



**ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI**

**Controinformazione:
la protezione dei processi decisionali
del Sistema-Paese**

Mario Mori

RESEARCH PAPER
Settembre 2016

**ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI**

www.fondazionegermani.org

L'Istituto Gino Germani, un ente senza fini di lucro costituito a Roma nel 1981 ha lo scopo di promuovere una sempre maggiore sinergia tra le scienze sociali e gli studi strategici.

L'Istituto svolge, in collaborazione con centri di ricerca, Istituzioni accademiche e organismi governativi in Italia e all'estero, attività di studio e ricerca interdisciplinare sui processi di modernizzazione e globalizzazione nel mondo contemporaneo.

L'Istituto dedica particolare attenzione all'analisi dei problemi dello sviluppo socio-economico, della democrazia e dell'autoritarismo, della sicurezza e della conflittualità nelle società contemporanee.

Mario Mori è un generale dei Carabinieri che tra l'altro ha comandato il Gruppo Carabinieri di Palermo, il Raggruppamento Operativo Speciale (ROS), la Scuola Ufficiali Carabinieri, la Regione Carabinieri Lombardia ed ha diretto il SISDE dal 2001 al 2006 venendo nominato prefetto della Repubblica. Recentemente ha scritto un libro sui Servizi segreti.

**ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI**

**CONTROINFORMAZIONE:
LA PROTEZIONE DEI PROCESSI DECISIONALI
DEL SISTEMA-PAESE**

Mario Mori

RESEARCH PAPER
Settembre 2016

Le opinioni espresse sono strettamente personali e non riflettono necessariamente le posizioni dell'Istituto Gino Germani.

© 2016 Istituto Gino Germani di Scienze Sociali e Studi Strategici
ISBN: 978-88-909073-2-6

ISTITUTO GINO GERMANI DI SCIENZE SOCIALI E STUDI STRATEGICI
PRESSO LINK CAMPUS UNIVERSITY
Via Nomentana 335 – 00162 Roma (Italia)
Tel. +39-06-40400232 Fax +39-06-40400211
info@fondazionegermani.org
www.fondazionegermani.org

Parlare di protezioni dei processi decisionali di un sistema-paese e di controinformazione non sortisce alcun effetto concreto se le relative considerazioni non vengono inserite nel più ampio contesto delle attività d'intelligence considerate nel loro insieme.

La competizione è una caratteristica costante nella vita degli Stati, sin dagli albori della storia. Nel tempo questa competizione ha visto modificate caratteristiche e modalità, in funzione, soprattutto, dei livelli di progresso raggiunto nelle varie epoche prese in esame, ma sempre connesso a questo costante confronto, si è sviluppato al suo interno il tentativo di conoscere le potenzialità degli altri per rapportarle alle proprie, se possibile migliorare eventuali rapporti di forze sfavorevoli evitando così pericolose sproporzioni a proprio danno.

Per un lasso di tempo di gran lunga il più esteso, che giunge sino alla Prima Guerra Mondiale inclusa, l'esigenza di acquisire i dati sulla consistenza politico-militare del potenziale nemico era quella assolutamente prevalente. Nella fase attuale la conoscenza dei segreti industriali e scientifici, ma anche, e forse ancor più, il condizionamento degli organismi della pubblica amministrazione e delle strutture culturali, economiche e finanziarie dei Paesi concorrenti, si prospetta come assolutamente prioritario se non indispensabile.

Le potenzialità complessive di uno Stato vengono danneggiate allorché una nazione antagonista entra in possesso, meglio sottrae, informazioni e tecnologia relative al suo potenziale complessivo.

La raccolta di informazioni di natura politica, militare, economica e scientifica è una specifica funzione di ogni Servizio d'intelligence, che agisce con lo scopo ultimo di migliorare la competitività internazionale del proprio paese, ovvero colmare i suoi ritardi conoscitivi, in specie di natura tecnologica.

