

MARCELLO TRISOLINI

INTELLIGENCE DI POLIZIA

LE FORZE DELL'ORDINE COME *HUMAN SENSORS*

Prefazione di Mario Caligiuri



SOCINT SOCIETÀ ITALIANA DI INTELLIGENCE



© 2020 Marcello Trisolini

Società Italiana di Intelligence
c/o Università della Calabria, Cubo 18-b, 7° piano
via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia

<https://www.socint.org>

ISBN 979-12-80111-13-5

Design di copertina: BESKEIE 

CREDITS

Immagine di copertina: Freepik.com

Font family: Roboto

MARCELLO TRISOLINI

INTELLIGENCE DI POLIZIA
LE FORZE DELL'ORDINE COME HUMAN SENSORS

INDICE

Estratto	p. 6
Prefazione di Mario Caligiuri	p. 9
Note introduttive	p. 21

CAPITOLO 1 COS'È LO HUMAN SENSOR

1.1 – Dalla guerra simmetrica alla guerra asimmetrica	p. 31
1.2 – L'antiterrorismo e la guerra asimmetrica: l'esperienza israeliana	p. 34
1.3 – Human Sensor e il 4° battaglione	p. 37
1.4 – Fondamenti dell'attività di Human Sensor	p. 42

CAPITOLO 2 UNA DIVERSA VISIONE DELLE FORZE DI POLIZIA

2.1 – Intelligence dei Servizi di informazione e delle Forze di polizia	p. 47
2.2 – L'attività di OES (osservazione, elicitazione e sorveglianza)	p. 51
2.3 – Le Forze di polizia in Italia	p. 57
2.4 – L'attività di polizia fuori dal servizio	p. 64
2.5 – Implementazione del modello OES nell'attività di Human Sensor: una questione di psicologia sociale e di statistica	p. 67

CAPITOLO 3 LO HUMAN SENSOR NELL'ATTIVITÀ DI INTELLIGENCE DI POLIZIA

3.1 – Intelligence di polizia e Sicurezza Nazionale	p. 83
3.2 – Il modello investigativo e informativo nell'attività pratica delle FF.pp.	p. 91

3.3 – L'importanza dello Human Sensor nei nuovi scenari demografici e tecnologici.	p.103
Conclusioni	p.118
Glossario	p.121
Bibliografia	p.123
Indice dei nomi	p.128

ESTRATTO

Se tutti sono rivolti a guardare il mondo virtuale, chi guarda quello reale?

INTELLIGENCE DI POLIZIA
LE FORZE DELL'ORDINE COME HUMAN SENSORS
di
Marcello Trisolini

Tutte le attività umane, siano esse sociali, economiche, politiche o militari dipendono sempre più da internet. Governare e controllare il mondo virtuale (o *cyberspace*) significa, non di meno, governare e controllare quello reale. Ed è per questo che Stati e privati stanno dirigendo le maggiori risorse ed intelligenze in questa direzione. Non tutto però accade o accadrà in internet. Anzi, proprio perché l'attenzione è maggiormente rivolta al mondo virtuale, possibili scenari di pericolo alla Sicurezza Nazionale potranno verificarsi nel mondo reale. Questo presuppone, quindi, la necessità non solo di trovare un modo efficace per non lasciare totalmente indifeso questo enorme fronte, ma che sia anche economicamente conveniente visto il costante disimpegno di risorse dal mondo reale a vantaggio del mondo virtuale. In simili circostanze è sempre conveniente valutare e valorizzare ciò di cui già si dispone nella propria organizzazione, prima di intraprendere nuove strade.

L'Italia è il terzo Stato al mondo con il maggior numero di Forze di polizia in relazione alla popolazione e resta l'unico paese ad avere quattro forze dell'ordine a carattere nazionale. Una organizzazione che, malgrado sollevi problemi di efficacia dell'attività informativa, d'indagine e di coordinamento, potrebbe essere utilizzata per determinare migliori risultati in riferimento alla Sicurezza Nazionale, proprio grazie a questo particolare assetto.

Le Forze di polizia in Italia, infatti, sono una forza: numerosa (più di 300mila unità), presente e distribuita su tutto il territorio nazionale, con un addestramento militare di base, già disponibile e senza maggiori costi d'impiego da doversi aggiungere.

Quindi, se le Forze di polizia venissero formate in modo "specifico", estendendo l'addestramento a tutti i suoi appartenenti in modo generalizzato, si potrebbero implementare quelle capacità di osservazione, elicitazione e sorveglianza (OES) del territorio che molto spesso non tutti gli appartenenti di polizia posseggono. Abilità queste che ciascun operatore eserciterebbe in modo più o meno efficace non solo quando è in servizio, ma soprattutto quando veste i panni di semplice cittadino. Questo nuovo orientamento, non solo darebbe alle Forze di polizia una maggior capacità informativa, utile al contrasto alla criminalità organizzata, ma aumenterebbe sensibilmente anche le *chance* dell'attività di Intelligence di intercettare quei "segnali deboli" così tanto difficili da riconoscere quanto pericolosi per la Sicurezza Nazionale.

Ogni giorno gli appartenenti alle Forze di polizia sono naturalmente immersi in luoghi reali e dinamici quali città, paesi, strade, negozi, chiese, musei, ecc.; parlano con conoscenti ed

estranei, osservano, ascoltano e ricevono informazioni d'ogni genere, ma non sempre e non tutti sanno ricavarne informazioni utili. Quindi, si tratta solo di dire loro *cosa* e *come* fare. Un "numerioso esercito" già disseminato su tutto il territorio e pronto ad essere attivato come fossero tanti sensori umani (Human Sensors - una teoria già utilizzata in ambito militare), capaci non solo di monitorare una più vasta porzione di popolazione e di territorio, ma di comprenderne le sottili sfumature.

Gli uomini, differiscono da altri sistemi artificiali di raccolta in quanto interagiscono tra loro e con l'ambiente circostante nei modi più imprevedibili e più di quanto potrà mai fare un sensore artificiale. Di qui il concetto che ogni operatore delle Forze di polizia è un sensore umano sul territorio.

Mentre la tecnologia avrà un impatto sul futuro della Sicurezza Nazionale di ciascuno Stato, il suo successo continuerà a essere determinato dalla sua risorsa, arma e sensore più importante: l'uomo.

PREFAZIONE

L'11 settembre venne considerato un fallimento internazionale dell'Intelligence, poiché la prevalenza tecnologica nella difesa della sicurezza nazionale non aveva impedito l'attacco terroristico più clamoroso di tutti i tempi. Eppure le informazioni, in vario modo, erano state preventivamente raccolte ma purtroppo vennero interpretate solo dopo l'evento¹.

Attualmente stiamo sperimentando le tecnologie per difenderci dalla pandemia che ha messo in ginocchio il pianeta e le varie soluzioni non dovunque danno risultati apprezzabili. In Italia abbiamo l'esempio ampiamente deludente dell'app "Immuni"².

Entrambi i casi dimostrano che affidarci adesso quasi completamente alle tecnologie non è la strategia adeguata per fronteggiare la dimensione del rischio che sarà sempre più endemica nel XXI secolo³.

Sembra, quindi, emergere una sorta di paradosso che dimostra come all'invasione incontenibile delle tecnologie e dell'intelligenza artificiale corrisponda la necessità di affiancare sempre di più il fattore umano. Non a caso, proprio per

1 W. Lawrence, *Le altissime torri. Come al-Qaeda giunse all'11 settembre*, Adelphi, Milano 2007.

2 Tra gli altri, vedi *Il fallimento di Immuni è costato molto caro. L'equivalente in Germania funziona benissimo*, 9.11.2020, <https://www.nonsprecare.it/fallimento-app-immuni>; *Lo spettacolare fallimento delle app contro il coronavirus*, 9.7.2020, https://www.repubblica.it/dossier/stazione-futuro-riccardo-luna/2020/07/09/news/lo-spettacolare_fallimento_delle_app_contro_il_coronavirus-261374292/

3 U. Beck, *La società del rischio*, Carocci, Roma 2000.

assicurare la fondamentale sicurezza nazionale, l'Intelligence israeliana sta assumendo da qualche anno contemporaneamente hacker e laureati in filosofia: i primi per individuare le informazioni nei recessi reconditi della Rete e i secondi per interpretarle⁴.

Nella nostra epoca le manifestazioni sociali si svolgono, direttamente e indirettamente, in modo considerevole nel cyberspazio, poiché oltre la metà della popolazione mondiale è collegata in Rete, la quale rappresenta l'ambito prevalente dal punto di vista economico e politico, comunicativo ed educativo.

Anche i reati si compiono sempre di più in modo esponenziale sul web tanto che il Cybercrime rappresenta per le mafie la seconda fonte di reddito dopo il commercio delle droghe⁵.

Pertanto, il tema della sicurezza cibernetica è centrale⁶. Non a caso proprio recentemente in Italia è stato creato per legge l'Istituto Italiano di Cybersicurezza diretta emanazione della Presidenza del Consiglio, che rappresenta un chiaro indicatore di come l'attività della sicurezza nazionale vada necessariamente orientata verso il cyber spazio⁷.

4 M. Caligiuri, *Intelligence e guerre dell'informazione nel XXI secolo: come respingere più efficacemente le minacce cyber*, in U. GORI (a cura), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Angeli, Milano 2019, p. 55.

5 Non è semplice stimare il costo crescente dello spionaggio informatico, che ammonterebbe a 445 miliardi dollari e che per il generale Keith Alexander, Direttore della National Security Agency (NSA) dal 2005 al 2014, rappresenta il "più grande trasferimento di ricchezza nella storia". <http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>.

6 Tra i più attenti studiosi del fenomeno è Umberto Gori, del quale tra i tanti vedi U. Gori, L.S. Germani (a cura), *INFORMATION WARFARE 2011, La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Angeli, Milano 2012.

7 M. Caligiuri, *Istituto Cyber? Modello Mossad*, 15.11.2020, <https://formiche.net/>

Infatti, l'interesse nazionale sarà sempre più assicurato in larga misura dalla sicurezza cibernetica, dalla quale si potrebbe presto far dipendere il *rating* di un Paese⁸. Non a caso, le guerre di fatto che oggi stiamo combattendo, a cominciare da quella del Covid-19⁹, sono soprattutto guerre di informazioni, interne ed esterne alle nazioni e alle persone¹⁰.

Altro aspetto che occorre considerare è la costante urbanizzazione, poiché tra pochi anni la maggior parte della popolazione mondiale vivrà in megalopoli organizzate da tecnologie sempre più potenti, le cosiddette *smart city*. Questo porrà inevitabilmente rilevanti problemi di sicurezza¹¹.

