Università degli Studi di Roma "Tor Vergata"
CISPA – Centro Interdipartimentale di Studi sulla PA
Master di II livello in **"Intelligence Economica"**

ABI
BANCHE ESICUREZZA 2013
Informazioni per la sicurezza, e la competitività del sistema Paese: una lettura combinata delle relazioni DIS e COPASIR

Prof. Luciano Hinna

Roma, 5 giugno 2013

Il master e le sue motivazioni

- **Dalla riforma del 2007 il "nuovo" approccio dell'Intelligence di Stato è stato quello di promuovere la cultura dell'Intelligence Economica**
- **L'Intelligence Economica è una disciplina in piena evoluzione che coinvolge Intelligence Istituzionale e Intelligence Aziendale nella tutela della competitività del sistema Paese**

L'oggetto dell'analisi di oggi

- La relazione del DIS (Dipartimento di Informazione per la Sicurezza) sulla "politica dell'informazione per la sicurezza" presentata qualche settimana fa
- La relazione annuale del COPASIR (Comitato Parlamentare per la Sicurezza delle Repubblica)
- Sono relazioni destinate a soggetti Istituzionali ma sono tuttavia ricche di spunti anche per l'operatività e l'azione strategica delle imprese

Lo scenario di fondo 1/3

- La sicurezza del Paese passa per la sicurezza delle sua aziende e la sicurezza delle aziende non può prescindere dalla sicurezza del paese.
- La riforma del 2007 ha esteso la competenza dell'intelligence alla protezione degli interessi economici scientifici ed industriali dell'Italia.
- La situazione è in evoluzione sia sotto il profilo delle istituzioni, che delle minacce e delle dinamiche delle imprese.
- Sono cambiate le minacce ed alcune di queste sono già nell'agenda delle imprese.

Lo scenario di fondo 2/3

- C'è un "nuovo corso" dell'intelligence di Stato che viene troppo spesso dato per scontato e che invece merita una riflessione.
- Si rende necessario un investimento comune (istituzioni, imprese ed università) in cultura dell'intelligence e cultura della sicurezza come funzione strategica.

Lo scenario di fondo 3/3

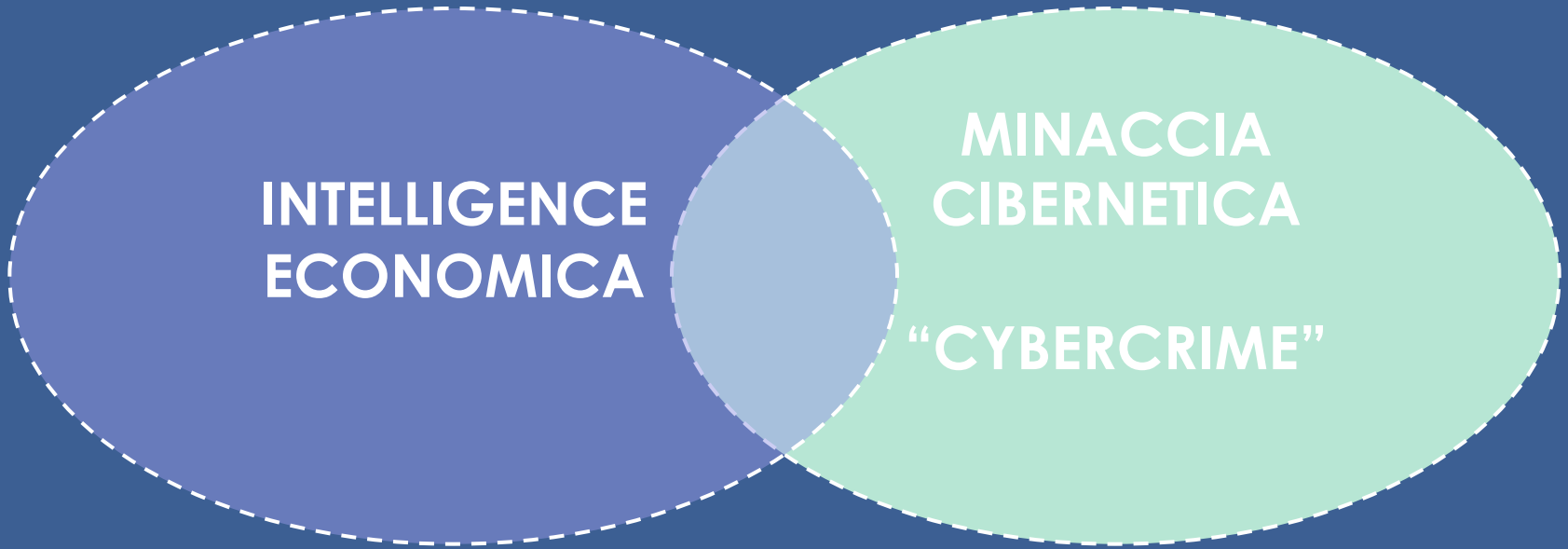
- Esistono dunque le premesse normative affinché il rapporto pubblico-privato possa esprimere tutte le sue potenzialità positive nel campo del sostegno intelligence al sistema Paese.
- Oggi ciò avviene, del resto, in moltissimi Paesi, col risultato che le imprese italiane si trovano spesso a operare all'estero in condizioni di particolare svantaggio nei confronti delle concorrenti straniere.

