# Corporate Intelligence

## Aziende e attività informative nel mercato globale

Alessandro Vivaldi

### Profilo dell'Autore

Alessandro Vivaldi è antropologo e storico delle religioni, dottore magistrale presso le università di Roma "Sapienza" (2015) e Roma "Tor Vergata" (2005). Ha prestato servizio nell'Esercito tra il 2001 e 2004 come Volontario e successivamente Riservista, venendo impiegato con la Brigata Meccanizzata "Granatieri di Sardegna" come Addetto alla Situazione Operativa nell'Operazione Joint Guardian (KFOR). Dal 2012 al 2018 è stato Chief Intelligence Officer e Senior Consultant di *Agatòs Syntagma*, firm di consulenza di Corporate Security, per la quale ha curato progetti in alcune delle maggiori aziende italiane ed europee. Dal 2019 dirige la propria start-up focalizzata sulla consulenza di Intelligence, *Intellego – Conoscere per decidere*. Nello stesso anno diventa Vicepresidente della Syrian Italian Networking Association, associazione che ha lo scopo di ricostituire i legami commerciali tra Italia e Siria.

### Abstract

Il *paper* affronta l'attuale situazione strategica e operativa globale in cui si devono muovere le aziende italiane, non solo le grandi controllate e le quotate, ma anche le PMI, e le potenziali necessità informative che possano garantire a esse non solo la costante protezione e tutela del patrimonio (solido e astratto), ma anche e soprattutto dei sostanziali vantaggi competitivi rispetto ai *competitor* nazionali e internazionali. In particolare viene affrontata la necessità di una riorganizzazione delle attività informative sotto il profilo di una funzione sviluppata *ad hoc*.

### Keywords:

Intelligence, Corporate, Aziende, Geopolitica, Geoeconomia, Analisi.

### Introduzione: il tessuto produttivo italiano di fronte ai contesti globali.

Secondo uno studio di Prometeia pubblicato da Infodata – Il Sole 24 Ore, "le piccole e medie imprese, qui definite come imprese attive con un giro d'affari inferiore a 50 milioni di euro, impiegano l'82% dei lavoratori in Italia (ben oltre la media Ue) e rappresentano il 92% delle imprese attive (dai calcoli sono escluse imprese dormienti con fatturato a zero nell'ultimo anno). Sono numeri che fanno delle PMI un tratto saliente dell'economia italiana e riflettono tradizioni e imprenditorialità diffuse nei territori. […] L'impatto economico delle Pmi non può peraltro essere valutato considerando semplicemente il loro coinvolgimento diretto, ma va letto in chiave di filiera. Anche le Pmi italiane fanno ormai parte di catene del valore complesse e globali"[1]. Significa, nella sostanza, che ognuna di queste imprese si trova

ad agire in un contesto complesso frutto della globalizzazione, diversamente da ciò che poteva avvenire nel secolo scorso, in cui l'esposizione globale era per lo più appannaggio delle grandi aziende e in particolar modo (ma non esclusivamente) di quelle che oggi chiamiamo "grandi controllate di Stato" o di specifici settori produttivi (il petrolchimico e il metalmeccanico per fare due esempi). La globalizzazione stessa è cambiata negli ultimi 20 anni del nuovo millennio: se una volta poteva essere definita come "*a variety of economic, cultural, social, and political changes that have shaped the world over the past 50-odd years, from the much-celebrated devolution in information technology to the diminishing of National and geo-politicl boundaries in an ever-expanding, transnational movement of goods, services and capital. The increasing homogenisation of consumer tastes, the consolidation and expansion of corporate power, sharp increases in wealth and poverty, the McDonaldisation of food and culture and the growin ubiquity of liberal democratic ideas are all, in one way or another, attributed to globalisation*"[2], oggi essa non può più rispondere a una definizione semplicistica, accompagnata com'è dal fenomeno della *glocalizzazione*, ovvero la presenza irriducibile di istanze interpretative locali delle spinte globali – siano esse religiose, culturali, sociali o economiche (la finanza islamica, il sistema economico cinese, il terrorismo islamico, l'utilizzo di droni civili nella guerra in Siria sono tutti esempi calzanti)[3].

L'intersecarsi di queste due spinte (globale e locale) ha portato la società e con essa i mercati contemporanei a strutturarsi come un sistema complesso adattivo, con la tipica forma a rete, nel quale entrano in gioco strutture concettuali come la *teoria del caos*, l'*effetto farfalla*, e in generale la nozione che minime variabili, anche impercettibili, in una parte del sistema, ancorché apparentemente periferica e priva di importanza, possano condurre a cambiamenti anche traumatici in tutto il sistema stesso, come ampiamente dimostrato per esempio dalle recenti analisi sui danni economici derivanti dal coronavirus (COVID-19)[4].