Le *smart city* saranno città che renderanno più agevole la qualità della vita ai cittadini, che però saranno costantemente controllati, delineando una società della sorveglianza¹².

Nelle aree strategiche delle città intelligenti saranno centrali i settori delle mobilità, delle opere pubbliche, dell'energia e dei rifiuti con prevedibili invadenze della criminalità organizzata collegata con la corruzione¹³.

2020/11/istituto-cyber-modello-mossad-scrive-caligiuri/.

- 8 É quanto sostiene il Ministro degli Esteri del Governo Monti, Giulio Terzi di Sant'Agata. P. Fiore, *Il rating di uno Stato dipenderà presto dal suo grado di cybersecurity?*, 3.12.2018, https://www.agi.it/innovazione/rating_sicurezza_informatica_difesa-4694301/news/2018-12-03/.
- 9 Caligiuri Mario (a cura), *Post Covid-19, Analisi di Intelligence e proposte di policy 2020-2021(2020)*, allegato a "Formiche", n. 5, maggio 2020.
- 10 G. Gagliano, *Guerra psicologica. Saggio sulle moderne tecniche militari cognitive e di disinformazione*, Fuoco, Roma 2013.
- 11 M. Caligiuri, *Potere e sicurezza nelle smart cities*, in "Limes", 5, maggio 2019, pp. 231-236.
- 12 Z. Bauman, D. Lyon, *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari 2014. La "società della sorveglianza" sta producendo a sua volta il "capitalismo della sorveglianza": S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, Roma 2019.
- 13 G. Galli, *Il golpe invisibile. Come la borghesia finanziario-speculativa e i ceti buro-*

In tale quadro, si sta rapidamente sviluppando l'impiego delle tecnologie dell'intelligenza artificiale nel campo della prevenzione dei crimini¹⁴.

Gli algoritmi del precrimine, però, vanno utilizzati con grande attenzione perché si potrebbero trasformare nel loro contrario, ponendo il problema centrale non tanto della privacy, di fatto inesistente, quanto della gestione umana delle istituzioni e delle élite politiche¹⁵.

Appunto per questo, facendo riferimento a quella che era ritenuta fantascienza, le qualità umane saranno sempre più fondamentali.

Nell'avveniristico "Minority Report", racconto di Philip K. Dick del 1956¹⁶ diventato un film di grande successo nel 2002¹⁷, c'è un'unità della polizia anticrimine denominata "Pre-

cratico-parassitari hanno saccheggiato l'Italia repubblicana fino a vanificare lo stato di diritto, Kaos, Milano 2015.

- 14 "Tra gli altri, a Los Angeles con il programma Predpol, a Chicago con la definizione di algoritmi per l'analisi dei crimini urbani e poi in Germania con le attività di Pre Crime Observation System e la Metropolitan Police di Londra che utilizza il software Accenture per individuare in anticipo i membri di una gang che può commettere un crimine. Anche in Italia, si stanno sviluppando queste esperienze. Si è iniziato nel 2007 a Milano con Key Crime che calcola gli obiettivi più a rischio e poi successivamente a Trento con il Laboratorio di sicurezza urbana predittiva "Esecurity", mentre a Venezia il 16 novembre del 2018 un algoritmo aveva già previsto un furto e a Napoli un ispettore della questura, Elia Lombardo, ha sviluppato il sistema "XLaw" basato sulle quattro P: prevenzione, previsione, proattività, partecipazione". M. Caligiuri, *Potere e sicurezza nelle smart cities*, cit., p. 234. Elia Lombardo ha precisato il suo progetto in E. Lombardo, *Sicurezza 4 P. Lo studio alla base del software XLAW per prevedere e prevenire crimini*, Mazzanti, Venezia 2019.
- 15 "Alla lunga il problema non sarà stabilire chi o come, di volta in volta, debba comandare, ma chiedersi se, e in tal caso come mai, qualcuno sarà ancora disposto ad obbedire". G. Azzolini, *Dopo le classi dirigenti. La metamorfosi delle oligarchie nell'età globale*, Laterza, Roma- Bari 2017, p. 161.
- 16 P.K. Dick, *Rapporto di minoranza e altri racconti*, Fanucci, Roma 2002. L'edizione originale è del 1956.
- 17 *Minority Report*, film diretto da Steven Spielberg (2002).

cog”, in cui attraverso i poteri della mente di alcuni superdotati vengono previsti i delitti prima di essere compiuti. Quindi la sicurezza viene garantita comunque dalle persone e non dagli algoritmi¹⁸.

In tale ampio e travolgente contesto culturale, si colloca l’innovativo lavoro di Marcello Trisolini che, come compimento di un brillante percorso di studi, approfondisce la figura dello *human sensor* nelle Forze di polizia¹⁹.

L’autore interpreta appunto le Forze di polizia come *sensori umani* nell’attività di Intelligence, attraverso l’approccio interdisciplinare della statistica, della psicologia sociale, dell’economia. In particolare propone specifici metodi di formazione per sviluppare capacità di osservazione e sorveglianza²⁰, utilizzando il modello sperimentato dal 4° battaglione di fanteria ameri-

-
- 18 Questa finzione letteraria porta però l’attenzione sui poteri della mente che durante la guerra fredda vennero esplorati dalle agenzie di intelligence. Vedi L. Buchanan, *Il settimo senso. I segreti delle spie psichiche dell’esercito americano*, Edizioni Il Punto di Incontro, Vicenza 2010; S. Ostrander, L. Schroeder, *Scoperte psichiche dietro la cortina di ferro. URSS/BULGARIA/CECOSLOVACCHIA*, MEB, Torino 1975; A. Lissoni, *Psicospie. Viaggio negli archivi segreti del paranormale in America, Russia e Medioriente*, Editoriale Olimpia, Sesto Fiorentino 2003. Vedi inoltre A. Teti, *PsychoTech. Il punto di non ritorno. La tecnologia che controlla la mente*, Springer Verlag, Milano 2011, dove un intero capitolo è dedicato alla visione remota citando alcune sperimentazioni come Semipalatinks. Inoltre, il film del 2009 *L’uomo che fissa le capre* di Grant Heslov rappresenta la parodia, in modo ironico, delle attività di un reparto segreto dell’esercito statunitense che si prefigge di usare attività paranormali per scopi bellici.
- 19 Marcello Trisolini ha conseguito il Master in Intelligence all’Università della Calabria nell’a.a. 2018-2019 con la votazione di 110 e lode accademica, discutendo una tesi dal titolo *“Intelligence di polizia. Le Forze di polizia come human sensors nell’attività di Intelligence”*, con relatore Marco Valentini. Una sintesi del lavoro sarà inserita nel volume in corso di pubblicazione M. Caligiuri (a cura), *Studi di intelligence 3. Avvicinarsi alla realtà*, Rubbettino, Soveria Mannelli 2021.
- 20 La capacità di “osservazione, elicitazione e sorveglianza”, viene indicata con l’acronimo OES. Il termine elicitazione dal punto di vista psicologico significa stimolare domande, porsi quesiti.

cana durante la seconda Guerra del Golfo nel 2003²¹.

Nel testo si sostiene che l'uso delle tecnologie potrebbe rivelarsi inefficace nella raccolta informativa di fronte alla trasformazione delle città che diventano una sconfinata periferia, popolata da un sottobosco composto da criminali e terroristi, disagiati sociali e lupi solitari. Un mondo "reale" difficilmente penetrabile dalle tecnologie, ma chi è preposto al controllo umano dovrebbe essere messo in condizione di individuare informazioni utili, cogliendo sfumature e identificando contesti.

Da qui allora il concetto, e la conseguente proposta, che ogni operatore delle Forze di polizia sia formato per essere un *sensore umano* sul territorio poiché gli uomini interagiscono tra loro e con l'ambiente circostante nei modi più imprevedibili e più di quanto potrà mai fare un dispositivo artificiale.

Come cornice c'è appunto l'Intelligence di polizia intesa in chiave di Sicurezza Nazionale, considerando che la trasformazione continua rende le minacce sempre meno identificabili.

In tale quadro, la figura dello *human sensor* può rappresentare un avamposto della sicurezza, una garanzia per i cittadini che hanno bisogno sempre di più di "simboli umani" ai quali fare riferimento.

Opportuno è l'approfondimento compiuto dall'autore riguardo all'esperienza israeliana, che dovendo affrontare costantemente organizzazioni combattenti non statali ha maturato una importante esperienza nell'ambito delle guerre irregolari e della lotta al terrorismo. Operando in una realtà diffici-

21 Nell'occasione della seconda guerra del Golfo si fece emergere in tutti i soldati la consapevolezza che le loro osservazioni quotidiane assumevano un ruolo essenziale nel fornire quelle "informazioni di contesto" che i sistemi più avanzati di Intelligence non erano in grado di assicurare.

le da prevenire e fronteggiare con metodi convenzionali, gli israeliani hanno implementato una raccolta informativa di contesto più ampia, coinvolgendo non solo le forze della difesa, dei corpi di polizia e dell'Intelligence, ma anche del settore privato e di tutta la popolazione, creando una collaborazione integrata di grande efficacia.

Tutto ciò evidenzia la necessità di rivedere l'attuale e prevalente formazione burocratica e giuridica delle Forze di polizia, chiamate sempre di più a prevedere che a reprimere.

Per fare questo occorre sviluppare una tendenza propria dell'Intelligence che è quella di cogliere i "segnali deboli", l'opposto di quelli che processano i Big Data.

Pertanto, alla figura dello *Human Sensor* si richiedono capacità di contestualizzare, unire i punti, partire dai fatti per interpretare e anticipare la realtà²².

In definitiva, questa figura prende atto dei mutamenti e del dibattito del ruolo della sicurezza degli ultimi 30 anni, proiettandosi verso il futuro dove è prevedibile la crescente presenza delle mafie che approfittano della prevalenza dell'economia sulla politica.

Non a caso, già a metà degli anni Novanta il direttore dello spionaggio tedesco Eckart Wertherbach sosteneva: "Con la sua colossale potenza finanziaria, la criminalità organizzata influenza segretamente tutta la nostra vita economica, l'ordine sociale, l'amministrazione pubblica e la giustizia, in alcuni casi detta la politica la sua legge, i suoi valori. Se questa evoluzione dovesse procedere, lo Stato sarebbe ben presto incapace di garantire i diritti e le libertà civiche dei cittadini"²³.

22 H. Rosling, *Factfulness. Dieci ragioni per cui non capiamo il mondo. E perchè le cose vanno meglio di come pensiamo*, Rizzoli, Milano 2018.

