NUOVE MINACCE ALLA SICUREZZA INTERNAZIONALE: *HACKTIVISM* E CIBERTERRORISMO

STEFANO BALDI

SOMMARIO: *1. Il ciberspazio. – 2. Pregi e difetti del mondo virtuale. – 3. Gli attori: da Hacker ad Hacktivist. – 4. Tipi di attacco informatico. – 5. Attacchi ad infrastrutture critiche. – 6. Le asimmetrie dell'attacco informatico. – 7. L'azione della Comunità internazionale. – Appendice.*

Quando si parla di *cyberterrorism*, di *cyberwar* o *hacktivism*, ovvero di quei casi in cui l'attivismo politico e sociale fa ricorso alle tecnologie della comunicazione e dell'informazione (ICT), si ha spesso l'impressione di avere a che fare con qualcosa di molto lontano e poco rilevante per la comunità internazionale e per l'ONU. Alcuni recenti studi hanno in realtà dimostrato quanto questa percezione sia sbagliata e superficiale[1].

Per dare un'idea delle potenzialità e dei rischi legati al fenomeno degli attacchi informatici, è sufficiente fare un rapido e semplice ragionamento di carattere numerico. Innanzitutto, possiamo sostenere che la stragrande maggioranza delle 620 milioni di persone che accedono a Internet si comporta "correttamente" facendo buon uso dei numerosi servizi e delle fonti di informazione disponibili (posta elettronica, formazione *on-line*, comunità professionali interessate a temi specifici come salute e ambiente). Tuttavia, se ipotizziamo che un solo utente su un milione abbia intenzioni poco benevole, ci ritroveremo di fronte a 620 individui potenzialmente pericolosi sul piano della sicurezza informatica, che con un comune

[1] S. BALDI, E. GELBSTEIN, J. KURBALIJA, *Hacktivism, cyberterrorism e cyberwar*, Geneva, Malta, Belgrade, 2003. Informazioni disponibili sul sito *http://www.diplomacy.edu/diplo* e sul sito *http://baldi.diplomacy.edu*.

accordo sarebbero più che sufficienti per danneggiare seriamente una qualsiasi impresa o istituzione che faccia pieno affidamento (o che dipenda strategicamente) su sistemi di computer e reti informatiche.

Lo scopo di questo intervento è far riflettere su alcuni fenomeni e sui rischi e sul potenziale impatto che tali fenomeni potrebbero avere sulla comunità internazionale nel suo complesso, andando ad incidere, a livello locale e globale, sulle nostre attività quotidiane.

