ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI

Sguardo all'attuale sistema di intelligence della Cina

L'efficacissima sintesi tra modalità tradizionali e capacità sempre più specialistiche

Arianna Pacioni

RESEARCH PAPER
Settembre 2016

ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI
www.fondazionegermani.org

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.

Arianna Pacioni dal 2007 lavora nell'ambito di una holding infrastrutturale italiana. I suoi principali interessi di ricerca si concentrano sull'analisi delle minacce ai sistemi-paese – con particolare riferimento al terrorismo e al crimine organizzato – e sullo studio delle pratiche di difesa degli *assets* strategici e degli interessi nazionali, con particolare riguardo all'analisi delle attività degli apparati di intelligence soprattutto non-occidentali.
E' Dottoressa magistrale cum laude in Scienze della Comunicazione presso La Sapienza di Roma con una tesi avente oggetto la Protezione delle Infrastrutture Critiche, e ha conseguito cum laude presso lo stesso ateneo il Master di specializzazione di II Livello in Geopolitica e Sicurezza Globale, con una tesi sull'emergenza ucraina.

ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI

SGUARDO ALL'ATTUALE SISTEMA DI INTELLIGENCE DELLA CINA

L'efficacissima sintesi tra modalità tradizionali e capacità sempre più specialistiche

Arianna Pacioni

RESEARCH PAPER
Settembre 2016

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

ISBN: 978-88-909073-0-2

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

INDICE

Sintesi del research paper 5

1) Gli assunti del paradigma della raccolta informativa in Cina:
gli elementi della tradizione 7
Letteratura di avanguardia: la cultura della "diffidenza e del sospetto" 7
Le tappe storiche: il transito dallo spionaggio domestico a quello rivolto verso l'esterno 9
La struttura di raccolta e processamento dell'informazione 12

2) La *business intelligence* di Stato:
economia di impresa versus sicurezza nazionale 26

3) Le modalità operative, le aree di intervento e il reclutamento:
la necessità di un parametro temporale insolitamente ampio
e di un approccio "olistico" per indagare le reali capacità
delle attuali Humint e Osint cinesi 31

4) Le avanguardie del sistema spionistico:
dagli attacchi cyber dei vecchi apparati della PLA
alla cyber-guerra permanente delle nuove unità spaziali,
elettromagnetiche e informatiche integrate 44

5) Conclusioni 50

SINTESI DEL RESEARCH PAPER

1) Il consueto appellativo di *human wave* e le connesse implicazioni concettuali, tradizionalmente usate per descrivere il *tradecraft* cinese, sono ancora attuali, ma non più esaustive per rendere conto dell'elevata acquisizione di *know-how* in termini di addestramento, specializzazione e tecnologia sviluppata in seno al comparto di intelligence della Cina negli ultimi decenni.

2) L'imponente apparato pluricentrico di emanazione informativa cinese gode ancora di bassi livelli di vulnerabilità, paradossalmente forniti proprio dal suo alto grado di complessità, ma uno sguardo attento alle dinamiche di transito ascensionale dei flussi informativi permette di identificare i centri primari di analisi da monitorare, ove il prodotto di intelligence si sedimenta e diventa "dialogo" tra le istituzioni "richiedenti" e gli apparati "rispondenti" ai bisogni informativi del decisore.

3) Il meccanismo di integrazione tra la raccolta di intelligence finalizzata alla sicurezza nazionale (militare e civile) e gli altri tipi e finalità di acquisizione informativa (*business intelligence*, *social intelligence*, *media intelligence*), posto totalmente sotto l'egida dello Stato, si dimostra fattore di sviluppo decisivo del sistema-paese, sia quando condotto clandestinamente, finanche con metodi illeciti, sia quando apertamente espresso dall'operatività e dalla politica economico-commerciale.

4) L'attuale riconoscimento del mondo Cyber come centrale per la difesa e la sicurezza nazionali – ma in termini più "offensivi" l'elezione dello stesso come ambiente operativo cardine per perseguire lo sviluppo del Paese a danno di altri sistemi concorrenti – rappresentano per l'apparato e la cultura di intelligence cinese un evidente passo avanti sulla via del rinnovamento. In particolare tale tendenza - resa manifesta dalla creazione dell'avanzatissima unità SSF (Strategic Support Force) per il controllo integrato dei satelliti, dello spazio elettromagnetico, del mondo Cyber e dell'ambito informatico - rappresenta l'eloquente emancipazione di un sistema per la raccolta informativa, da molti ritenuto finora organizzativamente semplicistico e obsoleto, verso un apparato sempre più complesso e più capace di misurarsi con le sfide proposte dalla competizione a livello globale.


ASTANA
RUSSIA
KAZAKHSTAN
Lake Balkhash
Lake Baikal
ULAANBAATAR
MONGOLIA
Hailar
Harbin
Changchun
Hunchun
Karamay
Ürümqi
BISHKEK
KYRGYZSTAN
Shenyang
NORTH KOREA
PYONGYANG
Korla
Kashi
TAJ.
Hohhot
BEIJING
PAK.
Hotan
Yinchuan
Shijiazhuang
Tianjin
SEOUL
SOUTH KOREA
Qinghai Hu
Taiyuan
Jinan
Qingdao
Lianyungang
Golmud
Xining
Lanzhou
Xi'an
Zhengzhou
CHINA
Nanjing
Shanghai
Hefei
Wuhan
Hangzhou
NEW DELHI
NEPAL
Lhasa
Chengdu
EAST CHINA SEA
BHUTAN
KATHMANDU
THIMPHU
Chongqing
Nanchang
Changsha
Fuzhou
Guiyang
TAIPEI
INDIA
Kunming
Xiamen
BANGL.
TAIWAN
INDIA
DHAKA
Guangzhou
Dongguan
Shenzhen
Foshan
Nanning
Macau
Hong Kong
PHILIPPINE SEA
HANOI
BURMA
Haikou
LAOS
Gulf of Tonkin
Hainan Dao
SOUTH CHINA SEA
ANDAMAN SEA
NAYPYIDAW
VIENTIANE
VIETNAM
PHILIPPINES
THAILAND
Paracel Islands
MANILA

1) Gli assunti del paradigma della raccolta informativa in Cina: gli elementi della tradizione

Ogni analisi che si occupi di indagare la cultura e l'apparato di intelligence della Cina non manca di fare riferimento ad alcune caratteristiche ritenute, da gran parte degli osservatori e studiosi, come elementi "assodati" della particolare modalità di "fare intelligence" delle istituzioni cinesi. Questa sorta di *consensus* attorno ad un *core* di elementi, per molti analisti non più in discussione, rappresenta quello che chiameremo la "tradizione", che appare oggettivamente presente (e innegabilmente operante) nel sistema spionistico come attualmente lo conosciamo, ma di gran lunga non più esaustiva per rendere conto di tutte le dinamiche oggi presenti nell'apparato nel suo complesso.

La presente analisi si propone di passare in rassegna tali "verità" acquisite, nel tentativo di prendere in esame come esse (o parte di esse) si siano modificate nel tempo, adattandosi alle esigenze imposte dall'apertura politica ed economica del paese verso relazioni internazionali sempre più complesse rispetto al passato e, soprattutto, come queste siano state trasformate da un inesorabile processo di secolarizzazione che, pur con tutte le accezioni e le lentezze del caso, è destinato ad interessare anche questa parte del mondo, all'apparenza rimasta finora più incolume dall'azione performante di questa variabile rispetto a quanto avvenuto altrove.

Letteratura di avanguardia: la cultura della "diffidenza e del sospetto"

La prima tra le verità incontrovertibili, generalmente presenti in numerosi studi sulla cultura di intelligence della Cina, è la diffusa attitudine del popolo cinese verso comportamenti di diffidenza e di sospetto verso l'altro in genere – specialmente se "straniero". Un tale atteggiamento risulterebbe legato all'importanza che "la raccolta informativa al fine di acquisire un vantaggio competitivo" rappresenterebbe in ambito cinese per il gestore del potere (che si tratti di decisore militare o politico) e viene spesso enfatizzata nella letteratura di settore facendo risalire le prime assunzioni a riguardo ad un'opera, di fatto riconosciuta come una pietra miliare dello studio sulle pratiche dello spionaggio, che fu per l'appunto prodotta in Cina: *l'Arte della Guerra* di Sun Tzu.

Al di là della nota querelle relativa al problema di attribuzione del testo[1], essa rappresenta la prova del fatto che la riflessione sull'essenzialità dell'acquisizione informativa sia stata, a livello globale, prerogativa dell'Impero di Mezzo e sia avvenuta in tempi oggettivamente molto più remoti (per questo testo in particolare si parla del VI secolo a.C.) rispetto a quanto avvenuto nel pensiero occidentale. Come effetto di tale primato, esisterebbe secondo molti osservatori una sorta di imprinting, determinato dalla tradizione sulla cultura cinese, che risulterebbe finanche nel modo di essere e di relazionarsi del cittadino medio che, nell'immaginario occidentale, sarebbe influenzato da una generale tendenza (tradizionalmente acquisita) alla diffidenza e al sospetto come attitudine intrinseca, piuttosto che come utile strategia, tesa alla salvaguardia del proprio interesse. In altre parole l'attività spionistica, intesa come risorsa in senso utilitaristico per il mondo occidentale, rappresenterebbe in Cina un carattere connaturato al modo di essere tipico cinese, un elemento insito nel DNA della loro cultura tradizionale.

Vero o no che si dimostri un assunto così generalizzante, è innegabile quanto il valore dell'acquisizione informativa sia sottolineato da un opera, quella di Sun Tzu, prodotta davvero precocemente in Cina e considerata non solo uno dei più importanti trattati di strategia militare di tutti i tempi, ma in senso lato uno strumento didattico di riferimento primario per l'operatività in contesti altamente competitivi - quali non a caso il mondo dell'economia e degli affari. In questa accezione, lo spionaggio ai fini della sicurezza nazionale o militare avrebbe lo stesso valore e la stessa rilevanza di quello condotto in ambito economico per fini di crescita e di sviluppo – binomio questo che, come è noto, è largamente attribuito all'attività offensiva portata avanti in Cina sotto l'egida dello Stato e di cui si tratterà nei paragrafi a seguire.

Inoltre, a suffragio dell'importanza attribuita all'utile prassi del sospetto, e dunque all'indispensabilità rivestita dall'attività della raccolta informativa, viene affiancata nell'opera la necessità della pratica della disinformazione che ancor più alimenterebbe quell'attitudine alla diffidenza che occorre praticare, sia in termini difensivi che offensivi, per risultare vincenti in contesti competitivi. Nel trattato infatti, e maggiormente nell'ambito dell'ultimo capitolo, il tredicesimo, interamente dedicato all'"uso delle spie", viene sottolineato che "il migliore degli stratagemmi che portano alla vittoria consiste nel fornire al nemico informazioni errate che lo inducano a valutazioni ingannevoli, al fine di sopraffarlo senza bisogno di combat-

[1] Etimologicamente, dietro all'appellativo Sun Tzu si nasconderebbe il titolo onorifico Sunzi (Maestro Sun) attribuito a Sun Wu, leggendario generale, stratega e filosofo cinese tradizionalmente riconosciuto come autore del libro e vissuto tra il VI e il V secolo a.C.. Ad oggi molti storici ritengono che l'attribuzione dell'opera a Sun Wu potrebbe in realtà essere un falso a causa della scoperta archeologica, avvenuta negli anni '70 del secolo scorso, di alcuni reperti che proverebbero l'esistenza di alcune parti, o parti nuove del testo, già note in epoca precedente alla nascita del presunto autore. Si veda in merito Wikipedia.it – voce: Sun Tzu.

tere". E' quanto mai legittimo ritenere che una sapienza millenaria di siffatto genere, sinteticamente espressa dall'esistenza (ed estrema attualità) di questa opera, abbia finito per confluire nel tessuto culturale di questo impero millenario e che influenzi in un certo modo oggettivamente la maniera di porsi nelle relazioni interpersonali, le modalità di condurre gli affari e l'azione nei contesti economici e, primariamente, per ciò che attiene questo studio, i metodi di acquisizione informativa tipici dell'intelligence e dello spionaggio.

Le tappe storiche: il transito dallo spionaggio domestico a quello rivolto verso l'esterno

Altro elemento primario nella tradizione degli studi sull'intelligence cinese è la trasformazione che il sistema di spionaggio avrebbe subito in seguito alla politica di apertura di Deng Xiaoping verso il mondo esterno, inaugurata fin dagli albori del suo insediamento al potere alla fine degli anni Settanta; in particolare, la fine dell'isolamento a cui condusse la sua politica commerciale e diplomatica avrebbe modificato la raccolta informativa cinese, inizialmente deputata al mantenimento del potere domestico e alla protezione dello status quo in patria, in un più moderno sistema di intelligence, votato ad una raccolta informativa più aggressiva verso competitors internazionali, al fine di consolidare la posizione strategica - soprattutto in senso economico commerciale - della Cina nel mondo. Mentre è indubitabile che un tale cambiamento sia di fatto avvenuto - e certamente per effetto di questo processo storico - vale la pena ripercorrere brevissimamente le tappe di questa evoluzione, per scorgere come il sistema spionistico abbia acquisito in origine in modo così forte la caratteristica "dell'operare in isolamento" da non essersene presumibilmente mai spogliato, anche successivamente allo sviluppo della politica di integrazione del paese nel sistema internazionale.

Il primo nucleo di moderna intelligence nazionale viene identificato secondo molta letteratura di settore nel CDSA (Central Department of Social Affairs) che in seno al Partito Comunista Cinese (PCC) rappresentò il primo organo strutturato di raccolta informativa, ampiamente costruito sulla base dell'esperienza dei Soviet[2]. Sappiamo che figura di spicco a capo della struttura – nonché generalmente riconosciuto come padre fondatore della moderna intelligence cinese - fu Khang Seng che nel corso dei suoi numerosi viaggi a Mosca apprese le modalità operative tipiche del *tradecraft* russo e le trasferì nell'unità sotto la sua direzione.

Notoriamente, con la vittoria del Partito Comunista sul Kuomintang di Chiang Kai-Shek avvenuta nel 1949, il sistema di intelligence subì una prima riorganizzazione che portò alla formazione di una struttura di intelligence duale costituita da

[2] Una diffusa trattazione della storia della nascita dei primi nuclei di spionaggio cinese negli anni '20, con ampia descrizione dei rapporti con la già avanzata intelligence russa, si trova in R. Faligot, *I servizi segreti cinesi* (Roma, Newton Compton, 2011).

un apparato civile (Ministry of Public Security-MPS) e uno militare (Military Intelligence Department-MID), sebbene questi risultassero sostanzialmente unificati dalla missione comune di proteggere il Partito da ogni possibile minaccia interna o esterna, tesa a mettere in discussione lo status quo nazionale appena costituitosi con la vittoria del Partito Comunista nella guerra civile.

Tale incarico, demandato ai servizi di intelligence, rimase invariato per tutti gli anni a seguire, dal '50 in poi, che rappresentarono l'era di dominio incontrastato di Mao Tse-Tung e della "Rivoluzione culturale" che ebbe il suo epilogo con la morte dello stesso avvenuta nel 1976 e la conseguente ascesa al potere di Deng Xiaoping. E' a quest'ultimo evento che viene fatto risalire l'inizio di quella dinamica trasformativa che renderà l'apparato di intelligence cinese più vicino alla forma con cui lo conosciamo oggi.

Dal punto di vista formale, per volere di Deng, le competenze in materia di raccolta informativa esterna vengono estrapolate dal MPS e fatte confluire in una nuova entità fondata nel 1983 e nota come Ministry of State Security (MSS). MID, MPS e MSS sopravviveranno nelle loro rispettive definizioni fino ai nostri giorni, come anche la propulsione assegnata da Deng alla specifica attività dell'MSS che diverrà importante in misura crescente nel corso degli anni proprio a seguito di quell'operazione di "apertura" di cui si è accennato rispetto alla politica estera della Cina.

Nel disegno di Deng infatti (portato avanti negli anni della sua reggenza dal '78 al '92[3]), il paese avrebbe dovuto aumentare il suo potere presso la comunità internazionale, uscendo dall'isolazionismo in cui era stata confinata dalla politica maoista, tessendo proficui rapporti diplomatici e commerciali che avrebbero portato di fatto la sua economia a svilupparsi incredibilmente negli anni a seguire.

In questo progetto, veniva assegnata all'attività di intelligence una funzione protettrice indispensabile, in quanto tale politica di apertura in nessun caso avrebbe dovuto implicare una pericolosa esposizione al contesto internazionale in termini di maggiore rischio e maggiore vulnerabilità del sistema-paese. Semplicemente, la Cina avrebbe dovuto sì svilupparsi economicamente e militarmente, ma senza che questo risultasse troppo evidente agli occhi di alleati come di nemici. Una tale

[3] Deng Xiaoping governò di fatto la Cina come capo del Partito, svuotando com'è noto di autorità la figura dei vari Capi di Stato che si succedettero nel corso della sua "reggenza". E' rilevante sottolineare che la fine della sua popolarità viene fatta risalire agli episodi di piazza Tienanmen avvenuti nel '89 a causa della dura repressione esercitata dallo Stato nei confronti dei manifestanti, al fine di sedare le rivolte di piazza. Le numerose vittime provocate dagli scontri portarono al decadimento dell'immagine di Deng presso la diplomazia internazionale, cosa che ne favorì la fine della carriera politica. Il fatto che il suo potere effettivo sia terminato anche per effetto del biasimo internazionale rappresenta un chiaro segnale storico dell'apertura effettivamente realizzata verso l'esterno dalla politica di Deng, dal momento che una tale capacità di influenza sulle vicende interne sarebbe stata impensabile in una fase isolazionista come quella appena precedente, sotto Mao Tse-Tung.

attitudine è ben espressa dal motto che sintetizzava la pratica di governo di Deng "nascondere la luminosità e nutrire l'oscurità", da intendersi nel senso di "aumentare il proprio potere clandestinamente, nascondendo il proprio potenziale crescente all'esterno", o anche "di nascondere le proprie ambizioni mentre si sviluppa la propria forza". Un'apertura dunque diffidente o per meglio dire più formale che sostanziale, un'applicazione perfetta della lezione appresa da Sun Tzu e puntuale reificazione del principio da lui promosso "se sei inattivo mostra movimento, se sei attivo, mostrati immobile".