L'azione di un Servizio peraltro non si ferma ai campi sopra enunciati, ma dacché le relazioni umane hanno raggiunto forme complesse, essa comprende anche le finalità concepite in maniera da influenzare, per lo più con modalità occulte, esponenti politici, dipendenti pubblici e personalità di spicco in campo scientifico e culturale di una nazione concorrente, condizionandone in conseguenza i processi decisionali.

Secondo stime recenti il danno procurato ad un sistema-paese da forme di sottrazione informativa praticate dall'esterno ammonterebbe ad una cifra oscillante mediamente intorno a cinquanta miliardi di euro annui. Al di là delle stime, in que-

sti casi sempre aleatorie, perdite di queste dimensioni quantitative non possono essere sostenute indefinitamente da uno Stato anche strutturalmente forte.

Risulta quindi scontato che ogni organizzazione statale, ma anche qualsiasi impresa che operi in settori qualificabili come strategici e detenga proprie e riservate tecnologie, cerchi di contrastare queste azioni.

Uno Stato si difende varando normative specifiche che contrastino ogni fattispecie ritenuta criminosa o comunque dannosa, le aziende approntando norme interne a tutela dei propri processi produttivi.

In questa sede tratteremo in prevalenza di attività a livello di Stati e conseguentemente di organismi e tecniche di cui essi si servono per le operazioni negli ambiti sopra descritti, ma tutto, con le debite proporzioni, può essere riferito e rapportato al campo delle imprese e delle aziende private.

Le azioni aggressive che uno Stato può portare con i suoi Servizi contro un'altra Nazione sono lo spionaggio, l'ingerenza, la disinformazione e l'influenza.

Lo *spionaggio* è un'attività clandestina svolta allo scopo di raccogliere informazioni su di uno Stato concorrente, utili da un lato a definire il suo potenziale sotto l'aspetto scientifico, economico, politico e militare, ma anche a carpire tecnologie e competenze atte a compensare eventuali *gap* di conoscenze di chi promuove l'operazione.

Un caso di spionaggio nell'era della Guerra Fredda:

- L'azione spionistica dei coniugi Julius e Ethel Rosenberg e dello scienziato inglese Klaus Fuchs, a favore dell'Unione Sovietica, volta a conoscere i segreti atomici degli USA.
- Fuchs, considerato dopo Einstein il più grande fisico nucleare teorico, già rifugiato tedesco nel Regno Unito all'avvento del nazismo, ammise (nel 1950) di avere passato ai Sovietici gli elementi fondamentali della bomba atomica americana (Progetto Manhattan) e i progetti di quella nucleare.
- Le indagini connesse portarono, negli USA, alla scoperta di una rete spionistica russa, collegata a quella operante in Inghilterra, composta da un gruppo di persone tra cui i coniugi Rosenberg che, al termine di un clamoroso processo seguito dalla pubblica opinione internazionale (1951), furono condannati alla sedia elettrica. Fuchs, dopo la condanna solo parzialmente scontata, riparò nella Germania Est.

L'*ingerenza* è l'intromissione negli affari interni di un paese al fine di influenzarne le decisioni e le condotte. Questa tipologia d'azione, quando realizzata, è molto efficace perché consente forme di penetrazione nel contesto socio-politico ed economico dell'avversario senza dovere assumere una funzione diretta nella gestione dell'operazione.

L'*ingerenza* è quindi un'attività subdola, infatti di per sé non costituisce sempre un comportamento illegale, ma può se ben concepita e portata avanti con accortezza:

- minare rapporti politici interni e internazionali consolidati;
- distorcere condotte di mercato consolidate;
- giungere al controllo di contesti produttivi allargati;
- costituire infine l'anticamera di un'attività spionistica o collegarsi ad essa, quando già questa fosse in atto.

Da quanto sopra si ricava che gli obiettivi di un'attività d'ingerenza portata in danno di uno Stato sono ambienti politici, strutture produttive, organismi per la formazione dell'opinione pubblica, i cosiddetti *think-tank*, società a partecipazione statale e ogni altro contesto organizzato che incida sul suo potenziale complessivo.

Chi mette in atto questi tipi di operazioni deve:

- avere chiari gli scopi da raggiungere;
- sapere mascherare i propri obiettivi;
- eludere gli eventuali controlli dell'avversario;
- disporre di buoni strumenti di comunicazione.