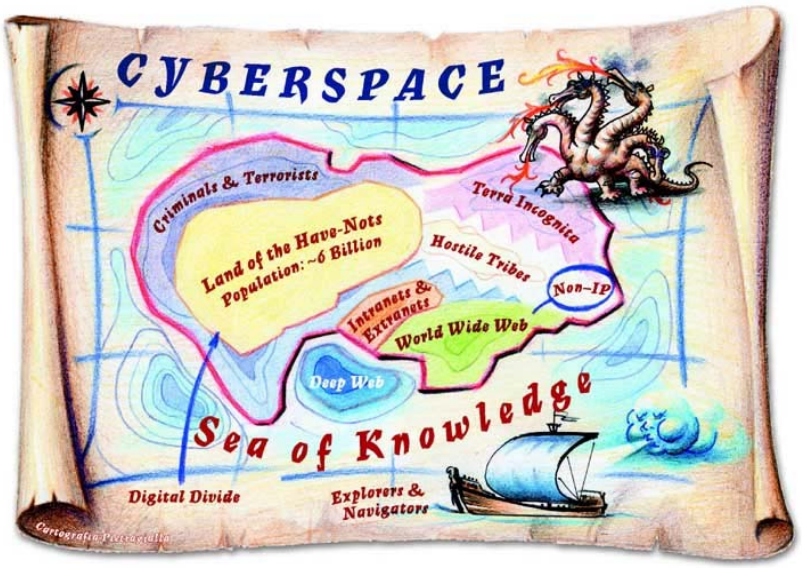
1. Il ciberspazio

Qual è il campo di azione di questa analisi? Uno spazio ampio, di cui ormai siamo parte, che viene definito con un termine piuttosto recente, *cyberspace* o ciberspazio. Quando usiamo *Internet* e il *World Wide Web* (WWW), ad esempio, siamo in uno spazio da cui in qualche modo dipendiamo non solo per l'uso intenzionale che ne facciamo, ma per molte funzioni e servizi di cui noi stessi non ci rendiamo conto. Nella fig. 1 si è cercato di visualizzare la complessa ed articolata realtà del ciberspazio. In questo mondo virtuale trovano spazio anche i "Criminali e Terroristi" (indicati nella mappa) che utilizzano gli strumenti informatici a disposizione per il perseguimento di finalità negative per la società civile.

Ai fini di questa trattazione sono stati riuniti, assieme a criminali e terroristi, anche gli *hacktivisti*, ovvero coloro che adoperano i mezzi informatici per la promozione o il perseguimento di una causa ideale[2] facendo ricorso a pratiche scorrette o illegali. Questi gruppi sono stati definiti la "società incivile", contrapposta a quella che comunemente definiamo la società civile.

[2] Molti attivisti usano Internet in modo tale da non causare particolari disturbi o danni, ma soprattutto per sostenere la propria causa, reclutare nuovi sostenitori e raccogliere fondi. Per un approfondimento storico del fenomeno si veda S. BALDI, *La protesta politica e sociale internazionale nell'era di Internet. Il caso di Seattle*, in *Affari Sociali Internazionali*, n. 1, 2002, Milano.

Fig. 1 – Mappa virtuale del Ciberspazio



Fonte: BALDI - GELBSTEIN - KURBALIJA, *Hacktivism, cyberterrorism e cyberwar*, Malta, 2003

2. Pregi e difetti del mondo virtuale

Perché il ciberspazio è divenuto, in poco tempo, così importante nella nostra vita quotidiana? Perché è tanto utilizzato e altrettanto abusato? In realtà ci sono moltissimi motivi, alcuni dei quali potremmo riassumere facendo ricorso all'analogia dello *Yin/Yang*, la parte scura e la parte chiara, il male e il bene, il negativo e il positivo che pervadono e caratterizzano ogni cosa.

Tra i principali aspetti positivi (lo *Yang*) del ciberspazio:

1. la facilità di connessione che rende semplice l'utilizzo della rete per apprendere, per essere informati e per diffondere informazioni;

2. la variabile tempo non rappresenta più un limite, essendo possibile collegarsi 24 ore su 24, 7 giorni su 7;

3. la facilità di raggiungere economicamente e tempestivamente qualsiasi punto della rete internet elimina, oltre a quello del tempo, il problema della distanza.

4. la possibilità di dare maggiori garanzie sulla riservatezza delle comunicazioni e scambio di informazioni. Il ricorso al criptaggio ne è un esempio.

Purtroppo esiste anche una parte oscura dello spazio virtuale (lo *Yin*), da cui emergono i suoi lati negativi. La semplicità d'uso degli strumenti a disposizione fa in modo che essi si prestino facilmente ad abusi. Se da un lato l'uso di programmi per il criptaggio, ad esempio, permette la garanzia della *privacy* – aspetto di per sé positivo – dall'altro consente di nascondersi, restare anonimi e di assumere facilmente identità virtuali, agevolando in tal modo chi vuole utilizzare questi mezzi per motivazioni poco gratificanti o costruttive, come nel caso, appunto, di criminali o terroristi.

