



Seconda conferenza annuale sull'*Information Warfare*

## **LA SFIDA DELLA CYBER-INTELLIGENCE AL SISTEMA-ITALIA**

**Strategie e tattiche di *info-war* e di *network intelligence*:  
dalla sicurezza delle imprese alla sicurezza nazionale**

**Roma, Sala conferenze di Confindustria, 27 ottobre 2011**

### **I) Obiettivi della conferenza**

La conferenza "*La sfida della cyber-intelligence al sistema-Italia*" si terrà a Roma il 27 ottobre 2011 presso la sala conferenze di Confindustria. Essa rappresenta la seconda di una serie di conferenze annuali sull'*information warfare* 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 & Intelligence. La conferenza - destinata ad un pubblico qualificato comprendente le istituzioni nazionali civili e militari, le imprese, le università e i centri di ricerca scientifica - si prefigge due obiettivi di fondo:

1) Approfondire la comprensione e aumentare la consapevolezza tra i decisori politici e aziendali italiani della crescente rilevanza strategica della *cyber-intelligence* per la sicurezza nazionale e la sicurezza e la competitività delle imprese italiane, con particolare riferimento a tre aspetti:

- a) Come la rivoluzione nelle tecnologie informatiche e delle comunicazioni sta trasformando l'intelligence governativa, la *business intelligence* e la *security aziendale*.
- b) Il ruolo e le funzioni della *cyber-intelligence* nella tutela della sicurezza nazionale e della sicurezza e competitività delle imprese italiane.
- c) La crescente minaccia del *cyber-espionage* condotto da servizi d'intelligence esteri, nonché da entità non-statali e strutture private d'intelligence, alle Istituzioni governative civili e militari, nonché alle industrie e ai centri di ricerca scientifica nazionali.

2) Riunire esperti e analisti provenienti da organismi governativi civili e militari, dal mondo dell'impresa e bancario, e dalle Università e i centri di ricerca scientifica per dare un contributo di idee e proposte innovative finalizzate al potenziamento delle capacità di *cyber-intelligence* del sistema-Italia.

La conferenza si articolerà in tre sessioni:

- Prima sessione: *cyber-intelligence e sicurezza nazionale italiana: prospettive strategiche*;
- Seconda sessione: *strumenti e tecniche operative di network intelligence e spionaggio cibernetico*;
- Terza sessione: *cyber-intelligence: sfide e opportunità per il sistema economico nazionale e le imprese*.

**II) Quadro di riferimento concettuale** (a cura di Luigi Sergio Germani e Umberto Gori, Responsabili scientifici della Conferenza, e Shai Blitzblau, Consigliere tecnico)

La rivoluzione nel campo delle tecnologie informatiche e delle comunicazioni (ICT) sta determinando una profonda trasformazione sia dell'intelligence governativa sia della business intelligence e della *security* aziendale.

Le comunità d'intelligence in tutto il mondo stanno affrontando le sfide della “*Revolution in Intelligence Affairs*” innescata dallo sviluppo e la diffusione sempre più pervasivi delle tecnologie ICT: una trasformazione del mondo dell'intelligence analoga alla “*Revolution in Military Affairs*” che già da diversi anni investe gli apparati militari.

La *Revolution in Intelligence Affairs* sta trasformando le quattro principali tipologie di attività svolte dai servizi d'intelligence:

- A) La *ricerca*, ovvero la raccolta di informazioni tramite fonti umane (HUMINT), mezzi tecnici (quale ad esempio la SIGINT) e fonti aperte (OSINT);
- B) L'*analisi e produzione*, e cioè la valutazione dell'accuratezza e attendibilità delle notizie raccolte, la loro integrazione, analisi, interpretazione, e la predisposizione di rapporti intelligence destinati al decisore politico;
- C) L'*influenza (covert action)*, vale a dire operazioni occulte finalizzate a influire sulle decisioni di un governo estero oppure a incidere sull'evolversi di determinate situazioni politiche, militari, economiche o sociali in un paese estero.
- D) La *controintelligence*, ossia le attività tese a conoscere (tramite la ricerca e l'analisi) e a contrastare le operazioni d'intelligence condotte da servizi informativi stranieri.

