INFLUENZA E
DECEPTION STRATEGICA

ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

INTELLIGENCE E *DECEPTION* STRATEGICA:

MANIPOLAZIONE PERCETTIVA ED INFLUENZA DEI PROCESSI DECISIONALI DI VERTICE

ALFONSO MONTAGNESE

APRILE 2012

EDIZIONI MACHIAVELLI

ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

AUTORE

Alfonso Montagnese

Coordina il programma di ricerca "Influenza e *Deception* Strategica" dell'Istituto Italiano di Studi Strategici "Niccolò Machiavelli".

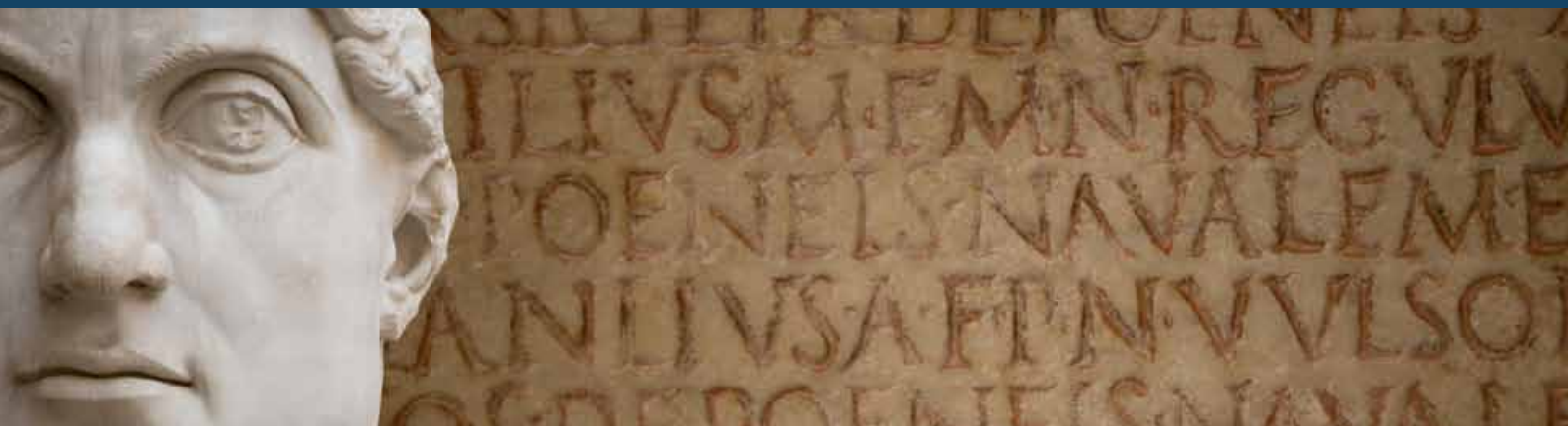
Ufficiale dell'Arma dei Carabinieri, Direttore di Ricerca presso il Centro Militare di Studi Strategici (Ce.Mi.S.S.) del Ministero della Difesa nonché membro del Gruppo di Lavoro "*Cyberworld*" dell'Osservatorio per la Sicurezza Nazionale (O.S.N.).

Ha conseguito la laurea in Scienze Politiche presso l'Università "La Sapienza" di Roma (2002) ed il Master in *Intelligence* e Sicurezza Nazionale presso la *Link Campus University* di Roma (2010).

I pareri espressi in questo documento sono personali dell'autore e non rappresentano le opinioni delle Istituzioni per le quali l'autore presta servizio e/o dell'Istituto.

Copyright © 2012
Istituto Italiano di Studi Strategici "Niccolò Machiavelli" – Roma

È vietata la riproduzione non autorizzata, anche parziale, realizzata con qualsiasi mezzo, compresa la fotocopia, anche ad uso interno o didattico.



INTRODUZIONE

Con il presente *paper* l'Istituto Italiano di Studi Strategici "Niccolò Machiavelli" inaugura un nuovo programma di ricerca, coordinato da Alfonso Montagnese e dedicato all'analisi dei metodi di influenza strategica, *deception* e *perception management* e delle loro implicazioni strategiche, sia in campo politico-militare che in quello economico-finanziario.

L'attuale "ambiente informativo" nonché le complesse dinamiche del sistema internazionale rendono, infatti, particolarmente rilevanti, sia per lo Stato sia per il mondo *corporate*, tutte quelle attività che sono volte ad influire sui processi decisionali di vertice dei soggetti avversari (Stati non alleati, aziende *competitor*, organizzazioni criminali, gruppi terroristici ed altre forze opponenti), condizionandone le scelte finali per conseguire vantaggi competitivi. La conoscenza approfondita delle modalità di esecuzione di tali attività è, inoltre, fondamentale per acquisire le capacità necessarie per rilevarle per tempo, qualora condotte dagli avversari, e contrastarle adeguatamente.

L'Istituto Machiavelli, coerentemente con gli obiettivi da esso perseguiti, ha ritenuto opportuno attivare nell'ambito del Dipartimento di Ricerca una specifica linea di approfondimento concernente le attività di influenza e *deception* allo scopo di contribuire ad elevare la conoscenza su temi strategici per il Sistema-Paese.

Claudio Neri
Direttore del Dipartimento di ricerca

PREMESSA

Lo scopo del presente contributo è quello di offrire una descrizione sintetica della *deception*, con particolare riguardo a quella di livello strategico, definendone i contorni ed individuandone gli elementi caratterizzanti, i meccanismi e le dinamiche di funzionamento, nonché le tecniche ed i metodi mediante i quali l'attività può essere eseguita ed, al contempo, contrastata. Il contributo è finalizzato, inoltre, ad evidenziare come l'uso della *deception* strategica da parte degli apparati di sicurezza ed *intelligence* possa, con un impiego relativamente limitato di risorse economiche, umane e strumentali, concorrere significativamente alla tutela degli interessi strategici dello Stato ed al contrasto delle minacce alla sicurezza nazionale.

Lo studio della *deception* comporta non poche difficoltà nell'approccio iniziale, in quanto si presenta quale fenomeno sfuggente, dai contorni sfocati, non puntualmente definiti, che si manifesta, secondo forme diverse e talvolta non facilmente riconoscibili (ad es. operazioni psicologiche, attività di propaganda, operazioni di influenza, *perception management*, campagne di comunicazione, etc. o mediante un'azione combinata e coordinata tra due o più tra queste attività[1]). La *deception*, la cui traduzione letterale è «inganno»[2], caratterizza peraltro l'intera catena evolutiva dell'uomo e delle specie animali e vegetali[3] ed è utilizzata sia per finalità offensive che per scopi difensivi. Limitandosi ad analizzarne la dimensione umana, la *deception* è uno strumento utilizzato, in forme più o meno complesse, sin dall'antichità. Sebbene sia tradizionalmente associata alle campagne militari, la *deception* è uno strumento che può essere impiegato efficacemente anche nel campo diplomatico ed economico[4].

1- La Central Intelligence Agency (C.I.A.) USA include nel concetto di deception diverse attività, tra cui "camouflage, concealment, [..] perception [management], magic, hoaxes, fraud, psychology, counterintelligence, counterespionage, security, special operations, psychological operations and unconventional warfare".
OFFICE OF RESEARCH AND DEVELOPMENT - CIA, (1980), Deception Research Program, Bibliography on Deception.
2- http://oxfordparavia.it/lemmaEng9565
3- SMITH, E. O., (1987), Deception and Evolutionary Biology, Cultural Anthropology, vol. 2, n. 1, Duke University, North Carolina.
4- CRAWFORD V.P., (2003), Lying for Strategic Advantage: Rational and Boundedly Rational Misrepresentation of Intentions, Department of Economics, University of California, San Diego.

