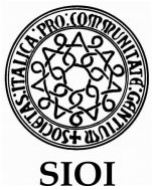
Società Italiana per l'Organizzazione Internazionale



MASTER IN SICUREZZA ECONOMICA, GEOPOLITICA E INTELLIGENCE

20 GENNAIO - 6 LUGLIO 2012

Il Controspionaggio Economico in Italia

Domenico Vecchiarino

PAPER GIUGNO 2012

“There are friendly nations, but no friendly intelligence services”

“L’intelligence economica si prefigge di sviluppare le tecniche di raccolta e di analisi dei dati, di decisione operativa e di verifica dei risultati, configurandosi come materia di comune interesse per le imprese e gli Stati . A causa della competizione globale, gli Stati hanno accentuato il loro impegno a difesa delle imprese del loro Paese, incorporando la tutela degli interessi nazionali tra gli obiettivi dei Servizi di sicurezza pubblici”

(Fondazione ICSA, Intelligence Culture and Strategic Analysis)

“the espionage is not game for archbishops “

Allen Dulles

“Dare l’informazione giusta alla persona giusta, nel momento giusto per prendere la giusta decisone”

Michael E. Porter

INDICE

PREMESSA

Dopo il crollo del muro di Berlino e la conseguente fine della Guerra Fredda in tutti i paesi economicamente avanzati è aumentata l'interdipendenza tra economia e sicurezza. Ciò è derivato da una crescita esponenziale del commercio internazionale che spinge aziende e Stati a una sempre più maggiore conquista di quote di mercati e settori economici strategici a scapito di altri Stati. Per questo motivo l'intelligence economica ha assunto un ruolo fondamentale nello scenario attuale. Cresciuta insieme alla globalizzazione dei mercati ed alla necessità di adottare un processo di anticipazione dei cambiamenti dei mercati e dell'ambiente economico, l'intelligence economica sta diventando un sostegno indispensabile al processo decisionale e strategico, usando l'informazione, in tempo reale (just in time), come strumento per migliorare le performance economica e/o tecnologica. Dovendo trattare soprattutto incertezze, la sua missione è "sapere per anticipare". Una buona intelligence economica è il risultato di una perfetta sinergia tra i vari attori che concorrono allo sviluppo del benessere economico nazionale. Se da una parte è necessario l'intervento del Governo, dall'altra è fondamentale che anche gli enti privati, le imprese, le associazioni di professionisti e di singoli, si impegnino, secondo le loro possibilità, per contribuire ad una maggiore efficienza del sistema. Inoltre, l'autorità statale non può limitarsi all'uso dell'intelligence economica per supportare il sistema produttivo della Nazione, ma deve anche adottare una strategia commerciale in grado di sostenere le produzioni intere all'estero.[1] Di conseguenza, i buoni risultati dell'intelligence economica sono inevitabilmente il frutto di un sapiente uso combinato di informazioni provenienti dai servizi informativi e dalla politica governativa a supporto delle esportazioni e della conquista dei settori strategici. Ovviamente trattandosi una materia come questa, non possiamo non parlare dello spionaggio economico, considerando che questo non è importante solo perché utilizzato come sistema per raccogliere informazioni, ma perché è una branca dell'intelligence che è cresciuta fortemente dopo il crollo del Muro di Berlino. Infatti si è passati da uno spionaggio molto più indirizzato verso il settore militare a uno spionaggio odierno caratterizzato da una durissima competizione economica tra diversi attori che si contendono quote sempre più grandi di mercato, dove l'attività di spionaggio spazia dall'acquisizione di tecnologie all'avanguardia alla scoperta della fallback position, passando per il controllo di settori strategici

[1] Mauro Morbidelli, *Intelligence Economica e Competitività Nazionale*, pag 28

delle economie di altri paesi. Secondo un articolo della BBC News [2], lo spionaggio economico vale un business di 200 miliardi di dollari annui, considerata questa cifra, si può capire facilmente la portata del fenomeno e si può capire anche come il DGSE, il servizio informativo francese, ha ammesso di utilizzare lo spionaggio per venire a conoscenza di tecnologie di Paesi all'avanguardia, soprattutto negli Stati Uniti. Ad esempio, Pierre Marion, ex direttore della DGSE, ha affermato " L'attività di spionaggio è un modo essenziale per la Francia, attraverso la quale essa si mantiene al passo nella competizione internazionale e nel commercio. Ovviamente è diretto conto gli Stati Unti come verso altri Paesi. Si deve ricordare che, mentre siamo alleati per quanto riguarda la difesa, siamo anche competitori economici nel mondo". [3] Di più, con lo sviluppo delle nuove tecnologie legate all'informatica e ad internet è divenuto molto più semplice il furto dei segreti. Basti pensare agli hackers che penetrano nella rete informatica di un'azienda senza lasciare traccia e di fatto diviene impossibile perseguire gli autori dell'intrusione. E allora, per prevenire atti di spionaggio, per difende uno stato, un segreto industriale, una nuova tecnologia, insomma per creare una vera e propria sicurezza economica, cosa diviene fondamentale? Il controspionaggio. Quest'ultimo però non deve lavorare solo in funzione passiva o difensiva, volto cioè a contrastare, individuare e neutralizzare le spie avversarie, ma deve essere soprattutto attivo o offensivo, volto cioè all'attività di ricerca e raccolta , e alla costruzione di una serie di misure e piani difensivi volti alla messa in sicurezza di tutte quelle informazioni, tecnologie e infrastrutture vitali per la sicurezza economica del nostro Paese. [4]

[2] http://news.bbc.co.uk/2/hi/technology/5313772.stm
[3] Carr Chiris, Morton Jack, Furniss Jerry, *The Economic Espionage Act: Bear Trap or Mousetrap?*, Texas Intellectual Proprety Law Journal, pag 166
[4] Carlo Mosca, *I servizi di informazione e il Segreto di Stato*, pag 206

1.1 L'INTELLIGENCE ECONOMICA IN ITALIA

Grazie al lavoro di due Commissioni guidate dall' Ambasciatore Egidio Ortona (1992) e dal Generale Jucci (1998), l'intelligence economica è divenuta materia di attenzione nazionale. Queste due commissioni sono nate con l'intento di riformare i servizi di sicurezza del nostro paese e si sono trovate a gettare le basi per la nascita dell'intelligence economica in Italia, data la rilevanza che quest'ultima stava iniziando ad avere nel mondo post Guerra Fredda.

Dall'analisi delle Relazioni dei Servizi di Sicurezza e Informazione del nostro Paese, che sono le principali fonti per analizzare l'effettivo stato e l'evoluzione dell'intelligence economica in Italia, appare evidente che l'intelligence economica nel nostro paese e basata su aspetti difensivi ed è riferita a due aree:

- Quella della protezione della base tecnologica, scientifica e industriale, con particolare riguardo alle tecnologie strategiche o critiche per la sicurezza nazionale ed alleato. Tale azione è estesa anche alla salvaguardia del patrimonio tecnologico e industriale nazionale dall'acquisizione da parte di soggetti caratterizzati da una certa opacità, come attori societari aventi sede in paesi off-shore.

