1ª CONFERENZA ANNUALE SU INFORMATION WARFARE

**INFORMATION WARFARE: LE NUOVE MINACCE PROVENIENTI DAL CIBERSPAZIO ALLA SICUREZZA NAZIONALE ITALIANA**

**ROMA, 6-7 OTTOBRE 2010**

## I) Obiettivi della conferenza

Il convegno "***Information Warfare: le nuove minacce provenienti dal ciberspazio alla sicurezza nazionale italiana***" si terrà a Roma il 6-7 ottobre 2010. Esso rappresenta la prima di una serie di conferenze annuali sull'*info-war* e le sue implicazioni per la sicurezza del sistema-Italia.

L'evento è promosso dalla Link Campus University, dal CSSI (Centro di Studi Strategici e Internazionali dell'Università di Firenze), dall'ISPRI (Istituto per gli Studi di Previsione), e dal Centro Studi "Gino Germani". Esso è ideato dai promotori d'intesa con la Maglan Information Defense and Intelligence e si avvale del supporto di Unicredit Group. La conferenza ha già ottenuto il patrocinio del Ministero degli Affari Esteri.

Nel primo giorno (il 6 ottobre) si terrà una riunione ristretta a porte chiuse (circa 25 - 30 personalità istituzionali) a Palazzo Salviati presso il Centro Alti Studi Difesa (CASD). Nel secondo giorno la partecipazione all'evento, che si terrà nella Sala Conferenze di Unicredit all'EUR, sarà estesa anche a partecipanti provenienti da tutte le istituzioni nazionali civili e militari, dal mondo economico, dalle università, dagli istituti di ricerca e dai mass media.

Il convegno si prefigge due obiettivi di fondo:

1) Approfondire la comprensione e aumentare la consapevolezza tra i decisori politici e aziendali italiani delle minacce cibernetiche e di *information warfare* alla sicurezza nazionale, nonché delle più efficaci contromisure e strategie per contrastare e contenere tali minacce.

2) Riunire esperti e analisti provenienti da organismi governativi civili e militari, dal mondo dell'impresa, dalle Università e i centri di ricerca scientifica per dare un contributo innovativo di idee e proposte utili all'elaborazione di una strategia italiana di sicurezza nazionale nel campo dell'*information warfare,* della *cyber-defense*, e della *network intelligence*.

## II) Quadro di riferimento concettuale

"*Information warfare*" è un concetto complesso che ha diverse dimensioni e significati. Dal punto di vista offensivo il termine "*Information warfare*" si riferisce ad attacchi informatici o comunicativi/mediatici, tesi ad aggredire, danneggiare, sottrarre o manipolare le "informazioni" di un avversario, ovvero a manipolare le sue percezioni della realtà o i suoi stati psicologici[1].

Le tecniche offensive di *information warfare* vengono applicate sia in contesti di conflittualità bellica sia, più in generale, in tutte le arene competitive politiche ed economiche. Lo scopo è sempre volto a conseguire un vantaggio competitivo sull'avversario attaccandolo con strumenti informatici, mediatici o dell'intelligence/controintelligence.

L'*information warfare* comprende pertanto un ampio spettro di minacce, dalle operazioni di disinformazione tese a manipolare le percezioni dei decisori politici o a diffondere stati di confusione e panico tra la popolazione, alle aggressioni cibernetiche di vario tipo.

Gli analisti prendono in considerazione quattro tipi principali di minaccia cibernetica alle società tecnologicamente avanzate:

A) La ciber-guerra (*cyber-war*);

B) Il ciber-terrorismo/ciber-eversione (*cyber-terrorism/cyber-subversion*);

C) Il ciber-spionaggio (*cyber-espionage*);

D) La ciber-criminalità (*cyber-crime*).

Si tratta di fenomeni in rapida evoluzione. Mentre attualmente sono il ciber-spionaggio e la ciber-criminalità a provocare i danni maggiori alle società avanzate (insidiando i loro sistemi economici), in un futuro non lontano i maggiori rischi per la sicurezza potrebbero venire dalla *cyber-war* e dal *cyber-terrorism*[2]. Diversi Stati hanno già acquisito la capacità di effettuare attacchi cibernetici contro infrastrutture critiche civili e militari di altri Paesi.

---

[1] Cfr. *Information Warfare: Una Nuova Minaccia alla Sicurezza Nazionale* (a cura di L. Sergio Germani), relazioni presentate al convegno "Information Warfare", organizzato dalla Link Campus University e dal Centro Studi "Gino Germani", edizioni *Modernizzazione e Sviluppo,* Roma 2004.

[2] Joseph Nye Jr., *Cyber Power,* Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, p. 16; Umberto Gori (a cura di) , *Modelling Cyber Security: Approaches, Methodology, Strategies*, NATO Science For Peace And Security Series, Amsterdam, 2009.

I fenomeni di *information warfare* e le minacce provenienti dal ciberspazio rappresentano una sfida inedita del XXI secolo e richiederanno profondi mutamenti nei modi di pensare e organizzare la sicurezza dei sistemi-paese e delle aziende.

## III) Quesiti della conferenza

I quesiti che verranno posti nel corso della conferenza sono i seguenti:

1) Qual è il profilo e il livello delle principali minacce di *information warfare* e di ciber-aggressione (ciber-guerra, ciber-terrorismo/ciber-eversione, ciber-spionaggio, ciber-criminalità) alla sicurezza dell'Italia? Come potrebbero evolversi a medio e lungo termine?

2) Quali sono le ripercussioni attuali e potenziali di tali fenomeni per la sicurezza nazionale italiana nelle sue varie dimensioni (sicurezza militare, sicurezza interna dello Stato, sicurezza economico-finanziaria nazionale, sicurezza e competitività delle imprese nazionali d'importanza strategica)?

3) Quali sono le più efficaci contromisure e gli strumenti operativi e giuridici per contrastare e contenere le minacce dell'*information warfare* offensiva?

4) Come rafforzare le capacità di protezione delle informazioni e di ciber-difesa del sistema governativo, del sistema militare e delle imprese? Come potenziare le capacità della comunità intelligence di prevenire eventuali attacchi di *information warfare* alle infrastrutture critiche civili o militari?

*5)* Quali sono i connotati del nuovo *information warfare battlespace*, che oggi include le infrastrutture di importanza vitale per il funzionamento dell'economia, del sistema governativo e degli apparati militari e di sicurezza delle società avanzate?

6) Come promuovere e sviluppare la cooperazione fra organismi governativi civili e militari, imprese e mondo accademico e della ricerca scientifica nelle attività di contrasto alle minacce cibernetiche e di *information warfare*?

7) Quali potrebbero essere i lineamenti fondamentali di una strategia di sicurezza nazionale nel campo della ciber-sicurezza e dell'*information warfare*?

Per ulteriori informazioni si prega di contattare i responsabili scientifici del convegno:

Prof. Umberto GORI (presidente@cssi.unifi.it);

Prof. Luigi Sergio GERMANI (l.germani@unilink.it).