23 E. Wertherbach, *Organisierte Kriminalität*, in "Zeitschrift für Rechtspolitik", 1994, n. 2.

Le asimmetrie della globalizzazione favoriscono di fatto la criminalità organizzata²⁴, che è spesso avanti nell'utilizzo delle tecnologie e nei comportamenti, in quanto adotta flessibili strategie di arretramento comunicativo per essere meno identificabile: celebre è il caso dei "pizzini" utilizzati dai mafiosi per non farsi intercettare²⁵.

In questo scenario, l'Intelligence si caratterizza sempre più come il tempo del futuro, poiché è una tecnica ed un sapere che mantiene l'umanità al centro dei processi sociali, in modo da sottrarla all'irrelevanza di popoli superflui a cui sembra essere inevitabilmente destinata²⁶.

Com'è noto, il cinema, come l'arte, anticipa spesso quello che verrà. E ritengo che in questa categoria possa essere considerato il film di James Bond del 2012 *Skyfall*, dove "M", la responsabile del Secret Intelligence Service di Sua Maestà, così si esprime davanti a una Commissione parlamentare: "lo vedo un mondo diverso dal vostro. E la verità è che quello che vedo mi spaventa molto. Sono spaventata perché non sappiamo più chi sono i nostri nemici. Non sono più rintracciabili, non sono nazioni. Sono individui. Il nostro mondo

24 M. Naim, *Illecito. Come trafficanti, falsari e contrabbandieri stanno controllando l'economia mondiale*, Mondadori, Milano 2006.

25 "Nel gergo della mafia, ciascuno dei foglietti scambiati tra i boss e i loro affiliati (per evitare di essere intercettati, telefonicamente o telematicamente), attraverso una fitta rete di intermediari, per dare informazioni o impartire direttive, adottando per motivi di sicurezza un linguaggio cifrato, comunque criptico". Vocabolario Treccani, <https://www.treccani.it/vocabolario/pizzino/>. Vedi C. FAVERZANI, D. Lanfranca (a cura), *La storia, le storie. Camilleri, la mafia e la questione siciliana*, Quaderni Camilleriani 2. Oltre il poliziesco: letteratura/multilinguismo/traduzioni nell'area mediterranea, Grafiche Ghiani, Monastir 2016.

26 "Quando gli algoritmi avranno estromessi gli umani dal mercato del lavoro, la ricchezza e il potere potrebbero risultare concentrati nelle mani di una minuscola élite che possiede i potentissimi algoritmi, creando le condizioni per una disuguaglianza sociale e politica senza precedenti". Y.N. Harari, *Homo Deus. Breve storia del futuro*, Bompiani, Milano 2017, p. 490.

non è più trasparente, ora. È più opaco. È nelle ombre. È lì che dobbiamo combattere”.

Ed è proprio questa l'idea del saggio di Marcello Trisolini, che ha un alto valore civile perché crede nel ruolo dello Stato e identifica nella dimensione umana quella più praticabile per difendere la sicurezza.

Soveria Mannelli, 9.11.2020

Mario Caligiuri

FONTI

Bibliografia

- Azzolini G., *Dopo le classi dirigenti. La metamorfosi delle oligarchie nell'età globale*, Laterza, Roma- Bari 2017.
- Bauman Z., Lyon D., *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari 2014.
- Beck U., *La società del rischio*, Carocci, Roma 2000.
- Buchanan L., *Il settimo senso. I segreti delle spie psichiche dell'esercito americano*, Edizioni Il Punto di Incontro, Vicenza 2010.
- Caligiuri M., *Intelligence e guerre dell'informazione nel XXI secolo: come respingere più efficacemente le minacce cyber*, in U. GORI (a cura), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Angeli, Milano 2019.
- Caligiuri M., *Potere e sicurezza nelle smart cities*, in "Limes", 5, maggio 2019.
- Caligiuri M. (a cura), *Post Covid-19, Analisi di Intelligence e proposte di policy 2020-2021(2020)*, allegato a "Formiche", n. 5, maggio 2020.
- Caligiuri M. (a cura), *Studi di intelligence 3. Avvicinarsi alla realtà*, Rubbettino, Soveria Mannelli 2021 (in corso di pubblicazione)
- Dick P.K., *Rapporto di minoranza e altri racconti*, Fanucci, Roma 2002.
- Faverzani C., Lanfranca D. (a cura), *La storia, le storie. Camilleri, la mafia e la questione siciliana*, Quaderni Camilleriani 2. Oltre il poliziesco: letteratura/multilinguismo/traduzioni nell'area mediterranea, Grafiche Ghiani, Monastir 2016.
- Gagliano G., *Guerra psicologica. Saggio sulle moderne tecniche militari cognitive e di disinformazione*, Fuoco, Roma 2013.
- Galli G., *Il golpe invisibile. Come la borghesia finanziario-speculativa e i ceti burocratico-parassitari hanno saccheggiato l'Italia repubblicana fino a vanificare lo stato di diritto*, Kaos, Milano 2015.
- Gori U., Germani L.S. (a cura), *INFORMATION WARFARE 2011, La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Angeli, Milano 2012.

- Harari Y.N., *Homo Deus. Breve storia del futuro*, Bompiani, Milano 2017.
- Lawrence W., *Le altissime torri. Come al-Qaeda giunse all'11 settembre*, Adelphi, Milano 2007.
- Lissoni A., *Psicospie. Viaggio negli archivi segreti del paranormale in America, Russia e Medioriente*, Editoriale Olimpia, Sesto Fiorentino 2003.
- Lombardo E., *Sicurezza 4 P. Lo studio alla base del software XLAW per prevedere e prevenire crimini*, Mazzanti, Venezia 2019.
- Naim M., *Illecito. Come trafficanti, falsari e contrabbandieri stanno controllando l'economia mondiale*, Mondadori, Milano 2006.
- Ostrander S., Schroeder L., *Scoperte psichiche dietro la cortina di ferro. URSS/BULGARIA/CECOSLOVACCHIA*, MEB, Torino 1975.
- Rosling H., *Factfulness. Dieci ragioni per cui non capiamo il mondo. E perchè le cose vanno meglio di come pensiamo*, Rizzoli, Milano 2018.
- Teti A., *PsychoTech. Il punto di non ritorno. La tecnologia che controlla la mente*, Springer Verlag, Milano 2011.
- Wertherbach E., *Organisierte Kriminalität*, in "Zeitschrift für Rechtspolitik", 1994, n. 2.
- Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, Roma 2019.

Sitografia

<http://foreignpolicy.com>.
<https://formiche.net>.
<https://www.agi.it>.
<https://www.nonsprecare.it>.
<https://www.repubblica.it>.
<https://www.treccani.it>.

Filmografia

L'uomo che fissa le capre, di Grant Heslov (2009).
Minority Report, di Steven Spielberg (2002).

INTELLIGENCE DI POLIZIA
LE FORZE DELL'ORDINE COME HUMAN SENSORS

NOTE INTRODUTTIVE

Negli ultimi trent'anni, a partire dalla fine del secolo *breve*, il mondo reale sembra voler divenire un mondo surrogato, dove non esistono più confini, né materia, né tempo, e dove tutti sono interconnessi e interdipendenti.

Un mondo che assume sempre più la connotazione di un "super cervello" dotato di una "propria intelligenza", ma del quale nessuno sa ancora dire a chi davvero appartenga o apparterrà in futuro, e dove ciascun individuo ad esso collegato per mezzo di un pc, di uno *smartphone* o di un altro *device*, altro non è che un semplice "elemento neuronale", necessario per ramificare e potenziare la sua stessa struttura¹.

Secondo recenti indagini², infatti, gli individui connessi alla rete nel mondo sono circa 4,4 miliardi e tale numero è in continuo aumento: ciò vuol dire che più della metà della popolazione mondiale è connessa a internet. L'altra faccia del pianeta, invece, quella che non accede al mondo digitale, ne resta esclusa principalmente per due motivi: a causa delle limitazioni imposte da alcuni Paesi alla libertà dei propri cittadini e a causa di limitazioni economiche che tagliano fuori i Paesi più poveri.

1 Basti pensare all'intelligenza artificiale (AI), all' internet delle cose (IOT – Internet of things), alla realtà aumentata (AR) e alla realtà virtuale (VR), alle *smart city*, alle tecnologie informatiche e della comunicazione (TIC).

2 ITU (International Telecommunication Union), *Report on the implementation of the Strategic Plan and the activities of the Union for 2018-2019 (ITU Annual Progress Report)*, ITU/Concil, Document C19/35-E, Geneva, 18 April 2019. Cfr. pure il «Rapporto sulle statistiche digitali globali Q3» pubblicato da *Hootsuite* e da *We Are Social*, 2019.

È spesso accaduto nella storia dell'uomo che l'introduzione di una nuova tecnologia abbia portato un cambiamento più o meno significativo nella vita delle persone, ma nessuna come l'avvento di internet è stata capace di mutare così profondamente, rapidamente e in maniera totalizzante il modo di vivere di gran parte della popolazione mondiale, tanto da potersi prospettare un mutamento antropologico della stessa società.

Oggi, come è stato saggiamente osservato, «stiamo vivendo non tanto un'epoca di cambiamenti, quanto un cambio di epoca»³; un mutamento come furono la scoperta dell'America o la Rivoluzione francese, giusto per citarne qualcuno. Gli effetti sugli individui, sulla società e sulle democrazie di questo nuovo mondo che si apre dinanzi a noi non sono ancora determinabili, sebbene i prodromi non lascino sperare nulla di buono.

Autorevoli studiosi ritenevano fino a qualche decennio fa che la televisione, uno strumento domestico, fosse uno dei maggiori pericoli per la società: un oggetto capace di influenzare i comportamenti e le opinioni delle persone, sin dalla tenera età⁴. Oggi la questione sembra non si ponga nemmeno. L'avvento di internet ha completamente stravolto le concezioni sociali, economiche e politiche finora elaborate. Se la televisione aveva bisogno di un luogo fisico per determinare il suo potere sull'individuo, lo *smartphone* ha bisogno semplicemente di divenire "protesi" di quest'ultimo. Oggi, ovunque ci si

3 Giansoldati Franca, *Papa Francesco: Il comunismo ci ha rubato la bandiera*, in «Il Messaggero», 29 giugno 2014.

4 Popper R. Karl, *Cattiva maestra televisione*, Marsilio Editori, Venezia, 2006. Cfr. pure Sartori Giovanni, *Homo videns*, Editori Laterza, Bari, 2007.

volti, è possibile vedere persone che non interagiscono con l'ambiente circostante perché chinate a fissare piccoli schermi luminosi. Un mondo, questo, a cui tutto e tutti sono profondamente e costantemente rivolti.