- Quella dell'interesse dei Servizi per il contrasto degli aspetti economico finanziari della criminalità organizzata nazionale, internazionale e al finanziamento del terrorismo. Di particolare rilevanza è attribuita al *money laundering* e alle attività dell'imprenditoria mafiosa, nonché ai sempre maggiori trasferimenti di denaro, effettuati al d fuori del sistema bancario, derivanti dal crescente numero d'immigrati in Italia che usano sistemi come il *money transfert* e *l'hawala banking*. [5]

Ad onor del vero c'è una terza aree di interesse dei nostri servizi di informazione e sicurezza, ovvero l'intelligence economica offensiva, cioè quella destinata ad accrescere la competitività economica nazionale e delle nostre imprese, a favorirne la penetrazione sui mercati esteri, a proteggerle da pratiche sleali (corruzione, contraffazione, pressioni politiche di altri paesi a favore delle loro aziende nazionali, ecc) nonché allo spionaggio e controspionaggio industriale. Data la riservatezza della materia, si può ben facilmente comprendere che dati certi e informazioni concrete sono difficilmente reperibili. Un dato però è riscontrabile dall'analisi delle Relazioni dei servizi,

[5] Carlo Jean e Paolo Savona, *Intelligence Economica*, pag 102-104

ovvero che la nostra intelligence dedica al settore economico lo stesso livello d'impegno riservato all'antiterrorismo e al contrasto delle attività criminali. [6]

Molto importate ai fini informativi è la campagna promossa negli ultimi anni da parte dei servizi di informazione e sicurezza con la diffusione della cultura della sicurezza, grazie al quale le attività di intelligence vengano meglio conosciute, nei loro lineamenti istituzionali, dall'opinione pubblica come dalle classi dirigenti, dal mondo accademico come da quello dei mezzi d'informazione.[7] Questa diffusione serve a rendere il lavoro dei servizi il più trasparente possibile in modo da aumentare l'indispensabile collaborazione fra pubblico e privato, fra i servizi e le imprese, l'Università e anche le agenzie o le associazioni private di intelligence, in modo sinergico al fine di rendere il mondo economico produttivo nazionale il più coeso possibile.

A questo proposito è necessario sottolineare l'importanza del contributo che il sistema delle aziende nazionali può fornire, tanto alla definizione degli obiettivi di ricerca riguardanti le informazioni da acquisire per garantire alle aziende sicurezza e competitività, quanto all'incremento del patrimonio informativo a disposizione del Governo, tenuto conto delle conoscenze che le aziende stesse acquisiscono grazie alla loro presenza all'estero.

Si tratta, come è facile capire, di una tematica assai delicata, perché non è affatto semplice individuare il confine oltre il quale non ci si muove più a tutela della sicurezza nazionale, ma si incide sul mercato, alterandone i meccanismi fino a creare, in qualche caso, serie difficoltà ad altre imprese o Stati. E, certamente, non si tratta di rincorrere qualunque forma di interesse economico proiettato verso l'estero o di tutelare l'incolumità di qualunque imprenditore che operi al di fuori dei confini nazionali. La tutela del sistema economico e industriale è sicuramente uno dei campi più delicati dal punto di vista della legittimità delle attività che i servizi di informazione per la sicurezza possono essere chiamati a svolgere, tanto in chiave "difensiva", nei confronti di aggressioni o intrusioni di varia natura a danno delle imprese, quanto in chiave "offensiva", in termini di informazione preventiva a sostegno della competitività delle imprese stesse sui vari scenari internazionali. Ma non vi possono essere dubbi di sorta sull'importanza strategica di immettere i dati e le informazioni raccolti dagli apparati della sicurezza nazionale in una "rete" che faccia gioco rispetto al sistema-Paese.

Interpretare la nozione di sicurezza nazionale in senso evolutivo e ricomprendervi la tutela degli interessi nazionali comporta, ad esempio, che i servizi di informazione e sicurezza possono essere

[6] Carlo Jean e Paolo Savona, *Intelligence Economica*, pag 102-104
[7] Art 4 comma 3 lett m legge n.124/2007

chiamati a operare per proteggere le grandi imprese o comunque le imprese di rilevanza strategica, quelle che i francesi chiamano imprese di rilevanza nazionale e vengono talvolta ricordate come "campioni nazionali". Si tratta di imprese che – giova ricordarlo – spesso ma non sempre si dotano di proprie organizzazioni informative e di sicurezza per sopravvivere in un mondo sempre più impegnativo sul piano della competizione [8]

2.1 IL RUOLO DEI SERVIZI DI INFORMAZIONE E SICUREZZA NELL'AMBITO ECONOMICO

Con la caduta del Muro di Berlino e la fine della Guerra Fredda il ruolo dei servizi di informazione e sicurezza è cambiato. Se dapprima il loro ruolo era legato alla minaccia sovietica e a tutto ciò che era legato a quest'ultima, ora le minacce sono più diffuse e imprevedibili. Nel caos geopolitico che è sopraggiunto dopo la caduta dell'URSS, uno dei settori nel quale possiamo riscontrare una forte competizione tra Stati è il settore geoeconomico, indi per cui, il ruolo dei servizi di informazione è naturalmente votato al contrasto di attività che possono metter in pericolo la sicurezza economica di un Paese. Circoscrivendo l'analisi al solo terreno geoeconomico, si può sottolineare da subito come le minacce alla sicurezza economica di un Paese provengano da una molteplicità di direzioni. In questo settore non esistono più alleati e i pericoli possono provenire dagli Stati con i quali non si hanno rapporti ostili, come da quelli amici, anzi soprattutto da questi. [9] Fondamentale è poi capire come i servizi di informazione si sono trovati, in parte, spiazzati da questa situazione, fino agli anni 90, data la specificità della minaccia sovietica, la maggior parte dei servizi non aveva minimamente preso in considerazione queste attività, considerando che ora le agenzie di intelligence si trovano di fronte ad una moltiplicazione degli attori, che non sono più esclusivamente gli Stati, ma anche imprese, società finanziarie e singoli attori dalle diverse caratteristiche e dimensioni. Per quanto riguarda la competizione geoeconomica, i Governi hanno riqualificato parte del lavoro delle agenzie di intelligence, adeguandolo al nuovo contesto. Inoltre, spinti dalla necessità di trarre nuova giustificazione alla loro esigenza e dall'esigenza di economizzare la loro attività, questi servizi hanno cominciato a diventare dei protagonisti sempre più importanti nella sfida economica internazionale.[10] Pare opportuno rilevare come il nuovo ruolo dei servizi d'informazione in campo

[8] *Quaderni di Intelligence*, n. 1 Anno 2012 , pag 13-14
[9] Mauro Morbidelli, *Intelligence Economica e Competitività Nazionale*, pag 37
[10] Germano Dottori, *Un'Intelligence per il XXI secolo*, pag 92-93

economico non si stia imponendo solo nei Paesi occidentali o comunque industrializzati. Anzi è importante sottolineare come per molte Nazioni in via di sviluppo l'intelligence economica rappresenti un metodo per saltare le tappe dell'evoluzione, al fine di poter accedere a mercati che altrimenti sarebbero loro preclusi. Non si può, per esempio, non valutare il ruolo svolto dall'intelligence economica nello sviluppo nei settori ad alta tecnologia dei Paesi asiatici, ed in particolare del Giappone. L'uso dei servizi informativi finalizzato allo sviluppo e al sostegno economico è sicuramente uno strumento di fondamentale importanza per questi Stati. Tuttavia, anche i soggetti all'avanguardia in termini scientifici, tecnologici ed industriali potrebbero progressivamente cedere alla tentazione (alcuni lo hanno già fatto) di cercare di rubare segreti ai Paesi del loro stesso livello. Ad ogni modo, tenuto conto di questi sviluppi, la funzione di controspionaggio economico dovrà essere progressivamente potenziata al fine di prevenire questo tipo di minacce. [11]