L'ingerenza richiama e quindi sfrutta i concetti di disinformazione, influenza e controinformazione.

Esempi di ingerenza:

- Sostenere le parti politiche contrarie o favorevoli al Governo di una nazione così da condizionarne a nostro favore le iniziative. E' il caso delle sovvenzioni economiche russe ed americane a PCI e DC nel secondo dopo guerra.
- Inserirsi, attraverso compartecipazioni ed acquisizioni di attività produttive, nel complesso socio-economico di una nazione sino a determinarne le scelte strategiche.

Un caso che può configurarsi come un tentativo d'ingerenza coperto è rappresentato a riguardo dalle attività della Repubblica Popolare Cinese in direzione del settore industriale italiano evidenziate nel tempo da una serie di acquisizioni delle maggioranze azionarie di gruppi industriali nazionali, e da ultimo manifestatesi con la generosa offerta in contanti fatta in questi mesi a Finmeccanica per l'acquisto di Breda e Ansaldo Sts.

Anche la Francia, profittando della crisi economica da cui il nostro Paese non riesce a venire fuori, sta facendo spese tra le aziende più significative del *made in Italy*.

La *disinformazione* è un'attività complessa e sviluppata nel tempo volta a:

- confondere con dati e notizie false i decisori istituzionali di un Paese;
- creare turbamenti nella pubblica opinione di un Paese concorrente;
- suscitare contenziosi tra Stati tra loro amici;
- denigrare personalità e uomini politici ostili;
- ingannare gli organi di controspionaggio del paese obiettivo.

La disinformazione si caratterizza per i tempi non brevi che richiede la sua corretta applicazione e la complessità della sua elaborazione, che può essere gestita solo da apparati in grado di svilupparla avendo il totale sostegno di organismi politi-

ci coesi e tali che possono contare su di una lunga permanenza al potere. In pratica regimi dittatoriali, ovvero Paesi con indirizzi geopolitici consolidati e immutati nel tempo. Un esempio é la Russia, la cui politica estera nelle sue linee generali non è cambiata passando dagli Zar al regime sovietico e confermandosi nell'attuale periodo caratterizzato dalla personalità di Vladimir Putin.

Due operazioni, tra loro combinate, mirate alla disinformazione e poste in essere dal KGB sovietico in relazione al sequestro ed all'assassinio dell'on. Aldo Moro, sono le seguenti:

- La prima, la cosiddetta "operazione Shpora" (Sperone), consistente nel fare pervenire, prima al segretario della DC Benigno Zaccagnini e poi ad altri parlamentari di quel partito, un documento, con i crismi dell'attendibilità, che attribuiva agli USA la responsabilità del sequestro e della morte di Aldo Moro per la politica in genere da lui condotta, ed in particolare per l'apertura al PCI di cui sosteneva l'ingresso nel suo prossimo Governo.
- La seconda si riferisce ad un documento (FM30-31B), prodotto effettivamente dell'Esercito degli Stati Uniti e modificato dai russi, così da fare apparire che gli americani teorizzassero infiltrazioni nelle organizzazioni internazionali di sinistra per utilizzarle a propri fini. Il materiale, creato nel 1975, e distribuito in più paesi, venne riproposto dopo l'assassinio del presidente della DC e fatto pervenire al settimanale *L'Europeo*, che lo pubblicò (il 28 ottobre 1978) con grande evidenza, venendo poi ripreso dalla stampa in genere e da quella orientata a sinistra in particolare.

Le due operazioni furono messe a fuoco come attività di disinformazione del KGB dall'on. Francesco Cossiga, quando il 16 novembre 1999 commentò la documentazione contenuta nel dossier Mitrokhin che trattava del complesso delle attività dello spionaggio sovietico.

L'influenza è l'attività che si realizza all'interno del Paese obiettivo reclutando, ma anche solo favorendo e sostenendo, soggetti in grado per la loro posizione ed autorità di orientarne e condizionare decisamente la pubblica opinione.

