LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Impresa e Management

Laurea in Economia e Management

Cattedra di Organizzazione Aziendale

IL BUSINESS DELL'INTELLIGENCE PER LA SALVAGUARDIA DELLA SICUREZZA PUBBLICA E INDUSTRIALE

I casi di studio Black Cube e Blackwater

Relatore:

Prof. Nunzio Casalino

Candidato:

Stefania Francavilla

Anno accademico 2017-2018

A mia Madre.
A mio Padre.
A Noi.

INDICE

INTRODUZIONE

Sicurezza: *"La condizione che rende e fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli, e simili."*

Dizionario Treccani.

Alla base di questo studio vi è il concetto di sicurezza, analizzata su vari livelli: dal Pubblico al Privato. Partendo dal contesto Pubblico, si analizza come sia un dovere dello Stato quello di assicurare la sicurezza all'interno del suo territorio, e come, in virtù del mutato contesto macroeconomico sia stato necessario un intervento normativo per modificare la configurazione del sistema di sicurezza preesistente. La nuova impronta normativa delinea un sistema organico ma allo stesso tempo decentrato in un'ottica di apertura verso il mondo esterno. Apertura, quest'ultima, su diversi fronti: in primis nel reclutamento di figure professionali, ricercate in atenei universitari e non più esclusivamente nelle Forze Armate; nel rapporto con fornitori esterni di servizi complementari ed infine nel rapporto col cittadino, in cui l'intervento normativo è orientato alla creazione di un rapporto trasparente volto alla consapevolezza delle minacce odierne.
La complessità della realtà attuale, rende difficile, nonostante la Riforma, la predisposizione di tutti i servizi di sicurezza internamente, porta perciò lo Stato a dover usufruire di alcuni in qualità di *contractors* (il fenomeno delle PMSCs). Tema, quest'ultimo, ancora molto discusso in Italia, in cui l'assenza di una chiara disciplina normativa al riguardo crea una confusione e un generale ritardo nello sviluppo di business di questo tipo (fenomeno, al contrario, crescente all'estero).

Tornando alla definizione di sicurezza, dalla stessa si evince come siano rilevanti a tal proposito sia le attività preventive che quelle risolutive, volte a minimizzare i danni e i rischi. In particolare, nel mondo aziendale, in virtù dei cambiamenti che la tecnologia ha apportato all'interno di tutti i business, i servizi di sicurezza rappresentano ormai un *must have*.

Si analizzerà in seguito lo sviluppo di un business vero e proprio legato alla sicurezza definito in tale elaborato "il business dell'intelligence". L'attività di intelligence si configura, infatti, come un'attività chiave per l'erogazione di tutti i servizi volti a garantire la sicurezza di persone fisiche e giuridiche.

Nello specifico si è provveduto ad effettuare una disamina dettagliata di queste tipologie di organizzazioni al fine di far emergere peculiarità ed eventuali criticità.

Nel capitolo 1 si analizza la configurazione del sistema di sicurezza pubblico, analizzando la struttura organizzativa dei vari organi che lo costituiscono e contestualmente evidenziando i mutamenti strutturali e culturali che sono stati apportati alla stessa mediante la Riforma del 2007. Nel capitolo 2, invece si procede analizzando la struttura organizzativa e la gamma di servizi offerta dalle società di intelligence private, sottolineandone la rilevanza per la garanzia di un corretto funzionamento di determinate funzioni aziendali e per la tutela dell'azienda in sé. L'operato di tali intelligence companies è rivolto principalmente a privati, siano essi persone fisiche o giuridiche. Nel capitolo 4, invece, vengono trattate le compagnie di tale settore che si rivolgono principalmente agli enti Governativi. Queste ultime, denominate in generale Private Military Security Companies, vengono classificate in modo opportuno in virtù delle loro caratteristiche specifiche all'interno del quarto capitolo. A tal proposito ci si sofferma anche sui driver di crescita del suddetto business, evidenziando vantaggi e svantaggi che la lacuna normativa italiana comporta per gli stessi.

Si portano, a conclusione della trattazione, due esempi di intelligence society che offrono servizi di sicurezza: Black Cube il cui operato è richiesto specialmente da grandi multinazionali; e Academi (ex Blackwater) compagnia i cui principali clienti sono gli Stati, come esempio di Pmsc, la quale offre anche servizi di natura offensiva.

CAPITOLO 1

IL SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

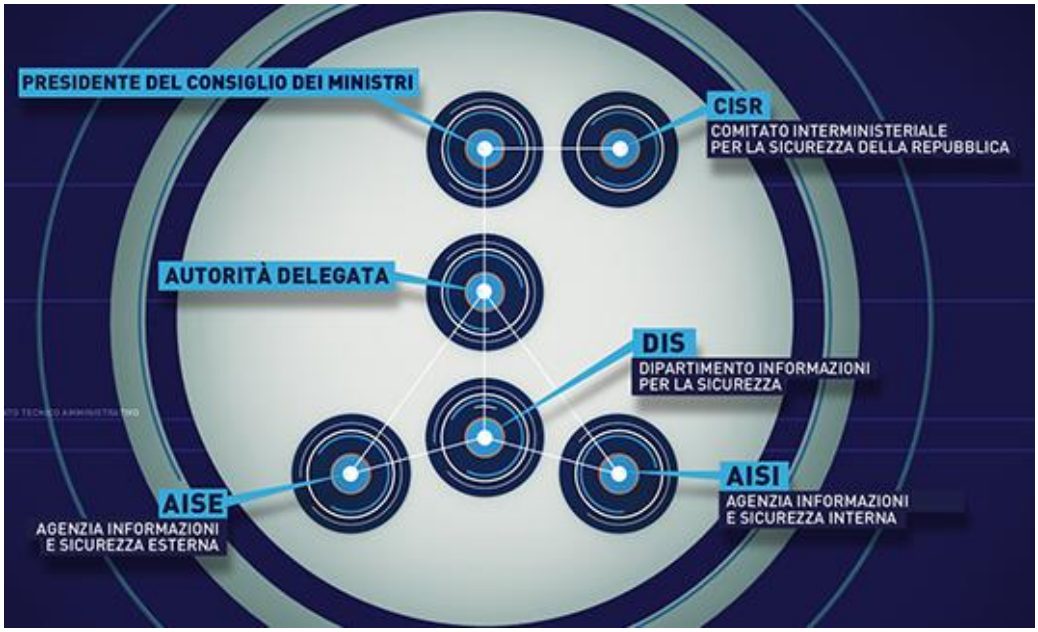
Principali strutture dell'intelligence.

1.1 I PRINCIPALI ORGANI DELLA SICUREZZA DELLA REPUBBLICA

Il sistema di informazione per la sicurezza della Repubblica è costituito da un complesso di organi che hanno il compito di assicurare l'attività informativa per salvaguardare la Repubblica da ogni tipologia di pericolo e minaccia interna ed esterna. Tali organi, pur essendo differenziati per le funzioni svolte, sono tutti strettamente integrati in un sistema organico in cui è di particolarmente rilevante la figura del Presidente del Consiglio dei Ministri.
Dalla figura sottostante è possibile dedurre la struttura prettamente divisionale di tale sistema, che mediante la Riforma del 2007 è stata modificata valorizzando i collegamenti tra divisioni, i rapporti con i vari Ministeri e l'organicità del tutto, proprio grazie al rafforzamento della posizione del PdC[1].

[1] PdC: Presidente del Consiglio dei Ministri.

Figura 1 Rappresentazione del Sistema per la sicurezza della Repubblica



1.2 GLI ORGANI

Gli organi che compongono il Sistema di sicurezza della Repubblica sono:

- Presidente del Consiglio dei ministri
- Autorità delegata
- Comitato interministeriale per la sicurezza della Repubblica (CISR)
- Dipartimento informazioni per la sicurezza (DIS)
- Agenzia informazioni e sicurezza esterna (AISE)
- Agenzia informazioni e sicurezza interna (AISI)

1.2.1 IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Al vertice di tale sistema vi è il Presidente del Consiglio dei Ministri, a cui sono affidate l'alta direzione, la responsabilità generale della politica dell'informazione per la sicurezza e i relativi poteri di coordinamento e direttiva. In particolare, Egli:

- Si occupa del coordinamento delle politiche dell'informazione per la sicurezza;
- impartisce le direttive ed emana le disposizioni necessarie per l'organizzazione e il funzionamento del Sistema, previa consultazione del Comitato Interministeriale per la sicurezza della Repubblica (CISR);

- autorizza il ricorso alle garanzie funzionali per tutelare l'attività degli operatori dell'Agenzia informazioni e sicurezza esterna (AISE) e dell'Agenzia informazioni e sicurezza interna (AISI);
- delega i direttori di AISE e AISI per quanto riguarda la richiesta all'Autorità giudiziaria dell'autorizzazione a svolgere specifiche attività di raccolta delle informazioni;
- sentito il CISR, impartisce al Dipartimento per le informazioni di sicurezza(DIS), all'AISE e all'AISI direttive volte a rafforzare le attività di informazione per la protezione delle infrastrutture critiche.

Rientrano nella sua competenze esclusiva:

- l'apposizione, la tutela e la conferma dell'opposizione del segreto di Stato;
- la nomina e la revoca dei Direttori dei vari organi del sistema (DIS,AISE,AISI);
- la determinazione delle risorse finanziarie annue da assegnare al DIS, all'AISE e all'AISI.

1.2.2 L'AUTORITA' DELEGATA

Il Presidente del Consiglio può delegare a tale figura alcune delle sue funzioni di competenza non esclusiva. È tuttavia, previsto che l'autorità delegata informi costantemente il Presidente del Consiglio sulle modalità di esercizio di tali funzioni delegate. La delega può essere attribuita ad un sottosegretario di Stato oppure ad un ministro senza portafoglio che non può esercitare ulteriori funzioni di governo.

L'Autorità delegata fa parte del Comitato Interministeriale per la sicurezza della Repubblica (CISR) e presiede il Collegio di vertice, composto dal Direttore generale del DIS e dai Direttori dell'AISE e dell'AISI.

1.2.3 IL COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA (CISR)

Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza. Tale organo è composto da:

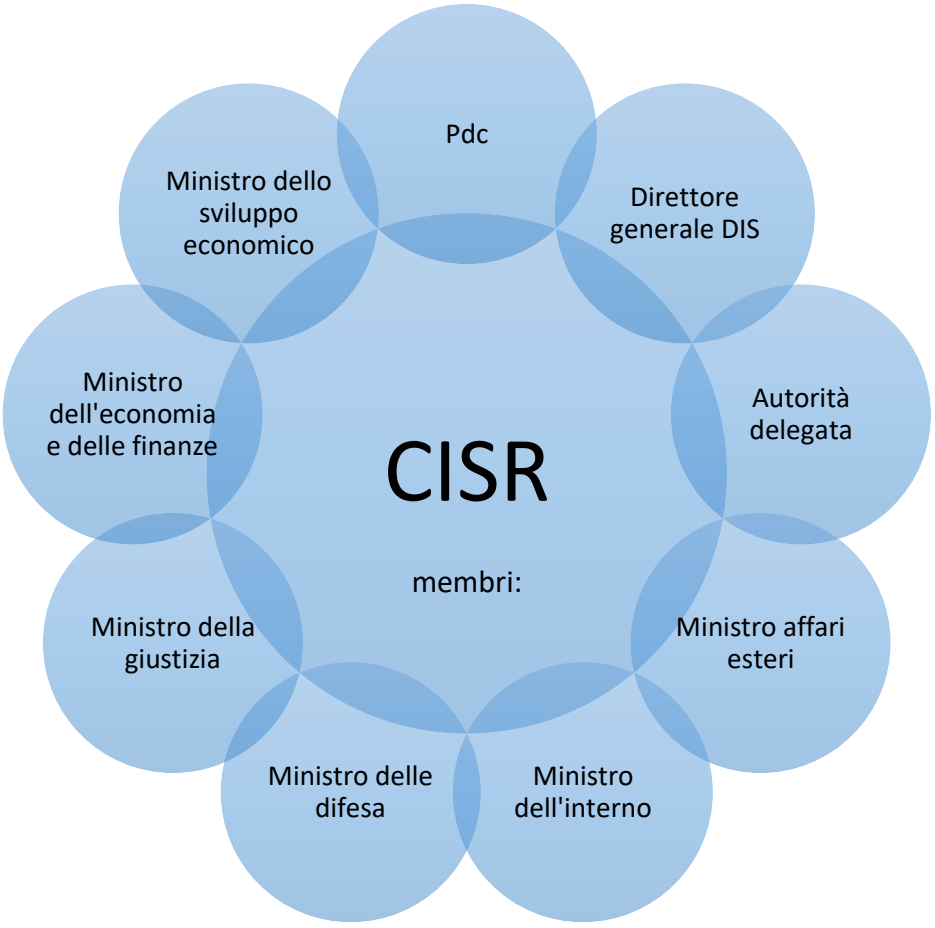
- Presidente del Consiglio dei Ministri, che lo presiede;
- Direttore generale del DIS, in veste di segretario del Comitato;
- Autorità delegata;

- Ministro degli Affari esteri;
- Ministro dell'interno;
- Ministro della difesa;
- Ministro della giustizia;
- Ministro dell'economia e delle finanze;
- Ministro dello sviluppo economico;

Data la sua composizione, tale organo va a configurarsi come un vero e proprio "gabinetto per la sicurezza nazionale" in linea con la più generale tendenza internazionale di centralizzazione del processo decisionale di vertice.

Inoltre, essendo strutturato come un «sistema integrato di comando» a livello politico-strategico, quest'organo delibera sulla ripartizione delle risorse finanziarie e sui bilanci preventivi e consuntivi degli organi del sistema ed esplicita il fabbisogno informativo necessario ai Ministri per lo svolgimento dell'attività di governo.

Figura 2 Rappresentazione del Comitato Interministeriale per la Sicurezza della Repubblica



1.2.4 IL DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)

Il Dipartimento delle Informazioni per la Sicurezza (DIS) è l'organo di cui si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata per l'esercizio delle loro funzioni e per assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative di AISE e AISI.

La sua attività principale è volta dunque al coordinamento degli organi dell'intero sistema e alla raccolta delle informazioni fornite da tali organi.

Con l'approvazione da parte del Parlamento della legge 133/2012, questo ruolo di coordinamento è stato ulteriormente rafforzato, demandando esplicitamente alla responsabilità di tale Dipartimento le funzioni di analisi strategica di intelligence e di gestione unitaria delle risorse umane e materiali del Comparto.

Complessivamente, il DIS:

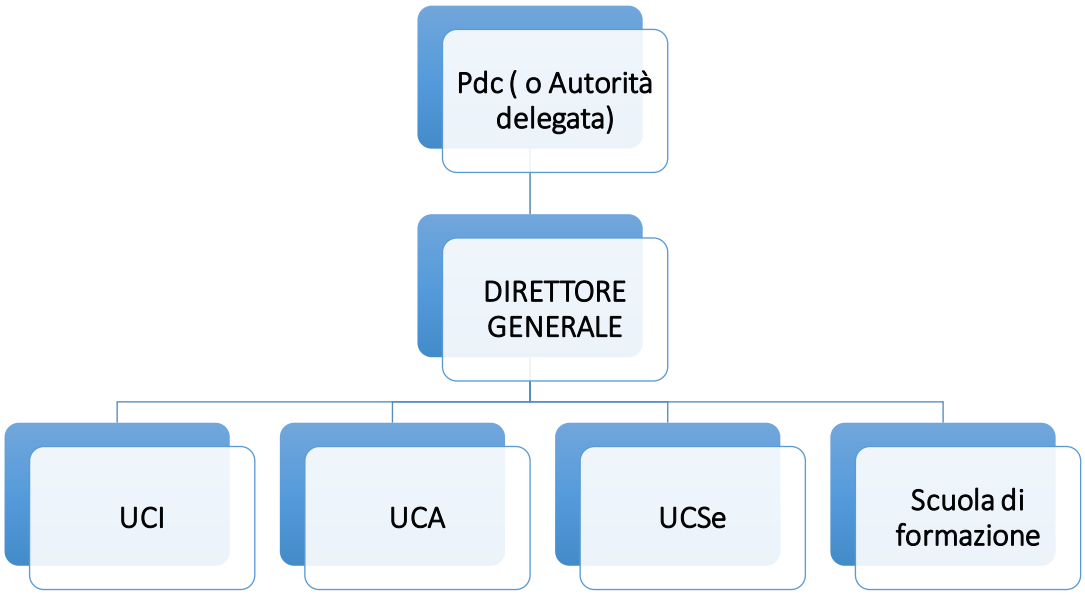
- coordina l'intera attività di informazione per la sicurezza, verificandone anche i risultati;
- è informato costantemente sullo stato delle operazioni di AISE e AISI e funge da tramite con il Presidente del Consiglio dei ministri informandolo sulle analisi prodotte dal Sistema;
- raccoglie informazioni, analisi e rapporti prodotti da AISE e AISI, da altre amministrazioni dello Stato e da enti di ricerca;
- elabora analisi strategiche o relative a situazioni da sottoporre al CISR o ai suoi singoli membri;
- promuove e garantisce lo scambio informativo con le Forze di polizia;
- attraverso l'Ufficio centrale ispettivo controlla l'operato di AISE e AISI;
- vigila sulla corretta applicazione delle disposizioni emanate dal PdC in materia di tutela amministrativa del segreto di Stato e della documentazione classificata;
- impartisce indirizzi di gestione unitaria del personale di DIS, AISE e AISI;
- gestisce unitariamente gli approvvigionamenti e i servizi logistici comuni a DIS, AISE e AISI;
- elabora con AISE e AISI il piano di acquisizione delle risorse umane, materiali e strumentali;
- cura le attività di promozione della cultura della sicurezza e la comunicazione istituzionale

per far fronte alla molteplicità di funzioni che gli sono attribuite.

La legge configura per tale organismo una struttura divisionale, istituendo quattro uffici con specifiche funzioni:

1. Ufficio centrale ispettivo (UCI): controlla l'operato di Aise e Aisi e ne verifica la conformità alle disposizioni di legge e ai compiti a loro affidati dal PdC.
2. Ufficio centrale degli archivi (UCA): coordinamento, controllo e disciplina della raccolta di dati.
3. Ufficio centrale per la segretezza (UCSe): si occupa del segreto di Stato.
4. Scuola di formazione: si occupa dell'addestramento degli agenti.

Figura 3 Rappresentazione della Struttura del Dis.



1.2.5 IL DIRETTORE GENERALE

La direzione generale del DIS è affidata a un dirigente di prima fascia o equiparato dell'amministrazione dello Stato, la cui nomina e revoca spettano in via esclusiva al presidente del Consiglio dei Ministri, sentito il CISR. Il direttore generale è direttamente subordinato al PdC o al suo delegato, qualora quest'ultimo abbia delegato l'attività di alta direzione del DIS.

Il Direttore generale può essere affiancato da vice-direttori nominati dal PdC previo suo parere.

