

Information Warfare

**Le nuove minacce
provenienti dal cyberspazio
alla sicurezza nazionale
italiana**

**a cura di Umberto Gori
e Luigi Sergio Germani**

FrancoAngeli

I lettori che desiderano informarsi sui libri e le riviste da noi pubblicati possono consultare il nostro sito Internet: www.francoangeli.it e iscriversi nella home page al servizio "informazioni" per ricevere via e-mail le segnalazioni delle novità o scrivere, inviando il loro indirizzo, a: "FrancoAngeli, viale Monza 106, 20127 Milano".

Information Warfare

**Le nuove minacce
provenienti dal cyberspazio
alla sicurezza nazionale
italiana**

**a cura di Umberto Gori
e Luigi Sergio Germani**

FrancoAngeli

La Conferenza è stata ideata dal Centro di Studi Strategici e Internazionali dell'Università di Firenze (CSSI), dalla Link Campus University, dal Centro Studi "Gino Germani" e dall'Istituto di Studi di Previsione (ISPRI) d'intesa con Maglan Europe, realtà leader internazionale nell'auditing e consulting per la Difesa delle informazioni in ambito civile, militare e governativo.



Un ringraziamento particolare va alla dottoressa Anna Casodi e alla dottoressa Alessandra Russo per l'editing del volume

Copyright © 2011 by FrancoAngeli s.r.l., Milano, Italy

L'opera, comprese tutte le sue parti, è tutelata dalla legge sul diritto d'autore. L'Utente nel momento in cui effettua il download dell'opera accetta tutte le condizioni della licenza d'uso dell'opera previste e comunicate sul sito www.francoangeli.it.

Indice

Prefazione , di <i>Vincenzo Scotti</i>	pag.	9
Lettera al Convegno della Presidenza della Repubblica , di <i>Donato Marra</i>	»	11
Introduzione. Le nuove sfide alla sicurezza dello spazio cibernetico , di <i>Paolo Campobasso</i>	»	13
Documento di sintesi della conferenza , di <i>Luigi Sergio Germani</i>	»	23
Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici , di <i>Umberto Gori</i>	»	31
Spionaggio industriale computerizzato e sicurezza nazionale , di <i>Paolo Lezzi</i>	»	39
Profilo delle minacce cibernetiche e ruolo della comunità intelligence nella protezione del sistema-Paese , di <i>Pasquale Piscitelli</i>	»	45
Cyber Warfare: un nuovo fronte per le Forze Armate , di <i>Nicola Gelao</i>	»	53
La minaccia strategica esterna di Infowar/Cyber War alla sicurezza nazionale , di <i>Paolo Scotto di Castelbianco</i>	»	59

Sicurezza informatica condivisa e protezione delle Infrastrutture Critiche nazionali da potenziali attacchi di <i>Cyber Warfare</i> , di <i>Domenico Vulpiani</i>	pag.	67
	»	81
La crescente rilevanza della guerra cibernetica , di <i>Ferdinando Sanfelice di Monteforte</i>		
<i>Cyberspace</i>: rischi ed opportunità negli scenari futuri , di <i>Massimo Pettoni</i>	»	89
Protezione delle Infrastrutture Critiche a livello nazionale e iniziative europee in materia di <i>Information Warfare</i> , di <i>Luisa Franchina</i>	»	95
Il sistema delle imprese e le minacce informatiche alla sicurezza nazionale , di <i>Giancarlo Galli</i>	»	107
Il nuovo <i>Information Warfare Battlespace</i>: l'impatto delle nuove tecnologie , di <i>Antonio Colella</i>	»	111
La <i>Cyber Defence</i> a garanzia della capacità di comando e controllo della Difesa , di <i>Catello Somma</i>	»	120
I dilemmi nelle operazioni <i>NetInt</i> nell'ambito della <i>Information Warfare</i> , di <i>Shai Blitzblau</i>	»	125
<i>Information Warfare</i> e sicurezza del sistema economico-finanziario nazionale: cenni su alcuni ambiti di intervento della Banca d'Italia , di <i>Tommaso Giacomino</i>	»	133
<i>Cyber Security</i> e <i>Cyber Espionage</i>: l'esperienza delle Poste Italiane , di <i>Stefano Grassi</i>	»	139
Attacchi informatici e attivazione di strutture dedicate all'<i>Infowarfare</i> , di <i>Gerardo Iovane</i>	»	150
Analisi tecnica delle capacità <i>NetINT</i> dei gruppi terroristici , di <i>Shai Blitzblau</i>	»	175
Riferimenti bibliografici	»	181