3. Gli attori: da Hacker a Hacktivist

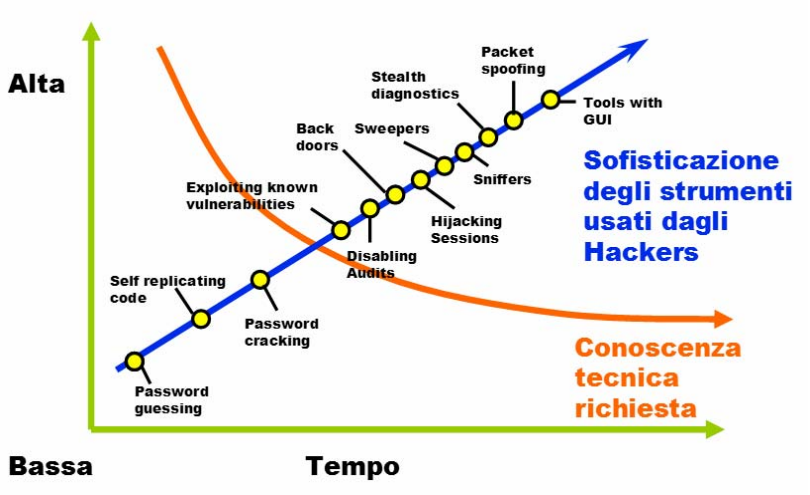
Se vogliamo individuare gli attori protagonisti di questa breve analisi, il primo termine che viene in mente è quello di *hacker*[3]. È sbagliato qualificare l'*hacker* come personaggio necessariamente negativo e che pertanto va combattuto. Gli *hackers* sono originariamente persone esperte in questioni tecnologiche, da sempre impegnate ad individuare quei problemi, quegli errori nei programmi, quelle debolezze che sono insite nei mezzi (*hardware* e *software*) e che possono mettere a rischio il buon funzionamento di un sistema. In questo senso l'*hacker* può essere considerato come un ricercatore intento a migliorare le condizioni di funzionamento e di rendimento dei vari mezzi a disposizione. È chiaro che quanto detto

[3] Un interessante libro sul tema è quello scritto da P. MASTROLILLI, *Hackers, i ribelli digitali*, Bari, 2002.

confina con un'altra serie di possibilità: l'*hacker* può naturalmente utilizzare le proprie conoscenze (e le carenze altrui) per effettuare un insieme di operazioni, che vanno dall'intrusione all'intercettazione, alla modifica di programmi e di pagine Web. Ciò che va tenuto presente è che in realtà queste operazioni sono relativamente facili da eseguire, ma difficili da individuare per chi prova a difendersi in caso di un abuso. Negli ultimi anni, peraltro, la sofisticazione dei mezzi usati dagli *hackers* è cambiata di pari passo con la conoscenza tecnica necessaria per il loro utilizzo. Rappresentando graficamente tali tendenze si può immaginare un grafico quale quello riportato nella fig. 2.

La linea ascendente si riferisce alla sofisticazione dei mezzi a disposizione degli *hackers*, che vanno da un livello iniziale (ad esempio programmi per scoprire le *password* usate), ad un ultimo, rappresentato dagli strumenti con GUI (*Graphic User Interface*), dotati di un'interfaccia grafica molto facile da usare. Sono programmi che non richiedono grandi conoscenze ma sono potenti e consentono di effettuare una ampia serie di operazioni.

Fig. 2 – Sofisticazione strumenti hackers



Fonte: adattamento da Dipartimento della Difesa degli Stati Uniti

La curva discendente rappresenta la conoscenza necessaria per l'utilizzo di tali mezzi. Se fino ad alcuni anni fa era indispensabile essere esperti del settore (proprio perché i programmi erano molto complicati), oggi la conoscenza necessaria è in continua diminuzione ed anche un utente non esperto può effettuare operazioni relativamente complesse.