3.1 COS'E' IL CONTROSPIONAGGIO ECONOMICO

La finalità del controspionaggio economico è quella di individuare le minacce al sistema economico nazionale e d'impedire l'acquisizione da parte di agenti stranieri di informazioni che potrebbero mettere in pericolo l'apparato produttivo del Paese, o più semplicemente, che potrebbero minare la presenza di una o più imprese nazionali sul mercato. [12]Il controspionaggio però non deve lavorare solo in funzione passiva o difensiva, volto cioè a contrastare, individuare e neutralizzare le spie avversarie, ma deve essere soprattutto attivo o offensivo, atto cioè all'attività di ricerca e raccolta , e alla costruzione di una serie di misure e piani difensivi volti alla messa in sicurezza di tutte quelle informazioni, tecnologie e infrastrutture vitali per la sicurezza economica del nostro Paese. [13] Ovviamente una condizione preliminare a questa funzione è quella di definire in anticipo quali siano i settori da definirsi strategici e quindi da tutelare maggiormente. Si possono pertanto delineare alcuni ambiti operativi dei servizi di informazione e sicurezza nell'ambito delle misure da adottare nel controspionaggio economico:

- *Tutela della competitività delle imprese*: sia sotto il profilo tecnologico che sotto il profilo commerciale. La protezione dei segreti industriali o dei prototipi viene attuata secondo le

[11] Mauro Morbidelli, *Intelligence Economica e Competitività Nazionale*, pag 52
[12] Mauro Morbidelli, *Intelligence Economica e Competitività Nazionale*, pag 39
[13] Carlo Mosca, *I servizi di informazione e il Segreto di Stato*, pag 206

linee guida della “proprietà intellettuale”, con la quale la disciplina giuridica tutela i frutti dell’inventiva e dell’ingegno.

- *Protezione della competitività commerciale delle aziende del paese*: in termini di tutela dell’immagine della protezione nazionale in generale, attraverso il sostegno ai settori a forte innovazione industriale, con la definizione di nuove politiche per le PMI, con il sostegno alla cooperazione e con il potenziamento della rete estera di supporto alle imprese.

- *Monitoraggio sugli assetti concorrenziali di settore dal lato dell’offerta e conseguente tutela della domanda di mercato*: a garanzia del mantenimento di normali livelli qualitativi e quantitativi di concorrenza, mediante il controllo sull’evoluzione di stati di concentrazione e accordi, iperconcorrenza o abuso di posizione dominante settoriale .
- *Contrasto, individuazione e neutralizzazione di spie e reti spionistiche*: siano esse al soldo di governi o multinazionali e aziende, ove individuate, devono essere neutralizzate e, nel caso vi fossero i presupposti, “doppiate”

- *Operazioni di deception*: ovvero operazioni che tendono a ingannare l’analisi che l’avversario conduce sulla situazione politica economica sociale ecc, tanto da fargli comporre un quadro che lo porterà a prendere decisioni che avvantaggino gli interessi propri e non quelli avversari.

- *Penetrazione sia umana che tecnica in una intelligence economica avversaria*: al fine di conoscere in anticipo e in dettaglio i piani; inoltre un infiltrato ben piazzato sarà in grado di segnalare se la propria intelligence economica è stata a sua volta penetrata.

- *Controllo sulla penetrazione d’interessi stranieri in settori vitali o strategici*: con particolare attenzione ai fenomeni di acquisizione massiccia di partecipazioni azionarie da parte di soggetti non meglio identificati e d’ingresso diretto sui mercati nazionali del credito e della distribuzione commerciale.

- *Previsioni di scenari geoeconomici critici*: con particolare riferimento alla criminalità economica ed ai mercati finanziari.

- *Sviluppo di programmi e sistemi per salvaguardare le informazioni sensibili:* attraverso l'uso di NOS, casseforti, rendicontazione dei documenti, codici e coperture, badges di accesso, perimetri di sorveglianza, educazione alla sicurezza.

- *Analisi delle principali minacce e soggetti vulnerabili*: al fine di individuare i rischi che tutti i soggetti posso trovare in tutte le circostanze in modo da prevenire tutte le possibili situazioni e circostanze critiche.

- *Operazioni di controinformazione*: queste posso essere utili sia per far circolare false informazioni, al fine di confondere le acque per il nemico, e sono utili anche per tendere trappole e smascherare le reti spionistiche avversarie.

- *Selezione del personale* : con particolare attenzione a reclutare e scegliere persone che non siano ricattabili in nessuna circostanza.

- *Protezione delle infrastrutture critiche*: per ragioni di natura economica, sociale, politica e tecnologica queste infrastrutture sono diventate sempre più complesse e interdipendenti, a causa di ciò necessitano di misure precauzionali e piani di sicurezza per ridurre il rischio che queste posso venire a mancare o a causa di una fenomeno naturale o a causa di un atto deliberato .

- *Esodo degli scienziati*: sono migliaia i giovani italiani che si trovano all'estero che ricoprono ruoli di responsabilità in organizzazioni importanti e nei più svariati settori. Si tratta di una risorsa particolarmente qualificata che non trova spazi nel nostro paese e che di conseguenza impoverisce la ricerca e lo sviluppo della nazione. Ma c'è un altro aspetto che può essere preso in considerazione, ovvero data la particolare presenza dei nostri giovani talenti in settori chiave di aziende e istituzioni straniere, alcuni di questi possono essere reclutati dai nostri servizi di informazione e sicurezza per costituire delle reti informative qualificate, a facilmente acquisibile e basso costo. [14]

[14] Mauro Morbidelli, *Intelligence Economica e Competitività Nazionale*

CHI FA IL CONTROSPIONAGGIO ECONOMICO

Per quanto riguarda il controspionaggio economico operato dai servizi di sicurezza e informazione del nostro paese i dati reperibili sono pochissimi, questo ovviamente è facilmente comprensibile data la riservatezza della materia. Dalle notizie che circolano in rete, però, risulta che nell´ambito dell´Aisi opera un Reparto economia e finanza che si occupa specificamente di monitorare flussi di denaro e speculazioni finanziarie potenzialmente destabilizzanti sul piano macroeconomico. Sempre nell´Aisi vi è un Reparto controspionaggio e controingerenza, che, insieme ad altre funzioni, ha il compito di proteggere le informazioni strategiche di carattere economico, finanziario, industriale e scientifico del sistema-Paese nei confronti di attività di spionaggio condotte da servizi d´intelligence esteri, effettuate anche con strumenti cibernetici, nonché di contrastare operazioni di ingerenza economica promosse da potenze straniere. Sempre nell'Aisi vi è un Reparto intelligence economico-finanziario, preposto al contrasto di minacce alla sicurezza economica e alla stabilità finanziaria provenienti dall´estero. Esso è suddiviso in una Divisione operazioni e in un Ufficio analisi. Le attività di Aisi e Aise in questo campo sono coordinate in maniera sempre più stringente dal Dis [15]. Con un'analisi delle fonti aperte è riscontrabile che sono state messe sotto osservazione 100 piccole e medie imprese, pubbliche e private, considerate le punte di diamante nei mercati ai quali fanno riferimento, aziende che per innovazione, ricerca, talento e originalità dei prodotti realizzati, sono le più riconosciute e apprezzate anche all'estero. Un elenco stilato dall'Aisi con la collaborazione di Confindustria e sotto l'osservazione della Presidenza del Consiglio dei ministri. In concreto, tale programma fortemente sostenuto dal capo dell'Intelligence interna, Giorgio Piccirillo, consiste in un sistema di controspionaggio economico che nei prossimi tre anni dovrebbe portare ad una mappatura completa di dove si colloca il know-how italiano di maggior valore da mettere sotto tutela. Information and Communication Technology, ricerca e produzione aerospaziale, meccanica di precisione, biomedica e nano-tecnologie i settori sotto osservazione. Le aziende avrebbero inoltre ricevuto un recapito telefonico diretto con i servizi segreti per porre rapidamente il problema se dovessero verificarsi anomalie. [16]

Solitamente il controspionaggio dovrebbe essere una peculiarità dei servizi d'informazione e sicurezza istituzionali, ma da anni ormai grandi aziende e multinazionali italiane ed estere hanno

[15] www.oipamagazine.ue, 23-07.2010
[16] www.formiche.net , 1-06.2011

creato delle strutture di intelligence vere e proprie. Queste strutture operano come apparati di informazione e sicurezza a protezione ovviamente dell'azienda per la quale operano, e sono formate per la maggior parte da ex membri dei servizi di intelligence. I compiti di queste strutture, che spesso prendono il nome di "security aziendale" sono svariati, ad esempio: la protezione del know how tecnologico e del segreto industriale, la protezione dei dati e delle informazioni sensibili dai crimini informatici, il monitoraggio degli assetti concorrenziali e del mercato, la protezione dei vertici aziendali, la preparazione di piani di emergenza ed evacuazione del personale per le sede nei paesi a rischio, e infine, l'attività che più ci riguarda da vicino, ovvero il contrasto alle attività spionistiche che mettono a rischio l'azienda.