Da cui *agente d'influenza*, tecnicamente il soggetto che sfruttando la propria posizione può influenzare un individuo o un gruppo in senso favorevole a una determinata tesi. L'agente d'influenza può essere consapevole, operare cioè sulla base dell'attivazione di un Servizio d'informazione, ovvero inconsapevole, vale a dire quando una persona autorevole in un determinato ambito viene solo indirettamente sostenuta ed agevolata nel propagandarne idee ed iniziative che coincidono con gli interessi di un'altra parte o nazione. Esemplificativa a questo riguardo l'attività posta tradizionalmente in essere dai Servizi inglesi, e più recentemente da quelli russi e americani, che hanno operato e si adoperano ancora oggi per influenzare alcune pubbliche opinioni tra cui anche quella italiana.

In merito riporto qui, letteralmente, il testo di una direttiva riservata dell'intel-

ligence britannica risalente al 1949 sulle attività d'influenza da sviluppare che appare come la codificazione formale di questa attività: "Il metodo principale da noi adottato consiste nel fornire del materiale concreto a personalità chiave che operano nei quotidiani, nei sindacati e nei partiti politici, affinché queste utilizzino autonomamente tali informazioni, senza però rilevare che la fonte è britannica".

Due esempi documentati di operazioni di influenza inglesi in Italia:

- L'attenzione rivolta già tra le due guerre mondiali verso il direttore del *Corriere della Sera*, Luigi Albertini, estesa poi e meglio qualificata (con la suddivisione in clienti, avvicinati e attenzionati) nel Secondo Dopoguerra con altri giornalisti, politici e uomini di cultura italiani a cui venivano forniti a vario titolo, attraverso attività interposte di personalità e/o enti privati, materiali e documenti i cui contenuti portavano a sostenere tesi e indirizzi favorevoli alla politica inglese.
- Le sovvenzioni (100.000 sterline a settimana) inglesi al quotidiano "Il Popolo d'Italia" di Benito Mussolini perché, dopo Caporetto, continuasse a sostenere la partecipazione italiana alla guerra contro le tesi pacifiste che ne volevano il ritiro dal conflitto.

L'attività cui compete la funzione di sventare le azioni aggressive di un Servizio informativo straniero si definisce *controinformazione* o *controintelligence*.

Per controinformazione si intende quel complesso di attività volte a prevenire, rilevare, contenere, contrastare ed, eventualmente, sfruttare a proprio vantaggio le iniziative in danno della sicurezza nazionale portate da altri Stati e Servizi d'informazione.

Nella sua concezione tradizionale la controinformazione è legata al confronto tra Stati e costituisce una forma di contrasto tipica nelle operazioni dei Servizi di sicurezza. Oggigiorno il termine, più frequentemente, si riferisce alle iniziative con le quali si tende a neutralizzare le insidie correlate in modo crescente al campo economico-industriale, dove le acquisizioni da parte avversaria di posizioni dominanti in settori d'interesse strategico producono un forte condizionamento delle scelte di governo.

La controinformazione è pertanto un'attività di sicurezza che mira essenzialmente ad individuare gli agenti di un Servizio d'informazioni straniero, anche quando essi agiscano per interposta persona, cioè con soggetti eterodiretti, per sventarne le azioni ostili o comunque contrarie agli interessi del Paese.

La controinformazione nel suo complesso è svolta da quella branca operativa che viene definita comunemente controspionaggio, ed è prevista specificatamente tra i compiti assegnati a quelle Agenzie con competenze rivolte alla sicurezza interna dei vari Stati.

L'azione della controinformazione consiste nel contrastare ogni forma aggressiva portata contro gli interessi di uno Stato. Non si esaurisce quindi con l'attività

di ricerca informativa (intelligence), ma si può dire che inizi proprio quando viene individuata o solo supposta un'azione di spionaggio da parte di un'organizzazione avversaria.