Gli eventi storici fin qui richiamati spiegano efficacemente perché non si sia mai estinta quella sorta di attitudine degli apparati spionistici cinesi a "lavorare in isolamento" e con uno spirito di diffidenza verso pratiche di collaborazionismo che, anche qualora non possano certo dirsi tipiche dei rapporti tra apparati di intelligence dei diversi paesi in genere, risultano quanto mai avulse dal *tradecraft* cinese in particolare. Ciò in primo luogo per tradizione (come già espresso nel paragrafo precedente), in secondo luogo per effetto di un'apertura solo formale della politica estera e in realtà più che mai blindata (come appena ricordato a proposito della *open door policy* di Deng) e infine per la contingenza storica peculiare della genesi dei primi nuclei di intelligence. A conferma di quest'ultimo punto, vale ricordare il clima di totale emarginazione ove si trovarono ad operare le prime formazioni dedite alla raccolta informativa per conto del Partito Comunista in Cina negli anni '20[4]. In proposito, sappiamo che nel 1927 il Partito prese la città di Shanghai in un primo momento con la collaborazione del Kuomintang, che di lì a poco però gli si oppose divenendo successivamente l'avversario da combattere per tutto il corso della guerra civile che ne seguì fino al 1949.

A seguito del "tradimento" del Kuomintang, il Partito Comunista rimase completamente isolato, dovendo affrontare nel contesto urbano di Shanghai un compatto fronte comune costituito dall'alleanza anti-comunista delle organizzazioni criminali operanti nella città – le cosiddette Green Gang – e dalle forze di polizia delle concessioni straniere simpatizzanti per il Kuomintang. Il periodo di accerchiamento delle formazioni comuniste, passato alla storia come il "terrore bianco", determinò la forte necessità di costituire uno Special Department (SD) in seno al Partito Comunista (primo embrione appunto del futuro apparato di intelligence cinese) orientato ad operare clandestinamente in totale isolamento, in quanto senza possibilità di alleanza e/o cooperazione alcuna al fine di garantirsi la sopravvivenza.

Inoltre, occorre considerare come tali circostanze fossero comunque destinate a peggiorare, allorché alla fine degli anni '50 sarebbe maturato l'allontanamento dalla Russia, unico alleato possibile nel contesto storico di allora. Il distacco dal co-

[4] Per il dettaglio degli eventi citati si veda P. L. Mattis, "Assessing Western Perspectives on Chinese Intelligence", *International Journal of Intelligence and Counterintelligence*, Vol. 25, no. 4 (Dicembre, 2012)

munismo dei Soviet, infatti, finì per rappresentare la definitiva accentuazione di un modus operandi già allora fortemente radicato e tutt'oggi determinante, quell'abitudine alla prassi spionistica e alla raccolta informativa solitaria - nel senso di una operatività totalmente priva di connessioni con potenziali *partners* strategici[5].

La struttura di raccolta e processamento dell'informazione: un sistema numericamente imponente, apparentemente pluricentrico e mal coordinato, che sorprendentemente funziona. Il collante valoriale/culturale del Confucianesimo

Altro elemento tipico della tradizione di studi che hanno come oggetto l'apparato di intelligence cinese è il riferimento ad una struttura di fatto molto complessa che appare difficilmente esaminabile a causa dei molteplici apparati che si sovrappongono gli uni agli altri e alle funzioni che si sovrascrivono le une sulle altre - senza peraltro che quelle sostituite smettano di esistere o perdano davvero capacità operativa. In effetti, data una siffatta proliferazione di enti e centri di potere – sottoposti tra l'altro apparentemente a diverse linee gerarchiche – non è sempre facilissimo determinare l'itinerario dei flussi informativi, riconoscere i centri di analisi che svolgono l'attività di elaborazione più complessa della mole di dati che arriva dal basso e soprattutto identificare i destinatari delle attività di raccolta che, come in ogni ciclo di intelligence da manuale che si rispetti, dovrebbero di fatto ridiventare alla fine del processo - ed essere in verità al tempo stesso - committenti delle richieste informative, per far sì che il ciclo soddisfi le esigenze reali del processo decisionale.

L'impossibilità di rintracciare gli elementi di cui sopra, finisce per far apparire tutta la struttura come un enorme nebulosa, la cui attività, a parte rimanere ovviamente clandestina per le oggettive necessità degli apparati deputati a tale funzione in ogni nazione – risulta essere a tratti completamente incomprensibile agli occhi degli osservatori. Inoltre, ad aggravare l'inafferrabilità della materia, tutta la struttura, osservata a livello macro, ma anche nel dettaglio dei suoi singoli dipartimenti, si mostra particolarmente imponente dal punto di vista numerico, con ingentissime quantità di risorse destinate alle diverse funzioni, elemento questo ovviamente in linea con la capacità demografica di una nazione che si è da sempre imposta per i numeri legati alla vastità della sua popolazione, sia in termini assoluti che relativi rispetto alla media degli Stati del globo.

Per produrre alcune osservazioni al riguardo, sarà utile servirsi di una delle forse più complete rappresentazioni figurative che siano state prodotte dell'apparato

[5] Nella parte conclusiva di questa analisi si accennerà a come questa attitudine al metodo solitario stia sottilmente e apparentemente venendo meno, dal momento che si rilevano recentissimamente diversi segnali di collaborazione con apparati di intelligence di nazioni strategicamente selezionate dalla Cina, sulla base soprattutto di suoi interessi economici.

spionistico cinese – quella proposta dal centro studi americano *Stratfor*[6] – che è anche una delle più recenti attualmente in circolazione. In primo luogo, essa consentirà di riflettere sulla complicata linea gerarchica cui è sottoposto l'insieme degli enti deputati alla raccolta informativa (figura 1).

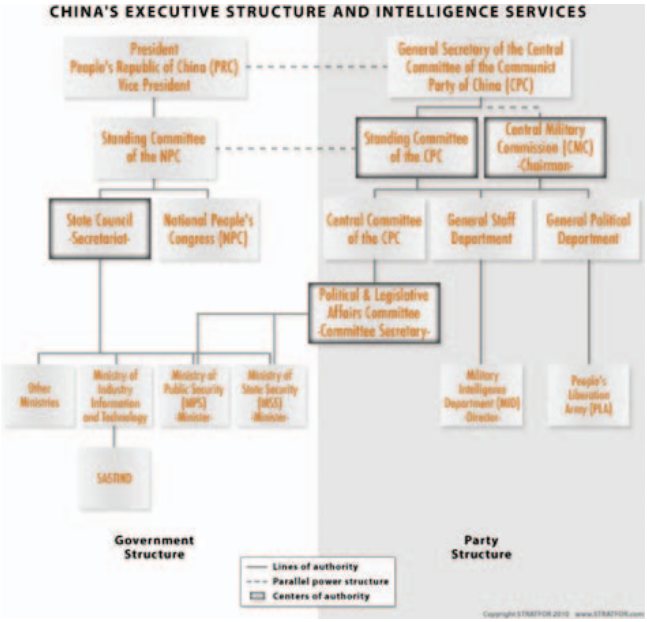

Figura 1 (Fonte: Report "Special series: Espionage with Chinese Characteristics", *Stratfor*, 24 marzo 2010)

Secondo *Stratfor*, nella struttura esecutiva dei servizi di intelligence della Cina[7], MPS e MSS (rispettivamente i servizi di sicurezza interni ed esterni) sono posti sotto l'autorità della struttura di governo – e precisamente sotto il Consiglio di Stato alle dipendenze del Presidente. Il MID invece, il Dipartimento di Intelligence Militare, è posto alle dipendenze dello Stato Maggiore Generale e dunque, attraverso l'autorità della Commissione Militare Centrale, direttamente sotto il Segretario Generale del Partito Comunista.

Uno schema di questo tipo suggerirebbe quindi la presenza di due grandi poli di emanazione di intelligence, una civile controllata dallo Stato/Governo (MPS e

[6] La fonte cui si fa riferimento è la seguente analisi: "Special Series: Espionage with Chinese Characteristics", *Stratfor*, 24 marzo 2010. Va però sottolineato che ovviamente essa – in quanto scritta in epoca precedente - non recepisce le modifiche al sistema di raccolta informativa apportate dall'operazione di risistemazione e riorganizzazione degli apparati – soprattutto militari – portata avanti da Xi Jimping e che sta interessando soprattutto i dipartimenti che si occupano di cyber-sicurezza di cui si parlerà diffusamente nei paragrafi conclusivi di questo lavoro.

[7] Si veda lo schema rappresentativo della struttura proposto dall'analisi di *Stratfor* e qui riportato in nella figura n. 1.

MSS) e una militare sotto l'egida del Partito (il MID). Eppure nel sistema cinese, sappiamo che lo Stato è direttamente controllato dal Partito e, data la presenza di un unico soggetto politico alla guida del paese, una tale distinzione di fatto perde di senso. In effetti, il Capo dello Stato/Presidente della Repubblica Popolare di Cina e il Segretario Generale del Partito di fatto coincidono (attualmente nella persona di Xi Jimping), rivelando un'estrema saldatura anche dal punto di vista formale.

Tale congiunzione è espressa (come figurativamente richiamato dallo schema) da un organo – la Commissione Permanente (Standing Committee) - presente sia nel governo sia nel Partito, come una sorta di struttura doppia, e ancor più palesemente dalla Commissione Militare Centrale, divisa addirittura in due istituzioni parallele ma identiche che condividono identici nome, composizione e presidenza[8].

In questo modo, quello che potrebbe essere usato come utile criterio di semplificazione - e cioè il principio che la struttura sia sottoposta comunque in modo forte al controllo del Partito – perde il suo carattere di esaustività, in quanto non riesce da solo a spiegare le dinamiche e i rapporti gerarchici tra le singole parti di una struttura così complessa. A prova di ciò, si veda come gli organi centrali del Partito, pur avendo un controllo indiretto su tutte le strutture come sopra descritto, non rinuncino a detenere in modo ridondante anche un controllo diretto, attraverso istituzioni create ad hoc per supervisionare apparati che, anche se solo formalmente, sarebbero sotto l'autorità dello Stato.

E' il caso della Commissione per gli Affari Politici e Legislativi, organo costruito ad hoc nella struttura di partito che possiede una linea gerarchica diretta proprio su MPS e MSS. Occorre tuttavia sottolineare che talvolta la doppia (anche triplice) linea di comando è giustificata dai rapporti operativi che una funzione deve tenere con i diversi comparti, a causa dell'uso molteplice che è possibile fare delle informazioni raccolte da un determinato dipartimento, ma in ogni caso tale esigenza non è primaria rispetto a quella di poter tenere sotto esame una stessa struttura da diversi punti di controllo diretti e indiretti.

Un esempio eclatante in proposito è rappresentato dalla State Administration for Science, Technology and Industry for National Defense (SASTIND). Essa costituisce il braccio scientifico della raccolta informativa (una funzione quindi com'è noto molto simile a quella della DARPA statunitense), orientando la raccolta informativa di MSS e MID, fornendo raccomandazioni alla Commissione Militare per pianificare l'attività di sviluppo tecnologico e, secondo *Stratfor*, mandando in missione suoi propri agenti al fine di acquisire segreti del comparto della difesa

[8] Si veda il dettaglio di questa particolare istituzione duale su Wikipedia alla voce "Commissione Militare Centrale (Cina)".

quando è richiesta un'alta specializzazione per l'attività spionistica[9]. E' chiaro che su un organismo così vitale, le istituzioni cinesi abbiano provveduto ad attivare molteplici linee di controllo. Così la SASTIND, posta alle dipendenze del Ministero dell'Industria, dell'Informazione e della Tecnologia, dipende nella struttura di governo dal Consiglio di Stato, ma è sottoposta altresì ad un controllo diretto della Commissione Militare Centrale[10] (figura 2).

Figura 2 Fonte: Report "Special series: Espionage with Chinese Characteristics", *Stratfor*, 24 marzo 2010.

Infine, é impossibile non citare in proposito la doppia linea di controllo cui è assoggettato il MID. Strutturalmente esso dipende dallo Stato Maggiore Generale della People's Liberation Army (PLA)[11] e quindi è direttamente alle dipendenze

[9] In particolare il *think thank* statunitense suggerisce che gli agenti della SASTIND siano per lo più scienziati coinvolti nella raccolta di *open source intelligence* che avverrebbe attraverso la partecipazione degli stessi a conferenze di settore in ambito internazionale e a scambi accademici di vario tipo. I dati così raccolti servirebbero per indirizzare l'attività più clandestina condotta da agenti del MID o MSS, al fine di acquisire i dati segreti veri e propri, giudicati prioritari dagli operatori della SASTIND per lo sviluppo e l'innovazione tecnologica dell'apparato di difesa della Cina. In realtà, è ragionevole pensare che tale competenza scientifica venga utilizzata per favorire l'acquisizione di tecnologia e *know-how* non solo a vantaggio della Difesa, ma dell'industria cinese in genere – come meglio spiegato nel paragrafo successivo. Inoltre quest'attività specialistica è particolarmente esemplificativa della raccolta informativa stratificata, nel senso di acquisita in modo plurale a diversi livelli, che è tipica del metodo spionistico cinese attuale e alla quale sarà dedicata una specifica trattazione in un paragrafo a seguire.

[10] Si veda schema proposto da *Stratfor* della Commissione Militare Centrale e dell'Intelligence Militare qui riportato nella figura 2.

[11] Cfr. nota 7.

della Commissione Militare Centrale, la quale però ha di nuovo provveduto ad attivare una parallela linea di controllo attraverso il General Political Department (GPD). Quest'ultimo sovraintende ad una attività di sorveglianza molto stretta su tutte le funzioni del MID, finanche alle singole persone che vi operano, piazzando agenti che fungono da cellule di monitoraggio ad ogni livello del sistema, al fine di verificare che i compiti assegnati vengano svolti nella direzione delle indicazioni fornite dal Partito, di sondare l'effettivo senso di appartenenza e fedeltà alle istituzioni e, in breve, di disinnescare le possibili derive di organi che, maneggiando di fatto lo strumento militare, potrebbero rappresentare una minaccia per il sistema, riuscendo quindi a prevenire in ultima analisi persino potenziali colpi di Stato.

Va detto che, nonostante la rilevanza soprattutto politica dell'organo e l'apparenza di una struttura disciplinare deputata soprattutto al controllo interno, si ritiene che dietro di esso si celi in realtà il braccio più operativo di controspionaggio del MID. D'altra parte, la verifica della lealtà degli ambienti operativi di intelligence è portata avanti in modo costante da una grande quantità di piccoli nuclei investigativi inseriti ad ogni livello – sebbene, anche in questo caso, non risulta per nulla di per sé evidente a chi arrivi e che percorso faccia la l'informazione raccolta da tali dipartimenti. Si veda a titolo esemplificativo, tra queste unità, il Bureau n. 9 (Contro-sorveglianza e Anti-defezione), inserito in una sorta di Ufficio Amministrazione del Personale all'interno dell'MSS.

Oltre alla molteplicità degli enti di controllo fin qui descritta, partecipano a rendere indistricabilmente complessa tutta la struttura due altri aspetti: la molteplicità dei luoghi deputati all'analisi ed elaborazione dei dati e l'estrema capillarità con cui il controllo dei servizi di informazione di sicurezza è distribuito sul territorio e sulla popolazione.

In merito al primo punto, come già sottolineato, l'individuazione dei luoghi di elaborazione e analisi consentirebbe di far luce sugli ambienti ove avviene effettivamente l'estrazione della conoscenza utile ai processi decisionali e permetterebbe di evidenziare le figure o le cariche che fungono da *leaders*/orientatori dei processi, o almeno da fruitori/consumatori finali dei prodotti informativi. *Stratfor* – come altre analisi a dire il vero – suggerisce che le funzioni che verosimilmente detengono a più alto livello tali responsabilità sono sicuramente il Direttore dell'MSS (con un ruolo rilevante nell'ambiente di governo, ma non nel Partito), il responsabile della Commissione per gli Affari Politici e Legislativi – per i compiti di controllo cui si è accennato sopra - e certamente più di tutti il capo della Commissione Militare Centrale e della Commissione Permanente del Partito Comunista.

Tuttavia, sebbene una realistica mappatura dei "luoghi" effettivi ove è presumibile che si produca l'attività decisionale e la fase di analisi non appare realizzabile con le informazioni attualmente a disposizione, è comunque possibile fare alcune considerazioni.

Dalla letteratura di settore emerge che l'estrema pluralità di enti in competizione tra loro[12] e l'ingente burocrazia presente nella struttura di intelligence nel suo complesso, blocca il transito delle informazioni e diminuisce le potenzialità collaborative tra le diverse parti dell'apparato in entrambe le direzioni possibili: dall'alto verso il basso (anzi bassissimo, se si considera l'estrema capillarità cui si accennava in merito al controllo della popolazione e del territorio da parte dei servizi informativi) e in modo orizzontale tra i diversi comparti ai vari livelli che svolgono funzioni diverse; una sorta di complicato sistema a camere stagne, intrecciate nelle due direttrici orizzontale/verticale e noto con il nome di *tiao-kuai guanxi*.

Tali cesure sono delle vere e proprie distorsioni dell'efficienza che il sistema dovrebbe essere in grado di produrre e rappresentano dunque una fortissima vulnerabilità che indebolisce la capacità operativa, potendo indubbiamente essere sfruttate da elementi esogeni che volessero infiltrare i vari comparti - a patto però di superare il sistema di controlli diffusamente estensivo di cui si è parlato che consente una sorta di autoprotezione dall'interno dei singoli dipartimenti, laddove dovesse venire meno, a causa della complessità del sistema, l'ombrello protettore fornito dalle posizioni gerarchicamente sovraordinate.

Molti analisti non mancano di sottolineare, infatti, come una tale vulnerabilità sia allo stesso tempo un elemento di forza, dal momento che riuscire ad orientarsi nei lacci e lacciuoli di un sistema di relazioni così eterogeneo e ridondante si rivela di fatto piuttosto improbabile, specialmente per un elemento estraneo al corpo. Inoltre, questa capacità di autodifesa rispetto a minacce esterne, cui è resa estremamente difficile la penetrazione degli apparati, si accompagna ad un'elevata capacita di protezione da possibili fenomeni endogeni di eversione interna che, ancorché risultino sottoposti ad una raffinata attività di controllo come visto, incontrerebbero comunque anche una forte difficoltà ad organizzarsi e rendersi operativi, proprio a causa della qualità rarefatta dei rapporti tra le parti e alla loro incapacità di comunicare efficacemente. In altre parole le Autorità cinesi, nella prassi e nella cultura, favoriscono e incentivano un sistema chiuso all'esterno, ma anche tra le sue singole parti, in quanto in tal modo avrà maggiori probabilità di rimanere tanto più vulnerabile al controllo centrale quanto meno vulnerabile agli attacchi esterni.