Ora, come spesso accade, quando tutti guardano da una parte non ci si accorge di cosa sta succedendo dall'altra. A questo riguardo ci sono molti studi ed esperimenti di psicologia sociale in grado di fornirci utili strumenti per comprenderne i diversi aspetti di questa questione. Contrariamente a quanto si crede, non siamo affatto osservatori. Non prestiamo attenzione, infatti, alla maggior parte di ciò che ci circonda proprio perché siamo troppo concentrati su ciò che attira la nostra attenzione in un determinato momento⁵. Tuttavia, per meglio introdurre questo aspetto, in una dimensione che possa chiarire l'idea di fondo che sarà alla base di questo studio, ci si riferirà alla finzione cinematografica.

Nel 2011 in Gran Bretagna andava in onda per la prima volta la serie televisiva intitolata *Black Mirror*, destinata a suscitare grande clamore. Il suo ideatore, Charlie Brooker, immagina un mondo ambientato nel futuro, ma in realtà ispirato al mondo di oggi, con lo scopo di mostrare come la tecnologia, i mass media ed i *social network* stiano cambiando le nostre vite, le stiano travolgendo e lentamente divorando. Nel primo episodio (*The National Anthem*), l'autore pone una questione importante riguardo ai limiti e ai pericoli dei mezzi di

5 Chabris Christopher, Simons Daniel, *Il gorilla invisibile. E altri modi in cui le nostre intenzioni ci ingannano*, Gruppo 24 ore, Milano, 2012. E' utile anche menzionare alcuni errori cognitivi, come: l'*effetto ancoraggio* (la tendenza a decidere affidandosi in modo eccessivo alla prima informazione di cui si dispone); l'*effetto gregge* (il fenomeno per cui le persone compiono alcuni atti o credono in alcune cose solo perché lo fa la maggioranza della gente).

comunicazione con i quali siamo interconnessi ogni giorno, che ci spingono a dimenticare o a non farci accorgere di ciò che davvero accade nel mondo reale: questo sarà il focus del presente studio, proiettato nell'ambito della Sicurezza Nazionale e della lotta alla criminalità organizzata.

Il film comincia con una telefonata ricevuta dal Primo Ministro inglese in piena notte che lo informa del rapimento della principessa, amatissima dal suo popolo. La richiesta del riscatto è sconvolgente: la principessa verrà uccisa se il Primo Ministro non avrà entro le ore seguenti un rapporto sessuale completo con un maiale in diretta televisiva e su tutti i network terrestri e satellitari. La scelta è durissima: perdere la propria dignità come uomo e come politico in diretta mondiale o perderla comunque agli occhi del mondo lasciando la principessa al suo destino? Per l'uomo è l'inizio di un incubo che metterà a durissima prova la sua morale e quella di tutto un popolo. Il tempo è scaduto e la decisione è presa. E mentre tutti sono rivolti e concentrati ad assistere ad un avvenimento così straordinario quanto disturbante, la principessa è già stata liberata dallo stesso carceriere nelle strade deserte della città senza che nessuno possa soccorrerla o impedire l'immondo gesto, perché tutti sono rivolti a guardare l'avvenimento in TV.

Un simile scenario è certamente possibile, sebbene riguardi la *fiction* televisiva, anche se alquanto improbabile. Naturalmente di eventi che potrebbero essere possibili ce ne sono davvero molti. Occorre sempre chiedersi se ciò che è possibile sia pure probabile: un esercizio, questo, utile per evitare di analizzare e fare previsioni su contesti fantasiosi, *hollywoodiani*. Eppure, l'11 settembre del 2001, quattro aerei di linea con civili a bordo furono dirottati da alcuni terroristi arabi

e utilizzati come fossero missili per colpire obiettivi militari e civili. Neanche la finzione cinematografica si era mai spinta sino ad allora a immaginare un simile evento. Le trasmissioni televisive, l'informazione giornalistica, gli apparati degli Stati e la stragrande maggioranza della popolazione mondiale era rivolta a guardare quegli incredibili eventi. In quelle ore e nei giorni seguenti tutti guardavano verso una sola direzione.

Oggi qualunque evento, drammatico o meno che sia, viene ripreso dagli *smartphone* di decine e centinaia di testimoni, inquadrato da qualsiasi prospettiva possibile e visualizzato in tempo reale in tutto il mondo come mai poteva accadere nel 2001.

Occorre, quindi, porsi delle domande ed interrogarsi se il volgere lo sguardo esclusivamente in una direzione, ovvero al controllo e all'uso del *cyberspace* come campo delle azioni umane, non possa lasciare mano libera a organizzazioni terroristiche o criminali nel predisporre attività pericolose ai danni di una nazione o di una popolazione fuori dalla rete internet, o permettere a individui isolati di potersi muovere liberamente fuori dal mondo *cyber* proprio per sottrarsi ai possibili controlli (vedi il sistema economico degli *hawala*⁶ utilizzato per finanziare il traffico di clandestini e le attività terroristiche).

Naturalmente nessuno mette in dubbio l'importanza e la necessità di dirigere le principali risorse e intelligenze al presidio e al controllo dello spazio cibernetico, visti i suoi numerosi riflessi in ambito economico, sociale, politico e militare; ma non di meno occorre riflettere su quali fronti restano

6 Vedi, Atti Parlamentari, *Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere*, Stabilimenti tipografici Carlo Colombo, XVII legislatura, Doc. XXIII - N. 30, 14 dicembre 2017.

sguarniti e poco difesi.

Se quindi l'idea che tutto possa essere previsto e scongiurato non è praticabile, e se la maggior parte delle risorse e delle sinergie deve essere necessariamente rivolta al mondo *cyber*, come e dove trovare nuove risorse da destinare all'acquisizione di informazioni e al controllo di ciò che si determina nel mondo reale?

La risposta potrebbe venire da un diverso approccio delle Forze di polizia alla concezione del proprio ruolo sul territorio, una ipotesi che trova conferme anche nella statistica.

Nel 2004 il giornalista statunitense Michael Monroe Lewis racconta nel libro *Moneyball: The Art of Winning an Unfair Game* la storica impresa della squadra di baseball degli Oakland Athletics che, durante la stagione 2002, vinse venti partite consecutive stabilendo un nuovo record con un budget limitato e una nuova forma di calcolo statistico per decidere quali atleti acquistare. Il *general manager* Billy Beane, dopo aver perso i suoi giocatori migliori, si vide negare dalla società un aumento del budget per poter competere con le squadre più ricche. E allora, come poter ottenere grandi risultati con piccole spese? La risposta gli fu data da Peter Brand, un giovane laureato in economia a Yale con idee radicali sul come valutare un giocatore. Assunto come assistente, Brand convinse il manager a selezionare i giocatori basandosi quasi esclusivamente sulla percentuale che indica il numero delle volte in cui il giocatore conquista una base senza aiuto di penalità, riuscendo in questo modo a creare una squadra competitiva con un potenziale maggiore di quanto avrebbero potuto fare utilizzando metodi di selezione tradizionali e con scarse disponibilità economiche.

L'Italia è il terzo Stato, dopo Russia e Turchia, con il maggior numero Forze di polizia in relazione alla popolazione (467,2 agenti in servizio ogni 100mila abitanti, dati Eurostat 2015), e resta l'unico paese al mondo ad avere quattro forze dell'ordine a carattere nazionale (la Polizia, i Carabinieri, la Guardia di Finanza e la Polizia Penitenziaria) a cui vanno sommati i Vigili del Fuoco e le Capitanerie di Porto. Ogni corpo ha naturalmente i suoi comandi, i suoi centri operativi, le sue caserme, i suoi generali che difendono i propri status. Per di più, oltre all'enorme spesa che questo comporta, alla sovrapposizione di materie e di competenze, bisogna valutare anche la mancanza di un sistema fondato sulla centralizzazione dell'analisi dei dati raccolti da tutte le forze armate e di polizia (fatta eccezione del C.A.S.A.)⁷. Mettendo da parte questo aspetto, che resta comunque centrale per qualunque attività di Intelligence si voglia svolgere, è possibile utilizzare questa numerosa Forza di polizia già disponibile e distribuita sul territorio come un "sensore del territorio", per monitorare, rilevare, acquisire informazioni utili alla Sicurezza Nazionale e al contrasto alla criminalità organizzata?

Non si tratta naturalmente di ribadire le prerogative, gli obblighi, i doveri e il *modus operandi* a cui fanno già riferimento gli appartenenti alle Forze di polizia, attività distinta e diversa da quelle dell'Intelligence istituzionale, ma di dotare le prime, per mezzo di una formazione *ad hoc*, di quella capacità di osservazione, elicitazione e sorveglianza del territorio e della

7 Il Comitato di analisi strategica antiterrorismo (C.A.S.A.) è un organismo del Ministero dell'Interno composto dai rappresentanti delle diverse Forze di polizia italiane e dei Servizi con il compito di favorire e condividere le informazioni relative alle minacce terroristiche interne ed esterne alla Repubblica. Il C.A.S.A. è stato istituito con d.m. del 6 maggio 2004 all'indomani dell'attentato al contingente italiano di istanza a Nassiriya.

gente, che spesso non tutti gli operatori di polizia posseggono. Più della metà degli appartenenti alle Forze di polizia, infatti, si occupa prevalentemente di attività burocratiche, mentre solo una piccola percentuale svolge regolarmente un lavoro investigativo e di controllo del territorio, attività queste utili a poter leggere l'ambiente circostante in modo diverso.

Se si implementasse, quindi, la formazione degli appartenenti alle Forze di polizia con un addestramento rivolto a migliorare quegli aspetti sopra accennati (osservazione, elicitazione e sorveglianza), si disporrebbe di una enorme quantità di “human sensor” sul territorio, non solo attivi durante le ore lavorative, ma soprattutto quando gli operatori sono fuori servizio. Facendo affidamento, quindi, all'elevato numero degli appartenenti alle forze dell'ordine, alla loro diffusione su tutto il territorio e all'essere già uomini e donne addestrati militarmente (addestramento basico), si potrebbe ipotizzare con buona ragione che statisticamente gli *Human Sensors* potrebbero aumentare di gran lunga le *chance* degli apparati di Intelligence o *Intelligence-led policing*⁸ di acquisire informazioni utili riguardanti attività terroristiche e di criminalità organizzata sul territorio nazionale.