Ma non solo. Il controspionaggio economico è anche un business, se proviamo a digitare la parola chiave "controspionaggio economico" su un motore di ricerca troveremo oltre trentottomila risultati. Tra tutti i link possiamo facilmente notare come siano nate tantissime agenzie di investigazione che offrono i loro "servizi" a tutti coloro che ne hanno bisogno. In Italia uno dei primi pionieri in questo settore è stato il famigerato Tony Ponzi, ma oggigiorno se ne posso contare a migliaia. Ovviamente vi sono anche "multinazionali" enormi come la Kroll, che a differenza di queste agenzie, sono dei veri e propri servizi di intelligence, con oltre quattromila dipendenti e sedi in venti sei paesi, che vedono i loro servizi anche a governi. Giusto per fare un esempio, la Kroll è stata incaricata di recuperare il tesoro di Saddam Hussain ed ha fornito assistenza al governo degli Stati Uniti in teatri come l'Iraq e l'Afghanistan. [17]

5.1CONTROSPIONAGGIO ECONOMICO E MINACCIA CIBERNETICA

L'Attenzione per la sicurezza cibernetica è andata aumentando negli ultimi anni sempre di più. Questo è dovuto al fatto che sono aumentati a dismisura gli attacchi ad aziende private, a organismi istituzionali e, anche se in casi rari e molto complessi, alle strutture preposte alla difesa nazionale. Per tal motivo il budget globale per la sicurezza del web ha raggiunto la cifra di 60 miliardi di dollari, prevedendone un incremento del 10% per i prossimi tre - cinque anni. Solo in Italia, ad esempio, si è passati dalle poco più delle 7600 intrusioni sul sistema web delle imprese nel 2009. A circa 14.000 registrate nei primi mesi del 2011, con un danno accertato di 200 milioni di euro

[17] Corriere della Sera, pag 8 , 7 giugno 2007

destinato a salire, secondo le stime di agenzie preposte alla sicurezza informatica, a 450 – 600 milioni di euro nel 2013. [18]

La maggior parte delle azioni di crackeraggio sono quelle che agiscono soprattutto con l'invio di e-mail, considerate i principali mezzi di attacchi informatici, con sistemi di *spearphishing*, che concretizzano quella molteplicità di illeciti che caratterizzano il *cyber crime* dai più comuni furti d'identità, truffe tramite *l'internet banking* e altre operazioni di frodo *cyber ransom*. Sono comunque intromissioni e manomissioni di basso livello tecnologico, che nonostante riguardano il settore economico, si distinguono da quelle a maggior impatto operativo come le DDoS, il cui obiettivo è la violazione delle proprietà intellettuale (IP), con più ragguardevoli propositi illeciti, che si configurano come spionaggio industriale vero e proprio.

Quando invece, con l'irruzione criminale sulla rete si arriva a violare l'IP di un'azienda e si tenta quindi di impossessarsi di informazioni personali, ma soprattutto di brevetti, studi e ricerche, oppure viola piani di gestione aziendale o direttamente tutto il hnow how aziendale, l'azione assume il carattere di spionaggio industriale vero e proprio. Si tratta quindi di una vera e propria guerra economica che fra diverse entità che mirano all'indebolimento del potenziale strategico avversario.

Facendo uso della terminologia militare, come strumenti esclusivi dei *target attacks* si parla di *advanced persistent theats*, ATP, intese a minacciare o addirittura ad aggredire entità economiche precise. Mentre gli attacchi indiscriminati tramite *spearphishing* ed e-mail, anche se più malevoli, sono diminuiti dell'80%, quelli *targeted*. Ed in particolare le ATP, per lo più miranti all'attività economica, commerciale e finanziaria delle aziende, nello stesso periodo, sono triplicati. Le ATP, infatti, si differenziano dai tradizionali attacchi di massa perché sono progettate appositamente per colpire obiettivi precisi e sono dotate di strumenti appropriati per azioni pianificate, anche se non fulminee ma lente, in grado di condurre, per lo più, spionaggio industriale. [19]Con il passare del tempo poi, le tecniche di infiltrazione nelle reti delle aziende si sono perfezionate e raffinate, al punto che è sempre più difficile scoprire da dove provengono gli attacchi e qual è il materiale che viene trafugato. Di più, un altro aspetto va preso in considerazione, la minaccia ATP, non è roba da ragazzini hakers, nel senso che quando avviene un'intrusione con questa modalità di attacco, i "pirati" sanno benissimo dove, e soprattutto cosa colpire, ovvero quale informazione sottrarre, indi per cui, è chiaro come il sole che si tratta di entità ben più importanti. Pertanto diventa fondamentale proteggere le aziende non solo dallo spionaggio industriale ma anche dal rischio di

[18] Shai Blitzblau, Cyber-Espionage Threts and Impacts on Italian Economy and Businesses, relazione presentata alla 2° International Warfare Conference.
[19] *La comunità internazionale*, trimestrale della Società Italiana per l'Organizzazione Internazionale, Vol LXVII 1 2012

sabotaggio, quando la violazione viene perpetrata da elementi come gruppi terroristici e malavita organizzata.

Molte multinazionali sono state le ultime vittime eccellenti di tutta una serie di intrusioni e di *malware* altamente nocivi e invasivi, il cui obiettivo è per lo più quello di ottenere l'accesso all'IP dell'industria colpita, con una chiara predilezione per i settori della difesa, chimica ed energia, ossia quelli più costosi in termini di ricerca e di produzione, ma altresì più strategici per l'economia e la politica mondiale.

Alcune volte, l'intrusione assume il carattere di un attacco offensivo sferrato ad un'entità statale e che vede contrapposti, abitualmente, da un lato, gli Stati Uniti e suoi alleati e, dall'altro lato, la Cina e la Russia. In questo caso però, si alza il livello dello scontro e degli obiettivi che si vogliono colpire e si riduce l'ambito di azione ai settori strategici per eccellenza di una nazione, ovvero alle infrastrutture critiche. Ciò rientra nella categoria dei *targeted attacks*, ossia alle azioni malevoli come l'affare Stuxnet e Flame, e qui ci troviamo di fronte alla vera e pura guerra cibernetica. Così si passa dal *cyber crime* più generico e tipico dell'ambiente civile, al *cyber warfare*, proprio e tipico delle strutture militare che comprende al suo interno, la minaccia *cyber war* e quella di *cyber terrorism*; la prima caratterizza lo scontro fra entità statuali, la seconda, invece, definisce azioni proprie di organismi o gruppi con fini eversivi o rivoluzionari, entrambe però, sempre nello spazio cibernetico e con i suoi strumenti specifici, o *cyber weapons*. [20]