L'effetto combinato di queste due tendenze comporta l'aumento del numero dei potenziali *hackers*. Da un lato, quindi, cresce il numero globale di utenti di *Internet* e di coloro che lo utilizzano a scopo di protesta o per sferrare attacchi. Dall'altro, diventa sempre più facile compiere la serie di operazioni che abbiamo già descritto. Talmente facile che tramite un motore di ricerca qualsiasi, come il noto *Google*, è possibile effettuare semplici ricerche – ad esempio, cercando "*hacking tools*" – e trovare una serie di indicazioni, consigli pratici e programmi talvolta anche molto specifici. Per esempio, sono disponibili programmi molto semplici che permettono di testare ed individuare *password* usate per entrare nella rete o per accedere a un certo servizio, che talvolta vengono incautamente salvate sul proprio computer.

Come già detto, il concetto di *hackers* è quello che più frequentemente viene indicato e facilmente percepito. In effetti non si tratta di una realtà omogenea ed è necessario distinguere i diversi gruppi riconducibili a tale concetto, in un'ideale scala crescente di motivazioni e potenziali danni che si possono causare.

Lo *script kiddy* è il meno esperto; potrebbe essere un utente qualsiasi che effettuando ricerche *online* come quelle sopra descritte, trova programmi e li prova con il rischio di provocare dei danni senza rendersene conto.

Il livello successivo è quello dell'*hacker* in senso stretto. Questi, acquisendo maggiore esperienza e conoscenza può poi

passare ad attività riconducibili al cosiddetto *hacktivist*, *cyberterrorist* o, infine, diventare *cyberwarrior*.

Quest'ultimo, può sembrare un personaggio da fantascienza e se ne sente parlare poco, ma sulla base degli schematici elementi descritti in questo articolo non ne possiamo escludere l'esistenza. Le principali differenze tra *cyberterrorists* e *cyberwarriors* possono essere individuate nelle fonti di finanziamento e nel diverso tipo di impatto delle loro azioni sulla popolazione civile.

Esistono diversi studi[4] che mostrano come gli *hacktivists* hanno iniziato diversi anni fa ad utilizzare le nuove tecnologie come complemento alle loro azioni di protesta "tradizionale". Il passaggio da *hacktivist* a *cyberterrorist*, all'apparenza difficile, se non improbabile, è un punto critico che merita un approfondimento.

Chi può diventare un *cyberterrorist*? Potenzialmente, chiunque abbia a disposizione capacità, tempo e mezzi per approfondire le proprie conoscenze informatiche. Non dobbiamo dimenticare che anche nei Paesi in via di sviluppo ci sono individui che hanno accesso alla rete e sono dotati di una sufficiente conoscenza tecnica.

Il passaggio da *hacktivist* a *cyberterrorist* è relativamente facile ed è sostanzialmente basato su un unico fattore: la componente motivazionale. Che sia ideologico-politica, economico-finanziaria o religiosa, è sostanzialmente la componente motivazionale che porta un *hacktivist* a diventare un *cyberterrorist* e lo spinge ad usare gli stessi strumenti prima utilizzati per proteste di carattere civile, per provocare gravi disservizi che causano perdite di tempo e di danaro e forse, in un futuro, di vite umane. Tutto ciò può essere potenzialmente realizzato senza alcuna necessità di spostamento fisico della persona. Quante volte, nel terrorismo "reale", il terrorista

[4] S. BALDI (pseudonimo TARAS), *La protesta in marcia. Il caso del Vertice delle Americhe*, in *Limes*, 3, 2001.

si è rivelato la persona della porta accanto, la persona che conduceva una vita normale e che aveva invece una doppia vita? Questo sdoppiamento diventa ancor più semplice nel campo delle tecnologie informatiche, nel mondo virtuale. Chi ha specifiche capacità ed "*expertise*" può potenzialmente metterle a disposizione di gruppi impegnati in azioni terroristiche.