Sitografia di riferimento	pag.	185
Documenti di riferimento	»	185
Lista degli acronimi	»	187
Indice analitico	»	191

Prefazione

di *Vincenzo Scotti* *

Lo spazio cibernetico è un nuovo campo di battaglia e di competizione geopolitica nel XXI secolo. La rivoluzione nel campo delle tecnologie dell'informazione e della comunicazione (la cosiddetta “terza rivoluzione industriale”) sta trasformando la natura del potere e delle relazioni internazionali. Tale trasformazione determina nuovi tipi di conflittualità e nuove forme di minaccia alla sicurezza degli Stati e del sistema internazionale. La comprensione dei rischi inediti derivanti dal cyberspazio rappresenta una grande sfida intellettuale, a livello mondiale, per decisori politici, comunità d'intelligence, forze armate, forze di polizia, sistema imprenditoriale e mondo accademico. I maggiori esperti internazionali in materia ritengono che non si è ancora raggiunta una piena comprensione della natura della nuova minaccia e delle sue implicazioni.

La sfida del futuro è sia teorica che *strategica*. Gli esperti sono consapevoli della necessità di elaborare una visione strategica di ampio respiro per fronteggiare i fenomeni di conflittualità e minaccia derivanti dall'uso di strumenti di aggressione cibernetica. Nonostante la crescente attenzione che governi, aziende e mondo accademico e della ricerca stanno dedicando alla *Cyber Security*, ancora manca una strategia chiara e coerente.

Come afferma Richard Clarke nel suo recente libro “*Cyber War*” le sfide che oggi la comunità internazionale è chiamata a fronteggiare nel campo della sicurezza nel cyberspazio sono analoghe, per alcuni aspetti, a quelle che emersero con l'avvento delle armi nucleari. In una prima fase non vi era una chiara strategia di sicurezza atta a gestire i pericoli degli armamenti nucleari. Successivamente, dietro l'impulso del Presidente degli Stati Uniti John F. Kennedy e l'allora Segretario della Difesa Robert McNamara, diverse Università e centri di ricerca statunitensi contribuirono all'elaborazione di una chiara visione strategica in campo nucleare, fondata

* Sottosegretario di Stato, Ministero degli Affari Esteri e Presidente della Link Campus University.

sul concetto centrale di *deterrenza* e su altri importanti concetti, come quello del controllo e la limitazione degli armamenti nucleari.

Nei decenni successivi, tale strategia diede un importante contributo al fine di prevenire l'insorgere di un conflitto nucleare tra le superpotenze.

È evidente che, accanto alle similarità, vi sono importanti differenze fra i problemi della sicurezza nucleare che caratterizzarono l'epoca bipolare e quelli della *Cyber Security* nel XXI secolo. Va tenuto presente, infatti, che un attacco cibernetico non ha un impatto distruttivo di massa paragonabile a un attacco nucleare. Tuttavia, un'aggressione cibernetica potrebbe potenzialmente paralizzare un intero Paese colpendo le sue Infrastrutture Critiche. Inoltre, il fenomeno crescente del *Cyber Espionage* economico-industriale (sponsorizzato da determinati Stati) è in grado di insidiare la sicurezza e la competitività dei sistemi economici di Paesi industriali avanzati. Una nuova visione strategica per contrastare le minacce cibernetiche non potrà basarsi sul concetto di deterrenza: il modello tradizionale della deterrenza non è applicabile ai conflitti nel cyberspazio, dove risulta estremamente difficile individuare in tempi utili l'autore di un attacco. Tale prospettiva strategica dovrebbe comunque prevedere lo sviluppo di una specifica normativa internazionale per il controllo e la limitazione delle "armi cibernetiche", di cui un crescente numero di Stati si sta dotando (tanto che si parla di "potenze informatiche" emergenti).