Tenendo a mente questo dato e proponendosi di voler indagare il viaggio che l'informazione effettuerebbe nell'ambito del sistema esaminato, è possibile partire dall'assioma che tutto il prodotto informativo raccolto deve fluire dal livello locale a livello nazionale, all'interno delle strutture di Partito, in quanto uno dei principi notoriamente operanti è quello che l'informazione deve essere resa obbligatoria-

[12] Per rendere l'idea della competizione esistente tra diversi enti e della loro frequente sovrapposizione funzionale, si pensi che *IHS Jane's* riferisce che in uno studio condotto nel 2012 da International Crisis Group vennero identificate ben 11 diverse agenzie di intelligence autoproclamantesi come agenzie primariamente responsabili della raccolta informativa per la sola area sensibile del Mar Cinese Meridionale.

mente ai vari livelli del Partito prima di poter transitare alle strutture di governo - e sappiamo in proposito che tale itinerario ascensionale si rivelerà per così dire molto lento[13] a causa della farraginosità dell'apparato.

Inoltre, una volta che l'informazione avrà raggiunto i vertici del Partito, sappiamo che esso tenderà per diffidenza a condividere molto poco con le strutture parallele presenti nell'ambito di governo e dunque è ragionevole ritenere che la maggior parte dei dati rimanga confinata proprio nell'ambito del Partito. Per effetto di ciò, tra le molteplici unità cui sembra deputata l'attività di analisi, occorre presumibilmente tenere in considerazione maggiormente quelle a più alto livello su cui vediamo che insiste un controllo più diretto da parte degli organi di vertice del Partito - come ad esempio le unità "attenzionate" dalla Commissione Permanente del Partito (Standing Committee).

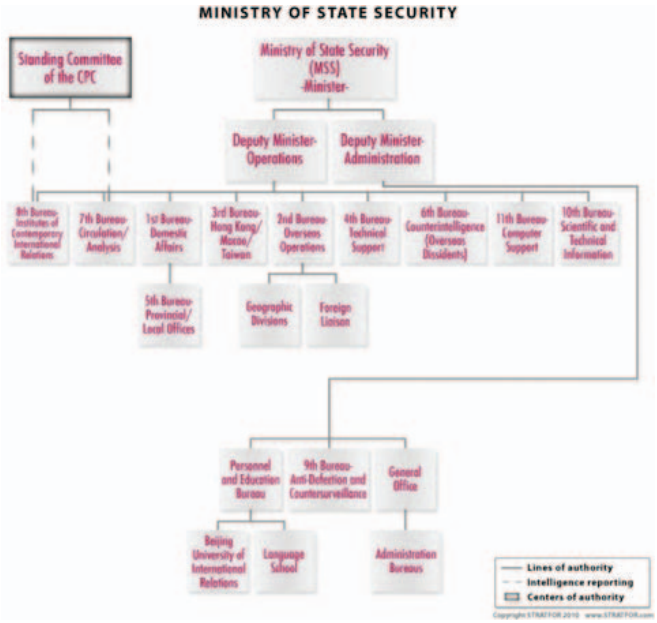

Figura 3 Fonte: Report "Special series: Espionage with Chinese Characteristics", *Stratfor*, 24 marzo 2010.

[13] Una conseguenza esemplare di tale lentezza è l'operatività locale cui finisce per essere confinata l'attività dell'MPS. Secondo *Stratfor* la cesura locale/nazionale è così forte in quest'organo che le operazioni di intelligence interna sarebbero efficaci solo nell'ambito delle città o delle singole province, nella totale assenza di connessioni che consentano un'analisi utile ad effettuare delle astrazioni più macro, permettendo così di contrastare i fenomeni a livello più elevato. Così i gruppi dissidenti tendono ad essere infiltrati e smantellati esclusivamente quando agiscono a livello locale. Questo genere di successi limitati tuttavia – sostiene ancora *Stratfor* – è risultato finora bastevole per mantenere sotto controllo il generale fenomeno della dissidenza, in quanto esso sembra tendere di fatto a prodursi efficacemente solo a livello urbano e dunque la sua genesi viene bloccata sul nascere prima che possa elevarsi a minaccia di carattere nazionale. Ma non è affatto detto che in futuro tale caratteristica perduri.

Volendo prendere in esame un caso pratico in proposito, si veda quello degli uffici preposti all'attività di analisi nell'MSS (Figura 3)[14]. Dalla struttura che è nota, la raccolta informativa a più basso livello viene qui effettuata dal Bureau n. 5 (attivo in un ambito locale/provinciale in cui l'MSS condivide l'operatività con l'MPS[15]) e da diverse altre entità diffuse a livello internazionale, note come Divisioni Geografiche e Collegamenti Esteri. E' presumibile ritenere che l'elaborazione dei dati raccolti da tali entità debba avvenire a livello superiore e cioè, rispettivamente, presso il Bureau n. 1, cui fanno capo gli Affari Domestici, e presso il Bureau n. 2 che sovrintende alle operazioni condotte all'estero - in modo tale quindi che il flusso informativo arrivi direttamente all'Ufficio del Vice Ministro delle Operazioni dell'MSS da cui entrambe queste unità dipendono.

In realtà però nella struttura effettiva, tale linearità è spezzata dalla presenza di una struttura parallela – il Bureau n. 7, deputato appositamente alla Circolazione dell'Analisi – che, benché dipenda anch'esso dall'ufficio del Vice Ministro delle Operazioni, è sottoposto addizionalmente al controllo diretto della Commissione Permanente del Partito (Standing Committee) ed è dunque ragionevole pensare che la primaria transizione del flusso avvenga proprio tramite quest'organo. Inoltre, applicando lo stesso ragionamento all'inverso, dal momento che nell'ambito dell'MSS un altro ufficio è sottoposto alla medesima autorità della Commissione Permanente – il Bureau n. 8, che funge da raccordo tra gli Istituti per le Relazioni Internazionali Contemporanee (ICIR) – si può presumere che anch'esso sia centro di analisi e ingranaggio fondamentale per il transito delle informazioni verso gli effettivi responsabili del processo decisionale[16].

Quest'ultimo dato in effetti appare perfettamente in linea con le note indiscrezioni circa il ruolo svolto dai centri studi in Cina, i quali risulterebbero attivissimi nelle prassi di spionaggio come anche nella conduzione di *covert operations*: si stima che circa il 70% del totale di quest'ultime sarebbero condotte dai *think tank* che ai diversi livelli popolano tutta la struttura pubblica della Cina, come anche da quelli attivi in ambito apparentemente privato. Tra questi merita menzione a titolo esemplificativo l'International Liaison Department che, ufficialmente costituito per intrattenere rapporti con le formazioni di orientamento comunista presenti nel mon-

[14] Si faccia riferimento allo schema proposto da *Stratfor* dell'apparato funzionale dell'MSS - qui riportato nella figura 3.

[15] E' noto agli osservatori che i dipartimenti di intelligence interna ed esterna collaborano molto attivamente nel contrasto a fenomeni che si sviluppano a livello locale, ma sulle dinamiche di questa collaborazione ci sono purtroppo pochissimi dati disponibili.

[16] Secondo *IHS Jane's*, l'ICIR funzionerebbe come *think thank*, ma anche come istituto di formazione e reclutamento dell'MSS – e dunque a maggior ragione sotto il totale controllo del Partito. Altre sue responsabilità prevederebbero l'analisi e il monitoraggio degli sviluppi della politica e sicurezza internazionali, nonché lo proattività a stabilire relazioni con ricercatori stranieri ospiti in patria che potrebbero potenzialmente rivelarsi candidati utili ad essere reclutati come informatori.

do, ha finito per essere impiegato per fomentare fenomeni di ribellione in territori strategici durante la Guerra Fredda.

Ancora – senza alcuna pretesa di essere esaustivi e oltre quelli di cui si è già parlato, quali la SASTIND o gli ICIR – si possono citare gli Istituti Confucio (che svolgerebbero attività di influenza, selezionando al tempo stesso per l'MSS opportunità di reclutamento), l'Ufficio di Informazione d'Oltreoceano del Dipartimento della Propaganda verso l'Estero, la Xinhua News Agency (che risulta aver fornito attività di copertura per ufficiali dell'MSS, oltre a condurre ricerca da fonti aperte traducendo e monitorando l'informazione delle agenzie di notizie estere).

Infine, una menzione a se stante merita in proposito il Dipartimento Centrale per il Fronte Unito. Si tratta di un'organizzazione costituita in seno e alle dirette dipendenze dal Comitato Centrale del Partito e che si comporta come un'agenzia di influenza - a tratti come un'organizzazione di contatto culturale - e in ogni caso risulta essere un autentico propulsore del *soft power* cinese nel mondo. Venne istituito durante la guerra civile – per alcuni sarebbe presente nel Partito fin dal 1921 – ma dopo diversi anni in cui rimase dismesso, la sua attività venne ripristinata a partire dal 1979 da Deng Xiaoping, in perfetto accordo con la prassi di colonizzazione dello spazio culturale e diplomatico esterno inaugurata dalla sua politica di apertura al mondo.

Questa struttura costituisce il legame primario del Partito con i gruppi di orientamento non comunista presenti in Cina e all'estero, comprese minoranze politiche concorrenti e gruppi etnici e religiosi minoritari. Dietro, e in aggiunta, a tale attività formale, viene ritenuto che l'agenzia svolga notevoli attività clandestine di infiltrazione e spionaggio. Secondo alcuni[17] si tratterebbe in particolare della gestione di importanti dossier relativi a diverse nazioni, attività di propaganda, controllo di studenti cinesi all'estero, reclutamento di agenti nell'ambito della cosiddetta diaspora cinese e altre similari operazioni clandestine a lungo termine. Secondo altri[18] invece, la sua principale funzione sarebbe il monitoraggio e la soppressione della dissidenza all'estero attraverso un'operatività ritenuta abbastanza irrituale per lo spionaggio cinese e cioè l'attività di ufficiali che opererebbero sotto copertura diplomatica come membri del Ministero degli Affari Esteri. Infine, sarebbe parte della sua attività precipua il processamento dell'informazione raccolta dal Ministero del Commercio – aspetto di cui si tratterà appositamente nel paragrafo successivo a proposito della "*Business Intelligence* di Stato".

Quanto fin qui esposto a proposito dei transiti informativi e dei criteri utili a mappare i luoghi di snodo dei flussi - individuando così quelli che mostrano la maggiore probabilità di essere identificati a ragione come i reali centri di analisi e

[17] Si veda in proposito Fabrice De Pierrebourg and Michel Juneau-Katsuya, *Nest of Spies: the Startling Truth about Foreign Agents at Work Within Canada's Borders* (Harper Collins Canada, Toronto, 2009).

[18] Tra questi anche analisi di *Stratfor* già citata in nota 6.

di elaborazione dell'informazione - trova un suo riscontro nel sistema del MID (Military Intelligence Department).

Si tratta anche in questo caso, come già evidenziato a proposito degli apparati civili di emanazione di intelligence, di una struttura molto complessa e ridondante per numero di enti, risorse e molteplicità di funzioni. La differenza sostanziale nell'intelligence militare risiede però nel fatto che, trovandosi già per definizione sotto il diretto controllo del Partito, sono molto meno presenti sulle singole parti dell'apparato linee secondarie o indirette di controllo dei flussi. Piuttosto, sono invece presenti, come spiegato sopra a proposito della funzione del GPD (General Political Department), controlli disciplinari, mirati a testare la fedeltà dei diversi comparti alla linea istituzionale del Partito. Osserviamo nel dettaglio lo schema (figura 2) relativo alla distribuzione dei centri di analisi nel MID, al fine di consentire alcune considerazioni valide per individuare i luoghi più plausibili di emanazione di intelligence.

La struttura si mostra in questo caso anche figurativamente molto lineare e accessibile. A cascata, sotto la diretta autorità della Commissione Militare Centrale, poi dello Stato Maggiore Generale della PLA, e infine dell'ufficio del Direttore del MID, esiste un unico grande centro di analisi identificato da un ufficio "senza numero" che riceve e processa tutta l'informazione proveniente dal basso, divisa per competenze, potremmo dire, "geografiche": un centro di raccolta per i paesi asiatici (Bureau 6), uno per zona USA/Occidente (Bureau 5), uno per l'area est Europa/Ex URSS (Bureau 4) e infine uno per il monitoraggio di carattere nazionale (Bureau 2) che avviene attraverso il complesso e capillare sistema di controllo delle regioni militari, le quali alimentano il drenaggio dell'informazione che si produce a livello più basso del sistema.

E' possibile a questo stadio osservare un'analogia molto forte con il sistema di "raccolta alla radice" che esiste anche in ambito civile, dove la funzione - qui svolta dalle unità militari - avviene ad opera delle cosiddette *Danwei*, le unità di lavoro cui tutta la popolazione cinese afferisce (come fossero una sorta di nostre circoscrizioni) a seconda dell'applicazione di diversi criteri, quali il luogo di residenza, di lavoro o di formazione scolastica. Per rendere l'idea della capillarità del controllo, si pensi che in ogni *Danwei* viene conservata documentazione relativa a dati sensibili anche molto privati, quali ad esempio la storia familiare o l'attitudine nei confronti del partito, la correttezza a livello ideologico e simili. Inoltre, ogni unità di lavoro è gestita da quadri del Partito con diverse funzioni che collaborano molto attivamente sia con l'MPS che con l'MSS – scambiando con essi notevoli quantità di dati.

All'apparenza dunque lo schema è di una chiarezza lapalissiana: il flusso informativo viaggia dal basso verso l'alto, viene elaborato dall'Ufficio Analisi posto in posizione apicale rispetto al resto degli apparati e sotto la diretta osservanza dei vertici del MID, poi della PLA e in ultima fase del partito. Eppure delle variabili inserisco-

no delle distorsioni nella linearità apparente della struttura anche in ambito militare.

Sappiamo che in questo ambito non esiste necessità di una doppia linea di controllo sulle singole parti, in quanto non c'è flusso dati da monitorare tra struttura di Governo e struttura di Partito - come invece osservato in ambito civile - dal momento che la forza militare e già posta sotto la diretta autorità del Partito, ma esiste tuttavia il rischio di eversione dello strumento di intelligence militare e il pericolo associato alla disponibilità da parte del MID di una grande mole di informazione preziosa e sensibile che rimarrebbe di fatto a lungo confinata all'interno di una singola struttura, prima di arrivare definitivamente nel suo livello più alto, a raggiungere i vertici del partito.

Occorrerà quindi sottrarre informazione (e dunque potere) all'intero apparato, diversificando l'attività di raccolta e creando dei percorsi ascensionali paralleli, ove il flusso ai vertici è più diretto e soprattutto alternativo al passaggio attraverso l'unità centrale di analisi di cui sopra. Ecco dunque comparire uno strategico Bureau 1, ufficialmente preposto alla raccolta informativa nelle regioni d'oltremare e confinanti, istituita per sottrarre all'elaborazione esclusiva del MID l'informazione preziosa[19] per il controllo delle aree periferiche. Tale unità, per il suo peculiare posizionamento, appare sottoposta comunque all'autorità del MID – sebbene strategicamente sovraordinata rispetto al suo principale ed unico Bureau di analisi - e aggiuntivamente assoggettata al diretto controllo della PLA (sotto la Commissione Militare Centrale del Partito) in una modalità palesemente distinta dallo Stato Maggiore Generale della PLA da cui invece dipende di fatto direttamente il MID[20].

[19] Per avere un'idea di tale "preziosità", si consideri che tale ente provvede alla raccolta, gestione e analisi di una gran parte di quel nucleo d'intelligence reputato vitale per il Partito Comunista Cinese. In particolare infatti, per la protezione e il mantenimento dello status quo, il Partito ritiene indispensabile l'acquisizione informativa su 5 fronti – i cosiddetti 5 veleni - che essa valuta come le 5 principali minacce da cui proteggersi o anche i 5 grandi targets da tenere sotto costante primario monitoraggio: Taiwan, il Tibet, l'etnia Uigura nello Xinjiang, i movimenti per la democrazia che traggono la loro linfa vitale dalle organizzazioni dissidenti spesso basate in India, e infine la setta del Falun Gong, che per le Istituzioni cinesi nasconde sotto la sua propaganda spirituale un pericolosissimo potenziale eversivo.

[20] L'estrema rilevanza strategica del Bureau n. 1 del MID è la ragione per la quale essa è posta così a latere dell'intero apparato e sotto il diretto controllo della PLA e del Partito. In parte la sua operatività è focalizzata sulle aree di Macao, Taiwan e Hong Kong e rappresenta per così dire "la versione militare" del Bureau n. 3 dell'MSS centrato sui medesimi targets. Tramite tali due entità la Cina acquisisce la tecnologia (o l'informazione sulla tecnologia) utile ad innovare i suoi apparati d'arma e in generale ad aumentare la sua capacità militare, tramite il business delle cosiddette *front companies*, spesso basate ad Hong Kong, e gestite da operatori dell'MSS o del MID. Secondo *Stratfor*, altresì peculiare del Bureau n. 1 sarebbe l'attività di traffico di armi, mai condotta in modo diretto, al fine di nascondere il coinvolgimento della PLA: attraverso fidati *dealers* – opportunamente individuati e reclutati a seguito di lunghe investigazioni – lo Stato Cinese avrebbe approvvigionato di armi negli ultimi decenni Iraq, Corea del Nord, Argentina, Iran, Pakistan, Arabia Saudita e Siria. Infine, secondo diversi analisti, questo stesso ufficio sarebbe responsabile del coinvolgimento della Cina in numerosi moti di insorgenza di diversi paesi asiatici e africani (come quelli in Angola, in Thailandia o in Afghanistan) e persino di aver fornito assistenza in loco per la realizzazione di scuole di addestramento alla guerriglia.

Un'altra unità "sospetta" in questo senso, per il suo peculiare collocamento, è certamente il Bureau n 3 deputato alla gestione degli addetti militari in ambasciata: anch'essa gestisce tali collettori di intelligence - soprattutto da fonti aperte[21] - con un rapporto di dipendenza dall'ufficio centrale del MID e dai vertici di Partito molto snello e diretto e, soprattutto, senza sottostare all'autorità dell'unità di analisi centrale del MID.

Dunque è di per sé evidente, osservando la struttura dell'intero apparato di intelligence militare, come i vertici del Partito promuovano un'organizzazione molto complessa e diversificata in seno alla PLA per il controllo del MID, una sorta di "presa a polipo" dove i diversi tentacoli afferrano direttamente parti strategiche dell'insieme, al fine di sottrarre informazione determinante alle unità centrali dello stesso[22]. Nella gestione dei flussi a livello delle regioni militari ciò si mostra in modo chiarissimo: le unità militari sotto le regioni e i collettori di intelligence a livello di tali unità sotto i centri di osservazione del MID, rappresentano da sole un quadrilatero autofunzionante per la raccolta informativa e un primo processamento dei dati alla base del sistema. Da qui l'informazione sale verso il centro di osservazione nazionale, poi verso il Bureau di Analisi Centrale del MID, ma allo stesso tempo in linea diretta a latere del MID, anche ai vertici della PLA che mantiene un controllo diretto sulle Regioni militari.