Un problema che merita particolare attenzione, a questo proposito, è quello legato alla presenza di un *malicious insider*, cioè di una persona che lavora in una determinata struttura/organizzazione/ufficio e che quindi dall'interno può compiere azioni che altri avrebbero difficoltà ad eseguire dall'esterno. Questi soggetti rappresentano un grave rischio, per l'evidente motivo che una "talpa" che si trovi in una buona posizione strategica, ha il privilegio di accedere a sistemi e ad altre informazioni non consultabili dall'esterno. Un *insider* ha maggiore facilità nell'acquisire una buona conoscenza del funzionamento del sistema in cui è inserito e soprattutto non ha bisogno di aggirare quelle barriere esterne (firewalls, reti private virtuali, etc.) che vengono ormai comunemente adottate nelle reti informatiche per proteggersi da attacchi esterni. Quante "talpe" informatiche, potenzialmente, possono essere presenti nella struttura di un'organizzazione complessa? È difficile dirlo, anche perché mentre per combattere il terrorismo "tradizionale" è possibile effettuare controlli fisici, quella della sicurezza informatica è una disciplina nuova, che necessita un approccio originale e maggiormente sofisticato. Una questione che rimane troppo sottovalutata dalla maggior parte delle organizzazioni.

4. Tipi di attacco informatico

Abbiamo brevemente visto che è relativamente facile passare da un uso proprio dei mezzi di protesta a disposizione di una società

civile ad un uso improprio, che si inquadra nell'ambito di quella società che abbiamo definito "incivile". È questo il caso di attacchi a reti e *server* di Istituzioni o società pubbliche o private che si vogliono, in qualche modo, ostacolare o combattere. Gli esempi sono molto numerosi. Il più comune e famoso di tali attacchi è sicuramente il *denial of service* (DOS), vale a dire il blocco degli accessi ad un determinato sito che si verifica quando tutti gli attivisti (o meglio *hacktivisti*) concordano sul collegarsi contemporaneamente ad un determinato sito. L'effetto è quello di sovraccaricare la linea fino a quando il *server* non è più in grado di operare e, come si dice in gergo, "cade", nel senso che non è più accessibile ad altri utenti per un certo periodo di tempo.

Un altro esempio di attacco molto semplice da realizzare che la maggior parte degli utenti ha avuto occasione di subire, e che può essere usato come strumento di protesta (ma spesso è utilizzato per finalità commerciali), è il fenomeno dello *spam*, vale a dire l'invio di enormi quantità di messaggi di posta elettronica. Lo si può definire un *soft attack*, vale a dire un attacco "leggero", ma non per questo meno efficace o invasivo. Se infatti si inviano migliaia di *e-mail* ad uno stesso indirizzo, non solo la specifica casella di posta elettronica presa di mira, ma anche tutte le altre caselle che risiedono sullo stesso servizio di posta risulteranno completamente bloccate: può accadere che per ore, talvolta per giorni, il servizio possa rimanere sospeso. Tenendo conto che la dipendenza dalla posta elettronica (anche in ambito lavorativo) è in continua crescita, oltre a comportare notevoli disservizi e ritardi, un blocco del servizio può produrre numerosi problemi e gravi conseguenze, anche economiche.

I potenziali tipi di attacco che si possono compiere sono molto diversi fra loro anche se considerati sotto il profilo "tecnico".

a) L'attacco *fisico* consiste, ad esempio, nella distruzione materiale di strutture informatiche di particolare interesse (come i

server o i *router* che assicurano il funzionamento di una rete). Questo può condurre, in particolare in assenza di opportune strutture di *back-up* (salvataggi di copie di riserva), a numerosi problemi dovuti alla perdita dei dati.

b) Ci sono tipi di attacco più sofisticati e più frequenti. L'attacco *sintattico* è ormai noto con il termine più generale e non sempre appropriato di "virus". Questo è un altro di quei problemi che la maggior parte degli utenti ha purtroppo avuto modo di sperimentare o subire personalmente. Le conseguenze di questo tipo di attacco, oltre che in termini di costi e di tempo, si misurano anche in termini di credibilità e fiducia.