L'elaborazione di una strategia per la sicurezza nel cyberspazio richiederà una crescente collaborazione internazionale e nuove sinergie fra governi, imprese e mondo accademico e della ricerca scientifica. Le Università e i centri di eccellenza non-governativi sono chiamati a svolgere un ruolo molto importante in questo processo di riflessione ed elaborazione strategica.

Inoltre, si renderà sempre più necessario potenziare la ricerca scientifica e tecnologica nel campo della *Cyber Security*, la formazione di ricercatori e tecnici in questo settore, le iniziative atte a favorire una maggiore conoscenza e consapevolezza tra i decisori politici e aziendali circa i rischi per la sicurezza provenienti dal cyberspazio. Le università dovranno assumere un ruolo importante in questo sforzo.

Lettera al Convegno della Presidenza della Repubblica¹

Gentile Professore,

la ringrazio per aver informato il Presidente della Repubblica dello svolgimento della Conferenza «Information Warfare: le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana», in programma a Roma il 6 e 7 ottobre 2010.

Il Capo dello Stato esprime a lei, e per il suo cortese tramite, all'Onorevole Scotti, al Professor Germani, agli istituti e agli studiosi che hanno concorso alla fare progettuale e organizzativa del convegno il suo convinto apprezzamento per le finalità dell'iniziativa che costituisce – per l'ampiezza degli argomenti, l'autorevolezza dei relatori e la qualità dei contributi – un'importante sede di riflessione e confronto su temi di stringente attualità e rilevanza.

Oggetto di crescente attenzione dei governi e della Comunità internazionale, le numerose e complesse questioni legate alla *Cyber Defense* confermano l'esigenza di rafforzare in ogni suo aspetto la sicurezza nella gestione dei flussi informativi da parte di tutte le strutture pubbliche e private.

Nell'auspicio che dalla Conferenza possano emergere nuovi e più efficaci indirizzi di analisi, progettuali e operativi, sviluppando le importanti indicazioni fornite dal Comitato Parlamentare per la Sicurezza della Repubblica, il Presidente Napolitano rivolge ai partecipanti un sentito augurio di buon lavoro e un cordiale saluto, cui unisco il mio personale.

Donato Marra
Segretario generale
della Presidenza della Repubblica

¹ Lettera inviata dal Quirinale al Prof. Umberto Gori.

Patrocini

Senato della Repubblica
Camera dei Deputati
Presidenza del Consiglio dei Ministri
Ministero degli Affari Esteri
Ministero della Difesa
Ministero dell'Interno
Ministero dell'Economia e delle Finanze
Polizia di Stato

Promotori

Link Campus University
Centro universitario di Studi Strategici e Internazionali (CSSI)
Centro Studi "Gino Germani"
Istituto per gli Studi di Previsione e le Relazioni Internazionali (ISPRI)

Ideata d'intesa con Maglan - Information Defense & Intelligence

Sponsor

UniCredit Group
IBM
Booz & Co.
Trend Micro
Selex Communications (Gruppo Finmeccanica)
Geotechnos
Beta 80 Group

Introduzione. Le nuove sfide alla sicurezza dello spazio cibernetico

di *Paolo Campobasso**

L'edizione 2010 della Conferenza Annuale sulla *Information Warfare* – per la prima volta in Italia – si è tenuta il 7 ottobre a Roma EUR presso la Sala Conferenze di UniCredit.

L'evento ha rappresentato una grande opportunità di incontro e di confronto grazie alla quale è stato possibile vedere riuniti l'intelligence, le FFAA, le autorità governative e le grandi Aziende private, per discutere e analizzare il tema ampio e in continua, rapidissima evoluzione dell'*Information Warfare*, cioè la guerra dell'Informazione e capire insieme:

- come si è evoluta;
- quali sono le nuove reali minacce del cyberspazio;
- su quali livelli si assesta il pericolo;
- “se” e “in che modo” le singole nazioni - così come i grandi gruppi e le multinazionali – possono prevenire gli attacchi e difendere i propri cittadini e i propri *asset*.