1. Cos'e' la *deception* strategica?

La *deception* strategica è uno strumento con il quale uno Stato (*deceiver*) tutela i propri interessi strategici, contrasta le minacce alla sicurezza nazionale e persegue le opportunità di crescita economica, di progresso scientifico, di espansione della sfera d'influenza e di rafforzamento della propria posizione geo-politica nello scacchiere internazionale.

La *deception* strategica è uno strumento con il quale uno Stato (*deceiver*) tutela i propri interessi strategici, contrasta le minacce alla sicurezza nazionale e persegue le opportunità di crescita economica, di progresso scientifico, di espansione della sfera d'influenza e di rafforzamento della propria posizione geo-politica nello scacchiere internazionale.

La *deception* strategica è impiegata per nascondere, in tutto o in parte, le effettive intenzioni, capacità e strategie all'avversario (*target*) e, al contempo, comprometterne le capacità di comprensione in merito ad un dato fenomeno, evento o situazione, al fine di indurlo ad un impiego irrazionale e/o svantaggioso delle proprie risorse. La *deception* è, quindi, caratterizzata da due elementi: la volontarietà dell'azione[5] e il conseguimento di un vantaggio[6]. Lo Stato che si avvale della *deception* intende acquisire una posizione di vantaggio strategico sull'avversario, inducendolo ad agire in senso favorevole ai suoi interessi. Tale scopo è perseguibile interferendo, più o meno direttamente, sui processi decisionali dei vertici politico-militari della parte avversaria ed influenzando le determinazioni finali di tali processi.

La *deception* strategica è approvata dal vertice politico-militare di uno Stato (*leadership* governativa, Stato Maggiore delle forze armate, organi centrali delle forze di sicurezza), di un'organizzazione internazionale (ad es. l'ONU), di un'alleanza politico-militare (ad es. la NATO), che si avvale dei propri organismi specializzati – in primo luogo apparati

5- DEWAR M., (1989), The Art of Deception in Warfare, Newton Abbot, David & Charles Publishers, Devon, UK.
6- DANIEL D. C., HERBIG K. L., (1982), Strategic Military Deception, Pergamon Press, New York.

intelligence militari e civili, ma anche con il contributo del mondo accademico, industriale, economico-finanziario – per la pianificazione, la gestione e l'esecuzione delle relative operazioni. L'attività di *deception* di livello strategico può essere anche svolta da attori privati, non aventi soggettività giuridica internazionale[7] (ad es. un gruppo bancario, un'azienda multinazionale, un movimento terroristico, un'organizzazione criminale internazionale, etc.).

La *deception* strategica, generalmente, è diretta contro l'*establishment* politico-militare di uno Stato[8], ma può essere rivolta anche nei confronti della *leadership* di un'organizzazione internazionale, di un'alleanza politico-militare o di altra struttura organizzata, che si avvale dei propri apparati di sicurezza ed *intelligence* per l'acquisizione, l'elaborazione e l'analisi delle informazioni al fine di avere un quadro di situazione sui fenomeni politici, diplomatici, militari, economici, criminali, etc..Il *target*, in definitiva, può identificarsi in un singolo individuo (ad es. un decisore politico o militare di uno Stato avversario), un numero ristretto di individui (ad es. gli organi di staff di un ministro, gli analisti di un organismo *intelligence*, gli addetti ad un'unità di crisi) o nell'intera architettura istituzionale di vertice di uno Stato (ministeri, apparati di sicurezza, forze armate, etc.)[9].

La *deception* di livello strategico ha, generalmente, obiettivi di rilevanza sistemica e si sviluppa su un orizzonte temporale di medio-lungo periodo per il conseguimento degli obiettivi programmati.

La *deception* di livello strategico ha, generalmente, obiettivi di rilevanza sistemica e si sviluppa su un orizzonte temporale di medio-lungo periodo[10] per il conseguimento degli obiettivi programmati.
E' un'attività molto articolata che richiede un'attenta fase di pianificazione e di esame preventivo dei meccanismi cognitivi e percettivi dell'avversario al fine di poter individuare gli strumenti più opportuni per manipolare tali meccanismi e, conseguentemente, influenzare i processi decisionali di vertice e orientarli verso decisioni favorevoli agli interessi del *deceiver*.

Le attività di *deception* possono avere un orizzonte temporale più limitato (a medio o breve termine) e obiettivi più contenuti[11].

7- Intesi come soggetti privi di soggettività internazionale secondo i principi del Diritto Internazionale consuetudinario e pattizio.
8- DANIEL D. C., HERBIG K. L., (1982), Strategic Military…cit.
9- WALTZ E. (1998), Information Warfare Principles and Operations, Artech House, Boston - London.
10- VEGO M., (2002), Operational Deception in the Information Age, Joint Force Quarterly, National Defense University Press, Washington.
11- Nell'ipotesi in cui la campagna di inganno sia caratterizzata da entrambi i fattori (breve termine e obiettivi di entità non sistemica) ci si riferisce a deception tattica e/o operativa, utilizzata soprattutto in ambito militare. A differenza della deception strategica, che coinvolge diverse sfere (politica, diplomatica, economico-finanziaria, etc.) e diversi attori (leader politici, corpo diplomatico, ministeri, vertice degli apparati intelligence, stato maggiore delle forze armate, etc.), quella condotta a livello tattico ed operativo è, soprattutto, uno strumento impiegato nelle campagne militari e i cui attori (deceiver e target) sono, quasi esclusivamente, appartenenti a strutture militari. Non vi sono linee di confine ben demarcate tra i tre livelli di impiego della deception (strategico, tattico, operativo) e spesso gli stessi sono complementari.

2. MODELLO DI FUNZIONAMENTO

Tenuto conto del livello di complessità che caratterizza la *deception* strategica, al fine di comprenderne i meccanismi di funzionamento può risultare utile elaborare un modello teorico semplificato.

La *deception* è un'attività strettamente correlata alla comunicazione, intesa quale scambio reciproco di informazioni tra due o più soggetti.

La *deception* è un'attività strettamente correlata alla comunicazione, intesa quale scambio reciproco di informazioni tra due o più soggetti.

Per tale motivo, per l'elaborazione di un modello semplificato di *deception*, occorre partire dal modello teorico di comunicazione[12]. Gli elementi fondamentali di un modello di comunicazione sono:

- l'emittente: il soggetto che emette il messaggio;
- il ricevente: il soggetto che riceve il messaggio
- inviato dall'emittente;
- il messaggio: è il contenuto oggetto della comunicazione;
- il referente: lo scopo e l'argomento della comunicazione;
- il codice: le regole fissate ed utilizzate per comunicare;
- il canale: lo strumento attraverso cui l'emittente trasmette il messaggio al ricevente.

