Telematic Journal of Clinical Criminology
www.criminologia.org

Data pubblicazione maggio 2005

Psicologia del Cyberterrorista

Di Marco Strano

Testo tratto dal libro Cyberterrorismo, Jackson Libri, Milano, 2001

Introduzione

Con lo sviluppo del cyberspazio si affianca allo spazio di interazione fisico convenzionale (caratterizzato da una serie di singole intelligenze che interagiscono), un sistema di relazioni digitali definito infosfera digitalizzata[1]. Questo sistema presenta delle peculiarità relazionali che sono al centro dell'interesse di molti studiosi del comportamento umano. I gruppi terroristici che si muovono nel nuovo ecosistema digitale comprendono presumibilmente soggetti che presentano delle caratteristiche diverse rispetto a quelli dei modelli terroristici tradizionali e questa diversità necessita di contenuti teorici nuovi anche per quanto attiene agli studi sulle dinamiche psicologiche correlate. L'avvento e lo sviluppo delle reti telematiche, con la loro capacità di travalicare i limiti spaziali e temporali ha infatti reso obsoleti in Criminologia i quadri teorici e metodologici relativi alla ricerca sulle modalità di proselitismo, di organizzazione, di reclutamento e di comunicazione da parte di molti sodalizi terroristici. Il mezzo informatico, nell'ambito delle organizzazioni terroristiche, suggerisce ad esempio delle valutazioni criminologiche sulle dinamiche di percezione del crimine e su quanto "l'acting out" possa essere facilitato dalla situazione più "distaccata" generata dalla mediazione del computer tra il soggetto terrorista e l'obiettivo dell'azione terroristica[2]. Dagli ambienti militari giungono indicazioni compatibili con tale quadro concettuale e si rileva la tendenza a considerare i nuovi soldati telematici come aventi delle caratteristiche specifiche. Qiao Liang e Wang Xiangsui affermano ad esempio, a proposito dell'InfoWar, che "*In un mondo in cui la <<guerra nucleare>> sembra destinata a diventare un'espressione desueta, è probabile che un gracile studioso con le lenti spesse sia più adatto a divenire un moderno soldato rispetto a un giovane nerboruto dalla fronte bassa. La miglior dimostrazione di ciò è la storia, che circola negli ambienti militari occidentali, di un tenente di vascello che usava il modem per tenere sotto controllo un'intera divisione navale. Il combattente digitale sta sostituendo il guerriero che affrontava di petto il nemico: un ruolo che per secoli è rimasto invariato*." [3] La dimensione psicologica più interessante è così attinente, a nostro avviso, alla peculiarità delle strutture personologiche dei militanti di gruppi terrroristici che hanno affidato al cyberspazio la loro dimensione logistica, organizzativa e comunicazionale. La personalità di tali soggetti potrebbe infatti presentare numerose differenze con quella degli appartenenti a gruppi terroristici tradizionali. Tali differenze sono relative, a nostro avviso, al fatto che una buona parte dell'attività operativa dei gruppi cyberterroristi può avvenire attraverso la mediazione di un computer con una grande limitazione dei contatti face-to-face. Di fatto, con l'utilizzo della telematica per comunicare e organizzare la struttura, gli appartenenti a una compagine terroristica potrebbero trovarsi ad uscire dalla dimensione digitale nella sola fase finale dell'esecuzione di un atto militare, o alcuni di loro addirittura non uscirne per niente in caso di attacco mediante sistemi informatici (es. con l'introduzione di virus). In un futuro scenario mondiale massivamente interconnesso dalla telematica, sarà quindi possibile per i

[1] Di Maria F., Cannizzaro S., *Reti telematiche e trame psicologiche*, Franco Angeli, Milano, 2001
[2] Strano M., *Computer crime*, ed. Apogeo, Milano, 2000.
[3] Articolo "*Guerra senza limiti*" di Qiao Liang e Wang Xiangsui con prefazione "I bravi colonnelli" di Fabio Mini nel volume Limes, Quaderni Speciali 30-ott-2001, "Nel Mondo di Bin Laden".

terroristi approfittare di persone psicologicamente e fisicamente inadeguate per operazioni militari ma adatte a operazioni distruttive "a tavolino" utilizzando un computer. In base a tali concettualizzazioni ipotizziamo così la configurazione di nuovi profili psicologici di terroristi, legati più alla cultura della tecnologia digitale che a quella paramilitare del secondo millennio[4].

