SecurityBrokers
Global Cyber Defense & Security Services

MASTER UNIVERSITARIO di II Livello

in

HOMELAND SECURITY

Università Campus Bio-Medico – Roma

Consorzio NITEL

PROJECT WORK

Analisi evolutiva delle dottrine e delle strategie in tema di Cyberwarfare, Cyberdefense e Cyberattack in riferimento agli Stati nazionali.

Analisi aggiornata a dicembre 2012.

Relatore: dott.ssa Flavia Zappa

Tutor: dott. Andrea Zapparoli Manzoni

ABSTRACT

Lo studio del *risk and crisis management* sta ricoprendo, negli ultimi anni, un ruolo sempre più strategico nella *governance* degli Stati. A livello globale i rischi di vario tipo sono diventati sempre più importanti a causa dell'intensificazione della globalizzazione e in questo scenario il *cyber crime* costituisce una minaccia sempre più importante e pericolosa.

Le guerre future sono suscettibili di essere effettuate, in parte o del tutto, nel *cyberspazio*. Il *cyberspazio* però ha le sue leggi: è facile colpire nell'anonimato; la *cyber war* produce effetti diversi, più efficaci, globali, cambia le dinamiche di attacco e di difesa; i tempi di reazione si fanno sempre più veloci; si perde la differenza tra ciò che è nazionale e ciò che è transnazionale; è soggetto a mutamenti tecnologici sempre più repentini; come scenario delle "nuove guerre", come le chiama Mary Kaldor, si sostituisce sempre di più allo spazio fisico, e la sua geografia è sempre più mutevole e fruibile da chiunque, non solo dagli Stati nazionali, che non sono più i detentori del monopolio della forza nel quinto dominio di combattimento.

Il progresso della società è stato da sempre accompagnato dall'evoluzione di tutti i suoi aspetti, come l'economia, la tecnologia e anche la guerra. Quest'evoluzione nel tempo è sempre più veloce, quello per cui ci prepariamo a combattere oggi, domani è già obsoleto e le generazioni di minacce si esauriscono sempre in minori anni, o addirittura mesi.

Per capire bene quanto siano letali le armi della *cyber war* odierna basti pensare al parallelismo del Professore Emerito Umberto Gori che ha paragonato la potenza distruttiva del virus Stuxnet a quella di un F-35 su un campo di battaglia della Prima Guerra Mondiale.

Appare sempre più evidente la necessità di rendersi sempre più flessibili per non fallire di fronte a queste nuove minacce, e di reinventarsi di fronte all'emergenza di eventi sempre più nuovi e inaspettati. In un mondo globalizzato il *cyber crime* è un

fenomeno da contrastare in modo transazionale. La logica che spinge i Paesi a convergere verso una policy globale non risponde solo ad un interrogativo su quali interessi ottenere da una politica comune, ma anche a quali costi si va incontro a restarne fuori. La condivisione delle informazioni in tempo reale è una delle chiavi di volta per la sicurezza proattiva e per evitare contagi esponenziali.

In questo scenario il Rapporto 2012 del sottogruppo Rosa del GdL *CyberWorld* presso il CASD/OSN nasce come punto di partenza per fornire ai diversi attori e alla comunità InfoSec italiana un'opera contenente informazioni, dati, concetti, ed elaborazioni utili per affrontare gli scenari globali sempre più mutabili e dinamici.

I temi affrontati in questo rapporto spaziano dal *cyber crime* all'*hacktivism*, dalla *cyber-information warfare* alla *cyber war*, con lo scopo di creare un documento che affronti il problema in modo completo e che ci permetta di non perdere il passo con le nuove minacce incentivando e sostenendo lo sviluppo di un elevato livello di sicurezza e capacità di resilienza. E questo lo fa creando un dizionario terminologico condiviso riferito alle tematiche affrontate, analizzando le maggiori minacce degli ultimi anni e tracciando le capacità in tema di *cyberwarfare, cyberdefense* e *cyberattack* dei diversi Stati nazionali.

L'anno 2011 è stato definito *annus horribilis*, il peggiore di sempre dal punto di vista delle *ICT Security* e le prospettive non sono di certo rosee, il trend per il 2012 non è affatto incoraggiante, sta emergendo un rilevante peggioramento della situazione.

In questo project work ci si prefigge il compito di integrare e aggiornare il Rapporto del sottogruppo Rosa del GdL *CyberWorld* a tutto il 2012 attraverso documenti recepiti da fonti aperte, organismi istituzionali, centri studi, paper di accademici ed esperti, articoli di organi di stampa di settore e attendibili per evidenziare e capire cosa e come sta cambiando, se si stanno configurando nuovi scenari nella scacchiera internazionale in ambito *cyber* e quali dinamiche regolano le nuove minacce che ci dobbiamo preparare a combattere o quanto meno a mitigare.