Le sue tecniche sono quelle tipiche delle attività d'investigazione e mirano a documentare, con gli strumenti propri delle azioni di polizia (intercettazioni, pedinamenti, riprese filmate, sopralluoghi riservati di ambienti in luogo di perquisizioni, etc.), le condotte spionistiche del sospettato e gli obiettivi che si prefigge. Individuati i protagonisti del caso e gli obiettivi a cui mirano, occorre determinare la misura più idonea per neutralizzarli.

Sostanzialmente le iniziative adottabili da parte di un Servizio per vanificare prima e rovesciare eventualmente poi a proprio favore l'attività avversaria sono: la repressione, la disinformazione e la controingerenza, che rientrano nelle operazioni di controspionaggio difensivo.

Quella parte di azioni di controingerenza che si propone invece il tentativo di sfruttare l'attività degli agenti avversari ai nostri fini, rientra nell'ambito del controspionaggio offensivo.

Con la *repressione* si interviene sull'agente nemico ovvero sulla sua rete e si procede con arresti e/o espulsioni. Questa soluzione, se elimina alla radice l'attività spionistica, può provocare conseguenze diplomatiche negative (proteste ufficiali, espulsioni per ritorsione di nostri funzionari all'estero, etc.), e soprattutto interrompe ogni possibilità di continuare un'attività conoscitiva in direzione del Servizio avversario.

Tale formula operativa, qualora non coinvolga cittadini del paese, può consentire al limite una soluzione "indolore", cioè l'allontanamento dell'agente avversario senza grande pubblicità, stroncandone l'attività ma evitando conseguenti, reciproci imbarazzi diplomatici.

Esempio di repressione:

- Il caso dell'azienda Microlito, protagonisti l'ing. Azelio Negrino e l'agente del GRU Viktor Pronin.
- Più di quarantamila microfilm relativi al sistema di navigazione del caccia Tornado che dovevano essere consegnati al GRU, il Servizio d'intelligence militare sovietico (febbraio 1983).
- Il colonnello Pronin fu inizialmente arrestato, poi quando il clamore del caso venne meno, gli fu concessa la libertà provvisoria rientrando quindi in patria.

Con la *disinformazione* nella sua fase difensiva ci si prefigge l'obiettivo di neutralizzare l'attività di un agente nemico, senza che egli se ne possa accorgere, fornendogli documentazione opportunamente confezionata con l'apporto di soggetti sia appartenenti alle istituzioni che al privato. Con ogni evidenza il materiale ovve-

ro le notizie fornite sono false, ma devono apparire credibili e funzionali alle esigenze di mantenere in piedi per più tempo l'operazione.

In tale modo sarà possibile conoscere gli specifici interessi dell'operatore nemico così da evidenziare anche le potenziali lacune del suo Paese nel settore trattato. In questo caso, attraverso l'intermediario istituzionale o privato, si farà pervenire alla controparte materiale fuorviante, ottenendo così quella che in termini tecnici viene definita *intossicazione* del competitore e realizzando un'*azione doppia*, cioè un'attività che consente di usare ai fini propri un agente appartenente a un'entità ostile.

Esempio di disinformazione:

- Il caso dell'agente del GRU Aleksandr Ermakov nel suo tentativo di reclutare un ufficiale dello Stato Maggiore Difesa italiano e conseguente sua intossicazione (1974) .
- Trasferimento successivo del nostro ufficiale ad altro incarico dello SMD per prolungare l'attività disinformativa e conoscere i livelli di conoscenze raggiunte dall'Esercito sovietico in altri settori militari.
- Propinati anche materiali superati e formule obsolete che avevano anche la funzione di confondere i Russi sugli effettivi livelli raggiunti dall'Alleanza occidentale in determinati ambiti tecnologici

La difesa dalla spionaggio avversario ovviamente si sviluppa anche con *azioni preventive* , che vanno sempre comprese sotto la voce del controspionaggio difensivo. Tra queste in primo luogo occorre considerare la rigorosa compartimentazione delle informazioni, in base al principio valido per ogni attività che “solo chi ne ha necessità deve poter conoscere”.

Importante in questo ambito appare l'opera di scrematura preventiva, che può essere fatta:

- interdichendo l'ingresso nel nostro Paese a persone sospette o già riconosciute come spie di un determinato Stato;
- agendo sui visti d'ingresso quando ancora previsti e sulla concessione o il rinnovo dei permessi di soggiorno.