D'altra parte anche in questo caso si tratta di dati che costituiscono un nucleo informativo prezioso che sarebbe alquanto pericoloso far fluire in modo lento fino ai vertici del partito tramite la via tradizionale: ci si riferisce infatti all'inestimabi-

[21] In realtà anche l'attività clandestina di raccolta informativa fa parte dell'operatività degli addetti militari di ambasciata, come per molte altre nazioni ovviamente, ma nel caso cinese essa passa per essere stata tradizionalmente molto più incapace di altre di arrivare al target o di riuscire a mantenere la segretezza associata agli incarichi, finendo per rivelarsi il più delle volte abbastanza fallimentare. Tuttavia più recenti casi – quali quello di Ronald Montaperto venuto alla luce nel 2006 - mostrano come la capacità e il *know how* a disposizione degli agenti cinesi si stiano in tal senso raffinando e se ne parlerà diffusamente in un paragrafo successivo a proposito dei metodi di reclutamento.

[22] Talvolta i vertici del Partito, oltre a produrre canali alternativi al flusso ufficiale, al fine di sottrarre informazione rilevante agli apparati, sono solite creare piccole unità ad hoc per la gestione di singole minacce ritenute particolarmente pericolose per la sicurezza dello Stato e la protezione dello status quo. Tali unità svolgono la loro funzione in aperta competizione con gli organi ufficialmente preposti alle medesime funzioni. Un caso esemplare è rappresentato dall'Ufficio 610, un'agenzia di sicurezza creata nel 1999, direttamente sottoposta al controllo del Partito e focalizzata sul monitoraggio e il contrasto all'attività della setta di Falun Gong – e dunque ovviamente in concorrenza con l'azione portata avanti nello stesso ambito dalla struttura dell'MSS. *IHS Jane's* riferisce che il suddetto ufficio sarebbe ad esempio responsabile dell'operazione clandestina condotta contro lo scrittore e attivista per i diritti umani Liu Xiaobo, al fine di evitare che questi fosse insignito del premio Nobel per la Pace che in effetti alla fine vinse. Indiscrezioni in ambito di politica internazionale sostengono che a causa del fallimento dell'operazione e dell'assegnazione quindi poi avvenuta del premio, i rapporti tra Pechino e Oslo si raffreddarono a tal punto da risultare in una sorta di temporaneo embargo imposto dalla Cina alla Norvegia per l'importazione di salmone.

le conoscenza relativa alla sicurezza e la protezione delle frontiere[23], acquisita tramite il reclutamento di fonti oltre confine ove le unità militari svolgono una peculiare e capillare attività di pattugliamento[24].

In definitiva insomma il controllo eterogeneo che la PLA esercita sul MID protegge il partito dalle potenziali derive eversive del sistema di intelligence militare, ma ciò pone il problema di come evitare che la PLA diventi un problema essa stessa per la medesima ragione. A tal fine, con il preciso obbiettivo di alienare l'informazione strategica più rilevante dalla gestione assoluta della PLA, la riorganizzazione delle forze armate da parte del Partito – ad opera attualmente di Xi Jimping – sta prevedendo un impianto riformatorio, in parte già attuato, che colloca al di fuori del comparto della PLA dominato dal potere dei reparti delle truppe di terra, le unità di raccolta informativa reputate al momento più preziose, quali quelle operanti in ambito cyber.

Sembra andare in questa direzione la predisposizione della nuova struttura denominata SSF (Strategic Support Force), di cui si tratterà nel paragrafo conclusivo di questa analisi, relativo alle evoluzioni più recenti del sistema di spionaggio cinese, con particolare riferimento alle avanguardie che interessano appunto lo sviluppo della cyber-intelligence.

Infine, occorre fare un'ultima importante considerazione: la descrizione fin qui resa dell'apparato di raccolta informativa della Cina mostra una tale complessità da rendere legittimo il quesito se esso effettivamente funzioni o meno, se riesca quindi nel complesso ad assolvere i compiti che gli sono assegnati e soprattutto se il decisore politico abbia effettivamente della struttura una capacità di gestione sufficiente a poterle davvero assegnare delle *missions* specifiche. Certamente la maggior parte delle ridondanze che la sua compagine mostra – oltre a quelle da considerarsi di fatto caratteristiche endemiche della sua costituzione – sono, come si è tentato di spiegare, artificialmente create dai vertici per migliorarne paradossal-

[23] Si pensi al problema di rilevanza crescente relativo all'immigrazione clandestina proveniente dalla Corea del Nord che si è recentemente elevato da fenomeno prodotto a livello di singoli individui a vera e propria tratta di esseri umani gestita da gang criminali. Ancora esemplificativo in tal senso è il delicato confine con la Birmania, dove i gruppi armati legati alla KIA (Kachin Independence Army) che conducono azioni di guerriglia con l'obbiettivo di produrre a tendere una forma statuale indipendente, mettono a rischio i gasdotti in costruzione da Kunming (nella provincia cinese dello Yunnan) e passanti appunto per il confine birmano in direzione dell'Oceano Indiano. E infine il confine occidentale che, pericolosamente adiacente a paesi quali Pakistan e Afghanistan, fortemente destabilizzati da fenomeni legati al terrorismo islamico, è suscettibile di contagiare la monitoratissima vicina provincia dello Xinjiang, ove risiede la vasta minoranza islamica degli Uiguri.

[24] *Stratfor* riferisce di ben 24 gruppi etnici tra cui sarebbero reclutati agenti oltreconfine: si tratterebbe in molti casi di comunità giacenti lungo la frontiera e tagliate virtualmente nel mezzo da confini nazionali astratti che i membri varcherebbero con estrema facilità e continuamente, al fine di muoversi all'interno del territorio su cui insiste la propria comunità di appartenenza – e rivelandosi essere quindi ottimi informatori per i servizi segreti cinesi in virtù di una tale capacità di libero movimento.

mente il funzionamento, rendendola più controllabile e rendendone più facilmente e velocemente fruibili i prodotti.

E' tuttavia un dato incontrovertibile che la fluidità che dovrebbe manifestare un apparato realmente efficiente è qui bloccata da molte cesure. Talvolta tali blocchi vengono bypassati da quella sorta di "autostrade velocizzanti" di cui si è parlato, cioè dei veri e propri canali preferenziali tramite cui i vertici hanno accesso privilegiato e attingono di fatto direttamente all'informazione più strategica, ma tali veicoli non bastano a spiegare come tutto sommato l'apparato finisca per assolvere magicamente alla sua funzione e risulti comunque efficace e produttivo – visto che a gran parte degli osservatori in ultima analisi esso non manca di apparire tale.

Esiste in proposito un dato che viene a ragione spesso richiamato per render conto di questa efficienza ed è il collante valoriale del Confucianesimo. Notoriamente, nei valori tradizionali della cultura cinese, questo costrutto filosofico di base è ancora molto forte ed è particolarmente operante per ciò che attiene l'attitudine delle masse verso il potere. Sappiamo che uno dei suoi elementi fondanti è il senso di rispetto radicale nei confronti dell'Autorità in genere, a livello generazionale per esempio, il riconoscimento dell'autorità degli anziani da parte dei giovani, come anche la deferenza del suddito nei confronti dell'Autorità politica[25]. Si tratta di una componente di per sé di difficile comprensione per il pensiero occidentale che, anche prendendola in considerazione come esistente, fatica a riconoscerle il ruolo performante che essa riesce invece ad avere nel determinare i rapporti tra i civili e tra questi ultimi e le Istituzioni. Particolarmente nell'ambiente degli apparati militari, essa funziona come collante naturale tra le parti, fornisce una ratio sufficiente a far sì che i singoli comparti agiscano in favore delle determinazioni dell'Autorità, come se fossero in qualche modo autodirette.

La fedeltà alle Istituzioni si inquadra in un generale atteggiamento comunemente condiviso del "fare il bene della Cina" che non necessità – o sarebbe meglio dire non ha necessitato in passato e almeno fino a questo momento – di un controllo eterodiretto ed eccessivamente vincolante. Questa stessa cultura, radicata in modo evidente anche negli ambienti di intelligence, spiegherebbe come, benché così eterogeneo, il sistema funzioni in modo coerente e coordinato. I pur numerosissimi casi di corruzione che sappiamo affliggere lo strumento militare (come anche quello politico in genere) non hanno avuto la forza di rappresentare fino ad oggi una mi-

[25] Molti storici sostengono che tale *imprinting* valoriale sia estremamente operativo anche negli stessi ambienti dei detentori del potere, a tal punto che essi faticherebbero a costruire delle equilibrate strategie di contrasto alle potenzialità di ribellione, in quanto appunto ritenute quasi razionalmente inconcepibili. Un caso esemplificativo a riguardo è rappresentato dalla modalità per così dire eccessiva e inadeguata con cui fu sedata la rivolta dei giovani in piazza Tienanmen, proprio perché completamente inaspettata da parte delle Autorità politiche che hanno valutato gli eventi non solo come un fatto meramente eversivo, ma come un inspiegabile e inaccettabile tradimento dei valori di fondo del tessuto sociale di riferimento.

naccia tale da mettere in discussione l'operatività generale e il conseguimento dei risultati.

Va sottolineato tuttavia che i processi di secolarizzazione, che hanno finito per infiltrarsi anche nel tessuto culturale cinese, stanno lentamente modificando tale sostrato valoriale e, specie per ciò che attiene all'attività di reclutamento delle fonti e degli agenti di cui si parlerà in seguito, le Istituzioni sembrano poter fare sempre minore affidamento sulla fedeltà automatica dei loro targets alla causa dello Stato ed è presumibile altresì che debbano in futuro esercitare una sempre maggiore pressione per rendere sempre più "conveniente" o imprescindibile per loro operare nella direzione imposta dai gestori del potere politico.

2) La *business intelligence* di Stato: economia di impresa versus sicurezza nazionale

Altro caposaldo largamente condiviso nella letteratura di settore è senza dubbio la convinzione relativa alla peculiare "*mission* economica " dello spionaggio cinese.

Va premesso ovviamente che ogni sistema di intelligence che si rispetti - e indipendentemente se si tratti dell'apparato di uno Stato con istituzioni democratiche o meno - tenderà in via di principio a salvaguardare per statuto l'interesse nazionale ed è indubbio che la protezione degli interessi economici ne sia una parte imprescindibile. E' altrettanto chiaro che tanto più lo Stato assumerà una forma autoritaria, non liberale e non democratica – quale di fatto è il sistema di governo in Cina - tanto più è presumibile che tenda ad accentrare questa funzione lasciando poco spazio all'iniziativa privata.

Tuttavia, anche tenendo conto di queste generalizzazioni, nel caso cinese il modello descritto in premessa appare operativo in modo esasperato. Per molti osservatori infatti, mentre lo sforzo spionistico estero nei confronti della Cina sarebbe diretto a decifrarne la reale capacità militare, le potenzialità belliche e le intenzioni strategiche, al contrario l'impegno dello spionaggio cinese verso l'esterno sarebbe volto soprattutto ad acquisire informazione segreta di natura industriale e commerciale[26]. In effetti, la maggior parte degli attacchi cyber che si sono registrati negli ultimi anni a danno di diverse nazioni e riconducibili direttamente – o indirettamente per il tramite di vari elementi terzi[27]- alla Cina, hanno interessato industrie strategiche per gli approvvigionamenti energetici e soprattutto imprese con un alto

[26] Si veda in proposito l'analisi Adam Brookes, "Is China Swarming with Foreign Spies?", *Foreign Policy*, 5 novembre 2014. Link: www.foreignpolicy.com.

[27] Si tratterà delle caratteristiche della guerra cyber "in appalto" tipica dell'ambito cinese nell'ultimo paragrafo di questa analisi.

grado di innovazione tecnologica che sappiamo essere elemento molto appetibile e *target* privilegiato per l'attività di penetrazione offensiva cinese.

Tale posizione si traduce spesso nel convincimento che la Cina sia quindi maggiormente interessata alla *business intelligence* piuttosto che all'intelligence politica e che l'attenzione verso quest'ultima sia secondaria o comunque da considerarsi un mero sviluppo recente, legato per lo più all'altrettanto recente ambizione, perseguita dal paese, di aumentare in modo considerevole il suo *soft power* nel mondo. Non c'è dubbio che tale conclusione sia più che realistica, ma occorre riflettere sul fatto che i Cinesi seguano di fondo un paradigma sostanzialmente diverso dall'approccio tipico occidentale, e cioè quello della completa indivisibilità degli interessi dello Stato da quelli dell'Industria, con la specifica attitudine a perseguire i primi attraverso i secondi e viceversa. In altre parole, l'attività dell'apparato di intelligence cinese è da considerarsi completamente a disposizione del comparto industriale, al fine di permettere ad esso l'acquisizione dell'informazione indispensabile per favorire uno sviluppo rapido dell'economia, il che si tradurrà a sua volta in un aumento di *soft power* necessario per il raggiungimento di obbiettivi geopolitici a vantaggio o a salvaguardia appunto degli interessi della nazione stessa.

Un proficuo e circolare scambio di favori dunque nella dinamica pubblico/privato che produce una sorta di *business intelligence* di Stato, costruita tra l'altro – come è tipico dell'atteggiamento programmatico di questa cultura che non dimentica mai di essere frutto di un impero millenario – su un orizzonte temporale molto vasto, che non si pone come obbiettivo di breve termine il furto di segreti al fine di favorire la competitività spicciola della singola impresa, bensì va alla ricerca dell'acquisizione di informazione strategica che le faccia guadagnare dei passaggi utili a sviluppare nel lungo periodo l'industria indigena[28].

La prova principe di un tale approccio risiede sicuramente nell'altissima collaborazione che le Istituzioni deputate allo sviluppo economico e commerciale hanno con gli apparati di intelligence e viceversa. Quando nel 2002 venne creato il Ministero del Commercio, vennero da subito istituite in seno ad esso delle specifiche unità di intelligence sistematicamente legate all'MSS, con il quale viene a tutt'oggi curata la realizzazione di numerose *covert operations* in ambito economico, nonché la gestione delle *front companies* – di cui si tratterà a seguire - la cui attività è tesa al perseguimento degli obbiettivi appena descritti. Altra collaborazione sintomo di tale impegno è quella tra il Ministero del Commercio, il Dipartimento del Fronte Unito (sotto l'egida del Partito) e il MID, triangolo dal quale si evince il desiderio di controllo diretto dell'attività commerciale da parte del Partito anche attraverso lo strumento di intelligence militare.

[28] Si veda in proposito l'analisi di Robert Pritchard, "Virtual reality – China Takes Industrial Espionage into Cyberspace", *IHS Jane's*, 5 aprile 2013.

Per gli occidentali, e specialmente per le società civili che storicamente non hanno sperimentato - o lo hanno fatto solo parzialmente – la statalizzazione della produzione economica, pensare ad uno spionaggio di impresa coordinato a livello centrale da un Governo, può risultare oggettivamente difficile, specie quando, ad aggravare un'attitudine già poco comprensibile, si aggiunga un aspetto culturale della prassi economica cinese che è quello della pressoché totale mancanza di scrupolo a perpetrare l'azione di "furto di segreto industriale" in sé per sé, in quanto tale comportamento non esercita affatto sull'attore economico medio il peso etico che è immaginabile eserciti invece in ambito occidentale.

In altre parole, sottrarre informazione riservata ad altri per acquisire un vantaggio economico, sia che lo si faccia per conto dello Stato o in modo autodiretto per un fine personale, non assume la valenza di una condotta gravemente contraria all'etica di impresa in Cina, né rischia di provocare una particolare riprovazione sociale che potrebbe eventualmente costituire elemento di deterrenza. Tenere in considerazione tali variabili aiuta a capire come tali comportamenti siano in un certo senso "sdoganati" e diffusissimi e come le Istituzioni possano operare esse stesse in questa direzione - e pretendere che altri lo facciano - dovendo affrontare per lo più bassissimi livelli di reticenza da parte degli attori pubblici, delle imprese come dei singoli individui[29].

In conseguenza di ciò, finiscono per essere largamente presenti in Cina forme eterogenee di spionaggio industriale – senza che sia sempre facilissimo discernere quando esse siano completo appannaggio dello Stato, mera iniziativa del singolo individuo o della singola impresa, iniziativa privata ma comunque sfruttata dalle istituzioni e via dicendo, finanche ad arrivare a modalità ibride anche molto più complesse.

Si riporta a seguire, a solo titolo esemplificativo, una lista[30] di cinque modalità possibili di furto industriale, corrispondenti a cinque diversi gradi di coinvolgimento del governo e dei servizi di intelligence - tutte largamente presenti nella prassi economica cinese:

• Sottrazione da parte dei servizi di intelligence di segreti economici per lo sviluppo industriale diretto/sostenuto dallo Stato.

[29] In realtà va sottolineato come tale situazione si stia lentamente modificando, forse, secondo alcuni, a causa del fatto che la formazione di molti *executives* avviene in ambiti diversi da quello della madrepatria o anche a causa semplicemente della prassi di apertura e di contatto delle nuove generazioni con mondi etici di riferimento differenti. Tali cambiamenti, in aggiunta ai processi di secolarizzazione e diffusione della ricchezza, stanno rendendo sempre più difficile per gli agenti manipolatori l'attività di reclutamento, visto che per sempre maggiori ragioni agenti e fonti tendono a sottrarsi a quel tipo di collaborazione spontanea e priva di scrupoli su cui le istituzioni spionistiche cinesi hanno finora potuto contare – specie quando non ravvisino in essa delle particolari convenienze o dei significativi vantaggi economici. Si veda in merito il paragrafo successivo sulle forme di reclutamento.

[30] L'elenco è tratto dall'analisi di Peter L. Mattis citata in nota 4 – pag. 683.

• Sottrazione da parte dei servizi di intelligence di segreti tecnologici per lo sviluppo e la pianificazione dell'intelligence militare come anche di quella economica.

• Raccolta informativa sponsorizzata dal Governo, ma non prodotta dai servizi di intelligence, per comparti industriali supportati dallo Stato.

• Sottrazione di segreti industriali dei *competitors* da parte di singoli attori economici, anche pubblici, al fine di accrescere il proprio vantaggio competitivo.