8 Intelligence-led policy: polizia diretta dai metodi di Intelligence o polizia dell'informazione. E' un modello di polizia che inquadra tutte le principali attività di polizia (dal contrasto della criminalità organizzata, del terrorismo, dei traffici di droga, dell'immigrazione, al controllo del territorio) in modo più efficiente (in termini di ottimizzazione delle risorse impiegate) e più efficace (in termine di risultati) grazie ad una adeguata analisi preventiva dei fenomeni criminali. Un approccio, quindi, che postula una stretta integrazione tra attività di Intelligence e attività di polizia in cui l'analisi dei dati è fondamentale per un quadro decisionale. Cfr. Ratcliffe Jerry H., *Intelligence-Led Policing*, Willan Publishing, Cullompton – UK, 2008, p. 6 e seguenti.

Due sono le realtà che hanno sperimentato e intrapreso una simile direzione: il 4° battaglione del 27° reggimento di artiglieria da campo USA (rischierato a Baghdad nel 2003); l'esercito israeliano – Israel Defense Forces, (IDF) nel quale la popolazione partecipa attivamente alla difesa della nazione.

Lo studio e lo sviluppo delle ipotesi considerate saranno analizzati e confrontati, infine, con gli aspetti pratici derivanti dall'attività investigativa e operativa di polizia, emersi dalla somministrazione di alcuni quesiti sottoposti agli stessi operatori.

CAPITOLO 1
COS'È LO HUMAN SENSOR

1.1

DALLA GUERRA SIMMETRICA ALLA GUERRA ASIMMETRICA

Sino alla Guerra del Golfo, la natura dei conflitti tra i diversi antagonisti sullo scacchiere mondiale era *simmetrico* ovvero di tipo tradizionale: due o più soggetti contrapposti e ben riconoscibili che si contendevano risorse, territori o vantaggi commerciali con la minaccia o con l'uso della forza. L'equilibrio tra le forze in campo o la vittoria dell'uno o dell'altro fronte dipendeva dalla superiorità in campo economico, scientifico e tecnologico.

Successivamente, la guerra diventa *asimmetrica*, ossia, una contrapposizione di forze in campo enormemente sbilanciate: dove una parte, più debole, obbedisce a regole proprie, usa metodi non convenzionali ed è irriconoscibile o incomprendibile agli occhi dell'avversario; mentre l'altra, pur essendo tecnologicamente, militarmente ed economicamente più forte dell'antagonista, ne subisce i pesanti attacchi nei punti più critici e delicati dei suoi centri di gravità¹.

Negli anni della Guerra Fredda, ad esempio, la logica della deterrenza nucleare ha garantito una certa stabilità e prevedibilità del sistema politico-militare mondiale. Un sistema nel quale tutti gli attori principali si muovevano in un quadro

1 Cfr. Mini Fabio (a cura di), Qiao Liang, Wang Xiangsui, *Guerra senza limiti – L'arte della guerra asimmetrica tra terrorismo e globalizzazione*, LEG Edizioni, Gorizia, 2002, p. 184.

di coordinate certe e ben definite: gli schieramenti ben conosciuti, le aree di influenza definite e gli interessi geopolitici determinati. Dalla caduta del muro di Berlino in poi, il sistema sembra invece scivolare in un mondo sempre più incerto e caotico². Accanto allo Stato westfaliano, emergono prepotentemente tutta una serie di altri attori internazionali che, al pari del primo, hanno la capacità di incidere sulle dinamiche politiche. Si è passati così dai conflitti tradizionali tra uno Stato e un altro, ai conflitti che hanno da un lato lo Stato o gli Stati, dall'altro un pulviscolo di soggetti non riconoscibili che, pur essendo strutturalmente più deboli dei primi, si dimostrano essere molto più pericolosi.

La natura dei conflitti contemporanei, quindi, si caratterizza proprio per l'imprevedibilità e l'inconoscibilità del nemico, rese possibili da due nuovi scenari che hanno stravolto completamente i precedenti rapporti di forza: il primo, il delinearci della guerra asimmetrica³; il secondo, gli attacchi ai sistemi informatici e di comunicazione.

I due nuovi aspetti, hanno di fatto prodotto un sistema internazionale a *geometria variabile* dove, accanto a quei soggetti per i quali valgono ancora le regole della politica internazionale, si è affermata una grande periferia, o più periferie, dove i rapporti tra i soggetti sono improntati a regole proprie.

-
- 2 L'ultimo decennio del ventesimo secolo si è caratterizzato, come mai prima di allora, da profondi rivolgimenti avvenuti nel mondo. Delle numerose cause poste alla base di queste trasformazioni una sembra imporsi su tutte: la Guerra del Golfo. *Ibidem*.
 - 3 Il concetto di guerra asimmetrica, ha avuto nel volgere degli anni un mutamento di significato. Dapprima, infatti, è stato utilizzato dagli Stati Uniti per indicare l'enorme divario tecnologico esistente fra le forze americane e gli avversari con cui esse dovevano confrontarsi (Cfr. Jean Carlo, *Manuale di studi strategici*, CSGE, Franco Angeli, Milano, 2017, pp. 250-252.

Durante gli anni della Guerra Fredda, quindi, le attività belliche erano progettate per affrontare un nemico in modo simmetrico e la forza veniva impiegata utilizzando metodi convenzionali. In questo contesto l'esercito dipendeva dalla tecnologia esclusivamente per poter guardare dietro le linee nemiche e distruggere obiettivi strategici. Nella guerra asimmetrica nulla di tutto questo è possibile. Il nemico può essere ovunque, non è identificabile e affronta il conflitto con atti di guerriglia o terroristici, colpendo i centri di gravità dell'avversario in modo da creare grande impressione e spavento sia nelle forze regolari che nell'opinione pubblica. Come risultato di questa nuova minaccia⁴, gli Stati hanno dovuto cambiare strategia e impiegare l'esercito e gli apparati di Intelligence per identificare e distruggere obiettivi sensibili utilizzando la propria capacità tecnologica e per raccogliere informazioni su qualsiasi avversario e in tutto il mondo.

Tuttavia, sebbene a livello strategico l'aumento costante della raccolta delle informazioni abbia fornito un vantaggio significativo nelle diverse fasi dei conflitti, sul piano tattico non è stato sufficiente a determinare un completo dominio delle informazioni. L'unico modo per sopperire a questa esigenza, almeno nei teatri di guerra, è stato un diverso impiego delle forze militari sul campo.

4 L'espressione Guerra globale al terrorismo (*Global War on Terrorism* - G.W.O.T.) venne utilizzato dai mass media e dal governo americano per riferirsi ad una serie di operazioni militari intraprese dopo l'11 settembre 2001. Cfr. Eric Schmitt, Thom Shanker, *Bombings in London: Hearts and Minds - U.S. Officials Retool Slogan for Terror War*, in «The New York Time». 26, July, 2005, p. 7

1.2

L'ANTITERRORISMO E LA GUERRA ASIMMETRICA: L'ESPERIENZA ISRAELIANA

Israele, più di qualsiasi altro Stato, si è trovato sin dalla sua nascita ad operare in uno scenario strategico fortemente asimmetrico, dovendo affrontare regolarmente organizzazioni combattenti non statuali come l'OLP, Hamas e Fatah¹.

L'apparato militare israeliano ha maturato a sue spese un'enorme esperienza nell'ambito delle guerre irregolari e della lotta al terrorismo, anche se i risultati, come si può ben comprendere, non sono stati sempre positivi.

In particolare negli ultimi anni, l>IDF (*Israel Defense Forces*) ha incontrato notevoli difficoltà nel rispondere alle minacce a causa dell'aumento della componente asimmetrica dei conflitti. Le tradizionali efficienza ed efficacia delle forze armate israeliane sono state messe in discussione proprio dall'elemento asimmetrico esaltato dall'avversario - le organizzazioni palestinesi o libanesi, la parte debole in questione - in ragione dei maggiori vantaggi che questo poteva portare sul campo.

Sebbene l'approccio israeliano all'antiterrorismo - il *Counter-Terrorism* (CT) - resti il sistema più avanzato ed efficace che si conosca, proprio perché il terrorismo è una realtà da

1 OLP (Organizzazione per la Liberazione della Palestina); Hamas (Movimento Islamico di Resistenza); Fatah (o *al-fatah*, è un'organizzazione politica e paramilitare palestinese).

sempre presente nella vita del paese, non esiste una dottrina ufficiale entro cui poterlo racchiudere ed il motivo sta nella natura stessa della minaccia (il terrorismo è sempre diverso ed imprevedibile) che ne impedisce di fatto una codificazione. Israele ha così adottato un approccio più organico e olistico al CT che fa leva sull'innovazione e sulla creatività al fine di scoraggiare e creare divisioni all'interno dei gruppi terroristici e dei loro sostenitori attraverso la coercizione e la persuasione².

Tuttavia, per far fronte alle continue minacce alla sicurezza dello Stato e dei cittadini, l'architettura dell'antiterrorismo israeliano poggia in modo variegato sul coinvolgimento di tutta la nazione: le forze di difesa israeliane (l'IDF); le unità specializzate degli apparati di sicurezza; la polizia; il settore privato; l'intera società.

A questo riguardo occorre tener ben presente che tutta la popolazione israeliana partecipa alla difesa dello Stato non solo prestando servizio di leva obbligatoria per diversi anni³, ma restando nella disponibilità dell'esercito come riservisti fino a età matura. Inoltre vi è l'obbligo, anche se in congedo, di prestare servizio nell'esercito per un mese all'anno.

Questo fa sì che tutta la popolazione israeliana partecipi costantemente alla sicurezza dello Stato, non solo quando tornano a indossare la divisa militare, ma anche quando tornano alla vita civile, mentre ad esempio passeggiano per

2 Isaac Kfir, *Israel's Approach to Counterterrorism*, in « The Strategist (ASPI - The Australian Strategic Policy Institute)», 27 settembre, 2018.

3 Il servizio di leva è obbligatorio sia per le donne (24 mesi) che per gli uomini (36 mesi). Ogni recluta viene sottoposta ad un addestramento basico (*Tironut* - termine ebraico con il quale si definisce l'addestramento delle reclute nelle forze di difesa israeliane, suddiviso in livelli) della durata di 6 mesi. Una volta concluso il servizio militare, restano a disposizione dell'esercito come riservisti (gli uomini fino ai 50 anni le donne fino a 46 anni).

Gerusalemme o in qualsiasi altra città del Paese.

La loro formazione militare e il contesto in cui vivono li predispone naturalmente a osservare e rilevare tutto quello che accade intorno proprio come fossero tanti *sensori* sul territorio.

1.3

HUMAN SENSOR E IL 4° BATTAGLIONE

Il 5 novembre 2003 apparve su un importante quotidiano americano un'intervista a un alto ufficiale dell'esercito statunitense¹ che sottolineava l'importanza di adottare una nuova strategia militare nel conflitto iracheno, fondamentale per far fronte alle crescenti difficoltà derivanti dal combattere una guerra asimmetrica. Era necessario allargare "l'attività informativa" a tutti i soldati:

ognuno è un agente dell'Intelligence, questo è il nostro tema. Se si parla di un mutamento di paradigma, eccolo qua: vedere tutte le persone con cui si entra in contatto come una risorsa per l'Intelligence².

