Computer Science and War: CyberWarfare and CyberTerrorism

Zennaro, Fabio Massimo

20 dicembre 2008

Sommario

Questo documento consiste in una breve introduzione sul moderno connubio tra guerra ed informatica. Si analizza innanzitutto il fenomeno della cyberwarfare, spiegando cosa sia, come sia nata, quali siano i suoi principi ed i suoi metodi. Nella seconda parte si esamina l'uso della cyberwarfare nel contesto della guerra al terrore, ovvero come si sia evoluto il cyberterrorism e quali siano le sue potenzialità. Nella terza sezione si illustrano le tecniche che sono state sviluppate per far fronte a cyberwarfare e cyberterrorism. Nella quarta sezione, per dimostrare la realtà di quanto spiegato fin a questo punto, si presenta un insieme di casi di studio, ovvero quelli che potrebbero considerarsi i primi esempi di cyberwarfare e di cyberterrorism. Nella quinta sezione si riportano alcune considerazioni di carattere etico, legale e politico riguardo a cyberwarfare e cyberterrorism. Infine, nell'ultima sezione si offrono delle riflessioni conclusive su quelle che in futuro potranno essere cyberwarfare e il cyberterrorism.

Indice

1 Cyberwarfare

1.1 War Games, ovvero una definizione di Cyberwarfare

La cyberwarfare è oggi una realtà bellica riconosciuta e studiata; già a metà degli anni '90 l'apparato militare statunitense riconosceva l'importanza e la criticità della cyberwarfare nei futuri conflitti e nel giugno del 2000, prima di dare nuovo impulso ad una riforma delle forze armate in questa direzione, il generale dell'Esercito statunitense Hugh Shelton dichiarava [12]:

> "the continued development and proliferation of information technologies will substantially change the conduct of military operations."[1].

La consapevolezza dell'esistenza della cyberwarfare è dunque chiara e ben radicata; altrettanto non si può però dire riguardo ad una precisa definizione di cosa sia la cyberwarfare. La difficoltà principale viene dal definire cosa sia il cyberspace [22], ovvero lo spazio, il contesto, il campo in cui la cyberwarfare dovrebbe avere luogo. Una possibile definizione di cyberspace è stata proposta nel 2006 da una task force dell'Aeronautica Militare statunitense [5]:

> "a warfighting domain bounded by the electromagnetic spectrum."[2].

L'obiettivo della cyberwarfare sarebbe dunque quello di "dominare lo spettro elettromagnetico" [9]. La stessa task force responsabile di questa definizione ha confessato però che [5]:

> "a full understanding of the domain is years away." [3].

Una definizione più pratica di cyberwarfare è offerta da L.J. Janczewski e A.M. Colarik in [10]:

> "information warfare is defined as a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses." [4].

Partendo da questa proposta, in questo documento, si considereranno come atti di cyberwarfare azioni dirette contro un sistema informatico volte ad interferire con il suo corretto funzionamento, così come previsto dal suo programmatore; si considereranno poi solo attacchi portati per mezzo di sistemi informatici, tralasciando attacchi di tipo cinetico (e.g.: bombardamento di impianti informatici) e di tipo elettromagnetico (e.g.: impulsi elettromagnetici d'altitudine)

[1] "il continuo sviluppo e diffusione delle tecnologie dell'informazione cambierà sostanzialmente il modo di condurre operazioni militari." (trad. propria).

[2] "un dominio di guerra delimitato dallo spettro elettromagnetico." (trad. propria).

[3] "per una piena comprensione del dominio ci vorranno ancora anni." (trad. propria).

[4] "cyberwarfare è definita come un attacco pianificato da parte di una nazione o di suoi agenti contro sistemi informatici, programmi e dati che risultano in perdite per il nemico." (trad. propria).

[22]. Inoltre per parlare di cyberwarfare sarà necessario il coinvolgimento di uno stato nazionale: ciò che distingue un comune cyber attack sulla Rete da un caso di cyberwarfare è l'appoggio, diretto o indiretto, durante l'attacco di uno stato nazionale contro un altro stato nazionale; è richiesto quindi che vi sia una volontà ed una progettualità da parte di uno stato per usare un simile attacco a livello militare e politico contro un altro stato.

1.2 Dal Campo alla Rete, ovvero come la guerra si è evoluta verso la Cyberwarfare

Le guerre cui si è assistito negli anni recenti hanno messo in luce come i metodi di combattere siano oggi più che mai cambiati e lontani dall'ormai vecchio concetto di un confronto sul campo tra forze convenzionali. Nell'evoluzione bellica di questi ultimi decenni si possono distinguere due importanti tendenze, tra loro apparentemente opposte, ma che hanno nelle tecnologie dell'informazione un fondamento comune: il concetto di network centric warfare e il concetto di asymmetric warfare.

1.2.1 Network Centric Warfare

Il concetto di una network centric warfare o di un network centric warrior è quello di sviluppare un apparato bellico che garantisca sistemi di comando e controllo efficienti, massima consapevolezza situazionale, armamenti precisi e rapidi. Queste idee e concetti sono già stati ampiamente sviluppati e sono stati messi in campo a partire dall'invasione dell'Iraq nel 1990 fino alla più recente invasione sempre dell'Iraq nel 2003.

Network Centric Warfare L'obiettivo della network centric warfare propriamente detta è quello di guadagnare una superiorità di informazione sugli avversari, sia sul campo di battaglia (per aumentare la letalità e la sicurezza dei propri soldati) sia in ambito civile (per poter manipolare l'opinione civile attraverso operazioni psicologiche mirate). Per ottenere questi scopi, è necessario un massiccio utilizzo delle più moderne tecnologie dell'informazione: dalla creazione di reti peer-to-peer altamente ridondanti e robuste all'uso della criptazione per proteggere le proprie comunicazioni, dall'uso di satelliti al controllo delle reti pubbliche [9].

Future System Combat I principali sostenitori di questo nuovo approccio alla guerra sono innanzitutto le potenze militari del Primo Mondo, le uniche dotate delle competenze tecnologiche e delle risorse finanziarie necessarie per rivoluzionare i propri eserciti secondo questo nuovo paradigma. I massimi fautori di tale riorganizzazione a livello militare sono ovviamente gli Stati Uniti che hanno per anni portato avanti il loro progetto FCS (Future Combat System) volto a rinnovare il proprio apparato bellico, dando maggiore importanza all'utilizzo di mezzi informatici e robotici; lo scopo dichiarato di questo progetto è rendere

le proprie unità e i propri armamenti tanto interconnessi quanto internet, tanto mobili quanto un cellulare, tanto intuitivi quanto un videogioco [9].

Xinxihua Un altro paese che ha dato grande enfasi al concetto della network centric warfare è la Cina; "xinxihua", che significa appunto informatizzazione, indica la volontà da parte dell'Esercito di Liberazione del Popolo (PLA) Cinese di adottare le ultime tecnologie nell'ambito del comando e controllo, dell'intelligence e dell'armamento [9].

In Cina, come del resto negli Stati Uniti, è infatti opinione diffusa che le tecnologie dell'informazione possano costituire una "shashoujian"; lo "shashoujian", o, in inglese, "assassin's mace", è un termine usato per indicare un'arma o una tattica che può infliggere un colpo decisivo attraverso una mossa di sorpresa attentamente studiata e cambiare così gli equilibri di potere; ignorando le regole di condotta prestabilite, l' "assassin's mace" è un'arma risolutiva, capace di sconfiggere un nemico in maniera completa ed improvvisa. Diversi scenari, ad esempio una possibile invasione di Taiwan da parte dell'esercito cinese, presentano la cyberwarfare come l' "assassin's mace" in grado di immobilizzare gli avversari e garantire una vittoria rapida e decisiva [9].

1.2.2 Asymmetric Warfare

Il concetto di asymmetric warfare è un antico concetto riguardo la strategia adottabile contro un nemico numericamente (o, nel caso odierno, tecnologicamente) troppo superiore per essere affrontato ad armi pari. Come nel caso della network centric warfare, anche i principi e le tattiche dell'asymmetric war sono state impiegati in contesti reali a partire dal conflitto in Vietnam nel 1960 fino all'attuale guerra in Iraq.

Asymmetric Warfare La strategia dell'asymmetric warfare si fonda sull'uso di guerriglia, tattiche di logoramento, operazioni psicologiche ed attentati[5]; è ritornata prepotentemente di attualità dopo la seconda guerra mondiale, in particolare in tutti quegli scenari che hanno visto il dispiegamento di grandi potenze contro stati con limitate risorse belliche.

Computer Attacks Uno degli ultimi fronti che l'asymmetric warfare ha aperto è proprio quello nel campo delle tecnologie dell'informazione. Per contrastare e negare il predominio informativo acquisito per mezzo della network centric warfare, i combattenti dell'asymmetric warfare hanno iniziato ad ingaggiare i loro nemici anche nel campo virtuale. Questo è reso possibile dal fatto che procurarsi i mezzi per un computer attack è estremamente economico e alla portata di chiunque: l'hardware necessario, generalmente costituito da un computer ed

[5]Si inseriscono tra le tecniche di asymmetric warfare anche gli attentati sebbene sia molto difficile riuscire a giudicare se un attentato sia da considerarsi un atto di guerra o un atto di terrorismo; la distinzione, che può sembrare irrilevante, è invece fondamentale per distinguere se chi commette un attentato è un combattente che ricorre a tecniche di asymmetric warfare o un terrorista.

una connessione alla Rete, può essere reperito con grande facilità; le competenze necessarie per lanciare attacchi semplici, ma comunque efficienti, possono essere acquisite in poco tempo sulla Rete stessa.

1.3 Colpire nella Guerra senza Sangue, ovvero quali sono le armi della Cyberwarfare

Spesso descritta come "bloodless war", o guerra senza sangue, e per questo erroneamente sottovalutata, la cyberwarfare si fonda su tattiche e metodologie ormai molto sviluppate. Un tipico attacco consiste generalmente di due fasi: la fase di cyber reconnaisance, ovvero di raccolta di informazioni, e la fase di cyber attack, ovvero di attacco vero e proprio; di seguito si dà una sommaria descrizione di queste fasi.

1.3.1 Cyber reconnaisance

Prima di ogni attacco è fondamentale essere in grado di ottenere informazioni sul proprio avversario e sulle sue debolezze; nell'ambito della cyberwarfare questo significa identificare le reti ed i computer da attaccare e le falle presenti nella rete o nelle macchine. Tra le tecniche di cyber reconnaisance più note vi sono [20, 1]:

IP Scanning L'ip scanning è utilizzato per determinare l'indirizzo IP di un computer, ovvero l'identificativo numerico che ogni macchina connessa ad una rete IP, come Internet, possiede;

Port Scanning Il port scanning è utilizzato per determinare le porte aperte su un computer, ovvero quali applicazioni sono attive su una macchina ed in attesa di una connessione;

Device Fingerprinting Il device fingerprinting è utilizzato per determinare la configurazione di un computer, ovvero quale hardware e quale software sono impiegati sulla macchina bersaglio;

Vulnerability Scanning Il vulnerability scanning è utilizzato per determinare quali vulnerabilità note sono presenti e non patchate sulla macchina bersaglio;

0-day Exploit Research Lo 0-day exploit research consiste nella ricerca e nella determinazione, per mezzo di test e di reverse engineering, di vulnerabilità non note;

Social Engineering Il social engineering consiste nell'ottenere informazioni chiave riguardo ad un sistema, ad esempio password, fingendo di essere un superiore autorizzato a chiedere e a conoscere tali informazioni;

Si noti che non sempre la raccolta di informazioni si conclude con un attacco; la fase di cyber reconnaisance può servire esclusivamente per testare le difese

dell'avversario oppure per compromettere il soft power di una nazione avversaria senza necessità di compiere un attacco completo. Inoltre tra una cyber reconnaisance e l'attacco vero e proprio può passare molto tempo; la raccolta di informazioni può essere il primo passo per un attacco futuro.

1.3.2 Cyber attack

Una volta ottenute le informazioni è possibile passare all'attacco vero e proprio del sistema. Si definisce attacco qualsiasi azione ostile volta a compromettere una delle seguenti proprietà di un sistema [1]:

Confidentiality La confidentiality significa che il contenuto di informazioni all'interno di un sistema è accessibile esclusivamente a coloro che hanno il diritto e l'autorizzazione ad accedere a quelle informazioni; qualsiasi accesso da parte di terzi non autorizzati costituisce una violazione della confidenzialità del sistema;

Integrity L'integrity significa che il contenuto di informazioni all'interno di un sistema è modificabile esclusivamente da coloro che hanno il diritto e l'autorizzazione a modificare quelle informazioni; qualsiasi modifica da parte di terzi non autorizzati costituisce una violazione dell'integrità del sistema;

Availability L'availability significa che il contenuto di informazioni all'interno di un sistema è sempre disponibile per coloro che hanno il diritto e l'autorizzazione ad usare quelle informazioni; qualora la disponibilità di queste informazioni fosse negata, ciò costituirebbe una violazione della disponibilità del sistema;

Privacy La privacy significa che l'attività eseguita da un utente autorizzato su un sistema non deve essere analizzata o tracciata da utenti non autorizzati; qualora l'attività di un utente fosse osservata da terzi non autorizzati, ciò costituirebbe una violazione della privacy.