Considerato che i processi decisionali di vertice sono strettamente interconnessi con l'attività degli apparati di *intelligence* (come si evidenzierà meglio di seguito) e che il «processo d'*intelligence*» è "*the reception and interpretation of signals emitted by the activities of the side under observation*"[13], è possibile osservare come tutti gli elementi fondamentali

12- Quello utilizzato è un modello semplificato, basato sulla combinazione tra gli elementi fondanti la teoria dell'informazione - elaborata con approccio matematico da Weaver e Shannon - ed il modello di comunicazione formalizzato da Jakobson.
WEAVER W., SHANNON C. E., (1949), The Mathematical Theory of Communication, University of Illinois Press, Urbana, Illinois.
JAKOBSON R., HALLE, M., (1956), Fundamentals of Language, Mouton & Co Printers, The Hague.
13- SHULSKY A. N., SCHMITT G. J., (2002), Silent Warfare - Understanding the World of Intelligence, Potomac Books, Washington.

del modello di comunicazione caratterizzino anche la *deception*, in cui l'emittente è il soggetto attivo nella *deception*: il *deceiver*, mentre il ricevente è il soggetto cui è diretta l'attività di *deception*: il *target*.
Rispetto al modello tradizionale di comunicazione, la *deception* si distingue per la presenza di tre ulteriori elementi:

- la volontarietà da parte del *deceiver* di confondere e disorientare il *target*, utilizzando messaggi veri, parzialmente veri, o falsi, e di alterarne la percezione, al fine di indurlo ad adottare (o a non adottare) specifiche determinazioni e/o compiere (o a non compiere) determinati comportamenti[14];
- la conoscenza approfondita da parte del *deceiver* dei processi cognitivi del *target*, necessaria per interferire nelle sue valutazioni e nelle sue azioni[15];
- il conseguimento di un vantaggio competitivo da parte del *deceiver* a seguito dell'acquisizione del messaggio ingannevole da parte del *target*.

Affinché l'emittente acquisisca effettivamente un vantaggio, è necessario, però, che il ricevente, inconsapevole della mancanza, totale o parziale, di autenticità del messaggio «confezionato» e trasmessogli dall'emittente, lo analizzi e lo utilizzi quale elemento fondante delle sue decisioni[16].

Si è già evidenziato che la *deception* strategica è un'attività particolarmente complessa ed articolata, che richiede un attento processo di pianificazione.

Prima di avviare un programma di *deception* è, infatti, necessario:

- individuare quello che Whaley[17] definisce il «traguardo strategico» che si intende perseguire;
- determinare quale decisione si vuol far adottare e/o azione (o inazione) si intende far compiere (o non compiere) al *target*;
- acquisire un quadro di situazione completo ed aggiornato circa:
  - il c.d. *mind-set* del *target*[18] (qualora la campagna ingannevole sia focalizzata su una persona), e cioè conoscerne profondamente la formazione culturale, le pregresse esperienze, le attitudini, le conoscenze su argomenti specifici, l'orientamento politico, l'origine geografica, l'appartenenza ad un determinato gruppo etnico, le aspettative, le intenzioni, etc.[19];
  - l'architettura organizzativa e le capacità del *target* (qualora l'inganno strategico sia orientato verso un sistema complesso, composto da strutture organizzate), e cioè individuare i flussi decisionali, le risorse disponibili, la suddivisione di competenze e funzioni;
- valutare il livello di rischio che il programma sia intercettato dalla controparte e stimarne le possibili conseguenze negative. Nell'ipotesi in cui gli apparati *intelligence* di uno Stato *target* rilevassero l'operazione di *deception* e decidessero di renderla pubblica, le possibili implicazioni negative potrebbero riverberarsi, infatti, sia sul piano interno dello Sato *deceiver* (ad es. impatto sull'opinione pubblica) sia su quello internazionale (ad es. deterioramento delle relazioni diplomatiche)[20].

14- WALTZ E. (1998), Information Warfare...cit.
15- J. Jr., (1981), Strategic Deception and Counter Deception - A Cognitive Process Approach, International Studies Quarterly, vol. 25.
16- WHALEY B. (1982), Toward a General Theory of Deception, The Journal of Strategic Studies, vol. 5.
17- WHALEY B. (1982), Toward a General…cit.
18- O'NEILL R., (1989), Toward a Methodology for Perception Management, Defense Technical Information Center, Newport.
19- JAJKO W. (2002), Deception: Appeal for Acceptance, Discourse on Doctrine, Preface to Planning, Comparative Strategy, vol. 21 (5), Routledge.
20- KISS E., (2003), Strategic Deception in Modern Democracies: the Ethical Dimension, Triangle Institute for Security Studies (TISS) - U.S. Army War College Strategic Studies Institute (SSI).

Successivamente, sulla base di questi quattro elementi occorre:

- individuare i canali di «approvvigionamento informativo» della controparte, al fine di veicolare adeguatamente le informazioni ingannevoli;
- confezionare un «pacchetto informativo ingannevole» da far pervenire all'avversario;
- programmare una «*story line*», che sia improntata su criteri di logicità, cronologicità, credibilità e congruenza, per eseguire una efficace somministrazione del «pacchetto informativo ingannevole» alla controparte[21];
- individuare i canali di *feedback* (che possono coincidere in tutto o in parte con i canali di «approvvigionamento informativo»), necessari a monitorare costantemente le reazioni della controparte in seguito all'acquisizione delle prime informazioni ingannevoli; tale monitoraggio è utile al fine di controllare progressivamente l'andamento della condotta dell'operazione di *deception* e di adottare, se necessario, le opportune modifiche in corso di esecuzione[22].

21- WALTZ E. (1998), Information Warfare...cit.
22 -SHULSKY A. N., SCHMITT G. J., (2002), Silent…cit.

Al fine di rendere più comprensibili le dinamiche di funzionamento del modello teorico della *deception* strategica e ridurne il livello di astrattezza[23], si può ricorrere ad esempi pratici, come quelli riportati nei box n. 1 e 2.

BOX N.1

Lo Stato X, potenza di dimensioni medio-piccole, ha acquisito la capacità di far detonare una bomba nucleare, con limitato potenziale, ad elevata altitudine sullo spazio extra-atmosferico sovrastante il territorio dello Stato Y, potenza di grandi dimensioni.

Tale detonazione, anche se non provocherebbe vittime e danni fisici diretti alle infrastrutture dello Stato Y, produrrebbe una quantità di impulsi elettromagnetici tale da causare il grave malfunzionamento dei sistemi di telecomunicazione e delle reti energetiche dello Stato Y. Tali effetti andrebbero a compromettere, conseguentemente, la catena di comando e controllo (C2) e la capacità di difesa e reazione dello Stato Y.

Lo Stato Y, dopo essere venuto a conoscenza della nuova capacità offensiva acquisita dallo stato X, decide di avviare una campagna di *deception* per evitare un confronto militare. Il programma di *deception* ha come *target* il vertice politico-militare dello Stato X e come obiettivo quello di convincere lo Stato X che lo Stato Y ha già sviluppato una nuova tecnologia in grado di schermare i sistemi di telecomunicazione e le reti energetiche dalle onde elettromagnetiche prodotte da una detonazione nucleare.

Il canali di comunicazione utilizzati per far giungere l'informazione non vera allo Stato X sono i network radio-televisivi, le reti di collegamento tra gli ambienti accademici e scientifici, la rete internet (con particolare riferimento ai *social* media).

Se il programma di *deception* viene pianificato accuratamente ed eseguito efficacemente dagli apparati *intelligence* dello Stato Y, il messaggio giungerà al *target* e contribuirà ad interferire nei processi decisionali della *leadership* dello Stato X in merito all'eventuale impiego dell'arma nucleare.

