d'intesa con

promuovono

la 2ª Conferenza Annuale sull'Information Warfare

La sfida della Cyber Intelligence al sistema-Italia.

Strategie e tattiche dell'Information Warfare e della Network Intelligence.
Dalla sicurezza delle imprese alla sicurezza nazionale.

Roma, 27 Ottobre 2011

Auditorium della Tecnica di Confindustria

Medaglia del Presidente della Repubblica quale Suo "Premio di Rappresentanza" alla IWC 2011

Con il patrocinio di:
Senato della Repubblica - Camera dei Deputati - Presidenza del Consiglio dei Ministri
Ministero della Difesa - Ministero per lo Sviluppo Economico
Ministro per la Pubblica Amministrazione e l'Innovazione
Polizia di Stato

Giovedì 27 ottobre 2011
Auditorium della Tecnica di Confindustria
viale Tupini 65, Roma EUR

La sfida della Cyber Intelligence al sistema-Italia.

Strategie e tattiche dell' Information Warfare e della Network Intelligence. Dalla sicurezza delle imprese alla sicurezza nazionale.

Programma provvisorio

8:30 Accreditamento partecipanti

9:00 Inizio Lavori

- Apertura**: Paolo Lezzi, Chairman** (CEO Maglan Europe)
- Prolusione**: On. Prof. Vincenzo Scotti** (Sottosegretario agli Affari Esteri e Presidente Link Campus University)
- Introduzione generale: **Prof. Umberto Gori, Emerito Università di Firenze - Direttore Scientifico della Conferenza** (Presidente CSSI e Direttore ISPRI) e **Prof. Luigi Sergio Germani – Condirettore Scientifico della Conferenza** (Link Campus University e Direttore Centro Studi "Gino Germani")

9:30 **Prima Sessione:**

Cyber-Intelligence e Sicurezza nazionale italiana: prospettive strategiche

Chairman **Amm. Sq. Ferdinando Sanfelice di Monteforte, Consigliere Militare della Conferenza**.

- Gen. Div. Salvatore Farina (Capo del III Reparto di SMD in rappresentanza del Sig. Capo di Stato Maggiore della Difesa): **"Strategie di Cyber-Difesa per la protezione dell'Interesse Nazionale"**.

- Paolo Scotto di Castelbianco (Presidenza del Consiglio dei Ministri): **"La cyberminaccia: attori, mutamenti, sfide al sistema Paese. Il ruolo della cyber intelligence"**.

- C. Amm. Nicola De Felice (Stato Maggiore della Difesa – Centro per l'Innovazione della Difesa): **"Il ciberspazio quale nuovo dominio operativo per lo strumento militare nazionale"**.

- Col. CC. Lucio Lepore (Capo Ufficio Analisi Minaccia Asimmetrica del II Reparto Informazioni e Sicurezza, Stato Maggiore Difesa): **"Minaccia cibernetica e intelligence militare"**

- **Giancarlo Grasso** (Finmeccanica): **"NATO ed EU – Cyberwarfare: una sfida da affrontare insieme"**.

-**Gen. Fabio Mini** : **"I Servizi d'intelligence cinesi: strategie di spionaggio e influenza nello spazio cibernetico"**

Conclusione della Sessione da parte del Chairman.

11:20 ***Coffee break***

11:40 **Seconda Sessione:**

Strumenti e tecniche operative di network intelligence e controintelligence

- Shai Blitzblau, Direttore Tecnico della Conferenza (Maglan Information Defense & Intelligence, Founder and Head of Information Warfare Labs): **"Network intelligence tactics and dilemmas"**.

- Martin Borrett (Director - IBM Institute for Advanced Security Europe): **"IBM's Cyber Security Perspective".**

- Andrea Rigoni (Director - Global Cyber Security Center): **" Tecniche e metodi di cyber-espionage e cyber-exploitation"**

- Gen. B. Enrico Bologna - (Direttore del programma Defence Information Infrastructure presso il VI Reparto di SMD)**: "Prospettiva militare della sicurezza nel campo della Information and Communication Technology nell'era cibernetica".**

Conclusione della Sessione da parte del Chairman.

13:15 **Light lunch**

14:15 **Terza Sessione:**

Cyber-intelligence: sfide e opportunità per l'economia italiana ed il sistema finanziario

- Shai Blitzblau, Direttore Tecnico della Conferenza (Maglan Information Defense & Intelligence, Founder and Head of Information Warfare Labs): **"Valutazione della minaccia del cyber-spionaggio industriale ed economico alle aziende Italiane".**

- Paolo Campobasso (gia' Senior Vice President e Chief Security Officer, Unicredit Group): **"Intelligence industriale e finanziaria nel cyberspazio: un vantaggio competitivo in momenti di crisi ".**

- Nicola Mugnato (Elsag)**: "Evoluzione della minaccia: aspetti procedurali ed operativi di prevenzione e risposta"**.

Ringraziamenti da parte dei **Promotori**.

Chiusura lavori da parte del Chairman **Paolo Lezzi** - (CEO, Maglan Europe)**.**

I) Obiettivi della conferenza

La Seconda Conferenza Annuale sull'Information Warfare è promossa 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 le Ricerche Internazionali), e dal Centro Studi "Gino Germani". Essa è ideata d'intesa con Maglan Information Defense & Intelligence.

La conferenza che ha ottenuto il patrocinio del Senato della Repubblica, della Camera dei Deputati, della Presidenza del Consiglio dei Ministri, del Ministero della Difesa, del Ministero per lo Sviluppo Economico, del Ministro per la Pubblica Amministrazione e l'Innovazione.

L'evento 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 competitività delle imprese italiane.

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

II) Quadro di riferimento concettuale

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 dalla diffusione e dallo sviluppo 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:

1. La *ricerca*, ovvero la raccolta di informazioni tramite fonti umane (HUMINT), mezzi tecnici (quale ad esempio la SIGINT) e fonti aperte (OSINT);
2. L'*analisi e produzione*, e cioè la valutazione dell'accuratezza e attendibilità delle notizie raccolte, la loro integrazione, l'interpretazione e la predisposizione di rapporti di intelligence destinati al decisore politico;
3. 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.
4. 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:

1. attività crescenti di *cyber-espionage* finalizzate all'acquisizione di informazioni segrete o sensibili di carattere politico, militare, economico-finanziario, industriale, e scientifico-tecnologico;
2. *information operations* effettuate nello spazio cibernetico miranti a manipolare le percezioni dei decisori politici nazionali e/o dell'opinione pubblica;
3. *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.

Conference Board

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:

- **Ing. Paolo Lezzi** (Amministratore Delegato Maglan Europe)

Direttore 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)