Il 1° maggio 2003, pochi mesi dopo l'avvio della seconda Guerra del Golfo³, il presidente degli Stati Uniti si affrettava a proclamare la superiorità militare americana e la conclusione

1 Vernon Loeb, *Instead of Force, Friendly Persuasion*, in «The Washington Post», 5 Novembre 2003, p. 24.

2 Cfr. Michael S. Patton (Maggiore del 4° Battaglione del 27° Reggimento di Artiglieria da Campo), *ES2: Every Soldier is a Sensor*, in «Association of the United States Army, voice for army – support for the soldier», agosto 2004.

3 La seconda Guerra del Golfo denominata *Iraqi Freedom* (marzo 2003 – dicembre 2011) è stato un conflitto bellico intrapreso in un più ampio progetto di "lotta al terrorismo" condotta dagli americani e da una coalizione di altri Stati (schieramento composto da 49 paesi ribattezzata "la coalizione dei volenterosi", 15 dei quali avrebbero chiesto l'anonimato) contro l'Iraq di Saddam Hussein, reo di voler utilizzare armi di distruzione di massa (una informazione poi rivelatasi infondata) e di dare presunti appoggi al terrorismo islamista.

delle operazioni militari in Iraq⁴, aggiungendo: «lasciemo un Iraq libero e democratico e ricostruito»⁵. Di lì a poco il conflitto si tramutò in una guerra di liberazione dall'esercito statunitense, considerato invasore da molti gruppi armati arabi sunniti e sciiti, per sfociare infine in una guerra civile fra le varie fazioni, causata da una squilibrata gestione del potere che agevolava la componente maggioritaria sciita.

L'esercito americano si trovava così a dover contrastare una guerra non convenzionale combattuta fuori dai tradizionali campi di battaglia. La guerra tecnologica occidentale, basata sull'utilizzo della forza aerea, ma soprattutto sull'uso dei droni, era stata decisiva nel mutamento del conflitto. Non potendo affrontare in campo aperto l'antagonista, vista l'assoluta disparità di forze, la parte più debole ha cambiato le proprie strategie e tattiche di guerra, rispondendo alla superiorità economica e tecnologica dell'avversario con tecniche di guerriglia e terroristiche⁶.

Tutta la capacità informativa e tecnologica di cui disponeva l'esercito americano non era in grado di prevenire o evitare gli attacchi di un nemico imprevedibile e "invisibile", e del quale non si conosceva nulla.

4 Atterro sulla portaerei *Lincoln*, il presidente degli Stati Uniti George Bush dichiarò, in diretta televisiva, la fine della guerra in Iraq (alle spalle uno striscione diceva: *Mission Accomplished* - "Missione Compiuta").

5 Cfr. Redazione, *Bush: finiti i combattimenti in Iraq*, in «Corriere della Sera», 2 maggio, 2003.

6 «La parte più debole combatte piuttosto il suo avversario utilizzando la guerriglia (principalmente urbana), la guerra terroristica, la guerra santa, la guerra prolungata, la guerra in rete ed altre forme di combattimento. Nella maggior parte dei casi, la parte debole sceglie come asse principale della battaglia quelle linee operative ove il suo avversario non si aspetta di essere colpito ed il centro di gravità dell'assalto è sempre un punto che provocherà un profondo shock psicologico nell'avversario». Vedi in, Qiao Liang, Wang Xiangsui, *Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione*, op. cit., p. 47.

Per far fronte a questo nuovo scenario, occorreva addestrare, integrare e massimizzare la risorsa più efficace a disposizione, necessaria per rilevare e riportare informazioni direttamente dal campo di battaglia e utili soprattutto a livello tattico: il Soldato.

I primi tentativi furono sperimentati dal 4° Battaglione del 27° Reggimento di Artiglieria da Campo degli Stati Uniti d'America così come descritto nell'intervista giornalistica sul *Washington Post*:

la pattuglia del tenente Chris Kane attraversò Haifa Street e si diresse velocemente verso i vicoli posteriori di Sheik Maruf dopo aver sentito esplodere la prima granata. Un altro gruppo di soldati americani era sotto attacco in un labirinto intasato da liquami.

Presto, non appena imboccarono un vicolo buio cercando un giovane uomo con una maglia nera che aveva lanciato una bomba a mano artigianale, ne esplose un'altra con un rumore assordante, seguito da uno scoppio separato di un colpo di fucile improvviso. Nel caos che seguì, un altro soldato gridò di aver visto qualcuno fare fuoco dal tetto di una casa. I suoi compagni irrupero all'interno e trovarono cinque uomini. Ordinarono agli iracheni di uscire. Le loro mogli terrorizzate e i bambini in lacrime li seguirono. Nessuno degli uomini indossava abiti di colore nero. Nessun bossolo venne ritrovato sul tetto.

Kane, 24 anni, un ufficiale biondo, alto e occhialuto, della contea di Fairfax, a due anni da West Point, si avvicinò ad un uomo anziano del gruppo e, tramite il suo interprete iracheno, disse: "Digli che ci serve il suo aiuto". L'interprete prese in disparte l'uomo anziano, che indossava un *dishdasha* bianco, un abito tradizionale, e che

tremava visibilmente. I due parlano a lungo.

In un primo momento l'uomo disse di non sapere nulla, ma dopo un po' di sollecitazioni e tentativi di persuaderlo da parte di Kane, l'uomo cedette. "Ho bisogno di tempo per riposarmi" disse, "dopo ti darò tutti i loro nomi."

Questo è il genere di guerra che gli "Old Ironsides", la 1° Divisione Corazzata dell'Esercito Americano, stanno combattendo a Baghdad non a colpi di carro armato e di artiglieria, ma attraverso persuasione e coltivata fiducia che sono munizioni di gran lunga più forti in una battaglia contro una promettente resistenza irachena.

"Il modo per vincere questa guerra è attraverso operazioni basate sull'Intelligence" disse il tenente colonnello Brian J. McKiernan, che dirige il 4° battaglione, 27° reggimento Artiglieria da Campo, "e in questo ambiente, tutto è guidato dall'Intelligence umana."

Con i loro veicoli corazzati fermi nei parcheggi, la 1° Divisione Armata si sta reinventando con il volo, adescando informatori di quartiere e inviando fonti pagate all'interno dei brulicanti quartieri di Baghdad, secondo lo stile della CIA, per raccogliere informazioni sui militanti islamici e sugli iracheni fedeli al presidente Saddam Hussein e al suo Partito Ba'th⁷.

Si è così compreso che il singolo soldato è il più efficace raccogliitore di informazioni, più abile e sofisticato di tutti i sistemi tecnologici a disposizione. Nei teatri di guerra asimmetrica, infatti, i soldati sono immersi in ambienti operativi estremamente dinamici e imprevedibili: nelle città, nelle campagne o ovunque si trovino, i soldati sorvegliano, osservano e parlano quotidianamente con la popolazione locale, acquisendo in

7 Vernon Loeb, *Instead of Force, Friendly Persuasion*, in «The Washington Post», 5 Novembre 2003, p. 24. traduzione It. Barletta Simona.

modo diretto informazioni molto più pertinenti al contesto nel quale operano di quelle che mai nessun sensore tecnologico sarà in grado di rilevare. Ma più importante ancora resta il fatto che gli uomini differiscono dai sistemi artificiali di raccolta informativa in quanto interagiscono tra loro e con l'ambiente circostante in modi imprevedibili e sorprendenti, più di quanto potrà mai fare un sensore artificiale.

Naturalmente per poter sfruttare appieno questa importante abilità umana è necessario che i soldati vengano addestrati a tali compiti facendo anche leva su quella naturale predisposizione all'adattamento e alla improvvisazione di cui l'uomo è capace, "trasformando così ogni combattente in un sensore sul territorio".

L'idea di fondo è semplice: ogni soldato non solo deve essere pronto al combattimento, ma in un contesto estremamente cangiante e imprevedibile deve saper servire anche da raccoglitore di informazioni. Di qui il concetto per cui "ogni soldato è un sensore" (Human Sensor)⁸.

Chiaramente, il valore di una notizia acquisita sul campo diventa significativa solo se raccolta, elaborata e integrata in un quadro operativo più ampio. Se non c'è una attività di analisi, che elabori le notizie e i dati raccolti, non c'è informazione utile a poter decidere.

⁸ FM 2-91.6, *Soldier Surveillance and Reconnaissance: fundamentals of tactical information collection*, Regular Army, Army National Guard, and Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 115979, requirements for FM 2-91.6., 10 October 2007.

1.4

FONDAMENTI DELL'ATTIVITÀ DI HUMAN SENSOR

Nel 2007 venne emesso dal quartier generale dell'esercito americano un importante manuale da campo (Field Manual n° 2-91.6)¹ che dava avvio su larga scala a una nuova dottrina a sostegno dell'iniziativa *Every Soldier is a Sensor* (ES2).

Quel famoso cambio di paradigma così tanto invocato in seguito all'esperienza del 4° battaglione qualche anno prima, divenne un programma strutturato e adottato dall'intero esercito. Un decalogo operativo che raggruppava un insieme di modus operandi per fornire a tutti i soldati gli strumenti necessari per la raccolta di informazioni durante le attività operative svolte sul campo quali ad esempio la sorveglianza, la ricognizione, il pattugliamento, l'interazione con la popolazione locale, lo sfruttamento tattico del sito².

Quindi, oltre che a corredare una sorta di vademecum su come fare attività "informativa" e a sostituire tutta una serie di precedenti manuali oramai superati sull'impiego tattico dei soldati, l'FM n°2-91.6:

-
- 1 Headquarters Department of the Army, *Field Manual No. 2-91.6 – Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*, General Dennis J. Reimer Training and Doctrine Digital Library, Washington, 2007.
 - 2 Per sfruttamento tattico del sito si intende le azioni intraprese per garantire che documenti, materiali e personale siano identificati, raccolte, protette e valutate al fine di facilitare le azioni successive.