Le modalità più note ed applicate di cyber attack sono [9, 1, 11]:

Exploit Un exploit è qualsiasi azione volta ad ottenere l'accesso ad un computer sfruttando una vulnerabilità nota e non patchata;

0-day Exploit Uno 0-day exploit è un tipo di exploit particolarmente pericoloso in quanto sfrutta una vulnerabilità non ancora nota alla comunità informatica e per la quale non esistono dunque protezioni o patches;

Privilege Escalation Il privilege escalation consiste nella capacità di innalzare i propri privelegi, da semplice utente ad amministratore o root, su un sistema in cui si è ottenuto un accesso non autorizzato;

Data Modification Il data modification consiste nel sottrarre, eliminare o modificare documenti classificati o pubblici sulla macchina bersaglio;

Spoofing Lo spoofing consiste nel far credere ad un utente o ad una macchina della rete di essere qualcuno che in realtà non si è; lo spoofing è spesso usato per implementare attacchi del tipo man-in-the-middle;

Phishing Il phishing, o webpage spoofing, consiste nel creare pagine web fasulle, simili a quelle originali, per mezzo delle quali convincere gli utenti ad immettere dati riservati; per aumentare l'efficienza il phishing è spesso accompagnato da attacchi di URL spoofing, DNS cache poisoning, local DNS attack o root DNS attack;

Webpage defacement Il webpage defacement consiste nella sostituzione della pagina web di un sito con una pagina web creata o scelta dall'attaccante;

Semantic attack Il semantic attack è una variante più raffinata del webpage defacement: anzichè sostituire l'intera pagina web, l'attaccante modifica solo alcune informazioni così che la pagina web sembri ancora la pagina originale affidabile, ma in realtà veicoli notizie false;

Trojan Horse Un trojan horse è un programma, generalmente nascosto o unito ad un altro programma, in grado di garantire ad un attaccante una porta aperta nel computer bersaglio da cui portare i suoi futuri attacchi;

Rootkit Un rootkit è un programma estremamente pericoloso, in grado di compiere diverse operazioni software a seconda della volontà dell'attaccante, e, soprattutto, in grado di nascondersi e difendersi dai tentativi di riconoscimento e rimozione;

Virus Un virus è un programma in grado di diffondersi attaccandosi a file eseguibili o documenti e le cui funzionalità variano a seconda del payload di cui dispone; varianti particolarmente difficili da riconoscere ed eliminare sono i virus polimorfici in grado di modificare il proprio codice;

Worm Un worm è un programma in grado di riprodursi e propagarsi automaticamente sfruttando vulnerabilità note dei sistemi connessi alla rete; come nel caso dei virus, le funzionalità dipendono dal payload del worm; uno degli effetti collaterali della diffusione di un worm, indipendentemente dal suo payload, è generalmente la congestione della rete;

Parasite Un parasite è un piccolo programma creato per risiedere in un sistema, rimanere non riconosciuto e corrompere dati critici in databases e nei backup dei databases;

Denial of Service Il denial of service (DoS) consiste nel rendere una macchina inutilizzabile inondandola di un numero di richieste tale da consumare tutte le sue risorse hardware;

Distributed Denial of Service Il distributed denial of service (DDoS) è una versione raffinata del normale denial of service, in cui un attaccante comanda una rete di computer compromessi (botnet o zombies) e li dirige contro il proprio bersaglio;

Phlashing Il phlashing, o permanent denial of service (PDoS), consiste nel compromettere una macchina, agendo ad esempio sul firmware, in modo da renderla inutilizzabile e richiedere una sostituzione hardware.

Ora, l'impatto di questi attacchi singolarmente presi è ben noto alla comunità informatica in quanto queste tipologie di attacco sono più volte state perpetrate da hackers o script kiddies. Ciò che tuttavia distingue un semplice cyber attack, come molti di quelli già avvenuti, da uno scenario di cyberwarfare è che in quest'ultimo caso l'infrastruttura informativa di un paese non sarebbe sottoposta ad un singolo attacco, già di per sé preoccupante e dannoso, ma ad una massiccia e coordinata serie di attacchi volti contro obiettivi precisi e con il fine di compromettere in maniera drastica le infrastrutture vitali dello stesso paese.

Gli attacchi noti fino ad oggi hanno sempre avuto come fine quello di mettere in mostra le capacità di un attaccante, di mostrare solidarietà per una causa o un ideale, di avere un tornaconto economico o, al più, danneggiare un'istituzione o una compagnia; questi attacchi sono spesso condotti con risorse limitate e generalmente consistono nell'uso di uno solo o pochi degli attacchi elencati sopra. Nel contesto della cyberwarfare, lo scopo di ogni attacco sarebbe quello di colpire il più letalmente possibile il proprio nemico; non ci sarebbero quindi più limitazioni: gruppi di hackers sostenuti da uno stato potrebbero godere di risorse economiche ed informative praticamente illimitate, potrebbero avere una giustificazione per ogni atto compiuto senza doversi preoccupare delle infrazioni legali compiute, potrebbero combinare gli attacchi sopra elencati con effetti devastanti. In altre parole, i danni provocati dagli attuali attacchi informatici, che tutti conosciamo, potrebbero essere di ordini di grandezza inferiori ai danni conseguenti ad una cyberwarfare.

1.4 Contro il Sistema, ovvero quali sono i bersagli della Cyberwarfare

Nelle moderne società dell'informazione sono numerosi i punti deboli e le infrastrutture critiche che possono costituire un bersaglio di interesse nel corso di una cyberwarfare; i sistemi che potrebbero essere sottoposti agli attacchi più pressanti comprendono:

Sistemi militari Qualsiasi sistema militare, dai mainframe dei quartieri generali ai sistemi di divisione, costituisce un bersaglio estremamente sensibile; specialmente in caso di conflitto aperto, avere informazioni sugli apparati militari nemici od essere in grado di interferire con la loro C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaisance) può garantire un vantaggio decisivo sull'avversario. Un esempio di possibile attacco a sistemi militari è stato quello portato da un hacker olandese che, nel corso della Guerra del Golfo, è riuscito a sottrar-

re dai computer del Department of Defense statunitense informazioni sui movimenti delle truppe americane[6] [6].

Sistemi logistici Qualsiasi sistema logistico, militare o civile, si affida pienamente alle tecnologie dell'informazione; compromettere un sistema logistico implica la generazione di disordine e caos: dopo l'attacco, se non sono disponibili piani d'emergenza, risulta estremamente arduo controllare l'apparato logistico senza il supporto informatico; tagliare le linee di rifornimento ad unità militari avversarie piuttosto che impedire l'arrivo di aiuti umanitari permette di logorare il nemico e minare il suo morale;

Sistemi finanziario-bancari Tra i maggiori utilizzatori delle tecnologie informatiche vi sono senza alcun dubbio le istituzioni finanziarie e bancarie; un attacco contro questi sistemi permette di scuotere i delicati equilibri economici su cui si regge l'economica mondiale moderna; tuttavia, dato il carattere transnazionale dell'economia moderna, un simile attacco potrebbe avere conseguenze globali; per questa ragione, un attacco a sistemi finanziario-bancari richiede una preparazione estremamente accurata per evitare che gli sconvolgimenti economici conseguenti non coinvolgano anche l'attaccante stesso;

Sistemi SCADA Tra i sistemi più critici per la società civile e più vulnerabili ci sono i sistemi SCADA (Supervisory Control and Data Acquisition) ed i sistemi EMS (Energy Management Supervision); si tratta di sistemi responsabili della gestione automatica dei processi di controllo delle infrastrutture che presiedono agli impianti elettrici, agli impianti nucleari, al trasporto di gas e petrolio, alle risorse idriche; originariamente concepiti come macchine stand-alone, questi sistemi sono stati poi connessi alla Rete per poter interfacciarsi con le macchine via Internet, minimizzando così gli spostamenti e le spese. Sebbene ciascun sistema SCADA differisca dall'altro, molti condividono le stesse vulnerabilità, dovute alla non-adozione di criptazione [7] e all'uso di COTS (Commercial Off-The-Shelf) software [22]; alcuni di questi, ad esempio, userebbero versioni di Microsoft Windows, spesso non opportunamente configurate [7]; l'effettiva vulnerabilità è stata provata nel Marzo 2007 con l'operazione Aurora Generator Test [22]: durante una simulazione organizzata dal Department of Energy statunitense, i dipendenti dell'Idaho Lab riuscirono ad ottenere l'accesso ad un impianto elettrico e disabilitare un generatore diesel [5];

Sistemi simbolici Un ultimo possibile bersaglio della cyberwarfare potrebbero essere sistemi simbolici, ovvero sistemi militari o civili che non erogano servizi critici all'esercito o alla popolazione, ma che hanno un ruolo rappresentativo; è il caso, ad esempio, dei siti governativi o ministeriali; lo scopo principale di una simile azione è quello di mostrare le proprie capacità e le proprie potenzialità per demoralizzare e sfiduciare il nemico.

[6] L'hacker ha poi proposto la vendita di queste informazioni ad alcuni ufficiali iracheni, ma questi ultimi hanno rifiutato l'offerta credendo che si trattasse di una trappola.

Si noti che questa distinzione tra i possibili bersagli è puramente concettuale; nel mondo moderno le interazioni tra i vari tipi di sistemi informativi che abbiamo elencato sono spesso talmente strette e ramificate che colpire un qualsiasi tipo di sistema implica compromettere anche molti altri sistemi differenti. Questo, in effetti, è stato presentato come uno dei pericoli più seri della cyberwarfare [22], ovvero che a causa delle moderne interdipendenze tra vari sistemi possa generarsi un effetto a cascata con risultati imprevedibili.

1.5 Guerra 2.0, ovvero quali sono i vantaggi della cyberwarfare

Il moderno sviluppo della cyberwarfare è dovuto in larga misura alla superiorità che è possibile ottenere per mezzo di azioni di cyberwarfare piuttosto che di atti bellici convenzionali; tutti gli attori internazionali riconoscono i seguenti vantaggi della cyberwarfare [9, 22]:

Low cost La cyberwarfare presenta notevoli vantaggi dal punto di vista economico; sebbene il tempo di istruzione di un tecnico per la cyberwarfare possa risultare maggiore del tempo necessario per addestrare un soldato per la guerra convenzionale, questo sforzo iniziale è largamente compensato a posteriori. Tutto il materiale necessario per la cyberwarfare è infatti di prezzo estremamente contenuto e facilmente reperibile: è molto più semplice procurarsi un laptop che non un carro armato [20]. Esclusi poi gli attacchi di tipo 0-day exploit, che richiedono grande esperienza e ricerche approfondite [19], gli altri attacchi possono essere eseguiti con discreta facilità facendo ricorso a tools pre-esistenti. Se poi gli effetti della cyberwarfare fossero davvero così devastanti come spesso ipotizzato, la cyberwarfare supererebbe di gran lunga la guerra convenzionale anche sotto l'aspetto del rapporto costi-effetti.

Deniability Un enorme vantaggio dell'attuale infrastruttura di rete di Internet è che essa permette ad un attaccante di nascondere facilmente le sue tracce; dirottando la sua connessione attraverso molteplici macchine che fungano da proxy e manomettendo i log di tali macchine, un attaccante può agevolmente mascherare la propria identità; questo significa che le ricerche ed i tentativi di tracebacking di un attacco spesso si fermano al computer compromesso di un utente innocente oppure, anche se raggiungono una macchina sospetta, difficilmente possono stabilire se si tratti dell'ultimo anello della catena di macchine creata dall'attaccante. A questo va aggiunto che, diversamente dagli attuali hackers che spesso agiscono solo per mettersi alla prova e che sovente si vantano delle proprie gesta in chatroom e forum (offrendo così una preziosa confessione agli investigatori), gli attori della cyberwarfare non indulgono in questo atteggiamento; essi non mirano ad azioni clamorose colpendo numerose vittime, ma puntano esclusivamente e nell'ombra al proprio bersaglio [4]. La possibilità di nascondere efficacemente le proprie tracce, redirigendo la propria connessione attraverso computer stranieri, da inoltre la possibilità di eseguire

false flag attacks [17], ovvero di eseguire degli attacchi facendo ricadere la colpa su una nazione od un'organizzazione estranea all'attacco; questa possibilità, invero molto pericolosa, permetterebbe ad uno stato di creare tensione o incidenti tra stati terzi e di approfittare di questo clima e delle ostilità che ne potrebbero scaturire.