c) Infine, meno frequenti e meno conosciuti sono gli attacchi *semantici*. Consistono nel nascondere all'interno di un programma una certa linea di istruzione che dopo un determinato periodo di tempo (ad esempio un anno), o quando viene eseguita una particolare operazione, avvia una data attività. Ipoteticamente un programma di amministrazione finanziaria potrebbe essere modificato in modo che, trascorso un anno a partire dalla prima esecuzione, vengano accreditati ad un determinato conto i centesimi (o millesimi) derivanti dalle approssimazioni delle operazioni effettuate. I pochi centesimi, che non si noteranno nelle singole operazioni di una grande struttura bancaria o finanziaria, in realtà arricchiranno l'autore di questa azione.

5. Attacchi ad infrastrutture critiche

Nel parlare di potenziali attacchi informatici, particolare attenzione deve essere rivolta a quelli che possono essere i possibili obiettivi, e tra questi quelle che sono comunemente definite "infrastrutture nazionali critiche". Si tratta di tutte quelle infrastrutture legate ai bisogni primari della società moderna (ad esempio acqua, elettricità, trasporti). Buona parte di queste attività

sono regolate da mezzi informatici. Si pensi alla rete di distribuzione dell'elettricità e a quanto avvenuto negli Stati Uniti nell'estate del 2003, quando una parte consistente della costa orientale del Paese rimase senza corrente a causa di una serie di guasti, amplificata dai sistemi informatici di controllo automatico.

Possiamo inoltre citare il regolamento del traffico aereo, oppure le transazioni finanziarie internazionali, o ancora i servizi di emergenza. Sono strutture o servizi quasi sempre completamente dipendenti da sistemi informatici complessi, nella maggior parte dei casi gestite da società private che nonostante non facciano sempre ricorso alla rete di *Internet* possono comunque essere oggetto di potenziali attacchi. Immaginiamo un attacco combinato che venga effettuato al sistema di controllo delle acque potabili: in una grande città potrebbero essere mischiate le acque nere e le acque bianche, accedendo ai sistemi informatici che ne regolano il servizio. È facile immaginare non solo le conseguenze di carattere sanitario, ma anche quelle di tipo psicologico con possibili fenomeni di panico collettivo o isteria diffusa.

Vanno quindi seriamente considerate soprattutto le potenziali ricadute, non solo in termini di vite umane, quanto in termini di turbamento all'ordine pubblico. Molte delle infrastrutture critiche hanno in realtà una caratteristica comune, quella di essere soggette all'effetto domino, per cui scatenando un problema in uno dei punti della struttura questi si ripercuote a catena anche altrove. Si pensi al traffico aereo: se si verifica un malfunzionamento al sistema di controllo in un determinato aeroporto, le conseguenze si estenderanno rapidamente anche agli altri aeroporti ad esso collegati[5].

[5] Purtroppo questo è stato il caso di quanto avvenuto negli aeroporti londinesi nel giugno 2004.

Non è questo il luogo per approfondire il concetto di *cyberwar*, che meriterebbe una trattazione a parte, ma certamente possiamo dire che si tratta di una potenziale evoluzione del *ciberterrorismo*. Possiamo idealmente parlare di *cyberwar* quando uno Stato utilizza i mezzi e le conoscenze informatiche a sua disposizione contro un altro Stato per sferrare attacchi mirati ad attività e centri di controllo (anche militari). È molto probabile che vi siano Paesi che stanno investendo sulla *cyberwar*, nonostante sia impossibile averne conferma e sapere in quale modo e con quali risultati.

Tuttavia è un dato di fatto che nei programmi di studio delle accademie militari americane, e non solo, siano previsti corsi specifici sulla guerra informatica. C'è quindi una percezione, negli ambienti militari, del possibile utilizzo dei mezzi informatici per finalità offensive o difensive. Quello che è interessante sottolineare è che, tenuto conto della natura e delle caratteristiche del fenomeno, sarà sempre più forte la necessità di far lavorare assieme, a fini costruttivi, persone molto diverse fra loro, come esperti *hackers* e militari. Le due conoscenze dovranno in qualche modo convergere e fondersi per far fronte o prevenire in modo efficace eventuali attacchi e per elaborare nuovi schemi difensivi.