I servizi d'intelligence di molti paesi del mondo (nonché determinate strutture private d'intelligence) conducono le sopramenzionate attività, in misura crescente, nel ciberspazio, avvalendosi di tecniche di ricerca e analisi fondate sull'uso di strumenti cibernetici (*cyber-tradecraft*). Ad esempio:

- Le tecnologie ICT hanno consentito lo sviluppo di nuove e potenti tecniche di ricerca informativa denominate *network intelligence*, tra cui vi sono le tecniche per l'acquisizione di notizie segrete o sensibili dai sistemi informatici di un bersaglio tramite intrusioni o intercettazioni.
- Oggi le attività di raccolta di notizie provenienti da fonti aperte (OSINT) sul web possono avvalersi di strumenti nuovi e molto più avanzati rispetto ai motori di ricerca classici.
- Una nuova frontiera dell'analisi delle fonti aperte è il monitoraggio di *blog* e *social network* finalizzato alla conoscenza dei trend nelle percezioni e negli atteggiamenti di opinioni pubbliche in paesi esteri d'interesse, il che può consentire a un servizio d'intelligence di prevedere l'insorgere di eventuali fenomeni di crisi socio-politica in tali paesi.
- Lo spazio cibernetico viene utilizzato da servizi d'intelligence stranieri per condurre operazioni di disinformazione strategica, una delle più tipiche forme di *covert action*, la cui finalità è la manipolazione delle percezioni dei decisori politici e/o delle opinioni pubbliche di un paese estero bersaglio.
- Molti servizi d'intelligence stanno sviluppando strategie e strumenti di “*cyber-controintelligence*” (*cyber CI*): un'attività volta a conoscere, contrastare e/o manipolare le operazioni di *cyber-intelligence* e *cyber-espionage* condotte da servizi avversari.

La “*Revolution in Intelligence Affairs*”, di cui abbiamo brevemente descritto gli aspetti più salienti, presenta una serie di complesse minacce alla sicurezza e alla competitività del sistema-Italia e delle sue imprese, tra cui: a) attività crescenti di *cyber-espionage* finalizzate all'acquisizione di informazioni segrete o sensibili di carattere politico, militare, economico-finanziario, industriale, e scientifico-tecnologico; b) *information operations* effettuate nello spazio cibernetico miranti a manipolare le percezioni dei decisori

politici nazionali e/o dell'opinione pubblica; c) *covert actions* condotte nello spazio cibernetico tese a destabilizzare l'economia nazionale tramite manovre speculative sui mercati azionari e valutari.

Dall'altra parte, la trasformazione in corso nel mondo dell'intelligence offre alla comunità d'intelligence nazionale la possibilità di avvalersi di nuovi e più potenti strumenti di ricerca e analisi basati sulla *network intelligence* e il *cyber-tradecraft*. Ciò al fine di potenziare le capacità del sistema d'intelligence italiano di fornire al decisore politico *early warnings* di carattere tattico e strategico circa possibili minacce o sviluppi critici sotto il profilo della sicurezza e dell'interesse nazionale.

La sfida della *cyber-intelligence* è molto significativa anche per il settore privato. Le imprese italiane sono vulnerabili di fronte al fenomeno crescente di *cyber-espionage* industriale, finanziario e scientifico-tecnologico pilotato da servizi d'intelligence esteri, nonché da attori non-statali e strutture private d'intelligence. Il *cyber-espionage* insidia, in particolare, il capitale intellettuale di un'impresa, che costituisce l'*asset* aziendale di maggiore valore. La rivoluzione in corso nel mondo dell'intelligence non è, tuttavia, soltanto una fonte di minaccia per le imprese italiane: essa offre alle aziende (anche alle PMI) un'opportunità per sviluppare le proprie capacità di *business intelligence* e di *corporate security intelligence*, grazie alla disponibilità di nuove metodologie e strumenti tecnologici per la raccolta e l'analisi di informazioni provenienti da fonti aperte sul web.

### **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, Sottosegretario agli Affari Esteri);  
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).