Liability Allo stato attuale risulta estremamente difficile perseguire i responsabili di attacchi di cyberwarfare; oltre alla difficoltà di identificare il reale autore, di cui abbiamo discusso nel punto precedente, l'assenza di convenzioni e norme internazionali permette ad un attaccante con una buona conoscenza delle leggi di sottrarsi facilmente alle proprie responsabilità; ad esempio il gruppo giovanile filo-russo The Commissar of the Nashi, coinvolto in alcuni cyber attacchi in Estonia nel 2007, ha portato i suoi attacchi dalla Moldova e dalla Transnistria, paesi al di là della giurisdizione dell'Interpol e degli accordi europei, riuscendo in questo modo ad ignorare i mandati di arresto, che si sono così ridotti ad atti simbolici [9]. Non si dimentichi, poi, che spesso questi attaccanti sono appoggiati da uno stato nazionale, che li considera propri agenti e non criminali internazionali; lo stato può quindi fornire tutto l'appoggio legale necessario e sfruttare il suo peso internazionale per difenderli.

Real-world impact L'ultimo grande vantaggio della cyberwarfare, a volte sottovalutato, a volte sopravvalutato, rimane l'innegabile impatto sulla realtà quotidiana. Un attacco di cyberwarfare non è mai limitato alla Rete, ma la ragione stessa per cui viene compiuto è che esso è in grado di modificare la realtà quotidiana; sono almeno tre i livelli a cui un tale attacco può avere impatto:

- Livello fisico: attaccare sistemi militari, logistici, bancari o SCADA è volto principalmente a creare disordine e caos a livello reale; sabotare ordini militari, bloccare linee di rifornimento, impedire pagamenti bancari o togliere la corrente ad una città sono atti volti a generare danni materiali ed economici, da cui un avversario in tempo di guerra può trarre vantaggio;
- Livello psicologico: attaccare sistemi simbolici o causare danni materiali a livello fisico per mezzo di attacchi di cyberwarfare contribuisce ad instillare nella mente del nemico paura ed insicurezza. L'uso di cyberwarfare per propaganda e PSYOPS (psychological operations) [9], al fine di minare l'appoggio della società civile ad uno stato in guerra, è ben noto a tutti gli attori internazionali e la cyberwarfare altro non è che una nuova applicazione di questa strategia;
- Livello politico: portare a termine con successo un attacco di cyberwarfare contro un nemico permette di evidenziare le sue debolezze e le sue mancanze a livello tecnologico e difensivo; questo spesso corrisponde ad uno smacco per l'immagine di uno stato, a cui potrebbe corrispondere una riduzione del suo soft power e del suo prestigio e

peso a livello internazionale [9]. A livello civile, è proprio il timore di compromettere la propria immagine e reputazione che spinge molte aziende colpite da hackers a tacere questi attacchi [22].

2 CyberTerrorism

2.1 Terrore virtuale, ovvero una definizione di Cyberterrorism

Per affrontare il problema del cyberterrorism nel mondo moderno è necessario anzitutto dare una precisa definizione di cosa sia il cyberterrorism; tale compito è estremamente arduo e sfuggente, in quanto il cyberterrorism nasce dall'unione di cyberwarfare e terrorismo, due concetti che, per loro stessa natura, sono di difficile comprensione.

Abbiamo già visto nella sezione precedente come il termine cyberwarfare sia di difficile determinazione. Altrettanto si può dire riguardo al terrorismo; è evidente che la linea che separa un terrorista da un semplice combattente è estremamente sottile e labile; questo giustifica la miriade di spiegazioni che sono state offerte per chiarire in maniera più o meno precisa il fenomeno del terrorismo [16]. Ad esempio l'FBI (Federal Bureau of Investigation) negli Stati Uniti ha fatto propria la seguente espressione:

> "The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[7].

Una definizione ben più ampia e precisa, che già prevede l'uso di attacchi informatici come mezzo di terrorismo, è stata adottata dal governo inglese:

> "Terrorism is the use of serious violence against persons or property, or the threat to use such violence, to intimidate or coerce a government, the public, or any section of the public for political, religious or ideological ends. The term serious violence would need to be defined so that it included serious disruption, for instance resulting from attacks on computer installations or public utilities."[8].

Volendo ora coniugare queste definizioni con il concetto di cyberwarfare, una sintesi è offerta ancora una volta da L.J. Janczewski e A.M. Colarik [10]:

[7] "L'uso illegittimo della forza e della violenza contro persone o cose per intimidire o costringere un governo, una popolazione civile, o qualsiasi segmento della società, ad appoggiare obiettivo politici o sociali." (trad. propria).

[8] "Il terrorismo è l'uso di grave violenza contro persone o cose, o la minaccia di usare tale violenza, per intimidire o forzare un governo, la popolazione, o qualsiasi parte della società per scopi politici, religiosi o ideologici. Il termine grave violenza dovrebbe essere definito così da includere interruzioni di servizi, risultanti ad esempio da attacchi su installazioni informatiche o servizi di pubblica utilità." (trad. propria).

> "Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that results in violence against non-combatant targets."[9].

Ciò che distingue dunque la cyberwarfare dal cyberterrorism è che quest'ultimo, pur essendo pianificato con la stessa cura della cyberwarfare, non ha il supporto di alcuno stato; inoltre, il fine ultimo del cyberterrorism non è quello di ottenere una superiorità sul proprio nemico, ma quello di costringere il nemico ad accettare le proprie richieste per mezzo di atti violenti.

È chiaro che discernere con precisione tra cyberwarfare e cyberterrorism è molto difficile e spesso a livello tecnico non vi sono differenze tra questi attacchi; pur tuttavia, anche se a livello puramente informatico tale distinzione può sembrare poco importante, ben maggiore è il suo rilievo a livello legale, politico e militare quando è necessario determinare la risposta ad un cyber attack [22].

2.2 Informatica del terrore, ovvero come la Cyberwarfare può essere usata per il terrorismo [16, 18]

Tra gli attori dello scenario internazionale più interessati agli strumenti della cyberwarfare ci sono senza dubbio le organizzazioni terroristiche. Uno dei principi fondamentali delle organizzazioni terroristiche è che esse operano in tutti gli ambienti [16] e la Rete non fa eccezione; anzi, la Rete risulta essere un terreno particolarmente adatto per i terroristi in quanto si coniuga perfettamente con le strategie del terrore. Essa potrebbe divenire lo strumento di azione privilegiato prima da quei gruppi terroristici che, operando in società post-industriali, sono più avvezze all'uso della Rete, e poi essere adottato anche dai restanti gruppi terroristici in contesti differenti [22].

2.2.1 Gli attacchi del cyberterrorism

La linea di confine tra cyberwarfare e cyberterrorism è estremamente labile e la distinzione tra la prima e la seconda risiede principalmente negli attori coinvolti e nelle motivazioni che muovono gli attaccanti; questo significa che a livello tecnico la differenza tra cyberwarfare e cyberterrorism è pressoché assente e tutte le metodologie impiegate dalla prima per cyber reconnaisance e cyber attacks possono essere utilizzate parimenti anche in uno scenario di cyberterrorism.

2.2.2 I bersagli del cyberterrorism

Se la cyberwarfare favorisce attacchi efficienti contro sistemi critici, il cyberterrorism mira innanzitutto a realizzare attacchi che possano avere una forte risonanza mediatica e a diffondere un'atmosfera di terrore ed incertezza. I sistemi

[9] "Cyberterrorism significa attacchi premeditati e politicamente motivati da parte di gruppi sub-nazionali, gruppi clandestini o individui contro sistemi informatici, programmi e dati che causino danni contro bersagli non-combattenti." (trad. propria).

simbolici sono spesso colpiti in quanto, per via della loro visibilità, permettono ai terroristi di raggiungere un grande pubblico. I sistemi finanziario-bancari sono un bersaglio appetibile in quanto costituiscono le fondamenta degli stati avversari; si noti infatti che se nella cyberwarfare gli stati contendenti rischiano entrambi di subire i danni di una crisi finanziaria-bancaria a causa della diffusione globale dell'economia, i gruppi terroristici, rifiutando l'ordine economico globale, sono gli unici a poter colpire questi sistemi con la certezza di non rimanerne coinvolti [22]. I sistemi logistici e SCADA possono essere bersagli di interesse, in particolare per il caos che potrebbe generarsi in seguito ad un attacco. Infine i sistemi militari sono colpiti più raramente in quanto maggiormente protetti.

2.2.3 I vantaggi del cyberterrorism

Come anticipato, i vantaggi della cyberwarfare che abbiamo elencato in precedenza, non possono che lasciar presumere che le organizzazioni terroristiche siano estremamente interessate alla Rete. Anzitutto, queste organizzazioni dispongono spesso di risorse economiche limitate, e dunque il ricorso a tattiche di cyberterrorism, che richiedono meno uomini e meno risorse, appare ovvio [8]. La deniability e l'assenza di liability sono altre due caratteristiche della cyberwarfare che risultano estremamente utili [8]: esse permettono di colpire senza possibilità di essere scoperti e perseguitati generando così nella popolazione quell'insicurezza e quella paura che è l'obiettivo primario di ogni organizzazione terroristica. Infine la possibilità di avere un real-world impact garantisce a questi gruppi che i loro attacchi possano avere effetto e peso a livello fisico, psicologico e politico.

2.3 Jihad elettronica, ovvero come il Cyberterrorism può sfruttare la Rete.

Oltre ad applicare le strategie della cyberwarfare, il terrorismo ha già mostrato di aver appreso come usare la Rete per i propri fini. In particolare il terrorismo di matrice fondamentalista islamica ha mostrato come sfruttare la Rete per finalità organizzative o per guerra psicologica, ad esempio:

Propaganda Numerose organizzazioni terroristiche hanno trovato in Internet il loro canale privilegiato per la comunicazione e la propaganda. Per questi gruppi è spesso difficile trasmettere messaggi attraverso i media convenzionali, e così, la Rete, priva di censure, è diventata il loro mezzo per diffondere messaggi politici, comunicazioni o rivendicazioni [21]. Erroneamente, si potrebbe pensare che la propaganda non abbia nulla a che fare con la cyberwarfare e il cyberterrorism; in verità la capacità di questi gruppi di comunicare ed ottenere l'attenzione del pubblico è fondamentale per raggiungere il loro obiettivo e per diffondere la paura. In quei paesi in cui l'accesso alla stampa è negato o il controllo e la censura proibirebbero di esprimere idee di stampo fondamentalista, Internet ha permesso a questi

di poter rendere pubbliche le proprie ideologie ed azioni [18]. Anzi, per i terroristi la possibilità di diffondere messaggi su Internet costituisce di per sé una "bomba perfetta": la sola minaccia è sufficiente, almeno per un limitato periodo di tempo, a diffondere timore e preoccupazione, senza necessità di organizzare nuovi attentati rischiosi e costosi [18]. Un chiaro esempio di questo uso è il rilascio dei video "Glory of Martyrdom" o "Winds of Paradise" , diffusi dal sito As Sahab, creati per alzare il morale dei sostenitori del terrorismo fondamentalista ed esaltare la vita e le azioni dei martiri [16, 18].

Arruolamento Oltre a diffondere terrore, un secondo fine della propaganda è quello di persuadere nuove reclute ad unirsi alle fila dell'organizzazione; messaggi audio e video che spiegano le ragioni degli attentatori e ne mostrano le azioni e il sacrificio servono a muovere l'animo di tutti i simpatizzanti e a spingerli ad arruolarsi per la causa. Attraverso Internet un potenziale terrorista ha modo di entrare nella cerchia più esterna del gruppo, dove, bombardato da slogan e indottrinato, impara a pensare come un vero affiliato; in seguito, quando la sua lealtà sarà provata, potrebbe avere modo di ottenere agganci per diventare parte integrante dell'organizzazione [18].

Addestramento Per mezzo della Rete, le potenziali nuove reclute possono essere addestrate ed istruite direttamente a casa loro, in modo rapido e senza costi; è abbastanza semplice reperire su Internet manuali sull'uso di armi da fuoco, sulle tecniche di guerriglia, sulla sopravvivenza in ambienti ostili o sulla fabbricazioni di ordigni esplosivi [18]. A questi documenti che possono fornire una prima infarinatura teorica sulle tattiche del terrorismo, si affiancano spesso siti simpatizzanti in grado di offrire raccolte di documenti e immagini ben più esplicative; ad esempio l'Università Al Qaeda per gli Studi della Jihad, sul sito Al Farouq, mette a disposizione testi di indottrinamento, pareri teologici, immagini e scenari di guerra tracciati dai leaders [18].

Finanziamento Se la propaganda non è sufficiente a convincere le potenziali reclute ad arruolarsi, può almeno servire a persuaderle ad offrire fondi o risorse all'organizzazione terrorista. Mostrando scene di sacrifici o di massacri, molti gruppi terroristici sperano così di ottenere delle sovvenzioni; i siti indicano spesso le coordinate bancarie dei conti di associazioni di copertura, creati esclusivamente per raccogliere il denaro ed inoltrarlo poi ad un'organizzazione terrorista [18]. Alternativamente, i terroristi possono fare anche ricorso a mezzi illegali, come truffe basate su phishing o furto dei numeri di carte di credito, per ottenere le risorse economiche di cui necessitano.