Le aree di interesse per le imprese che emergono dalla lettura congiunta delle relazioni

- Minacce di impatto anche per le imprese
- Settori merceologici interessati
- Aree geografiche e geopolitica
- Esigenze di coordinamento/collaborazione tra imprese ed istituzioni dedicate e ruolo delle università

Minacce di impatto anche per le imprese

- Due aree emergono con forza e sono due aree strategiche "nuove" per l'intelligence di Stato



Minacce di impatto anche per le imprese: Cybercrime (1/4)

- La minaccia cibernetica per il sistema paese rappresenta al momento la sfida più impegnativa *(si veda DPCM pubblicato il 19/03/13 per la creazione di un sistema nazionale di sicurezza cibernetica)*, che rappresenta un'occasione fondamentale per sviluppare le potenzialità del rapporto tra pubblico e privato in un altro settore cruciale per l'intelligence.

Minacce di impatto anche per le imprese: Cybercrime (2/4)

La minaccia cibernetica per il sistema paese rappresenta al momento la sfida più impegnativa per:

–La natura diffusa e transnazionale.

–Gli effetti potenziali in grado di provocare ricadute peggiori di quelle degli attacchi convenzionali.

–La capacità di incidere sull'esercizio delle libertà essenziali del sistema democratico.

–Il mutare veloce degli attori, dei mezzi, delle tecniche di attacco e dei bersagli.

–Coinvolgere le piattaforme di stati ed imprese, computer e smartphone dei singoli cittadini.

Minacce di impatto anche per le imprese: Cybercrime (3/4)

- Impatta sulla sicurezza di infrastrutture critiche
- Impatta sulle reti di comunicazione
- Impatta sull'utilizzo del web per atti dimostrativi e terrorismo industriale
- Può manifestarsi come possibili attacchi da imprese concorrenti (sottrazione di informazioni/paralisi informatica)
- Utilizzo del web a fini propagandistici (ispirazione qaidista); il web favorisce le possibilità di imitazione e migrazione di attacchi da un settore all'altro (nessuno si può dire al sicuro)

Minacce di impatto anche per le imprese: Cybercrime (4/4)

Considerazioni a margine

- Non tutti gli attacchi vengono denunciati e censiti
- Sugli attacchi esiste una certa riservatezza per evitare di suggerire idee "ai cattivi"
- Difficile trasformare i dati in informazioni e conoscenze in tempi utili per il contrasto

Minacce di impatto anche per le imprese: Intelligence Economica (1/2)

- Competizione internazionale ed acquisizione di patrimonio tecnologico da parte di soggetti esteri soprattutto nelle PMI in settori quali energia rinnovabile, logistica aeroportuale, turismo e immobiliare di lusso (da parte dei paesi del Golfo), agroalimentare e tessile
- Pratiche illegali che minacciano l'erario e le imprese che operano i certi settori esposti a contraffazione

Minacce di impatto anche per le imprese: Intelligence Economica (2/2)

- Sicurezza fisica degli impianti di aziende italiane all'estero
- Investimenti esteri in Italia: ruolo dei fondi sovrani
- Infiltrazioni della criminalità organizzata nell'attività produttiva e nel settore
- Apertura di banche asiatiche come avamposto delle imprese

Minacce di impatto anche per le imprese: dalla combinazione tra intelligence economica e cybercrime

- Spionaggio informatico industriale ed economico utilizzando il cyberspazio:
  - Entità statali ed imprese acquisiscono in modo illecito informazioni e knowhow in settori strategici provocando danni enormi
  - Nuove tecniche di hacking
  - Impossibilità di risalire alla provenienza delle azioni ostili

Settori merceologici (in parte già citati)

- Settore industriale dell'alta tecnologia
- Settore finanziario
- Informatica e telecomunicazioni
- Settore energetico (focus)

Settori merceologici (focus energetico) 1/2

- Esistono fattori di vulnerabilità legate al fatto che nel medio termine l'asse portante degli approvvigionamenti energetici sarà ancora legato agli idrocarburi:
  - ½ del traffico di greggio del Golfo Persico passa dallo stretto di Hormuz
  - ½ delle riserve naturali di gas sono in Russia, Iran, Qatar
  - Le imprese che operano nel settore dell'energia (paesi del nord africa: 50% del gas da Libia ed Algeria)

Settori merceologici (focus energetico) 2/2

- Negli stati dell'Africa le risorse energetiche sono "beni sovrani" e quindi gestiti direttamente dai governi: da qui l'esigenza della geopolitica e l'interazione con i servizi di altri paesi
- Approvvigionamento energetico (paesi di produzione, trasferimenti materie, stabilità dei sistemi economici e difesa delle infrastrutture critiche)