Il convegno si è proposto due obiettivi di fondo:

1. approfondire la comprensione ed aumentare la consapevolezza, tra i decisori politici ed aziendali italiani, delle minacce cibernetiche e di *Information Warfare* alla sicurezza nazionale, nonché delle più efficaci contromisure e strategie per contrastare e contenere le minacce.

2. riunire esperti ed analisti provenienti da organismi governativi civili e militari, dal mondo dell'impresa, dalle università ed i centri di ricerca scientifica, per dare un contributo innovativo di idee e proposte utili all'elaborazione di una strategia italiana nazionale nel campo

* Senior Vice President, Group Chief Security Officer, UniCredit SpA.

dell'*Information Warfare*, della *Cyber Defence*, e della *Network Intelligence*.

Un'intera – e intensa – giornata dedicata alle tematiche complesse legate a criticità in continua evoluzione: si tratta di battaglie o meglio di “partite” che i governi e i grandi gruppi privati giocano sul tempo. È facile intuire come probabilmente anche in questo momento ci siano organizzazioni (o singoli) che per gioco, per denaro, per ragioni politiche o militari, stanno “studiando” soluzioni che consentano di aggirare le barriere che sono state erette a protezione di coloro che per i governi e le istituzioni sono “cittadini”, e per le aziende “clienti”.

Vince quindi chi anticipa il pericolo, chi parte dal presupposto che non esistono soluzioni definitive, che ogni barriera è sormontabile...che è solo una questione di tempo.

Per questo l'evento è stato accolto con grande successo. Perché c'è la consapevolezza che la società attuale sia caratterizzata da una forte informatizzazione e interconnessione dei servizi che, se da un lato hanno portato a indubbi benefici, dall'altro hanno reso i servizi stessi vulnerabili a tipologie di attacchi sempre nuovi, con impatti potenzialmente enormi, che molto spesso non sono misurabili se non a posteriori.

Pensiamo ad esempio all'infrastruttura digitale globale che, pur garantendo la possibilità di trasmettere le informazioni su differenti percorsi (permettendo l'utilizzo di strade alternative in caso di interruzione di quelle primarie) presenta alcuni punti ad elevata vulnerabilità:

- circa il 90% del traffico transita su canali in fibra ottica sul fondo oceanico, che si riuniscono in pochi nodi (i principali sono dislocati vicino a New York, Mar Rosso e Luzon Strait nelle Filippine).
- il traffico in Internet è gestito da solo 13 *cluster* di *Domain Name Server*.
- la crescente connettività di Stati in cui non è presente una legislazione in materia di sicurezza informatica crea nuovi “terreni fertili” per i criminali informatici.

Nel corso della giornata i relatori provenienti dal mondo civile e militare hanno presentato analisi, dati, studi, esperienze per capire meglio lo scenario in cui viviamo e lavoriamo, trattando il tema dell'*Information Warfare* da diversi punti di vista, passando dalle grandi minacce su scala globale ai pericoli quotidiani che possono riguardare le nostre singole vite private

come la tutela della privacy, il furto di identità o la clonazione delle carte di pagamento.

La guerra dell'informazione si combatte nel "non-spazio" e pertanto non sempre ha contorni ben definiti. Il "nemico" è difficile da identificare e persino il confine fra legalità e illegalità a volte sfugge.

La giornata dei lavori è stata articolata in tre sessioni:

1. *Information Warfare* e Sicurezza Nazionale Italiana: la prospettiva strategica"

2. "Operational Information Warfare: metodologie offensive e difensive, tecniche e tecnologie"

3. "Information Warfare e Cyber-Spionaggio Economico Industriale: minacce all'economia nazionale e ad alle aziende strategiche"

I temi principali trattati nel corso della conferenza sono stati i seguenti:

- *Cyber War*
- *Cyber Terrorism* (a cui sono riconducibili anche la sovversione e la propaganda)
- *Cyber Espionage*
- *Cyber Crime*

Cyber War

I miei trascorsi a Modena, dove ho iniziato l'Accademia Militare nel 1983, mi fanno ricordare l'epoca in cui al concetto di guerra era possibile associare solo tre aree di intervento possibili: terra, acqua e cielo.