Comunicazione La Rete globale consente anche ai membri di un gruppo terrorista di comunicare piani ed idee in modo sicuro. Nel 2000 George Tenet, direttore della Central Intelligence, aveva dichiarato che diverse

organizzazioni, tra cui Hezbollah, Hamas, Abu Nidal e Al Qaeda usavano e-mail, scambio di file e messaggi criptati per supportare le loro attività [8]; Ramzi Yusef, organizzatore dell'attentato al World Trade Center nel 1993, archiviò sul suo laptop dei file criptati contenenti dettagli riguardo al sequestro di aerei di linea statunitensi [8]. Le tecnologie informatiche consentono dunque ai terroristi di salvare e mantenere al sicuro i loro dati e, nel contempo, di comunicare con i loro affiliati e le loro cellule in tutto il mondo.

2.4 Digital 9/11, ovvero come il Cyberterrorism potrebbe colpire in futuro

Non sono ancora noti attacchi di cyberterrorism significativi, ma nonostante questo si possono identificare alcune caratteristiche che un futuro atto di cyberterrorism presenterà.

È sensato ritenere che un futuro attacco di cyberterrorism colpisca più sistemi critici contemporaneamente [7]; la possibilità di raggiungere più obiettivi sensibili e sabotarli con il conseguente aumento di disordine e caos e il disordine conseguente permetterebbe ad un attentato terroristico di avere una notevole risonanza.

È inoltre probabile che nel breve periodo, data l'inesperienza delle organizzazioni terroristiche sulla Rete, queste preferiscano riunire in un unico attacco cyberterrorism e terrorismo convenzionale; in questo caso, il cyberterrorism dovrebbe funzionare come un supporto all'attacco convenzionale al fine di massimizzarne l'efficacia. Uno scenario verosimile potrebbe essere quello di effettuare un attentato terroristico convenzionale e quindi disabilitare le reti di comunicazione dei servizi di emergenza per impedire o rallentare l'arrivo dei soccorsi [8]; ancora più catastrofico potrebbe essere lo scenario in cui atti di cyberterrorism siano usati per amplificare l'effetto di un possibile attacco NBC (Nuclear Biologial Chemical) [22].

È anche possibile che i futuri attacchi di cyberterrorism colpiscano direttamente a livello informatico, sabotando in maniera subdola sistemi critici: ancora una volta gli effetti potrebbero essere catastrofici; Bruce Schneier, esperto di sicurezza, ha detto: "Se vuoi causare disordine su un volo aereo, saboti il sistema per riservare i posti. Ma sei vuoi compiere del cyberterrorism, allora saboti i sistemi che regolano la misura del rifornimento dell'aereo e del peso dei bagagli." [8].

3 Counter-cyberwarfare and Counter-cyberterrorism

3.1 Counterstrike, ovvero come rispondere agli attacchi di cyberwarfare e cyberterrorism

Di fronte ai pericoli della cyberwarfare e del cyberterrorism, molti paesi hanno cercato di prepararsi e prevenire quelli che potrebbero esseri i danni provocati da

attacchi sulla Rete. Le nazioni moderne hanno appreso dalla storia un'importante lezione: quasi sempre, nel corso di una guerra, i vincitori sono stati coloro che potevano contare su un C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaisance) superiore rispetto a quello del nemico [17]; essere autore di un cyber attack che comprometta sistemi critici, che sia in grado di rendere il nemico paralizzato, cieco, sordo e muto [17], potrebbe decidere il corso di una guerra.

Il generale dell'Air Force statunitense Robert Elder ha pubblicamente riconosciuto che ogni volta che si parla di velocità, raggio e flessibilità del dominio aereo statunitense, non bisogna dimenticare che tale possibilità è resa fattibile dall'attuale cyber-superiorità statunitense [5]; è evidente che atti di cyberwarfare e cyberterrorism potrebbero limitare notevolmente questo dominio. Per questo, fino dalla metà degli anni '90, l'esercito statunitense si è impegnato ad affrontare tali realtà. Il primo manuale operativo in cui si affronta il tema della cyberwarfare è il Field Manual 100-6 IO dell'Agosto 1996 [12]. In seguito l'Esercito creò il primo CERT (Computer Emergency Response Team) all'interno del corpo responsabile per il LIWA (Land Information Warfare Activity) [12]; l'Air Force sviluppò gli IOS (Information Operations Squadron) ed integrò l'AFIWC (Air Force Information Warfare Center) con i nuovi AFCERT (Air Force Computer Emergency Response Team) a loro volta collegati con i NOSC (Network Operations Security Centers), responsabili della C4I (command, control, communications, computers, intelligence) dell'Air Force [12]; infine la Marina creò il proprio NAVCIRT (Navy's Computer Incident Response Team) e istituì a Norfolk il NETWARCOM (Naval Network Warfare Command) [12]. Tutte queste decisioni ed innovazioni nelle strutture militari dell'esercito statunitense permettono di capire che il problema della cyberwarfare e del cyberterrorism è realmente presente e che ormai tutti riconoscono la Rete e i sistemi informatici come armi.

A livello pratico, diverse tecniche possono essere adottate per prevenire e contenere la cyberwarfare e il cyberterrorism [20]:

Enforcement of good practices il primo passo per garantire la sicurezza minima di un sistema è l'applicazione di una serie di procedure standard di good practices che dovrebbero essere applicate da tutti gli utenti, anche a livello personale. Tra queste good practices vi sono: mantenere il sistema operativo, gli antivirus e i software aggiornati; utilizzare passwords forti; conservare le passwords al sicuro; disabilitare i servizi non necessari; conservare i log ed eseguire backup dei dati;

Adoption of secure software talvolta è possibile richiedere anche ai programmatori dei software che dovranno essere utilizzati l'applicazione di una serie di procedure standard di good practices oppure selezionare solo quei software che soddisfano requisiti minimi di sicurezza;

Encryption tecniche di criptazione forte dovrebbero essere utilizzate per garantire la segretezza di tutti i dati riservati e per assicurare le comunicazioni protette;

Authentication and access control tecniche di autenticazione dovrebbero sempre essere implementate per l'identificazione di chi voglia interagire con il sistema; tecniche di access control dovrebbero sempre essere definite per assicurare che un utente possa accedere solo ai dati a cui ha diritto di accedere;

Firewall sistemi di firewall software e hardware dovrebbero sempre essere implementati per controllare e regolamentare gli accessi e le uscite dal sistema;

IDS un sistema di IDS (intrusion detection system) dovrebbe sempre essere implementato per monitorare l'attività degli utenti e riconoscere comportamenti sospetti o pericolosi;

Honey pot gli honey pot, ovvero parti del sistema lasciate volontariamente vulnerabili per attirare l'attenzione di potenziali attaccanti, possono essere implementate per condurre in trappola gli intrusi;

Coopertation with ISP al fine di identificare gli attaccanti o di essere in grado di contenere e limitare gli effetti di un denial of service è fondamentale sviluppare rapporti di cooperazione con gli ISP (Internet Service Provider);

Quick recovery strategies nel caso tutte le strategie sopra elencate si rivelino inutili, è bene avere previsto un insieme di contromosse per ripristinare rapidamente un sistema compromesso da un attacco; queste soluzioni possono comprendere l'uso di sistemi ridondanti, il mirroring dei sistemi e l'applicazione di politiche di backup;

Alternative networks development per far fronte ad eventi catastrofici, in cui l'uso di Internet sia completamente negato, è possibile sviluppare delle reti di sicurezza alternative; ad esempio il governo statunitense sta sviluppando CWIN (Cyber Warning and Information Network), una rete sicura ed affidabile che connette 50 locazioni ed è totalmente indipendente da Internet, così da garantire una connettività minima sempre assicurata in caso di cyberwarfare [22].

Tutte queste misure puntano ad assicurare i sistemi critici di uno stato, ma è inevitabile che durante una vera cyberwarfare molti sistemi di supporto, in particolare civili, risulterebbero vulnerabili; questi ultimi sono infatti gestiti da società che raramente hanno interesse ad investire sulla sicurezza e che difficilmente si preoccupano di scenari di cyberwarfare o cyberterrorism. Tuttavia molti governi fanno affidamento su questi servizi civili (ad esempio il Department of Defense statunitense utilizza i servizi commerciali di trasporto FEDEX per far arrivare truppe e rifornimenti in Iraq [12]) e dunque, pur proteggendo i propri sistemi, la compromissione di sistemi non militari può sempre causare un grave danno allo stesso stato.

4 Casi di Studio

Si riportano di seguito alcuni casi degni di nota di cyberwarfare, cyberterrorism, counter-cyberwarfare o counter-cyberterrorism.

In molte situazioni è difficile riuscire a determinare con precisione se un attacco sia un atto di cyberwarfare o cyberterrorism soprattutto per le inevitabili difficoltà nell'identificazione dei responsabili di tali attacchi o crimini; senza essere in grado di scoprire chi sia l'autore primo di un attacco o senza la possibilità di sapere se gli attaccanti abbiano avuto o meno il supporto di uno stato, risulta particolarmente difficile categorizzare questi attacchi. Ad ogni modo, i seguenti casi sono in grado di dare un'idea delle possibilità e dei danni che potrebbero essere causati da un attacco informatico.

Si noti inoltre che tutti gli esempi sottoelencati, nonostante le conseguenze, sono da considerarsi solo come delle scaramucce o delle prove di quella che potrebbe essere una vera e propria cyberwarfare; nel presente scenario internazionale, gli stati tendono a limitare il loro supporto e negare il loro coinvolgimento in qualsiasi evento etichettato come cyberwarfare al fine di non rovinare i propri rapporti con la comunità internazionale. È presumibile che tali stati appoggino azioni di cyber reconnaisance in previsioni di possibili conflitti futuri, ma osteggino azioni dirette di cyber attacks. Si noti che la volontà di frenare possibili azioni di cyber attacks è dettata non solo da ragioni squisitamente diplomatiche, ma anche da considerazioni di carattere strategico e militare: è, infatti, indubbio che essendo le armi di cyberwarfare e cyberterrorism armi relativamente nuove, l'impatto maggiore si avrà con il primo attacco; quindi utilizzare queste armi in uno scenario di pace, senza che ad essa seguano ulteriori azioni militari sarebbe uno spreco: oltre a compromettere l'immagine e la fiducia verso il paese attaccante, la vittima avrebbe tempo di correre ai ripari e acquisirebbe sufficiente esperienza per fermare, o comunque limitare, un attacco analogo in futuro. Massimizzare l'effetto della cyberwarfare richiede dunque di conservare la propria possibilità di lanciare un cyber attack solo in una situazione di conflitto reale.

Date queste premesse, è chiaro che nessuno dei casi riportati di seguito è in grado di rappresentare completamente la portata di reali atti di cyberwarfare o cyberterrorism; nel caso di cyberwarfare perché le condizioni non sono ancora propizie e nessuno dei grandi attori internazionali sembra essere apertamente coinvolto; nel caso di cyberterrorism semplicemente perché nessun attacco consistente è ancora stato portato.

4.1 Operation Eligible Receiver and Operation Evident Surprise: 1997

Operation Eligible Receiver ed Operation Evident sono due estese operazioni di addestramento alla counter-cyberwarfare e al counter-cyberterrorism. Entrambe le esercitazioni hanno avuto luogo negli Stati Uniti ed il loro obiettivo era di testare la vulnerabilità dei propri sistemi informatici. Agli albori dell'età della cyberwarfare, i risultati non furono per nulla incoraggianti.

Operation Eligible Receiver fu organizzata nel giugno 1997 dal Department of Defense statunitense: il team rosso, costituito da hackers dell'NSA con il compito di attaccare i sistemi governativi [12], riuscì ad ottenere accessi a livello amministratore (root) su 36 delle 40000 reti del Department of Defense, disabilitare parte della rete elettrica statunitense, disattivare il servizio 911 di Washington D.C. e di altre città ed accedere al sistema di un incrociatore della Marina al largo della costa [6].

Questi risultati vennero poi confermati nel corso di Operation Evident Surprise, organizzato dal Comando Atlantico stanziato a Norfolk in Virginia; nel corso di questa esercitazione, nuove vulnerabilità del sistema informativo del Department of Defense vennero colpite, tra cui i registri medici che conservano traccia delle riserve di sangue [12].

4.2 Solar Sunrise: 1998

Uno dei primi casi di cyberwarfare potrebbe considerarsi quello che venne battezzato come Solar Sunrise. Nel corso dei preparativi per dell'operazione Desert Fox agli inizi del 1998 vennero registrate una serie di intrusioni nei sistemi del Department of Defense. Le prime indagini sull'origine degli attacchi portarono in Medio Oriente e suscitarono il timore di trovarsi di fronte ad un caso di cyberwarfare sostenuta da qualche stato mediorientale; le indagini successive, tuttavia, rivelarono che l'attacco era stato condotto da due teenagers californiani [12]. Sebbene non si tratti di un caso di cyberwarfare o cyberterrorism, il caso di Solar Sunrise è tuttavia di rilievo in quanto, per la prima volta, rese evidente ai comandi statunitensi il possibile impatto di una vera cyberwarfare.