In questo comparto è ovviamente importante la collaborazione tra Servizi alleati e la disponibilità di aggiornate banche dati (vedasi il Trattato di Schengen).

Fondamentale però risulta l'opera volta a sensibilizzare il comportamento di politici, dei funzionari dello Stato e degli alti dirigenti di grandi industrie operanti in settori di valenza strategica, allertandoli sulla possibilità che possano divenire oggetto di mirate operazioni spionistiche. Il fine ultimo di questo complesso di azioni è quello che, attraverso un'opera specifica di indottrinamento, sia possibile realizzare una *coscienza difensiva* diffusa che, se ottenuta, può consentire la più efficace e concreta delle misure di controspionaggio.

Tra le misure difensive di controinformazione è compresa la *controingerenza*,

costituita da un serie di modalità idonee a stroncare tutte quelle azioni volte a condizionare i processi decisionali, organizzativi e produttivi di cui può essere oggetto uno Stato nel quadro di un'attività aggressiva attuata da un Paese avversario, interessato ad aumentare la sua competitività in campo internazionale.

Tale compito in Italia è affidato all'Agenzia per la sicurezza interna (AISI). Peraltro, mai come in questo ambito occorre che il potere politico definisca senza margini di equivoco quelli che sono gli interessi irrinunciabili della Nazione, oltre i quali una competizione economica e politica, accettata nella prassi dei rapporti economici internazionali, diviene inserimento negli affari interni altrui e quindi si configura come un'operazione che deve senz'altro essere stroncata.

Attualmente, da noi, questo confine non è sempre tracciato con precisione, anche per un approccio da parte dei nostri governanti che sin dall'inizio del Secondo Dopoguerra hanno fatto costantemente prevalere gli interessi del momento a considerazioni di più ampio respiro strategico. Ne consegue che il Paese sia molto esposto a forme diversificate di ingerenza e gli organismi dei Servizi, interessati a questo settore, stentino a condurre un'azione efficace.

Una componente molto importante nel confronto in atto tra le potenze mondiali è rappresentata dalle attività che vengono svolte secondo modalità coperte. La consistenza reale di uno Stato si misura oggi anche in funzione della sua capacità di sviluppare un'efficiente organizzazione di spionaggio, ma soprattutto di realizzare mirate campagne di ingerenza unite a validi approntamenti posti a difesa dei rispettivi interessi strategici.

In buona sostanza, per ogni Paese, gestire questi tipi di operazioni significa affrontare temi assolutamente vitali, sia ai fini della rilevanza politica in campo internazionale, che per la sicurezza in generale e la tutela in particolare dei settori pregiati dell'economia.

La controingerenza si basa su attività preliminari di prevenzione e di sensibilizzazione del complesso politico e produttivo di uno Stato, di protezione poi e, infine, se del caso, di neutralizzazione allorquando l'ingerenza appaia manifesta e non altrimenti controllabile.

Decidere di stroncare una condotta d'ingerenza comporta peraltro la valutazione di una serie di aspetti legati ad interessi di natura pubblica e privata che rendono indubbiamente difficili interventi radicali.

In un contesto di relazioni interconnesse e globalizzate è sempre complicato adottare indirizzi strategici che preservino, da un lato, il profitto nazionale e, dall'altro, non danneggino relazioni e accordi di rilevanza internazionale da cui a volte è impossibile prescindere.

Talché anche qui si ripropongono, aumentate significativamente, le difficoltà evidenziate nei casi di contrasto radicale alle azioni di spionaggio, e l'azione dei Governi, generalmente, si orienta sempre verso soluzioni di compromesso che, almeno da un punto di vista della risonanza pubblica, evitino imbarazzi politicamente difficili da gestire.