L'incarico ha durata di 4 anni ed è rinnovabile per una volta sola

1.2.6 AGENZIA INFORMAZIONI E SICUREZZA ESTERNA (AISE)

L'Agenzia informazioni e sicurezza esterna (AISE) ha il compito di ricercare ed elaborare tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica dalle minacce provenienti dall'estero.

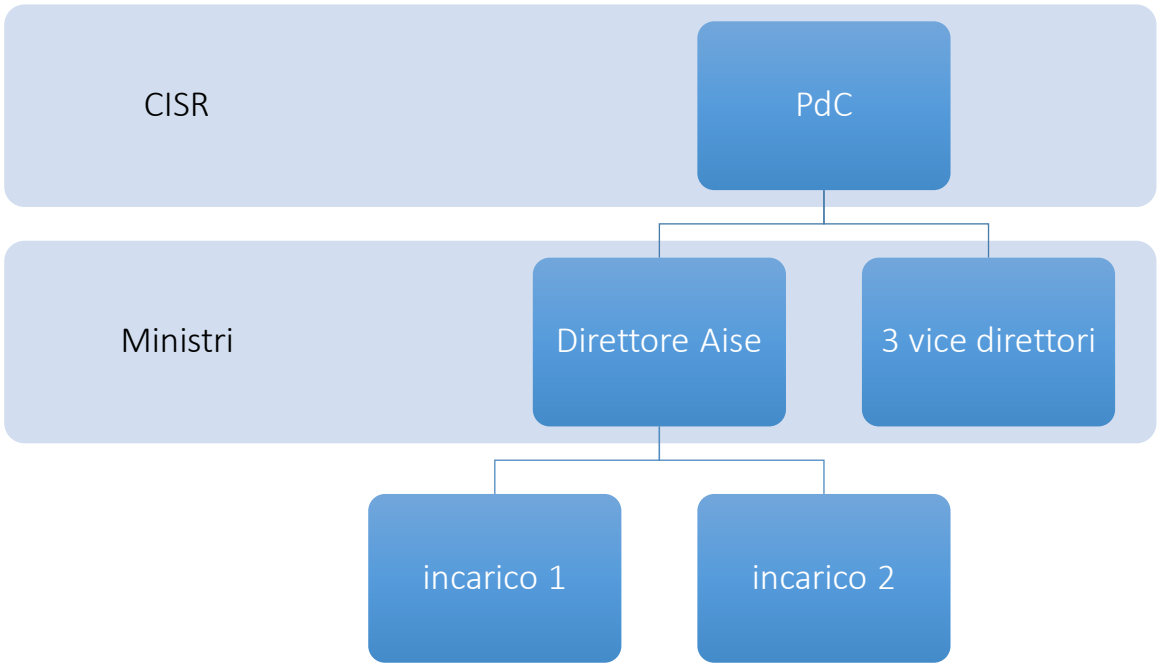
In particolare sono di competenza dell'AISE:

- Tutte le attività di informazione per la sicurezza che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia;
- l'individuazione e il contrasto, al di fuori del territorio nazionale, di attività di spionaggio fatte a danno del Paese (Italia) e di attività volte a ledere gli interessi nazionali in generale;
- le attività di contro proliferazione di materiali strategici.

L'AISE risponde al Presidente del Consiglio dei Ministri, tuttavia è tenuto a fornire un'informativa tempestiva e continua al Ministro della difesa, al Ministro degli affari esteri e al Ministro dell'interno.

Tale organo è presieduto da un direttore nominato e revocato dal PdC, previa consultazione del CISR, scelto tra i dirigenti di prima fascia o equiparati dell'amministrazione dello Stato. L'incarico ha durata di quattro anni ed è rinnovabile una sola volta. Il direttore dell'AISE è affiancato da tre vice-direttori, anch'essi nominati dal PdC sentito il Direttore, mentre le nomine relative ad altri incarichi nell'AISE sono di competenza del Direttore.

Figura 4 Rappresentazione struttura AISE e collocamento nel sistema con evidenza dell'influenza del rapporto che l'organo è tenuto a intrattenere con il Cisr e con i singoli Ministri.



1.2.7 AGENZIA INFORMAZIONI E SICUREZZA INTERNA (AISI)

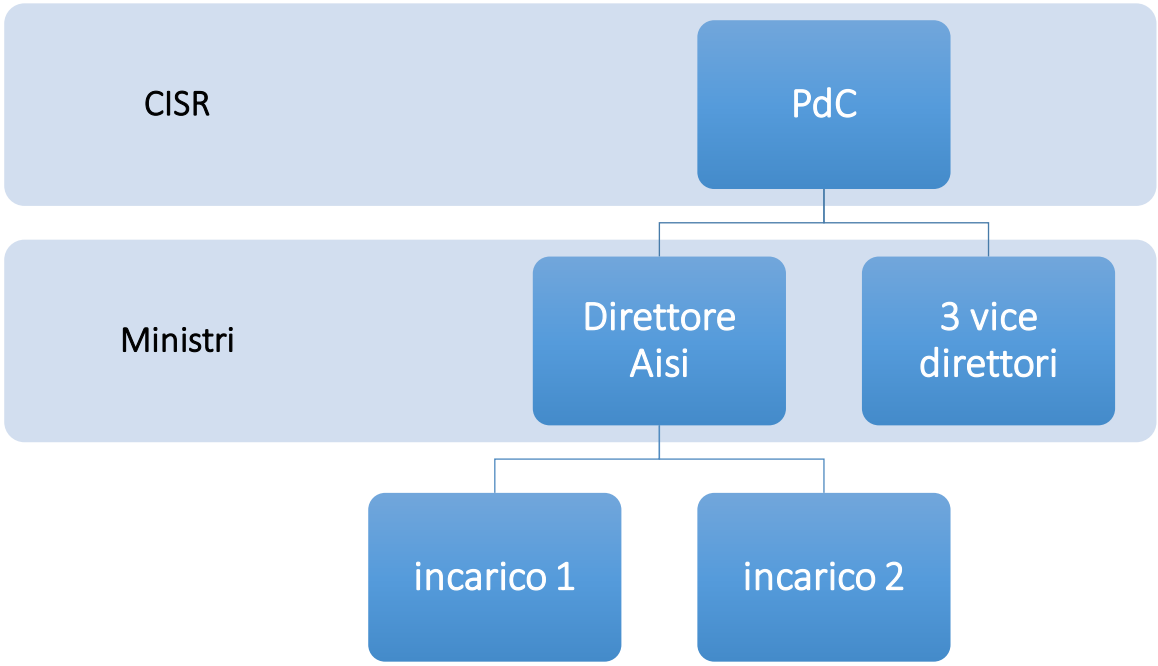
L'Agenzia informazioni e sicurezza interna (AISI) ha il compito di ricercare ed elaborare tutte le informazioni utili per difendere la sicurezza interna della Repubblica e le istituzioni democratiche da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

L'AISI si occupa:

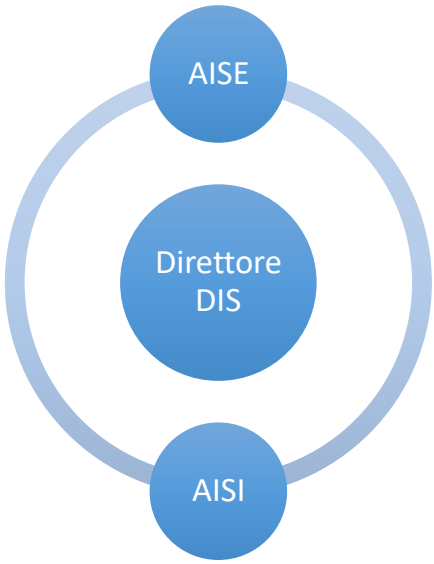
- di tutte le attività di informazione per la sicurezza che si svolgono all'interno del territorio italiano, con la finalità di tutela degli interessi politici, militari, economici scientifici e industriali italiani;
- di individuare e contrastare le attività di spionaggio fatte ai danni dell'Italia, e quelle volte alla lesione degli interessi nazionali effettuate all'interno del territorio italiano.

L'AISI risponde al Presidente del Consiglio dei Ministri ed è tenuto ad informare tempestivamente e con continuità, il Ministro dell'interno, il Ministro degli affari esteri e il Ministro della difesa per le materie di rispettiva competenza.

Figura 5 Rappresentazione struttura AISI e collocamento nel sistema con evidenza dell'influenza del rapporto che l'organo è tenuto a intrattenere con il Cisr e con i singoli Ministri.



Il 4° comma dell'art. 6 della legge 124/2007 stabilisce in particolare il divieto di eseguire operazioni all'estero; queste sono consentite, con l'obbligo di coinvolgere anche la corrispondente Agenzia informazioni e sicurezza esterna (AISE), soltanto in casi di stretta connessione con la propria attività. In questo caso è previsto un intervento coordinato dal direttore generale del dipartimento, con l'intento di evitare sovrapposizioni funzionali e territoriali con l'AISE ed il II Reparto Informazioni e Sicurezza.



Da queste descrizioni emerge come la struttura divisionale dell'intero sistema sia stata pervasa da una corrente di organicità. Infatti i vari organi, strutturati in maniera divisionale, si uniformano in un unico sistema che vede come fulcro il Presidente del Consiglio dei Ministri.
Tale configurazione è in realtà frutto della Riforma del 2007 del Sistema per la sicurezza della Repubblica, che ha rinnovato la struttura risalente al 1977 proprio all'insegna dell'organicità e della cooperazione tra i vari organi per rispondere alle esigenze che il nuovo scenario socioeconomico porta con sé.

2. I FATTORI CHE HANNO RESO NECESSARIA LA RIFORMA

Gli eventi che hanno segnato il 2017 in un'ottica di intelligence evidenziano come la tutela della sicurezza nazionale richieda contestualmente capacità di prevenire e contrastare minacce tradizionali, e di far fronte a profili di rischio che, pur non nuovi, assumono, per caratteristiche e modalità, veste e valenza inedite. Tale compito di pertinenza statale, comporta per gli Organismi informativi un costante affinamento di prassi e metodologie per far si che la propria azione sia adeguata a contesti e problematiche che sono e restano per definizione fluidi.

La riforma del 2007 innovando la struttura preesistente e concependo un nuovo modo di operare degli Organismi informativi cerca proprio di far fronte a tale necessità.

I mutamenti sociali da cui essa nasce sono riconducibili al piano geopolitico, economico-finanziario

e tecnologico.

2.1 IL PROFILO GEOPOLITICO

Sotto il profilo geopolitico si assiste all'affermazione di nuovi colossi globali, gli assi mondiali sembrano inclinarsi ponendo l'Occidente in una posizione di negoziazione del suo *status quo* con l'emergente Oriente.

A tali dinamiche si è accompagnato il perdurare, e talvolta l'aggravarsi di criticità che sembravano appartenere al passato, pur restando sempre nell'occhio del mirino dell'intelligence, come la minaccia atomica e quella militare convenzionale.

Tra i fattori geopolitici di maggior rilievo va anche annoverato l'affermarsi di attori non statuali in grado di rapportarsi da una posizione di forza a Stati e Governi che, spesso, superano per potere e capacità finanziarie. Tale riferimento è da intendersi ad una varietà di attori, leciti ed illeciti, tutti caratterizzati da una dimensione transnazionale, la cui evoluzione globale è coincisa temporalmente con il ridimensionamento del ruolo delle potenze mondiali tradizionali e con la sfiducia maturata rispetto alla credibilità e alla tenuta delle leadership a livello di singoli Paesi. In particolar modo, la perdita di fiducia nei vari governi nazionali ha indotto un malcontento diffuso e la nostalgia del modello Stato-nazione. Il caso Brexit e i risultati dei partiti conservatori raggiunti nelle recenti elezioni delle principali potenze occidentali sono una forte evidenza di ciò.

Infine, ultimo fattore geopoltico di elevata rilevanza è quello del terrorismo, minaccia che è sempre esistita ma che tramite la globalizzazione e la tecnologia ha assunto una nuova veste, molto più intrusiva e difficilmente controllabile.

I recenti attentati di matrice jihadista verificatisi nelle principali capitali europee evidenziano non solo la volontà di affermazione culturale, ma soprattutto mostrano come il terrorismo si stia facendo strada nella vita di ognuno attraverso nuovi mezzi, quelli che l'evoluzione tecnologica ha portato con sé. Detto ciò, emerge chiaramente l'aspetto duale del progresso tecnologico: da un lato è possibile considerare le tecnologie un asset strategico; dall'altro, esse possono rappresentare anche uno strumento offensivo.

2.1 IL PROFILO ECONOMICO-FINANZIARIO E TECNOLOGICO

I profili economico-finanziario e tecnologico sono strettamente collegati, infatti la rivoluzione digitale ha contribuito all'affermarsi dell'economia 4.0.
I principali tratti dell'economia 4.0 (nota anche come Industria 4.0) sono: la fabbrica digitale, la sharing economy, il risk management, i social media, il digital marketing e i servizi digitali; tutti elementi che presuppongono l'utilizzo della rete e dei supporti tecnologici.
Tuttavia, la rivoluzione digitale non ha solo contribuito alla nascita di un nuovo modello di economia e di nuove modalità di impresa, essa ha infatti rivoluzionato la vita del cittadino in vari ambiti. In primo luogo l'istantanea fruibilità a livello globale di notizie e dati, l'ampia disponibilità di conoscenze a portata di tutti, rappresentano un grande vantaggio per la diffusione della conoscenza e dell'informazione, tuttavia, nel mondo della rete trovano spazio anche rappresentazioni mistificate o tout court infondate e narrazioni distorte o falsificate della realtà, risulta perciò prioritario per lo Stato tutelare i suoi cittadini anche dalle minacce derivanti da tale sistema. Con il d.lgs 2017 del governo Gentiloni sulla Cyber security si mira proprio a questo.

Inoltre, la spinta pronunciata verso la digitalizzazione e la disintermediazione, correlata all'ubiquità dello strumento cyber, ha fatto emergere anche rischi nel mondo della finanza. Qui, gli spazi di opacità e di anomia generati dall'oggettiva difficoltà di assicurare un tempestivo adeguamento normativo e regolamentare a livello statale ed internazionale, si prestano ad essere sfruttati per una serie di attività illecite, dal riciclaggio al finanziamento del terrorismo. La nascita di fenomeni come quello delle criptovalute caratterizzate da elevata volatilità e anonimato e di piattaforme alternative per la loro negoziazione necessitano di una mirata attenzione anche per le possibili ricadute sul piano della sicurezza finanziaria.

A tal proposito il riferimento è soprattutto alla tecnologia blockchain che consente di scambiare dati a prescindere dalla conoscenza delle controparti e dall'esistenza di un garante del sistema, e allo shadow banking, ovvero quel sistema di operatori che svolgono attività parallele di intermediazione creditizia al di fuori dei circuiti bancari tradizionali.

In linea generale, quello che si è affermato con la rivoluzione digitale è un mondo inter e iper-connesso; marcato da una sfiducia generalizzata verso meccanismi ed attori statali; fortemente orientato verso una disintermediazione a livello politico, finanziario e mediatico; caratterizzato da un'intensa competizione economica che sfrutta al massimo le potenzialità della dimensione cibernetica.

"Su questa tela di fondo, le previsioni della Legge 124/2007 hanno costituito una preziosa base di riferimento per permettere al Comparto nazionale di evolversi e venire incontro alle istanze della società e dell'Autorità politica nell'interesse di una collettività che beneficia sempre più dei vantaggi della globalizzazione ma che è sempre più esposta alle minacce che essa comporta."[2] .

3. FOCUS RIFORMA: le Innovazioni.

Le principali novità indotte dalla riforma sono relative:

- al coordinamento interno;
- al rafforzamento della figura del presidente del Consiglio dei Ministri, entrambi necessari per conferire organicità ad un sistema concepito in maniera divisionale a fortemente gerarchizzata;
- all'apertura al mondo esterno di tale realtà;
- alla creazione di partnership con università;
- alla cooperazione internazionale.

In primo luogo, il ripensarsi in una logica "di sistema", declinata nel segno del coordinamento interno, ha comportato il mantenimento del modello binario, eleggendo unità e unitarietà come pilastri fondamentali del sistema.

Il coordinamento realizzatosi con tale riforma ricomprende l'accesso delle Agenzie agli strumenti giuridici/operativi, la ricerca e lo scambio informativo nonché la collaborazione con gli enti esterni al Comparto. La funzione è svolta anche mediante la creazione di meccanismi e tavoli dedicati, attraverso un modo di operare che ha ormai assunto la valenza di *Grundnorm c*ondivisa e che, adeguandosi in modo dinamico al mutare del quadro della minaccia, continua a evolversi, dando vita a configurazioni nuove dei perimetri d'impiego e ad un *fine tuning* costante di compiti e processi, nel segno dell'ottimizzazione e della sinergia.

Altro obiettivo della riforma era quello di rafforzare l'interazione con il decisore politico. La proficua interlocuzione tra intelligence e Autorità di governo ha trovato nel tempo snodo efficace nel cd. "CISR tecnico", istituito nel 2012 e composto dai Direttori degli Organismi informativi e da dirigenti di vertice dei Ministeri rappresentati in Comitato. Inoltre, sono state intensificate anche le

[2] Cit. Relazione Parlamentare 2017.

occasioni di interazione e confronto con le articolazioni operative di Forze Armate e di polizia.

Di rilievo, resta infine il rapporto stabilito con il Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR), la cui funzione di controllo democratico sulla conformità alla Costituzione e alle leggi dell'attività del Sistema di informazione è garanzia degli equilibri tra Parlamento ed Esecutivo, da cui l'intelligence dipende, nonché della correttezza del suo operato.

Altro obiettivo della riforma è stato quello di consentire e favorire in un'ottica di trasparenza, una apertura alla società civile Tale apertura è duplice: da un lato si osserva come il mondo dell'intelligence, da sempre caratterizzato dal velo della segretezza, abbia aperto le porte al cittadino proprio per sensibilizzarlo nei confronti delle nuove minacce insite nella quotidianità di tutti (vedi ad esempio la pubblicità progresso: *Be aware. Be digital*); dall'altro lato si osserva come tale apertura sia rivolta all'instaurazione di partnership con università ed enti privati, ed al reclutamento di personale proveniente non più solo dalle Forze Armate. La società civile, quindi, non è più vista come mero fruitore e beneficiario di sicurezza fornita ab externo, ma è anch'essa chiamata a fare la sua parte all'interno di un "ecosistema" nazionale.

Infine, ultimo aspetto è quello della collaborazione internazionale tra le varie agenzie mondiali di intelligence. L'approccio collaborativo tra le stesse risulta fondamentale per la gestione delle minacce di portata internazionale.

I rapporti con le Agenzie estere hanno quindi conosciuto sviluppi senza precedenti, per quantità e modalità, facendosi più intensi ed articolati, soprattutto per quanto riguarda la condivisione di dati utili a scongiurare minacce trasversali, terrorismo in primis. Sono altresì aumentate, le occasioni di interazione multilaterali e multisettoriali, prima veramente rarissime per il mondo dei Servizi.