23- Un limite degli studi concernenti la deception strategica, come osserva Zotti, è proprio l'eccessivo livello di astrattezza con cui si formalizzano i concetti e gli elementi fondamentali che la caratterizzano. Tale livello di astrattezza, infatti, spesso rende le rappresentazioni del modello di inganno strategico "squisitamente accademiche" e, quindi, distanti anche dalla "più elementare forma di applicazione pratica".
ZOTTI D. (2010), La ´Deception´ - L'inganno nell'analisi delle informazioni e nella strategia - un pericolo ed un'opportunità, GNOSIS vol. 3/2010.

BOX N.2

Lo Stato Z, paese emergente quale nuova potenza globale, intende espandere la sua capacità di influenza geo-economica oltre i propri confini territoriali, acquisendo quote societarie di imprese di rilevanza strategica dello Stato K, paese avanzato di grandi dimensioni. I paesi emergenti, infatti, mediante mirati programmi di investimento ed acquisizione possono assicurarsi una presenza più strutturata nelle economie di paesi più avanzati, conquistando così "leve" di natura politica e strategica (sia direttamente nel paese in cui investono, sia nel sistema finanziario e politico internazionale) e rilevando il *know-how* e le tecnologie delle imprese estere nelle quali acquisiscono poteri di *governance*.

Lo Stato Z, al fine di conseguire il proprio obiettivo, rientrante nella sua *grand strategy*, valuta necessaria una operazione di mascheramento delle proprie attività al fine di eludere, in tutto o in parte, gli strumenti di protezione (normativi, finanziari ed *intelligence*) predisposti dallo Stato *target* per tutelare le proprie aziende di rilevanza strategica e difendere i suoi interessi nazionali. Lo Stato Z, conseguentemente, pianifica ed avvia una campagna di *deception* volta ad operare sui mercati internazionali - con particolare focus sul mercato dello Stato K - su due livelli:

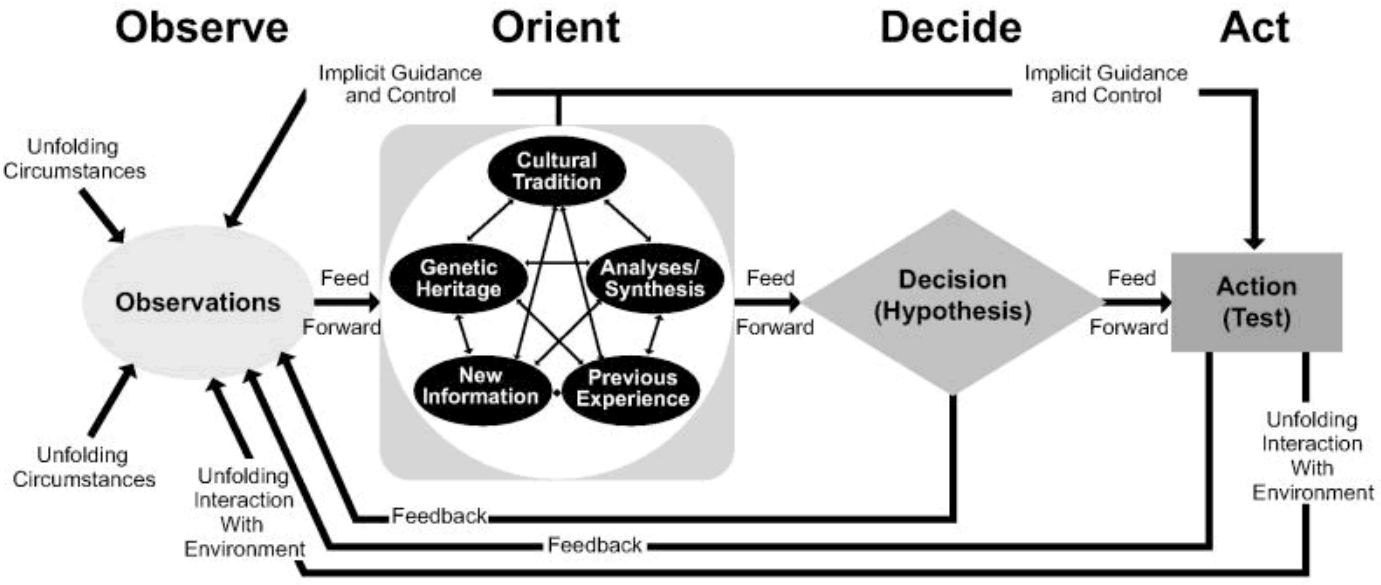
- in modo palese, utilizzando il Fondo Sovrano S1-Invest che vada ad investire nello Stato K in funzione delle prestazioni ottenibili rispetto agli indici di riferimento, con o senza coinvolgimento diretto nella *governance* delle società in cui investe. Tali operazioni di investimento del Fondo Sovrano sono vincolate ad obiettivi commerciali e di business e regolamentate - a livello internazionale - dai principi guida stabiliti nel 2008 a Santiago dal Fondo Monetario Internazionale e dall'OCSE (principi ad adesione volontaria), e - a livello nazionale - da specifiche norme dell'ordinamento interno (sia dello Stato Z, che controlla e gestisce il Fondo, sia dello Stato K *target* di investimento). La dotazione del Fondo S1-Invest è fondamentalmente alimentata da ricavi generati dall'esportazioni e dalla vendita di materie prime (di cui lo Stato Z è ricco), e, in secondo luogo, da surplus della bilancia dei pagamenti e da stock eccedenti di riserva di valuta ufficiale;

- in modo occulto, impiegando un organismo V3-Bank che, sebbene ufficialmente istituito quale ente depositario dell'intero ammontare delle riserve di valuta estera dello Stato Z (e, quindi, per finalità e competenze diverse da quelle proprie di un Fondo Sovrano), di fatto, per autonomia di investimento e per disponibilità di capitali, ha le stesse capacità di investimento all'estero di un Fondo Sovrano. Anzi, rispetto al Fondo Sovrano "ufficiale", tale organismo potrà operare svincolato dalle regole comportamentali fissate dai principi guida di Santiago del 2008, avere una dotazione finanziaria più elevata e mirare ad acquisire il controllo di aziende che svolgono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale dello Stato K o ad investire in strumenti, caratterizzati da un elevato tasso di rischio e/o da un alto tasso di liquidità, capaci di interferire sensibilmente sulla stabilità economico-finaziaria dello Stato K.

La campagna di *deception* ha come *target* il vertice politico ed economico-finanziario dello Stato K e come obiettivo quello di convincere il *target* che le attività di investimento all'estero dello Stato Z sono circoscritte al Fondo Sovrano S1-Invest.

I canali di comunicazione utilizzati per far giungere l'informazione non vera allo Stato K sono, in primo luogo, quelli relativi alla comunicazione istituzionale dello Stato Z (con specifico riferimento alle competenze ufficiali di S1-Invest e V3-Bank) e, secondariamente, i network inter-bancari, la rete degli operatori di borsa, i *social* media (con particolare riguardo a quelli maggiormente impiegati dagli operatori finanziari e broker).