4.3 Sri Lanka: 1998

Nel 1998, un cyber attack contro le ambasciate dello Sri Lanka viene ad oggi considerato come il primo caso noto di attacco ad un'infrastruttura statale da parte di un gruppo terroristico, ovvero il primo caso noto di cyberterrorism. L'attacco fu un denial of service prolungato contro le ambasciate per mezzo di un massiccio invio di e-mails; 800 e-mails al giorno per un periodo di 2-3 settimane misero in difficoltà i sistemi delle ambasciate dello Sri Lanka. Le mail rivendicavano l'attacco da parte delle Internet Black Tigers e spiegavano che il loro unico scopo era quello di bloccare le comunicazioni [8].

4.4 Moonlight Maze: 1998

Precursore del più celebre Titan Rain, Moonlight Maze identifica una serie di atti di cyber reconnaisance che hanno colpito i sistemi governativi statunitensi nel corso del 1998. Le prime intrusioni furono identificate a marzo e, nei mesi seguenti, una serie sostenuta di attacchi colpì il Pentagono, il Department of Energy e la National Aeronautics and Space Administration (NASA) [20]. L'origine di questi attacchi fu identificata in Russia. Le autorità statunitensi

dichiararono che nessun sistema protetto contenente dati classificati fosse stato violato; tuttavia, è probabile che documenti tecnici della difesa siano stati scaricati illegalmente [20]. In un caso, addirittura, sembra che una stampante Hewlett-Packard al Navy's Space and Naval Warfare Systems Command Center (SPAWAR) a San Diego fosse stata riprogrammata per inviare copie dei documenti in stampa ad una stampante in Russia [20].

4.5 Pacific Paradise: 2000

Sebbene non si tratti di un caso di cyberterrorism, ma di un semplice cyber attack da parte di un ingegnere, il caso di Pacific Paradise, nel Queensland, Australia, è spesso addotto come caso esemplare delle potenzialità del cyberterrorism. Tra marzo ed aprile del 2000, l'ingegnere Vitek Bodek, dopo diversi tentativi ed attacchi non scoperti [8], riuscì ad introdursi nei sistemi di controllo delle acque fognarie della stazione di Pacific Paradise; dall'interno, riuscì poi a rilasciare le acque di scarico nei corsi d'acqua della Sunshine Coast, contaminando così una zona molto frequentata da famiglie [2]. Questo atto evidenzia in modo esplicito come un atto di cyberterrorism possa avere un impatto molto concreto e diretto sulla realtà: il sabotaggio di Bodek ebbe conseguenze sia economiche, poiché a causa dell'inquinamento e dell'odore le persone preferirono evitare quella zona, sia ambientali, poiché parte della flora e della fauna marina locale morì [2].

4.6 Palestina: 2000-today

A partire dal Settembre 2000, l'interminabile conflitto tra Israele e Palestina iniziò ad essere combattuto anche sulla Rete; a metà tra cyberwarfare e cyberterrorism, questo conflitto vede schierati da una parte lo stato di Israele, dall'altra i guerriglieri palestinesi ed i loro vari sostenitori, tra cui Libano, Iran e Arabia Saudita [16]. I cyber attacks palestinesi, tra cui defacements, distributed denials of service, worms, trojans ed altre tecniche di violazione di sistemi, hanno colpito sistemi governativi, militari e finanziari; gli attacchi coincidono spesso con eventi pubblici o seguono gli attacchi militari portati dalle truppe israeliane. Il progetto "Electronic Jihad" concepito dai palestinesi prevede quattro fasi durante le quali colpire in ordine sistemi governativi, sistemi finanziari, sistemi infrastrutturali come gli ISP (Internet Service Provider) e infine sistemi esteri di paesi alleati di Israele [20]; l'idea alla base di "Electronic Jihad" è quella che tutti i sostenitori della causa palestinese possono essere utili alla causa combattendo sul web, e più denaro gli israeliani devono impegnare per riparare e rinforzare i loro sistemi, meno soldi avranno per comprare proiettili e missili da usare contro i palestinesi [16]. Ovviamente, altrettanto agguerrita è anche a risposta israeliana sulla Rete: denials of service sono stati spesso usati contro i sistemi dell'Autorità Palestinese, di Hezbollah o di Hamas.

4.7 India: 2000-today

Un altro stato, l'India, che condivide due confini molto caldi, quello con la Cina e quello con il Pakistan, è stato spesso coinvolto in atti di cyber reconnaisance e cyber attacks con questi due paesi.

Fin dal 2000 le tensioni tra India e Pakistan, a causa del Kashmir, trovarono sfogo sulla Rete; i sistemi indiani, in particolare, furono ripetutamente colpiti con defacement di carattere politico da diversi gruppi di hackers filo-pakistani, tra cui G-Force, Doctor Nuker e Pakistan Hackerz Club [20].

Nel 2008, il quotidiano Times of India ha sostenuto che diversi cyber attacks provenienti da computers localizzati in Cina hanno colpito il National Informatics Centre (la backbone del governo indiano), il Ministero degli Affari Esteri e il Segretariato del Gabinetto, ed anche siti legati al governo del Tibet in esilio. Gli indiani accusano che tali attacchi non sono da considerarsi opera di hackers isolati, in quanto la loro raffinatezza e la loro organizzazione lasciano supporre un'origine comune. Gli attacchi prevedono la creazione di bot, l'installazione di keyloggers e la scansione delle reti; l'obiettivo sembra quello di costruire una mappa delle reti indiane da poter utilizzare in caso di conflitto per colpire o disabilitare reti critiche [3].

Questo pericolo è particolarmente sentito in India; infatti, mentre in Occidente le precedenti violazioni si considererebbero violazioni della sicurezza o, al più, cyber attacks, in India esse vengono considerate atti di terrorismo, nello specifico cyberterrorism [3].

Il governo cinese, da parte sua, nega tutte queste affermazioni ed asserisce di non esser in alcun modo coinvolto in questi atti di cyberwarfare o cyberterrorism; tuttavia sembra che Pechino, per quanto non supporti azioni di questo genere, sia favorevole alla formazioni di gruppi hacker, come la Honker Union of China, in particolare di stampo nazionalista e patriottico [3].

4.8 Hainan Incident: 2001

L'incidente di Hainan, o incidente EP-3, avvenne il primo aprile 2001 quando un aereo di sorveglianza statunitense, nei pressi dell'isola cinese di Hainan, entrò in collisione con un caccia cinese a mezz'aria; in seguito all'impatto il caccia cinese precipitò e il pilota perse la vita. A questo evento seguì un incidente diplomatico ed un raggelamento nelle relazioni tra Stati Uniti e Cina. Nel frattempo sulla Rete hackers patrioti di entrambe le nazionalità si scatenarono contro lo stato nemico. Gli hackers cinesi, tra cui i gruppi Honker Union of China e Chinese Red Guest Network Security Technology Alliance, organizzarono una campagna, durata diverse settimane, contro siti americani militari ed industriali [20]. Gli hackers statunitensi risposero con altrettanti web page defacements [9].

All'interno di questo contesto internazionale bisognerebbe far probabilmente rientrare il caso del worm Code Red [9]. Sebbene non vi sia alcun indizio su un coinvolgimento di hackers cinesi, il comportamento del worm sembra confermare l'ipotesi che sia stato sviluppato come arma per la piccola cyberwarfare scoppiata tra Stati Uniti e Cina dopo incidente di Hainan. Lanciato il 12 luglio

2001 come Code-Red v1 ed aggiornato a Code-Red v2 il 19 luglio 2001, il worm si diffuse molto velocemente sfruttando una vulnerabilità nota, ma spesso non patchata di Microsoft IIS; il worm era progettato per defacciare le pagine dei siti ospitati su Microsoft IIS con la frase "Hacked by Chinese" e per utilizzare la macchina infetta e prendere parte a un denial of service contro www1.whitehouse.org il 20 e 28 di ogni mese [15]. La presunta risposta statunitense a Code Red fu Code Blue, worm che tracciava i sistemi infetti da Code Red e li riprogrammava per indirizzare il loro attacco di denial of service contro macchine localizzate in Cina, tra cui il sito di sicurezza informatica cinese NS Focus [9].

Sebbene nessuno dei due stati, Cina e Stati Uniti, abbia riconosciuto gli attacchi informatici all'indomani dell'incidente di Hainan, questi eventi possono dare un'idea su piccola scala di come potrebbe essere una vera cyberwarfare.

4.9 Titan Rain: 2003-2006

Titan Rain denota la più massiccia e consistente serie di atti di cyberwarfare condotti ai danni degli Stati Uniti; il termine Titan Rain è infatti usato per raggruppare tutti quegli atti di cyber reconnaisance e cyber attack che tra il 2003 e il 2006 hanno colpito i sistemi statunitensi. I principali bersagli di questa campagna furono la U.S. Defense Information Agency (DISA), la U.S. Redstone Arsenal, la Army Space and Strategic Defense Installation, il Department of Defense (DoD), la National Aeronautics and Space Administration (NASA), la Sandia National Laboratories, la Lockheed-Martin ed altri sistemi critici militari e logistici [22, 9]. Durante questa serie di attacchi coordinati sono stati sottratti molti documenti; la maggior parte di questi, comunque, sebbene non destinati al pubblico, non erano dati classificati; resta comunque il timore che, nonostante i singoli dati sottratti non contenessero informazioni critiche, l'unione degli stessi possa rivelare informazioni segrete [9]. La strategia adottata durante questi attacchi consisteva generalmente nel dispiegare un team di hackers composto da 6 a 30 elementi per ottenere l'accesso su un computer bersaglio, copiare tutto il contenuto dell'hard disk entro 30 minuti, inviare i dati verso computer localizzati in Corea del Sud, Hong Kong o Taiwan per depistare le tracce e quindi, in un secondo momento, redirigere tutti i dati verso computer locati nella provincia cinese di Guangdong [9]; inoltre, spesso gli attaccanti installavano sui computer violati un rootkit per poter ottenere accesso in futuro e cancellavano tutte le loro tracce dai log [17].

Un prodotto di questa cyberwarfare potrebbe essere il virus Myfip, nato per copiare i documenti presenti su un computer infetto ed inviarli ad un indirizzo remoto [4]. A differenza di altri virus e worm più noti che puntano a diffondersi in maniera rapida ed estesa, questo virus, un vero prodotto da cyberwarfare, non mira ad un ampia diffusione, ma punta a passare inosservato così da colpire non indistintamente, ma solo bersagli precisi. Una volta infettato il sistema, Myfip scansiona i dischi alla ricerca di file .pdf (nella prima versione) e di altri file di testo o di progetto (nella versione successiva) per copiarli ed inviarli sulla Rete. Ciò che spinge a considerare Myfip come un'ulteriore arma utilizzata durante la cyberwarfare Titan Rain è che il computer da cui si è diffuso originariamente

questo virus ed i computer a cui Myfip invia le copie dei documenti sono tutti localizzati nella provincia cinese di Tianjin [4].

4.10 Operation Spam Zombies: 2005

Uno delle più grandi minacce sulla Rete è oggi costituita dalle botnet, o reti di bot; si tratta di reti di computer compromessi che possono essere utilizzati per generare attacchi di tipo denial of service; dal momento che cyber attacks di questo tipo risultano semplici da condurre, ma estremamente difficili da prevenire, una botnet può rivelarsi una valida arma in uno scenario di cyberwarfare o cyberterrorism.

Operation Spam Zombies è stata un'imponente operazione di counter-cyberwarfare eseguita nel corso del 2005. Secondo le stime attuali circa un quarto di tutti i personal computer connessi ad Internet potrebbe fare parte di una botnet e si è stimato che 50% delle copie pirata di Microsoft Windows contengano dei trojan pre-installati al fine di sfruttare la macchina durante attacchi di denial of service [9]. Nel corso di Operation Spam Zombies, che ha visto la collaborazione di 25 stati, numerosi nodi di diverse botnet sono stati individuati e rimossi [9].

4.11 Younes Tsouli, Tariq al-Daour e Waseem Mughal: 2007

Younes Tsouli, ribattezzato "il cavaliere della Jihad mediatica", noto sulla Rete con il nome di "Irhabi[10] 007" [18], ha mostrato al mondo come chiunque possa diventare un sostenitore del terrorismo per mezzo del cyberterrorism, indipendentemente dalla sua esperienza e dalla sua locazione geografica. Younes è infatti un giovane marocchino trasferitosi in gioventù in Gran Bretagna, che ha deciso di sfruttare il suo talento nell'uso del computer al servizio del terrore [18]. La sua prima attività è stata di propaganda: inizialmente copiava e ridistribuiva filmati e documenti a sostegno della Jihad; in un secondo momento, ottenuta la fiducia del leader Abu Maysara, divenne una delle fonti più affidabili sulla Rete per la pubblicazione di nuovi video ed immagini [18]. Younes trovò presto degli alleati con i quali proseguire la sua attività di cyberterrorism; si formò così un trio di cui Younes era la mente, Tariq al-Daour il cassiere e Waseem Mughal l'addetto alla logistica [18]. Il gruppo non si limitò più alla semplice propaganda, ma decise di dedicarsi anche all'attività di finanziamento del terrorismo; per mezzo di phishing ed altre azioni di cyberterrorism, i tre ottennero i numeri di migliaia di carte di credito [18], effettuarono prelievi, riciclarono il denaro su siti di gioco d'azzardo online ed utilizzarono poi i soldi per acquistare biglietti aerei, visori notturni, tende, sistemi GPS, credito telefonico per i terroristi sul campo [22]. L'intensa attività dei tre attirò però l'attenzione delle autorità e si aprì così la caccia ad Irhabi 007: le ricerche di Aaron Weisburd, un cacciatore di video del terrore, la denuncia di Gregor Loock, un amministratore di domini Internet che aveva scoperto dei file di Younes, ed infine la cattura a Sarajevo

[10] Irhabi in arabo significa terrorista [18].

di un paio di terroristi in contatto con Younes permisero a Scotland Yard di arrestare Irhabi 007 [18].