Tale assetto organizzativo e socioeconomico rende opportuno anche il miglioramento e l'aggiornamento delle risorse umane e tecnologiche, la cui virtuosa sinergia rappresenta il vero *atout* di qualsiasi apparato informativo, rimandando ai versanti che costituiscono il fulcro dell'attività intelligence: ricerca e analisi.

La nebulosa di nuove tecnologie, digitali e non, caratterizzata non solo da un'impressionante velocità, ma anche da una elevata accessibilità alle stesse, si fonde in nuovi sistemi e rapidamente è in grado di entrare nella vita quotidiana, scalzando i preesistenti.

Siamo ormai abituati agli annunci di imminenti rivoluzioni tecnologiche tanto che ci limitiamo a subirne le conseguenze e ad adattarci alla novità. Tuttavia, questo approccio da "utente", è

completamente opposto a quello che invece sono obbligati ad avere gli operatori della sicurezza, ai quali, invece, non è permesso abbassare la guardia nel vortice di innovazioni tecnologiche tutte potenzialmente capaci di impattare sulla sicurezza di una società che fa del rinnovamento tecnologico ormai un "equilibrio dinamico".

Essendo tale rivoluzione caratterizzata dalla grande accessibilità alle tecnologie, aumentano anche i rischi legati a un loro utilizzo malevolo, rendendole mezzi per potenziali attacchi alla sicurezza e alla privacy dei vari utenti.

La natura delle minacce dell'era 2.0 non solo ha bisogno di un differente sistema di gestione e prevenzione delle stesse, che è quello delineato dalla riforma del 2007; ma necessita anche di nuove figure professionali e competenze tecniche e multidisciplinari per affrontarle.

In tale ambito ha un ruolo rilevante la collaborazione con le università italiane, che si configurano come centri di eccellenza e di conoscenze multidisciplinari. L'intelligence negli ultimi anni ha organizzato diversi *road show* all'interno dei principali Atenei, durante i quali gli studenti hanno potuto esprimere le proprie opinioni in merito alle tematiche.

Le università rappresentano il partner perfetto per il sistema di intelligence in quanto esse godono sia di conoscenze tecniche costantemente aggiornate, sia di conoscenze multidisciplinari, che risultano funzionali per la gestione di minacce sempre più globali quali quelle odierne.

Alcuni Atenei stanno inserendo nella loro offerta formativa master e percorsi di studio specifici relativi al ramo dell'intelligence. In particolare le aree che in vista degli sviluppi futuri delle dinamiche mondiali potrebbero riscuotere più interesse sono quelle relative all'intelligenza artificiale, in stretta correlazione con l'esigenza di gestire e analizzare un considerevole numero di dati; assumerà, dunque, un rilievo crescente anche la figura del data scientist, che rappresenta in un certo senso una sintesi della formazione multidisciplinare richiesta agli esperti di intelligence.

Da tali considerazioni emerge come la figura di agente dell'intelligence richiesta sia notevolmente cambiata: innanzitutto, non si tende solo a reclutare personale dalle Forze Armate, ma come appena detto si cercano esperti anche nel mondo dell'Università, ciò vuol dire che tra gli 007 del 2018 potremmo ritrovare un James Bond, ma benissimo anche un hacker informatico, oppure un professore di sociologia.

Le competenze più innovative richieste al momento sono quelle legate al mondo tecnologico, e in particolare al cyber dato che al giorno d'oggi anche le principali minacce si servono anche di questi

mezzi assumendo configurazioni del tutto nuove, tuttavia considerata la portata globale e le nuove vesti delle tradizionali minacce il settore tende a reclutare anche esperti in materie economico-sociale nonché legale e finanziario.

Inoltre, è da sottolineare il fatto che anche le modalità di reclutamento all'interno del sistema sono decisamente cambiate: basti pensare che oggi è possibile inviare la propria candidatura al sito https://www.sicurezzanazionale.gov.it/sisr.nsf/lavora-con-noi.html, mentre in passato per tali incarichi, non ci si proponeva, si veniva scelti.

CAPITOLO 2

IL BUSINESS DELL'INTELLIGENCE

1. SCENARIO: LA CRESCITA DEL SETTORE

Al giorno d'oggi è possibile parlare di un vero e proprio business dell'intelligence, in quanto le attività rientranti in quest'area non sono più strettamente legate all'ambito di sicurezza nazionale.
Dalla definizione di intelligence, presente nel Glossario pubblicato dalla Rivista Gnosis, emerge come tale termine non sia solo utilizzato per identificare il "prodotto dell'elaborazione di una o più notizie di interesse per la sicurezza nazionale", ma che come esso sia largamente "impiegato anche con valenza generica spesso accompagnato da aggettivi intesi a specificarne: finalità (strategica, tattica, operativa), natura (situazionale o previsionale), fonte di provenienza o materia cui si riferisce (economico-finanziaria, militare, etc.), volti ad evidenziarne la vastità delle aree in cui tale attività è richiesta.
Attingendo, invece, ad una definizione più generica del Dizionario Treccani, è possibile definire il termine come "servizio di raccolta e analisi delle informazioni". L'intelligence risulta perciò, un'attività che può benissimo configurarsi come una prerogativa non necessariamente statale, le cui attività possono essere volte anche alla tutela dell'interesse del privato.
In particolar modo, oggi in seguito al mutato contesto macroeconomico, analizzato nel capitolo precedente, alle nuove configurazioni di vecchie minacce e alla nascita di nuove, si assiste ad una notevole crescita della domanda di questi servizi da parte di imprese e singoli cittadini.

Osservando i dati forniti dall'Osservatorio Nazionale Investigazioni del 2015 emerge come dal 2007 (anno di riforma del sistema di informazione per la sicurezza nazionale) il numero di agenzie investigative in Italia sia generalmente aumentato. (In Italia non possiamo ancora parlare di agenzie di intelligence per questioni normative, perciò facciamo riferimento a quelle agenzie investigative che tuttavia adottando un approccio "corporate", si avvicinano a quella che nel resto del mondo è definita come una "private intelligence company").

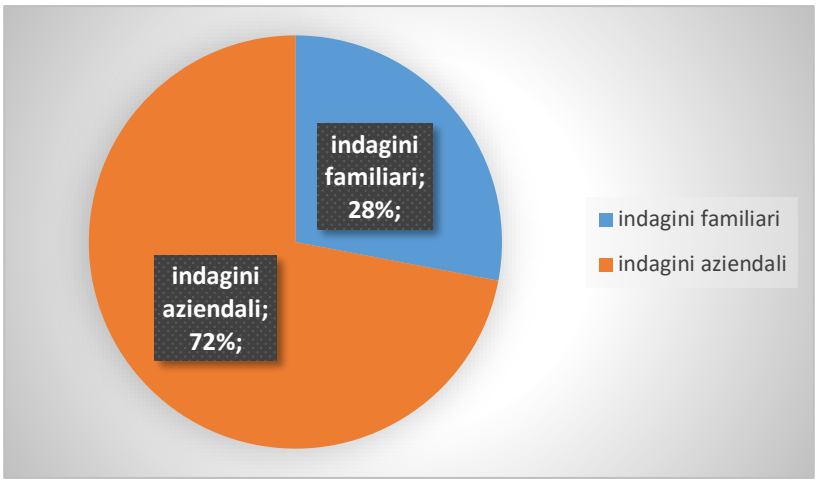
Figura 6 Dati: rappresentazione dell'incremento del numero di strutture di intelligence privata dal 2007 al 2010 in Italia.

REGIONE	NUMERO STRUTTURE NEL 2010	INCREMENTO 2007 > 2010
Lombardia	512	+9,87%
Campania	393	+23,58%
Lazio	310	+67,57%
Sicilia	250	+3,73%
Puglia	248	-1,98%
Piemonte	195	+1,04%
Emilia Romagna	195	-0,51%
Toscana	185	-1,07%
Veneto	171	-3,39%
Calabria	105	+2,94%
Abruzzo	103	+4,04%
Liguria	93	+3,33%
Sardegna	73	-9,88%
Marche	61	-1,61%
Umbria	53	+6,00%
Friuli	51	-3,77%
Trentino Alto Adige	32	+28,00%
Basilicata	32	+3,23%
Molise	22	+10,00%
Valle D'Aosta	5	-28,57%

Generalizzando i dati relativi ad alcune delle principali agenzie investigative italiane (come Axerta[3]), nell'ottica di fornire un'ampia visione, è possibile osservare come la maggior parte dei casi affidati a queste agenzie sia un incarico a livello industriale, e solo una parte residuale dei casi riguardi invece il livello familiare.

[3] AXERTA: Azienda leader in Italia nell'investigazione aziendale.

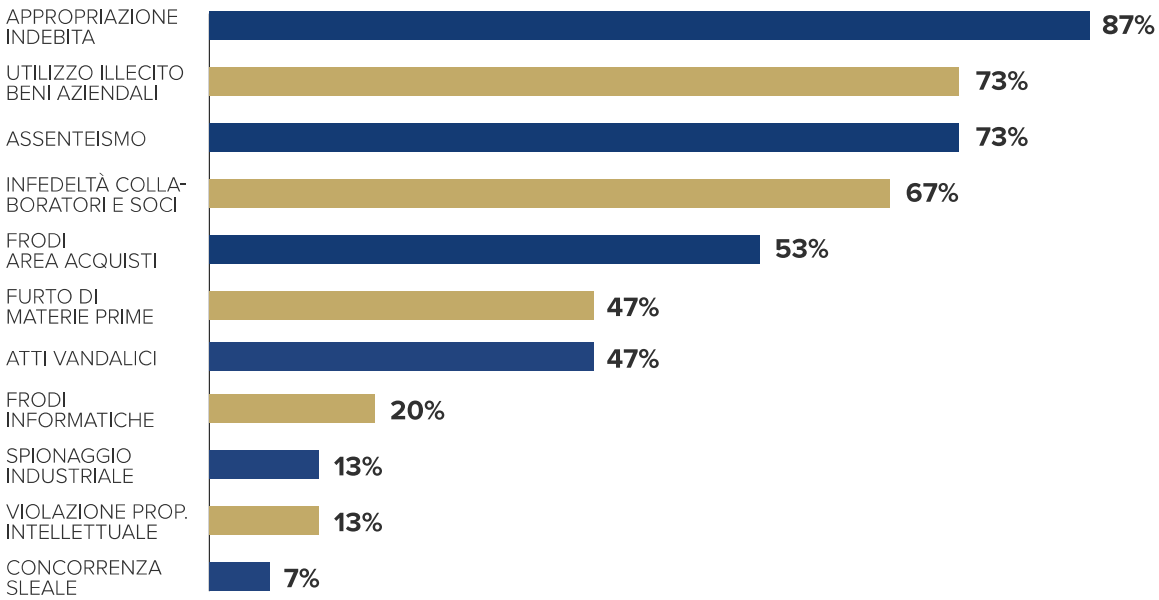
Figura 7 Tipologie di indagini effettuate da tali agenzie.



Da uno studio fatto in collaborazione con AIPSA[4] emerge che il fenomeno delle frodi aziendali, nel periodo 2013/2015, è fortemente presente nelle organizzazioni italiane. In particolare il 41% degli intervistati ha dichiarato che la propria azienda è stata vittima di frode.

L'incidenza media annua registra 10 fenomeni fraudolenti per azienda.

Ecco invece il peso percentuale di ciascuna tipologia di frode subita tra quelle dichiarate dagli intervistati.



[4] **AIPSA**: Associazione italiana professionisti security aziendale

2. I SERVIZI OFFERTI

I servizi richiesti alle agenzie sono perciò quelli principalmente legati a queste tipologie di frodi. Si osserva come l'agenzia debba configurarsi non solo attraverso un intervento attivo, svolgendo un'analisi accurata e tempestiva del caso volta a scovare i vari casi di frode; ma ad essa possa essere richiesto anche un intervento "passivo" volto cioè alla prevenzione di eventuali attacchi.
Il ruolo dell'agenzia di intelligence si concretizza nella predisposizione di contromisure per contrastare i possibili attacchi e per porre rimedio a quelli effettivi, ma anche nella predisposizione di prospetti informativi che possono essere rilevanti per l'individuazione di buone opportunità per l'azienda.

Per contromisure si intende l'insieme di azioni che concorrono, attivamente o passivamente, a:

- minimizzare la probabilità che gli eventi indesiderati accadano (azione preventiva);
- rilevare il fatto che siano accaduti (azione investigativa, ruolo attivo dell'agenzia);
- individuare e minimizzare le conseguenze (ruolo attivo dell'agenzia);
- ripristinare il corretto funzionamento del sistema.

Una prima possibilità di classificare le contromisure consiste nell'osservarle in funzione degli eventi indesiderati che vanno a contrastare, affiancando a ciascun evento indesiderato quelle applicabili. Vi sono, pertanto:

- contromisure preventive: finalizzate a minimizzare la probabilità che un evento indesiderato accada. Sono principalmente legate al settore della cyber security mediante la predisposizione di sistemi di sicurezza volti a fornire una protezione da attacchi esterni, ma anche una garanzia in caso di perdita involontaria di dati aziendali da parte di dipendenti. Altri campi in cui vi è una contromisura di natura preventiva possono individuarsi nei servizi di Due Diligence, ovvero all'attività di analisi delle informazioni oggetto di una trattativa volta a determinare una corretta valutazione del rischio e dei problemi connessi al contratto in corso di trattativa, affinché si possa ottenere un equo trattamento.

– contromisure correttive: tese a riparare i danni causati dal verificarsi eventi indesiderati che, nonostante le contromisure preventive. A tale ramo possono essere riconducibili non solo i servizi nell'area Itc, ma anche quelli legati al Litigation support.

– contromisure informatiche: basate sulla tecnologia informatica.

– contromisure organizzative: riconducibili all'organizzazione che utilizza il sistema informatico ed alle norme e regole di comportamento stabilite dal personale.

– contromisure operanti a livello fisico: proteggono i dispositivi (calcolatori, cavi, apparecchiature di rete, locali, impianti di alimentazione e condizionamento, ecc.) da attacchi di tipo fisico quali furto e danneggiamento.

– contromisure operanti a livello logico (come ad esempio i software anti-virus): proteggono risorse logiche (basi di dati, registri di configurazione, moduli software, ecc.) da attacchi di tipo logico.

Tuttavia, la recente configurazione delle società private di intelligence, non si limita a fornire solo servizi legati strettamente ad attacchi potenziali o effettivi, bensì tali strutture cercano di sfruttare complessivamente le potenzialità dell'attività di reperimento e analisi dei dati, offrendo anche servizi di corporate investigation volti ad identificare oltre a frodi e attacchi di vario genere, anche opportunità per il business aziendale.

Quindi, da un punto di vista attivo le intelligence company offrono:

- servizi investigativi volti al reperimento di dati sensibili sia per intraprendere contromisure, sia per raccogliere informazioni rilevanti per lo sfruttamento e l'identificazione di opportunità.
- Servizi di verifica del rispetto di clausole contrattuali (Royalty auditing [5], Rispetto patti di non concorrenza).
- Servizi di supporto legale in fusioni, acquisizioni e affari rischiosi per l'impresa.
- Servizi di supporto informatico (tracciamento di dati e identificazione fuga dati, attacchi cyber).

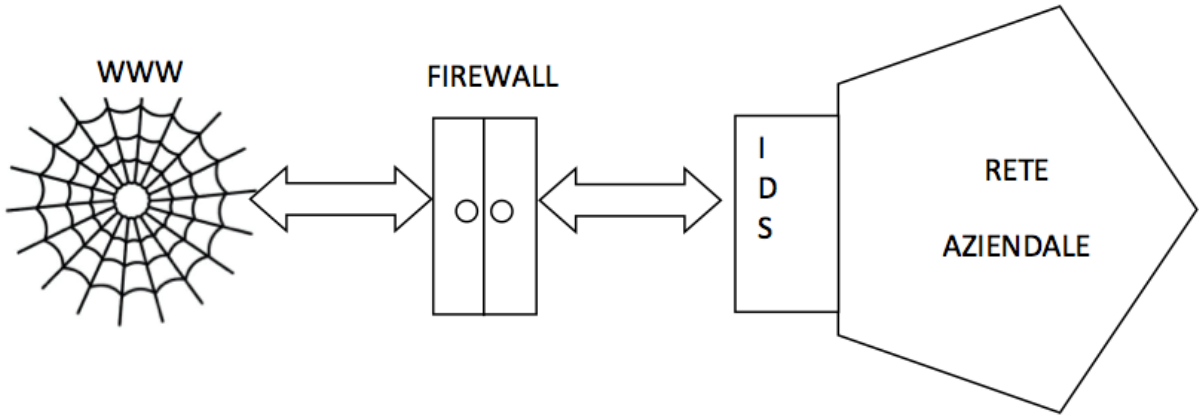
[5] Royalty Auditing: attività investigativa finalizzata a tutelare i proprietari di brevetti e di marchi da possibili frodi che vadano ad intaccare i proventi derivanti dallo sfruttamento di tali beni immateriali a fronte di contratti di licenza.

Da un punto di vista passivo invece, tali agenzie si configurano come fornitori di servizi volti alla prevenzione di eventuali attacchi e frodi, in tale ramo sono riconducibili i servizi di:

- Due Diligence[6]
- Supporto e consulenza legale
- Supporto informatico mediante l'implementazione e l'utilizzo di sistemi informatici "sicuri" di archiviazione e circolazione interna dei dati. Ad esempio, le aziende dovrebbero premunirsi di sistemi informatici in grado di scovare gli "intrusi" che sono all'interno di computer e reti di organizzazioni. Questi sistemi prendono il nome di Intrusion Detection Systems e hanno il compito di identificare, prevenire e reagire ad una entry non autorizzata e/o ad un'attività maliziosa. Hanno perciò l'obiettivo di classificare le attività in intrusive e non intrusive, e di bloccarne l'accesso alla rete aziendale e attraverso l'analisi dei vari casi storici del sistema accaduti sono in grado di apprendere dagli stessi. I sistemi di IDS, non vanno confusi con i firewalll, le due tecnologie sono infatti complementari, poiché i firewall si limitano a bloccare l'entrata dei file non autorizzati all'interno del circuito aziendale, filtrando dunque il pacchetto di informazioni prima del loro ingresso, mentre invece gli IDS si collocano in un secondo step di "scrematura" monitorando i pacchetti informativi interni all'azienda.[7]

[6] Due Diligence: un'attività fondamentale in caso di operazioni straordinarie che consiste nella raccolta di tutte le informazioni utili al fine di determinare punti di forza e di debolezza della società, anche al fine di arrivare ad una valutazione economica della stessa, e di una valutazione attendibile dei rischi connessi all'oggetto dell'accordo.
Attività fondamentale soprattutto in previsione di accordi di fusione, scissione e cessione di asset aziendali volta a ridurre al minimo la possibilità che una delle due controparti venga danneggiata da tale accordo.