6. Le asimmetrie dell'attacco informatico

La caratteristica comune a tutti i tipi di attacco informatico a cui finora abbiamo fatto riferimento, siano essi catalogabili come *hacktivism, cyberterrorism o cyberwar*, è quella di essere fenomeni caratterizzati da una asimmetria di fondo. Chi compie un attacco gode di vantaggi enormemente superiori rispetto a chi invece lo subisce. Tentando di schematizzare gli elementi di asimmetria presenti nel *ciberspazio*, possiamo individuare:

a) Il costo. I costi per organizzare un attacco informatico (pochi PC, alcuni strumenti di programmazione e conoscenze di base) sono molto limitati se confrontati con quelli necessari per costruire, rafforzare e rendere operativi i sistemi difensivi necessari. Chi compie un attacco ha necessità di infrastrutture relativamente modeste per metterlo in pratica, mentre chi deve difendersi deve dotarsi di infrastrutture decisamente complesse e costose. Si pensi semplicemente alla "questione virus": creare un virus, (o una sua variazione), e diffonderlo online è estremamente facile (più difficile è farlo in modo da non farsi individuare), proteggersi, invece, diventa sempre più complicato ed oneroso. Le reti devono avere un firewall costantemente aggiornato e soprattutto tutti i PC devono avere un programma di antivirus, anch'esso costantemente aggiornato. In organizzazioni particolarmente grandi e complesse tutto diventa ancora più impegnativo e difficile da gestire.

b) Il rischio. Chi compie un attacco, operando a distanza, affronta rischi minimi o nulli. Anche quando un *insider* è coinvolto in un attacco, questi può rimanere anonimo in tempi brevi per poi far perdere le proprie tracce. È quindi relativamente facile compiere un attacco ma è spesso molto difficile, da parte di chi lo subisce, determinare chi ne è l'artefice.

c) Le motivazioni di colui che attacca sembrano in genere essere molto più forti di colui che è tenuto a difendersi.

La sicurezza informatica può essere raffigurata come una catena costituita da vari anelli. Se questi anelli non sono tutti solidi e saldamente legati, la sicurezza del vostro PC, o di un PC che regola, ad esempio, i servizi idrici nazionali o i sistemi dedicati alle transazioni internazionali, è a rischio.

Gli anelli di questa catena sono idealmente quattro:

1. l'elaborazione di un sistema di sicurezza informatica;
2. la realizzazione di questo sistema;

3. lo sviluppo delle capacità di reazione ai problemi che si verificano;

4. la validazione del sistema, attraverso test e simulazioni.

Se uno solo di questi anelli è debole, l'intero sistema è a rischio e aumenta la possibilità di subire abusi e violazioni di vario tipo.

7. L'azione della Comunità internazionale

A livello internazionale, non si sta facendo abbastanza riguardo alla sicurezza informatica. In ambito ONU questa tematica è ancora ad uno stato molto iniziale di discussione essenzialmente per due motivi: in primo luogo, perché la percezione di chi dovrebbe occuparsi del problema è limitata, così come è limitata la conoscenza sull'argomento. In secondo luogo, perché l'attenzione mondiale è ora concentrata sui casi di terrorismo e di guerra "reale" (molto più eclatanti ed urgenti) che purtroppo comportano la perdita di molte vite umane. È una costante storica quella di prestare maggiore attenzione agli avvenimenti (o alle emergenze) a breve termine, rispetto a ciò che si sviluppa o si presenta come una tendenza di lungo periodo, per quanto preoccupante essa possa essere. L'unico passo concreto finora realizzato dalla comunità internazionale è quello del Consiglio d'Europa di Strasburgo che ha elaborato una convenzione sul *cybercrime*[6], il crimine internazionale compiuto attraverso le nuove tecnologie. A livello ONU, sono state approvate risoluzioni da parte dell'Assemblea Generale che contengono raccomandazioni su alcuni aspetti particolari della sicurezza informatica[7]. La maggior parte del lavoro, nonostante ciò, rimane

[6] La "*Convention on cybercrime*" è entrata in vigore l'1 luglio 2004.

