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

Il convegno "*La sfida della cyber-intelligence al sistema-Italia*" si terrà a Roma il 27 ottobre 2011 presso la sala conferenze di Confindustria. Esso rappresenta la seconda 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.

L'evento è destinato ad un pubblico qualificato comprendente le istituzioni nazionali civili e militari, le imprese, le università e i centri di ricerca. Il convegno 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 il mondo dell'intelligence governativa, della business intelligence e della security aziendale.

b) Il ruolo e le funzioni della *cyber-intelligence* - e della *cyber-controintelligence* - 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* e *network intelligence* del sistema-Italia.

II) Quadro di riferimento concettuale[1]

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.

I servizi d'intelligence di molti paesi del mondo effettuano operazioni nello spazio cibernetico, sviluppando nuove tecniche operative d'intelligence e di *information warfare* fondate sull'uso di strumenti cibernetici (*cyber-tradecraft*)[2]. Ciò è destinato a trasformare le quattro principali tipologie di attività svolte dai servizi d'intelligence:

A) la ricerca (ovvero "raccolta") di informazioni tramite fonti umane, mezzi tecnici o fonti aperte.
B) l'analisi;
C) l'influenza (*covert action*);
D) la controintelligence.

A) *Ricerca*

Le tecnologie ICT hanno consentito lo sviluppo di nuove e potenti tecniche di ricerca informativa tramite lo spazio cibernetico denominate *network intelligence* (NETINT), che sono di due tipi: 1) tecniche per l'acquisizione di notizie segrete o sensibili (di carattere politico, militare, economico-finanziario, industriale o scientifico) dai sistemi informatici di un bersaglio tramite intrusioni, intercettazioni o lo sfruttamento di fughe di dati (ciò viene denominato *cyber-espionage* o *cyber-exploitation*) ; 2) strumenti nuovi, molto più avanzati rispetto ai motori di ricerca classici, per la raccolta di notizie da fonti aperte (OSINT) sul web.

Molti servizi d'intelligence esteri conducono attività di ricerca, in misura crescente, con strumenti di *cyber-espionage*. Inoltre, le tecnologie ICT hanno un notevole impatto sia sulle attività di ricerca con mezzi tecnici - in particolare SIGINT e COMINT - sia sulla HUMINT (la ricerca tramite fonti umane).

L'impiego del *cyber-tradecraft* facilita molto e moltiplica l'efficacia delle operazioni di HUMINT condotte da servizi d'intelligence esteri. Questi ultimi, ad esempio, effettuano un sistematico monitoraggio di fonti OSINT disponibili sul web (tra cui i *social network*) al fine di individuare persone in possesso di informazioni segrete o riservate da reclutare come fonti

[1] A cura del Prof. Luigi Sergio Germani e del Prof. Umberto Gori (responsabili scientifici della conferenza) .

[2] Anche le strutture private d'intelligence ricorrono in misura crescente al *cyber-tradecraft* . La diffusione di tecnologie ICT è infatti uno dei fattori che in anni recenti hanno favorito l'espansione del settore dell'intelligence privata e la crescente "privatizzazione" delle attività d'intelligence e spionaggio.

occulte. Inoltre, la gestione delle fonti viene facilitata e resa più sicura e meno costosa grazie all'impiego di strumenti di comunicazione clandestina nel ciberspazio.

B) *Analisi*

La rivoluzione tecnologica in campo ICT ha altresì un forte impatto sulle attività di analisi d'intelligence, soprattutto per quanto riguarda l'analisi delle fonti aperte (OSINT), che va configurandosi come una funzione sempre più importante nel ciclo d'intelligence a causa della crescita vertiginosa di notizie OSINT disponibili sul web (una parte non trascurabile delle quali sono di scarsa pertinenza, errate o frutto di attività di disinformazione), che rischia di provocare un "sovraccarico informativo" negli apparati d'intelligence.

L'aumento esponenziale di flussi informativi richiede pertanto un continuo potenziamento dell'analisi e degli strumenti tecnologici di supporto all'analista, che ha il compito di selezionare le notizie pertinenti, valutare la loro accuratezza e attendibilità, e interpretarle.

Una nuova frontiera dell'analisi OSINT è il monitoraggio di blog e *social network* finalizzato alla conoscenza dei trend nelle percezioni e gli 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 instabilità crisi socio-politiche in tali paesi.

C) *Influenza* (*covert action*)

Le attività dei servizi d'intelligence denominate *covert action* (operazioni di influenza) vengono svolte con sempre maggiore frequenza nello spazio cibernetico e si avvalgono di tecnologie informatiche di *info-war* strategica e tattica.