In questo sistema gli attori non sono più solo gli stati nazionali, le organizzazioni internazionali e le aziende di dimensioni globali (che per produzione oramai superano anche piccoli stati), ma anche le medie e piccole aziende che, per tipologia di prodotto o mercato di destinazione, hanno una esposizione che oltrepassa i confini originari e arriva perfino in contesti esotici impensabili fino a 10 anni fa. Non è solo il caso di produttori di software (che per peculiarità propria del prodotto possono lavorare da remoto), né dei classici marchi della moda e del lusso: si tratta anche e soprattutto di produttori di piccola meccanica (dalla componentistica specializzata di alta precisione alla produzione di macchinari industriali per il tessile o l'etichettatura, solo per menzionarne alcuni), di prodotti (e competenze) specifici per la bonifica e l'idraulica, costruttori e specialisti nel petrolchimico, etc.. Tutti questi micro attori di calibro internazionale, ancorché sconosciuti al di fuori del pubblico specializzato, sono esposti a tutte le intemperie globali, le quali di volta in volta possono comportare tante minacce quante opportunità, alle quali però non sempre possono far fronte per motivazioni che vanno dalla

mancanza di una struttura organizzativa adeguata alla carenza di una governance sufficientemente in linea con i grandi cambiamenti del contesto globale: non è un caso KPMG abbia affrontato un argomento simile in una sua pubblicazione, toccando la necessità, per le aziende, di un CEO come *Geopolitical officer*[5].

**Corporate Intelligence: stato dell'arte.**

La maggior parte degli specialisti di intelligence provenienti dall'ambito istituzionale tende a definire l'intelligence sulla base dell'ente di provenienza. Viene infatti definita spesso in base al decisore che ne richiede le analisi, quindi spesso e volentieri un attore statale, non necessariamente in relazione a nemici specifici (quindi l'intelligence come sicurezza nazionale); tali definizioni sono già troppo "chiuse" per il fine del presente paper. Converrà quindi partire dalla definizione data da Wheaton e Beerbower: "*Intelligence, then, is a process, focused externally and using information from all available sources, that is designed to reduce the level of uncertainty for a decisionmaker*[6]". Per quanto apparentemente neutra, è necessario partire da questa definizione per delineare di cosa dovrebbe trattare la Corporate Intelligence e in cosa differisce dall'intelligence più propriamente istituzionale. Definire a chi è destinata l'intelligence aziendale può aiutarci a delimitare il campo: *la corporate intelligence è il processo che usa le informazioni disponibili da ogni fonte al fine di ridurre il livello di incertezza per il management aziendale*. Abbiamo in questa versione definito il decisore (il management) e rimosso la limitazione del *focused externally* per includere due delle più comuni versioni (parziali) dell'intelligence aziendale, invero la *business intelligence* e la *competitive intelligence*, le quali non sono affatto esclusivamente focalizzate esternamente. Tuttavia questa definizione raggiunta è parzialmente scorretta, poiché esistono specifici limiti alle informazioni utilizzabili da parte di un ente privato quale un'azienda, limiti definiti nei quadri del diritto nazionale e internazionale in cui l'azienda opera; la nostra definizione quindi necessita di ulteriore apposita specifica: *la Corporate Intelligence è il processo che usa le informazioni legalmente disponibili da ogni fonte al fine di ridurre il livello di incertezza per il management aziendale.* Il vantaggio di una tale definizione è che essa non presenta – rispetto alle controparti istituzionali – il termine *sicurezza*, il quale, oltre a determinare nell'ambito dello Stato quale sia il ruolo dell'intelligence, ne determina anche il rientro nel quadro costituzionale (in particolare quello italiano) che ne delimita gli ambiti più prettamente "offensivi": tale limite non si pone nel contesto aziendale, che per propria natura si fonde su una competizione (ancorché iscritta nel quadro del diritto) in cui la capacità di aggredire (il mercato, ad esempio) e di cogliere spunti strategici e operativi di tipo offensivo è imprescindibile.