Il pericolo di ingerenza deve essere opportunamente considerato anche da chi opera esclusivamente nel privato e con giuste finalità di profitto. L'attacco di un Servizio straniero ad un obiettivo sia pure non statale ma di valenza strategica, è un danno inferto non solo all'obiettivo attaccato, ma anche a tutta la comunità nazionale. L'approntamento di misure di controingerenza, non significa coltivare la cultura del sospetto a prescindere, bensì razionalizzare e mettere a sistema procedure e comportamenti contrapposti a quelli che l'avversario sicuramente pone in essere.

Ogni dirigente aziendale, al di là del proprio dell'interesse, dovrebbe considerare il danno economico che può essere recato alla sua produzione quando determinate tecnologie riservate e specifiche dell'impresa si trasferiscano in mani estranee. In tale ottica occorrerà quindi:

- disporre di regole interne con precisi disciplinari di condotta;
- esercitare revisioni e controlli a campione sul proprio sistema di sicurezza;
- analizzare il comportamento dei dipendenti e provvedere alla loro formazione;
- aggiornarsi sulle casistiche relative a conclamate azioni di spionaggio e ingerenza industriali attuate in altri casi;
- considerare il Servizio di sicurezza, anche per quanto disposto dalle leggi vigenti, il proprio *tutor*.

Infatti, in relazione al disposto della recente legge n.124/2007 che ha ridefinito l'attività d'intelligence in Italia, i nostri Servizi sono chiamati a svolgere un'opera di sensibilizzazione nei confronti di soggetti pubblici e privati.

E ciò in relazione al fatto che, ai primi, come appartenenti alla Pubblica Amministrazione, competono specifiche responsabilità istituzionali, e i secondi, quali detentori di produzioni pregiate, risultano indispensabili allo sviluppo economico del sistema-paese.

Questa funzione deve quindi essere considerata una vera e propria campagna nazionale di controingerenza, e quindi di controspionaggio ai fini degli interessi nazionali da condurre senza interruzione.

Il *controspionaggio offensivo*, si propone lo scopo di reclutare l'agente avversario al fine di ottenerne la collaborazione. Con questa tecnica operativa si realizza non solo lo smascheramento di un operatore ostile, ma si ottiene anche, attraverso le informazioni ricavate, di conoscere gli obiettivi dell'avversario, il suo radicamento sul nostro territorio e l'individuazione di parte o di tutti gli agenti operanti nel Paese.

Se questa è l'operazione sicuramente più produttiva nel campo della controinformazione, essa è anche la più difficile e problematica, perché oltre all'intrinseca difficoltà di reclutare un professionista di un Servizio avversario, in caso del fallimento della sua cooptazione, si corre il rischio di rimanere a nostra volta vittime di un'azione doppia, svelare il complesso delle operazioni sino a quel punto svolte nello specifico ambito informativo gestito, e divenire eventualmente oggetto di operazioni ritorsive della controparte.

Esempio di un'azione riuscita volta alla defezione di un agente avversario:

- Un classico caso di defezione di un agente segreto è dato da quella che si realizzò in Italia agli inizi degli anni settanta dopo il ristabilimento delle relazioni diplomatiche tra l'Italia e la Repubblica Popolare Cinese (7 dicembre 1970)
- Individuata preventivamente la sede scelta dai Cinesi per insediare la propria ambasciata, nei relativi locali, ad opera del settore controspionaggio del SID furono collocate una serie di microspie.
- Dall'attento ascolto delle conversazioni tra i vari diplomatici, si poté individuare un addetto al settore commerciale che appariva il più idoneo a un tentativo di avvicinamento.
- L'operazione fu messa in atto ricorrendo ad un piano d'azione che prevedeva il ricorso a persona estranea al Servizio, ritenuta particolarmente idonea allo scopo.
- Attratto con una serie di motivi leciti al di fuori dell'ambasciata, fu possibile sorprenderlo in atteggiamento ingiustificabile di fronte ai suoi superiori, talché posto di fronte al dilemma tra la denuncia alle autorità del suo Paese e la collaborazione, optò per quest'ultima soluzione. Egli fu il primo diplomatico-agente della Cina comunista a defezionare verso l'Occidente.