Se il programma di *deception* viene pianificato accuratamente ed eseguito efficacemente dagli apparati *intelligence* dello Stato Z, in stretto coordinamento con il vertice delle istituzioni governative coinvolte (S1-Invest e V3-Bank), gli strumenti di protezione delle aziende di rilevanza strategica dello Stato *target* risulteranno orientati, inizialmente, verso il Fondo S1-Invest e, quindi, parzialmente compromessi. Lo Stato Z, infatti, riuscirà a condurre efficacemente la sua strategia di penetrazione negli asset strategici dello Stato K mediante l'organismo V3-Bank, che, almeno nel breve periodo, non sarà rilevato come minaccia ed opererà come un Fondo Sovrano "occulto", garantendo un significativo vantaggio strategico al *deceiver*.



3. *Deception* strategica e processo decisionale di vertice

Il soggetto che conduce l'operazione di *deception* strategica ha come scopo quello di influenzare le scelte della *leadership* avversaria, modificando la sua percezione della realtà o di uno specifico evento, fenomeno o situazione.

Come messo in risalto in precedenza, il soggetto che conduce l'operazione di *deception* strategica ha come scopo quello di influenzare le scelte della *leadership* avversaria, modificando la sua percezione della realtà o di uno specifico evento, fenomeno o situazione.

Vi è, pertanto, una stretta correlazione tra l'attività di *deception* strategica ed i processi decisionali di vertice della controparte.
Il bersaglio di un'attività di *deception* strategica "*is not the specific systems that are actually attacked, but rather the adversary's decision process*"[24]. In particolare, l'attenzione del soggetto che pianifica e gestisce un'operazione di *deception* deve essere rivolta al modo in cui le informazioni prodotte, trattate e «confezionate» sono acquisite, elaborate ed utilizzate dal *leader* avversario e, quindi, alla capacità di interferire ed influenzarne il processo decisionale.
I *decision maker* molto spesso non hanno il tempo necessario per raccogliere, filtrare, selezionare e valutare adeguatamente le informazioni a loro disposizione e sono, quindi, costretti ad assumere decisioni con livelli di incertezza, anche elevati, ed entro scadenze temporali molto ravvicinate. Tale condizione è potenziale causa di errori di valutazione e/o di decisione[25]. Per tali motivi, le *leadership* si avvalgono del supporto informativo e delle analisi e valutazioni prodotte, in primo luogo, dagli organismi *intelligence* e dalle strutture di staff, ma anche da altri fonti (ambiente accademico, *think-tank*, centri studi, media, internet, stampa, etc.).

24- JOHNSON L. S., (2007), Toward a Functional Model of Information Warfare, Center for the Study of Intelligence, C.I.A., consultabile all'indirizzo: www.cia.gov/library/center-for-the-study-of-intelligence
25- TEITELBAUM L., (2005), The Impact of Information Revolution on Policymaker's Use of Intelligence Analysis, Rand Corporation, Santa Monica, CA.

I processi decisionali di vertice, oltre ad essere strettamente connessi con l'efficienza e la funzionalità delle strutture *intelligence* e degli organi di staff, sono caratterizzati da quattro punti deboli che, dal punto di vista del *deceiver*, divengono quattro punti focali su cui fondare la pianificazione e la condotta di un programma di *deception* strategica affinché la stessa possa avere successo:

• mancanza di tempo del *leader* avversario e delle strutture di supporto (ad es. una tecnica che sfrutta tale elemento di debolezza è quella di saturare i canali di trasmissione con una quantità elevatissima di informazioni vere, parzialmente vere e/o false allo scopo di compromettere la capacità analitica e di valutazione del *decision maker*, dei suoi consiglieri e degli organismi *intelligence*);
• la ricerca da parte del *leader* avversario del consenso dei gruppi di potere, delle lobby, dell'opinione pubblica e, più in generale, della società civile; "*i decisori politici, condizionati dalla brevità del mandato, tendono a pensare a breve termine, sono ossessionati dall'agenda politica e in particolare dai problemi politici interni, avendo come primo problema il consenso dell'elettorato*[26] (una tecnica che, ad es., sfrutta tale elemento di debolezza consiste nell'influenzare i gruppi di potere, l'opinione pubblica e la popolazione dello stato avversario mediante mirate operazioni psicologiche, di disinformazione e propaganda; le reazioni di tali gruppi, infatti, potrebbero riverberarsi sul *decision maker*, sulla sua percezione e, di conseguenza, potrebbero orientare il processo decisionale nel senso desiderato dal *deceiver*);
• i *cognitive biases*[27] del decisore e degli organismi che lo supportano nelle decisioni (ad es. una tecnica che sfrutta tale fattore di debolezza consiste nel far pervenire delle informazioni al *leader* avversario – direttamente o per il tramite dei suoi apparati informativi – che confermino le sue aspettative o quelle delle sue strutture di supporto[28]; tale attività richiede, a monte, una profonda conoscenza dei processi cognitivi e percettivi della controparte che, come già posto precedentemente in risalto, costituisce uno dei fattori fondamentali della fase di pianificazione della campagna di inganno strategico);
• la molteplicità delle fonti e dei canali di informazione utilizzati dal decisore; si è già osservato che i *decision maker*, sebbene facciano ampio ricorso alle strutture tradizionalmente preposte ad offrire supporto informativo, acquisiscono informazioni anche da altri canali - i quali non sono sempre adeguatamente monitorati, filtrati e validati - come i media tradizionali, i *social media*, le reti socio-relazionali, etc. (una tecnica che, ad es., sfrutta tale elemento di debolezza consiste nell'individuare le fonti ed i canali utilizzati dal *leader* avversario per acquisire informazioni, «intossicarli» ed utilizzare gli stessi per veicolare i «pacchetti informativi ingannevoli»).

L'individuazione dei canali di «approvvigionamento informativo» e dei punti deboli del processo decisionale di vertice, è il presupposto per la pianificazione di un programma di *deception* strategica e, quindi, di quelle attività volte ad influenzare ed orientare le capacità di percezione del *target*.

26- GIANNULI A., (2009), Come funzionano i servizi segreti, Ponte alle grazie, Adriano Salani Editore, Milano.
27- I cognitive biases sono i giudizi (o pre-giudizi) non necessariamente corrispondenti all'evidenza, elaborati e sviluppati sulla base dell'interpretazione delle informazioni in possesso, anche se non logicamente o semanticamente connesse tra loro. In altri termini il cognitive bias è una forma di distorsione della valutazione causata dal pre-giudizio. Come evidenziato da Heuer, ciascun individuo vede e percepisce la realtà che lo circonda attraverso una «lente cognitiva», costituita dai propri preconcetti e dalle proprie inclinazioni, e tende inevitabilmente a ricorrere a «strategie semplificative» per formulare giudizi e/o assumere decisioni.
HEUER R. J. Jr., (1981), Strategic Deception…cit.
28- Il c.d. effetto "tunnel vision".

L'interferenza sui meccanismi percettivi della controparte avviene combinando in maniera coordinata due tipologie di azioni: una finalizzata a celare le reali intenzioni e capacità di chi conduce il programma di *deception* strategica, creando ambiguità ed incertezza su fatti e situazioni vere; l'altra indirizzata a creare certezza e fiducia nella controparte su fatti e situazioni non vere, rafforzando così le sue convinzioni preesistenti e inducendola a effettuare valutazioni errate.

L'interferenza sui meccanismi percettivi della controparte avviene combinando in maniera coordinata due tipologie di azioni: una finalizzata a celare le reali intenzioni e capacità di chi conduce il programma di *deception* strategica, creando ambiguità ed incertezza su fatti e situazioni vere; l'altra indirizzata a creare certezza e fiducia nella controparte su fatti e situazioni non vere, rafforzando così le sue convinzioni preesistenti e inducendola a effettuare valutazioni errate.

