applicabilità di una dottrina di deterrenza all'ambito della *cyber- war*. Si tratta, come è evidente, di uno sforzo teorico audace, considerato che il principale beneficio di cui gode l'autore di un attacco informatico è l'alto tasso di anonimato e protezione fisica garantitagli dalla rete. La medesima copertura che, ad oggi, sembra confinare qualunque strategia di difesa a una dimensione esclusivamente di prevenzione e di « *damage control* » eliminando, o quasi, credibili prospettive di misure di ritorsione. In ogni caso, appare evidente che quanto maggiore è la percezione della minaccia come « operativa » e immediata, tanto più operativa deve essere la risposta, che diviene quindi in misura maggiore compito del Governo;
• rendendo ardua la quantificazione della minaccia. La scarsità di elementi circa l'ubicazione fisica dell'attaccante e delle sue risorse rende estremamente complessa la valutazione del danno che egli è potenzialmente in grado di infliggere. L'unico elemento tangibile di valutazione è il danno che l'attaccante è già stato in grado di fare. Questo complica enormemente la definizione generale del rischio e di conseguenza il calcolo e la ripartizione delle risorse da allocare per proteggersi. Gli unici dati certi sull'entità della minaccia cibernetica è che essa è in aumento, a un

ritmo tale da farla assurgere al rango di questione urgente e prioritaria nelle agende di sicurezza e difesa delle maggiori Nazioni occidentali. Secondo un sondaggio, citato dal presidente Obama il 5 giugno 2009, « negli ultimi due anni il crimine informatico è costato agli USA più di 8 miliardi di dollari ». Inoltre, mentre nel 2006 il CERT del DHS ha riportato 5.503 « incidenti » relativi alla sicurezza dell'infrastruttura informatica del governo, la cifra è salita a 16.843 nel 2008, pari a un aumento del 206%. Ancora, la società di sicurezza informatica McAfee ha affermato, nel suo rapporto annuale del 2007, che « circa 120 Paesi stanno sviluppando la capacità di usare Internet come un'arma offensiva da sfruttare sui mercati finanziari, sui sistemi informatici governativi e sulle infrastrutture critiche ». Un *trend*, quello descritto, che ha portato il Direttore dell'Unione Internazionale delle Telecomunicazioni (ITU) a dichiarare che « la prossima guerra mondiale potrebbe essere combattuta nel *cyber*-spazio ». Le attività delittuose di *cyber-crime* sono facilitate in generale dalla crescente presenza di vulnerabilità nei sistemi e nelle infrastrutture informatiche da cui vengono erogati servizi di *e-government* e di *e-commerce* oppure sono gestite infrastrutture critiche tra loro interdipendenti. I rischi associati alla presenza di vulnerabilità nei sistemi non sono collegati esclusivamente alla mancanza della necessaria *patch.* Esiste spesso un intervallo di tempo tra la scoperta di una vulnerabilità e il rilascio della relativa soluzione tecnologica. Tale spazio temporale può essere sfruttato liberamente dall'attore criminale. Insieme alle vulnerabilità a livello di sistema operativo, sono da segnalare quelle sempre più crescenti per l'ambiente *web* da dove è possibile montare attacchi multipli sfruttando ignari utenti individuali diventati *botnets*. Sebbene il numero delle vulnerabilità in questo specifico contesto sia calato nel 2008, esiste tutta una serie di nuove applicazioni *web* che creano delle nuove « falle digitali » anche in quei sistemi dove sono state applicate tutte le necessarie contromisure. Esempi in questo senso sono l'installazione di nuove soluzioni di comunicazione *Voice over IP* all'interno di *browsers* oppure di soluzioni per la visione interattiva di documenti elettronici o di contenuti multimediali. Le vulnerabilità di cui si è parlato precedentemente sono associate, in