Oggi indubbiamente le cose sono cambiate radicalmente.

Già da tempo lo scenario tecnologico della società moderna ha indotto a considerare il cyberspazio come un nuovo campo di battaglia in cui è possibile causare gravi danni alle nazioni o alle entità "nemiche", es. tramite attacchi (principalmente *DoS* o intrusioni) diretti ai sistemi informativi e alle infrastrutture tecnologiche vitali, finalizzati a comprometterne la disponibilità e/o causare malfunzionamenti dei servizi.

Nell'ambito della *Cyber War* sono inoltre emerse tecniche di "Information Operation", consistenti nell'utilizzo dei mezzi di comunicazione per influenzare l'opinione pubblica con informazioni tendenziose.

La *Cyber War* implica però conseguenze di tipo politico, legale e militare:

- uno Stato non può essere certo degli esiti di un attacco digitale, che potrebbe coinvolgere sistemi appartenenti a entità neutrali o diffondersi presso la propria infrastruttura informatica (es. virus fuori controllo);
- la difficoltà nell'individuare l'origine certa di un attacco informatico rende più difficile giustificare eventuali controffensive e comporta il rischio di errori di valutazione;
- non sono ben chiare le modalità di entrata in guerra (quando un attacco informatico può essere considerata un'azione di guerra? Uno Stato della NATO deve entrare in guerra contro un'altra nazione sospettata di aver attuato un attacco informatico verso un alleato?)

Nell'ambito della *Cyber War* risulta inoltre arduo siglare trattati internazionali, a causa della difficoltà di quantificare ed individuare le armi informatiche. Al più gli Stati o le organizzazioni internazionali possono stabilire accordi informali per aumentare il costo politico ed economico in caso di cyber-attacchi (es. dichiarazione simile alla convenzione di Ginevra che metta al bando attacchi informatici diretti verso infrastrutture civili, attuazione di pressioni economiche verso gli stati che non adottano adeguate misure per fronteggiare il crimine online, etc.).

Tra gli Stati più attivi nell'ambito della *Cyber War* si segnalano l'Iran, la Federazione Russa e la Corea del Nord (che ha creato una scuola per l'addestramento di "cyber-soldati").

Gli Stati Uniti hanno invece creato un "*Cyber Command*" con finalità di difesa delle proprie infrastrutture e attacco dei sistemi informativi di possibili nemici.

Nonostante i possibili impatti, ad oggi le armi informatiche, date le difficoltà di controllo e le implicazioni di carattere politico/legale, vengono utilizzate solo in ambiti ristretti (es. per interruzione temporanea delle comunicazioni o dell'accesso a siti istituzionali).

E a tal proposito desidero citare un articolo pubblicato lo scorso settembre dal «Corriere della Sera» in merito ad un attacco informatico ai danni di migliaia di computer in Iran infettati da un misterioso "baco", compresi quelli dello staff all'impianto nucleare di Natanz.

"Un attacco informatico che gli esperti ritengono sia stato lanciato non da hacker ma da un'intelligence.

E dicendo questo gli stessi esperti sospettano un coinvolgimento di un Paese storicamente avverso alle politiche iraniane, deciso ad ostacolare con ogni mezzo la ricerca atomica degli ayatollah. Il primo allarme risale alla metà di giugno, quando una piccola società bielorusa segnala la presenza di un virus maligno, costruito per paralizzare lo *Scada*, un sistema computerizzato che può gestire grandi