La combinazione di questi due fattori indotti dal *deceiver* (incertezza su ciò che è vero e certezza su ciò che non è vero), provoca il disorientamento del sistema percettivo e cognitivo del *leader* dello Stato avversario, il quale tende ad assumere delle decisioni a lui sfavorevoli da cui, al contrario, lo Stato *deceiver* trae vantaggio strategico.

4. *DECEPTION* ED AGENZIE DI *INTELLIGENCE*

Tutte le volte che un'attività di *deception* strategica va a buon fine, il soggetto attivo consegue un vantaggio competitivo per i suoi interessi strategici (e, conseguentemente, un successo), mentre il *target* subisce un fallimento. Nella maggior parte dei casi questo fallimento è attribuibile, in tutto o in parte, agli apparati *intelligence*: "*deception and intelligence failure are related concepts*"[29]. Ma cosa si intende per «fallimento dell'*intelligence*»? Citando un'autorevole definizione: "*an intelligence failure is essentially a misunderstanding of the situation that leads a government (or its miliary forces) to take actions that are inappropriate and counterproductive to its own interests*"[30].
Dall'esame della citata definizione, proveniente dalla letteratura statunitense, è possibile formulare due considerazioni:

- *deception* ed *intelligence failure* sono due facce della stessa medaglia;
- l'individuazione delle cause di fallimento dell'*intelligence* (e la predisposizione degli adeguati strumenti correttivi per evitare o ridurre la probabilità di manifestazione di *intelligence failure*) può contribuire significativamente a evitare e/o ridurre il rischio di essere ingannati mediante programmi di *deception* strategica condotti dall'avversario.

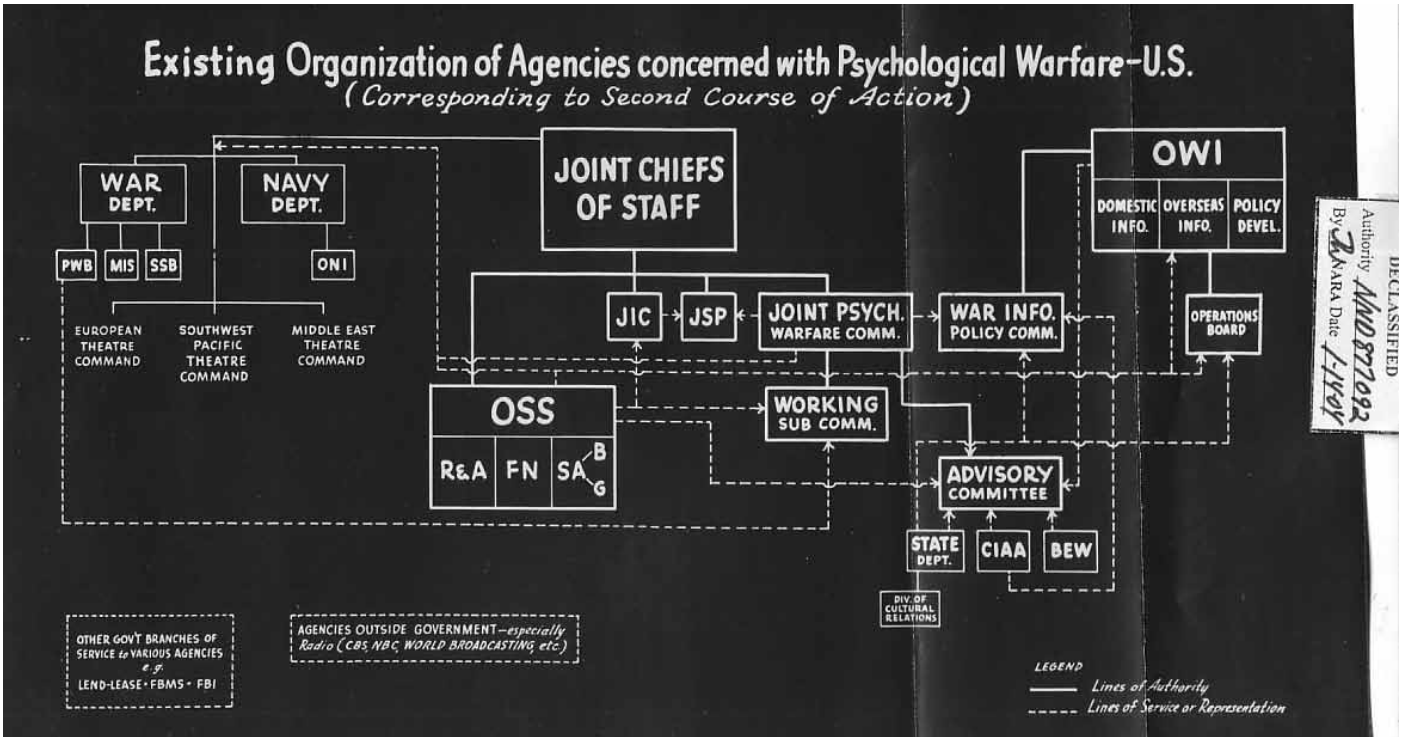
Per contrastare efficacemente le attività di *deception* condotte dagli avversari, oltre a conoscerne i meccanismi e le tecniche, è necessario:

- mascherare quanto più possibile i propri canali informativi reali, nel senso di predisporre delle misure che proteggano la riservatezza di tali canali; in altre parole, gli avversari, potenziali *deceiver* (stati, alleanze politico-militari, organizzazioni terroristiche, gruppi criminali organizzati, etc.), non devono essere in grado di conoscere i canali informativi della *leadership* di uno Stato o, comunque, possono riuscire ad individuarne solo un numero limitato, soprattutto in considerazione della loro specifica veste istituzionale (ad es. è ovvio che gli apparati *intelligence* siano i primi ad essere conosciuti e monitorati dalle *intelligence* straniere, in quanto tradizionalmente e funzionalmente preposti ad essere tra i primi canali informativi del decisore);
- rendere immediatamente conoscibili all'avversario alcuni canali di «approvvigionamento informativo», al fine di orientare su di essi le attività ingannevoli condotte;

29- SHULSKY A. N., SCHMITT G. J., (2002), Silent…cit.
30- SHULSKY A. N., SCHMITT G. J., (2002), Silent…cit.

• ampliare il numero dei propri canali informativi, non perdendo di vista, però, la necessità di validarne costantemente l'attendibilità e l'integrità; se il numero dei canali utilizzati è particolarmente elevato, la controparte, anche nell'ipotesi in cui sia riuscita ad individuarli, non disporrà delle risorse sufficienti per condurre su tutti attività di inganno strategico;

• alternare frequentemente i canali informativi, avendo cura di non utilizzare gli stessi per un periodo di tempo particolarmente prolungato; se i canali di «approvvigionamento informativo», oltre ad essere numerosi, sono utilizzati in modo alternato, per l'avversario sarà molto difficile rilevare quali siano impiegati in un dato momento e scegliere su quali focalizzare le attività di *deception*.



Gli organismi *intelligence*, ed in particolare le articolazioni di questi preposte all'analisi, devono continuamente considerare la possibilità di essere oggetto di attività di *deception* e, quindi, che la controparte stia provando a confonderli e/o ingannarli, celando qualche informazione rilevante o veicolandone qualcuna, in tutto o in parte, falsa. "*The possibility of deception cannot be rejected simply because there is no evidence of it*"[31].