• Sottrazione di segreti economici da parte di singoli individui/imprenditori al fine di effettuarne la vendita ad altri attori citati (pubblici o privati)[31] o con lo scopo di entrare in determinati *business*[32].

Come si evince chiaramente, il coinvolgimento delle Istituzioni si sposta su un continuum tra i due poli nullo/assoluto per cui risulta molto difficile capire se una sottrazione di segreto economico possa identificarsi come mero furto industriale o come intelligence di Stato e soprattutto valutare correttamente quanto sia direttamente/indirettamente sponsorizzata dal Governo[33].

Tra l'altro, come già descritto in questa sede, l'acquisizione d'intelligence tecnologica è considerata notoriamente un target chiave tra le finalità operative dell'MSS ed è primariamente realizzata proprio attraverso le modalità sopradescritte: gli agenti di tale comparto reclutano giovani ricercatori nei loro viaggi studio all'estero, persuadendoli a sottrarre informazioni sulle avanguardie tecnologiche identificate come strategicamente rilevanti; le società straniere, proprietarie di tali tecnologie, vengono acquistate da compagnie cinesi più o meno direttamente connesse all'MSS[34]; infine le cosiddette *front companies* con sede ad Hong Kong e gestite dall'MSS (più raramente in realtà dal personale MSS in modo diretto e più frequentemente da tramiti e collaboratori) acquistano equipaggiamenti contenenti la tecnologia desiderata direttamente dal mercato.

La realtà delle *front companies*, in particolare, sembra essere oggetto di una cre-

[31] E' il caso ad esempio di Bill Moo che fu arrestato nel 2005 per aver trafugato alla General Electric segreti tecnologici relativi alla produzione degli allora nuovissimi cacciabombardieri F-16 e che era in procinto di vendere per un prezzo già concordato pari a un milione di dollari all'intelligence militare cinese.

[32] Emblematico in questo senso il caso di Yu Xiang Dong, condannato nel 2006 per aver sottratto informazione strategica alla Ford Motor Company statunitense al fine di usarla per iniziare una nuova carriera presso l'Automotive Group di Pechino.

[33] Una lista molto dettagliata dei numerosi casi di spionaggio industriale cinese venuti alla luce negli ultimi anni è contenuta in W. C. Hannas, J. Mulvenon, A. B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (London e New York, Routledge, 2013) – Appendix 1: "Case Histories of Chinese Industrial Espionage".

[34] Relativamente a questo tipo di acquisizioni, si vedano gli esempi proposti nell'analisi di *Stratfor* già citata in nota 6 e tra questi, in particolare, l'acquisto della società statunitense Mamco Manufacturing da parte della cinese CATIC o il caso di Da Chuan Zheng, arrestato negli USA per aver acquistato illegalmente tecnologia di sorveglianza elettronica e radar per conto della Cina.

scente attenzione da parte degli apparati di controspionaggio di molti paesi, in special modo di quello statunitense[35]. Si tratta per lo più di grandi gruppi industriali, finanziari e commerciali – principalmente basati ad Hong Kong - che risultano far capo apparentemente ad imprenditori privati, ma che nascondono legami più o meno stretti con il governo e diverse agenzie di intelligence. Sarebbero, secondo molti osservatori, le propaggini attraverso cui lo Stato cinese riesce a fare *business*, soprattutto all'estero, in modo "aperto", ma mantenendo clandestino il suo diretto coinvolgimento e dunque il fine strategico nazionale che si cela dietro l'impalcatura della tradizionale impresa di carattere privato.

Si tratta di un sistema ormai noto come *Sina model*, dove, alla proprietà e gestione solo apparentemente non pubbliche dell'impresa, si affianca l'altrettanto apparente coinvolgimento di imprese straniere nel capitale e nel management delle società, così da rendere la connessione delle loro attività alle istituzioni di Governo estremamente oscura e difficile da accertare. Emblematico in proposito il caso dell'88 Queensway Group*,* il cui nome fa riferimento all'indirizzo ove risultano ubicati una serie di edifici che ospiterebbero, proprio nel centro di Hong Kong appunto, il quartier generale della Dayuan International Development*,* società privata proprietaria al 99% della China International Fund (CIF), un fondo di investimento privato che avrebbe come *mission* la costruzione e il finanziamento di progetti infrastrutturali su larga scala, primariamente in paesi in via di sviluppo dell'Africa e dell'America Latina, ma anche nel Sud Est Asiatico e negli Stati Uniti.

Secondo la United States-China Economic and Security Review Commission - che ha pubblicato uno specifico *report*[36] in proposito nel luglio del 2009 - il *business* di questa multinazionale, ben al di là della sua veste apparente di impresa di investimento di natura privata, sarebbe gestito indirettamente dagli apparati di intelligence cinesi. E' corretto sottolineare che tali legami non sono mai stati appurati in modo incontrovertibile, ma risulta con certezza che le cariche strategiche del management della capogruppo, come anche di molte delle sue trenta controllate, avrebbero stretti legami con elementi direttivi di imprese pubbliche e agenzie governative.

Solo a titolo esemplificativo: una delle Direttrici del CIF, Lo Fong Hung, risulta essere anche Direttrice della Sonangol Sinopec International Ltd., una joint-venture tra la compagnia petrolifera pubblica cinese Sinopec of China e la Sonangol di Angola; tra i Direttori del CIF, Wu Yang è stato vice presidente di Sinopec nel marzo del 2006[37]; infine è ritenuto essere realmente a capo del CIF e dell'intero si-

[35] Secondo *Stratfor* l'FBI riterrebbe che operino solamente negli Stati Uniti circa 3000 *front companies* la cui gestione è riconducibile ad apparati di intelligence cinesi.

[36] Si fa riferimento alla seguente pubblicazione: Lee Levkowitz, Marta McLellan Ross, and J.R. Warner, "The 88 Queensway Group: A Case Study in Chinese Investors' Operations in Angola and Beyond", U.S.-China Economic & Security Review Commission*,* 10 Luglio 2009.

[37] Si veda Wikipedia alla voce CIF – China International Fund

stema dell' 88 Queensway Group - sebbene il suo nome non risulti ufficialmente in nessun documento societario – Sam Pa, una sorta di *tycoon* cinese dal passato oscuro e inesplorabile, conosciuto con numerosi pseudonimi, recentemente arrestato a Pechino per una vicenda di corruzione e, soprattutto, da molti ritenuto essere uomo-chiave dell'intelligence di Cina[38].

3) Le modalità operative, le aree di intervento e il reclutamento: la necessità di un parametro temporale insolitamente ampio e di un approccio "olistico" per indagare le reali capacità delle attuali Humint e Osint cinesi

Alcune considerazioni di fondo relative alle capacità di reclutamento e alle modalità operative degli *asset* spionistici cinesi sono ritenute oggi dei veri e propri dogmi nel panorama più tradizionale di studi – tra queste:

• L'Osint sarebbe prioritaria e più utilizzata come metodo di raccolta informativa rispetto alla Humint.

• La Humint non appare particolarmente specializzata, recluta maggiormente *assets* nazionali, procede con metodi grezzi e la sua attività poco professionalizzata è spesso facilmente tracciabile.

• La Humint si sta tuttavia modificando e tende a divenire uno strumento maggiormente qualificato e capace di raggiungere specifici *targets* al fine di soddisfare in modo più puntuale le richieste specifiche del committente.

Come è innegabile che ci sia del vero in ognuna di queste tre affermazioni, si rileva che un numero sempre maggiore di ricerche, di recente, tende a riformulare questi assunzioni di fondo, miticando di esse la presunta capacità esplicativa di un sistema che di per sé sfugge alle classificazioni semplicistiche, a causa della sua evidente e forte complessità.

E' senz'altro vero che gli apparati di intelligence cinesi - e di essi soprattutto le modalità di reclutamento delle fonti e le tecniche operative – stiano procedendo ad una attività di indubbio rinnovamento e di maggiore specializzazione, ma il ritenere che una Humint specializzata e *target-oriented* – in una parola potremmo dire "una Humint alla occidentale" - stia facendo la sua comparsa in Cina solo a partire dagli ultimi decenni, può davvero rappresentare uno sguardo fuorviante e disgiunto da una reale capacità di comprensione del peculiare *tradecraft* cinese.

Nulla in realtà del "vecchio modo di fare intelligence della Cina" è davvero tramontato o è stato definitivamente deposto, ma esso è oggi compresente – e di fat-

[38] Si veda in proposito l'articolo di David Connett, "Sam Pa, the Fall of China's Trailblazer in Africa", *The Indipendent*, 24 ottobre 2015 – Link: www.independent.co.uk.

to lo è sempre stato – con modalità operative molto simili a quelle in essere negli apparati spionistici che riteniamo "più avanzati". Una valutazione davvero realistica delle capacità di intelligence del vecchio Impero di Mezzo non può prescindere dal veder operare insieme "il vecchio" e "il nuovo", anzi, occorrerebbe lo sforzo di comprendere che quelle che riteniamo nuove acquisizioni sono invece sempre esistite nel metodo di spionaggio cinese, fin dagli albori della formazione delle prime unità di raccolta informativa negli anni trenta del secolo scorso.

Nello specifico, sarà utile riflettere sul fatto che, sebbene molti ritenessero finora che la Cina fosse poco in grado di infiltrare suoi agenti o reclutare fonti in ambiti specifici, al fine di soddisfare altrettanto specifici *needs* informativi, una grande quantità di casi venuti alla luce negli ultimi decenni hanno dimostrato ampiamente il contrario, rendendo palesi "adescamenti di fonti", ad esempio, in luoghi che si pensavano erroneamente impermeabili alle capacità di intrusione degli apparati di intelligence della Cina. Inoltre, molti di essi si sono rivelati essere casi di flussi informativi occulti più che decennali, consentendo la logica deduzione, quindi, che non si tratti affatto di un'operatività acquisita di recente e soprattutto che l'attività clandestina messa in opera meriti in qualche modo di essere considerata più che specializzata, o comunque capace in qualche misura di almeno autoproteggersi, se tali operazioni si sono mostrate in grado di resistere alle insidie del tempo.

Sarà utile a questo punto procedere per gradi, partendo da ciò che in letteratura appare generalmente assodato circa le modalità operative dello spionaggio cinese, per approdare infine alle avanguardie di ricerca cui si è accennato e cui vale senz'altro la pena di prestare particolare attenzione.

Prendiamo in esame innanzitutto il primato della Osint rispetto alla Humint. Tale convinzione è legata all'idea che dalla fine del suo isolamento, nella seconda metà degli anni '70, la Cina si sia trovata a scoprire di essere in una condizione di estrema arretratezza sul piano dell'innovazione tecnologica da tutti i punti di vista e abbia dunque iniziato un'opera di aggressivo monitoraggio di tutte le fonti disponibili tramite le quali recuperare quelle lunghezze che la separavano dall'avanzamento economico, tecnologico e militare proprio di altri paesi.

Ovviamente, per quest'attività di ricongiunzione con il livello di progresso tecnologico almeno medio globale, non si rivelava strettamente necessario portare avanti un'operatività tipicamente clandestina a danno di altre nazioni e condotta da agenti specificamente addestrati (quella Humint che comunque non è di certo mai venuta meno), ma risultava più che sufficiente attenzionare il mondo pubblico della ricerca, o delle avanguardie industriali, attraverso il paziente lavoro di una gran mole di persone che nel normale esercizio delle loro funzioni lavorative, o nell'ambito proprio dei loro contatti privati, reperissero informazioni utili allo sviluppo della madrepatria.

Tale missione generale - nota come *human wave* – per intendere appunto la caratteristica di una vera e propria onda umana al lavoro su molteplici fronti e indefiniti *targets* di ricerca – era resa possibile, e si sposava di fatto perfettamente, con alcune specificità tipiche della demografia e della cultura cinese.

In primo luogo, ovviamente le quantità di soggetti a disposizione, data l'enorme popolazione della Cina e l'associata cosiddetta diaspora cinese che davano luogo insieme allo spostamento e l'emigrazione di un altissimo numero di persone verso tutti i paesi del mondo.

In secondo luogo, la capacità delle Istituzioni di poter pretendere una tale attività di reperimento informativo da parte della cittadinanza nei propri ambiti di competenza e di frequentazione sociale. Su questo punto si è già riferito nei paragrafi precedenti a proposito dell'attitudine naturale della popolazione al rispetto dell'Autorità e all'agire in favore della nazione - entrambe mediate dal Confucianesimo - come anche del minor scrupolo associato all'attività di sottrazione informativa per ottenere un vantaggio competitivo, piuttosto in linea con una prassi spionistica consolidata da una tradizione - persino letteraria - millenaria. Numerose indiscrezioni negli ambienti dello spionaggio riferiscono in proposito di un vero e proprio "giuramento", comprendente oltre 40 punti, cui tutti i cittadini emigranti usavano essere sottoposti prima della loro partenza - e tra questi l'obbligo di riferire tutto ciò che avveniva sul posto di lavoro all'estero, di non familiarizzare con gli stranieri e di fare comunque e sempre gli interessi della Cina.

In terzo luogo, infine, come corollario per la spiegazione del metodo della *human wave*, è d'abitudine richiamare la cosiddetta pratica del "granello di sabbia" o anche detta – specie in ambito anglosassone - *mosaic collection*[39] o *vacuum cleaner* (aspirapolvere), tipica della produttività cinese in ambiente non solo spionistico. Si tratta del primato che nella cultura del paese riveste notoriamente l'impegno minimo, ma paziente e costante nel tempo, associato ad un orizzonte temporale molto vasto per poter godere dei frutti del lavoro svolto.

In altre parole, la raccolta informativa avverrebbe per tradizione tramite la collezione di piccoli pezzi di informazione di quasi nullo significato presi in sé per sé, ma che acquisterebbero senso solo nel lungo periodo, quando aggregati e/o inquadrati in contesti più ampi[40]. Logica premessa di un siffatto metodo, naturalmente,

[39] Questa definizione si trova anche in *Stratfor* – opera citata in nota 6.

[40] E' tipico veder richiamata nella letteratura di settore la metafora del granello di sabbia che si riporta di seguito per curiosità – ma soprattutto perché si dimostra molto eloquente per la capacità che ha di descrivere in modo esaustivo la dinamica della *human wave*: "immaginando che l'intelligence sia la sabbia di una spiaggia, i Russi faranno avvicinare un sottomarino nella notte, sbarcare un team specializzato in operazioni anfibie che sparirà nell'oscurità dopo aver sottratto diversi secchi di sabbia dal sito indicato. I cinesi di contro, invieranno un migliaio di persone a prendere il sole, a giocare e divertirsi per tutto il giorno proprio su quel tratto di litorale. Alla fine della giornata, ogni bagnante andrà a scuotere il suo asciugamano nel medesimo angolo" (Peter Mattis, "Assessing Western Perspectives on Chinese Intelligence", op. cit., p. 680).

è l'idea della collezione amatoriale dell'informazione, intesa come operazione svolta da individui non addestrati allo scopo (non agenti insomma) e non finalizzata soprattutto al soddisfacimento di un bisogno informativo specifico e presupposto a tale attività. Il risultato quindi ne sarebbe un'intelligence completamente diretta dal basso, un prodotto informativo risultante dall'analisi e dal processamento di "quel che è capitato di riuscire a raccogliere", come se fosse completamente assente una gestione sovraordinata, o come se questa fosse solo successiva e conseguente alla fase primaria di raccolta. Una sorta insomma di ciclo di intelligence rovesciato[41], una visione indubbiamente molto romantica delle prassi cinesi - ma sicuramente anche molto lontana dalla realtà delle cose.

D'altra parte tale visione è confortata dal concetto stesso di intelligence, che nella lingua cinese è completamente sovrapposto a quello di informazione, esistendo un solo termine (*qingbao*) per indicare sia l'una che l'altra. Nella pratica appena descritta infatti si rivelerà difficilissimo distinguere cosa sia una banale notizia e cosa un vero e proprio prodotto di intelligence.

In una modalità così "amatoriale" di raccolta informativa, condotta per lo più da cittadini operanti nei loro distretti umani e professionali naturali e con il solo obbligo di produrre un *debriefing* sulle notizie di cui sono venuti in possesso alle istituzioni richiedenti, sarà parimenti difficile procedere all'accusa di spionaggio nei confronti di chiunque risulti appartenere a questa massa informe operante per conto dello Stato.

Altresì tale attività verrà condotta in modo pubblico e non necessariamente clandestino e si prefigurerà come una consultazione di fonti aperte più che come una vera e propria appropriazione occulta di informazione riservata. Alcuni autori arrivano in estremo a suggerire una realtà in cui i cittadini-agenti siano perfino all'oscuro del valore strategico rappresentato dalle informazioni fornite che prese singolarmente apparirebbero appunto irrilevanti e che la sottilissima abilità dei vertici dei sistemi di intelligence risiederebbe propria in questa particolare capacità di produrre tale forma di "spionaggio senza prove".[42]

A questo stadio sarà legittimo porsi in merito il seguente interrogativo: fino a che punto è plausibile pensare che tale situazione si sia conservata invariata nel tempo e sia di fatto operativa ancor oggi? E' credibile la condizione secondo cui i

[41] E' noto che nel tradizionale ciclo di intelligence questa fase esista e sia di fatto il momento in cui il prodotto informativo – divenuto prodotto di intelligence a seguito dell'analisi dell'informazione – contribuisce a ri-orientare i *needs* informativi del decisore e ad incidere quindi sulle successive richieste da esso impartite agli apparati di raccolta. Ma è da intendersi solamente come uno dei momenti di un processo di fatto circolare e cui è impensabile dare un primato nel ciclo nel suo complesso.

[42] Si tratta della celebre definizione della *human wave* fornita da Paul Moore – ex analista di controspionaggio dell'FBI – in un'intervista. Si veda Jeff Stein, "Espionage without Evidence: Is It Racism or Realism to Look at Chinese-Americans When Trying to Figure Out Who's Spying for China", *Salon.com*, 26 agosto 1999.

cinesi farebbero ancora (e abbiano fatto davvero in questi anni) spionaggio in questo modo?

Molti osservatori sottolineano il fatto – già peraltro richiamato più volte in questa sede – che lo status quo debba aver proceduto ad un mutamento anche solo per l'erosione della cultura confuciana sottostante al tessuto valoriale di fondo della società cinese che per effetto della secolarizzazione che si è abbattuta su molte porzioni sociali - specie quelle più a contatto con mondi occidentali o altre culture di riferimento concorrenti – ha finito per perdere la capacità di fungere da collante del sistema sociale.

In tal modo le nuove generazioni hanno finito per sviluppare un sentimento critico nei confronti dell'attitudine all'obbedienza cieca all'autorità, implicita nei valori tradizionali, mettendo in discussione l'operato delle Istituzioni, specie in concomitanza con i numerosi episodi di corruzione riguardanti la classe dirigente del Paese (e i vertici del Partito in particolare) venuti alla luce negli ultimi anni.