Aree geografiche prese in considerazione dai rapporti

- Nelle relazioni un'analisi attenta di geopolitica:
  - Nord Africa
  - Corno d'Africa
  - Somalia
  - Medio oriente
  - Penisola araba
  - Balcani
  - Asia
  - America meridionale
  - Aree di conflitto

I rapporti tra intelligence istituzionale ed imprese (1/3)

- Non ci sono mai stati muri, ma neanche ponti strutturati
- Esistono rapporti consolidati spesso personali tra intelligence e grandi aziende ma vanno strutturati meglio
- L'articolo 13 della legge n. 124/2007, secondo cui gli Organismi possono corrispondere con i soggetti che erogano servizi di pubblica utilità e chiedere la loro collaborazione stipulando apposite convenzioni, a giudizio del Comitato non è sufficiente ad affrontare in modo compiuto le questioni sul tappeto

I rapporti tra intelligence istituzionale ed imprese (2/3)

- Il dialogo tra il Sistema di informazione per la sicurezza della Repubblica e il mondo della sicurezza aziendale deve essere costante, anche in una logica di partecipazione e divisione dei compiti per gli obiettivi comuni o in funzione sussidiaria per talune finalità specifiche
- E' necessario realizzare un circuito stabile di condivisione delle informazioni e dei dati in possesso delle agenzie e delle imprese

I rapporti tra intelligence istituzionale ed imprese (3/3)

- Esempi stranieri non mancano:
  - UK: il *Centre for the protection of national infrastructure* (CPNI) che svolge un significativo ruolo a favore degli operatori economi britannici;
  - USA: l'*Overseas security advisory council* (OSAC), che si configura come un network composto di soggetti pubblici e privati che operano nei diversi paesi, in grado di realizzare un quadro informativo efficace a disposizione degli stessi soggetti.

L'intelligence al supporto delle imprese (1/2)

- Nuovi settori e nuovi paesi: è indispensabile il supporto delle istituzioni; supporto da codificare e coinvolgimento da attivare in maniera istituzionale
- L'intelligence a supporto della sicurezza aziendale (infrastrutture critiche/cybercrime etc)
- La globalizzazione ha fatto insorgere nuovi rischi per le aziende con relativo incremento dei compiti/costi della security interna, divenuta fondamentale per la competitività e la protezione del patrimonio tecnologico

L'intelligence al supporto delle imprese (2/2)

- L'Italia ha sempre difeso i suoi "campioni" all'interno del territorio nazionale, ora si tratta di supportarli anche all'estero come fanno altri paesi
- Nasce l'esigenza di contrastare la criminalità organizzata, e le manovre di aziende concorrenti che si muovono in maniera illecita nel comparto economico e scientifico con particolare riferimento alla innovazione industriale, ai dati finanziari e commerciali oggetto di attenzione da parte di circuiti illegali
- Si sono verificate frequenti minacce al corretto funzionamento del circuito economico da parte di organizzazioni criminali

Le imprese a supporto dell'intelligence di Stato

- Le imprese nella loro operatività vengono in contatto con una serie di informazioni utili all'intelligence di Stato
- Da declinare bene i canali, le modalità e le aree in maniera istituzionale
- Focus su golden share senza piano industriale che definisce ciò che è strategico da ciò che non lo è per il paese: questo è un settore che richiede grande collaborazione tra istituzioni ed imprese

Le aree oggetto di collaborazione ed il potenziale ruolo dell'Università (1/3)

- Nelle istituzioni stanno cambiando i criteri di selezione e quindi la gestione delle risorse umane dedicate all'intelligence; può esse un terreno di collaborazione (formazione, recruitment, percorsi formativi, tesi finalizzate, stage etc)
- Cybercrime: dal prossimo anno grazie alla collaborazione di alcune aziende avanzate nel settore informatico l'Università metterà a disposizione borse di studio per ingegneri informatici per frequentare il master in modo da diventare vivaio per recruitment delle imprese e delle istituzioni

Le aree oggetto di collaborazione ed il potenziale ruolo dell'Università (2/3)

- L'università potrebbe studiare il modello inglese e quello americano citati nei rapporti e fare un approfondimento tecnico ed operativo, come ha già fatto su altri temi (corruzione, performance audit per altre agenzie pubbliche)
- L'università potrebbe fornire assistenza nel gestire tavoli e focus group in maniera asettica mettendo a disposizione metodologie di analisi e studio, supporto scientifico multidisciplinare

Le aree oggetto di collaborazione ed il potenziale ruolo dell'Università (3/3)

- Ovviamente si continua nella formazione specialistica su intelligence economica cooperando con imprese ed istituzioni

Per qualsiasi ulteriore informazione

- Luciano Hinna
- luhinna@tin.it
- hinna@juris.uniroma2.it
- 06 72592211
- 335 8183344