Quanto detto fin'ora è stato ampiamente sottolineato dalla Lewis, del *Global Intelligence and Threat Analysis Team* della Walt Disney Company: "*Wheter we think about suplly chains, global markets, multinational partnerships or International technology platforms, the impact of geopolitics and the dynamic pace of business on companies*

*– large and small – have increased in scope such that having an intelligence capability has become integral to strategic decision-making. In many companies, this capability helps to forecast key trends that could impact a business's bottom line or mitigate personal security or brand risks; in others, it serves as a strategic advantage across sectors: identifying new markets limiting liabilities, and enabling decision-makers to direct operations with greater insight. In this context, as the cadre of professionals in the private sector intelligence arena continue sto grow, the profile of those who have the necessary skills to be successful in the field continues to evolve, as well. Moreover, given the number of sub-fields within this genre (including technical, protective, business, and geopolitical), many organisations benefit from these intelligence professionals' work. Technology firms, the oil and gas sector, media and entertainment conglomerates, startups, restaurants, hospitality organisations, and non profit businesses have all expanded to utilize private sector intelligence in their strategic decision-making*"[7]. Il punto di vista della Lewis è ovviamente quello di una manager americana, che ha davanti agli occhi una situazione tendenzialmente evoluta del campo rispetto a quanto non avvenga in Europa e in particolar modo in Italia. L'attuale situazione nazionale vede infatti quello che potremmo chiamare *intelligence management* schiacciato tre due pilastri tradizionali: quello commerciale della *business intelligence* e quello "difensivo" della *security*. Se il primo di per sé comporta un limite collaterale minimo, essendo troppo specifico e "interno" all'area commerciale, il secondo pilastro, quello della tutela del patrimonio aziendale, ha storicamente comportato una compressione sia del campo d'azione della Corporate Intelligence che delle competenze necessarie per svolgerla al meglio. La delimitazione del campo nasce certamente dalla tradizione della security italiana, storicamente "nata" con la necessità di proteggere le grandi famiglie di imprenditori, svolta da personale precedentemente in servizio presso le Istituzioni. *Mutatis mutandis*, l'intelligence si è sovrapposta all'investigazione (e alla protezione fisica di persone e strutture), e le sue competenze sembrano essere diventate comuni a chiunque abbia servito con l'una o con l'altra divisa. Ovviamente ciò non corrisponde al vero (essendo l'intelligence una branca specifica sia nell'ambito militare che civile, richiedente un'altrettanto specifica formazione), e intelligence e security rimangono campi attigui, comunicanti e cooperanti, ma non sovrapposti, così come non sono necessariamente sovrapponibili le competenze necessarie per svolgere al meglio l'una piuttosto che l'altra.

Come già sottinteso esistono in quasi tutte le aziende, di qualsivoglia dimensioni, delle attività di intelligence, anche quando non individuata come tale: stando a quanto citato della Lewis, possiamo asserire che l'intelligence aziendale corrisponde in un certo qual modo ai cinque sensi dell'azienda, permettendole di muoversi nel contesto in cui opera. Tuttavia tali funzioni permangono separate e quasi mai strutturate su un'organizzazione aziendale *ad hoc*, risultando quindi in un meccanismo tutt'altro che perfetto e spesso espletato da una singola persona nelle aziende di medie e piccole dimensioni, sia esso l'Amministratore Delegato, il Direttore Generale o chi per lui, il quale di volta in volta delega *request for information* o *intelligence requirements* a specifiche unità.

Per quanto concerne sempre quanto già si fa, nell'ambito della security l'intelligence vede due applicazioni in particolare: da una parte la valutazione delle informazioni economico finanziarie di terze parti, soprattutto in contesto *due diligence* (attività svolta da appositi fornitori per quanto previsto dal Testo unico delle leggi di pubblica sicurezza e derivati), e dall'altra la gestione delle informazioni necessarie per l'espletamento delle policy di Travel Security. In quest'ultimo ambito è necessario specificare che la parte più prettamente di intelligence dovrebbe essere ciò che anticipa il rischio e ne valuta la potenziale evoluzione, ovvero le cosiddette "schede paese", nella realtà dei fatti ridotte per lo più a una dozzina di pagine di informazioni base quasi irrilevanti sul paese di destinazione. Diverso è sviluppare un serio sistema di indicatori che possono anticipare il rischio e quindi servire a mitigarlo (l'altra parte dell'attività di Travel Security, concernente i cosiddetti *feed* cioè la ricezione in tempo reale degli eventi a livello globale, permettendo le necessarie contromisure, tocca solo di striscio l'intelligence e ricade totalmente nell'operatività della security, la quale tuttavia dovrebbe rifarsi all'intelligence in fase di pianificazione ed espletamento delle contromisure stesse, quali evacuazione, protezione del personale e simili, attività la cui preparazione dovrebbe prevedere quella che in gergo tecnico si chiama *Urban Intelligence Preparation of the Battlefield*, che ancorché di derivazione prettamente militare, ben si adatta all'attività di cui sopra, in questa versione tuttavia sconosciuta alle attuali Policies di Travel Security presenti nelle aziende italiane).