[7] Riferimenti: *"Cyber security, intrusion detection systems e intelligenza artificiale*" di Caterina Patrizia Morano



3. MINACCE PER I SISTEMI INFORMATICI AZIENDALI.

Le minacce per l'azienda possono derivare da qualsiasi accesso non consentito e possono configurarsi come attacchi intenzionali o attacchi accidentali.

I primi, possono essere classificati in base alla risorsa (fisica o logica, umana) su cui si esplica per la prima volta la violazione. Per risorse fisiche si intendono elementi come dischi, periferiche, gruppi di continuità; mentre le risorse logiche sono i elementi architetturali come i Sistemi operativi, il sistema di posta, o file di configurazione e processi. Le risorse umane invece, in riferimento a dipendenti, dirigenti e personale in genere rappresentano una minaccia di questo tipo qualora violassero i vincoli sul tema dell'accordo contrattuale.

Le minacce di questa natura rappresentavano la fonte investigativa prevalente del secolo scorso, in cui come già sottolineato nel capitolo precedente il ruolo della spia si configurava in modo più pratico e diretto nel sito oggetto di indagine.

Tra gli attacchi a livello fisico e quelli i a livello logico vi è una sostanziale differenza anche in merito alle tecniche di attacco utilizzate.
Per quanto riguarda gli attacchi a livello fisico essi si configurano come:

- Furto (prevedibile per i nastri di backup, dischi o interi server) è un attacco alla disponibilità e alla riservatezza. Dove per disponibilità si intende la capacità del sistema di rendere disponibili

determinati dati esclusivamente a chi ne possiede i diritti d'accesso; e dove per riservatezza si fa riferimento alla protezione degli stessi da chi non ne ha i diritti.

- Danneggiamento (prevedibile per apparecchiature e cavi di rete) è un attacco alla disponibilità e all'integrità. Ove per integrità si fa riferimento alla capacità del sistema di impedire l'alterazione diretta e indiretta dei dati, sia da parte di soggetti non autorizzati che a seguito di eventi accidentali (ad esempio anche la perdita dati è considerata una alterazione).

Gli attacchi a livello logico invece sono tesi a sottrarre informazioni o a degradare l'operatività del sistema agendo sugli strati architetturali e configurandosi come:

- Attacco alla riservatezza: se si accede senza modificare, dunque per finalità di intercettazione e deduzione.
- Attacco all'integrità e alla riservatezza: se si accede e si modificano i dati, mettendo in atto una vera e propria intrusione.
- Attacco alla disponibilità, ovvero volto essenzialmente a degradare l'operatività del sistema (disturbo).

TECNICHE DI ATTACCO

È possibile classificare le tecniche d'attacco in base alla finalità dello stesso, individuando:

- Tecniche di intercettazione;
- Tecniche di deduzione;
- Tecniche di disturbo;
- Tecniche di intrusione.

Le tecniche di intercettazione possono richiedere un attacco preventivo a livello fisico per installare dispositivi pirata o per allacciarsi alla rete. Si basano dunque su analizzatori di traffico (LAN,WAN), server pirata che si spacciano come router, programmi che emulano i servizi del sistema (come ad

esempio il login).

Le tecniche di deduzione, invece, consistono nel monitoraggio incrociato di dati ottenuti mediante l'analisi del monitoraggio del sistema congiunta ad informazioni ottenute per altre vie.

Infine, le tecniche di intrusione, consistono nell'accesso mediante password altrui ottenuta con preventivo attacco di intercettazione, o mediante lo sfruttamento di protocolli di rete, dove ad esempio si possono generare pacchetti IP falsificati (tecniche IP-spoofing; Source-routing); o ancora tramite l'installazione di una Blackdoor. Tale procedura permette, una volta ottenuti i diritti di amministratore (anche temporaneamente), di installare nel sistema un meccanismo in grado di consentire l'accesso privilegiato anche in seguito. Si tratta di un attacco insidioso in quanto la backdoor, finché non viene individuata e rimossa, continua a garantire l'accesso all'intruso anche se il primo accesso illegale viene scoperto e la password di admin è cambiata.

Le tecniche di disturbo, sono volte a degradare l'operatività del sistema e sono considerabili come atti di sabotaggio. Gli esempi più comuni di tali procedure sono i virus, gli Worms e di Denial of service (la negazione del servizio).

I Virus sono programmi auto-replicanti, spesso inseriti nel sistema come cavalli di troia, generalmente pericolosi per la integrità del file- system e per la disponibilità dei servizi.

I Worms, invece, sono software particolari che si limitano a degradare le prestazioni del sistema ad esempio lanciando molte immagini dello stesso processo, portano cosi ad un netto rallentamento del sistema, in grado di rendere lo stesso di fatto inutilizzabile (violazione del requisito di disponibilità).

Per Denial of service si fa riferimento all'insieme di tecniche tese a far sì che il sistema neghi l'accesso anche ad utenti autorizzati, minacciando così i requisiti di disponibilità del sistema.

Riassumendo, tali tecniche sono volte alla violazione dei requisiti di disponibilità, integrità, autenticità e riservatezza, che rappresentano gli elementi base della sicurezza informatica del sistema aziendale.

4. FOCUS: *"ENISA, il cyber spionaggio nel 2018 crescerà ancora"*[8]

Il cyber spionaggio crescerà ancora nel 2018. Lo farà a seguito di motivi geopolitici, di sanzioni economici e di obiettivi strategici nazionali. Lo ha rilevato l'Agenzia UE per la Network e l'Information Security (ENISA) nel suo rapporto sul panorama delle minacce informatiche nel 2017 (Threat Landscape Report 2017).

Il rapporto dell'agenzia[9], in particolare, riconduce il 20% della responsabilità dei cyber attack del 2017 alle Nazioni stesse. Il loro obiettivo è rubare proprietà intellettuale e segreti di stato, perciò in tale contesto gli hacker non solo programmano l'attacco al bersaglio specifico, ma delineano anche strategie in grado di sviare le indagini mediante la tecnica del "*denial and deception".*[10]

Le principali minacce odierne derivano dagli Advanced Persistent Threat (APT).

Il NIST definisce un'Advanced Persistent Threat (Minaccia Avanzata e Persistente) come:

Un avversario che possiede sofisticati livelli di competenza e una quantità significativa di risorse che gli permettono di creare le opportunità di raggiungere i propri obiettivi utilizzando molteplici vettori di attacco (ad esempio di tipo software, di tipo fisico o tramite l'uso dell'inganno). Questi obiettivi includono tipicamente stabilire ed estendere la propria presenza all'interno dell'infrastruttura tecnologica delle organizzazioni "bersaglio" allo scopo di "esfiltrare" informazioni, indebolire o impedire aspetti critici di una missione, di un programma o dell'organizzazione stessa; ovvero insinuarsi all'interno dell'infrastruttura per portare a termine i propri obiettivi in futuro.

L'ENISA ha classificato i principali APT, evidenziando come questi siano strettamente legati alle Nazioni, e come le loro azioni siano finalizzate non solo allo spionaggio industriale, ma anche a quello statale.

---

[8] ENISA: Agenzia europea per la sicurezza delle reti e dell'informazione
[9] ENISA: Threat Landscape 2017.
[10] *Una Joint Publication del Joint Chiefs of Staff del 1996, riveduta e ripubblicata nel luglio 2006, definisce la Military Deception (MILDEC) come "l'insieme di azioni messe in atto per ingannare (mislead) deliberatamente i decisori avversari riguardo alle proprie capacità, intenzioni e operazioni, in modo da indurre l'avversario ad intraprendere determinate azioni (o non-azioni) che daranno un contributo alla riuscita della propria missione.*

Ad esempio, gli APT responsabili di azioni di spionaggio a livello aziendale sono :l'APT33 che ha effettuato nel 2017 azioni di spionaggio informatico contro aziende dei settori militare, petrolchimico, aeronautico civile negli Usa, Medio Oriente e Asia; E l'APT32, (gruppo di hacker del sud est asiatico) accusato di azioni contro compagnie multinazionali operanti in Vietnam, e di una campagna di cyber spionaggio anche contro due sussidiarie locali di aziende statunitensi e filippine nel mercato dei beni di consumo. A seguire, APT 28, una formazione di hacker di stato russi che lo scorso luglio ha lanciato una campagna contro diverse imprese nel settore ospedaliero e alberghiero in almeno sette paesi europei e uno mediorientale.

Mentre, invece, sono responsabili di attacchi contro entità statali l'APT29, e l'APT17. L'APT29 si ritiene sia associato con l'intelligence di Mosca e che abbia lanciato nel 2017 attacchi contro i ministeri degli Esteri e della Difesa ed il Partito dei Lavoratori in Norvegia e in Olanda. L' APT17, è invece, una formazione legata alla Cina che ha condotto intrusioni cibernetiche nei network di entità governative, industrie della difesa, studi legali, imprese legate all'IT, compagnie minerarie e organizzazioni non governative (ONG). Sembra, ma non ci sono conferme, che anche l'aggressione con CCCleaner sia attribuibile ad questi ultimi.

In seguito, una classificazione dei mezzi potenziali da cui tali attacchi potrebbero nascere, con evidenza dell'incremento della rischiosità da essi derivante dal 2016 al 2017.

enisa

ENISA Threat Landscape Report 2017
ETL 2017 | 1.0 | HSA | January 2018

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2017 with the one of 2016.

Il malware, ad esempio, è il sistema che è stato utilizzato sia per attacchi nei confronti di imprese che per attacchi di spionaggio a vertici politici di vari Paesi.

Con il termine malware si fa riferimento ai programmi realizzati per danneggiare i sistemi su cui vengono eseguiti o per sottrarre informazioni sensibili. Esistono varie tipologie di malware (ad esempio: virus, trojan, worm), le cui differenze sono legate essenzialmente alla capacità di autoreplicarsi e alle finalità per cui sono programmati; tuttavia, il modello strutturale da esse posseduto è lo stesso, ed è composto dalle seguenti fasi :

1. Infezione: consiste nell'introduzione del malware nel sistema e nella modifica delle impostazioni dello stesso adattandole alle proprie esigenze.
2. Quiescenza. Il codice virale rimane residente in memoria in attesa che si realizzi una determinata condizione di attivazione.
3. Replicazione e propagazione (solo per virus e worm). Al determinarsi di certi eventi o condizioni, il malware si replica e seleziona i bersagli verso cui propagarsi, infettando altri sistemi.
4. Azioni malevole. Al verificarsi di certi eventi o condizioni, il codice virale esegue i propri compiti malevoli, come distruzione o furto dei dati del sistema. Se il sistema non viene compromesso definitivamente, il software ritorna nella fase di quiescenza.

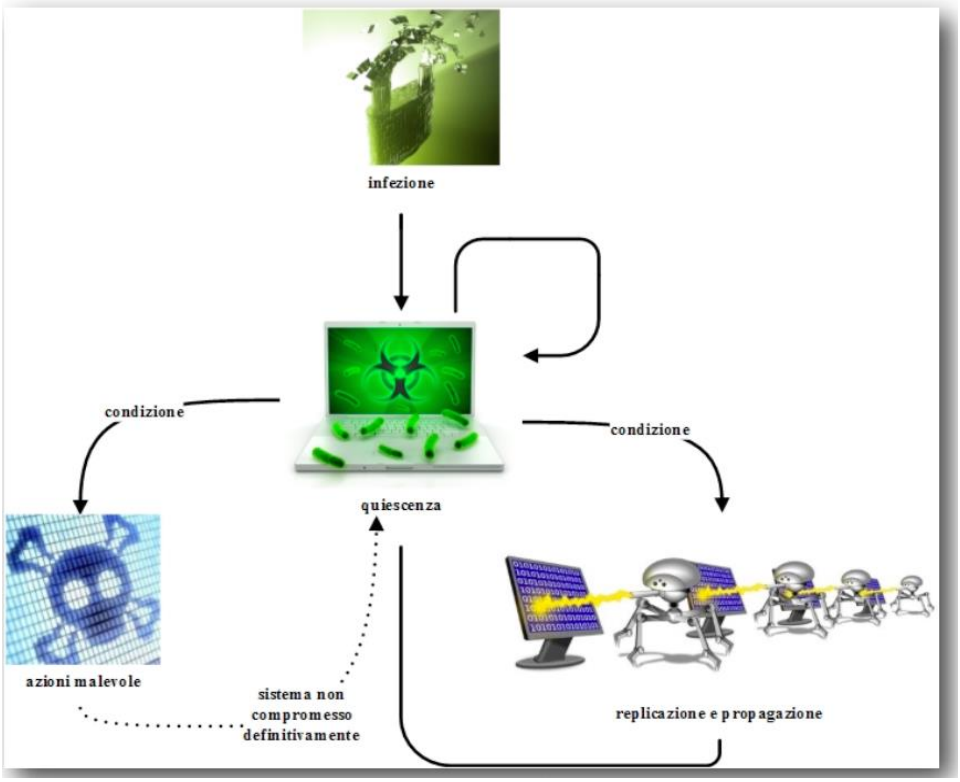


Figura 8 Struttura di funzionamento del Malware.

Relativamente agli attacchi di spionaggio industriale, un caso abbastanza recente è quello del malware

che ha infettato alcune versioni del software CCcleaner.
CCcleaner è un software di ottimizzazione del sistema operativo dei Pc, su cui sono disponibili più versioni, una gratuita ed una a pagamento rivolta a un pubblico professionale. La versione a pagamento è utilizzata anche da alcuni colossi del mondo informatico (Samsung, Microsoft, Sony).
L'attacco è stato concepito principalmente per raggiungere i server di queste aziende e sottrarre dati sensibili, tuttavia, per non destare sospetti è stato il malware è stato lanciato anche su altre versioni del software (come quelle gratuite), in questi casi, però, il payload (cioè il codice dannoso che i pirati puntano ad installare) non si era poi attivato.
Si è osservato che tale fase dannosa era stata avviata su una ventina di computer tra cui quelli di aziende che operano nel mondo dell'informatica: Microsoft, Samsung, VMware, MSI, Sony, D-Link e Cisco.
Dai risultati delle indagini emerge che il malware utilizza il fuso orario cinese per determinare alcune operazioni e che gli analisti di Kaspersky avrebbero individuato alcune analogie tra il codice usato nell'attacco con quello usato in passato dal Group 72, che in passato qualcuno aveva ipotizzato essere collegato in qualche modo alla Cina.

Un caso di utilizzo di malware per sottrarre informazioni nel contesto politico italiano ad esempio, è quello invece che ha portato, il 10 gennaio del 2017 a Roma, all'arresto dell' ingegnere nucleare Giulio Occhionero e di sua sorella, con l'accusa di far parte di una centrale di cyberspionaggio che per anni ha raccolto notizie riservate e dati sensibili violando gli account di posta elettronica di 18.237 persone, inclusi quelli dell'ex premier Matteo Renzi e del governatore della Bce Mario Draghi.
Gli autori degli attacchi sono riusciti a entrare negli account di politici, banchieri, militari e rappresentanti delle istituzioni italiane grazie ad un malware chiamato Eye Pyramid. Risultano hackerati, anche:@bancaditalia.it, @esteri.it, @pdl.it, @unibocconi.it, @tesoro.it, @gdf.it e @partitodemocratico.it.

La versatilità di tali malware, rende le tecnologie un'arma a doppio taglio: uno strumento di notevole utilità, ormai fondamentale nella vita quotidiana; ma allo stesso tempo un mezzo in grado di colpire silenziosamente.

È per questo che gli Stati Uniti d'America, nutrendo sospetti nei confronti della società cinese Huawei, hanno vietato l'utilizzo per i propri funzionari Governativi di apparecchiature di tale azienda.

"Siamo profondamente preoccupati circa il rischio che qualsiasi compagnia o entità legata a governi stranieri che non condividono i nostri valori possa guadagnare posizioni di potere all'interno della nostra rete di telecomunicazioni", ha detto il direttore dell'Fbi , Chris Wray. "Tale posizione permette

di esercitare pressione o controllo sulla nostra infrastruttura e offre la possibilità di condurre campagne di spionaggio non rilevabili".

5. STRUTTURA E FIGURE PROFESSIONALI

L'erogazione di una così vasta gamma di servizi permette di sfruttare a pieno le potenzialità insite nell'attività di intelligence, tuttavia richiede anche conoscenze e competenze multidisciplinari, è perciò che il profilo di un agente richiederà competenze trasversali e allo stesso tempo specifiche in una determinata materia.

Queste agenzie infatti si sviluppano intorno a diverse figure professionali (variano in base ai servizi offerti, in questo ambito prendiamo in considerazione l'agenzia investigativa -in Italia- nell'accezione di agenzia di intelligence):

- Investigatori;
- Esperti Avvocati e Giuristi;
- Consulenti Scientifici;
- Specialisti in Digital Forensics;
- Esperti Finanziari.

L'Investigatore risulta la figura chiave del core business della società di intelligence, infatti affinché vi sia l'analisi e lo sfruttamento nei vari servizi offerti, è necessaria l'attività investigativa per il reperimento dei dati rilevanti.

Per tale attività è necessario poter contare sull'operato di professionisti, essendo l'attività di raccolta prove e dati estremamente delicata, deve essere svolta con perizia e nel rispetto dei limiti normativi, altrimenti si rischia di compromettere la validità delle prove e dell'intero processo investigativo. Le prove raccolte nel non rispetto della procedura e dei limiti normativi rischiano di non essere ammesse in giudizio come atti probatori. L'investigatore dunque oltre a dover essere abile nel reperimento del materiale richiesto deve essere anche in grado di comparire in giudizio e di saper destreggiare tra i limiti normativi.

L'investigatore può operare servendosi di tecnologie avanzate, ma anche dell'aiuto di altri membri

dell'agenzia a cui può richiedere consulenza in vari ambiti, può infatti sfruttare le conoscenze di un ingegnere informatico per poter meglio comprendere il funzionamento di sistemi informatici di interesse per l'indagine.

Le figure di avvocati e giuristi sono fondamentali nella fase di definizione della strategia investigativa e nell'analisi delle prove, nella stesura dei dossier. Tuttavia, tali figure assumono anche un ruolo di consulenza soprattutto nelle agenzie che offrono servizi di litigation support.

Altra figura imprescindibile al giorno d'oggi è quella dello Specialista in Digital forensics, una figura che possiede esperienza e competenza nell'individuazione di prove in ogni tipologia di apparato digitale.

Inoltre, altre figure richieste in tale team sono quelle dei consulenti scientifici, in quanto le aree di indagine sono caratterizzate da una crescente multidisciplinarietà e interconnessione. La consulenza fornita da tali figure risulta rilevante per la gestione tempestiva di situazioni critiche durante le indagini e per la stesura di una strategia investigativa che tenga conto delle caratteristiche specifiche di più ambiti.

L'esperto finanziario, ha un ruolo apicale soprattutto nell'individuazione di casi di frode, nell'analisi quantitativa di dati aziendali, e nella stima di fattori di rischio relativi ad accordi in grado di alterare dinamiche aziendali e societarie. Tuttavia, la sua rilevanza all'interno dell'agenzia dipende essenzialmente dall'offerta di servizi in cui quest'ultima è specializzata.