complessi industriali, fabbriche, oleodotti e siti militari. In particolare il «baco» sembra essere stato «allevato» per distruggere i programmi usati dalla compagnia tedesca Siemens che ha venduto i suoi prodotti agli iraniani. Dalla metà di giugno il fronte si è allargato infettando decine di migliaia di computer in Iran e, in misura minore, in Indonesia. Pochi giorni fa le autorità iraniane hanno ammesso dei problemi, anche se hanno escluso che sia stato coinvolto l'impianto di Natanz. Soltanto i PC dello staff – hanno spiegato – hanno subito l'assalto esterno. Ed un alto funzionario ha ipotizzato una manovra straniera. Il ricorso al «baco» non è una sorpresa per gli analisti dell'intelligence. Nel 2008, fonti accreditate hanno rivelato che un famoso servizio di intelligence aveva lanciato un programma di sabotaggio dei siti atomici iraniani. Un'operazione condotta su più livelli. Il primo prevedeva la vendita a Teheran – attraverso società ombra create in Occidente – di tecnologia fallata o contenente «virus» programmati per esplodere nei sistemi più avanti nel tempo. Il secondo livello, invece, consisteva in attacchi informatici diretti.

Un anno dopo emergevano informazioni su un progetto «top secret» autorizzato dal presidente Usa Barack Obama e che contemplava incursioni elettroniche contro il progetto dei mullah. L'operazione «baco» dunque, sarebbe solo la coda di un'offensiva ben più ampia. E tecnici occidentali aggiungono che il vero bersaglio sia il «Sadac» che coordina le centrifughe per l'arricchimento dell'uranio a Natanz. Altri non escludono un secondo target: la nuova centrale di Busher, attivata con l'assistenza dei russi. Già nei mesi precedenti Teheran aveva ammesso ritardi e problemi tecnici nella ricerca. Non solo. Ali Ashtari, ufficiale dei pasdaran incaricato degli acquisti di tecnologia, è stato giustiziato con l'accusa di aver collaborato con un'agenzia di intelligence straniera.

Per le autorità avrebbe favorito i sabotaggi. Nell'estate del 2009, poi, diversi alti funzionari dell'ente atomico iraniano sono stati sostituiti dopo un misterioso incidente a Natanz. Oltre a Israele – aggiungono fonti americane – altri Paesi sono in grado di lanciare temibili «missili informatici». Gli Stati Uniti, che di recente hanno ampliato le strutture per la *Cyber War*, i cinesi, che dispongono di un poderoso apparato dell'esercito nel Guangdong, i francesi e i russi”¹.

Cyber Terrorism/Cyber Subversion

Gli attacchi informatici in precedenza descritti possono essere utilizzati anche dalle organizzazioni terroristiche per colpire gli Stati e gli organismi istituzionali antagonisti. Ovviamente le organizzazioni terroristiche non dispongono della “potenza di fuoco” degli Stati nazionali, ma agendo al di fuori delle convenzioni internazionali, non sono soggetti a vincoli e deterrenti di tipo legale, politico o morale. Inoltre l'economicità delle armi informatiche ne rende facile l'acquisizione.

¹ Olimpio G (2010). *Iran: attacco informatico contro i pc degli impianti nucleari, sospetti su Israele*, «Corriere della Sera», 26 settembre.

Tuttavia, ad oggi, le organizzazioni terroristiche sono maggiormente interessate a perpetrare attacchi utilizzando le armi convenzionali (gli attentati hanno un impatto mediatico decisamente superiore rispetto agli attacchi informatici), utilizzando la tecnologia principalmente per fini propagandistici (es. le tristemente note immagini dall'Iraq) o come mezzo di divulgazione per fare proseliti.

I gruppi terroristici hanno inoltre appreso e sfruttato le potenzialità di Internet come mezzo di coordinamento tra le varie cellule sparse per il mondo, al fine di pianificare e preparare attentati, oltre che fornire materiale “formativo” agli affiliati. Ad esempio i gruppi jihadisti fanno largo uso di chat o siti Web, che sono spesso in lingua inglese per poter diffondere le proprie ideologie anche presso le comunità islamiche presenti da anni e integrate negli Stati occidentali.