Alla data attuale le *Private Intelligence Companies* e le unità di analisi in Italia si contano nell'ordine di una manciata, diversamente da quanto accade nel mondo anglosassone e francofono. Quando esistono, sono state limitate a funzioni specifiche (la brand reputation o la travel security), o spesso mancano di svolgere la loro effettiva funzione: "*to develop a deep understanding of a specific business issue with the intent of developing strategy-relevant insights, action possibilities, and recommendations that add a significant value to decision making*"[8]. Va soprattutto rilevato che il "tempo dell'intelligence" è prima di un dato evento (sia esso rischio o opportunità). Tutto ciò che viene dopo o non è intelligence o è intelligence con l'orizzonte di un nuovo evento: in entrambi i casi, considerato ad esempio gli eventi "rapimento di un manager" o "comunicazione del brand errata rispetto alla cultura locale", l'intelligence è tutto ciò che c'è prima, mentre tutto ciò che viene dopo è tendenzialmente security reattiva, con la sola vistosa eccezione di pratiche volte a implementare un miglior processo di intelligence per i tempi a venire.

Vista con piglio maggiormente strategico, la Corporate Intelligence di matrice italiana manca soprattutto di visioni larghe. Manca cioè la capacità di rispondere a quanto espresso da Duncan Wales, CEO di Exotix: *"Investors today are confronted with a dramatic increase in the political risk profile of what were supposedly low-risk, or indeed risk-free, developed markets. A dozen years ago it seemed geopolitical risk was a thing of the past, and that the apparent dominance of the liberal economic and political model had indie heralded the end of history. Now geopolitical risk has returned as a great shadow on the horizon of all significant investment decisions*"[9]. Tale

funzione in Italia è in parte assolta da istituzioni e società controllate (MAECI, MISE, SACE-SIMEST, ICE), in parte dai think tank di geopolitica: tuttavia, se nel primo caso si può parlare di *basic intelligence* (e quindi non sufficientemente approfondita, come nel caso delle citate schede paese), nel secondo è evidente la carenza di informazioni di base provenienti dal territorio, l'approccio molto accademico e poco pratico (manca in sostanza il reale "polso" della situazione e una vera e propria *situation awareness*). In entrambi i casi manca soprattutto la metodologia propria dell'intelligence, che è e rimane un insieme di processi specifici fondati sul ciclo di intelligence, insieme che richiede una sapiente applicazione (e ancor prima una formazione), tutt'altro che scontata.

**Corporate Intelligence: principi, potenziale organizzazione e competenze.**

Allo stato attuale già l'ambito della security soffre in Italia un sottodimensionamento, dovuto sia alla mancanza di cultura manageriale propria sia all'ambito che al management italiano in generale, sia al fatto che essa, come anche l'intelligence, è un'attività di supporto al business e alle operazioni che non può essere misurata con i classici indicatori imprenditoriali quali, ad esempio, KPI (Key Performance Indicator) e ROI (Return on Investment), venendo quindi sviluppata solo quando vi è uno stimolo esterno basato sulla necessità di adattamento, cioè il dovere di essere *compliant* con specifiche normative. Attualmente circa una dozzina delle corporate maggiori presenti sul territorio nazionale hanno nella propria organizzazione una funzione di security di livello dirigenziale indipendente da altre direzioni (sono i cosiddetti *vicepresident security*, o *chief security officer*), mentre le restanti pongono il ruolo sotto il più o meno diretto controllo delle direzioni HR o HSE. In alcuni casi anche le attività di controllo in fase di due diligence e di brand reputation di terze parte viene asportato dalla funzione security e spostato verso le unità logistiche o quelle adibite alla normale gestione dei fornitori (Acquisti). Ne consegue che non solo non siano per lo più previste figure come un *intelligence officer* e conseguente unità operativa, ma nella maggior parte dei casi anche che le funzioni imprescindibili di intelligence già presenti siano spezzettate tra più divisioni aziendali, violando uno dei principi fondanti dell'attività informativa, cioè la sua centralizzazione al fine di garantirne l'efficienza (anche in fase di distribuzione delle analisi).