Come emerge dall'integrazione tra le varie figure professionali necessarie, il lavoro all'interno di queste agenzie è orientato ad un'ottica di organicità, flessibilità e interconnessione. Talvolta vi è la formazione di team multifunzionali per la risoluzione di casi più complessi, in cui viene coniugata l'offerta dei vari servizi dell'agenzia.

Le elevate competenze tecniche richieste ai funzionari di queste agenzie evidenziano l'importanza della formazione universitaria degli agenti, per cui sono richieste conoscenze tecniche e pratiche elevate, che difficilmente possono essere frutto della mera esperienza sul campo.

Il cambiamento della conformazione di servizi offerti da queste agenzie di intelligence private, comporta la richiesta di figure professionali dotate di titoli e altamente qualificate; mentre nella classica configurazione di società investigativa era sufficiente il possesso di una licenza per esercitare attività investigativa da parte del titolare.

Si osserva quindi che anche nel reparto del privato, oltre che come si è già analizzato prima nel

pubblico, la principale fonte di reclutamento è rappresentata dagli Atenei Universitari, in cui sono stati istituiti anche corsi di laurea in business intelligence e security intelligence.

Tuttavia, resta da evidenziare che nel settore pubblico nonostante si ricerchino figure già esperte e altamente qualificate, è stata istituita anche un'apposita scuola di Formazione per agenti segreti; nel privato invece si tende a ricercare personale già in possesso di determinate abilità, acquisite mediante esperienze pregresse.

Nelle agenzie di intelligence private più note, il team è composto principalmente da ex agenti segreti, ex militari, che dunque oltre a possedere conoscenze teoriche in materie variegate, possiedono anche abilità pratiche acquisite proprio durante gli anni di dipendenza dal pubblico.

Osserviamo ora come la struttura organizzativa e l'offerta dei servizi appena analizzata si configura concretamente in una società di intelligence privata che da un po' di anni fa parlare di sé: Black Cube.

CAPITOLO 3

SECURITY COMPANIES

1. DIFFERENZE TRA INTELLIGENCE PRIVATA E INTELLIGENCE PUBBLICA

Il settore dell'intelligence privata è un business che da molti anni in USA e in altri Potenze mondiali affianca il settore di intelligence pubblica, fornendole servizi complementari o addirittura coprendo aree tipicamente di competenza pubblica mediante il processo di privatizzazione ed esternalizzazione della Difesa in corso in questi Paesi.
La differenza principale tra intelligence pubblica e intelligence privata è da ricercare negli interessi che tali attività tutelano: la prima tutela gli interessi vitali nazionali, la seconda tutela gli interessi privati.
Per interessi vitali nazionali si intende: integrità territoriale, sicurezza del cittadino (in patria e all'estero), benessere economico e sociale, e infrastrutture critiche; tali interessi sono vitali perché non sono negoziabili. Mentre, gli interessi privati sono quelli strettamente riconducibili all'impresa e ai suoi interessi. Potrebbe succedere che queste due tipologie di interessi divergano, in tal caso è compito del Governo riportare l'azienda sulla retta via, sottolineando che la difesa nazionale, e quindi gli interessi vitali nazionali, non sono negoziabili. Inoltre, qualora nell'esercizio dell'attività di intelligence privata si venisse a conoscenza di informazioni istituzionalmente rilevanti, la società è tenuta a comunicarle all'ente Statale, evidenziando così il ruolo prioritario della comunicazione tra le due aree.

Come già accennato questo settore all'estero è in forte crescita, in Italia invece non essendo esplicitamente regolamentato trova varie barriere di carattere legislativo e si configura principalmente come attività di investigazione privata svolta da Procuratori o da Studi legali internazionali, o come aree aziendali create ad hoc all'interno delle grandi aziende.

Secondo alcuni esperti di diritto, infatti, non esiste un quadro normativo preciso, esaustivo e ben strutturato al quale l'intelligence privata italiana possa far riferimento. Per esempio nel TULPS, Testo Unico di legge per la Sicurezza Pubblica, non c'è una sezione dedicata esclusivamente all'attività di ricerca e analisi informativa di carattere privato. Il Testo si riferisce alle investigazioni di carattere privato solamente in concomitanza con le attività di vigilanza privata.

Questa mancata organizzazione normativa, oltre a rischiare di alimentare le già esistenti confusioni in materia di sicurezza, rischia di compromettere, o comunque di limitare, l'operato e la potenziale evoluzione dell'intelligence privata italiana. E' un settore che, ad oggi, non sembra reggere il confronto se paragonato a quello presente in Paesi come gli Stati Uniti e l'Inghilterra, che godono al contrario di un settore di intelligence privata avviato e maturo.

In merito a ciò si apre però il dibattito inerente la privatizzazione della sicurezza: facendo riferimento ai principi costituzionali per cui è un dovere dello Stato quello di garantire la sicurezza dei suoi cittadini, risulterebbe incostituzionale la privatizzazione di tale settore (fenomeno che è ampiamente diffuso in altri Stati). Si ritiene però possibile una collaborazione tra Stato e privati, mediante un comprehensive approach che vede il privato come un contractor[11] in determinati ambiti (come è avvenuto per le Maritime Security Companies), contratti del genere sono concessi in virtù di direttive e leggi ad hoc.

In particolare un passo in tale direzione è stato fatto nell'ambito della cyber security, in cui gli organi statali non avendo competenze adeguate hanno avviato una partnership con privati ed università. Tale collaborazione è alla base del sistema volto a tutelare i cittadini dalla minaccia cyber.

2. PRIVATE SECTORS MERCENARY FIRMS

I contratti effettuati dallo Stato con compagnie private per servizi legati al settore della sicurezza vengono associati all'antico fenomeno del mercenariato. Con il termine mercenario ci si riferisce al soldato che si offre di combattere per chiunque gli offra un compenso senza seguire ideali patriottici ed etici.

[11] contractor: persona che lavora a contratto per agenzie che ricevono incarichi da grandi aziende o anche da governi. (definizione da Dizionario Garzanti)

Tuttavia, oggi, l'impiego di *contractor* per la partecipazione ad operazioni di carattere offensivo riguarda una minoranza di agenzie al mondo (tra queste una delle più note è Blackwater USA, ingaggiata dal governo americano in Iraq ed Afghanistan) perciò è necessario classificare bene queste agenzie, evidenziando il fatto che i servizi da loro offerti non sono esclusivamente legati al combattimento armato, come l'associazione con il mercenariato lascia intendere.

Doug Brooks, presidente e fondatore dell'International Stability Operations Association (ISOA)[23]definisce tali servizi *Military Service Providers* (MSPs), che vengono a loro volta suddivisi in: *Nonlethal Service Providers* (NSPs), *Private Security Companies* (PSCs) e le *Private Military Companies* (PMCs).

Tabella 2. Military Service Providers

Military Service Providers (MSPs)		
NSPs Nonlethal Service Providers	**PSCs** Private Security Companies	**PMCs** Private Military Companies
Mine Clearance Logistics & Supply Risk consulting	Industrial Site Protection Humanitarian Aid Protection Embassy Protection	Military Training Military Intelligence Offensive Combat
PA&E Brown & Root ICI of Oregon	ArmorGroup Wackenhut Gurkha Security Guards	Executive Outcomes (Active) Sandline International (Active) MPRI (Passive)

Fonte: Doug Brooks, *Protecting People: the PMC Potential*, cit., p. 3.

Le NSPs sono le imprese specializzate nel supporto logistico, vale a dire che forniscono una serie di servizi "civili" alle Forze Armate sul campo di battaglia, come ad esempio il rifornimento o la manutenzione.

Le PSC offrono servizi di protezione ma non intraprendono azioni di tipo offensivo. Questi servizi vengono spesso commissionati per la sorveglianza di ambasciate, negli interventi umanitari o da parte di imprese private interessate alla protezione dei propri asset in scenari critici. Sono aziende specializzate nell'ambito della consulenza, dell'analisi del rischio e dell'elaborazione strategica, dunque non sono dotate di una riserva significativa di capitale armato.

Le PMCs, invece, operano generalmente per conto degli Stati ed offrono una vasta gamma di servizi come ad esempio: la protezione ravvicinata di personalità tramite guardie armate, l'addestramento di tiratori e la protezione armata di convogli. Data la natura dei servizi offerti, queste società reclutano essenzialmente ex militari, spesso provenienti dalle migliori unità speciali. All'interno di questo ramo è possibile distinguere ancora le PMCs attive da quelle passive. Le prime, sono impegnate in operazioni di combattimento e di conquista del territorio, mentre le seconde nelle attività di difesa,

training e consulenza. [12]

Le PMCs possono, a loro volta, essere distinte in "attive" e "passive", con le prime impegnate in operazioni di combattimento e conquista del territorio e le seconde nella difesa del territorio, nel training e nella consulenza.

Da questa classificazione emerge come le società di prive military security in realtà non si configurino al 100% come attività di mercenariato, infatti l'erogazione di servizi funzionali a quelli della difesa militare non le rende assimilabili completamente a quel termine.

Un'altra classificazione funzionale ad evidenziare queste differenze è quella proposta da Peter Singer, che prevede la suddivisione delle PMCS in tre sottocategorie:

- Military Provider Firms : Si tratta di *war fighters* o comunque di aziende che svolgono funzioni di controllo e comando in operazioni che prevedono lo scontro armato.
- Military Consulting Firms; specializzate in consulenza ed addestramento.
- Military Support Firms: si occupano della logistica, del supporto tecnico e dell'intelligence.

Il termine Firms sta a sottolineare proprio la natura privata delle società.

Dopo aver compreso attraverso queste classificazioni, la dualità insita in tali servizi, si ritiene, tuttavia che sia pertinente adottare la definizione di PMSCs elaborata nell'ambito del"*Private Security Database* (PSD) *Project*"[13]. Secondo questo progetto, per essere considerate tali, le PMSCs devono soddisfare i seguenti criteri:

- logica di azione orientata al mercato;

- alto livello di professionalizzazione;

- organizzazione disciplinata dal diritto privato;

[12] la dicotomia attive-passive è stata adottata anche da Tim Spicer, ex veterano delle forze armate britanniche.

[13] Il PSD Project, realizzato dalla Freie Universität Berlin, si occupa della raccolta di dati relativi all'impiego di PMSCs da parte di attori pubblici in aree a statualità limitata, al fine di creare un database che consenta di effettuare un'analisi di tipo quantitativo.

- entità giuridica.

- la funzione contrattata deve essere relativa al processo di implementazione interna e/o esterna di obiettivi relativi a politiche di sicurezza di Stati e/o organizzazioni internazionali;

- la funzione contrattata deve essere equivalente a funzioni generalmente erogate da organizzazioni militari o di polizia;

- l'impiego di risorse umane private deve essere volto all'erogazione di servizi militari e di sicurezza, non alla produzione di beni militari (come ad esempio le armi).

L'utilizzo di questi criteri permette di includere nella categoria di PMSC sia compagnie militari, nell'accezione di fornitori di servizi offensivi sul campo; che compagnie di polizia, cioè i fornitori di servizi di consulenza, protezione, manutenzione.

Concludendo, è possibile affermare che in tale ramo sono sì, ricomprese società che svolgendo attività offensive sul campo al posto degli Stati possono effettivamente configurarsi come mercenari; ma che buona parte delle compagnie del settore invece opera nella gamma di servizi funzionali alla sicurezza e complementari a quelli di difesa armata che, in alcuni paesi, come il nostro, resta una prerogativa statale.

3. L'OFFERTA DI SERVIZI DI SICUREZZA PRIVATA

3.1 LA CRESCITA DEL SETTORE

Il settore della sicurezza privata è al giorno d'oggi in piena espansione, grazie alla capacità di configurarsi come una credibile alternativa ai mezzi pubblici, tali società rappresentano ormai un tratto distintivo dello scenario securitario mondiale odierno.

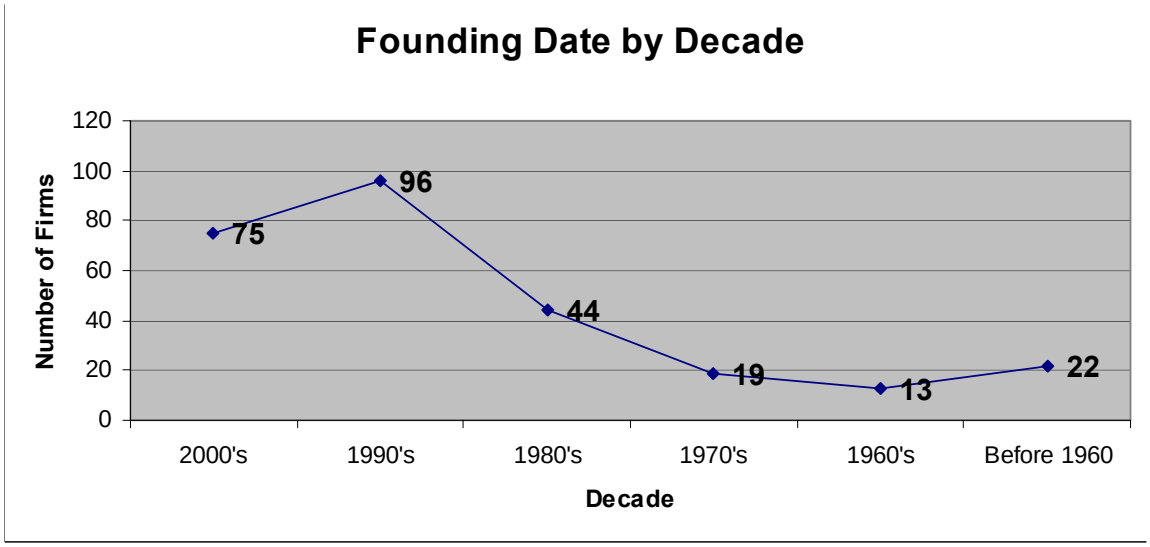
Il loro sviluppo si deve innanzitutto alle mutate dinamiche del contesto strategico mondiale; con la fine della Guerra Fredda, molti Stati hanno ridotto le loro spese militari, tale riduzione è stata accompagnata da un calo degli effettivi in armi che ha toccato tutti i grandi eserciti (il numero totale

di soldati si è ridotto del 22% dal 1987 al 1997).

Tale riduzione, unita al basso livello retributivo dei soldati e a una progressiva riluttanza ad accettare i costi dei conflitti, specialmente quello in termini di vite umane, sono stati i principali driver dello sviluppo del business delle PMCs.

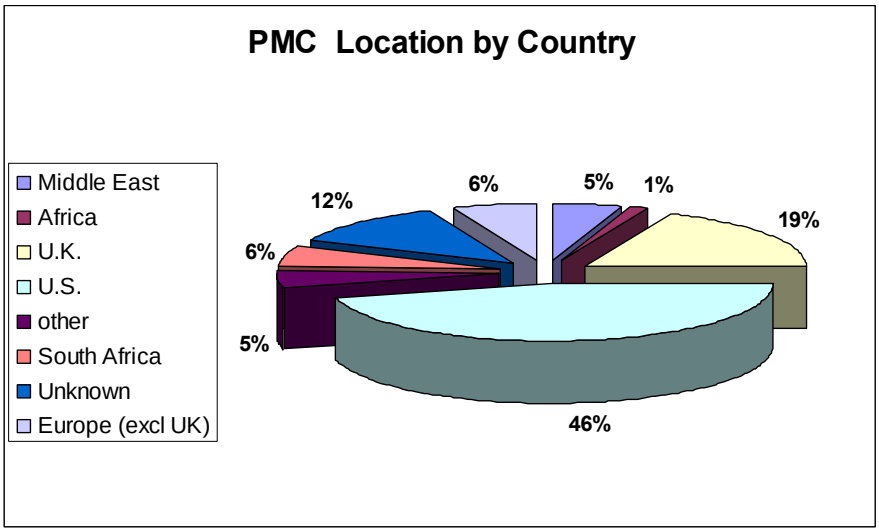
Il grafico sottostante illustra l'incremento del numero di queste compagnie, evidenziando come il picco si sia verificato proprio negli anni '90, al termine dunque della Guerra Fredda, e come un altro picco sia riscontrabile negli anni 2000 in concomitanza con la *Global War on Terror* (GWOT) seguita dall'inizio della guerra in Iraq.

Figura 9: Espansione del settore delle Pmcs.

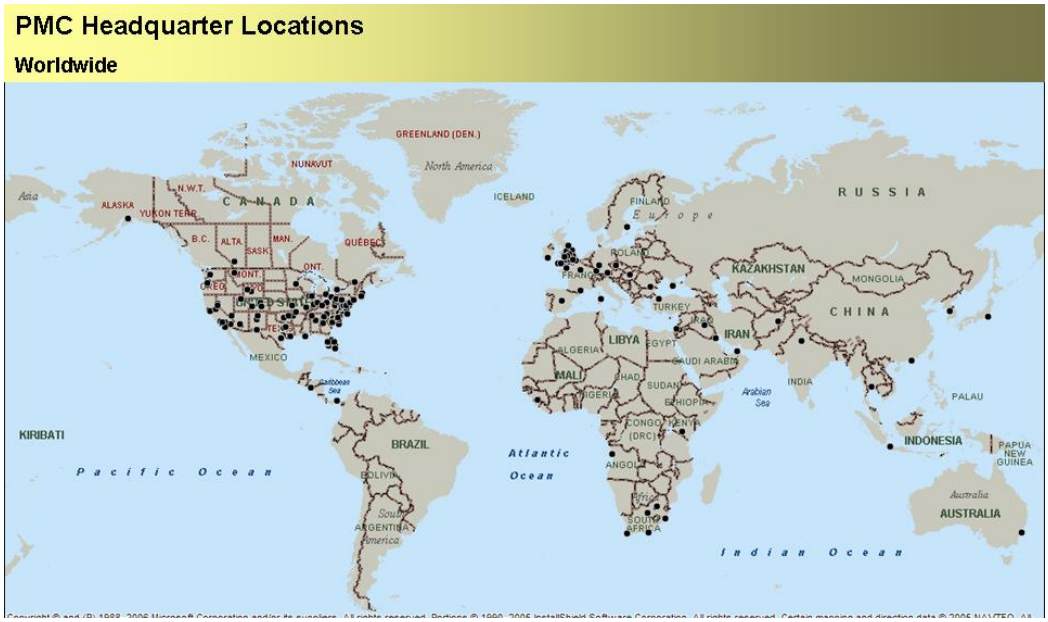


Doug Brooks, Protecting People: the PMC Potential, Comments and Suggestions for the UK Green Paper on Regulating Private Military Services, Alexandria, 2002, http:// www.hoosier84.com/0725brookspmcregs.pdf.

Inoltre, è possibile evidenziare l'impatto di tale tendenza nei diversi Stati: una regolamentazione specifica, l'assenza della stessa, lo stile del Governo e il predominio dei principi di libero mercato possono influire molto sulla crescita di tale settore. Si evince infatti, come la maggior parte delle aziende siano statunitensi o britanniche (rispettivamente il 46% e il 19%); mentre successivamente vi è il Sud Africa in cui è presente il 6% dell'offerta (pari a 35 imprese), Europa (escludendo l'UK) con 35 imprese, Medio Oriente con 3° imprese ed infine Canada, Australia, America Centrale ed Estremo Oriente contano invece la presenza di 28 PMSCs.



