Terza conferenza annuale sull'*Information Warfare*

# ARMI CIBERNETICHE E PROCESSO DECISIONALE

## Giovedì 8 Novembre 2012

## Aula Magna Università di Roma "La Sapienza"

*Per informazioni si prega di contattare* rome2012@infowar.it
*Per iscrizioni* www.infowar.it

### I) Obiettivi della conferenza

La conferenza "*Armi cibernetiche e processo decisionale*" si terrà a Roma l'8 novembre 2012 presso l'Aula Magna dell'Università di Roma "La Sapienza". Essa rappresenta la terza di una serie di conferenze annuali sull'*info-war* e le sue implicazioni per la sicurezza del sistema-Italia.

L'evento è promosso dal CSSII (Centro di Studi Strategici, Internazionali e Imprenditoriali dell'Università di Firenze), dalla Link Campus University, dall'ISPRI (Istituto per gli Studi di Previsione) e dal Centro Studi "Gino Germani". Esso è ideato dai promotori d'intesa con Maglan Information Defense & Intelligence.

La conferenza è destinata ad un pubblico qualificato comprendente le istituzioni nazionali civili, militari e della sicurezza, le imprese, le università e i centri di ricerca. Essa si prefigge due obiettivi di fondo:

1) Approfondire la conoscenza e aumentare la consapevolezza, tra i decisori politici ed economici del sistema-Italia, dell'emergere di **nuove armi cibernetiche** offensive e difensive, della loro futura evoluzione, nonché dei problemi inediti che esse creano per i **processi decisionali** nel campo della sicurezza nazionale e nel settore privato.

2) Riunire esperti e analisti - provenienti da organismi governativi civili e militari, dal mondo economico e finanziario, dalle Università e i centri di ricerca scientifica - per dare un contributo di idee e proposte concernenti:

   a) l'elaborazione di una **strategia di sicurezza cibernetica nazionale** per il sistema-Italia;

   b) l'introduzione di innovazioni organizzative nell'**architettura decisionale** di sicurezza nazionale allo scopo di potenziarne le capacità sia di prevenzione sia di reazione efficace e tempestiva a eventuali minacce o attacchi di *cyber-war* contro interessi vitali del nostro Paese.

**La conferenza si articolerà in tre sessioni:**

- **Prima sessione –** La sfida delle *cyber-weapons* al processo decisionale: verso una strategia di sicurezza cibernetica nazionale.

- **Seconda sessione -** Le armi cibernetiche difensive e offensive e la loro futura evoluzione: profili tecnologici e implicazioni per il ciclo OODA

- **Terza sessione -** L'impiego delle cyber-weapons nella business intelligence offensiva.

## II) Quadro di riferimento e spunti di riflessione

Un numero crescente di Stati, a partire dalle grandi potenze, sta sviluppando *cyber-weapons* a elevata potenza distruttiva (esempi di tali armi sono "Stuxnet" e "Flame" , mentre "Duqu", secondo alcuni esperti, non rientrerebbe fra le armi cibernetiche perché sarebbe essenzialmente uno strumento di spionaggio e non di distruzione).

Benché la costruzione delle più avanzate *cyber-weapons* per ora sia alla portata solo di attori statali, aspirano ad acquisire tali armi anche attori non-statali illeciti, come determinate formazioni terroristiche e organizzazioni criminali transnazionali. Molti Paesi, inoltre, si stanno dotando di dottrine strategiche, sia difensive che offensive, di *cyber-war.*

La creazione di armi cibernetiche sempre più sofisticate e potenti, resa possibile da innovazioni scientifiche e tecnologiche prodotte a ritmo accelerato, è destinata a trasformare la geopolitica globale, dando vita a nuove forme di conflittualità e nuovi fenomeni di minaccia alla sicurezza degli Stati e del sistema internazionale.

Gli attacchi con armi cibernetiche più pericolosi sono sia quelli che mirano a paralizzare un intero paese colpendo le sue infrastrutture critiche (con effetti potenzialmente catastrofici sulla popolazione) sia quelli tesi a colpire precipuamente il processo decisionale e la capacità di reazione dello Stato bersaglio dell'aggressione. Anche quando non perseguono deliberatamente quest'ultima finalità, tutti gli attacchi cibernetici su vasta scala, o anche la sola loro minaccia, creano enormi problemi di *decision-making* per il bersaglio.

Le armi cibernetiche rappresentano un problema che non riguarda solo i settori militare, politico, diplomatico, della protezione civile o della sicurezza nazionale. Alcuni tipi, non-militari, di *cyber-weapons* cominciano a essere impiegati anche da attori privati nella lotta per il potere economico e finanziario, nonché come strumento di influenza e "manipolazione delle percezioni" (*perception management*).

Le *cyber-weapons* conferiscono a chi le detiene capacità senza precedenti per influenzare le decisioni di un avversario oppure per disturbare e paralizzare i suoi centri di comando e controllo. Ciò può essere fatto sferrando un cyber-attacco massicciamente destabilizzante (una sorta di "11 settembre 2001 cibernetico") alle infrastrutture critiche di un paese, ovvero tramite azioni più subdole di manipolazione ed "eterodirezione" della sua opinione pubblica e leadership politica.