- fornisce il quadro dottrinale per i soldati e gli ufficiali di tutti i settori e costituisce la base per i curricula ES2 all'interno del sistema di istruzione dell'esercito. È rivolto ad un vasto pubblico, che comprende sia i militari (soldati e ufficiali) e sia i civili. È essenziale che tutti i militari e i civili si rendano conto come le loro osservazioni quotidiane alimentino il più ampio processo di Intelligence e contribuiscono a creare un ambiente più favorevole per il successo degli Stati Uniti in una regione;
- è una raccolta di strumenti per aiutare tutti i soldati a raccogliere informazioni attraverso domande tattiche, gestione dei detenuti e gestione di documenti e attrezzature in operazioni offensive, difensive, di stabilità e di operazioni di supporto civile;
- non intende rendere il Soldato un esperto nella raccolta di informazioni. Non ha lo scopo di addestrare i soldati nell'attività di Intelligence né di autorizzare i soldati a condurre interrogatori e operazioni alla fonte;
- presenta le basi per porre domande e rapporti, fornendo alcuni strumenti per pattuglie e S-2;
- vale per le operazioni a largo spettro. I principi delineati sono validi in condizioni che implicano l'uso di prodotti chimici, biologici, radiologici, nucleari e ad alto potenziale esplosivo (CBRNE – *chemical, biological, radiological, nuclear, and high yield explosives*)³.

Per superare l'*impasse* dovuto ad uno scenario bellico fortemente asimmetrico, gli americani si resero conto che dove-

3 Headquarters Department of the Army, *Field Manual No. 2-91.6 – Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*, op. cit. p. iii.

vano intraprendere un altro modo di guerreggiare, che passava necessariamente da una conoscenza tattica del territorio nel quale operavano e della gente che lo abitava. Era fondamentale, cioè, implementare in tutti i soldati la consapevolezza che le loro osservazioni quotidiane giocavano un ruolo essenziale nel fornire quelle "informazioni di contesto" che i sistemi più avanzati di Intelligence non erano in grado di fornire.

Nel quadro delle attività principali alle quali i soldati devono prestare maggior attenzione ci sono innanzitutto le interazioni con la popolazione locale. Il manuale sottolinea come costruire e migliorare tali relazioni permetta di poter ottenere "informazioni di immediato valore" importanti per la comprensione dell'ambiente⁴. Anche il dotarsi di una guida, utile per l'interazione con la gente del posto e gli spostamenti sul territorio, viene fortemente raccomandato. Naturalmente ci sono restrizioni alle quali i soldati devono attenersi. Ad esempio, sebbene sia utile e necessario porre domande agli autoctoni per acquisire notizie e stabilire dei contatti, non è permesso ai soldati pagare o ricompensare le informazioni ricevute, come pure chiedere o incaricare qualcuno di cercare specifiche informazioni. Ciò equivarrebbe a intraprendere operazioni che rientrano nel campo dell'attività d'Intelligence (*source operations*)⁵, attività negate a chiunque non abbia un addestramento nella gestione della fonte.

4 A questo scopo vengono fornite a tutti i soldati sia alcune nozioni di psicologia e di comunicazione verbale e non verbale, sia elementi pratici, ad esempio, su come porre domande, quali domande fare o non fare, e così via. Cfr. Field Manual No. 2-91.6, op. cit., p. 3-1 e seguenti.

5 Headquarters Department of the Army, *Field Manual 2-22.3 (FM 34-52) Human Intelligence Collector Operation*, General Dennis J. Reimer Training and Doctrine Digital Library, Washington, 2006, pp. 1-4; 5-1; 8-7.

Malgrado l'esistenza in ciascun soldato di un diverso livello di consapevolezza e di competenze nell'attività di raccolta delle informazioni (dovuto ad una serie di variabili tra le quali l'esperienza acquisita sul campo), l'adozione di questo programma ha dimostrato senza alcun dubbio l'importanza e la centralità del ruolo ricoperto da ogni soldato come *Human Sensor* in contesti fortemente asimmetrici. Un diverso impiego dell'attività militare che ha favorito l'acquisizione di quelle notizie utili alla comprensione dell'ambiente circostante, determinando un successo informativo lì dove sistemi sofisticati e tecnologicamente avanzati avevano fallito.

I soldati, infatti, sono spesso i primi a notare cambiamenti nel proprio teatro operativo proprio perché ne hanno conoscenza. In definitiva, identificare immediatamente i possibili indicatori di pericolo significa evitare situazioni disastrose per l'incolumità dei militari e dei civili.

Sulla base dell'esperienza americana (ES2), sarebbe interessante elaborare e sperimentare un modello formativo (ed un manuale operativo) volto all'addestramento di tutte le Forze di polizia, allo scopo di implementare le capacità di "osservazione, elicitazione, e sorveglianza"⁶, utili a raccogliere informazioni d'ambiente per la protezione della Sicurezza Nazionale e il contrasto alla criminalità organizzata, verificando infine se e quanto siano state significative.

6 Vedi paragrafo 2.2

CAPITOLO 2

UNA DIVERSA VISIONE DELLE FORZE DI POLIZIA

2.1

L'INTELLIGENCE DEI SERVIZI DI INFORMAZIONE E DELLE FORZE DI POLIZIA

Quando ci si riferisce alle attività di Intelligence (ovvero ai processi di acquisizione, organizzazione e gestione delle informazioni)¹ svolte dai Servizi di Informazione e dalle Forze di polizia, occorre tenere ben presente che le finalità di questi due soggetti afferiscono ad ambiti diversi². Una distinzione questa presente in tutti i paesi con alcune sfumature che possono riguardare sia l'assetto organizzativo³ che quello funzionale.

Mentre *l'Intelligence Istituzionale* è lo strumento con cui lo Stato raccoglie, analizza, custodisce e dissemina (ai soggetti interessati) informazioni e dati utili al processo decisionale del governo in tema di Sicurezza Nazionale e Interesse Nazionale, *l'Intelligence di polizia* è l'attività con cui, le forze dell'ordine, raccolgono, analizzano e dif fondono le informazioni ai livelli superiori o all'autorità giudiziaria o di governo. Si

1 Mosca Carlo, Gambacurta Stefano, Scandone Giuseppe, Valentini Marco, *I Servizi di Informazione e il Segreto di Stato : (Legge 3 agosto 2007, n.124) - presentazione di Giovanni Conso*, Giuffrè Editore, Milano, 2008, p. 193 ss.

2 Vedi tabella 2.1 – A.

3 L'assetto organizzativo dei Servizi di Sicurezza dei vari paesi può essere *unitaria* (come in Spagna, dove c'è un unico servizio informativo con compiti di spionaggio e controspionaggio sia interno che esterno allo Stato), *binaria* (come in molti paesi NATO tra i cui l'Italia dove esiste una distinzione tra attività di Intelligence interna ed esterna) oppure *comunitaria* (un sistema suddiviso in più agenzie, come negli USA).

tratta del processo informativo declinato attraverso le tre fasi principali in funzione di una triplice direzione, in base alla natura delle informazioni elaborate o richieste (organi superiori interni, autorità giudiziaria, autorità politica)⁴.

In riferimento al nostro ordinamento, i Servizi di Intelligence sono i titolari esclusivi delle funzioni informative per la sicurezza interna ed esterna della Repubblica e dipendono dal Presidente del Consiglio. Le Forze di polizia si occupano principalmente di prevenzione e repressione dei reati e sono subordinati funzionalmente all'Autorità Giudiziaria. A tal proposito è possibile dire che mentre per le Forze di polizia l'Intelligence è una attività strumentale alla tutela della sicurezza pubblica e dell'ordine pubblico, per i Servizi di Informazione costituisce invece la sua ragion d'essere, necessaria per garantire la sicurezza nazionale dai pericoli interni ed esterni.

Tuttavia la legge di riforma dei servizi di sicurezza del 2007⁵, fermo restando la netta separazione delle funzioni dei due soggetti, si è preoccupata di stabilire una più stretta collaborazione tra Servizi di Informazione, Forze armate e Forze di polizia:

Nell'ambito delle rispettive attribuzioni, le Forze armate, le Forze di polizia, gli ufficiali e gli agenti di polizia giudiziaria e di pubblica sicurezza forniscono ogni possibile cooperazione, anche di tipo tecnico – operativo, al persona-

4 Cit. di Caligiuri Mario in: *Predictive Policing. Il futuro della sicurezza è nei modelli di prevenzione*, convegno regionale, Napoli, 24 maggio 2019.

5 Vedi, legge 3 agosto 2007, n. 124, "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto".

le addetto ai servizi di informazione per la sicurezza, per lo svolgimento dei compiti a questi affidati⁶.

È l'interscambio informativo il principale *leitmotiv* della collaborazione tra i diversi organi dello Stato, coordinato e diretto dal DIS (Dipartimento delle Informazioni per la Sicurezza), cuore pulsante di tale scambio⁷. In particolare è parso indispensabile implementare i rapporti di collaborazione tra Servizi di Informazione e le Forze di polizia nell'ambito della lotta alla mafia e al terrorismo, istituendo in entrambi i casi organi *ad hoc* con cui migliorare lo scambio informativo: il Consiglio generale per la lotta alla criminalità organizzata⁸ e il Comitato di analisi strategica antiterrorismo (C.A.S.A.).

L'Intelligence, quindi, fatte le dovute e necessarie premesse, non è una attività esclusiva dei Servizi di Informazione, ma piuttosto un metodo che trova il suo naturale utilizzo in alcuni specifici uffici delle Forze di polizia, sempre più finalizzati all'analisi dei fenomeni criminali, delle indagini e della ricerca di fonti di prova per la repressione dei reati.

6 Ivi, Art. 12 com.1.

7 IZZI S., *Intelligence e gestione delle informazioni – Attività preventiva contro i traffici illeciti*, Ed. Franco Angeli, Milano, 2011, pp. 61 – 64.

8 Art. 1, D.L. 29 ottobre 1991, n. 345, convertito dalla L. 30 dicembre 1991, n. 410.

Tabella 2.1 – A

Tavola comparativa			
SOGGETTO ISTITUZIONALE	FUNZIONE ISTITUZIONALE	DIPENDENZA FUNZIONALE	ATTIVITÀ DI INTELLIGENCE
SERVIZI DI INFORMAZIONE PER LA SICUREZZA	<i>Garantire la sicurezza esterna e interna della Repubblica contro le minacce e a protezione degli interessi nazionali</i>	<i>Presidente del Consiglio</i>	<i>Attività informativa rivolta ad ottenere ogni genere di informazione utile a garantire la protezione della Repubblica e degli interessi nazionali.</i>
FORZE DI POLIZIA ⁹	<i>Tutela della sicurezza e dell'ordine pubblico</i>	<i>Autorità Giudiziaria</i>	<i>Attività informativa rivolta alla prevenzione e repressione dei reati a tutela della sicurezza pubblica e dell'ordine pubblico.</i>

9 Occorre tener presente che nell'ambito delle funzioni e dell'attività di Intelligence delle quattro FF.pp., due hanno competenze generali (Polizia di Stato e Carabinieri) e le altre due hanno competenze specifiche e distinte (Guardia di Finanza e Polizia Penitenziaria). A queste ultime però, è anche attribuita una funzione di concorso nelle attività di ordine e di sicurezza pubblica.