Questo caso ci mostra come il cyberterrorism possa permettere a simpatizzanti del terrore di appoggiare le attività di gruppi terroristici per mezzo di attività di propaganda e finanziamento e di come sia spesso difficile riuscire ad identificare e consegnare alla giustizia i colpevoli.

4.12 Estonia: 2007

Gli eventi che hanno preso luogo in Estonia nel 2007 sono considerati ad oggi l'esempio più evidente degli effetti e dei danni che la cyberwarfare può arrecare ad uno stato fortemente basato su sistemi informatici, come lo è l'Estonia [5, 9].

La scintilla che diede inizio alle ostilità fu quando, nella primavera del 2007, il governo estone decise di spostare un monumento ad un soldato dell'Armata Rossa dal centro di Tallinn alla periferia. La risoluzione ovviamente infiammò gli animi: da una parte il governo ed il popolo estone che ormai vedevano in quella statua solo un monumento agli oppressori comunisti del dopoguerra, dall'altra gli estoni di origine russa ed il governo e il popolo russo che consideravano invece quella statua un monumento ad un soldato ignoto morto per liberare quella terra dal giogo nazista.

Il 27 aprile, tra le manifestazioni locali e le proteste del governo russo, la statua fu comunque rimossa. Sulla Rete, esplose la cyberwarfare. Iniziò la campagna di denial of services più lunga mai vista, diretta contro siti governativi ed amministrativi estoni; i siti governativi, che avevano una media di 1000 visite al giorno, iniziarono a riceverne 2000 al secondo; i server crasharono; i denial of service, che generalmente durano ore o giorni, proseguirono per settimane [22]. Gli utenti che tentarono di accedere ai siti del parlamento, delle banche, dei ministeri, delle scuole e dei giornali non ebbero modo di collegarsi oppure raggiunsero pagine sulle quali trovarono foto di soldati dell'Armata Rossa o citazioni da Martin Luther King [9]. Il sistema estone rasentò il collasso. Si è stimato che le 10 richieste dati più ingenti lanciate contro la rete estone abbiano consumato 90 megabits per secondo di banda per oltre 10 ore: l'equivalente del download dell'intero sistema operativo Microsoft Windows XP ogni 6 secondi per 10 ore [9].

Il governo estone accusò il governo russo di essere il mandante di questi attacchi, ma Mosca, ovviamente, negò qualsiasi coinvolgimento. Esperti della Commissione Europea e della NATO giunsero in Estonia per studiare questi attacchi senza precedenti e farne tesoro; le loro indagini riconobbero che parte degli attacchi provenivano da computer localizzati in Russia, ma non furono in grado né di confermare né di negare il coinvolgimento del Cremlino [22]. Gran parte di questi attacchi furono lanciati da cittadini russi senza alcun appoggio da parte del governo: si trattava spesso di ferventi sostenitori della politica russa che, adirati dalle decisioni di Tallinn, apprendevano su Internet come condurre cyber attacks e quindi si univano al denial of service.

Il caso estone è la dimostrazione di come la cyberwarfare consenta di piegare uno stato nazionale eseguendo una serie di attacchi debilitanti, di costo conte-

nuto, di origine difficilmente precisabile, impossibili da perseguire legalmente e capaci di attirare l'attenzione globale [9].

4.13 Georgia: 2008

Se la cyberwarfare in Estonia nel 2007 può considerarsi il primo caso significativo di cyberwarfare contro uno stato in tempo di pace, quella in Georgia nel 2008 potrebbe essere ricordata come la prima cyberwarfare aperta tra due stati in guerra.

Lo scontro armato del 2008 tra la Russia e la Georgia per il controllo dell'Ossezia del Sud segnò l'inizio di un conflitto non solo convenzionale, ma anche sulla Rete. All'avanzata delle truppe di terra di Mosca si affiancarono per la prima volta i cyber attacks degli hackers russi: sei botnet colpirono siti di news georgiani; vennero diffusi strumenti per denials of service e liste di siti georgiani vulnerabili; vennero pubblicati indirizzi di ufficiali georgiani ed inviti allo spam. Il livello di sofisticazione sembrò aumentato rispetto al caso estone; questo fu dimostrato anche dalla nuova tattica adottata dagli hackers russi che puntarono subito a mettere fuori gioco i loro avversari diretti colpendo alcuni dei siti hacker georgiani più noti, come hacker.ge e warez.ge. La risposta georgiana non mancò di farsi sentire: vennero compromessi alcuni siti di news russi ed i suoi visitatori furono re-diretti su siti di news filo-georgiani [9].

Ancora una volta, le parti si scambiarono accuse, ma nessuna delle due sembra in grado di poter provare il reale coinvolgimento dello stato o dell'apparato militare nella cyberwarfare.

Il caso georgiano mostra per la prima volta una cyberwarfare che coinvolge due parti a volto scoperto sulla Rete e determinate a darsi battaglia; inoltre, sebbene il supporto di uno stato nazionale sia ancora incerto, sono evidenti due tendenze che saranno certo presenti nelle future cyberwarfare: il confronto e l'attacco diretto verso gli hackers avversari e la compromissione dei siti di news per influenzare l'opinione pubblica.

4.14 Project Chanology: 2008

Un caso di cyber attack piuttosto controverso, ma interessante dal punto di vista didattico, è costituito da quello che è stato denominato Project Chanology; Project Chanology denota un'insieme di cyber attacks orchestrati dal gruppo Anonymous contro la Chiesa di Scientology.

L'esatta natura di Project Chanology è controversa: Anonymous ha organizzato questa campagna come una forma di protesta volta ad "espellere la Chiesa di Scientology da Internet", in quanto accusata di praticare forme di censura su Internet, di usare tecniche di reclutamento non ortodosse e di sfruttare economicamente i suoi membri; la Chiesa di Scientology non ha invece esitato a denunciare Project Chanology e ad etichettarlo come cyberterrorism [9].

Dopo attività di spam e pubblicazione di dati riservati riguardo alcuni membri di rilievo della Chiesa di Scientology, Project Chanology, forte di 9000 sostenitori, lanciò il 18 gennaio 2008 un attacco di tipo denial of service contro

i server della Chiesa di Scientology. Sebbene il numero degli attaccanti fosse contenuto (una tipica botnet conta fino a 50000 computer), il denial of service ebbe successo; la Chiesa di Scientology dovette optare per un provider più sicuro e tra l'attacco e questo trasferimento, il sito ufficiale rimase irraggiungibile per circa due settimane [9].

Project Chanology è un caso di interesse rilevante soprattutto perché mostra come sia possibile, anche per organizzazioni prive di appoggi statali, quali potrebbero essere i gruppi terroristici, organizzare attacchi di successo sfruttando tools pre-esistenti e facendo leva su una massa di internauti poco esperti ma facili da plagiare e da convincere a partecipare ad un atto di cyberterrorism o cyberwarfare apparentemente innocuo.

4.15 Altri casi degni di nota

I casi sopra elencati costituiscono gli esempi più noti e rilevanti di cyberwarfare e cyberterrorism; per comprendere completamente la portata e le potenzialità future della cyberwarfare può essere utile considerare anche altri attacchi portati da semplici hackers o gruppi di hackers contro obiettivi governativi o militari. Questi attacchi non si considerano casi di cyberwarfare o cyberterrorism in senso stretto, ma dal momento in cui colpiscono obiettivi sensibili diventano dei precedenti preziosi per predire le future dinamiche della guerra sulla Rete. Non si può non citare, anche se lo spazio a disposizione non consente di approfondire, l'intrusione di Hess nei sistemi militari americani nel 1986 [13]; l'infiltrazione nei sistemi della Griffis Air Force Base nel 1994 [13]; l'ingresso nelle reti della Guam Air Force Base ad opera di un quindicenne croato nel 1997 [6]; il blocco delle comunicazioni in un aeroporto del Massachussets ad opera di hackers teenagers nel 1997 [9]; il defacing ed il furto di mail dall'India's Bhabha Atomic Center nel 1998 [8]; il sequestro, da parte di un gruppo di hackers, di un satellite militare britannico per le comunicazioni nel 1999 [6]; la sottrazione da parte di Jonathan "c0mrade" James dei codici di un modulo della International Space Station nel 1999 [9]; gli attacchi informatici durante la guerra in Kosovo nel 2000 [20]; la violazione dei sistemi russi di Gazprom nel 2000 [9]; il furto di dati commerciali statunitensi da parte dell'intelligence francese [13]; le intrusioni di Gary "Solo" McKinnon nelle reti militari americane alla ricerca di prove sull'esistenza degli alieni nel 2001 e 2002 [9]; la simulazione di war game Digital Pearl Harbor nel 2002 [22]; la diffusione sulla Rete del worm Slammer considerato da alcuni un test di cyberwarfare nel 2003 [17, 7]; gli attacchi di gruppi filo-islamici come la Unix Security Guard contro i sistemi statunitensi nel corso della guerra in Iraq nel 2003 [21]; l'azione di counter-cyberwarfare Operation Web Snare nel 2004 [13]; gli attacchi con impiego di trojan al Oak Ridge National Laboratory e al Los Alamos Laboratory nel 2005 [9]; gli attacchi contro lo U.S. Naval War College di Newport nel 2006 [22]; i denials of service contro le macchine cinesi nel corso delle Olimpiadi del 2008 [9].

5 Etica, Cyberwarfare e Cyberterrorism

5.1 Quando il grilletto si chiama Enter, ovvero brevi considerazioni etiche su cyberwarfare e cyberterrorism

L'uso della definizione "bloodless war" per descrivere cyberwarfare e cyberterrorism è senza dubbio un termine infelice per indicare questa moderna evoluzione della guerra. Il concetto, quasi paradossale, di una "guerra senza sangue" non rende infatti conto della portata della cyberwarfare e del cyberterrorism sul mondo reale e delle responsabilità di coloro che sono coinvolti in questa guerra.

Una tendenza della guerra moderna è quella di tenere i soldati sempre più lontano dai loro nemici e dalla battaglia: gli avversari vengono ingaggiati a maggior distanza con armi più precise, bombardati dall'alto da aerei invisibili, centrati da missili teleguidati lanciati da cacciatorpediniere dispiegate in mare aperto ed, ora, infine, colpiti da operatori informatici dall'altro capo del globo. Questo spostamento dal cuore della battaglia aumenta la sicurezza dei soldati impegnati nello scontro e, contemporaneamente, li allontana dagli orrori della guerra diminuendo il carico psicologico ed emotivo che dovrebbero sostenere se fossero realmente presenti sul campo.

Indipendentemente dunque dalla distanza, un soldato dietro ad un computer, perché tale è un operatore informatico impiegato nella cyberwarfare, ha la stessa responsabilità etica che ha un soldato in prima linea[11]. Non si vuole ragionare in questa sede riguardo alle ragioni per cui una guerra scoppia, per cui un uomo decide o è costretto a combattere, se esista o meno una guerra giusta; quello che si vuol far notare è che quando un soldato preme Enter per compromettere un sistema nemico, egli dovrebbe porsi le stesse domande che si pone un soldato che sta per premere un grilletto per uccidere il nemico; ancora una volta si sottolinea che non si intende dare un giudizio sull'azione di premere un grilletto o pigiare un tasto, ovvero sul fine ultimo di tali azioni, quanto piuttosto equiparare queste due azioni; il fine ultimo (e.g.: "sparare per difendersi" piuttosto che "sparare per uccidere un uomo di una razza inferiore"), ciò che giustifica o condanna a livello etico l'azione, non vuole essere preso in considerazione in questo ragionamento; ciò che interessa è l'azione in sé: sparare o premere un tasto sono sostanzialmente equivalenti: in entrambi i casi si tratta di danneggiare il proprio nemico.

L'azione di premere un tasto sembrerebbe lasciare un soldato con le mani pulite, senza macchie di sangue; ciò è dovuto al fatto che premere un pulsante è una sorta di azione simbolica, non un intervento diretto sulla realtà; esiste una sorta di dereferimento operato dall'informatica, una sorta di struttura interposta che permette al soldato della cyberwarfare di perdere il legame tra la sua azione ed i risultati della sua azione; ma la causalità tra il computer dell'attaccante ed il campo di battaglia non viene mai meno, e, per quanto le mani dell'attaccante possano essere monde, tale non può dirsi la sua coscienza.