La crescita vertiginosa dei crimini informatici e delle violazioni a siti istituzionali e a quelli delle imprese, e relativo spionaggio industriale ad essi collegato (34% delle azioni malevoli sul web), è dovuta, infatti, a diversi fattori, primo fra tutti l'aumento esponenziale della diffusione di laptop, smartphone e tablet. Se a questi congegni così diffusi si sommano i vantaggi del cloud computing nello stoccaggio di dati, è comprensibile la facilità con cui si può agire con malware per "intossicare" un sistema per accedere e carpirne informazioni, dalle più generiche e personali a quelle strategiche di industrie e aziende. Non è una caso infatti, che nell'ultimo anno vi siano stati così numerosi incontri e dibattiti proprio sulla cyber security: mai prima d'ore vi era stata una così stretta sinergie tra il mondo privato e quello istituzionale per affrontare rischi e minacce del cyberspazio. Il motivo è semplice: in internet si colloca tutto il know how e quelle attività che fanno di una nazione un sistema-Paese, ancora più prezioso in un momento di crisi economica globale come quello attuale. Si tratta di un'insieme di informazioni su progetti, brevetti, piani strategici e quant'altro messo in rete che, anche se garantita da muri digitali di protezione è, a quanto sembra,

[20] *La comunità internazionale*, trimestrale della Società Italiana per l'Organizzazione Internazionale, Vol LXVII 1 2012

ancora troppo vulnerabile. Per cui, l'esposizione di questo sapere impone, per il carattere proprio dello spazio cibernetico in cui è ospitato, una sua condivisione globale, che però deve essere controllata e salvaguardata da possibili attacchi perché a rischio vi sono i fondamenti economici, finanziari e industriali che definiscono i trend di sviluppo di una nazione e lo fanno emergere da quell'amalgama generalizzata che è la globalizzazione.

Proprio per l'importanza del know how a disposizione e per i rischi a cui è esposto, non è permesso sottovalutare i soggetti e gli ambiti della minaccia cibernetica, considerandoli solo come un'abile operazione di marketing delle aziende di sicurezza informatica. Anche perché, il danno non è esclusivamente tecnico o finanziario immediato (truffa o furto): il più delle volte si tratta, infatti, anche di "reputazione negativa" che è costretta a subire la vittima (impresa, nazione, azienda).tanto che, può essere sei volte superiore al danno finanziario.

I responsabili della gran massa di azioni malevole che vanno dal cyber crime al cyber warfare sono individuati, generalmente ma anche molto generalmente , per il primo ambito nelle organizzazioni criminali, e per il secondo, nella Cina e nella Russia, ciò, per lo meno, dal punto di vista occidentale. Secondo fonti dell'intelligence americana, "lo spionaggio industriale è un fattore integrante della politica economica di Pechino" [21]

Il rischi di venir violati nei proprio database - privati, aziendali o istituzionali – soprattutto attraverso azioni malevole che colpiscono tramite e-mail, non appartiene, quindi, solo a quelle categorie più redditizie dal punto di vista economico: si tratta, infatti, in questo caso, dell'ambito più delicato, ovvero quello militare, la cui violazione (come il caso del drone catturato dagli iraniani dopo un attacco cibernetico) mette a rischio la stabilità di una nazione e l'incolumità fisica della sua popolazione. Meno adeguata è consapevolezza del rischio e sia le difese da parte di organismi come aziende private, istituti di credito e finanziari, pubblici e privati. In pratica sia ha la consapevolezza della minaccia e si hanno i mezzi per contrastarla solo in ambito militare.

I vertici politi ed economici delle nazioni più innovative e quindi più esposte ai rischi della guerra economica connessa con il cyberspazio, stanno pian piano acquisendo la consapevolezza che dìè necessario un'adeguata difesa della spazio cibernetico. Vi sono anche dei segnali di incoraggiamento per quanto concerne la cooperazione, anche se ancora troppo lenti rispetto ai tempi propri dell'evoluzione tecnica e delle emergenze che quotidianamente coinvolgono la competizione economica e industriale tra i grandi protagonisti dell'economia mondiale. Inoltre, se le imprese, con la condivisione delle informazioni, temono la perdita di reputazione, allora, nell'attuale scenario di

[21] *La comunità internazionale*, trimestrale della Società Italiana per l'Organizzazione Internazionale, Vol LXVII 1 2012

crisi economica globale si pone l'urgenza di creare fra gli organismi governativi preposti, sia civili che militari, e le aziende, un ambiente di fiducia in cui queste ultime possono condividere i timori e i rischi per la loro sicurezza, mettendo disposizione degli addetti ai lavori i dati circa le minacce, temute ed effettive, di attacchi cibernetici. Dato che ad essere messa in pericolo è la ricchezza economica , industriale e finanziaria di un Paese e con essa la stabilità politica e il suo quieto vivere sociale, in una strategia difensiva globale, in grado di proteggerla da attacchi provenienti dal cyber spazio diventa un imperativo a cui non è più possibile sottrarsi. [22]

6.1 I PRINCIPALI CASI DI SPIONAGGIO E CONTRO-SPIONAGGIO IN ITALIA

6.1.1IL CASO FERRARI VS MCLAREN

Il campionato di Formula 1 2007 è stato segnato dalla controversia del caso di spionaggio perpetuato a danno della scuderia Ferrari da parte della scuderia McLaren. Il personaggio principale di questa spy story è Nigel Stepney, capo meccanico da molti anni in Ferrari, che a fine campionato 2006, ritiratosi momentaneamente Ross Brawn sperava di poterne prendere il posto e di divenire così direttore tecnico. Questo non successe: come direttore venne scelto Mario Almondo, mentre all'inglese fu riservato un posto diverso, lontano dal muretto. Il fatto indispettì Stepney e da qui si suppone che partano i motivi della sua azione nei confronti della Ferrari. La Spy-Story viene scoperta all'incirca dopo il Gran Premio degli Stati Uniti 2007 quando alla Ferrari si parla di sabotaggio nel GP di Monaco. Il tutto sarebbe stato opera dell'ex-capo meccanico Nigel Stepney, che avrebbe sparso nei serbatoi delle vetture di Raikkonen e Massa una polvere bianca. A ottobre 2008 tale fatto è stato dimostrato, la polvere bianca era stata appositamente inserita da Stepney per provocare "grippaggio" nei motori del cavallino. Ma andiamo con ordine, Stepney, ha un carissimo amico alla McLaren, Mike Coughlan, al quale nell'aprile del 2007, consegna un dossier di 780 pagine dettagliato dei disegni tecnici della Ferrari F2007. Pochi mesi dopo, la moglie di Mike Couglan, Trudy, tentò di fotocopiare il dossier consegnato da Stepney in una copisteria di Woking, tra le altre cose quartier generale della McLaren, ma il dipendente, insospettito dal