[7] In particolare la risoluzione 58/32 su "Developments in the field of information and telecommunications in the context of international security" prevede la costituzione di un gruppo di esperti governativi nominati dal Segretario Generale dell'ONU, incaricati di individuare quelle misure necessarie per far fronte alle

ancora da fare. A tale proposito va ricordato il Vertice Mondiale sulle nuove tecnologie (WSIS) che ha avuto luogo a Ginevra nel 2003, e che continuerà i suoi lavori a Tunisi nel 2005. È auspicabile che in questo contesto ci si occuperà anche dei problemi della sicurezza internazionale e sarà importante mettersi d'accordo su cosa può e cosa non può essere accettato, e come individuare e trovare una soluzione a questi problemi.

L'analogia della tartaruga e della lepre, molto usata in ambito giuridico, può essere molto efficace per spiegare come la velocità con cui avanza la tecnologia rischia di far aumentare pericolosamente il divario esistente con l'attuale quadro giuridico di riferimento. È quindi auspicabile che la comunità internazionale inizi presto ad occuparsi seriamente della questione della sicurezza informatica e delle molteplici conseguenze che ad essa sono legate.

---

minacce esistenti nell'ambito della sicurezza dell'informazione e delle telecomunicazioni.

APPENDICE

Tabella riassuntiva dei tipi attacchi e dei gruppi di aggressori

Gruppo	Motivazione	Tipo di attacco	Casi riportati (selezione)
Script kiddy	*Hackers* privi di esperienza	Usano programmi pronti all'uso e codici scaricati da *Internet*	Casi frequenti contro utenti privati o aziende
Hacker	*Hackers* con maggiore esperienza - Tentano di introdursi in nuovi sistemi difensivi - Ritorno economico (talvolta)	Strumenti automatici più sofisticati. Possono organizzare attacchi coordinati. Danno potenziale: medio-alto.	Come per lo *script kiddy* - Danneggiamenti - *Denial of Service (DoS)* - Casi di attacchi organizzati contro grandi compagnie e istituzioni - Attacco DDoS contro Yahoo!, *eBay* e CNN (febbraio 2000)
Malicious insider	- Vendetta - Estorsione e ricatto	Azione illegale attraverso un pieno accesso ai sistemi di informazione. Danno potenziale: medio-alto.	Società ed istituzioni hanno subito questo tipo di attacco. Caso del sistema di fogne australiano (2000).
Hacktivist	- Propaganda - Politica - Socio-economica - Religiosa	Stesso di *script kiddy* e *hacker* ma per motivazioni differenti. Pericolo potenziale: medio-alto. Il costo definitivo di un attacco è generalmente maggiore per obiettivi commerciali che per le istituzioni.	Da Seattle (1999) in poi, i contestatori hanno spesso combinato le proteste tradizionali con attacchi in rete. - Conflitto di hackers israelo-palestinese (1999-2002) - Schermaglie tra *hackers* cinesi e americani (maggio 2001)
Cyber-terrorist	-Propaganda -Politica economica -Minaccia alla sicurezza nazionale -Spionaggio	Potenziali attacchi a Infrastrutture Nazionali Critiche (CNIs): centrali elettriche, oleodotti e gasdotti, reti idriche, traffico aereo, sistemi bancari. Danno potenziale: alto.	Nessun caso ufficialmente riportato.
Cyber-warrior	- Attività di *intelligence* politica ed economica - Sottrazione di segreti commerciali - Interferenza nell'attività delle infrastrutture critiche	Stesso del *cyber-terrorist*	Nessun caso ufficialmente riportato