Se a ciò si aggiunge la maggiore attenzione che si registra, specie tra i giovani, al perseguimento delle aspirazioni individuali e allo sviluppo di carriere soddisfacenti e redditizie, è facile prevedere come sia oggi verosimilmente molto più difficile poter contare su quell'auto-asservimento delle masse utile ad ottenere informazioni tramite il metodo della *human wave*[43].

Ciò nonostante, non solo è lecito pensare che tali modalità operative tradizionali coesistano con forme più emancipate di raccolta informativa, ma è altresì plausibile ritenere che ad esse sia assegnato ancora un ruolo preminente - se non altro con il fine dalla comprensione generale dei fenomeni, magari utile ad orientare in una fase successiva la raccolta informativa più specializzata. Ne è certamente prova illuminante il recentissimo intervento legislativo che ha provveduto a riorganizzare l'attività di contrasto ai fenomeni terroristici.

Nell'articolatissima legge, emanata dall'esecutivo di Xi Jimping alla fine del 2015 e operativa fin dai primi mesi del 2016[44], la partecipazione dei singoli cittadini alla "guerra contro il terrore" riveste un ruolo fondamentale tale che ad essa è dedicata una specifica sezione proprio nell'ambito della raccolta di intelligence cui è dedicato il capitolo IV. Nello specifico vi si legge testualmente che nell'ambito della "strategia della guerra della gente", i cittadini sono obbligati ad agevolare la

[43] *IHS Jane's* riporta in proposito le risultanze di un'investigazione condotta dalla CIA nel novembre 2010 circa le difficoltà che il sistema informativo degli studenti - gestito dall'MPS - starebbe incontrando nella sua attività di monitoraggio studentesco specie in ambito universitario. In particolare gli studenti sembrerebbero risultare molto meno collaborativi nella prassi di *debriefing* alle Autorità – come ad esempio tenderebbero a rifiutarsi di riferire dati relativi a discussioni "indesiderabili" avvenute negli atenei, come anche di fornire rapporti dettagliati circa le lezioni tenute da docenti ospiti o di nazionalità straniera. Si veda l'analisi di Stephan Blancke "Chinese whispers – Chinese intelligence capabilities", *IHS Jane's*, 3 Luglio 2013.

[44] Si veda in proposito l'articolo di Zunyou Zhou, "China's Comprehensive Counter-Terrorism Law", *The Diplomat*, 23 gennaio, 2016.

raccolta informativa e ad agire essi stessi come agenti-informatori (art. 44) dal momento che vivendo i terroristi fra la gente comune e costituendo essi primariamente una minaccia proprio per la popolazione, quest'ultima godrà di un vantaggio di posizione incomparabile rispetto alle capacità delle più specializzate forze di sicurezza.

Naturalmente il provvedimento può essere banalmente inteso come un intelligente, quanto mai moderno, sforzo di sicurezza partecipata – comune a molti altri ordinamenti nazionali e particolarmente utile allo scopo, considerata la peculiare natura asimmetrica della minaccia terroristica – ma è del tutto impossibile non scorgervi, specie nella forma in cui è espresso, il tradizionale approccio alla mobilitazione delle masse fin qui descritto.

Molta letteratura di settore ci riferisce di questa tipologia generale di reclutamento operato particolarmente dall'MSS per operazioni su larga scala condotte all'estero. Si tratta della grande mole di cosiddetti *short-term agents*[45], individuati tra coloro che decidono autonomamente di lasciare il paese per diversi motivi personali o professionali e reclutati poco prima di partire per le varie nazioni di destinazione con il fine soprattutto di stanare elementi dissidenti in loco – ma non esclusivamente per questo tipo di missioni. Le modalità di ingaggio sarebbero in questo caso molto rapide e comprenderebbero la promessa di aiuti economici o buone occupazioni al rientro in patria in cambio di informazioni, come anche la minaccia di ritorsioni in caso di eventuale rifiuto a collaborare, quali ad esempio la revoca dei documenti per l'espatrio[46].

Più ampia in letteratura la definizione del reclutamento *long-term,* che mira a selezionare i cosiddetti *chen di yu* o "pesci in fondo al mare" o - per usare un gergo occidentale - i tipici "agenti dormienti"[47]. In questo caso ovviamente le modalità di ingaggio si rivelano più sottili, e pur non escludendo quelle già citate, gli agenti dei servizi tenderebbero a far leva maggiormente sulle maglie del sentimento nazionale/patriottistico o su leve economiche. Il reclutamento avverrebbe in Ci-

[45] La definizione di questo tipo di agenti è presa da *Stratfor* - analisi citata in nota 6 – in contrapposizione con i *long-term targets* di cui si tratta subito di seguito.

[46] Molto nota tra gli addetti ai lavori è in proposito la famigerata minaccia di potenziale ritorsione nei confronti delle famiglie rimaste in patria, tanto che parrebbe esistere (o perlomeno vi sono indiscrezioni che fosse esistito in passato) per gli emigranti l'obbligo di rendere noto alle Autorità prima di partire le generalità di tutti i familiari più stretti a tale scopo di ricatto. Taluni sostengono addirittura che avesse maggiori chances di poter lasciare il paese chi avesse lasciato un figlio in patria.

[47] Oltre che nel report di *Stratfor* già citato, si trovano dettagli su questo tipo di reclutamento nella famosa opera Nicholas Eftimiades, *Chinese Intelligence Operations* (Naval Institute Press, febbraio 2011), in particolare nel capitolo 5: "Foreign Operations". Inoltre, il rapporto "2009 Report to Congress of the U. S.", China Economic and Security Review Commission*,* Novembre 2009, costituisce forse uno sguardo di insieme molto più recente sulle attuali capacità di infiltrazione della Cina – anche se solo in ambiente USA ovviamente. Si veda di questo in particolare la parte relativa al reclutamento (pp. 149-166). Il report è disponibile al link www.uscc.gov.

na, prima dell'espatrio e in una prima fase si punterebbe a "formare" l'ambiente dell'informatore prima che a renderlo subito operativo.

Per questo tipo di attività verrebbero adescati, tra gli altri, soprattutto studenti o giovanissimi manager scelti tra coloro che risulterebbero non compromessi per il fatto di non aver mai viaggiato all'estero o per aver avuto in generale pochi contatti al di fuori della Cina. Essi sarebbero incentivati a fare carriera nei paesi di destinazione e ad acquisire meriti e vantaggi anche economici, al fine di conquistare posizioni sempre più rilevanti per l'acquisizione di informazione sensibile. Talvolta questo lavoro di "preparazione dell'ambiente operativo" può durare anni, ma essere poi efficace a sua volta per anni – in un ottica di lungo periodo per gli occidentali difficilmente concepibile - come dimostrano diversi casi venuti alla luce negli ultimi decenni.

Assolutamente esemplificativo di questo modus operandi è il caso di Glenn Duffie Shriver, reclutato nel 2004 appena laureato attraverso un *call for papers* - in particolare un concorso per la scrittura di un'analisi sui rapporti sino-americani – a seguito della quale il potenziale informatore fu spinto dagli agenti dell'MSS a partecipare negli anni successivi a selezioni per posizioni-chiave in USA (un posto nel Dipartimento di Stato per cui ricevette 30.000 dollari, una selezione per la CIA dietro compenso di 40.000 dollari) fino a quando non venne arrestato sei anni dopo, nel 2010.

In questo caso si tratta ovviamente di un tentativo con un esito in ultima fase fallimentare, ma secondo l'FBI esisterebbero centinaia di migliaia di agenti dormienti solo negli Stati Uniti ed è dunque immaginabile che siano ben presenti anche altrove. Il loro *debriefing* avverrebbe ogni paio d'anni in paesi terzi – spesso ad Hong Kong – ma anche tramite il monitoraggio della corrispondenza che sarebbero obbligati ad inviare alle famiglie rimaste in patria e il cui contenuto verrebbe controllato dagli agenti manipolatori anche al fine di trarne informazioni di contesto. Infine, il loro coinvolgimento in attività spionistiche sarebbe aiutato a restare clandestino attraverso la proibizione dei contatti con le ambasciate – da sempre viste come potenziali luoghi di azione della controintelligence dei vari paesi ospitanti.

Il reclutamento e le modalità operative dei *long-term agents* fin qui richiamati - e che rappresentano ormai una sorta di sapere condiviso tra i numerosi analisti di settore - dovrebbero spingere ad archiviare in modo definitivo la convinzione che l'operatività spionistica cinese appaia rozza e senza obbiettivo - come quella solitamente chiamata in causa quando si evoca il fenomeno della *human wave*. In particolare, si aggiunge in questa sede che occorrerebbe altresì prendere le distanze dal convincimento che essa si stia ammodernando e qualificando solo in tempi recenti, dal momento che esistono numerose prove di operazioni clandestine costruite ad hoc che, come già detto, sono apparse operative da decenni e per decenni, e che sa-

rebbe un grave errore di valutazione ritenere dei banali casi isolati, mentre di fatto si palesano come indicatori di un *trend* opportunamente celato, ma da sempre esistente.

Si pensi ad esempio al notissimo caso di Jin Wudai, che, reclutato dall'MSS quando ancora studente, portò avanti una carriera di agente doppio in USA per 30 anni, fornendo alla Cina informazioni così rilevanti da permettere al suo decisore politico persino di orientare in modo efficace la politica estera[48]. Va rilevato che l'attività clandestina di Ji Wudai venne alla luce negli anni '80 – egli commise suicidio in carcere nel 1986 - ma il suo reclutamento avvenne tre decenni prima, elemento questo che rende piuttosto poco plausibile considerare questo *tradecraft* avanzato uno sviluppo davvero recente.

Certamente, a questo particolare punto di vista, è possibile obbiettare la lettura classica secondo cui, della grande mole di studenti e giovani manager ingaggiati *long-term* e inviati in missione in giro per il mondo, la Cina sfrutterebbe nel lungo periodo la condizione di coloro che riescono ad acquisire posizioni rilevanti, senza che ci sia quindi un orientamento specifico assegnato su alcuni di loro o un disegno preciso esistente già nella fase di ingaggio.

Il fatto è però che - anche se in una cornice temporale così ampia, le occasioni più produttive sono senza dubbio suscettibili di rivelarsi nel tempo e possono effettivamente essere considerate degli sviluppi imprevisti all'inizio del processo - all'esordio dell'operazione clandestina si rivela essere presente almeno uno specifico progetto di insediamento in ambiente utile, se non altro per la comprensione e il monitoraggio di tali ambiti, anche solo per la costruzione di rapporti, fino a quando – in alcuni casi certo, non tutti forse – finisce per prodursi un'attività di sottrazione di segreto più tradizionale.

Per i cinesi in altre parole la fase dell'infiltrazione in sé, intesa come presenza e monitoraggio, è già valevole e rilevante, in quanto costituisce presa sull'ambiente, semina per potenziali e più utili mietiture future, poco importa se concepite fin dall'inizio, o definite in itinere. Un tale approccio non è per nulla da liquidare come una sorta di banale "pesca a strascico" – che pure tramite il fenomeno della *human wave* senz'altro in parte esiste – in quanto il progetto di insediamento della cellula esiste ed è specifico e soprattutto diretto in modo costante nel tempo, anche se può risultare meno determinato il *target* particolare della missione che si usa valutare invece nell'ottica occidentale solitamente come più rilevante.

Insomma, le operazioni clandestine cinesi tendono ad essere operazioni che potremmo definire "di insediamento", ma che erroneamente stimiamo senza obbietti-

[48] Ci si riferisce all'importante indiscrezione, resa dall'informatore ai servizi segreti cinesi, relativa al fatto che il presidente Nixon avesse maturato nel corso del 1970 l'intenzione di stabilire migliori rapporti con la Cina.

vo preordinato, in quanto non consideriamo che spesso l'obbiettivo presupposto risiede nell'insediamento stesso.

Come caso da manuale a riguardo può essere annoverato quello di Chi Mak, che reclutato già nel 1960 quando era appena un giovane ingegnere, finì poi per sottrarre importantissima informazione classificata sui progetti di ricerca della Marina Usa solo nel 1990 (ben 30 anni dopo) e solo dopo aver acquisito una specifica *security clearance* presso la Power Paragon presso cui lavorava, posizione alla quale non giunse certo per caso o per soli suoi meriti, ma tramite una prudente e paziente etero-direzione condotta dai suoi agenti manipolatori. Si pensi che alla data del suo arresto, avvenuto nel 2005, quando alla fine giunse al termine del suo percorso, erano trascorsi quarant'anni dal suo reclutamento. In questa lunghissima missione quadri-decennale l'intelligence cinese diresse l'ascesa dell'agente trasferendolo prima ad Hong Kong, poi negli Usa, fino a farlo divenire un cittadino americano e commissionandogli, quando fu allocato nella corretta funzione, una specifica lista di *targets* informativi da coprire.

Peter Mattis, nella sua analisi d'avanguardia[49] sulla prospettiva di valutazione tipicamente occidentale dello spionaggio cinese, riferisce che presso la Power Paragon, controllata della L-3 Communication, Chi Mak aveva accesso ad importanti informazioni sulla tecnologia navale che costituisce un obbiettivo particolarmente strategico per la Cina. In particolare fu oggetto della sottrazione di dati il progetto del sistema *Quiet Electronic Drive* (equipaggiamento della nuova classe di sottomarini Virginia) e della relativa tecnologia DD(X). Tuttavia, al di là della tipologia di informazione sottratta, vale qui la pena di sottolineare il carattere specifico delle richieste operate dall'intelligence cinese al suo agente infiltrato, che rivela un'operatività molto più produttiva di quella aspecifica cui si è soliti far riferimento.

Nella stessa analisi è richiamata un'ulteriore prova storica di prassi spionistiche palesemente *target-oriented*, condotte peraltro in tempi davvero non sospetti. Si tratta dell'operazione di infiltrazione di tre agenti dello Special Department del Partito Comunista Cinese presso alte posizioni dell'apparato del Kuomintang alla fine degli anni '20. Tali agenti, passati alla storia cinese come i "tre eroi della tana del Dragone" fornirono informazione indispensabile per la sopravvivenza del Partito tra il 1928 e il 1932, fino a quando resero il loro più importante compito di trasferimento informativo, essendo messi a conoscenza, nell'esercizio delle loro funzioni, della defezione di Gu Shunzhang, uno dei quattro responsabili proprio dello Special Department. E' opinione condivisa che tale operazione, modernissima nella sua modalità, costituì per il Partito la *chance* di mantenersi in vita, disinnescando una minaccia in grado di debellarlo definitivamente quando era di fatto in uno stadio ancora embrionale, e fu condotta quasi un secolo fa.

[49] Cfr. opera citata in nota 4.

In conclusione, sarà più che ragionevole ammettere l'ipotesi che il *tradecraft* cinese si avvalga in realtà di numerosissime e diversificatissime forme di azione spionistica e che utilizzi i più diversi metodi per il reclutamento e l'infiltrazione dei suoi agenti, comprendendo tra essi forme mediate dalla tradizione e ritenute da molti desuete, accanto ad un'operatività molto moderna per scopi specifici, da non ritenersi di certo solo recentemente acquisita, ma della quale essi hanno mostrato di essere perfettamente padroni già da tempi piuttosto remoti.

Non stupirà quindi veder esercitati, accanto alle avanguardie operative sin qui descritte, vecchi metodi da manuale di adescamento delle fonti anche *short-term*, quali lo sfruttamento della seduzione sessuale[50] o dell'avidità o anche il famoso sistema del *guanxi*[51], a tutti noto come quella paziente tessitura di rapporti di fiducia

[50] Ci si riferisce alla classica forma di reclutamento anche conosciuta come *honey trap*. Si pensi ai numerosi casi di stranieri in visita in Cina sedotti – più che direttamente da agenti, da collaboratori dei servizi di intelligence, di genere maschile e femminile, appartenenti alle cosiddette "aree grigie" - col preciso intento di instaurare una relazione sessuale e il fine ultimo di trasformare il malcapitato in un informatore. Le aree grigie costituiscono un bacino molto rilevante per gli operatori dei servizi, in quanto, essendo ambiti che gravitano ai confini della legalità, offrono molte occasioni per ingaggiare persone disposte a svolgere compiti non esattamente ortodossi e dai quali è facile poi all'occorrenza prendere le distanze, facendo apparire opaco e remoto il coinvolgimento degli apparati di spionaggio. La seduzione sessuale è solo una tra le famigerate tecniche cosiddette di *entrapment*. Un'altra prevede il passaggio di informazione classificata a stranieri in terra cinese (giornalisti, ricercatori e similari) per poi arrestarli con l'accusa di spionaggio, la quale appartiene alla più grande famiglia delle cosiddette *false flag operations*, ove il reclutamento di stranieri avviene ad opera di agenti di nazionalità diversa da quella cinese, ma assoldati o controllati dalla Cina (si veda il caso dell'agente di nazionalità taiwanese Kuo Tai-shen). Naturalmente si tratta di tecniche utilizzate a livello globale in ambito spionistico, ma non mancano di far parte altresì del metodo tradizionale cinese che tuttavia capita ne resti a sua volta attaccato. Si pensi in proposito al caso del agente dell'MSS – collaboratore ad alto livello di Lu Zhongwei, vice ministro dell'MSS, di recente arrestato in Cina per spionaggio in favore della CIA proprio grazie alla tecnica dell'*honey trap*.

Un caso molto noto di seduzione sessuale a fine di reclutamento, invece, è senz'altro quello di Bernard Bursicot. Si tratta di un diplomatico francese che iniziò una relazione con una cantante d'opera, Shi Pei-pu, nel periodo in cui lavorava in Cina come addetto di ambasciata. Tornato di nuovo nel paese nel 1969 come Ambasciatore a Pechino, fu indotto a pensare che la cantante avesse generato un figlio (mentre in realtà era un uomo) e, per far sì che gli fosse consentito mantenere i rapporti con la neo famiglia – ma anche minacciato di venire di fatto arrestato per spionaggio – accettò di collaborare con l'intelligence cinese, trasferendo una grande quantità di materiale riservato e di informazione classificata.