[11] Si noti che l'assunzione fatta in queste righe circa l'identità tra operatore informatico impiegato nella cyberwarfare e soldato non ha alcun riscontro legale; anzi, proprio la definizione dello status giuridico di un una persona impegnata nella cyberwarfare resta una questione ancora da dirimere [19].

Un'obiezione scontata a questo ragionamento è che sarebbe inesatto equiparare l'azione di sparare ad un nemico con l'azione di compromettere un sistema informatico; le conseguenze delle due azioni sono infatti diverse, nel primo caso la morte di uomo, nel secondo la distruzione di un sistema informatico artificiale; quindi, essendo apparentemente le conseguenze della prima azione più gravi delle conseguenze della seconda azione, la prima risulta moralmente "più condannabile" della seconda. Tuttavia, sebbene le conseguenze di un'azione possano essere un metro utile per giudicare quantitativamente la gravità di un'azione e stabilire, ad esempio, una punizione, in questa sede si assume che il valore etico di un'azione non sia dato dalle sue conseguenze o dal suo fine ultimo, quanto dall'azione in sé; riconoscendo, cioè, che esistono azioni moralmente ingiuste, pur con conseguenze o finalità buone e viceversa, non resta altra scelta che valutare un'azione considerando la validità dell'azione stessa; ma abbiamo già dimostrato che, in sé, l'azione di premere un grilletto e l'azione di pigiare un tasto sono equivalenti. Ad ogni modo, è bene anche ricordare che le conseguenze di un attacco informatico sono generalmente molto più estese e non si limitano alla compromissione di un sistema informatico; si consideri ad esempio il caso del worm Slammer che ha colpito Internet all'inizio del 2003 [14]; sebbene non si sia trattato di un caso di cyberwarfare o cyberterrorism, questo semplice cyber attack resta comunque emblematico per spiegare il punto in questione; una delle tante conseguenze della diffusione di Slammer, oltre ovviamente alla paralisi di Internet, è stato il blocco dei terminali del servizio di emergenza 911 di Washington; sebbene non siano noti casi di complicazioni, è chiaro che disattivare il servizio di emergenza sarebbe potuto costare la vita a più persone (soprattutto in uno scenario di guerra); premere un tasto per avviare un atto di cyberwarfare o cyberterrorism può dunque avere gli stessi effetti, o effetti ancora più gravi, che premere un grilletto; d'altronde, una delle ragioni per cui si sviluppano nuove armi, compresa la cyberwarfare e il cyberterrorism, è, purtroppo, quella di essere in grado di produrre più danni al nemico con meno costi e fatica.

5.2 Bushido.net, ovvero brevi considerazioni legali su cyberwarfare e cyberterrorism

Le guerre moderne sono regolate, almeno a livello teorico, da una serie di accordi come la convenzione di Hague (1899, 1907) e la convenzione di Ginevra (1949, 1977) [19]; questi trattati, che dovrebbero porre le basi di una legge di guerra internazionale, sono firmati dalla maggior parte delle nazioni del mondo. Ora, se si analizzassero la cyberwarfare e il cyberterrorism alla luce di questi accordi, apparirebbe chiaro che la guerra sulla Rete, così come è stata descritta nei paragrafi precedenti, costituisce una grave violazione di questi accordi o, addirittura, potrebbe considerarsi un crimine di guerra [19].

Anzitutto, un attacco, per essere legittimo, dovrebbe garantire l'immunità dei non combattenti; l'articolo 57 della Convenzione di Ginevra recita: "Constant care should be taken to spare the civilian population, civilians, and civilian

objectives."[12] [19]. Chiaramente, gran parte degli attacchi di cyberwarfare e cyberterrorism che sono stati descritti non rispettano questa norma; colpire i sistemi civili, causare disagi e generare insicurezza nel pubblico sono spesso gli obiettivi stessi della cyberwarfare e del cyberterrorism; molti attacchi, come virus e worm, colpiscono indistintamente sistemi civili e non civili per massimizzare i danni. Puntare ai sistemi civili è spesso un modo per colpire indirettamente sistemi militari o governativi; gli ultimi si fondano spesso su sistemi civili e così paralizzare questi equivale a paralizzare gli altri; a ciò si aggiunga che, ovviamente, i sistemi civili sono più facili da colpire che non i sistemi militari, i quali sono più difesi e dispongono di backup e dispositivi ridondanti in grado di riportare rapidamente il sistema in linea. Volendo attenersi alla Convenzione di Ginevra, nel caso di cyberwarfare, uno stato attaccante potrebbe forse disporre di informazioni sufficienti per eseguire attacchi mirati, ma anche in questo caso non potrebbe fare a meno di colpire sistemi civili: infatti, tra i sistemi dell'attaccante e quelli del difensore vi sono numerosi altri sistemi interposti che potrebbero rimanere coinvolti [19]; è invece certo che nel caso di cyberterrorism, gli attaccanti, non disponendo generalmente dell'intelligence sufficiente per identificare e danneggiare bersagli precisi, hanno maggiori ragioni per colpire i sistemi civili [19].

Un attacco dovrebbe essere proporzionale alla provocazione; in altre parole, per essere legittimo, un attacco non deve sconfinare in una overreaction [19]. Rimanendo confinati alla Rete, non è però semplice determinare il rapporto tra provocazioni ed attacchi e, soprattutto evitare overreactions. Ciò è dovuto al fatto che molto spesso le vulnerabilità identificate sulla Rete possono essere sfruttate una volta soltanto, dopodiché verranno patchate; è dunque nell'interesse di chi esegue tale attacco sfruttarlo al limite e massimizzarne gli effetti. Inoltre, anche volendo contenere la portata della propria cyberwarfare o cyberterrorism non è detto che questo sia possibile o che l'attaccante abbia la competenza e la lungimiranza sufficiente per controllare l'attacco opportunamente.

Un attacco dovrebbe contenere e limitare gli effetti collaterali. Nel momento in cui si decide di lanciare un attacco si dovrebbero considerare i possibili effetti collaterali e valutarne la portata. Nell'ambito di cyberwarfare e cyberterrorism è estremamente probabile che un attacco abbia invece effetti indesiderati, ad esempio coinvolga sistemi civili che non fanno parte dell'obiettivo; ciò è dovuto sia alla difficoltà intrinseca nell'informatica di determinare a priori tutti gli effetti di una modifica ad un sistema sia ad una serie di altre cause tra cui pressioni politiche per sperimentare armi nuove anche se non completamente testate, errori in fase di progettazione, mancanza di responsabilità da parte dell'attaccante dovuta alla grande distanza dalla vittima dell'attacco ed ovviamente presenza di imprevisti non contemplati in fase di testing all'interno di ambienti controllati (si noti che questi problemi sono comuni a cyberwarfare e cyberterrorism, così come all'uso di armi convenzionali moderne) [19].

I danni di un attacco dovrebbero poter essere evidenti e quantificabili, così

[12]"Bisognerebbe avere massima cura di risparmiare la popolazione civile, i civili e gli obiettivi civili." (trad. propria).

da poter assicurare una ricostruzione efficiente [19]. Ora, mentre gli attacchi convenzionali hanno effetti lampanti e facili da stimare, altrettanto non si può dire per gli attacchi di cyberwarfare e cyberterrorism; è difficile valutare l'entità dei danni in quanto è arduo essere certi che un attacco sia realmente cessato ed il nemico non sia più "in casa". Questo compito è più che mai complesso quando in campo vi siano armi come rootkits, trojans, virus polimorfici; tali armi sono infatti nate per nascondersi ed evitare di essere scoperte ed è perciò difficile capire se un sistema sia realmente sicuro o vi siano annidate delle minacce, pronte a colpire di nuovo; è poi sufficiente che solo una macchina di un sistema sia vulnerabile perché tutte, presto, lo diventino.

Un attacco deve sempre poter essere attribuito a qualcuno, cosicché la risposta all'attacco possa essere diretta contro i responsabili [19]. Contrariamente a quanto avviene nella guerra convenzionale, in cui le responsabilità di ciascuno stato sono quasi sempre determinabili, la Rete è il dominio dell'anonimato; cyberwarfare e cyberterrorism garantiscono infatti la non rintracciabilità e conseguentemente l'impunità. Non solo. La possibilità di compiere false flag attacks, semplicemente redirigendo la propria connessione attraverso paesi terzi permette ad un attaccante di coinvolgere e responsabilizzare altre nazioni estranee ai fatti; questo comportamento, assimilabile all'uso delle uniformi di uno stato nemico durante una guerra, è severamente condannato dalle attuale convenzioni internazionali [19].

5.3 Cyber equilibrio freddo?, ovvero brevi considerazioni politiche su cyberwarfare e del cyberterrorism

Il primo riconoscimento ufficiale a livello politico della realtà di cyberwarfare e cyberterrorism avvenne nel 1998, quando l'allora direttore della CIA, George Tenet, dichiarò pubblicamente che gli Stati Uniti stavano sviluppando un'infrastruttura tale da poter portare attacchi attraverso la Rete ad altri sistemi. La dichiarazione non aggiunse nulla di nuovo rispetto a quanto già noto, per via ufficiosa, a tutte le nazioni; questo costituì tuttavia il primo caso in cui un rappresentante di un'autorità pubblica riconobbe la Rete come un possibile campo di battaglia e, nel fare questo, indirettamente, ammonì tutti coloro che volessero colpire gli Stati Uniti che questi ultimi erano pronti a raccogliere la sfida [6].

Rob Clyde, esperto di sicurezza, riconosce in queste dichiarazioni un'applicazione nel campo della cyberwarfare e del cyberterrorism del principio del prudent approach [6]. Il prudent approach è la stessa politica adottata dagli Stati Uniti nel caso delle armi nucleari dopo la Caduta del Muro di Berlino: sviluppare un armamento, sia questo una testata nucleare o un rootkit, e rendere pubblico che questo armamento è efficiente e pronto a colpire, serve come deterrente per evitare lo scoppio di un conflitto reale; in questo modo, qualunque nemico che voglia colpire utilizzando missili nucleari o attacchi sulla Rete sa che non potrà sfuggire ad una severa ritorsione. Si noti tuttavia che questo principio ha dei limiti: anzitutto deve essere possibile identificare senza errore l'attaccante e, mentre determinare l'origine di un missile nucleare è scontato, non altrettanto si può dire per stabilire l'origine di un cyber attack; inoltre, il

prudent approach ha un effetto limitato contro realtà come i gruppi terroristici, che, per loro stessa natura, si nascondono all'interno della società e sono dunque difficili da scovare e colpire.

Queste riflessioni, associate al riconoscimento del possibile impatto di cyberwarfare e cyberterrorism, potrebbero portare alla conclusione che una politica di prudent approach non sia una soluzione adatta al problema delle minacce sulla Rete. In molti scenari, l'impatto di attacchi riusciti di cyberwarfare e cyberterrorism è tale da compensare il divario tecnologico militare tra paesi del primo mondo e paesi del secondo e terzo mondo; cyberwarfare e cyberterrorism avrebbero cioè un potere livellante tale da minare il dominio delle attuali superpotenze sul campo di battaglia. Il timore di vedere le proprie posizioni di vantaggio negate, potrebbe indurre molti paesi militarmente all'avanguardia ad adottare una strategia di first strike [17]. Il first strike è la stessa politica adottata dagli Stati Uniti nel caso delle armi biologico-chimiche presenti, o che avrebbero dovuto essere presenti, in Iraq: l'unico modo di garantire la sicurezza nazionale sarebbe quella di intervenire prima che il nemico possa utilizzare le proprie capacità offensive. Ovviamente, sebbene questa politica possa essere per molti paesi un'assicurazione migliore nel breve periodo, contribuisce enormemente all'aumento della tensione internazionale.

John Arquilla, studioso di relazioni internazionali e di guerra, ha sostenuto che una soluzione al problema di cyberwarfare e cyberterrorism potrebbe essere un'applicazione del principio del no first use [19]. Il no first use è la stessa politica adottata dagli Stati Uniti riguardo l'uso di armi chimiche nel corso della Seconda Guerra Mondiale: ogni nazione riconosce di avere la capacità di portare attacchi, chimici o cyber attacks, ma si impegna a non usare mai questi attacchi se non in risposta ad un attacco analogo. Questo approccio è molto simile al prudent approach, ma, a differenza di quest'ultimo che è unilaterale, il no first use è multilaterale e fornisce maggiori garanzie nel caso più paesi decidano di adottare questa politica.