A parte il loro già noto potenziale distruttivo, le armi cibernetiche vengono impiegate per ottenere due diversi tipi di effetti sul processo decisionale:

a) influenzare le scelte del decisore avversario, nell'interesse dell'attaccante, provocando forti reazioni nell'opinione pubblica, oppure manipolando e danneggiando i suoi dati e informazioni;

b) diffondere incertezza e confusione tra i decisori avversari allo scopo di complicare, rallentare e, se possibile, paralizzare il loro processo decisionale e la loro capacità di risposta.

Le caratteristiche peculiari degli attacchi cibernetici rappresentano quindi una sfida senza precedenti al *decision-making* degli Stati. In primo luogo, tali attacchi sono caratterizzati da una "compressione del tempo": è praticamente nullo l'intervallo che intercorre tra il lancio di un attacco e i suoi effetti. I decisori politici e militari del paese bersaglio non dispongono, pertanto, di tempi sufficienti per elaborare e mettere in atto una risposta efficace *in kind*, e hanno anche la difficoltà di individuare con certezza l'attaccante, in tempo reale. Unica possibile soluzione, oltre a misure di prevenzione tramite operazioni di *cyber-* e *network-intelligence*, sarebbe quella consistente in un attacco *pre-emptive* suscettibile di porre, per alcuni, problemi di costituzionalità e di compatibilità con i principi della Carta dell'ONU.

In secondo luogo - come già detto - gli attacchi producono una situazione di diffusa e intensa incertezza che indebolisce le capacità dello Stato aggredito di contrastare l'*escalation* di una eventuale crisi. Tale incertezza deriva, in parte, dall'estrema difficoltà di individuare l'autore dell'aggressione. Inoltre, risulta molto problematico per la *leadership* politica stabilire, in tempo utile, se l'attacco rappresenti o meno un'azione di guerra da parte di uno Stato o provenga invece da un attore non-statale ostile.

Alla luce delle brevi considerazioni di cui sopra, si rende sempre più necessaria l'elaborazione di una strategia di sicurezza cibernetica nazionale per l'Italia, atta a proteggere gli interessi vitali del nostro Paese da minacce provenienti dal ciberspazio sia in tempi di pace che in condizioni di guerra o di crisi. Una *cyberspace strategy* italiana dovrà tenere in attenta considerazione lo sviluppo di nuove armi cibernetiche e le minacce ai processi decisionali sensibili del sistema-paese.

Un elemento centrale di tale strategia dovrebbe essere l'accelerazione del ciclo OODA (*Observe-Orient-Decide-Act*), che richiede un continuo potenziamento della *warning* intelligence, la massima velocizzazione delle decisioni e l'adozione di un concetto di "difesa offensiva" (cioè non meramente passiva) che non esclude perciò la possibilità di risposte "*pre-emptive*" nell'eventualità di una concreta e immediata minaccia di attacco di *cyber-war* al sistema-paese.

Gli elementi fondamentali del ciclo OODA nella guerra cibernetica (difensiva o offensiva) sono i seguenti:

- "Osservazione": i potenziali avversari e le vulnerabilità (proprie e degli avversari) devono essere identificati tramite attività di intelligence (e in particolare la raccolta tecnologica di dati).
- "Orientamento": i dati raccolti devono essere analizzati e sintetizzati in una gamma ampia di possibili scenari.
- "Decisione": deve essere presa una chiara decisione circa il corso di azione da intraprendere.

- "Azione" : la decisione deve essere attuata tramite determinati meccanismi fisici o logici.

L'accelerazione del ciclo OODA difficilmente potrà essere realizzata senza l'introduzione di significative innovazioni organizzative nell'architettura decisionale in materia di sicurezza e difesa, tra cui la creazione di un *national security council* italiano: una struttura chiamata a garantire una elevata integrazione dei processi decisionali in tema di sicurezza nazionale. In una situazione di crisi provocata da attacchi o concrete minacce di *cyber-war* tale struttura dovrebbe consentire ai decisori di reagire con la massima rapidità ed efficacia. In tempi di normalità, invece, essa

dovrebbe svolgere un'attività accurata e costante di prevenzione e di pianificazione strategica e operativa.

## III) Board della Conferenza

***Comitato Scientifico***

Prof. Umberto Gori (Emerito Università di Firenze, Presidente CSSI e Direttore ISPRI)*;*
On. Prof. Vincenzo Scotti (Presidente Link Campus University);
Prof. Luigi Sergio Germani (Link Campus University e Direttore del Centro Studi "Gino Germani")

***Chairman della conferenza:*** Ing. Paolo Lezzi (Amministratore Delegato Maglan Europe)

***Consigliere tecnico*****:** Dr. Shai Blitzblau (Fondatore e Direttore Tecnico di Maglan - Information Defense & Intelligence; Head, Information Warfare Research Labs)

***Consigliere militare****:* Amm. Sq. Ferdinando Sanfelice di Monteforte (Presidente del Gruppo di Lavoro Militare del Comitato Italiano Atlantico, già Rappresentante Militare d'Italia presso la NATO e la Commissione Europea).