[22] *La comunità internazionale*, trimestrale della Società Italiana per l'Organizzazione Internazionale, Vol LXVII 1 2012

materiale, avvisò tramite telefono, Maranello, sede della Ferrari. Da qui iniziano le indagini interne della squadra di sicurezza della Ferrari, che porteranno il 3 luglio al licenziamento di Nigel Stepney e all'annuncio tramite comunicato della casa automobilistica di Maranello, nel quale dice:"Ferrari annuncia che ha recentemente presentato una causa contro Nigel Stepney e un ingegnere della McLaren-Mercedes del team Vodafone con il Tribunale di Modena, per quanto riguarda il furto di informazioni tecniche. Inoltre, l'azione legale è stata promossa in Inghilterra e un mandato di perquisizione è stato emesso sulla ingegnere. Questo ha prodotto un risultato positivo."[23] A questo punto la FIA decide di aprire un'inchiesta. La McLaren è accusata dalla Ferrari di avere utilizzato i disegni a proprio vantaggio, mentre la casa inglese sostiene di non sapere niente e che il tutto era noto al solo Coughlan. Dopo una prima udienza saltata si arriva al 26 luglio, giorno del giudizio. La McLaren viene ritenuta colpevole di essere entrata in possesso di materiale confidenziale Ferrari, ma non viene presa nessuna sanzione in quanto non esistono prove che il materiale sia stato effettivamente utilizzato dal team inglese. Cinque giorni dopo, però, il presidente della FIA Max Mosley decide di fare ricorso. Come data per la seconda udienza viene fissato il 13 settembre. Viene alla luce uno scambio di mail tra il pilota della McLaren Fernando Alonso e il collaudatore Pedro de la Rosa in cui vengono citate informazioni riservate della Ferrari sulla monoposto del 2007. Il contenuto di queste riguardava la distribuzione dei pesi della Ferrari di Raikkonen nel GP d'Australia di quell'anno, nonché dell'impianto frenante della concorrente, in modo da poter provare nei test che risultati avevano sulla McLaren. Tuttavia dallo scambio di messaggi non emerge alcuna prova concreta dell'utilizzo di tali dati, anche se appare chiaro che le informazioni non era in possesso del solo Coughlan. Questi fatti inducono la FIA a sostituire il ricorso in appello con una convocazione del consiglio mondiale. Durante tale riunione la Ferrari porta come presunte prove della colpevolezza McLaren le mail di Alonso e De La Rosa, oltre ad alcuni sms. La FIA emette una nuova sentenza a sfavore della McLaren. Alla casa inglese vengono tolti tutti i punti del mondiale costruttori; le viene inoltre comminata una multa di 100 milioni di dollari.[24]

6.1.2 IL DELLA NUOVA PIGNONE

Il 18 maggio 2012 il Tribunale di Firenze ha emesso una condanna a 6 mesi di reclusione con risarcimento del danno demandato al giudizio in sede civile a un ex dipendente di 68 anni per il

[23] www.en.wikipedia.org
[24] www.it.wikipedia.it

caso di spionaggio industriale a danno dell'azienda Nuovo Pignone- Ge Oil&Gas per la quale l'uomo ha lavorato per diversi anni. La spia, che aveva mansioni di addetto alle vendite e l'accesso alla banca dati dell'azienda, tra il 2004 e il 2006, ha sottratto quasi tutto il know how tecnologico. Stando infatti a quanto emerso dalle indagini, il dipendente infedele ha scaricato 5000 file contenti disegni per la realizzazione di parti di ricambio come pompe, valvole per turbine, codici, prezzi praticati sui ricambi, quest'ultima informazione assolutamente top secret coperta da identificativi in codice. Nel corso delle indagini sono state compiute anche perquisizioni nell' abitazione dell' uomo e sul luogo di lavoro, durante le quali sono stati trovati riscontri alle imputazioni. Secondo l'accusa le informazioni andavano a concorrenti del Nuovo Pignone, che potevano così interferire nelle trattative commerciali con clienti di Russia e Iran, potendo produrre esse stesse ricambi 'copiati' dai disegni scaricati dalla banca dati e conoscendo anche il prezzo che Nuovo Pignone- Ge Oil&Gas avrebbe offerto. [25] [26]

6.1.3 IL CASO OLIVETTI

Il gruppo industriale Olivetti si è trovato al centro di un caso di spionaggio a favore dell'Urss, trattato davanti al tribunale di Ivrea e finito con una significativa condanna, a cavallo degli anni novanta che ha visto coinvolti due dipendenti della sua azienda e un'agente del Kgb.

Tutto nasce dopo due anni di indagini del controspionaggio italiano che il 13 luglio 1990, portano all'arresto a Torino di Victor Dimitri, un funzionario del GUT, l'organismo sovietico incaricato di provvedere agli acquisti di materiale elettronico all'estero. Con lui viene arrestata anche una funzionaria modello dell'Olivetti, Maria Antonietta Valente, che gli sta per consegnare un involucro: all'interno vi sono i dati relativi al "Tempest", vale a dire il sistema per proteggere i computer in uso alla NATO. Lo scambio è stato organizzato dal capoarea dell'Olivetti a Mosca, Roberto Mariotti, che si è servito di un sistema di triangolazioni già collaudato, utile a esportare materiali elettronici "embargati", cioè non muniti di permessi del Cocom (l'organismo atlantico che filtra la collocazione in aree sensibili di prodotti di tecnologici a valenza strategica). Mariotti in particolare si è servito di una società intermediaria del Lichtenstein e poi ha incaricato la sua funzionaria di acquisire il "Tempest", a nome dell'Olivetti, presso una ditta fornitrice dell'azienda ad Ivrea, ignorando che il SISMI aveva infiltrato un proprio agente nell'operazione. Appena

[25] http://www.lanazione.it/firenze/cronaca/2012/05/18/714949 - spionaggio_industriale_condannato_dipendente_nuovo_pignone.shtml
[26] http://www.toscanatv.com/leggi_news?idnews=NL063138

giunge a Mosca la notizia degli arresti, Mariotti viene spostato dai servizi segreti sovietici a Blagovedcensk, una località – praticamente sotto il controllo totale del Kgb - al confine con la Cina. Più tardi assumerà il nome di Roberto Stepanov che mantiene fino a quando dopo undici anni di latitanza decide, per complicatissime vicende familiari, di tornare in Italia e di costituirsi. Lo aspetta una pena di sei anni di carcere per spionaggio politico-militare.[27] A Dimitriev e alla Valente erano stati inflitti quattro anni di carcere, ma poi il russo è stato graziato dal presidente della Repubblica Cossiga, dopo un accordo con Gorbaciov, che prevedeva lo scambio di Dimitriev con l'uscita dall'Urss della moglie e delle figlie del grande generale fuggiasco del Kgb, Oleg Gordiewski. [28]

6.1.4 IL CASO PIRELLI

Nel 1976 la Pirelli aveva concluso un importate accordo con l'americana Corning Glass per impiegare nelle fibre ittiche la tecnologia OVD (Outside Vapour Deposition, deposizione di vapore esterna) sviluppata da questa società. L'uso di tale tecnologia ha reso possibile la produzione di fibre ottiche con ossido di silicio sintetico conseguendo grossi vantaggi in termini di qualità e prestazioni. Gli sviluppi successivi hanno portato a introdurre i primi sistemi di di telecomunicazione fotonica nelle linee telefoniche italiane.

Nel 1983 lo stabilimento di Battipaglia della POS (Fibre Ottiche Sud, società controllata dalla Pirelli) aveva iniziato a produrre cavi a fibre ottiche. Nello stesso periodo la Pirelli aveva iniziato a sperimentare la tecnologia MCVD (Modified Chemical Vapour Deposition, deposizione chimica di vapore modificata), inizialmente sviluppata negli USA dalla AT&T e dalla Corning. Sempre negli anni ottanta la Pirelli decise di acquistare la tecnologia VAD (Vapour Axial Deposition, deposizione di vapore assiale), messa a punto dalle giapponesi Sumitomo e NTT, adottandola per prima in Europa, nel 1985, nello stabilimento di Bishopstoke, nel Regno Unito.

Da quanto appena illustrato appare chiaro come la Pirelli avesse percepito fin dall'inizio del loro sviluppo l'importanza delle tecnologie fotoniche di telecomunicazioni, e come avesse deciso di adottare una strategia di alleanze internazionali fondate sulle tre tecnologie di fabbricazione delle fibre ottiche che apparivano più interessanti e fra loro complementari.

[27] Giuliano Tavaroli e Giorgio Bottai, *Spie*, pag 108
[28] IL GIORNALE, 11 agosto 2005 , di Paolo Guzzanti

E proprio su questo terreno si muovono gli avversari.