Attacchi esclusivamente digitali e attacchi misti

Tra le attività delle organizzazioni cyberterroristica analizziamo per prime le intrusioni telematiche che costituiscono una dinamica criminale di grande interesse per gli studiosi del settore e un fattore di notevole allarme istituzionale. Le ragioni che fanno accedere un hacker terrorista abusivamente all'interno di sistemi critici hanno ipoteticamente tre motivazioni:

1. per neutralizzarli o rallentarli
2. per acquisire informazioni, dati e codici (di accesso, di carte di credito eccetera)
3. per far fare al sistema delle operazioni non autorizzate

Come spiegherà in maniera più esaustiva e dettagliata Benedetto Negre nella seconda parte di questo libro, gli attacchi ad un sistema critico possono essere: parzialmente informatici (quando per effettuare l'intrusione vengono acquisite informazioni anche in ambienti fisici) ed esclusivamente informatici (quando per effettuare l'intrusione l'hacker terrorista opera solo nell'ambito delle reti telematiche). Una intrusione *parzialmente informatica* o "mista", sfrutta appieno le potenzialità disponibili nel cyberspazio senza tralasciare azioni fisiche che solitamente saranno di supporto all'attacco. Le azioni fisiche di supporto potranno, come ovvio, spaziare in base alla capacità organizzativa, economica e militare del gruppo terrorista. È da ritenere che questa potrebbe essere la forma più preoccupante di terrorismo informatico del prossimo futuro in cui saranno "fuse" tecniche e potenzialità tipiche dell'intelligence e dello spionaggio "Nation-State" a tecniche digitali. Le operazioni miste necessitano di strutture organizzative sufficientemente ampie e dotate di risorse economiche e addestrative elevate. La seconda tipologia di attacco, quella esclusivamente informatica, è probabilmente più limitativa poiché alcune intrusioni a sistemi critici molto ben protetti sono oggettivamente difficili da realizzare senza un supporto all'attacco di tipo fisico (operato in ambiente non-digitale). Le operazioni interamente digitali presentano però dei vantaggi poiché, come è noto, "l'asimmetria" tra attaccante e attaccato è massima. In sostanza la necessità di risorse e di strutture organizzative che l'offensore deve acquisire in tali operazioni è minima rispetto al danno che potrebbe provocare all'obiettivo in caso di attacco portato a buon fine. Con buona probabilità questo tipo di attacco potrà essere effettuato anche da piccole organizzazioni o addirittura da forme di "terrorismo individuale" secondo un modello che potremmo definire da "unabomber virtuale". Altro grande vantaggio degli attacchi interamente digitali è costituito dall'assenza di un contatto fisico tra il terrorista e l'ambiente fisico che viene attaccato, con intuibile riduzione dei rischi di cattura. Nel valutare tali ipotetiche operazioni occorre a nostro avviso non dimenticare che il terrorista non è necessariamente un hacker in senso classico e non è necessariamente un appassionato di computer e reti. Un hacker terrorista potrebbe addirittura avere una certa avversione nei confronti di ciò che è "tecnologico". L'Information Technology può essere infatti percepita dal terrorista, o dal "generico" criminale, come un semplice strumento di cui si servirà solo fintanto che gli sarà utile e solo per specifici "lavori". In altri termini, se per il raggiungimento di un determinato obiettivo sarà ritenuto necessario un mix di competenze e strumenti sia digitali sia tradizionali il terrorista progetterà ed eseguirà presumibilmente un'azione mista, comprendente operazioni digitali e convenzionali insieme. In sostanza perché

[4] BINETTI G., "*L'estremismo politico: ricerche psicologiche sul terrorismo*", Angeli, Milano, 1982.

predisporre una comunque complessa operazione via rete se si ha la certezza di poter liberamente entrare, ad esempio, in un ospedale e sottrarre cartelle cliniche e/o l'hard disk di un computer? Ci saranno, quindi, strutture in cui sarà opportuna una intrusione fisica, altre in cui sarà più opportuno un'azione di tipo esclusivamente "digitale" e sicuramente strutture in cui l'approccio più remunerativo sarà tradizionale e digitale insieme. E' proprio tale pragmatismo a distinguere a nostro avviso l'hacker tradizionale da quello terrorista. Per il primo l'intrusione in un sistema critico è soprattutto una dimostrazione di competenza tecnica ed eventuali segmenti dell'operazione svolti nello spazio fisico (esempio la sottrazione di un computer portatile) sminuirebbero di fatto la soddisfazione legata alla riuscita dell'attacco. Per il secondo l'obiettivo finale è invece la riuscita dell'operazione a qualsiasi costo, anche a scapito dello "stile hacker".Dal punto di vista criminologico le differenze tra le operazioni esclusivamente informatiche e quelle parzialmente informatiche (o miste) sono riferibili principalmente alla differenze percettive nell'ambito dell'azione criminale. Nel primo caso assumono infatti valenza le concettualizzazioni tipiche della cybercriminologia legate all'intermediazione del computer tra autore e *scena criminis*. Nel secondo caso, essendo una parte dell'azione criminale condotta nell'ambiente non-digitale e in assenza quindi di tecnomediazione, la percezione della vittima e dei rischi di cattura da parte dell'autore è forse maggiormente assimilabile a dinamiche criminologiche di tipo tradizionale[5].

[5] Strano M., Computer crime, edizioni Apogeo, 2000