Per capire quanto la funzione sia potenzialmente importante – non solo nell'ambito difensivo della security, ma anche in quello del supporto alle operazioni "offensive" proprie delle imprese – possiamo appoggiarci sui tre stadi evolutivi della Corporate Intelligence proposti dalla Widhalm e da Lunardi[10]. Secondo tale modello, la funzione dovrebbe partire dall'attuale stato dell'arte, quello cioè di funzione di security, per diventare una più ampia intelligence prescrittiva, a supporto di tutte le operazioni inerenti la tutela del patrimonio. In tale stadio i maggiori utilizzatori dell'intelligence sono gli addetti di security a ogni livello, e lo scopo primario è quello di supportare le policies e le operazioni di security. Lo stadio successivo è la *risk intelligence*, e prevede un ampliamento dell'orizzonte verso una prima forma di

intelligence strategica, attraverso l'analisi dei contesti operativi e dei rischi geopolitici (ciò che attualmente avviene in alcune aziende italiane sotto la direzione dei rapporti istituzionali internazionali). A questo punto la funzione dovrebbe rivolgersi a utilizzatori al di fuori dell'ambito security, cercando di cogliere le necessità informative di altre funzioni aziendali quali la *supply chain*, il *product development*, il *retail*, la comunicazione, etc.. Tuttavia questo stadio, anche se al di là della security, ricade ancora sotto il concetto di *risk management*: pur considerando il rischio sotto un punto di vista più ampio rispetto al solo rischio di security, essa permane come attività puramente difensiva rivolta alla mitigazione dei rischi e alla previsione delle minacce. Il modello auspica quindi un terzo stadio evolutivo, la cosiddetta *opportunity intelligence*: essa si muove sul piano soprattutto strategico (diversamente dalla prescrittiva, tendenzialmente pertinente al livello tattico, e la risk intelligence, che afferisce per lo più al livello operativo), con lo scopo di potenziare la capacità dell'azienda di individuare non solo i rischi, ma anche e soprattutto le potenziali opportunità. Nello specifico, essa si fonda sull'intelligence nella sua forma più essenziale, invero **dare informazioni predittive di valore per permettere all'organizzazione aziendale e ai suoi decisori di intraprendere una strategia decisionale efficiente, flessibile e di vantaggio competitivo.**

Ovviamente una tale evoluzione richiede dei paletti ben precisi che differiscono in base all'azienda, in particolar modo - *ça va sans dire* – in base al budget a disposizione. Implementare una nuova funzione aziendale per una Corporate è relativamente semplice, diverso è invece per le PMI che già stentano ad avere una funzione di security; in quest'ultimo caso tuttavia la soluzione più agile è l'*outsourcing* attraverso società di consulenze e servizi, cosa che già avviene nell'ambito della Travel Security, e che è già previsto nello studio della Robson sul tema dell'intelligence privata[11].

Diversamente, le aziende più grandi necessitano di una funzione che sia al tempo stesso in grado di comunicare con tutti gli stakeholders (interni ed esterni), di recepirne le necessità informative e di diffondere in modo efficiente le risposte alle stesse (ovviamente sulla base del principio del *need to know*).

Al fine di garantire tale funzionalità, una ipotetica direzione di Corporate Intelligence deve essere gerarchicamente alle dipendenze dirette del decisore strategico (Amministratore Delegato o Direttore Generale) e rispondere funzionalmente a tutte le necessità informative delle altre direzioni (intese come decisori ai livelli operativi e tattici), inclusa la Corporate Security, relazioni/comunicazioni che possono essere garantite istituendo dei "presidi" (intesi come una persona formata appositamente) che presso ogni direzione funga da punto di contatto (un "traduttore") con la Corporate Intelligence.