particolare, a errori nella programmazione o nell'integrazione di complessi sistemi e soluzioni *software*. Possono anche essere causate dall'errata implementazione di regole di sicurezza informatica da parte degli utenti. Queste vulnerabilità, tuttavia, sono anche causate da codici malevoli meglio conosciuti con i termini *virus, worm o Trojan*. Essendo ognuno di essi un'opera di ingegno, le loro funzionalità variano sulla base degli obiettivi o delle esigenze del suo programmatore, sebbene alla fine vi sia una certa somiglianza funzionale tra tutti loro. Esistono, per esempio, codici malevoli che, una volta installati, disattivano le funzionalità di sicurezza informatica di una postazione di lavoro o di una rete aziendale, facilitando il successivo scarico di altri codici malevoli oppure l'ingresso abusivo. Esistono altri *software* che hanno invece l'obiettivo di facilitare il furto di dati commercialmente sensibili. Sebbene siano adesso sul mercato soluzioni di sicurezza informatica dai prezzi contenuti, esistono su internet programmi simili ma totalmente « modificati » in modo tale da dare un falso senso di sicurezza all'operatore che invece si ritrova uno strumento informatico completamente vulnerabile. Come nel caso delle vulnerabilità, anche per questi *software* esiste « un mercato nero digitale » dove la domanda e l'offerta criminale si incontrano. La diffusione massiva di vulnerabilità e di codici malevoli è anche facilitata dal crescente fenomeno della posta elettronica spazzatura meglio conosciuta come *spam*. Sulla base di dati offerti dai principali produttori di *software* alla Commissione Europea, circa il 28% dello *spam* mondiale ha origine in Europa, mentre il 20% proviene dal Nord America. Il poco invidiabile primato spetta alla Polonia, seguita da Romania, Russia e Italia. Tuttavia, come precedentemente indicato, l'identificazione della provenienza di tali messaggi non è sempre certa per la facilità con la quale è possibile nascondere la propria residenza geografica su internet. Di per sé lo *spam* non crea particolari problemi agli utenti se non quello di ricevere messaggi elettronici dai contenuti indesiderati. Il problema è che, come anticipato precedentemente, lo *spam* può essere veicolo per altri rischi. Collegato al problema dello *spam* esiste quello del furto dell'identità elettronica attraverso attività di *phishing*. Con questo termine si intende principalmente la richiesta via posta

elettronica ad un ignaro utente delle credenziali di accesso ai propri conti bancari tramite *link* ad una pagina surrettizia di un istituto bancario presente *online*. Che tale truffa possa avere un buon ritorno economico è dimostrato dal fatto che il 72% dei messaggi di *phishing* hanno una connotazione finanziaria, mentre gli altri presentano offerte per servizi internet, per giochi d'azzardo o per l'acquisto di materiale elettronico. Come altri fenomeni di *cyber-crime*, anche il *phishing* finanziario presenta una spiccata trans-nazionalità, in quanto gli artefici delle truffe sovente appartengono a Paesi diversi da quelli delle vittime. In Italia, come in altri Paesi, è stato registrato un significativo aumento di tali truffe. Secondo la Centrale Rischi Finanziari (CRIF), principale agenzia italiana di *consumer credit information*, nel 2008 è stata registrata una crescita dell'11% e del 16%, rispettivamente, nel numero e nel volume medio delle frodi elettroniche via *phishing* rispetto all'anno precedente. Tutte queste forme di *cyber-crime* di per sé hanno un impatto indiretto sulla sicurezza nazionale del Paese.

Mario Avantini

Riferimenti:
« *Relazione Copasir* » luglio 2010

« *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* », ottobre 2009.

« *Cyberspace and the National Security of the UK* », Chatham House, 3/2009.

« *Terrorist Capabilities for Cyberattack: overview and policy issues* », CRS, 22/1/2009.

« *Cyber Security Strategy* », Governo dell'Australia, 2009.

« *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy*
« *Cyberdeterrence and War* », Rand Corporation, 2009.

« *Cyber Crime*: A 24/7 *Global Battle* », McAfee, 2007.