È scontato a questo punto fare un paragone tra politica di prudent approach, first strike e no first use e domandarsi quale paradigma si adatti maggiormente alle future guerre sulla Rete. La prima ha la sua applicazione più nota nelle relazioni tra Stati Uniti e paesi detentori dell'atomica invisi agli Stati Uniti: il suo funzionamento è dovuto all'esistenza di un interlocutore noto che è responsabile delle proprie azioni e che può essere avvertito. La seconda ha la sua applicazione più evidente nella moderna guerra al terrorismo; non avendo una controparte da poter ammonire, ma un nemico sfuggevole che non combatte con le stesse regole, la logica di first strike permette di colpire per incapacitare gli avversari prima che essi possano agire. La terza ha la sua applicazione più conosciuta nei mutui accordi durante la Seconda Guerra Mondiale riguardo l'uso di armi chimiche: dati degli interlocutori, sapendo che ciascuno di essi si atterrà ad usare certi attacchi solo in risposta ad attacchi analoghi, è stato possibile mantenere un equilibrio. Ora, le caratteristiche di deniability proprie di cyberwarfare e cyberterrorism sembrano negare la possibilità di avere un interlocutore responsabile. La politica di prudent approach o no first use che applicate finora hanno dato buoni risultati, sembrano meno utilizzabili sulla Rete; d'altra parte, è però

evidente che l'approccio first strike ha costi politici e diplomatici che rendono il suo possibile utilizzo limitato.

Un altro problema di carattere politico è la capacità di diverse realtà non-statali di condurre cyberwarfare e cyberterrorism. Ad oggi, infatti, le guerre propriamente dette sono sempre state condotte da nazioni; altre organizzazione non hanno il diritto di dichiarare guerra e, soprattutto, non dispongono dei mezzi per sostenere un conflitto [19]. Questo non è vero per cyberwarfare e cyberterrorism: diverse multinazionali, ad esempio, hanno la possibilità di procurarsi i mezzi ed il know-how necessario per sostenere un tale conflitto sulla Rete; mentre esistono delle leggi che impediscono alle multinazionali di acquistare armamenti, non esistono leggi che vietino loro l'acquisto di strumenti per la cyberwarfare (i.e.: computers). Questo aprirebbe scenari politici completamente nuovi in cui grandi corporations potrebbero avere un loro peso politico negli equilibri mondiali; dopotutto corporations multinazionali hanno già oggigiorno un potere ed un'influenza sulle società pari a quelli degli stati nazionali e potrebbero dunque facilmente essere coinvolte in una guerra sulla Rete [19]. Se, ad esempio, atti di cyberwarfare fossero compiuti contro i sistemi di proprietà della Microsoft a Taiwan[13], tale attacco sarebbe da considerarsi un attacco contro Taiwan o contro la Microsoft? La risposta a questa domanda determina chi può rispondere all'attacco subito; e, mentre per un attacco convenzionale, ad esempio un attacco missilistico, è evidente che il bersaglio sia Taiwan e questa solo abbia la possibilità di rispondere, giacchè Microsoft, per quanto potente, non può disporre di armi e missili, la stessa risposta non è così scontata quando si parla della Rete; in questo caso infatti, una corporation come Microsoft ha mezzi sufficienti, e forse migliori di quelli di Taiwan, per rispondere ad un cyber attack e difendere i propri interessi.

Infine, un ultimo punto su cui è necessario riflettere è quello della sorveglianza. Uno dei mezzi a disposizione di uno stato per prevenire possibili atti di cyberwarfare o cyberterrorism è quello di monitorare i dati in Rete. Questo tuttavia solleva inevitabilmente problemi connessi al tema della privacy. Esaminare il traffico attraverso un ISP può costituire un caso di sorveglianza non autorizzata; la creazione di database con dati riguardanti i cittadini costituisce un punto critico che molti potrebbero essere desiderosi di violare; la profilazione dei cittadini porterebbe ad una raccolta di dati personali che i cittadini stessi non avrebbero possibilità di conoscere o validare; su grandi numeri, anche una ridotta percentuale di falsi positivi causerebbe molte indagini su cittadini onesti; la fuga di informazioni potrebbe essere usata per ricattare cittadini onesti [8]. In definitiva la volontà di controllare e monitorare la Rete, per mezzo di progetti come il TIA (Total Information Awareness) statunitense [8], porterebbe ad una costante violazione dei diritti dei cittadini che utilizzano Internet.

[13]Si tratta di un caso puramente esemplificativo; all'autore non è noto la reale esistenza di sedi Microsoft a Taiwan.

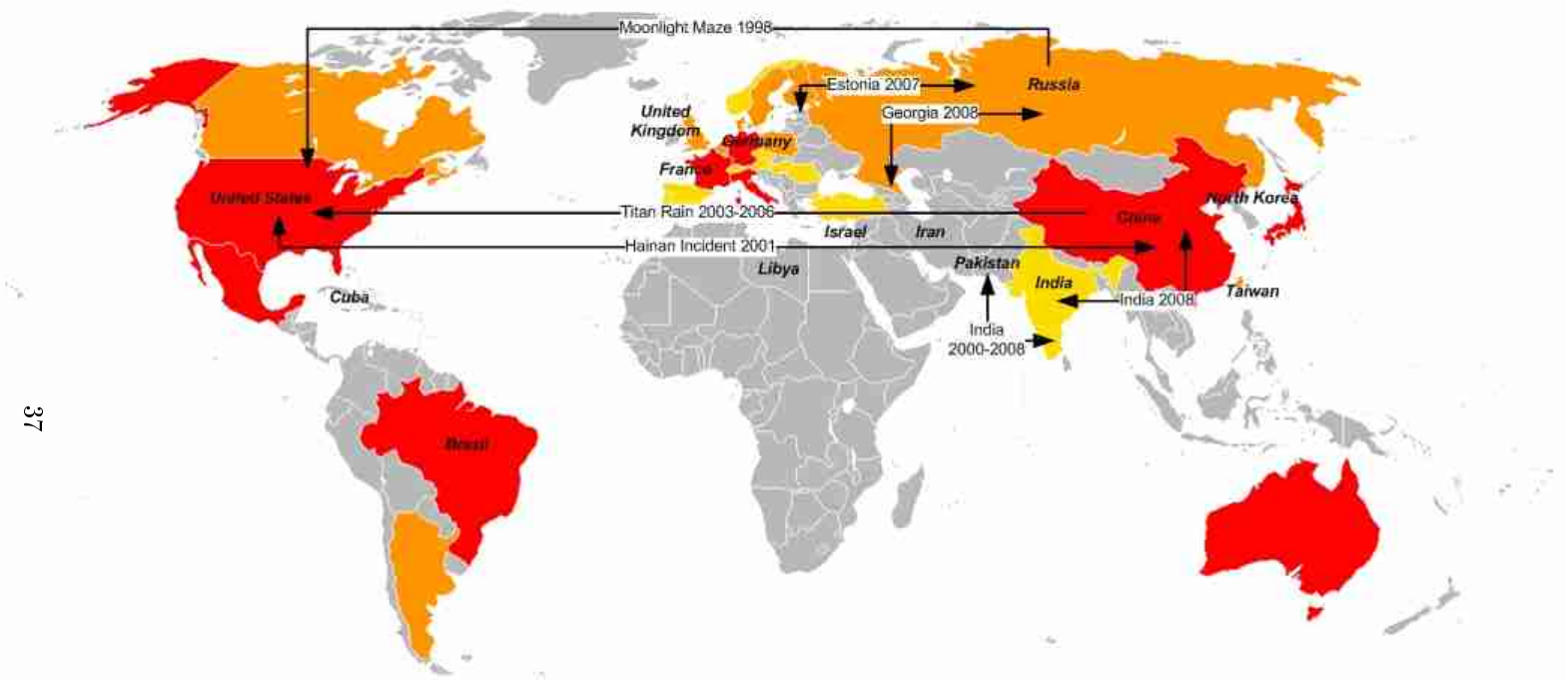
6 Conclusioni

In queste pagine si sono analizzati i concetti di cyberwarfare e cyberterrorism e si sono evidenziati alcuni casi di studio di particolare rilievo. Sebbene finora si sia assistito solo a quella che potremmo definire una low level information warfare [8], è indubbio che cyberwarfare e cyberterrorism siano due realtà le cui vere possibilità ed i cui veri effetti devono ancora essere scoperti.

Nel 2001 si stimava che oltre 30 paesi (tra cui Stati Uniti, India, Cina, Taiwan, Israele, Francia, Russia, Brasile e Pakistan [13, 5]) e decine di altre organizzazioni non-statali [6] avevano le possibilità di sostenere una cyberwarfare. A riprova dell'attualità di cyberwarfare e cyberterrorism, nel Febbraio del 2008, nel suo discorso annuale sulle minacce alla nazione, Michael McConnell, direttore della National Intelligence statunitense, ha citato lla Rete prima della guerra in Afghanistan [5].

Il fatto che non si sia assistito ancora a cyberwarfare di rilievo non significa che queste non siano reali; cyber reconnaisances e cyber attacks avvengono tutti i giorni sulla Rete e questi potrebbero essere gli atti precursori di una vera cyberwarfare. Dopotutto, a differenza di una guerra tradizionale, una cyberwarfare potrebbe scoppiare in qualsiasi momento e, se le difese dello stato attaccato dovessero resistere, la cyberwarfare potrebbe addirittura esaurirsi senza che il pubblico ne venga a conoscenza [12].

Parimenti, il fatto che non si sia ancora assistito a cyberterrorism di rilievo non significa che questo non sia reale; anzi è proprio la calma e l'assenza di atti terroristici significativi a far presagire la possibilità di prossimi attacchi devastanti. Infatti la pianificazione lunga e meticolosa di un attacco che sia drammatico e spettacolare è un marchio di organizzazioni terroristiche come Al Qaeda [16]; si è stimato che un attacco di cyberterrorism contro sistemi e reti multiple potrebbe richiedere da 2 a 4 anni di preparazione, mentre un attacco coordinato contro sistemi eterogenei, in grado di generare un consistente livello di caos, potrebbe richiedere da 6 a 10 anni di preparazione [22].



United States: paesi con note capacità di cyberwarfare o capacità di cyberwarfare in sviluppo (Fonte: Rapporti del Congresso US)

Rosso: paesi con un numero di host (i.e. computer connessi direttamente a Internet come gli ISP) compreso tra 316.000.000 e 9.000.0000 (Fonte: CIA World Factbook)

Arancione: paesi con un numero di host (i.e. computer connessi direttamente a Internet come gli ISP) compreso tra 8.000.000 e 3.500.000 (Fonte: CIA World Factbook)

Giallo: paesi con un numero di host (i.e. computer connessi direttamente a Internet come gli ISP) compreso tra 3.500.000 e 1.800.0000 (Fonte: CIA World Factbook)

Riferimenti bibliografici

[1] Tuomas Aura. Notes on network security. None, 2008.

[2] Garry Barker. Cyber terrorism a mouse-click away, July 2002.

[3] Indrajit Basu. India faces cyber challenge from china, May 2008.

[4] Bill Brenner. Myfip's titan rain connection, August 2005.

[5] Greg Bruno. The evolution of cyber warfare, February 2008.

[6] John Christensen. Bracing for guerilla warfare in cyberspace, April 1999.

[7] Richard Clarke. Pbs interview with richard clarke, March 2003.

[8] Kevin Curran, Kevin Concannon, and Sean McKeever. *Cyber Warfare and Cyber Terrorism*, chapter Chapter I: Cyber Terrorism Attacks, pages 1–6. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[9] Jason Fritz. How china will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala*, 8:28–80, 2008.

[10] Lech J. Janczewski and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[11] Brad Karp. Notes on distributed systems and security. None, 2008.

[12] Richard J. Jr. Kilroy. *Cyber Warfare and Cyber Terrorism*, chapter Chapter LI: The U.S. Military Response to Cyber Warfare, pages 439–445. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[13] Kenneth J. Knapp and William R. Boulton. *Cyber Warfare and Cyber Terrorism*, chapter Chapter III: Ten Information Warfare Trends, pages 17–25. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[14] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. Inside the slammer worm. *IEEE Security and Privacy*, 3:33–39, 2003.

[15] David Moore, Colleen Shannon, and Jeffrey Brown. Code-red: a case study on the spread and victims of an internet worm, 2002.

[16] Malcom W. Nance. *Terrorist Recognition Handbook*. CRC Press, 2008.

[17] John H. Nugent and Mahesh Raisinghani. *Cyber Warfare and Cyber Terrorism*, chapter Chapter IV: Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare, pages 26–34. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[18] Guido Olimpio. *AlQaeda.com*. BUR, 2008.

[19] Neil C. Rowe. *Cyber Warfare and Cyber Terrorism*, chapter Chapter XIV: Ethics of Cyber War Attack, pages 105–111. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[20] Michael A. Vatis. Cyber attacks during the war on terrorism: A predictive analysis. Technical report, Institute for Security Technology Studies, 2001.

[21] M. J. Warren. *Cyber Warfare and Cyber Terrorism*, chapter Chapter VI: Terrorism and the Internet, pages 42–49. Janczewski, Lech J. and Colarik, Andrew M., 2008.

[22] Clay Wilson. Botnets, cybercrime and cyberterrorism: Vulnerabilities and policy issues for congress. Technical report, Congressional Research Service, 2008.