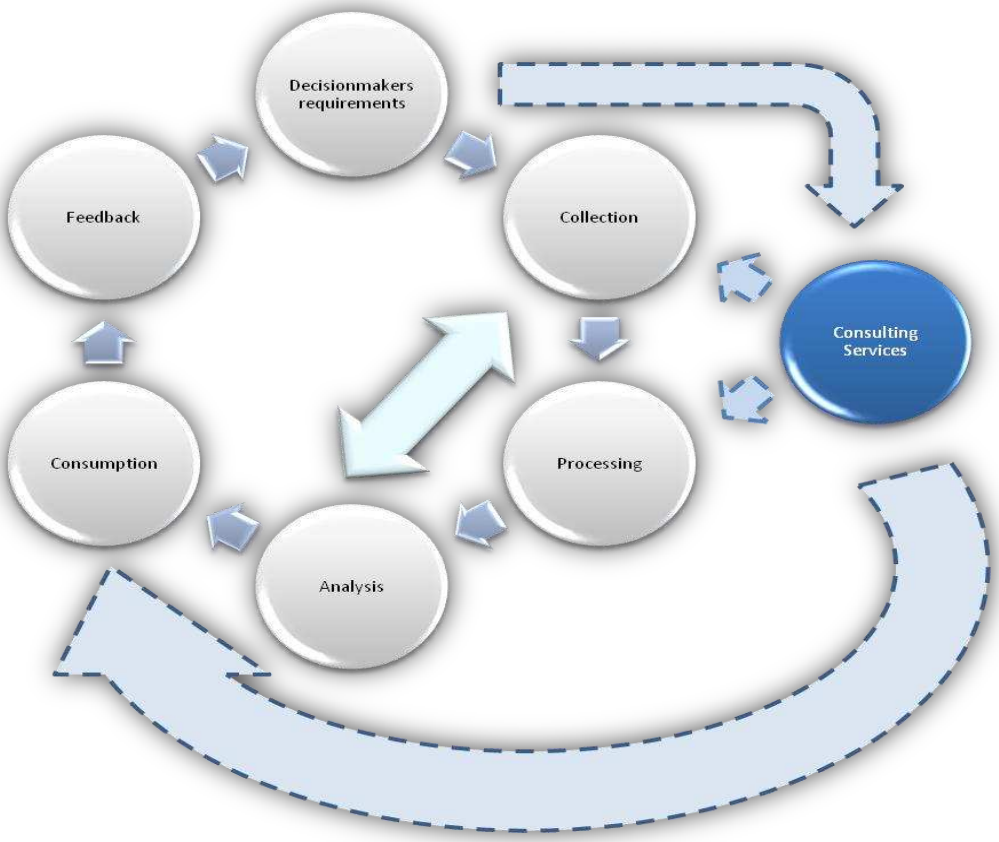


**Figura 1:** ***Adaptation of the Intelligence Cyble for the Private Sector, including Consulting Firms*** **- rielaborazione dall'originale di Maria A. Robson**

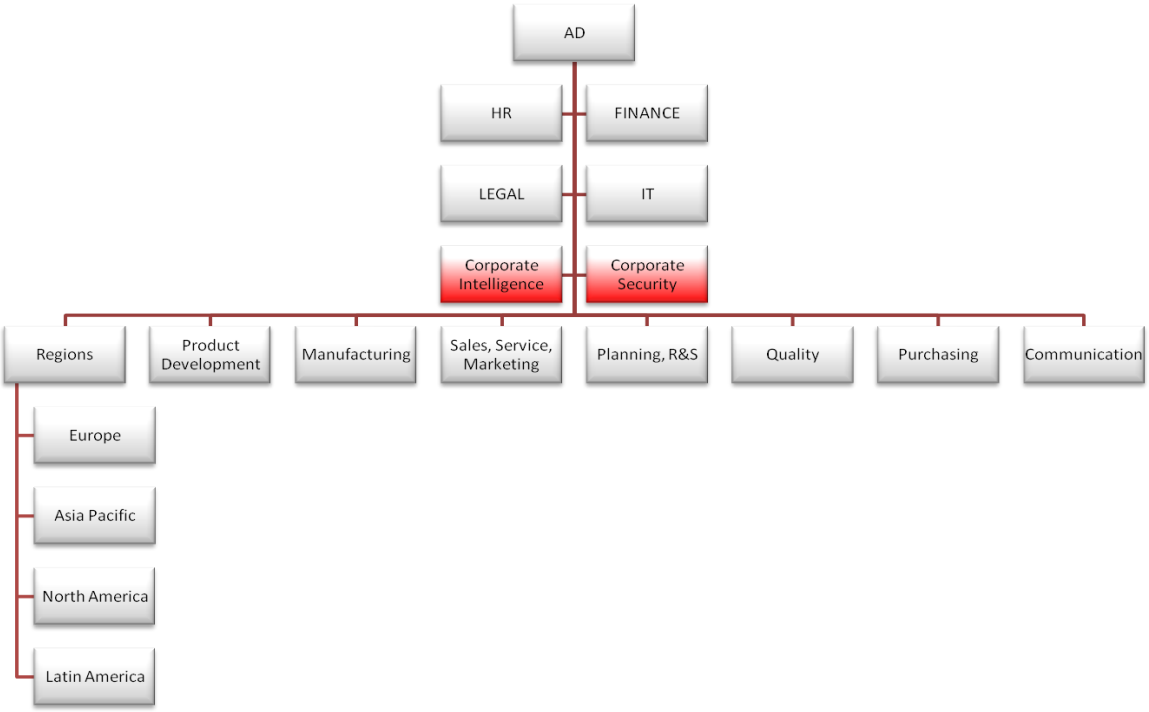


**Figura 2: Rielaborazione dell'organigramma funzionale di General Motor presente in Costa, Gubitta e Pittino, 2013. Sono state aggiunte le funzioni in rosso.**