Paradossalmente anche alcuni meccanismi di sicurezza possono essere sfruttati dai gruppi terroristici per i propri fini; si pensi all'utilizzo della crittografia per rendere indecifrabili i messaggi scambiati su Internet. Le armi informatiche vengono spesso utilizzate anche da gruppi di attivisti (*Hactivism*). Le azioni effettuate da tali gruppi sono principalmente rivolte a utilizzare le reti di telecomunicazioni a fini propagandistici (es. tramite blog, community, siti tematici) e per azioni dimostrative, come attacchi di tipo *Denial of Service* o *Defacing* diretti ai siti istituzionali delle entità avverse (es. siti governativi, siti di aziende).

Un curioso metodo di *Information Warfare* utilizzato nell'ambito dell'attivismo è costituito dal “*Google Bombing*”, che consiste nell'alterare i risultati delle ricerche di Google creando (es. sui blog) un elevatissimo numero di link diretti al sito che si vuole attaccare e associando ai link stessi le parole di ricerca con cui si vuole far apparire la pagina attaccata. Tal metodo è tipicamente utilizzato per screditare singoli individui o organizzazioni, facendo comparire le pagine personali degli stessi in risposta a ricerche su termini diffamatori.

Cyber Espionage

Lo spionaggio elettronico (*Cyber Espionage*) consiste nell'intrusione, principalmente utilizzando tecniche di *hacking* o *social engineering* (comuni anche nel *Cyber Crime*), nei sistemi di concorrenti economici o nazioni rivali per ottenere informazioni riservate, che possono portare ad un vantaggio competitivo a livello economico o tecnologico (es. sviluppo di nuove apparecchiature militari). Tali azioni possono essere svolte da indivi-

di indipendenti, gruppi organizzati, o coordinate da organi statali (es. si hanno concreti sospetti su attività di spionaggio commissionate dalla Cina).

Le azioni di *Cyber Espionage* non si limitano alla sola intrusione illecita nei sistemi degli enti antagonisti, ma sovente sfruttano tecniche di tipo silente, monitorando il traffico ordinario su Internet o le e-mail non classificate, che spesso contengono informazioni riservate. Altre tecniche prevedono l'abbandono di chiavi USB o altri supporti di memorizzazione contenenti software malevoli in luoghi frequentati da persone che potrebbero trattare dati riservati (es. parcheggi di aziende concorrenti), in attesa che qualcuno le raccolga e le connetta al proprio PC.

Cyber Crime

Il *Cyber Crime* consiste nell'attuare operazioni illegali principalmente su Internet, sfruttando informazioni (per lo più legate all'identità digitale degli utenti) recuperate in modo illecito.

Le tecniche "storiche" per recuperare i dati includono le intrusioni di hacker e l'uso di *malware* (virus, trojan, worm...). Negli ultimi anni si sono però diffusi gli illeciti legati all'abuso dei diritti di accesso alle informazioni aziendali da parte di dipendenti infedeli e l'utilizzo di tecniche di *social engineering* quali il *phishing*. In particolare sono in crescita i casi di *phishing* mirato, focalizzato verso i dipendenti che hanno accesso ai database contenenti informazioni aziendali riservate (es. credenziali, numeri di carte di credito). Generalmente il contatto verso i dipendenti avviene via mail o per telefono.

I casi di furto di dati sono per lo più riconducibili alla criminalità organizzata (l'84%, prevalentemente dell'Europa dell'Est). Questi però intervengono direttamente solo nel 24% dei casi di furto, mentre di solito agiscono per interposte persone, reclutate su Internet e generalmente non coinvolte nella frode finale. La facilità di reclutamento è dovuta al fatto che i collaboratori delle organizzazioni criminali sono comuni utenti attratti dalla possibilità di ottenere facili guadagni, che non hanno generalmente reale percezione dell'illegalità delle proprie azioni.

Negli ultimi anni si sono diffuse diverse tipologie di comunità criminali online, che sfruttano *chat room* e forum per comunicare tra loro, condividere informazioni recuperate illecitamente e strumenti per condurre attacchi informatici. Tali comunità possono essere costituite da gruppi di persone provenienti dalla stessa area geografica e che si conoscono personalmente, oppure possono comprendere individui distribuiti su tutto il globo che sono