31- HEUER R. J. Jr., PHERSON R. H., (2010), Structured Analytic Techniques for Intelligence Analysis, CQ Press.30- SHULSKY A. N., SCHMITT G. J., (2002), Silent…cit.
32 -HEUER R. J. Jr., PHERSON R. H., (2010), Structured Analytic…cit.

Oltre ad adottare gli accorgimenti sopra descritti, gli apparati *intelligence* - al fine di individuare per tempo e contrastare le operazioni di *deception* degli avversari - dovrebbero tenere sempre conto dei seguenti principi guida[32]:

• evitare di accordare un quantità eccessiva di fiducia su un'unica fonte e di alimentarsi prevalentemente da un unico canale informativo (come già evidenziato per i *decision maker*);
• essere costantemente diffidenti delle fonti umane, soprattutto se le stesse non hanno accesso diretto alle informazioni che forniscono ma si avvalgono, a loro volta, di altre fonti la cui attendibilità non è stata validata direttamente;
• non fondare le analisi esclusivamente su fonti «verbali», ma integrarle con elementi d'informazione tangibili e concreti (ad es. documenti, foto, numeri di telefono, etc.) e la cui attendibilità possa essere verificata;
• conoscere i limiti e le capacità dei potenziali soggetti *declive*, nonché i metodi e le tecniche impiegate in passato per condurre campagne di inganno strategico (a tal fine è fondamentale l'osmosi continua e la condivisione info-analitica, sia all'interno della comunità *intelligence* nazionale sia tra le *intelligence* di paesi alleati).

5. CONCLUSIONI

La *deception* strategica è un importante strumento a disposizione di uno Stato per il conseguimento di rilevanti obiettivi strategici in campo politico, militare, economico e tecnologico.

Come posto in risalto precedentemente, le dinamiche di funzionamento dell'attività di inganno strategico sono essenzialmente fondate sulla manipolazione della percezione, sulla compromissione della capacità di valutazione e sull'interferenza nei processi decisionali della controparte.

La *deception* di livello strategico è, infatti, "*the amalgamation of political, sociological, and psychological manipulation* […] *closely* [tied] *to the political objectives of a nation and directly affects the national fortune and interests*".

Gli Stati sono riluttanti ad utilizzare le attività di *deception*, sottovalutandone sensibilmente il valore e la capacità offensiva[33] e ritenendole spesso in contrasto con i principi etici e giuridici[34]. Sebbene le dinamiche caratterizzanti la *deception* di livello strategico non prevedano l'utilizzo di armi, così come convenzionalmente intese[35], e dall'impiego della stessa non derivino, in modo diretto, danni fisicamente rilevabili e/o perdite umane[36], tale strumento può essere annoverato tra i più avanzati ed efficaci mezzi a disposizione di uno Stato per la tutela dei propri interessi e per il contrasto alle minacce alla sicurezza nazionale. La condotta di operazioni di *deception* strategica, se portate a termine con successo, consente, infatti, ad uno Stato di conseguire legittimamente[37] un vantaggio competitivo nei confronti di uno o più attori avversari, con un impiego di risorse relativamente contenuto[38].

33- JAJKO W. (2002), Deception: Appeal for…cit.
34- PUMPHEREY D., ECHEVARRIA A., (2004), Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges, Triangle Institute for Security Studies (TISS) - U.S. Army War College Strategic Studies Institute (SSI).

La *deception* strategica, se implementata nell'alveo delle capacità degli apparati di *intelligence*, può divenire un utile strumento per consentire al sistema di sicurezza nazionale di raggiungere livelli più elevati di efficienza.

E' possibile affermare, in definitiva, che la *deception* strategica, se implementata nell'alveo delle capacità degli apparati di *intelligence*, può divenire un utile strumento per consentire al sistema di sicurezza nazionale di raggiungere livelli più elevati di efficienza[39].

Considerata la complessità che caratterizza la pianificazione e la gestione delle operazioni di *deception* strategica, la letteratura specializzata in materia[40] e la dottrina dominante[41] convergono nel sostenere che tale attività, per risultare efficace, debba essere attentamente pianificata a livello di vertice decisionale e realizzata integrando i principali attori strategici nazionali (governo, ministeri, forze armate, agenzie di *intelligence*).

In particolare, si ritiene opportuna l'istituzione di un organismo, permanente ed altamente specializzato[42], preposto esclusivamente alla *deception* strategica[43] (ed alla *counter-deception*) e collocato il più vicino possibile al vertice decisionale. Tale struttura, con un organico ristretto, dovrebbe essere composta da personale dotato di particolari e qualificate *expertise*, selezionato tra funzionari pubblici (provenienti da agenzie di *intelligence*, forze armate, ministeri, altre PP.AA.) ed esperti provenienti dal settore privato (economia, finanza, industria, telecomunicazioni, etc.) e dal mondo della ricerca (università e *think-tank*).
La ristrettezza dell'organico è necessaria a garantire:

- la massima riservatezza, sia in sede di pianificazione sia durante le fasi di esecuzione (nell'ipotesi in cui dovessero trapelare informazioni all'esterno, non solo andrebbe vanificata l'operazione, ma si correrebbe il rischio di provocare reazioni offensive dello Stato contro cui la *deception* è diretta);
- la continua e tempestiva condivisione delle informazioni all'interno dell'organismo;
- la dinamicità e la flessibilità della struttura (che sarebbero penalizzate da un organico elevato).

35- Oggi l'informazione, nella sua accezione più generale, così come sostenuto da Whitehead, è impiegata come un'arma, che può rivelarsi più potente e sofisticata delle armi convenzionali.
WHITEHEAD Y. L., (1997), Information as a Weapon: Reality Versus Promise, Airpower Journal, vol. 11, n. 3.
36- PIERANTONI F. e M., (1998), Combattere con le informazioni, Franco Angeli, Milano.
37- Come argomentato da Kiss, e anche da Pumphrey ed Echevarria, la deception strategica è da intendersi uno strumento legittimo per proteggere e/o difendere i valori fondanti di una società democratica e/o per contrastare i piani di un avversario che è intenzionato a minacciare l'ordine democratico di uno Stato e, conseguentemente, non si pone in contrasto con i principi etici universalmente riconosciuti. Il diritto internazionale non pone dei limiti o dei divieti relativi all'uso della deception; le norme del diritto internazionale umanitario vietano espressamente solo il ricorso alla «perfidia», intesa come attività ingannevole, condotta utilizzando segni distintivi e/o emblemi di istituzioni la cui neutralità e gli scopi pacifici sono riconosciuti universalmente (ad es. la Croce Rossa), al fine di infliggere un danno ad un avversario.
KISS E., (2003), Strategic Deception…cit.
PUMPHEREY D., ECHEVARRIA A., (2004), Strategic Deception...cit.
38- CADDELL J. W., (2004), Deception 101 - Primer on Deception, U.S. Army War College Strategic Studies Institute (SSI).
39- La deception strategica potrebbe garantire un ottimo rapporto costi/benefici, poiché richiede una quantità di risorse relativamente contenuta per la sua realizzazione, soprattutto se comparata con l'entità degli oneri di altri strumenti mediante i quali lo Stato persegue i propri interessi strategici e/o tutela la propria sicurezza nazionale (ad es. le attività diplomatiche, le campagne belliche, etc.).
40- A tale riguardo, vedasi, tra gli altri, i già citati autori Waltz, Daniel, Herbig, Jajko, Whaley.