Doug Brooks, *Protecting People: the PMC Potential*, Comments and Suggestions for the UK Green Paper on Regulating Private Military Services, Alexandria, 2002, http:// www.hoosier84.com/0725brookspmcregs.pdf.



Doug Brooks, *Protecting People: the PMC Potential*, Comments and Suggestions for the UK Green Paper on Regulating Private Military Services, Alexandria, 2002, http:// www.hoosier84.com/0725brookspmcregs.pdf.

Lo sviluppo di tale settore, oltre ad aver ricevuto una spinta notevole dal mutamento delle dinamiche strategiche statali e dal cambiamento delle politiche militari, è stato mosso anche dalla forte globalizzazione verificatasi negli ultimi decenni. Le PMSCs sono compagnie transazionali, coprono un ampio raggio d'azione, e rappresentano la soluzione ideale per imprese multinazionali che in alcuni dei paesi in cui operano, essendoci una disciplina normativa differente, non sono dotate dello stesso livello di tutela che invece viene loro garantito nel loro Paese di origine.
È il caso di molte multinazionali italiane che stipulano contratti con queste agenzie per tutelarsi nei Paesi in cui la normativa in termini di sicurezza si discosta molto da quella italiana (ancora strettamente legata al ramo pubblico).

3.2 L'ORGANIZZAZIONE DELLE PMSCs

La crescita di tale settore è dovuta, tuttavia anche alla conformazione organizzativa di tali società che risponde adeguatamente ai bisogni odierni.
A tal proposito, Stefano Ruzza in Guerre contro Terzi, ha delineato una sintesi dei principali tratti caratterizzanti l'organizzazione di tali compagnie.
Il primo aspetto è l'integrazione sia verticale che orizzontale, che riflette la capacità di tali aziende di fondersi sia con altre dello stesso settore sia con altre di settori differenti. L'integrazione può rispondere sia a finalità strategiche che a motivi legati al profitto.
Il secondo tratto rilevante è la flessibilità che queste società godono sia per mutamenti relativi alla propria immagine che al proprio profilo giudico. Infatti non esistendo una normativa specifica del settore, e rispondendo quindi a quella dedicata alle generiche attività private con scopo di lucro esse possono mutare il loro regime e la loro conformazione nel caso in cui ciò risulti conveniente, mantenendo in tal modo comunque un'apparenza legittima. L'elevata flessibilità normativa di queste organizzazioni rende le barriere all'entrata del settore basse e di conseguenza il settore anche molto attrattivo.
Altro tratto saliente è quello relativo alla scala organizzativa: queste imprese lavorando su un'ampia scala geografica, si configurano come imprese di elevate dimensioni, con ampia gamma di servizi disponibili anche contemporaneamente. Si tratta di multitasking society, questo aspetto permette loro di avere una predisposizione all'ampiamento di gamma di servizi e conseguentemente di potenziali clienti.

3.3 I SERVIZI OFFERTI

Come già accennato nei paragrafi precedenti, l'offerta di servizi erogati dalle PMSCs è molto diversificata.

Tali compagnie offrono servizi nel:

- Ramo logistico;
- Ramo manutenzione;
- Ramo intelligence;
- Ramo sorveglianza;
- Ramo ricognizione e monitoraggio;
- Ramo sminamento;
- Ramo consulenza;
- Ramo training;
- Ramo di sicurezza marittima.
- Ramo azione offensiva sul campo.

I servizi logistici sono relativi alla costruzione di caserme o campi di accoglienza, il ramo manutenzione è relativo alla manutenzione degli stessi. Mentre, i servizi di intelligence e consulenza possono tradursi in delineazione di programmi di riforma e ristrutturazione delle Forze Armate, di pianificazione tattica e operativa, ma anche in studi sull'analisi del rischio in specifiche aree geografiche.

I servizi di training, ampiamente utilizzati dal governo britannico, sono volti alla formazione del personale dell'esercito. Famosa in questo settore è ad esempio Viennel, ingaggiata nel 2003 dal Dipartimento della Difesa statunitense per ricreare il nuovo esercito iracheno.

I servizi di sicurezza marittima, invece, vengono forniti attraverso team armati o scorte alle navi. Sono servizi che molte compagnie richiedono, in quanto le azioni antipirateria intraprese dagli Stati talvolta non sono sufficienti a garantire la sicurezza di tutte le imbarcazioni. L'Italia fa uso di questa categoria di servizi, risultando tali contratti più economici rispetto all'aumento dei premi assicurativi

derivante dall'incremento di attacchi di pirateria. Inoltre, anche le compagnie assicurative sono favorevoli all'impiego di Maritime security companies, tanto da arrivare a ridurre del 40% i premi assicurativi per quelle navi che usufruiscono di team privati di protezione a bordo.

Infine, i servizi armati offensivi sono quelli che vedono la PMSC impegnata direttamente sul "campo di battaglia"; mentre quelli armati difensivi rientrano nella categoria di force protection; svolgono, cioè, prestazioni volte alla protezione di persone fisiche come politici, diplomatici ed alla protezione di convogli stradali civili, siti strategici, fabbriche.

3.4 IL PERSONALE

L'erogazione di una cosi vasta gamma di servizi altamente specializzati, rende fondamentale l'arruolamento di uomini con elevata esperienza nel settore della sicurezza. Si osserva, come la maggior parte di queste compagnie siano state fondate da ex membri dei servizi segreti statali, e come esse reclutino essenzialmente personale che ne faceva parte. Il personale viene individuato mediante database che contengono un grande numero di nominativi di ex militari e membri delle forze di polizia; riescono in tal modo ad accedere ad un bacino di reclutamento composto da soggetti altamente qualificati e ad un costo relativamente basso.

Infatti, i bassi salari dei militari di professione rappresentano un incentivo per tali soggetti a prestar servizio per queste private companies che promette salari più alti, per compensare essenzialmente l'incertezza derivante dalla durata del rapporto lavorativo.

3.5 I VANTAGGI DEL RICORSO A COMPAGNIE DI SICUREZZA PRIVATA

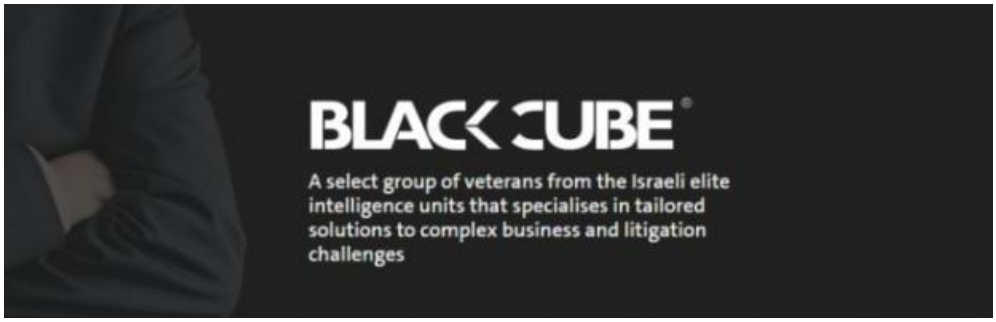
In conclusione, i fattori che spingono l'industria privata ad esternalizzare la propria sicurezza, sono essenzialmente l'efficienza dei servizi, sia in termini di flessibilità e adattabilità alle proprie esigenze, che in termini di tempistica; l'affidabilità derivante dal rapporto B2C tra cliente e provider; il fatto che talvolta lo Stato in cui l'impresa è situata (tipicamente per le imprese transazionali) non offra determinate garanzie; ed infine i benefici derivanti dal miglior controllo sulla controparte contrattuale e sugli standard qualitativi del servizio richiesti.
Anche dal punto di vista dello Stato, l'outsourcing di determinati servizi di sicurezza comporta alcuni

vantaggi, in primis in termini di efficienza economica poiché si delegano determinate funzioni ad agenzie altamente qualificate, con cui è possibile proteggere i propri interessi e determinare i livelli di protezione richiesti semplicemente attraverso un chiaro accordo contrattuale. Tale prassi comporta un costo minore rispetto a quello da sostenere per garantire l'erogazione interna di tali servizi, ciò consente inoltre di alleggerire la struttura del sistema di sicurezza, smobilizzando personale e di renderla più flessibile alle odierne esigenze. Inoltre, l'adozione di un comprehensive approach tra pubblico e privato rappresenta la soluzione migliore per poter fronteggiare le nuove minacce cyber, per le quali il livello di competenze possedute dal settore pubblico non risulta ancora completamente adeguato agli standard qualitativi necessari.

In Italia, in generale, l'esternalizzazione della sicurezza alle compagnie private non è vista di buon occhio, essendo la sicurezza una prerogativa pubblica, la cessione di tale compito a privati appare incostituzionale; nonostante ciò, l'utilizzo di queste compagnie da parte del pubblico è avvenuto in casi limitati anche in Italia mediante la predisposizione di decreti ad hoc (come ad esempio per il servizio fornito dalle Msc). Per quanto riguarda invece la nascita di compagnie di sicurezza all'interno del territorio italiano, il fenomeno risulta nettamente ridotto rispetto a quello degli altri paesi europei, tuttavia le PMSCs presenti nel nostro territorio sono principalmente relative ai rami di consulenza, intelligence, supporto strategico e logistico; lasciando fuori le Military provider, a sottolineare la prerogativa statale per le azioni offensive e difensive armate, e il rifiuto della "pratica del mercenario".

CAPITOLO 4

IL CASO BLACK CUBE



Black Cube è una società di intelligence privata, fondata nel 2010 da ex funzionari dei servizi segreti israeliani Dan Zorella e Avi Yanus e ha sedi a Londra, Parigi e Tel Aviv.
Il business principale della società è quello relativo al litigation support, nel quale la compagnia sfrutta al meglio le potenzialità offerte da evolute analisi di intelligence, è stata infatti coinvolta in vari scandali in cui le si chiedeva di cercare dati sulle controparti in grado di poter apportare vantaggio o tutela al proprio cliente.
La società tuttavia, si configura come una multiservices company, l'ampia gamma di servizi da essa offerti è raggruppabile in quattro macroaree:

1. *Corporate intelligence;*
2. *Consulenza legale e gestione dei conflitti;*
3. *Investiment;*
4. *Cyber intelligence.*

1. CORPORATE INTELLIGENCE

Per quanto riguarda l'area relativa la corporate intelligence, essa offre analisi di:

- Competitive intelligence;
- Identificazione di nuove opportunità
- Due Diligence
- Report di conformità

La Competitive intelligence consiste nell'identificazione di opportunità e rischi utilizzando una metodologia all'avanguardia che include la raccolta di informazioni e una capacità di ricerca di alto livello rafforzata da competenze tecniche e legali. L'analisi fatta dalla società viene poi fornita al cliente in una chiara rappresentazione che evidenzia i concorrenti, la loro politica, i comportamenti, i servizi, le attività di R&S, e identifica i possibili conflitti/frodi.
Indagini del genere risultano anche funzionali all'erogazione di un servizio volto all'identificazione di nuove opportunità per il cliente sul mercato. Infatti in ogni azienda lo sviluppo di un nuovo business o l'ampliamento del preesistente presuppongono un'attenta analisi di mercato e di ricerca di business strategici. Black Cube identifica uniche opportunità di business e assiste i clienti per coglierle, creando profili dettagliati in grado di monitorare i movimenti del business.

Il servizio di Due Diligence rappresenta uno dei principali business di Bc[14], per Due Diligence ci si riferisce all'attività di investigazione e di approfondimento di dati e di informazioni relative all'oggetto di una trattativa. Il fine di questa attività è quello di valutare la convenienza di un affare e di identificarne i rischi e i problemi connessi, sia per negoziare termini e condizioni del contratto, sia per predisporre adeguati strumenti di garanzia, di indennizzo o di risarcimento.[15]
In particolare, il servizio di due Diligence fornito da Black Cube è di alto livello, viene fatta un'analisi profonda (si parla infatti di Deep Level Due Diligence) che analizza gli interessi delle controparti, l'operato passato della controparte (informazioni storiche), informazioni finanziarie, legali e altri aspetti tecnici, predisponendo un profilo dettagliato della società oggetto o controparte della trattativa. Inoltre, attività complementare a quella di Due Diligence è quella svolta dalla società per la produzione di report di conformità. Sfruttando ben 240 database Black Cube riesce ad indentificare in potenziali partner violazioni, riciclaggio di denaro e presenza di altre operazioni riconducibili al crimine organizzato e alla violazione della legge. Attraverso queste analisi, BC produce un report di conformità delle aziende in oggetto di esame, che attesta il rispetto dei requisiti del Normativa di riferimento.

[14] Bc abbreviazione di Black Cube.
[15] Due Diligence definizione da Dizionario Treccani.

2. CONSULENZA LEGALE E GESTIONE DEI CONFLITTI (LITIGATION SUPPORT)

Tale area rappresenta il core business della compagnia, BC impiega tutte le sue risorse (tecnologiche, umane) per assistere il cliente in operazioni legali che potrebbero intaccare negativamente la sua posizione, utilizzando un approccio pro-attivo per la risoluzione dei conflitti e la chiusura di affari di vario genere. I risultati delle indagini poste in essere possono impattare notevolmente sulla strategia dell'impresa o sulla posizione del cliente, la società grazie al suo team di esperti e consulenti è in grado di offrire anche un consiglio professionale in merito.

I principali servizi rientranti in questo ramo sono:

- **La raccolta e l'analisi di informazioni critiche per il cliente.** Attraverso una stretta collaborazione con lo stesso, gli agenti di BC riescono a reperire materiale e report in aree specifiche necessari per promuovere l'interesse del cliente. L'attività di raccolta dati include anche l'identificazione di potenziali minacce, e la valutazione dei punti di forza dei concorrenti.

- **L'attivita' di recupero e tracciamento di dati**. Grazie alla profonda familiarità con la legislazione pertinente e con le procedure giudiziarie relative al recupero dei beni, Bc riesce ad offrire un servizio di tracciamento e recupero dati in grado di operare in diverse giurisdizioni con diversi sistemi legali, estendendo fino all'analisi di società offshore e trust.

- **L'analisi degli interessi e supporto nei conflitti.** Essendo la conoscenza della controparte un elemento chiave per la gestione del contenzioso Bc utilizza la sua metodologia per identificare interessi, vulnerabilità, priorità e strategie della controparte ed evidenze di cattiva condotta, fornendo e analizzando informazioni difficilmente reperibili.

- **L' analisi volta all'identificazione di cattiva condotta e di sviluppo eccessivo della leva finanziaria.** Tale attività è complementare alle precedenti, infatti attraverso l'attività investigativa e di analisi delle informazioni raccolte, gli esperti di Bc riescono ad identificare possibili casi di frode, violazione di vincoli/ requisiti normativi e a segnalarli non solo al cliente, ma anche alle autorità di competenza aprendo azioni civili.

3. INVESTMENT INTELLIGENCE

I servizi di investment intelligence sono rivolti essenzialmente a fondi rischio, private equity e investment houses, tutti soggetti giuridici per cui l'attività investigativa rappresenta un servizio fondamentale per i loro business.

In tale ramo BC offre non solo un'analisi accurata delle informazioni raccolte (sempre nei confini della liceità), ma anche una consulenza strategico-legale.

I principali servizi richiesti in tale ambito sono:

- **Strategy & Leadership Mapping.**

  Tale servizio si occupa della raccolta di informazioni relative al personale aziendale e in particolare a quelle relative ai membri del management, analizzando i loro interessi, le strategie poste in essere e le circostanze personali. Queste informazioni sono fondamentali per fornire una rappresentazione veritiera della direzione del management della compagnia e per supportare o meno determinate operazioni, come ad esempio IPO.

- **Internal Fraud and Misrepresentation.** Il servizio di frode interna e rappresentazione non veritiera in bilancio è volto a tutelare l'azienda dal rischio insito nel rapporto di agenzia con il management aziendale. Infatti, i manager avendo una visione di breve periodo, spesso volta alla massimizzazione dei propri bonus, tendono a mettere in atto operazioni che spesso si traducono in frodi finanziarie attraverso la "Contabilità creativa" [16]in bilancio. Black Cube è specializzata in tale ramo, riesce a scoprire ciò che l'azienda vuole nascondere attraverso giochi in bilancio e comunicazioni pubbliche non trasparenti e a fornire al cliente una rappresentazione veritiera dello status dell'azienda oggetto d'esame.

- **Attivita' di stima degli asset aziendali** (Asset Valuation and Impending Dissolutions). Tale servizio consiste nel fornire una stima attendibile del valore degli asset aziendali, prevalentemente finalizzata all'utilizzo in casi di scissione, fusione e fallimento aziendale.

[16] Contabilità creativa: insieme di trucchetti contabili posti in essere in bilancio per modificare i risultati di esercizio o la situazione patrimoniale aziendale. si tratta di operazioni che possono essere finalizzate all'erosione fiscale o alla modifica del valore aziendale.

- **L’analisi dei cambiamenti futuri del mercato.** Analisi dei mercati e delle loro prospettive future per poter fornire una stima del valore aziendale che tenga conto anche delle sue prospettive future. Le indagini svolte a tal fine risultano di rilevanza strategica sia in casi di vendita e fusione d’azienda, sia per l’identificazione di opportunità future per la stessa, risultando complementare al servizio di identificazione di opportunità esaminato nell’area di corporate intelligence.

4. CYBER INTELLIGENCE

Il ramo Cyber, è un’area emergente, i rischi derivanti dalle nuove tecnologie sono quelli che al giorno d’oggi spaventano più le compagnie. Direttive normative, e buon senso aziendale impongono alle società di dotarsi di piattaforme e servizi volti a garantire l’incolumità dei propri dati da attacchi cyber.

Gli attacchi cyber possono avere diverse finalità: ledere la reputazione aziendale, rubare dati, modificare dati esistenti nei sistemi informatici a tal riguardo Bc offre servizi volti a:

1. Difendere la reputazione aziendale da attacchi informatici volti a ledere l’azienda identificando le voci e mettendole a tacere nel minor tempo possibile.
2. Proteggere le aziende dalla fuga di dati, prestando molta attenzione alle mosse dei dipendenti, identificando quelli potenzialmente più rischiosi ponendo in essere un’attività di monitoraggio.
3. Identificare possibili minacce tramite l’analisi dei dati.
4. Garantire l’autenticità delle informazioni attraverso l’informatica forense che è in grado di tracciare il DNA dell’informazione e di evidenziare i documenti che sono stati alterati.

SCHEMA RIASSUNTIVO DELLA GAMMA DI SERVIZI OFFERTA DA BC :

I CLIENTI

Le compagnie legali ed istituzioni finanziarie sono i principali clienti di questa società, anche se Bc è stata più volte oggetto di vari scandali legati a clienti che non rientrano in tali profili, come ad esempio il caso Weinstein o il recentissimo caso Trump.