Un caso di azione doppia conseguente ad un'azione di reclutamento dell'agente avversario:

- Il caso dell'agente dello MI6 Harold Adrian Russell ("Kim") Philby, che unitamente ad altri quattro appartenenti ad una cellula comunista formatasi negli anni 30 del secolo scorso all'interno dell'Università di Cambridge, i così detti "Cinque di Cambridge", agì a favore delle spionaggio sovietico.
- Philby, agente del Servizio inglese, svolse attività per l'NKVD prima e poi per il KGB dal 1936, quando fu reclutato, sino al 1963. Lavorò anche in Turchia e negli USA, formalmente sempre come agente dell'MI6, recando danni gravissimi al blocco occidentale per il complesso delle notizie che riuscì a fornire ai suoi mandanti.
- Nel 1963, resosi conto di essere stato scoperto, si rifugiò nell'URSS.

Un altro caso di azione doppia conseguente ad un'azione di reclutamento dell'agente avversario:

- Il caso di Oleg Gordievskij, responsabile della *rezidentura* del KGB a Londra, cioè del complesso degli agenti sovietici operanti nel Regno Unito, che venne reclutato nel 1974 dal MI6, con cui collaborò per anni.
- Scoperto e richiamato in patria riuscì a riparare in Occidente dopo una rocambolesca fuga degna dei migliori romanzi di spionaggio (1985).
- La collaborazione di Gordievskij portò alla scoperta di 31 funzionari russi operanti in Inghilterra e all'individuazione di parte degli organigrammi delle *rezidenture* dei Servizi sovietici di molti paesi europei.

Un caso di fallimento dell'intelligence: l'attacco alle Torri Gemelle di New York (11 settembre 2001).

- Gli americani, nei miliardi di dati ricavati dalle intercettazioni a strascico praticate dalla NSA, disponevano preventivamente dei nomi di coloro che avrebbero preso parte agli attentati, ma confusi come erano in mezzo ad altri innumerevoli dati, non sono riusciti ad evidenziarli e a metterli a fuoco.
- Solo una preventiva attività informativa nell'ambito del terrorismo islamista avrebbe potuto consentire, in ipotesi, di scremare quelle figure di soggetti potenzialmente in grado di operare ai livelli di un attacco portato agli Stati Uniti e rivolgere su di loro un'attenzione mirata (frequenza di una scuola pilotaggio da parte di alcuni soggetti poi coinvolti nell'attentato).
- Ciò non è stato possibile, così CIA e FBI hanno continuato a girare a vuoto e gli USA hanno subito il più grave degli attacchi sul proprio territorio dopo quello realizzato a Pearl Harbour il 7 dicembre 1941.

Ultimo settore da prendere in esame per le operazioni d'intelligence difensiva è il contrasto a quello che costituisce l'ambito più recente nell'attività di spionaggio, e cioè il *cyber-spionaggio*, che si realizza con l'accesso illecito a programmi e sistemi informatici di nazioni o enti concorrenti. Qui entriamo in un ambito, quello del web, di tali dimensioni da richiedere puntuali azione preliminari prima di affrontare una ricerca d'intelligence definibile seria.

Si pensi al web nascosto, quello cioè non indicizzato, che comprende secondo stime recenti il 98% dell'intero settore. Solo un'azione preventiva di Humint può

consentire la riduzione dei campi di interesse e produrre nella ricerca informatica risultati conclusivi effettivamente utili.

In pratica quando in un'operazione d'intelligence si vuole o si deve fare ricorso allo strumento informatico, non si può procedere *random*, cioè in maniera casuale, ma delimitando con la massima precisione consentita il settore verso cui indirizzare l'indagine.

La formula operativa valida per questo comparto è: prima Humint, poi web e infine di nuovo Humint, che solo può concludere la ricerca. In tale modo si potranno avere effettive possibilità di successo.

Così, nella controintelligence informatica, solo avendo definito quadri conoscitivi sufficientemente ridotti è possibile attuare misure difensive potenzialmente utili. Altrimenti c'è il rischio concreto di clamorosi fallimenti. E quello del girare a vuoto tra le notizie disponibili è il pericolo più grande per ogni attività sia di intelligence che di controinformazione.