Il termine *covert action* abbraccia un ampio spettro di attività 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.

L'utilizzo del ciberspazio moltiplica l'efficacia delle azioni 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 paesi estero bersaglio, al fine di indurre tale paese ad assumere decisioni che sono nell'interesse dello Stato che ha promosso l'operazione d'influenza. Le *covert actions* effettuate nello spazio cibernetico possono avere finalità ostili di natura economico-finanziaria, quali ad esempio la destabilizzazione dell'economia di un paese tramite manovre speculative sui mercati azionari e valutari.

D) *Controintelligence*

Il campo della controintelligence è altresì destinato a subire significative trasformazioni come conseguenza della rivoluzione delle ICT[3]. Molti servizi d'intelligence stanno sviluppando

[3] La controintelligence è una branca dell'intelligence che comprende molteplici attività, sia difensive che offensive, tese a conoscere (tramite la ricerca e l'analisi), a contrastare e a manipolare (eventualmente sfruttando a proprio vantaggio) le operazioni ostili d' intelligence condotte dagli avversari.

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.

Tra le tecniche proattive di cyber CI vi è l'impiego dei cosiddetti *honeypots* e *honeynets*: sistemi appositamente predisposti per essere penetrati da un avversario al fine di raccogliere informazioni sui suoi obiettivi, modalità operative e tecniche di *cyber-espionage*. Inoltre, la *deception* – un'attività tipica della controintelligence – oggi viene condotta anche nel ciberspazio. Ad esempio, si consente a un servizio d'intelligence avversario di effettuare intrusioni informatiche per indurlo ad acquisire notizie false o fuorvianti, al fine sia di screditare i suoi sforzi di ricerca informativa (agli occhi dei decisori politici) sia di ridurre le probabilità che esso intraprenda azioni offensive più intense.

La "*Revolution in Intelligence Affairs*", di cui abbiamo brevemente descritto gli aspetti più salienti, presenta una serie di complesse minacce al sistema-Italia, ma costituisce anche un'opportunità per rafforzare il sistema d'intelligence nazionale e per sviluppare le capacità di business intelligence e corporate security intelligence delle imprese italiane.

Si tratta anzitutto di una sfida per la comunità d'intelligence nazionale, il cui ruolo nella tutela della sicurezza nazionale è destinato a crescere. La comunità d'intelligence dovrà fronteggiare nuovi fenomeni di minaccia al sistema-Paese derivanti da attività ostili di cyber-intelligence, tra cui:

1) Le 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* strategiche effettuate nello spazio cibernetico miranti a manipolare le percezioni dei decisori politici nazionali e/o dell'opinione pubblica per influenzare il processo decisionale nazionale nell'interesse di uno Stato (o attore non-statale) estero.

3) *Information operations* tattiche condotte nel ciberspazio tese a manipolare le percezioni dei decisori militari e influenzare il processo decisionale militare in teatri operativi.

4) Campagne di disinformazione economico-finanziaria sul web miranti a danneggiare la reputazione dell'Italia e/o delle sue più importanti imprese, o a influire sui mercati finanziari.

5) *Covert actions* cibernetiche tese a destabilizzare l'economia nazionale tramite manovre speculative sui mercati azionari e valutari.

Dall'altra parte, la trasformazione dell'intelligence offre alla comunità d'intelligence nazionale la possibilità di sviluppare nuovi e più potenti strumenti di ricerca e analisi basati sulla *network intelligence* e il *cyber-tradecraft* . Ciò consentirebbe il potenziamento delle capacità dei nostri Servizi d'intelligence di fornire al decisore politico *early warnings* di carattere tattico e strategico

circa possibili minacce (cibernetiche e non-cibernetiche) o sviluppi critici sotto il profilo della sicurezza e dell'interesse nazionale[4].

Per rispondere efficacemente alle sfide, e cogliere le opportunità, della *cyber-intelligence* è necessario attivare un rapporto sinergico fra organismi d'intelligence e sicurezza, industria (in particolare i gestori delle infrastrutture critiche), centri di ricerca scientifica e università.