Su questa struttura si devono poi costruire due pilastri fondanti una funzione efficiente: la selezione del personale da una parte, e la creazione di processi standardizzati (ma non soffocanti) che agevolino – oltre il normale svolgimento delle attività di intelligence intorno al ciclo – la comunicazione tra la Corporate Intelligence e gli stakeholders, in particolare assicurando la corretta formulazione e ricezione degli *intelligence requirements* e l'efficiente diffusione/distribuzione delle risposte generate. Entrambi questi pilastri a loro volta si fondano sulla formazione del personale che costituisce la funzione. Allo stato attuale l'Italia, rispetto sia ad altri stati europei che ai maggiori competitor extra europei, è sostanzialmente indietro: gli *intelligence studies* a livello universitario scarseggiano, con poche vistose eccezioni su cui spicca l'Università della Calabria. In generale la formazione universitaria verte sulle relazioni internazionali e la global security, mentre quella post universitaria sulla homeland security o sul security management. In entrambi i casi sono quasi completamente assenti sia un approccio olistico e multidisciplinare all'intelligence – giustamente supportato dal lavoro di Mario Caligiuri e UniCalabria -, sia un approccio pratico e pragmatico alle metodologie di ricerca, processo e analisi delle informazioni (quindi l'attività pratica professionalizzante, la quale però deve basarsi su una capacità di costante studio a 360°: non per niente la Lewis nel già citato paper batte moltissimo sulla necessità, per gli analisti, di essere dotati anzitutto di *intellectual curiosity*, alla quale deve affiancarsi, aggiungeremmo, una dose massiccia di *critical thinking*, entrambe generalmente più semplici da trovare in chi proviene dalle scienze umane/sociali che non in chi proviene dalle aree più prettamente tecniche o afferenti alle scienze dure).

**Conclusioni**

Il campo degli *Intelligence studies* si sta rapidamente evolvendo, a livello globale. Come tutti i campi di studio giovani e figli di un approccio olistico e molto vicino alla Teoria della Complessità, tende ad affrontare in contemporanea una miriade di definizioni problematiche e delimitazioni di campo, accentrando i propri studi intorno a specifici centri accademici (UniCalabria in Italia, il Research Institute for European and American Studies in Grecia, l'EUISS a livello UE, etc.), e solo pochissimi di essi (il RIEAS in primis) hanno cominciato una seria attività di discussione sulla *private sector intelligence*, che se per metodi e teorie rientra a pieno titolo nell'intelligence, al tempo stesso si discosta per limiti e scopi dall'intelligence intesa come sicurezza nazionale. Ed è proprio in questo campo che l'Italia è in deficit sia di professionisti che di formatori e studenti, nonché, punto ancora più debole, di decisori che ne capiscano la portata rivoluzionaria per le aziende esposte globalmente.

Lo sviluppo sia di funzioni di Corporate Intelligence nelle aziende che di una *Intelligence community* che non si focalizzi solo sulla sicurezza nazionale (che è e deve essere appannaggio delle istituzioni), ma si estenda al "sistema Paese" inteso anche come sistema di produzione che necessita di cogliere in anticipo dei vantaggi competitivi, è *conditio sine qua non*, non solo per difendere gli interessi del paese e il

suo patrimonio (anche e soprattutto astratto: know how e dati), ma soprattutto per renderlo progressivamente più competitivo attraverso la possibilità di cogliere, creare, intercettare costantemente nuove opportunità a discapito dei maggiori competitor internazionali.

## Bibliografia


M. CALIGIURI (a cura di), *Intelligence e scienze umane*, Rubettino, Soveria Mannelli 2016.

P. GUBITTA, G. COSTA, D. PITTINO, *Organizzazione aziendale*, McGraw Hill Education, Milano 2013.

S. GUTTAL, *Globalisation*, in *Development in practice*, Volume 17, Numeri 4-5, Taylor&Francis, Abigdon (UK) Agosto 2007.

KPMG - The Eurasia Group, *The CEO as Chief Geopolitical Officer*, Marzo 2018, s.l., ultimo accesso 11 Febbraio 2020 <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/the-ceo-as-chief-geopolitical-officer.pdf>, 2018.

E. MORIN, *Introduzione al pensiero complesso*, Sperling & Kupfer, Milano, 1993.

C. K. SHARMA, *Emerging Dimensions of Decentralisation. Debate in the Age of Globalisation,* Indian Journal of Federal Studies 1/2009, ultimo accesso 4 Febbraio 2020, <ttp://dx.doi.org/10.2139/ssrn.1369943> s.l. 2009.