La composizione eterogenea dell'organico, invece, assicurerebbe che il programma di *deception* possa acquisire il livello sufficiente di credibilità e coerenza agli «occhi» dell'avversario. Al fine di poter celare, in tutto o in parte, determinati eventi, fatti o situazioni e/o di poter creare delle certezze su eventi, fatti o situazioni non reali (o parzialmente reali) è indispensabile il coinvolgimento e la collaborazione di tutti i settori della pubblica amministrazione e del mondo privato, che, qualora necessario, potranno fornire le risorse adeguate per tutelare gli interessi nazionali mediante attività di *deception* di livello strategico.

Nel quadro della attuale architettura del sistema di sicurezza nazionale italiano, un organismo - permanente e specializzato - la cui *mission* istituzionale sia quella di pianificare, coordinare e gestire attività di *deception* strategica, troverebbe la sua collocazione più idonea nell'ambito della Presidenza del Consiglio dei Ministri e, precisamente, all'interno del Dipartimento delle Informazioni per la Sicurezza (DIS), istituito dall'art. 3 dalla legge n. 124/2007, legge costitutiva del Sistema di Sicurezza per le Informazioni della Repubblica (SISR). L'attività di contrasto alle operazioni di *deception* strategica condotte dagli avversari, invece, sempre mantenendo fermo il riferimento alle disposizioni ad oggi vigenti, sembrerebbe rientrare tra le funzioni dell'Agenzia informazioni e sicurezza esterna (AISE) e dell'Agenzia informazioni e sicurezza interna (AISI), ciascuna in base alle competenze previste rispettivamente dall'art. 6 (in particolare commi 1 e 3) e dall'art. 7 (in particolare commi 1 e 3) della citata legge n. 124/2007.

In prospettiva di una futura riforma normativo-organizzativa del SISR, tenuto conto delle esigenze di rafforzamento delle competenze del DIS[44] e di razionalizzazione della spesa[45], anche la funzione di *counter-deception* potrebbe essere attribuita al DIS, fermo restando il ricorso, qualora necessario, alle risorse umane e strumentali delle Agenzie, nonché a specifiche articolazioni delle altre pubbliche amministrazioni e/o a soggetti privati, per l'esecuzione di singole e circoscritte attività rientranti nei programmi di contrasto alle campagne di inganno strategico avversarie.

44- Per garantire maggiore unitarietà d'azione del Sistema.
45- Per conseguire gli obiettivi di contenimento della spesa dettati dal recente processo di spending review riguardante, più in generale, tutti gli apparati statali.

Editing e realizzazione grafica a cura di:

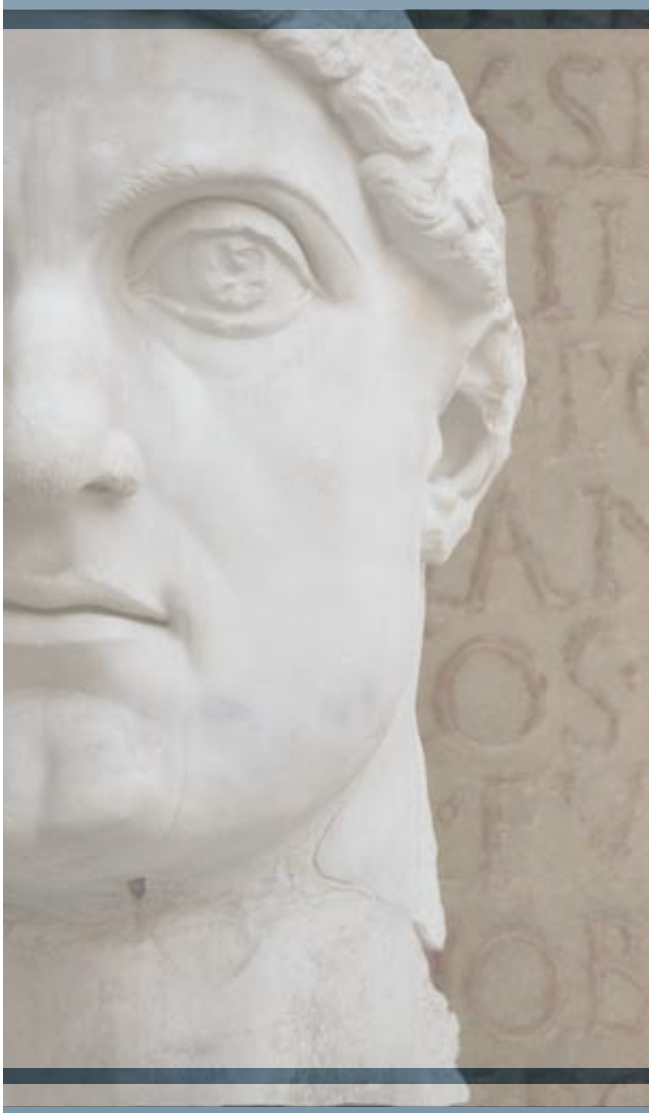
Leader in Digital Brand Management

Famebridge è partner del Think Tank
“Niccolò Machiavelli”.

Fondata e guidata da un executive manager che proviene da aziende quali Procter & Gamble, Johnson & Johnson e Adidas, FameBridge è una realtà Leader nel Digital Brand Management.

FameBridge ha di fatto una expertise unica nella realizzazione delle strategie digitali di Celebrities nazionali e internazionali di tutti i settori (Sport, Cinema, Giornalismo, Moda, Tv, Politica ecc). Questa expertise, unita alle solide competenze nei Social Media, parte integrante della strategia di business, rende FameBridge una società particolarmente efficace nel monitorare e influenzare i Consumatori, gli Utenti e la Pubblica Opinione per scopi di marketing.

www.famebridge.com



ISTITUTO ITALIANO
DI STUDI STRATEGICI

ITALIAN INSTITUTE
OF STRATEGIC STUDIES

Niccolò Machiavelli

L'Istituto Italiano di Studi Strategici "*Niccolò Machiavelli*" è un'associazione culturale senza scopo di lucro costituita a Roma nel 2010.

L'Istituto, think tank indipendente, nasce dall'iniziativa di un gruppo internazionale di personalità del mondo economico, accademico ed istituzionale civile e militare, con l'obiettivo di contribuire alla rinascita del pensiero strategico italiano.

La complessità e l'ampiezza delle sfide che attendono il Paese nel XXI secolo richiede conoscenza, consapevolezza e capacità prospettiche. L'Istituto Machiavelli, anche grazie al proprio network globale, promuove l'interscambio culturale tra il decisore italiano ed internazionale, pubblico e privato, e svolge attività di ricerca finalizzate ad elevare il livello di competitività globale del "Sistema Paese".

L'Istituto Machiavelli, autonomamente o in collaborazione con istituzioni, organizzazioni ed aziende nazionali ed estere, realizza studi ed analisi strategiche *policy-oriented*, organizza briefing, seminari e workshop, cura corsi di alta formazione per i *leader*.

Per ulteriori informazioni:

Istituto Italiano di Studi Strategici "Niccolò Machiavelli"
Via di San Basilio, 64
00187 – Roma
Tel.: (+39) 06 45422952
Fax.: (+39) 06 97259168
email: info@strategicstudies.it
http://www.strategicstudies.it