La sfida è molto significativa anche per il settore privato, nell'ambito del quale le attività di *business intelligence* e di security aziendale sono destinate ad acquisire sempre maggiore importanza. 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 privati, sia leciti che illeciti (quali la criminalità organizzata). Il *cyber-espionage* insidia, in particolare, il capitale intellettuale delle imprese, che costituisce l'*asset* aziendale di maggiore valore. Considerata la gravità della minaccia si rende sempre più necessario per le aziende formulare una propria strategia di sicurezza da integrare nella loro *business strategy.*

La rivoluzione in corso nel mondo dell'intelligence non è soltanto una fonte di minaccia per le imprese italiane: essa offre alle aziende (anche alle PMI) un'opportunità per potenziare le proprie capacità di *business intelligence* (l'attività di raccolta e analisi di informazioni a sostegno del *decision-making* aziendale e della formulazione di strategie di business) e di *corporate security* intelligence. Ciò soprattutto grazie alla disponibilità sul web di una vasta gamma di fonti OSINT, nonché di nuove metodologie e strumenti tecnologici per la raccolta e l'analisi di informazioni provenienti dal web .

La *business intelligence*, praticata con strumenti legali ed etici e sulla base di informazioni OSINT, è una attività sempre più necessaria per le imprese. In una economia globalizzata, in cui la conoscenza è il principale motore di crescita, le informazioni rivestono una valenza strategica di primo piano, e la capacità di acquisirle e analizzarle in modo tempestivo è cruciale per la sopravvivenza e la crescita di un'azienda[5].

III) Struttura della conferenza e temi di discussione

Prima sessione – Cyber-intelligence e sicurezza nazionale italiana: prospettive strategiche

Possibili temi delle relazioni (indicazioni di massima da precisare con i relatori):

[4] L'*early warning* tattico é una tempestiva segnalazione al decisore politico di un attacco o evento critico imminente, mentre l'*early warning* strategico comunica al decisore importanti cambiamenti di medio-lungo periodo nel livello e/o nella natura della minaccia: l'emergere di nuovi tipi di avversari, lo sviluppo di nuove tecnologie offensive, cambiamenti nelle intenzioni o nelle capacità degli avversari.

[5] In considerazione di ciò, diversi governi (ad esempio, Francia, Svezia, Giappone e Germania) ravvisano nella *business intelligence* (detta anche "intelligence competitiva") un elemento importante delle loro politiche di sicurezza economica nazionale, e ne promuovono attivamente lo sviluppo e la diffusione nell'ambito del mondo dell'impresa.

- L'intelligence nel ciberspazio e nuove sfide alla sicurezza nazionale: minacce e opportunità per la comunità d'intelligence e per il sistema-Paese.

- *Information Warfare* e *cyber-defense* nazionale: una visione militare

- Spionaggio, influenza e ingerenza con strumenti cibernetici: profilo dei rischi per la sicurezza interna e gli interessi nazionali dell'Italia.

- Il ruolo della *cyber-intelligence* nella tutela della sicurezza esterna e degli interessi nazionali dell'Italia.

- Il supporto d'intelligence alla pianificazione per la gestione di crisi di sicurezza nazionale (con particolare riferimento a eventuali crisi provocate da azioni di *cyber-war*, *cyber-terrorism* o *info-war*).

- *Early warning* tattico e strategico di attacchi cibernetici alle infrastrutture critiche nazionali.

Seconda sessione - Strumenti e tecniche operative di network intelligence e spionaggio cibernetico

Possibili temi delle relazioni (indicazioni di massima da precisare con i relatori):

- Panoramica degli strumenti e tecniche operative del *cyber-espionage*

- Cyber-intelligence militare, *psy-ops* e *information warfare* tattico nei teatri operativi

- Tattiche delle *covert actions* in campo economico: l'uso di armi cibernetiche ai fini della destabilizzazione economico-finanziaria.

- *Cyber-espionage* finanziario e tecniche di manipolazione dei mercati borsistici

- Tecniche di *network intelligence* per lo sfruttamento delle fonti aperte.

Terza sessione - Cyber-intelligence : sfide e opportunità per il settore privato

Possibili temi delle relazioni (indicazioni di massima da precisare con i relatori):

- Profilo della minaccia *di cyber-espionage* industriale alle imprese italiane e strumenti di contrasto.

- Tecnologie ICT e nuove opportunità per il potenziamento della *business intelligence/ competitive intelligence* e della *corporate security intelligence*.

- L'analisi di *social media* e *social networks*: una nuova frontiera della OSINT nel settore privato:

- Covert actions economiche e disinformazione nel settore privato: profilo dei rischi e strumenti di contrasto.

- Profilo del fenomeno della privatizzazione delle attività di intelligence e spionaggio: implicazioni per le strategie di *security/ cyber-security* aziendale.

- Nuove tecnologie anti-spionaggio cibernetico per il settore privato.