Tuttavia, con i nuovi sviluppi dello scenario macro economico-giuridico vi sarà un incremento nell'utilizzo anche in altri settori, come ad esempio quello industriale. Questo, infatti, rappresenta uno dei principali driver della crescita del business di intelligence privata.

I VANTAGGI COMPETITIVI DI BLACK CUBE

La società sostiene che ciò che rende unici i servizi da essa offerti sono derivanti dalle abilità analitiche all'avanguardia da essa possedute, dalle competenze all'avanguardia relative al mondo Cyber, dalle conoscenze multilinguistiche e culturali del loro team; nell'ampio Data-base di dati a loro disposizione e infine dal loro approccio proattivo.

Il primo punto di forza, ovvero le abilità analitiche, è dovuto all'elevata esperienza maturata dai membri della società durante il loro precedente servizio per le agenzie governative. Gli agenti hanno

infatti sviluppato un approccio di pensiero creativo in grado di cogliere sottigliezze e collegare vari punti. Tale capacità risulta rilevante anche per l'applicazione del approccio pro-attivo che Bc utilizza per la ricerca dati. Infatti qualora le informazioni ricercate non siano disponibili o facilmente rintracciabili, Bc attraverso metodi unici, soprattutto nel campo ingegneristico riesce a trovare una soluzione per estrarre tali dati.
A tal proposito può risultare un buon esempio la citazione dei casi Weinstein e Trump, da cui emerge come per ottenere informazioni sui soggetti coinvolti nei vari casi, la società abbia utilizzato sistemi informatici e in particolar modo abbia in entrambi i casi utilizzato mail mandate da "società veicolo" create ad hoc.
In seguito, un estratto dell'articolo: -Usa, "gli spioni di Weinstein ingaggiati da Trump per far fallire l'intesa sul nucleare con l'Iran" di Fabio Scuto per "Il Fatto Quotidiano" dell'8 Maggio 2018.

" *Le rivelazioni indicano che la moglie di Ben Rhodes – ex consigliere senior di Obama e membro del Consiglio di Sicurezza Nazionale – ha ricevuto mail sospette l'anno scorso da una società cinematografica con sede a Londra – la Shell Productions – che si è rivelata poi una falsa compagnia creata dalla Black Cube. Una tattica simile era stata usata per contattare la moglie di Colin Kahl, un altro ex funzionario della Sicurezza Nazionale, attraverso una finta società finanziaria – la Reuben Capital Partners – anch'essa basata nella capitale inglese. Il nome Reuben Capital Partners è stato menzionato per la prima volta l'anno scorso in una inchiesta del New Yorker, in cui si descrivono i tentativi di Weinstein di spiare le donne che lo accusavano di violenza sessuale. L'inchiesta, che ha vinto un premio Pulitzer, ha descritto Reuben Capital Partners come una falsa compagnia usata da Black Cube, ingaggiata da Weinstein per infangare le sue vittime e screditare così le loro testimonianze contro di lui."*

Inoltre, l'operatività di questa società a livello transnazionale, rende necessaria la conoscenza dei vari background socio-economici e linguistici. È perciò che Bc è dotata di 30 soggetti madrelingua e di specifiche conoscenze che le permettono di offrire un servizio di alta gamma in: Europa, Unione Sovietica, USA e molti altri paesi (ricordiamo che Bc ha già operato con successo in ben 70 paesi).
Infine, grazie all'ampiezza del loro business, la società è dotata di un piattaforme che le garantiscono un accesso a ben 240 siti con accesso limitato, ed è in grado di instaurare nuovi accessi a seconda dei bisogni del cliente.
Da questa analisi dei vantaggi competitivi, emerge come i profili professionali dei membri rappresentino in realtà la principale risorsa per la società, osserviamo nello specifico le caratteristiche dei vari agenti.

I MEMBRI

Black cube è stata fondata da alcuni ex membri dei servizi segreti israeliani, soggetti che continuano ad avere un legame con il governo e i servizi di intelligence governativa.
I suoi membri sono quindi dotati di elevate conoscenze tecniche, strategiche, capacità di leadership e di un'elevata conoscenza delle varie regolamentazioni.

Volendo tracciare un profilo dell'agente tipo di Bc egli dovrebbe possedere le seguenti caratteristiche:

- Capacità di leadership;
- Strategic approach;
- Abilità operative sul campo;
- Abilità di analisi dati;
- Capacità mediatiche (anche rapporti governativi);
- Conoscenze normativo-legali;
- Conoscenze in abito finanziario- risk management;
- Conoscenze ramo Itc.

Attualmente, i componenti di spicco del gruppo possiedono quasi tutti queste competenze, essendo ciascuno però specializzato magari in un ambito specifico. Ciò fa pensare ad un approccio organizzativo organico, basato sul lavoro in team, nonostante la provenienza dall'ambito militare lasci trasparire l'idea di una organizzazione fortemente gerarchizzata.
Lavorando su diversi progetti infatti, il lavoro di gruppo si rivela più efficiente e consente non solo risparmio in termini di tempo, ma consente al gruppo di focalizzarsi su un determinato progetto senza perder di vista l'obiettivo principale.
Una struttura matriciale, dati i vari servizi offerti potrebbe essere efficiente, perché permetterebbe di sfruttare le conoscenze specifiche di ogni funzione coordinandole mediante la figura del project manager, tuttavia l'approccio organico "puro" conferendo più flessibilità e reattività all'organizzazione credo si presti meglio.

LA RICETTA PER IL SUCCESSO

In conclusione, possiamo affermare che la loro ricetta per il successo sia basata su :

- PROFESSIONALITA' dei loro agenti e dell'elevata specializzazione delle loro conoscenze in ogni ambito.
- ENTUSIASMO. Elemento necessario per la creazione di valore per il cliente e per l'azione dell'approccio pro-attivo volto al raggiungimento del miglior risultato possibile per il cliente.
- INTEGRITA': la società garantisce un approccio di totale trasparenza nei confronti del cliente, cooperando con lo stesso e informandolo costantemente sullo stato delle indagini.
- EFFICIENZA: la società si impegna a garantire il miglior risultato nel minor tempo possibile, offrendo al termine delle indagini una rappresentazione chiara e precisa del risultato.
- CONFIDENZIALITÀ: il rapporto di fiducia con il cliente è alla base della politica aziendale.
- INTRAPRENDENZA: L'approccio creativo e la politica del "*thinking out of the box*" consentono alla società approcci del tutto innovativi in grado di risolvere anche i casi più complessi.

IL CASO ACADEMI (EX BLACKWATER)

LE ORIGINI

Il gruppo Constellis è specializzato nella fornitura di servizi di risk management, sicurezza, training e servizi umanitari, rivolti sia al privato che al settore pubblico. La società nasce nel 2010 attraverso l'acquisizione di ACADEMI, meglio nota come ex Blackwater, e successivamente di altre società specializzate nel ramo che le hanno permesso di estendere così tanto la gamma di servizi specializzati offerti.

Come è possibile osservare dalla figura, l'attuale configurazione del gruppo è frutto di acquisizioni strategiche che vedono ad oggi convergere sotto la stessa holding società come: Academi, IDS, Strategic Social, Olive Group, Centerra, tdi, Amk9, Omniplex, Triple Canopy ed Edinburgh International. L'intero gruppo è stato poi acquisito da Apollo nel 2016.

L'acquisizione di ACADEMI coincide con la fondazione stessa del gruppo. Academi è una PMSC fondata nel 1997 da Erik Prince con il nome Blackwater, rinominata nel 2009 come Xe Services e successivamente come Academi. La società, utilizzata dal governo statunitense per interventi armati in Iraq, ha acquisito una cattiva notorietà in seguito all'attacco fatto dai suoi agenti in Iraq nel 2007 che ha portato alla morte di 14 cittadini.

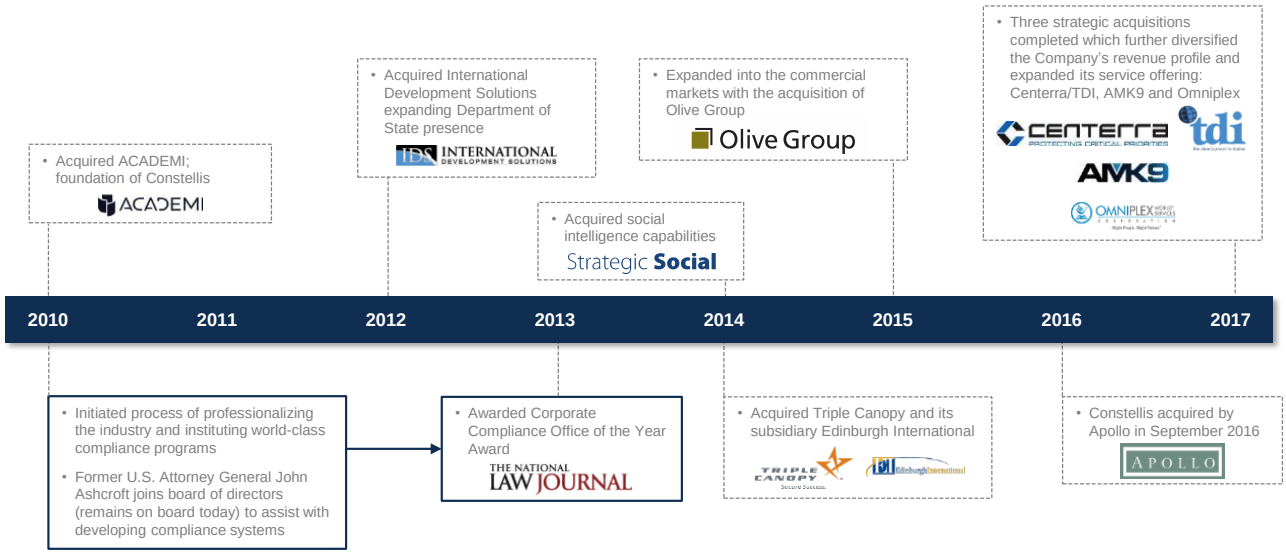
Successivamente, nel 2014, la società è finita nuovamente in prima pagina in seguito a un'imboscata fatta durante un'insurrezione sunnita in cui quattro uomini appartenenti alla società caddero. Essi furono uccisi, carbonizzati e i loro cadaveri appesi ad uno dei ponti sull'Eufrate. Ovviamente tale

vicenda portò poi alla alla pianificazione ed esecuzione di un assalto su vasta scala condotto dal Corpo dei Marines statunitense.

Academi in virtù dell'alta specializzazione ed esperienza del suo staff era (ed è tutt'ora) una delle maggiori compagnie impiegate dal Dipartimento di Stato per lo svolgimento di operazioni armate e non su scala mondiale.

Le successive acquisizioni poste in essere dal gruppo avevano la finalità di espandere ancor più la gamma di servizi offerti con un elevato livello di specializzazione. Si osserva come queste acquisizioni strategiche abbiano portato il gruppo ad avere una posizione di leadership in più business nel settore della sicurezza.

Figura 10 La storia del gruppo (da Constellis overview)



I SERVIZI

Il gruppo offre una gamma di servizi diversificata di alto livello. È possibile racchiuderli in tre macro aree:

- Risk Management;
- Protective Security;
- Servizi di Assistenza Umanitaria e Addestramento.

RISK MANAGEMENT

Constellis offre un servizio di risk management e consulenza volto a supportare i clienti in decisioni di rilevanza strategica e nella programmazione di progetti. In particolare, il cliente viene assistito nell'ideazione di strategie volte a fronteggiare una crisi presente, e a dotarsi dei giusti mezzi per poter affrontare una potenziale crisi futura riducendone il più possibile l'impatto. Inoltre, la natura integrata di team composti da professionisti specializzati in varie materie, conferisce al servizio reso una completezza in grado di offrire al cliente una panoramica dettagliata delle situazioni.

In particolare, le soluzioni offerte in tale ambito sono relative a:

- Servizi investigativi: i principali beneficiari di questo servizio sono i Governi.
  In tale ramo il gruppo si pone come leader del settore, con un network composto da 1800 investigatori e l'utilizzo dei più avanzati software tecnologici. La società inoltre, è l'unica a condurre l'attività investigativa a livello mondiale e l'integrità del suo team e la qualità dei suoi servizi la rendono una dei miglior contractor per l'erogazione di servizi di sicurezza anche per Stati.
- Servizi di Analisi: lo svolgimento di un'accurata attività di intelligence permette alla società di offrire un servizio di risk management evoluto, in grado di condurre ad efficienti strategie e all'identificazione non solo di rischi ma anche di opportunità. La suddetta attività è di notevole rilevanza per gli Stati, tale servizio è in grado di offrire analisi dettagliate anche in materie come la sicurezza navale e aerea, fermo restando la sua flessibilità di utilizzo in varie aree (geografiche e settoriali).

Sulla base di queste due attività Constellis riesce ad identificare rischi, ad ideare soluzioni strategiche e a tutelare il cliente offrendo servizi specifici come:

- *Crisis management;*
- *Risk & security consulting;*
- *Security system;*
- *Safety management;*
- *Due diligence;*

PROTECTIVE SECURITY

Constellis è molto nota per i servizi offerti in tale ramo, per i quale i principali clienti sono di natura governativa. In questa macro area troviamo servizi volti a garantire la sicurezza di postazioni mobili e fisse, volti a salvaguardare infrastrutture critiche da possibili attacchi. Il tipo di servizio offerto in questo ambito può essere anche armato e viene spesso richiesto non solo da entità governative, ma anche da privati per la protezione ad esempio di asset specifici (es giacimenti petroliferi).

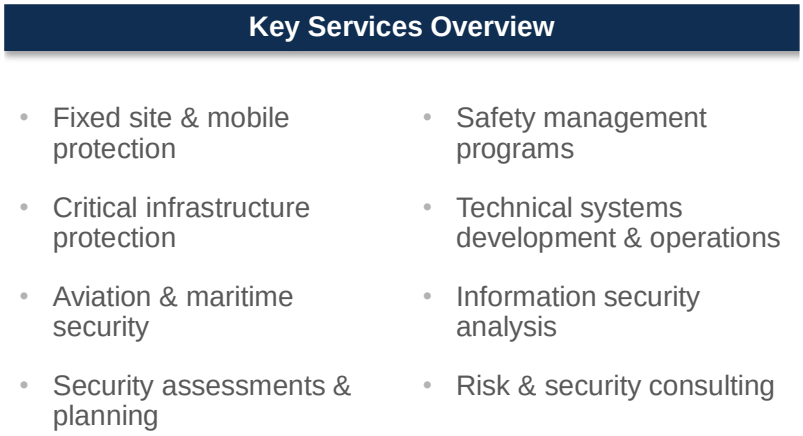
Inoltre, sono specializzati nell'offrire servizi di sicurezza marittima monitorando e programmando i tragitti migliori per imbarcazioni e offrendo anche una scorta alle stesse durante i viaggi; ma anche di sicurezza aerea, Constellis in qualità di contractor offre i suoi servigi ad aeroporti per garantirne la sicurezza sia a terra che in volo.

Il gruppo possiede un'elevata esperienza nella gestione di operazioni antiterrorismo essendo dotata di esperti in esplosivi, strategia, training.

Il primato posseduto in tali ambiti deriva da costanti investimenti in qualità e sicurezza fatti per rispondere agli standard richiesti da ogni singolo cliente. La creazione di teams che integrano alte conoscenze multidisciplinari permette all'azienda di essere in grado di rispondere ai cambiamenti contestuali con rapidità e flessibilità.

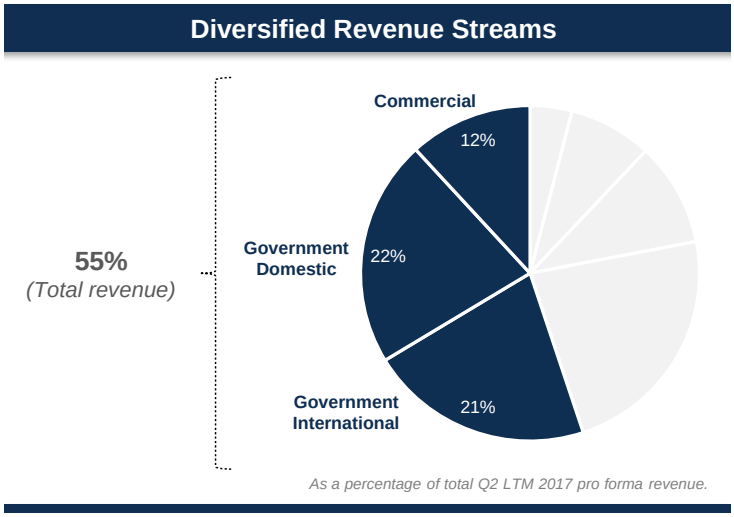
Constellis è considerato una Private Security Company Standard, ciò comporta che esso abbia aderito al Codice di condotta internazionale per i fornitori privati di servizi di sicurezza (ICoC); inoltre la copertura globale offerta dai suoi servizi viene monitorata 24/7 dal Global Operations & Communications Centre (GOCC) mediante un software in grado di tracciarne tutti i movimenti.

Figura 11 Servizi principali delle macro aree di Risk Management e Security (da Constellis Overview)



Da queste due aree, come si osserva dal report del gruppo in basso, proviene il 55% dei ricavi del gruppo, i cui principali clienti sono i Governi (nazionale e non), in cui tuttavia i privati rappresentano una fetta del 12%.

Figura 12 Incidenza sui ricavi complessivi (da Constellis Overview)



ASSISTENZA UMANITARIA E ADDESTRAMENTO

I servizi relativi al ramo umanitario vedono Constellis impegnata in scopi sociali, la società offre infatti servizi specializzati per la rimozione di mine e il rilevamento di aree contaminate. In tale ambito il gruppo, affianca gli Stati Uniti nella rimozione di ERW (Explosive remnants of war) aderendo all'International Mine Action Standards (IMAS).

Per quanto riguarda invece l'addestramento, tali servizi sono sempre più richiesti dal Governo, soprattutto in seguito ai tagli in bilancio sulla spesa militare. Gli istruttori sono professionisti con esperienza in ambito di security management e tecniche di sicurezza, diplomazia, gestione, legge ed hanno tutti una consolidata esperienza nel servizio militare.
Vengono offerti piani differenziati per ogni cliente, in modo da poter costruire su basi specifiche i programmi di addestramento. Le soluzioni proposte in questo ambito sono ad esempio: *Tactical training, Canine training, Exercise planning and support, Simulation & Scenario-based training.*

Nell'immagine seguente è possibile trovare una panoramica più dettagliata dei servizi offerti in questa macro area, da cui emerge l'elevata specializzazione dell'offerta nonostante essa sia ampiamente diversificata.