[51] Il *guanxi* è per definizione la rete di rapporti fiduciari/amicali che in accordo con la dottrina confuciana costituiscono una sorta di vero e proprio obbligo dell'individuo nell'ambito della socialità. Il fine è, secondo il dettato della tradizione, quello di costituire attorno a sé un universo di relazioni fin dalla prima infanzia che funga da ombrello protettore nel corso di tutta l'esistenza e a cui sia possibile rivolgersi per ogni istanza, anche pratica, che possa manifestarsi nell'arco della vita, quale ad esempio ottenere un posto di lavoro, velocizzare una pratica burocratica e finanche ottenere collaborazione per agganciarsi a *guanxi* altrui - se tramite essi si ritiene risulti più semplice arrivare alla soluzione dei propri problemi o al soddisfacimento dei propri bisogni. Si tratta di una prassi, va detto, presente ovviamente in tutte le società civili (dal momento che ogni individuo tende naturalmente a contornarsi di una rete di protezione cui ancorarsi in caso di necessità), ma che in Oriente gode di una specifica dimensione ontologica, oltre che solo utilitaristica, la quale in ambito occidentale è finita per venir meno a causa dell'atomismo verso cui tendono gli individui nelle collettività contemporanee. Esistono corrispondenti del *guanxi* in molte culture nazionali d'oriente e fra le altre (con accezioni a vol-

con potenziali candidati a divenire informatori, e che lentamente nel tempo vengono attirati nella rete di dipendenza dalle relazioni costituite.

Semplicemente, i cinesi usano tutto. Il vecchio e il nuovo, tradizione e innovazione, lo spionaggio di massa della *human wave* e il *tradecraft* specialistico delle missioni clandestine cucite sul *target* da perseguire e con orizzonti temporali decisamente vastissimi. E sono abili - nostro malgrado - a celare se si tratti ogni volta dell'una o dell'altra cosa e non - come spesso erroneamente ritenuto – perché non avrebbero il *know-how* per esercitare il controllo su fenomeni troppo estesi e dispersivi (sebbene è innegabile che anche questo accada), ma più spesso perché sono straordinariamente in grado di nascondere il controllo esercitato da remoto su fenomeni di intrusione che finiamo per credere autodiretti o addirittura "non diretti".

Quando il controllo non è visibile, non è per nulla detto che non esista. Così, ad esempio, finiamo per convincerci che all'apparenza gli apparati di intelligence preferiscano reclutare fonti Han, solo perché trascuriamo come quelle fonti strategicamente divengano a sua volta reclutatori di fonti che Han non sono. Una sorta di "reclutamento in appalto" quindi, dove la relazione reale tra il gestore e il gestito sarà molto difficile da individuare e contrastare, mentre gli amministratori ultimi dell'attività clandestina avranno presa su un ambiente estraneo tramite un elemento fiduciario - o più elementi fiduciari - appartenente alla stessa cultura di origine, ma allo stesso tempo meno profano dell'ambito da infiltrare.

Un controllo da remoto dunque, protetto da più passaggi sovrapposti a uno stesso oggetto – nulla di nuovo se pensiamo al procedimento tradizionale delle famose scatole, non a caso, cinesi – o per dirla con il concetto evocato dall'ex analista della CIA, Douglas Paal, e ricordato anche da Peter Mattis, un approccio stratifica-

te più positive, a volte più negative) il *kone* in Giappone, il *bapakism* in Indonesia o il *blat* russo. Con riferimento ai metodi di spionaggio, il *guanxi* opera attraverso la costituzione di rapporti, prima professionali, poi amicali, poi quasi famigliari, con stranieri in terra cinese, al fine di stabilire con essi un rapporto di tale confidenza ed intimità per cui i passaggi informativi avverranno come una sorta di pura e innocente condivisione del sapere, dove sarà difficile persino rinvenire il momento specifico della vera e propria acquisizione o sottrazione di informazione rilevante. In particolare, nel costume spionistico più tipico, il punto di partenza è rappresentato da uno scambio alla pari di informazione - accademica tra ricercatori o economica tra uomini d'affari ad esempio – che porterà ad un coinvolgimento anche personale, tale da interessare persino i rapporti famigliari, fino a che la produttività professionale del reclutando straniero diverrà fortemente legata alle informazioni fornite dall'agente cinese e egli stesso dipendente dalla relazione. A questo stadio ovviamente il rapporto sarà maturo per l'ottenimento di informazione anche molto riservata. La tecnica del *guanxi* è nota per abbassare a tal punto le difese dell'informatore da indurlo in una condizione di quasi inconsapevolezza, come dimostra uno dei casi più eclatanti venuti alla luce negli ultimi anni, quello di Ronald Montaperto. L'analista dell'intelligence statunitense, che fu ritenuto colpevole nel 2006 di aver passato alla Cina (in particolare a due addetti militari di ambasciata) importante informazione classificata, dichiarò che tali trasferimenti informativi avvennero nel contesto di quella che riteneva essere allora un normale scambio professionale nell'esercizio delle sue funzioni. Per dettagli sulla vicenda si veda il capitolo 3 di B. Gertz, *The China Threat: How the People's Republic Targets America* (Washington DC, Regnery Publishing, 2000).

to, dove un *core* di operatori di intelligence altamente professionalizzati gestiscono una rete (o una rete di reti si potrebbe qui aggiungere) di tecnici ed esperti più introdotti – o per i quali risulta più facile introdursi - nei mondi oggetto dell'azione di spionaggio. Tali elementi appariranno certamente meno professionalizzati dal punto di vista delle tecniche di protezione delle identità e dei dati, rappresentando essi l'ultimo anello della catena, la punta dell'*iceberg*, le masse per le quali finiamo per giudicare erroneamente "grezzi e poco abili" gli operatori degli apparati di raccolta informativa cinese in genere.

Ancora, in merito al carattere "multiforme" del metodo cinese, Peter Mattis richiama nella sua analisi l'approccio olistico ai fenomeni che, più tipico delle culture d'Oriente, è più faticoso in quelle di Occidente, in quanto in queste ultime prevale il primato della distinzione piuttosto che della compresenza, della separazione invece che dello sguardo d'insieme, che tradotto in termini di acquisizione di conoscenza e analisi diventerà la ricerca delle verità puntuali per gli occidentali e, al contrario, la comprensione delle dinamiche di sistema per le culture d'Oriente.

Ecco perché i cinesi, nell'acquisizione di intelligence, non rinunciano alla *human wave* che permette una penetrazione degli ambienti poco profonda, ma comunque efficace per un primo addentramento, né all'uso estensivo della Osint, che consente orientamento e preparazione per concepire poi piani di intervento più specifici.

Una volta assodate tali reali capacità degli apparati di raccolta informativa cinese e messe da parte inservibili credenze su fantomatiche estese incapacità di controllo degli stessi, sarà forse più utile per la ricerca di settore concentrarsi sul tentativo di individuare gli obbiettivi che i gestori del sistema si propongono (in quanto è certo che se li propongano) e sulla tipologia di ambienti selezionati a divenire oggetto di infiltrazione - specie se si tratta di ambienti usati come mezzi per approdare ad altri *targets* definiti - ben consapevoli, alla luce di quanto espresso, che tali penetrazioni saranno effettuate con modalità tanto estensive (*human wave*, *open source intelligence* e similari) che intensive (operazioni clandestine mirate e costruite ad hoc su orizzonti temporali anche molto ampi).

Oltre a tutti quelli già citati nei vari paragrafi di questo studio, un ambito principe cui varrebbe forse la pena di dedicare attenzione potrebbe essere quello poco indagato dei rapporti degli apparati di intelligence con il crimine organizzato, che pur costituendo una minaccia per il sistema-paese – e che a dire il vero le Istituzioni cinesi non mancano di perseguire in modo molto offensivo, soprattutto per ciò che attiene al traffico di stupefacenti – rappresenta comunque un ambiente particolarmente produttivo per l'attività spionistica.

Si pensi alle informazioni sulla dissidenza presso nazioni estere che è possibile ottenere tramite il mantenimento di utilitaristiche relazioni con le Triadi sparse nelle varie comunità oltre confine, come anche al reclutamento di hackers dal sot-

tobosco criminale a cui affidare obbiettivi per attacchi cyber[52], o al reclutamento di mediatori di cui il MID usa servirsi per attuare operazioni clandestine di compravendita di armi.

Ancora, è possibile ipotizzare (o perlomeno non si può escludere) che dietro alcuni fra i casi di banche cinesi poste sotto investigazione per riciclaggio possano nascondersi operazioni finanziarie occulte, gestite con il coinvolgimento anche solo indiretto degli apparati di intelligence.

E' d'obbligo rimarcare in proposito che la Cina è stata di recente identificata da un'investigazione condotta dall'Associated Press come nuovo *hub* globale per le attività di riciclaggio di denaro che coinvolgono organizzazioni criminali internazionali quali, fra le altre, quelle europee, colombiane e israeliane. Tali attività interessano spesso servizi import-export e *money transfers*, e mostrano dunque all'apparenza una gestione "privata", ma esistono diversi casi relativi anche a banche di Stato, quale ad esempio la Bank of China[53], che, per effetto di un'indagine condotta dalla Guardia di Finanza, risulta ora tra i 299 imputati del maxi-processo per riciclaggio, inaugurato di recente a Firenze, per un'attività di trasferimento illecito di denaro, per somme che si aggirano attorno ai 4 miliardi di euro e che sarebbero transitate illegalmente dall'Italia alla Cina tra il 2006 e il 2010.

Per ciò che attiene, di questi fatti di cronaca, all'oggetto di quest'analisi, la possibilità che possa essere presente in casi come questo (trattandosi di una banca di Stato appunto) il coinvolgimento di elementi degli apparati di intelligence è suggerita da un'altra investigazione condotta dal Dipartimento di Giustizia statunitense sul fondatore della società di contractors Blackwater, Erik Prince, per traffici illeciti in Africa e riciclaggio di denaro. In particolare, il dato rilevante in questa sede è rappresentato dal fatto che sarebbero emersi forti legami dell'imputato - in occasione in particolare di un sospetto viaggio da egli condotto a Macao – con diversi comparti dell'intelligence cinese, la quale avrebbe funzionato da intermediaria, al fine di far ottenere a Prince contratti illegali in territorio libico e con una contropartita la cui natura sarebbe interessante approfondire[54].

[52] La materia relativa all'offesa cyber e alla cyber-intelligence viene trattata nel paragrafo successivo.

[53] Lo schema del funzionamento di questo tipo di operazioni di *money laundering*, e in particolare quella per cui è indagata la Bank of China, è abbozzato nell'articolo di Antonio Talia "I passaggi sospetti di denaro tra Italia e Cina" pubblicato da *Internazionale* il 23 dicembre 2015. Non a caso, sia la Bank of China che un'altra grande banca di Stato cinese, la China Construction Bank Corp., sono state di recente oggetto di un atto ingiuntivo, una sorta di diffida (la prima da parte dell'OCC- l'ufficio di controllo della valuta statunitense e la seconda da parte della FED), ad imporre controlli meno blandi sull'operatività interna, al fine di perseguire adeguatamente le transazioni finanziarie sospette. Si tratta ovviamente di realtà enormi, anche solo per questo difficilissime da monitorare, e le cui attività risultano diffuse in modo capillare in tutto il mondo. Si pensi che secondo Bloomberg, la Bank of China detiene da sola *assets* globali per un importo di circa 2.5 trillioni di dollari.

[54] La notizia fa riferimento allo *scoop* giornalistico pubblicato dal sito *The Intercept* ad opera di Jeremy Scahill e Matthew Cole. Si veda, per dettagli in merito, la ricostruzione che ne fa Andrea Pira nell'articolo "I legami cinesi dell'imprenditore-mercenario", pubblicato su *China-Files.com* il 30 marzo 2016.

Infine, un'analisi di *IHS Jane's*[55] ci ricorda che una popolazione suscettibile di essere particolarmente attenzionata dai servizi cinesi per il reclutamento e la pianificazione di operazioni occulte è quella dei detentori di *security clearance*, coloro cioè che nell'esercizio delle loro funzioni professionali sono in possesso di particolari autorizzazioni che consentono l'accesso ad informazioni sensibili. In particolare lo studio solleva il problema della sempre maggior tendenza ad appaltare la materia *security* ad imprese di carattere privato, i cui operatori rischiano di essere maggiormente esposti all'infiltrazione posta in essere dalla criminalità organizzata e, tramite essa o anche direttamente senza mediazione, a quella di apparati spionistici[56].

A conclusione di questa analisi relativa al metodo, occorre accennare infine a come esso si sia in parte privato dell'isolamento che tradizionalmente lo ha contraddistinto, da che la prassi spionistica è stata implementata nel sistema di potere del Partito Comunista Cinese. Complici infatti gli interessi commerciali (relativi alla protezione dei *business*, alla definizione di rotte sicure per la movimentazione delle merci e al controllo dei porti e dei luoghi di approdo) e soprattutto quelli correlati agli approvvigionamenti energetici, lo spionaggio cinese sembra essersi reso più cooperativo in minima parte con quello di sistemi che ritiene potenzialmente alleati, con le cui agenzie di intelligence ha provveduto a stipulare proficue forme di collaborazione - particolarmente in Africa e in America Latina - che varrebbe senza dubbio la pena di indagare in modo più approfondito.

4) Le avanguardie del sistema spionistico: dagli attacchi cyber dei vecchi apparati della PLA alla cyber-guerra permanente delle nuove unità spaziali, elettromagnetiche e informatiche integrate

Il fatto che l'offesa spionistica internazionale abbia guadagnato da tempo un ulteriore ambito principe per la sua operatività, e cioè quello cyber, non è certo una novità, come non lo è il fatto che la Cina abbia giocato fin dagli albori di questa nuova tendenza un ruolo decisamente da protagonista. La protezione dell'ambiente cyber è divenuta per ogni nazione una necessità vitale, soprattutto per la protezione che, proprio tramite l'invulnerabilità di esso, è possibile fare delle infrastrutture critiche dei sistemi-paese, ormai sempre più informaticamente interconnesse.

Nell'ottica della spregiudicatezza tipica dello spionaggio industriale cinese –

[55] Si veda l'analisi citata in nota 43.

[56] L'analisi riferisce che secondo il rapporto *Security Clearance Determinations*, pubblicato dall'ODNI (US Office of Director of National Intelligence), sarebbero 4.9 milioni i detentori di tali peculiari credenziali di accesso ad informazione privilegiata solo in USA ed è dunque plausibile che questi rappresentino un campo particolarmente florido per l'attività di reclutamento delle fonti messa in opera dallo spionaggio cinese.

già noto e richiamato anche in questa analisi a proposito della business intelligence di Stato - la Cina non manca certo di sfruttare appieno anche le potenzialità di questo ambito per l'acquisizione di conoscenza utile allo sviluppo della propria economia e, non a caso, la maggior parte degli attacchi di fatto attribuiti alla Cina, dalle investigazioni condotte da diverse agenzie e aziende del comparto sicurezza, hanno finito per avere come oggetto imprese nei settori considerati essenziali per lo sviluppo industriale del paese.

In particolare, se ci si riferisce ai sette settori identificati come economicamente strategici dal piano quinquennale annunciato in Cina nel 2012, sono risultate penetrate da azioni offensive di natura cyber una rilevante quantità di aziende afferenti proprio a ben cinque di questi.[57]

Accanto a questa esigenza di natura economica, primaria per la Cina, occorre tuttavia rilevare la ricerca persistente dell'ammodernamento del sistema d'arma e di quell'innovazione tecnologica indispensabile per aumentare il potenziale militare offensivo e difensivo. A questo scopo, al di là delle operazioni Humint mirate ad acquisire questo tipo di conoscenza cui si è già fatto riferimento, si assiste ad una attività sempre più aggressiva messa in opera proprio dai comparti di cyber-intelligence.

Fra gli obbiettivi ritenuti essenziali sembra essere predominante la conoscenza relativa al controllo dei satelliti nel dominio spaziale ed elettromagnetico cui la Cina ha di recente dedicato la creazione di una speciale unità – la SSF (Strategic Support Force) – di cui si parlerà nel seguito del paragrafo.

Tra i diversi di cui si ha notizia, va in questa direzione l'attacco cyber - presumibilmente operato dalla Cina[58] - ai danni del sistema antimissile israeliano Iron Dome, lo scudo d'acciaio che sarebbe stato in grado di neutralizzare circa un quinto dei duemila missili lanciati da Hamas verso Tel Aviv nel più recente conflitto[59]. La notizia, tenuta a lungo riservata da ambo le parti coinvolte, è stata svelata da un'inchiesta condotta dal giornalista indipendente Brian Krebs.[60]

Ciò che ci si propone di sottolineare dell'evento è che, secondo lo *scoop*, l'attacco informatico sarebbe stato diretto in particolare verso quelle aziende del com-

[57] La notizia è riportata da *IHS Jane's*. Gli attacchi sono stati identificati e attribuiti alla Cina dalla società Mandiant e i sette settori cui si fa riferimento nel "Piano quinquennale sui comparti nazionali industriali emergenti e di importanza strategica" sono: carburanti di nuova generazione per l'industria automobilistica, information technology, biotecnologie, materiali di nuova generazione, industria manifatturiera di lusso, energie rinnovabili e protezione ambientale.

[58] Le prove della violazione informatica e della potenziale attribuzione agli apparati di Pechino sono state fornite da un'investigazione condotta da una società del Maryland, la Cyber Engineering Services.

[59] Si veda in proposito l'articolo di Michele Pierri "Come e perché gli hacker Cinesi hanno rubato i segreti dell'Iron Dome", pubblicato da *Formiche.net*, il 29 luglio 2014.

[60] Si veda l'articolo scritto proprio da Krebs "Hacker Plundered Israeli Defense Firm that Built Iron Dome Missile Defense System" pubblicato da *krebsonsecurity.com* il 28 luglio 2014.

parto difesa responsabili della progettazione e costruzione materiale del sistema[61] e che quindi sono suscettibili di essere di fatto detentrici del *know-how* indispensabile ad una potenziale riproduzione dell'apparato.

Quindi, al di là delle implicazioni geopolitiche del dibattito sorto a seguito della pubblicazione della notizia – e tese a sostenere ad esempio un desiderio da parte della Cina di mettere fuori uso il sistema, al fine di indebolire Israele e gli Stati Uniti e rafforzare Hamas – è molto più plausibile la lettura della sottrazione di conoscenza utile all'avanzamento tecnologico nel settore. Nello specifico, gli attacchi e le interferenze che sarebbero state registrate ai danni dello scudo da parte cinese e che di per sé sembrerebbero avallare l'ipotesi geopolitica, possono invece essere intesi, nell'ottica che qui si propone, come potenziali test all'efficacia ed impermeabilità degli apparati e meno presumibilmente ad una volontà reale di metterli fuori uso. Ne è prova il fatto che la medesima azione di hackeraggio è stata diretta a sottrarre informazione tecnica per la potenziale riproduzione di anche altri sistemi di difesa – quali ad esempio l'intercettore missilistico Arrow 3 progettato da Boeing.