Un caso da manuale di spionaggio industriale emerge quando ci si accorge che un dipendente, che a un certo punto viene improvvidamente "dimissionato", aveva venduti,o dato, informazioni tecniche, sul processo di produzione industriale delle fibre ottiche a personaggio che agivano come intermediari per un gruppo intenzionato a costruire una fabbrica di fibre ottiche in Malaysia.

Questa persona fornisce a terzi informazioni relative alle tecnologie messe a disposizione su licenza di produzione alla Pirelli dalla statunitense Corning, questione quanto mai delicata, perché può fornire all'azienda licenziataria il pretesto per revocare la licenza, cose che peraltro gli americani avevano intenzione di fare in quel momento, e perché il mercato dei cavi stava andando per la maggiore e loro avrebbero potuto dettare migliori condizioni.

L'operazione FOS si svolge tra il 1999 e il 2001 e si conclude con un nulla di fatto per un motivo semplice: il crollo del mercato dei cavi. Alla Malaysia l'investimento non interessava più.

I primi passi del caso sono alimentati da un dirigente della strutture industriale: i dirigenti di stabilimento individuano questo quadro infedele e prendono la decisione di chiederne le dimissioni. Hanno dato incarico a un osservatore locale di monitorare questa persona e salta fuori un tenore di vita ben superiore a quanto potuto permettersi. Dal dossier che viene presentato a Giuliano Tavaroli, capo delle sicurezza aziendale di Pirelli, risulta che questo signore ha ricevuto pagamenti importanti, dell'ordine di 800 o 900 milioni di lire da un ufficio legale svizzero specializzato in brevetti. L'investigatore privato in pratica accede ai conti di questa persona e può dire a chi ha commissionato l'accertamento: guardate che ha ricevuto pagamenti importanti che non si giustificano. Il dossier arriva sul tavolo del capo della security aziendale quando la decisone di allontanare il quadro è già stata presa: una scelta quanto mai improvvida perché bisognerebbe più che mai tenerlo sotto controllo e vedere cosa combina. Ricostruire con chi s'incontra, la sua mappa relazionale. Nel momento in cui lo dimissioni, facendogli capire di fatto che tu sai, lui non può che diventare molto prudente e rendere tutti gli accertamenti molto più difficili. Mentre se fosse rimasto in azienda sarebbero di fatto diventate più facilmente disponibili informazioni utili a ricostruire il quadro d'insieme e, soprattutto, fondamentali per arrivare a quelli che stavano dietro la sua azione, la rete che aveva in lui il suo terminale.

La security aziendale ricostruisce – con un'operazione di counterintelligence, partendo dallo stabilimento di Battipaglia, la FOS, dove lavora- con chi è in contatto. E individuiamo quindi questo ufficio legale svizzero, specializzato in brevetti. Verifichiamo come il terminale

dell'operazione sia la Malaysia, in particolare un Invest Park industriale in cui è presente una multinazionale americana che è stato inaugurato del primo ministro malese.

Sull'operazione sono a lavoro, in Svizzera, inizialmente due squadre: quella di Emanuele Cipriani, per i pedinamenti, mezzi, etc e un altro fornitore, un professionista svizzero, per tutto quanto riguarda il fronte malese. E in questo modo viene identificato un gruppo di italiani, tra cui alcuni tecnici, che avrebbero dovuto far partire la nuova fabbrica di cavi in Malaysia.

Viene individuato e fotografato il capannone, vengono ricostruiti gli incontri tra il gruppo degli italiani e i loro interlocutori d'affari malesi interessati al progetto e vengono fotografati e identificati a loro volta. Viene dato un nome a coloro che in Italia potevano forse finanziare il progetto, o almeno, a loro si era rivolto sempre il solito gruppo di italiani in azione ed era un istituto finanziario di Roma.

Con questa attività investigativa viene individuata anche la frangia italiana che opera sotto l'egida di un'organizzazione internazionale.

Comunque l'operazione per bloccare il trasferimento del know how, o spionaggio industriale che dir si voglia per la Malaysia, era pronta, ready to go.

Poi succede che il capo della security di Pirelli non riesce a trovare la disponibilità da parte degli ambienti giudiziari e degli investigatori dello Stato che, in un caso analogo, ha trovato ad esempio la Ferrari. Sta di fatto che se non ci fosse stato il crollo del mercato a bloccare l'azione di spionaggio dei "malesi", ci sarebbero stati parecchi danni per l'azienda. [29]

7.1 CONTROSPIONAGGIO E CRISI ECONOMICA

La crisi economica che sta interessando l'Italia negli ultimi anni ha dei risvolti significativi nel tessuto economico e produttivo del nostro Paese, pertanto, i nostri servizi di informazione e sicurezza hanno messo nero su bianco quest'aspetto della crisi nell'ultima Relazione al Parlamento. Dal testo emerge con chiarezza che la crisi economico-finanziaria ha ristretto gli spazzi di accesso al credito e i margini di redditività di molte aziende nazionali, ne ha accresciuto le esposizioni alle mire espansionistiche di grandi multinazionali estere e di diretti competitors, interessati a

[29] Giuliano Tavaroli e Giorgio Bottai, *Spie*, pag 108

diversificare le proprie attività e a incrementare gli utili, nonché ad assumere e consolidare la leadership in specifiche fasce di mercato. Ciò a detrimento della competitività nazionale, specie in settori di eccellenza, e dei livelli occupazionali, soprattutto in relazione all'eventuale delocalizzazione degli impianti produttivi. Si è rilevato, nel contempo, un decisivo incremento di politiche di agevolazione fiscale e amministrativa che Paesi, geograficamente in particolare alle regioni del Nord-est Italia, hanno attuato per attirare verso il loro territorio nazionale le piccole e medie imprese nazionali di maggior pregio.

La congiuntura sfavorevole ha poi reso più vulnerabile il tessuto imprenditoriale italiano anche rispetto al fenomeno dello spionaggio industriale, che rischia sia di depauperare il potenziale produttivo e innovativo nazionale, sia di costituire in serio danno alla sicurezza e alla competitività del nostro sistema Paese.

Tale minaccia è sicuramente amplificata nel cyberspazio,in termini incidenti, soprattutto, sulla tutela delle proprietà intellettuale, sull'elaborazione delle strategie di mercato e sulla formazione dei pacchetti clienti. La sottrazione di informazioni tramite le reti e i sistemi ICT (Information and Communication Technology) in futuro acquisterà maggiore rilevanza rispetto alle tecniche "tradizionali", anche perché i dati aziendali di significativo interesse sono allocati in più database che moltiplicano le possibilità di accesso illecito alle informazioni.

Inoltre, la necessità per le aziende nazionali di utilizzare forme di finanziamento alternative al credito al credito bancario ha sollecitato l'interesse degli operatori stranieri verso il mercato nazionale, esponendo le aziende target, indipendentemente dall'esito delle operazioni trattate (acquisizioni, fusioni, partnership, joint-venture, finanziamenti), alla dispersione di dati sensibili, di natura commerciale, finanziaria od operativa.

L'attenzione informativa in tema di investimenti e partecipazioni straniere nel tessuto interno ha pertatno concorso a tutelare le infrastrutture e i comparti di rilevanza nazionale sotto il profilo economico-strategico, del know-how, dei livelli occupazionali e di produzione.

In tale contesto, si è rilevato un particolare attivismo di operatori economici stranieri nei settori dei trasposrti, delle telecomunicazioni e dell'energia. Nello specifico, si evidenzia la crescente presenza nella distribuzione di gas e di prodotti petroliferi di operatori dell'Est Europa, già leader nel settore dell'estrazione, che perseguono una mirata strategia di integrazione verticale del ciclo produttivo energetico. In prospettiva, su un piano più in generale, grandi investitori del'est Europa e asiatici potrebbero ulteriormente accrescere il proprio ruolo sul mercato italiano.