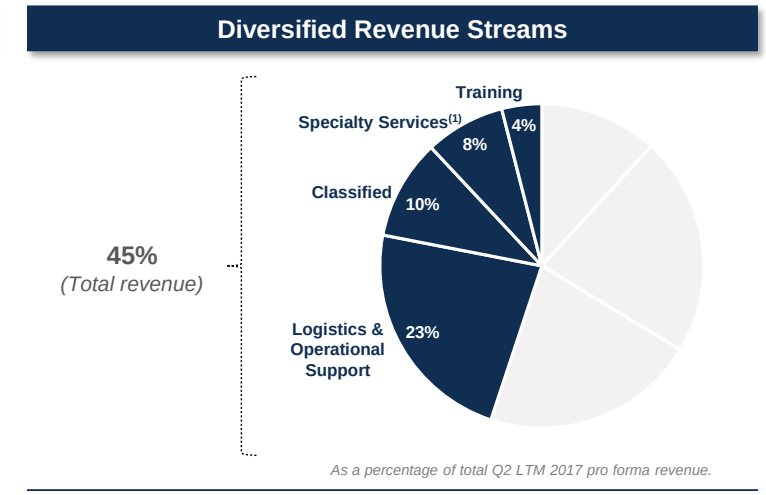
Key Services Overview

Logistics & Operational Support	Specialty Services	Training
• Life & logistics support	• Humanitarian services	• Curriculum development
• Operations & maintenance; fleet management	• Investigative services	• Tactical training
• Engineering, procurement & construction	• Unmanned aircraft systems	• Exercise planning & support
• Capacity building & mentoring	• Social intelligence solutions	• Simulation & scenario-based
• Fire protection & medical	• Biometrics collection & analytics	• Mobile training units
• Disaster relief & planning	• C4I system integration	• Client-based, customized training
• Contingency operations	• K-9 training	• Rule of law / cultural sensitivity

(1) Specialty Services includes investigative services, humanitarian, unmanned aircraft systems and K-9 services.

Infine, è possibile osservare come sui ricavi complessivi della macro area, l'impatto più rilevante sia quello dei servizi di Logistics & Operational Support, a conferma del largo utilizzo fatto degli stessi dalle autorità Governative.

Figura 13 Incidenza sui ricavi complessivi (da Constellis Overview)



IL PERSONALE

Essendo i servizi offerti di alto livello e dovendo rispettare precisi standard qualitativi, Constellis prevede una rigorosa selezione per il reclutamento dei suoi agenti. Innanzitutto nella fase di selezione viene prima accertata la sana costituzione e vengono fatti test antidroga sui soggetti; dopodiché si procede con la selezione. Per tali posizioni sono fondamentali elevate performance psico-fisiche, capacità di leadership, maturità e il saper lavorare in squadra, nonché un interesse innato per la sicurezza e l'attenzione verso il cliente.

La politica aziendale, è molto solidale verso i dipendenti, offrendo loro premi incentivo, benefits e piani di carriera volti a motivare il dipendente e ad incentivare la creazione di un ambiente lavorativo diversificato e collaborativo. Inoltre, il gruppo è molto attento alla loro formazione, predispone infatti frequenti corsi di aggiornamento con conseguimento di certificazioni.

Tuttavia, nonostante la precedente appartenenza alle forze armate non sia un requisito fondamentale, il 50% dei loro 17000 dipendenti ne era un membro. Ciò sta ad evidenziare l'importanza che l'esperienza in tale campo sia un aspetto fondamentale per la formazione dell'agente unitamente alle conoscenze in merito alle leggi internazionali.

I CLIENTI

Come si evince dalla descrizione dei servizi, il gruppo si rivolge a due soggetti: i Governi, e gli Enti privati tra cui vi sono varie società commerciali.

Tuttavia, è stato evidenziato che l'impiego da parte dei Governi è molto più incisivo sul business complessivo della società, essa infatti è in una posizione di leadership nel settore ed ha ottenuto vari riconoscimenti, nonostante sia stata anche oggetto di alcune vicende che hanno leso alla sua reputazione come l'attacco del 2007 quando il gruppo però non era ancora costituito (e dunque facciamo riferimento solo alla vicenda accaduta alla società Academi, ai tempi nota come Blackwater), o la vicenda che ha visto i suoi agenti vittima di un'imboscata nel 2014.

In particolare, John F. Kerry, ex Segretario di Stato, in una lettera indirizzata a Constellis nel 2013 si esprime in questi termini:

"There are not really words to convey the profound appreciation of the Department of State and the entire United States Government for the performance of your team...the onsite FBI team told my Consul that they had rarely seen a security plan better executed – testament to your team's courage, professionalism and patriotism... you kept our diplomats safe. God bless you, and thank you for all that you do."

Dal seguente report, emerge come i principali clienti siano agenzie governative americane (87% dei ricavi proviene dai servizi resi a loro); dopodiché seguendo l'ordine dettato dall'incidenza nei ricavi, vi sono i clienti commerciali tra cui emergono alcuni dei colossi mondiali con un'incidenza del 9%, ed infine i governi stranieri e le NGOs, con un'incidenza del 4%.

Figura 14 I clienti (da Constellis Overview)

I VANTAGGI COMPETITIVI

Complessivamente è possibile dedurre che la posizione competitiva del gruppo derivi da una serie di scelte strategiche che avevano proprio l'obiettivo di renderla Leader del settore.

In particolare, le molteplici acquisizioni di aziende specializzate in diversi business del settore, hanno permesso di mettere in piedi a livello di gruppo una grande impresa che le consente di offrire una gamma di servizi diversificata a livello complessivo, ma altamente specializzata a livello di singola area di business.

Inoltre, un altro notevole punto di forza è quello derivante dalle relazioni a lungo termine (e di vecchia data) costruite con gli enti governativi e commerciali, e dall'approvvigionamento di licenze dal governo degli Stati Uniti insieme alla concessione di garanzie di sicurezza per i loro agenti.

Infine, una particolare caratteristica dei loro servizi che può rappresentare un vantaggio competitivo, è quella dell'indipendenza in termini di tempistica dall'operato delle forze militari, vale a dire che la loro attività non dipende dall' OPTEMPO[17] militare, risultando così più reattiva.

LA RICETTA PER IL SUCCESSO

Il gruppo ritiene che il proprio successo sia da ricercare nella compresenza in uno stesso gruppo dei seguenti fattori:

- STRONG LEADERSHIP: Essi ritengono infatti che una forte leadership sia fondamentale per il successo dell'organizzazione.
- QUALITA'DEI SERVIZI OFFERTI, garantita dall'elevata specializzazione.
- RIGOROSI STANDARD DI ADDESTRAMENTO: essi infatti oltre ad avere nella loro gamma di servizi il training, utilizzano lo stesso per l'addestramento dei loro stessi agenti.
- FLESSIBILITA' nello svolgimento dell'attività, e nell'offerta stessa dei servizi che risultano personalizzabili in vari casi.
- PROFESSIONALITA' intesa sia in termini di rigore e correttezza nel rapporto lavorativo con il cliente, che in termini di qualifiche professionali dei vari membri.
- ESPERIENZA INTERNAZIONALE derivante dal loro ampio raggio d'azione e dalla multietnicità dei loro clienti.
- LEGAMI GOVERNATIVI che come si è detto precedentemente sono alla base del loro vantaggio competitivo.

[17] OPTEMPO: Operational tempo.

CONCLUSIONI

In tale elaborato si è cercato di analizzare il ruolo e il significato dell'attività di intelligence nell'ambito della sicurezza di soggetti fisici e giuridici.

Partendo da un'analisi del sistema di sicurezza della Repubblica predisposto appunto dallo Stato Italiano ed evidenziandone i cambiamenti effettuati per rendere lo stesso adatto alle attuali contingenze, dal mutamento della configurazione interna, alla duplice apertura al modo esterno in un'ottica di trasparenza e di ricerca di personale esterno alle Forze Armate, fino ad arrivare all'esternalizzazione di alcuni servizi di sicurezza, è emersa la centralità dell'attività di intelligence (intesa come ricerca e analisi dei dati) per l'erogazione di tali servizi.

In virtù della realtà odierna, anche le imprese hanno dovuto modificare i loro sistemi di sicurezza, implementandone di nuovi in grado di poterle proteggere da vecchie minacce che, attraverso il progresso tecnologico, hanno assunto nuove vesti e da nuove rischiosità. Si fa perciò riferimento alla cyber security, all'utilizzo della tecnologia come arma e allo stesso tempo come strumento di protezione e prevenzione.

Le aziende possono essere vittime di attacchi di varia natura, conviene loro perciò usufruire della offerta di alcune società di intelligence private, che offrono servizi di protezione/consulenza, oppure dotarsi internamente di uffici in grado di fare lo stesso.

Le società private che operano in questi settori riescono ad erogare servizi altamente specializzati ed è perciò che spesso si preferisce far ricorso a loro anziché predisporre internamente tali funzioni.

A tal proposito sono stati passati in rassegna tutti i servizi principalmente offerti dalle stesse e le competenze richieste alle figure professionali che compongono i loro team. È emerso infatti che i membri di tali società sono ex agenti segreti, ciò spiega la loro elevata esperienza e professionalità nel campo. Tali soggetti, inoltre intrattengono buoni rapporti con i vari governi, elemento che conferisce loro fonti e margini operativi rilevanti per l'attività da essi svolta.

Data l'importanza di questi servizi in un'ottica di tutela e prevenzione, si osserva come intorno all'attività di intelligence sorga un vero e proprio business ad oggi fiorente più che mai.

Tra i principali erogatori di tali servizi è tuttavia possibile fare una distinzione tra

le società che offrono servizi di consulenza/investigazione e quelle che oltre a questi due offrono anche servizi di carattere offensivo. Ovviamente tale diversa configurazione apre le porte a clienti diversi, le compagnie di intelligence rientranti nella prima tipologia erogano servizi principalmente ad imprese, mentre l'operato delle seconde è indirizzato agli Stati.

Queste ultime, definite in generale Private Military Security Companies sono utilizzate da alcuni Governi anche per interventi armati (ad esempio dagli USA), tuttavia nella trattazione si è evidenziata l'ostilità verso questa tipologia di servizi da parte dello Stato Italiano che essendo privo di una normativa specifica in materia, limita il loro utilizzo ad operazioni di carattere non offensivo e straordinario, mediante la predisposizione di norme ad hoc. Tale area, al contrario, risulta all'estero molto utilizzata anche per azioni offensive, in virtù del forte ridimensionamento dei compiti delle Forze Armate nei Paesi in questione.
Per evidenziare le differenze tra queste due macro categorie si è scelto di analizzare due note società: Black Cube e Academi (ex Blackwater del Constellis Group).
La prima offre evidenza dei servizi principalmente richiesti da privati, gode di notorietà per aver investigato per conto di alcune personalità della politica e del mondo dello spettacolo tra cui il presidente Trump.
La seconda invece, nata come una società di erogazione di servizi militari (di carattere offensivo e difensivo), finita più volte in prima pagina soprattutto quando operava sotto il nome di Blackwater, ha esteso oggi i suoi servizi ad una vastità di aree mediante l'acquisizione all'interno del gruppo Constellis di società altamente specializzate in ciascuno di essi.
La tesi ha cercato di evidenziare quelli che possono essere i principali benefici derivanti dall'utilizzo di questi servizi e dall'acquisizione esterna degli stessi. Attraverso la descrizione della struttura organizzativa e delle modalità operative delle intelligence company si evince come in tal ramo il livello di specializzazione del personale e il network posseduto dalla compagnia, giochino un ruolo chiave per l'ottenimento della "best performace".

Le difficoltà riscontrate nello sviluppo interno di organismi in grado di erogare servizi di alta qualità, unite al bisogno di garanzia di un elevato grado di sicurezza da parte di enti pubblici e privati, hanno comportato la nascita e determinano, anche in virtù della lacuna normativa in materia, il crescente sviluppo di quello che è stato definito nell'elaborato come il Business dell'intelligence per la salvaguardia della sicurezza pubblica e industriale.

BIBLIOGRAFIA

- Ahmand S., Schroeder R.G., The impact of human resource management practices on operational performance: recognizing country and industry differences, Published by Elsevier Ltd, 2013.

- Allen T.D., Eby L.T., Lentz E., The role of interpersonal comfort in mentoring relationships, Journal of Career Development, 31, 155–169, 2005.

- Anderson E., Sbannon A.L., Toward a conceptualization of mentoring, 1988.

- Armstrong M., Human Resourse Management, Practice, 2010.

- Axerta Report, dati ONI.

- Bartlett C.A., Ghoshal S., Building Competitive advantage Throught People, 2010.

- Bassetti M., Un Sistema integrato di gestione delle risorse umane, settima edizione, 2007.

- Black Cube society : www.blackcube.com .

- Cardani M., Martone A., Quintarelli L., Tassarotti S., Business Coaching. Una tecnica per migliorare le performance aziendali, Ipsoa, 2008.

- Casalino N., Armenia S., Canini D., A system dynamics approach to the paper dematerialization process in the Italian public administration, in the interdisciplinary aspects of information systems studies, 2008.

- Casalino N., Capriglione A., Draoli M., A Knowledge Management System to Promote and Support Open Government, Proceedings of XIII Workshop di Organizzazione Aziendale - WOA 2012 Desperately seeking performance in organizations, Università degli Studi di Verona, 2012.

- Casalino N., Cavallari M., De Marco M., Gatti M., Taranto G., Defining a Model for Effective e-Government Services and an Inter-organizational Cooperation in Public Sector, Proceedings of 16th International Conference on Enterprise Information Systems - ICEIS 2014, INSTICC, Lisbon, Portugal, vol. 2, pp. 400-408, 2014.

- Casalino N., Ciarlo M., De Marco M., Gatti M., ICT Adoption and Organizational Change. An Innovative Training System on Industrial Automation Systems for enhancing competitiveness of SMEs, Proceedings of 14th International Conference on Enterprise Information Sy-stems - ICEIS 2012, Maciaszek, L., Cuzzocrea, A., Cordeiro, J. (Eds.), INSTICC, Setubal, Portugal, pp. 236-241, 2012.

- Casalino N., D'Atri A., Manev L. (2007), A quality management training system on ISO standards for enhancing competitiveness of SMEs, Proc. 9th International Conference on Enterprise Information Systems - ICEIS 2007, 12-16 giugno, Funchal, Madeira - Portogallo, Cardoso J., Cordero J., Filipe J. Eds., INSTICC, Setubal, Portugal, pp. 229-235.

- Casalino N., D'Atri., Braccini A.M. (2012) A Management Training System on ISO Standards for Organisational Change in SMEs, International Journal of Productivity and Quality Management (IJPQM), Inderscience Publishers, USA, vol. 9 no. 1, pp.25-45.

- Casalino N., Draoli M., Governance and organizational aspects of an experimental groupware in the Italian public administration to support multi-Institutional partnerships, in Information systems: people, organizations, institutions, and technologies, D'Atri, A., De Marco, M. (Eds), ItAIS, Physica-Verlag, Springer, Heidelberg, Germany, pp. 81-89, 2009.

- Casalino N., Draoli M., Martino M., Organizing and Promoting Value Services in Public Sector by a New E-government Approach, Proceedings of XIV Workshop dei Docenti e Ricercatori di Organizzazione Aziendale (WOA 2013), Università La Sapienza, Roma, 2013.

- Casalino N., Gestione del cambiamento e produttività nelle aziende pubbliche. Metodi e strumenti innovativi, volume, pp. 1-201, Cacucci Editore, Bari, 2008.

- Casalino N., Innovazione e organizzazione nella formazione aziendale, pp. 1-212, Collana di Economia Aziendale – Serie Scientifica diretta da Nicola Di Cagno, n.10, Cacucci Editore,

2006.

- Casalino N., Learning to Connect: a training model for public sector on advanced E-Government services and InterOrganizational cooperation, International Journal of Advanced Corporate Learning (iJAC), Austria, 2014, vol. 7, no.1, pp. 24-31

- Casalino, N. Behavioural Additionality and Organizational Impact of Eruopean Policies to Promote Internationalisation of High-growth Innovative SMEs. Journal of International Business and Economics, 2014.

- Casalino, N. (s.d.). Strategia, Progettazione Organizzativa ed Efficacia.

- Ciborra C., Lanzara G.F., Labirinti dell'innovazione. Tecnologia, organizzazione, apprendimento, Milano, Etas libri, 1999.

- Cicchetti A., La progettazione organizzativa, Franco Angeli, Milano, 2004.

- Constellis Group : www.constellis.com .

- Costa G., Nacamulli R., Manuale di Organizzazione Aziendale, UTET, 1996.

- D'Atri A., De Marco M., Casalino N., (Eds), Physica-Verlag, Springer, Heidelberg, Germany.

- Daft R.L. (2017), Organizzazione Aziendale, 5 ed., Maggioli Apogeo.

- ENISA: Threat Landscape 2017;

- Fontana F., Caroli M., Economia e gestione delle imprese, McGraw-Hill, 2013.

- Fontana F., Il sistema organizzativo aziendale, Franco Angeli, 1999.

- Fontana F., Lo sviluppo del personale, Giappichelli, 1994.

- Garvet B., Stokes P., Megginsons D., Coaching and Mentoring: theory and practice, 2014

- Gatewood R.D., Field H.S., Barrick M., Human resource selection, Sixth Edition, 2008.
- Ghazzawi K., Accoumeh A., Critical Success Factors of the E-Recruitment System, Vol. 2, No. 2, pp. 159-170, 2014
- Ghoshal S., Building competitive advantage throught people, 2010
- Gov, sito ufficiale per la tutela della sicurezza nazionale, www.sicurezzanazionale.gov.
- Jones G.R. (2012), Organizzazione. Teoria, progettazione, cambiamento, Egea.
- Kaggle Inc.: The home of data science. (www.kaggle.com) (2014).
- Management delle informazioni aziendali. Pearson (2005).
- Manfredi G., "Alleanza strategica tra intelligence e universita' ", GNOSIS Rivista di Intelligence.
- Marchetti E. "Private Military and Security companies: il caso italiano nel contesto internazionale", Edizioni Nuova Cultura; Quaderni di IAI.
- Marro, E. (2017). Nuove tecnologie e lavoro, la chiave del successo è l'istruzione. Il Sole 24Ore.
- Melissa A. Schilling, F. I. (2017). Gestione dell'innovazione (quarta ed.). Milano: McGraw-Hill.
- Ministero dello Sviluppo Economico. (2017). Piano Nazionale Industria 4.0.
- Morano C. P., "Cyber security, intrusion detection systems e intelligenza artificiale" .
- Nascio: Data Governance Part II: Maturity Models - A Path to Progress, USA (2009).

- Pfeffer J., Seven practices of successful organizations, California Management, 1998

- Radicchi, D. (2014). Cultura d'impresa e gestione del cambiamento: analisi e riorientamento dei valori e della cultura organizzativa. Tratto da https://www.unistrapg.it/sites/default/files/docs/university-press/gentes/gentes-2014-1-135.pdf

- Relazione Parlamentare 2017.

- Rogers, D.: The network is your customer: 5 strategies do thrive in a digital age. Yale University Press, UK (2011).

- Russom, P.: The Four Imperatives of Data Governance Maturity. TDWI Monograph (2008).

- Varvelli, R. (2004). Innovazione tecnologica e innovazione organizzativa. Organizzazione aziendale.