Altro elemento dell'inchiesta, su cui vale la pena riflettere, è l'individuazione degli esecutori materiali degli interventi illeciti. Si tratterebbe del famigerato gruppo di hackers cui si fa riferimento con il nome di Comment Crew, e che sarebbero già stati indicati come responsabili della messa in opera di molteplici altri attacchi rilevati dalla società statunitense Mandiant, e che quest'ultima ritiene essere membri appartenenti alle forze cyber della PLA.

Fino a qui nulla di nuovo. Sappiamo che nell'ambito della PLA esistono delle specifiche unità adibite allo sfruttamento di tali potenzialità, di cui la più nota è la famigerata unità 61398, ossia il Bureau n. 2 del III Dipartimento dello Stato Maggiore Generale della PLA. La Cyber Blue Team*,* la cui creazione venne annunciata dalla stessa Cina nel 2011, doveva ufficialmente essere costituita da un numero ristrettissimo di tecnici altamente specializzati, ma esistono indiscrezioni – riportate anche dalla stessa Mandiant[62] – di una manodopera vastissima messa a disposizione di tali intenti illeciti che suggeriscono ben altre cifre – addirittura centinaia, forse migliaia, di esperti che presenterebbero un elevatissimo standard di addestramento, alte capacità cyber-ingegneristiche sommate a particolari abilità linguistiche.

Esso sarebbe solo uno dei ben 12 bureau di cui appare essere costituito, assieme a tre peculiari istituti di ricerca, il III Dipartimento sopra citato, anche conosciuto come San Bu, stimato essere l'apparato di Sigint (*Signals Intelligence*) più vasto

[61] Si tratterebbe di circa 700 files equivalenti a 762 megabytes sottratti a Elisra Group, Israel Aerospace Industries e Rafael Advanced Defense Systems nel periodo che intercorre tra il 10 ottobre 2011 e il 13 agosto 2012.

[62] Si veda il *report* pubblicato dalla Mandiant, ormai divenuto un classico in letteratura: "APT1 Exposing One of China's Cyber Expionage Units", disponibile su intelreport.mandiant.com**.**

ed efficace al mondo - dopo quello statunitense e quello russo - per il monitoraggio delle comunicazioni militari e diplomatiche internazionali. Di questi 12 uffici in particolare, sarebbe diretto alla sorveglianza dell'Europa (sia Occidentale che Orientale) il Bureau n. 8, anche detto unità 61046, mentre il Bureau n. 2 risulterebbe apparentemente avere come particolari targets gli Stati Uniti e il Canada[63].

Nonostante una così possente struttura al servizio di tali scopi intrusivi e appartenente ufficialmente e di fatto al mega-apparato della PLA, esiste, come già accennato, un'attitudine molto diffusa all'*outsourcing* delle operazioni clandestine di hackeraggio. Per questo genere di attività che potremmo definire "in appalto" - benché sia poco plausibile ritenere che possa trattarsi davvero di un'operatività completamente delegata, mentre è più ragionevole pensare che sia concepita piuttosto come un affidamento parziale e controllato – gli apparati spionistici cinesi possono contare su una manovalanza esperta molto comune nella popolazione cinese Han, la quale si mostra diffusamente competente nell'utilizzo di tecnologia informatica.

In tali circostanze, il reclutamento si avvarrebbe ovviamente di tutte le modalità già descritte in precedenza - comprendendo tra le altre anche la leva patriottica di un'*expertise* messa al servizio della madre patria - ed è pensabile che il gestore ne sia il Bureau n. 7, detto di Scienza e Tecnologia, posto alle dirette dipendenze del MID. Secondo *Stratfor*, esso si servirebbe per la sua attività di due computer centers, sei istituti di ricerca collegati al Governo e di una serie di aziende che producono equipaggiamenti elettronici, tecnologia satellitare e apparecchiature di ascolto di vario genere.[64]

Nell'ottica di allontanare il più possibile da sé la potenziale attribuzione delle responsabilità per i numerosi attacchi di natura cyber perpetrati in modo diffuso, ma sempre più scomodi da gestire per il biasimo che finiscono per generare sul piano della diplomazia internazionale, gli apparati di intelligence della Cina sembrano divenuti - secondo alcuni[65] – molto più attivi nei loro rapporti con il crimine organizzato, al fine di reclutare hackers utili a tale scopo.

All'occorrenza infatti, ogni qual volta le operazioni clandestine vengono alla luce, risulta di fatto più semplice evitare il danno d'immagine, condannando gli eventuali accadimenti come semplicemente generati da una realtà di fatto criminale e dunque come semplici episodi di devianza. Inoltre, il reclutamento dal sostrato del crimine organizzato consente una disponibilità di addetti a livello internazionale che, mentre renderanno ancora più semplice dribblare potenziali problemi di attribuzione, consentiranno altresì attacchi più diffusi e più complessi.

[63] Per una descrizione dettagliata dell'organizzazione del III Dipartimento, si veda lo studio di M.A. Stokes, J.Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure", pubblicato da *Project 2049 Institute*, 11 Novembre 2011.

[64] Cfr. analisi citata in nota 6.

[65] Si veda ad esempio la posizione espressa dall'autore dell' analisi *IHS Jane's* citata in nota 43.

A questo proposito, capita spesso che il governo cinese abbia di recente provveduto ad arrestare hackers resisi responsabili di attacchi segnalati dalle Autorità statunitensi, dimostrando formalmente e ufficialmente una collaborazione che, per quanto non si possa di certo archiviare come sicuramente non veritiera, non è però possibile valutare nemmeno come inequivocabilmente autentica, proprio alla luce di tali presunte commistioni con ambiti delinquenziali[66].

Va sottolineato a questo punto che la Cina non manca certo di essere essa stessa vittima di attività *cyber-offensive* messe in opera da sistemi concorrenti, quali non ultimo quello americano. A tal proposito, al di la degli attacchi puntuali, anche verso singole imprese - come ben documentato dal materiale emerso a seguito del caso Snowden nel 2013, correlato ad esempio alla nota intrusione dell'NSA statunitense negli apparati del colosso Huawei – la Cina sembra mal sopportare l'attività di permanente sorveglianza praticata dalla Sigint straniera – soprattutto americana – che sfruttando l'integrazione di risorse aerospaziali ed informatiche la espone ad un monitoraggio contro cui sta di recente riorganizzando la sua difesa.

Nello specifico, dall'analisi delle recenti attività di riforma che le Autorità di Pechino sembra stiano attuando sul comparto militare e di difesa, emerge la considerazione dell'importanza di una strategia che integri gli ambiti cyber, satellitare/aerospaziale ed elettromagnetico, al fine di potersi confrontare più adeguatamente con l'offensiva posta in essere dalle nazioni più sviluppate.

Oltre a quanto già descritto a proposito delle strutture deputate all'operatività cyber e alla Sigint del III Dipartimento, la Cina appare avere una struttura deputata *all'Electronic Intelligence* (Elint)[67] abbastanza avanzata, nonché una struttura all'interno del II Dipartimento dello Stato Maggiore Generale della PLA, da sempre operativa per il controllo delle immagini da satellite.

Tuttavia, la mancanza di un'efficace integrazione tra i dipartimenti – associata alla preoccupazione della loro completa sottomissione al sistema della PLA, dominata fino ad oggi com'è noto dal potere e dall'influenza del comparto delle forze di terra – ha spinto le istituzioni cinesi ad elaborare una serie di interventi legislativi tesi a rendere più produttivo il sistema di difesa cyber/satellitare e soprattutto più direttamente disponibile per l'esecuzione dei desiderata espressi dall'Esecutivo.

Tra i provvedimenti a cui si fa riferimento, è utile annoverare in questa sede la recente disposizione[68] che prevede lo spostamento del quartier generale delle for-

[66] Si veda l'articolo di Brian Krebs, "Arrest of Chinese Hackers not a First for US", *krebsonsecurity.com*, 13 ottobre 2015.

[67] Per dettagli sulle capacità Elint della Cina, si veda L. Easton e M.A. Stokes "China's Electronic Intelligence (Elint) Satellite Developments: Implications for U.S. Air and Naval Operations"*, Project 2049 Institute*, 23 febbraio 2011.

[68] Ci si riferisce all'impianto riformatorio della PLA emanato direttamente dall'Esecutivo di Xi Jimping il 31 dicembre 2015 ed operativo già dai primi mesi del 2016.

ze di terra della PLA in una sede distaccata rispetto allo Stato Maggiore Generale, in modo tale da creare una realtà separata, più facile da controllare e meno indistricabilmente legata all'operatività specifica della raccolta informativa – specialmente di natura cyber, Sigint ed Elint – che rimarrebbe invece confinata sotto lo Stato Maggiore Generale - sebbene è convinzione diffusa tra gli analisti che si sia prossimi ad una sua ulteriore riorganizzazione.

Tale riforma, apparentemente un intervento prettamente formale e basato su necessità di natura logistica, potrebbe invece nascondere la specifica volontà strategica di porre questi comparti d'intelligence in una posizione separata, e in parte forse sovraordinata, rispetto alla forza militare di base, assegnandogli appunto una posizione di avanposto al fine del perseguimento degli obbiettivi di difesa e non solo.

La parte più interessante del provvedimento - e quella peraltro più direttamente connessa alla materia di questo studio – riguarda la creazione di due nuovi organi militari, la Rocket Force e la SSF (Strategic Support Force).

Secondo gli osservatori[69], la prima di queste, anche detta People's Liberation Army Rocket Force (PLARF), rappresenta l'azione di rinnovamento del vecchio PLASAF (il noto corpo di seconda Artiglieria) e dunque un segnale strategico dell'incremento di investimento e di sviluppo che la Cina intende portare avanti sulla sua capacità missilistica (specie di raggio lungo e intermedio); la seconda invece, la definizione di una forza di supporto strategica, rappresenta il tentativo di realizzare quell'integrazione mancante cui si è accennato, basata su un uso combinato - per così dire - dell'ambito cyber, aerospaziale ed elettronico, dove il primo comprenderebbe le azioni di hackeraggio mirate ad obbiettivi sia offensivi che difensivi, il secondo la ricognizione e navigazione satellitare e il terzo la gestione della più generale guerra elettronica mirata soprattutto al disturbo delle comunicazioni, anche radar, del nemico e specialmente alla protezione da esse.

L'integrazione di tali domini[70] permetterebbe una sorta di "cyber-guerra permanente" che, emancipandosi dal concetto di un'operatività legata a singoli attacchi perpetrati dalle singole unità per il perseguimento di obbiettivi specifici, renderebbe possibile un'azione costante di monitoraggio difensivo e all'occorrenza anche di

[69] Si veda l'analisi di John Costello "China Finally Centralizes its Space, Cyber, Information Forces", *TheDiplomat.com*, 20 gennaio 2016.

[70] L'analista Costello - nell'analisi citata in nota precedente – denomina questo nuovo ambito integrato come CoG, *Information Center of Gravity*, il quale risulterebbe maggiormente in grado di contrastare le azioni offensive dei moderni apparati militari stranieri – specie americani – per l'uso che viene fatto proprio dell'ambito satellitare. L'autore ricorda infatti che, nella convinzione di molti ricercatori cinesi, la gestione dei satelliti rappresenta un elemento vitale del comparto difesa americano, al punto di potersi riferire ironicamente alla sua produttività con l'espressione "*no satellites, no fight*". Sotto questo aspetto, quindi, un'intensificazione del controllo di questo ambiente precipuo da parte di un paese può rappresentare un significativo cambiamento di contrappesi sul piano della deterrenza strategica.

offesa permanente. In particolare, quest'ultima sarebbe consentita dal superamento dell'ostacolo detto "del *First Strike*", relativo alla presumibile chiusura dei sistemi nel momento subito successivo all'attacco cyber.

Secondo l'analista John Costello[71] infatti, l'uso esclusivo del vettore internet, caratteristico degli attacchi cyber tradizionali, presume ovviamente il distacco dalla rete aperta pressoché immediato da parte del sistema della parte offesa, al fine di auto-proteggersi, fin dai momenti subito successivi alla produzione dell'azione offensiva (o per meglio dire subito successivi alla fase in cui ci si rende di fatto conto di essere sotto attacco), cosa che rende inefficace, e in verità completamente inattuabile, il proseguimento del conflitto.

Al contrario invece, la possibilità di far leva su attacchi coadiuvati dal controllo dell'ambito aerospaziale, o attraverso l'uso sapiente di un'efficace attività di disturbo delle trasmissioni in ambito elettromagnetico, aumenterebbe di gran lunga la vulnerabilità dei sistemi offesi, diminuendo la loro capacità di sottrarsi all'azione intrusiva anche solo – ad esempio – differendo il momento in cui si produce l'autoconsapevolezza di essere sotto attacco e la messa in opera delle attività di autoprotezione che ne conseguono.

In un approccio di tal genere verrebbe a confondersi, per quanto attiene all'offesa cyber, la prassi di guerra con la prassi di pace, e a prodursi un contesto dove diventerebbe persino indistinguibile il momento specifico dell'attacco come siamo abituati ad intenderlo nella modalità tradizionale. Il risultato ne sarebbe un'attività intrusiva permanente, quand'anche confinata al solo scopo del monitoraggio e della sorveglianza, perfettamente in linea con quell'approccio alla "mobilitazione permanente" - mediata dalla tradizione maoista - che specie in campo militare costituisce per i cinesi un'ambizione costante cui tendere.

5) Conclusioni

A conclusione di questa analisi, ove ci si proponeva di fornire una panoramica, benché non esaustiva, ma il più possibile attuale, delle reali capacità degli apparati di raccolta informativa cinese, si evidenzia come l'attività di ammodernamento dei vari comparti si riveli indubbiamente primaria per le istituzioni della Cina. Tuttavia, essa non dovrebbe intendersi necessariamente come una tendenza al superamento delle modalità tradizionali, ma sostanzialmente come il tentativo di procedere ad un'integrazione di tutte le risorse disponibili, pur non rinunciando a perseguire certamente *know-how*, addestramento e specializzazione.

[71] Si veda report di Costello citato in nota 69 e, per maggiori dettagli circa il problema del *First Strike*, l'analisi ad opera dello stesso autore "Chinese Views on the Information 'Center of Gravity': Space, Cyber and Electronic Warfare", *The Jamestown Foundation*, 16 aprile 2015.

Gli studi più avanzati, disponibili in letteratura, esortano a giudicare le abilità spionistiche cinesi con una prospettiva meno miope e il più possibile avulsa da un approccio tipicamente occidentale, al fine di individuare le potenzialità latenti di un sistema che finisce per apparire obsoleto e inefficace ogni qual volta si fallisce nel cogliere come sia in realtà semplicemente diverso.

Equipaggiamenti e *tradecraft* cinesi possono talvolta innegabilmente essere ritenuti a ragione obsoleti - e di fatto spesso è indubbio che lo siano – ma questo aspetto diventa assai irrilevante se essi appaiono essere sfruttati in modo tale da funzionare ed essere efficaci; in altre parole, occorrerebbe valutare maggiormente l'utilità e la produttività dei mezzi al termine dei processi prima che solamente la loro presunta qualità/capacità alla fonte.

In quest'ottica, si dimostra assolutamente ininfluente stimare modalità di ingaggio o *debriefing* di agenti e fonti cinesi come superate, se poi questi ultimi finiscono per riuscire a sottrarre informazione classificata, indisturbatamente per archi temporali di 30-40 anni!

Allo stesso modo, sarà poco utile crogiolarsi sulla convinzione – peraltro sicuramente corretta – di una flotta navale datata e lontana ancora di parecchie lunghezze dalle avanguardie ad esempio statunitensi, se un più che vetusto sottomarino cinese appare poi improvvisamente in grado di ombreggiare per ore navi militari americane in esercitazione[72]. Valutare realisticamente la portata di una minaccia significa anche assegnare realisticamente il giusto peso ai targets raggiunti da chi la mette in opera – evitando la pericolosa propensione ad archiviarli semplicisticamente come banali episodi isolati, rispetto a presunte tendenze, a volte dogmaticamente poco messe in discussione.

L'attitudine dei cinesi a "fare intelligence" nel lunghissimo periodo, differendo

[72] Il 13 Novembre 2006 l'*Adnkronos* rilanciò la notizia, già pubblicata dal *Washington Times*, secondo cui, il 26 ottobre 2006, un sottomarino cinese riuscì ad ombreggiare (e dunque "a seguire senza essere a sua volta intercettato") il gruppo navale della portaerei statunitense Kitty Hawk nelle acque del Pacifico e venne individuato solo una volta riemerso, ad una distanza di fuoco dalle unità americane. Nel pezzo venne precisato che il sottomarino da combattimento di classe Song, a motore diesel, fù in grado di arrivare a cinque miglia (solo otto chilometri) dalla Kitty Hawk, prima di essere scoperto da un volo di routine degli aerei da ricognizione del gruppo navale.

Occorre per correttezza riferire che questo episodio passato – avvenuto nel 2006 e quindi a distanza ormai di circa 10 anni dal tempo in cui si scrive - non sia stato in realtà per nulla sottovalutato e che il monitoraggio delle flotte americane da parte cinese continui, ma apparentemente sotto il controllo attento degli USA. Tra i numerosi casi che si sono ripetuti in questi anni, nell'ultimo segnalato, avvenuto a fine 2015, quando la portaerei americana Ronald Reagan venne osservata per 12 ore da un sottomarino cinese, un portavoce del Pentagono puntualizzò in merito come il sommergibile fosse stato a sua volta monitorato per tutto il tempo dai sistemi radar americani, cosa ancora tecnologicamente piuttosto semplice da eseguire dal momento che, per quanto i cinesi stiano procedendo ad un rapidissimo ammodernamento degli equipaggiamenti, le loro unità appaiono essere ancora significativamente "rumorose" - e dunque per il momento facilmente individuabili. Si veda in proposito l'articolo di Franco Iacch, "Sottomarino Cinese spia per 12 ore la USS Reagan: Pentagono: 'non lo abbiamo perso un solo istante'", *Difesaonline.it*, 5 novembre 2015.

il momento della raccolta informativa più utile ad orizzonti temporali incredibilmente estesi, la tendenza all'osservazione costante, e, allo stesso tempo però, l'integrazione di questo esercizio paziente con forme di reperimento informativo più rapido, suggeriscono un uso dello strumento spionistico diversificato e spregiudicato che sarebbe decisamente un grave errore sottostimare, al fine ovvio di evitare spiacevoli sorprese certo, ma anche solo per acquisire una conoscenza che sia il più possibile veritiera delle potenzialità di un sistema concorrente che già di per sé, per opacità e complessità, sembra sfuggire a ogni più semplicistica classificazione.