I primi, proseguendo la strategia già avviata da alcun anni, potrebbero rivolgersi alle realtà produttive medio-grandi (per fatturato o livello di occupazione) del settore metallurgico nazionale. Con investimenti mirati su acciaierie e industrie meccaniche a elevato tasso di tecnologia, dalla raffinazione e distribuzione degli idrocarburi, e in via residuale, del turistico-alberghiero.

Gli operatori asiatici, attratti dal brand manifatturiero italiano, potrebbero sfruttare la opportunità offerte dai nuovi accordi logistici con interporti nazionali, soprattutto dell'Italia Centrale, per incrementare i piani di investimento.

Secondo gli indicatori raccolti, inoltre, competitors stranieri, soprattutto orientali, potrebbero tentare di accedere a progetti di ricerca nazionale e di acquisire nuovi moduli di tecnologia innovativa, per ottenere la disponibilità di importanti "brevetti" da sfruttare nei mercati, specie se caratterizzati da opportunità di sviluppo industriale o commerciale a breve termine. Questa progressiva espansione conta sul crescente supporto di istituti bancari asiatici che, in futuro, potrebbero erodere significative quote di mercato agli operatori italiani, soprattutto nelle transazioni finanziarie internazionali di supporto delle nostre aziende operanti da e con l'estero.[30]

[30] *Relazione al Parlamento 2011*

CONCLUSIONI

A conclusione di questo lavoro è doveroso ricordare come l'Italia sta facendo dei passi in avanti nell'ambito dell'intelligence economica. Sicuramente le politiche di sdoganamento dell'attività di intelligence attuate dal Dis, con la nascita del concetto della cultura della sicurezza aiutano ad aumentare la consapevolezza del rischio e della minaccia anche nel settore economico. Sicuramente è bene partire da un approccio culturale e formativo in modo che questo possa essere proiettato per il futuro, ma non basta.

Rispetto ad altri Paesi europei, come la Francia ad esempio, siamo indietro di parecchi anni, loro hanno l'*École de guerre économique* (EGE), creata nel 1997, che supporta l'attività industriale ed economica del loro paese. Quindi, non è un caso se l'economia francese va bene e i prodotti francesi vengono venduti in tutto il mondo e non deve sorprenderci se i francesi, tramite delle brillanti operazioni finanziarie, hanno acquisito in pratica la distribuzione alimentare in Italia.

Stessa cosa anche per paesi come la Germania, dove è vi è una forte sinergia tra servizi di informazione e sicurezza e i privati come la Simens, che ha servito ai servizi informativi tecnologie all'avanguardia. In effetti, i servizi tedeschi si sono poi specializzati nella "pirateria informatica", con la quale hanno avuto accesso alle banche dati delle imprese e amministrazioni di tutto il mondo.[31]

Per non parlare poi di paesi come il Giappone, che con il Miti e il Jetro fa intelligence economica dalla fine della seconda guerra mondiale, o come la Cina, che forse è diventato il primo paese al mondo per lo sviluppo dell'intelligence economica.

E in questa cornice internazionale che l'Italia si deve misurare, deve mostrare il suo valore. Non può più restare a guardare mentre gli altri paesi aumentano quote di mercato e copiano i nostri prodotti. E' importante capire che c'è una crescente attenzione riposta dai governi dei Paesi più sviluppati verso l'implementazione di politiche a supporto della propria produzione nazionale, lascia intendere come i rapporti economici saranno considerati sempre più importanti nelle realzioni internazionali.

Detto questo, va sottolineato come sia urgente in Italia una strategia di lungo periodo che coinvolga non solo i settori pubblici, ma anche e soprattutto il settore privato, in tutti i campi strategici e

[31] Mauro Morbidelli, Intelligence Economica e Competitività Nazionale, pag 82

tecnologici al fine di avere una visone unitaria della direzione che deve prendere il paese. Cioè, in parole povere, dove vogliamo andare e come ci dobbiamo arrivare.

Inutile poi, sottolineare il valore tattico-strategico della funzione del controspionaggio economico del nostro paese, che deve implementare le sue funzioni di difesa del sistema economico dalle minacce degli attori siano essi governi o grandi imprese private. Non solo, va tutelato maggiormente il patrimonio tecnologico e scientifico delle nazionali, così come le tecniche e le procedure di gestione delle attività private. Ovviamente l'attività del controspionaggio in Italia deve essere orientata anche al contrasto delle attività di intelligence straniere interessate alla conoscenza anticipata e all'eventuale condizionamento delle politiche nazionali; in sostanza si devono arginare le pratiche di ingerenza e di influenza esterna. [32]

Infine, va creato un cordone culturale attorno alla nostra intelligence economica in modo che vi sia una maggiore sinergia tra pubblico e privato, e magari con le università, centri di ricerche e fondazioni, che spesso producono lavori e menti di altissimo livello, al fine di sviluppare un sistema –Paese efficiente e competitivo .

[32] Mauro Morbidelli, Intelligence Economica e Competitività Nazionale, pag 88

BIBLIOGRAFIA

Mauro Morbidelli, *Intelligence Economica e Competitività Nazionale*

Carr Chiris, Morton Jack, Furniss Jerry, *The Economic Espionage Act: Bear Trap or Mousetrap?*

Carlo Mosca, *I servizi di informazione e il Segreto di Stato*

Umberto Fava, *Importanza dell'Intelligence economica nella realtà della Globalizzazione*, 2002, Biblioteca CASD

Carlo Jean Paolo Savona, *Intelligence Economica*

Quaderni di Intelligence N.1 Anno 2012

Relazione dei servizi di sicurezza e informazione 2009 - 2010 – 2012

Giorgio Bottai e Giuliano Tavaroli, *Spie*

Aldo Giannuli, *Come funzionano i Servizi Segreti*

Legge 114/2007

Steven Fink, *Managing the global risk of economic espionage*

Thomson Gale, *Encyclopedia of Espionage, Security and Intelligence*

Christopher Andrew, *Secret Intelligence*

Ira Winkler, *Case study of industrial espionage through social engineering*

Phillip c. Wright e Geraldine Roy, *Industrial espionage and competitive intelligence: one you do;one you do not*

Hedieh Nasheri, *Economic espionage and industrial spying*

Douglas Bernhardt, *Competitive intelligence. how to acquire and use corporate intelligence and counter-intelligence*

Presenza cinese in italia e sicurezza economico-finanziaria, comando generale della guardia di finanza, ii reparto – ufficio analisi d'intelligence

U. Rapetto e R. di Nunzio, *L'atlante delle spie*

Giuseppe de Lutis, *I Servizi Segreti Italiani*

Loretta Napoleoni, *Terrorismo SpA*

Paul m. Joyal , *Industrial espionage today and information wars of tomorrow*

Minacce alla sicurezza economica nazionale, Senato della Repubblica xv legislatura

Massimo Franchi, *Intelligence Economica*

SITOGRAFIA

www.bbc.co.uk

www.sicurezzanazionale.it

www.silendo.it

www.servizisegreti.it

www.ilsole24ore.com

www.corriere.it

www.repubblica.it

www.lastampa.it

www.pmi.it

www.senato.it

www.camera.it

www.cia.gov

www.ege.fr

www.fondazioneicsa.it

www.formiche.net

www.oipamagazione.eu

www.lanazione.it

www.toscanatv.com

www.ilgiornale.it

www.youtube.com

www.interno.it

www.sviluppoeconomico.gov.it

www.esteri.it

www.espersso.it

www.panorama.it

www.servizisegreti.com

www.ilmessagero.it

www.globalsecurity.org

www.stratfor.com