RIEAS, *Journal of European and american Intelligence Studies*, Vol. 1, No. 2, Atene, Dicembre 2018.

V. ROUDOMETOF, *Glocalization: A Critical Introduction*, Routledge, New York 2016.

M. Trentini, *Rischio e società*, Carocci, Roma 2006.

A. VALLEGA, *Geografia culturale: luoghi, spazi, simboli,* UTET, Torino 2003.

G. E. VALORI, *Intelligence e Geopolitica*, Rubettino, Soveria Mannelli, 2015

K. J. WHEATON, M. T. BEERBOWER, *Towards a new definition of intelligence*, in *Stanford Law and Policy Review*, Vol. 17, , ultimo accesso 11 Febbraio 2020 <https://law.stanford.edu/wp-content/uploads/2018/03/wheaton_beerbower_319.pdf>, Stanford 2006.


---

[1] *PMI, quanto conta in Italia il 92% delle aziende attive sul territorio?,* Il Sole 24 Ore, Milano, 10 Luglio 2019, ultimo accesso 4 Febbraio 2020, <https://www.infodata.ilsole24ore.com/2019/07/10/40229/>.

[2] S. GUTTAL, *Globalisation*, in *Development in practice*, Volume 17, Numeri 4-5, Agosto 2007, Taylor&Francis, Abigdon (UK), pag. 523.

[3] Il concetto di glocalizzazione è oggi dibattuto ancor di più di quello di globalizzazione. Per una disamina della storia del concetto, si veda C. K. SHARMA, *Emerging Dimensions of Decentralisation. Debate in the Age of Globalisation,* Indian Journal of Federal Studies 1/2009, s.l. 2009, pag. 47-65, ultimo accesso 4 Febbraio 2020, <ttp://dx.doi.org/10.2139/ssrn.1369943>; per una revisione critica e maggiormente aggiornata sul piano multidisciplinare, V. ROUDOMETOF, *Glocalization: A Critical Introduction*, Routledge, New York 2016.

[4] M. MARCHESANO, *Coronavirus, S&P vede il picco ad Aprile ed è una buona notizia,* Il Foglio, 6 Febbraio 2020, s.l., ultimo accesso 7 Febbraio 2020 <https://www.ilfoglio.it/economia/2020/02/06/news/coronavirus-s-p-vede-il-picco-ad-aprile-ed-e-una-buona-notizia-300449>; F. MASSARO, *Coronavirus, in Cina crolla la domanda di petrolio, industria ferma*, Il Corriere della Sera, 3 Febbraio 2020, s.l., ultimo accesso 7 Febbraio 2020 <https://www.corriere.it/economia/finanza/20_febbraio_03/coronavirus-cina-crolla-domanda-petrolio-industria-ferma-e8c36e1e-4671-11ea-afe7-221784afa655.shtml>.

[5] KPMG - The Eurasia Group, *The CEO as Chief Geopolitical Officer*, Marzo 2018, s.l., ultimo accesso 11 Febbraio 2020 <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/the-ceo-as-chief-geopolitical-officer.pdf>.

[6] La definizione è tratta da K. J. WHEATON, M. T. BEERBOWER, *Towards a new definition of intelligence*, in *Stanford Law and Policy Review*, Vol. 17, Stanford 2006, ultimo accesso 11 Febbraio 2020 <https://law.stanford.edu/wp-content/uploads/2018/03/wheaton_beerbower_319.pdf>; la definizione viene adottata nel presente paper al fine di partire da un minimo comun denominatore di tutte le definizioni di intelligence, per altro esaminate nel documento citato, applicabile in ambito corporate.

[7] A. LEWIS, *The profile of a successful private sector intelligence analyst,* in *Journal of European and american Intelligence Studies*, Vol. 1, No. 2, pag. 66, Atene, Dicembre 2018.

[8] L. FAHEY, J. HERRING, *Intelligence teams*, in *Strategy&Leadership,* Vol. 35, no. 1, Emerald Publishing, Bingley 2007, pag. 14.

[9] Citato in KPMG – The Eurasia Group, *op. cit.*, pag. 4.

[10] K. WIDHALM, T. J. LUNARDI, *From prescription to opportunity: an evolutionary model for Corporate Intelligence*, in *Journal of European and american Intelligence Studies*, Vol. 1, No. 2, pagg. 49 - 64, Atene, Dicembre 2018.

[11] M. A. ROBSON, *Risk Analysis beyond government agencies: conceptualizing private sector intelligence*, in *Journal of European and american Intelligence Studies*, Vol. 1, No. 2, pagg. 31 - 48, Atene, Dicembre 2018.