2.2

L'ATTIVITÀ DI OES (OSSERVAZIONE, ELICITAZIONE E SORVEGLIANZA)

Sin dai tempi più remoti dell'organizzazione umana, l'arma più potente al soldo di re o di potenti signori per conoscere i piani, i segreti o i pensieri più reconditi di alleati e nemici in ambito militare, economico e politico, è stata certamente l'uso delle spie. Non a caso, una delle espressioni maggiormente ricorrenti nel mondo dello spionaggio definisce la spia il secondo mestiere più antico del mondo.

La necessità di apprendere e praticare “quest'arte oscura”¹, così importante per il destino d'ogni regno o per la sorte d'ogni potente², ha portato fini intelletti nel corso del tempo a

1 A seconda dei periodi storici e del paese considerato l'opinione verso le spie non varia di molto, ritenendola generalmente un figura riprovevole, ma necessaria. Nella seconda metà dell'Ottocento, ad esempio, Lord FitzRoy Somerset Reglan, generale inglese nella Guerra di Crimea dichiarò che «l'acquisizione di notizie tramite mezzi clandestini ripugna ai gentiluomini». Infatti, perse la battaglia di Balaclava nel 1854 contro i russi.

2 Sin dalla sua origine lo spionaggio si è prevalentemente collocato nella parte militare. Bisogna attendere la fine del XVI sec. per veder nascere una concezione nuova di organizzazione delle spie. L'ideatore e fondatore dell'Intelligence moderna fu il politico e diplomatico inglese Walsingham. Scrive Alain Charbonnier che «la leggenda sull'abilità spionistica degli inglesi nasce durante il regno di Elisabetta I, quando sir Francis Walsingham organizza la prima rete di spionaggio politico-militare in senso moderno. Da allora gli agenti dell'Intelligence britannica, salvo alcune parentesi non molto onorevoli, ma certo molto “ideologiche”, per usare un eufemismo (vedi il Circolo di Cambridge), si sono sempre adoperati a tutte le latitudini “in difesa del Regno”». Vedi Charbonnier Alain, *L'Intelligence Service apre gli archivi del MI5*, in «Gnosis – Rivista italiana di Intelligence», aprile 2009.

codificarne i principi, a partire dai due più antichi e autorevoli trattati di spionaggio che si conoscano: l'*Arte della guerra* di Sun Tze (generale cinese vissuto tra il VI e il V sec a.C.); e il meno diffuso, ma altrettanto importante *Arthaśāstra* di Kautilya³ (politologo indiano vissuto nel IV sec. a.C.).

Tuttavia qualsiasi attività di spionaggio o controspionaggio si voglia considerare, sia esso militare, economico, politico, tecnologico e così via, occorre tener presente (ieri come oggi) l'importanza del fattore umano quale elemento centrale dell'attività e dell'organizzazione di Intelligence, in particolar modo nelle interazioni tra gli individui e nella comprensione dell'ambiente circostante.

In tutti i testi di spionaggio e di tecniche investigative è sovente ribadito quali abilità sono necessarie nella raccolta di informazioni provenienti da fonte umana, tra cui: il saper osservare (guardare con attenzione persone e ambiente per identificare possibili indicatori di pericolo); il saper stimolare una conversazione per ottenere informazioni (elicitazione); il saper sorvegliare (tenere sotto controllo qualcuno o qualcosa).

3 *Arthaśāstra* il cui significato in sanscrito è "codice del potere", è un opera di equilibrio, di saggezza e di strategia politica e militare su come conquistare il potere e come mantenerlo. Scritto più di ventiquattro secoli fa, il documento fu riportato alla luce solo all'inizio del XX sec. d.C. Kautilya, l'autore di questa importante opera, è considerato l'Aristotele e il Macchiavelli hindū: «Ai tempi del confronto strategico tra Stati Uniti e Unione Sovietica qualcuno disse che Macchiavelli e Metternich non sarebbero serviti a Henry Kissinger, se l'inossidabile decano del ministero degli Esteri sovietico Andrej Gromyko avesse letto *Il Codice del Potere*. Max Weber e il Primo ministro indiano Jawaharlal Nehru, per i quali *Il Principe* di Machiavelli è inoffensivo a confronto con questo gioiello di razionalità pura, sarebbero stati certamente d'accordo» Cfr. Magi Gianluca (a cura di), Kautilya, *Il codice del potere. L'arte della guerra e della strategia indiana*, Edizione Il Punto d'Incontro, Vicenza, 2011, p. 8.

A questo proposito occorre fare però una breve distinzione tra l'attività informativa umana dell'Intelligence istituzionale (Humint) e quella dell'Intelligence di polizia (Humint di polizia), proprio per evitare incertezze riguardo alle loro funzioni e finalità.

L'Humint istituzionale consiste nella ricerca, nella raccolta e nell'elaborazione di notizie riguardanti la sicurezza e l'interesse nazionale provenienti da persone fisiche⁴. La NATO definisce l'Humint come “una categoria di Intelligence derivata dalle informazioni raccolte e fornite da fonti umane”.

L'Humint di polizia, invece, si occupa principalmente di trovare tutte le informazioni e le fonti di prova possibili su fatti penalmente rilevanti. È costituito da quel flusso informativo che include le notizie dei confidenti, degli informatori e degli stessi poliziotti, le dichiarazioni spontanee su fatti e persone di gente comune, le attività di sorveglianza, i rapporti e i verbali delle attività di sicurezza.

Sebbene alcuni settori delle Forze di polizia siano particolarmente versati ed esperti nella pratica OES (basti pensare a chi svolge il lavoro investigativo, il controllo del territorio, i pattugliamenti stradali, la sorveglianza e le scorte), poter disporre potenzialmente di un maggior numero di appartenenti alle forze dell'ordine con abilità simili, grazie ad una formazione

4 Nella gestione dell'Intelligence la ricerca informativa prevede diversi sistemi in riferimento alla fonte tra i quali: Humint (Human Intelligence, per le notizie provenienti da persone fisiche); Masint (Measurement and Signature Intelligence, per i dati metrici, angolari, spaziali, di lunghezza d'onda, etc. di eventi ed obiettivi di interesse informativo) Osint (Open Source Intelligence, per le informazioni tratte da fonti aperte); Sigint (Signals Intelligence, per i segnali e/o le emissioni elettromagnetiche dall'estero); Geoint (Geospatial Intelligence, per dati ed immagini georeferenziati). Vedi tabella 2.2 – A.

specifica che fornisca tutti gli elementi necessari a tale scopo, aumenterebbe di molto le probabilità di raccolta di notizie utili a massimizzare l'efficienza tattica di un'operazione o addirittura a migliorare quella strategica, come l'esperienza americana ha dimostrato.

Quando ci riferiamo all'elicitazione, invece, la questione è un po' più complessa, proprio perché le abilità personali dell'agente non operano più in due sfere distinte e distanti, dove da una parte c'è chi agisce come spettatore/rilevatore (la parte passiva), e dell'altra chi o cosa fa parte dell'evento (la parte attiva), ma operano in un contesto dove le due sfere di azione si sovrappongono. In questo caso, quindi, per poter stabilire un contatto con il soggetto dal quale si vogliono raccogliere informazioni, occorrerà che l'agente sia dotato, oltre che di buone capacità relazionali e di comunicazione, anche di nozioni base di psicologia.

Il termine elicitare, infatti, viene utilizzato in particolare nel campo della psicologia in riferimento a comportamenti o condotte utili a ottenere informazioni in modo discreto mediante domande o altri stimoli. Una tecnica, questa, così importante da essere utilizzata non solo nel mondo dell'Intelligence, ma sempre più spesso anche in quello privato. Un mezzo, quindi, per raccogliere notizie o dati senza dichiarare le proprie intenzioni con lo scopo di carpire informazioni sensibili da un interlocutore restio a rivelarle, sfruttando una conversazione apparentemente normale.

Contrariamente alle prime due tecniche (l'osservazione e la sorveglianza), l'elicitazione resta un'attività difficile da praticare, tanto da essere sconsigliata a chi non abbia quelle caratteristiche sopra richiamate, in particolare se si tratta di av-

vicinare individui di cui non si ha conoscenza⁵.

L'appartenente alle Forze di polizia rimane, quindi, una fonte indispensabile e qualificata nell'acquisizione di notizie d'ambiente proveniente dalla gente del luogo (ad esempio da commercianti, professionisti, conoscenti, amici, ecc.).

5 A questo riguardo sarà utile riferirsi all'esperienza pratica investigativa, affrontata nel prossimo capitolo.

Tabella 2.2.A

Gestione dell'Intelligence	
	<p>Ricognizione speciale (organizzazioni)</p> <p>Clandestino</p> <p>Reclutamento di risorse · Sistema cellulare · Azione segreta · Azione diretta · Tecniche operative.</p> <p>Humint</p> <p>Spionaggio</p> <p>Agenti (campo · maneggio) · Beni · Operazione nera (borsa nera) · Dispositivo di occultamento · Crittografia · Ritaglio · Goccia morta · Negazione e inganno · Intercettazioni · Falsa bandiera · Spionaggio industriale · Interrogatorio · Stazione numerica · Copertura ufficiale (non ufficiale) · Collegamento vocale unidirezionale · Spia residente · Steganografia · Sorveglianza.</p>
	<p>Segnali (SIGINT)</p> <p>Da alleati, nazioni e industrie · Nella storia moderna · Piattaforme operative delle nazioni · Individuazione della direzione · Analisi del traffico · TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions)</p>
Collezione	<p>Raccolta intelligence non classificabile (MASINT)</p> <p>Elettro-ottici · Geofisico · Nucleare · Radar · Frequenza radio · Materiale · Stima delle vittime (terremoto).</p> <p>Altro</p> <p>Culturale (CULTINT) · Finanziario (FININT) · Geospaziale (GEOINT) · Immagini (IMINT) · Mercato (MARKINT) · Open-source (OSINT) · Tecnico (TECHINT).</p>
Analisi	<p>Trappole cognitive · Ipotesi contrastanti · Obiettivo-centric · Probabilità stimata · Intelligence all-source · Intelligence di base · Valutazione dell'Intelligence · Intelligence medica · Geografia militare · Intelligence scientifica e tecnica.</p>
Diffusione	<p>Sturezza del ciclo di intelligence · Controspionaggio (organizzazioni) · Organizzazioni di controspionaggio e antiterrorismo</p>

2.3

LE FORZE DI POLIZIA IN ITALIA

L'Italia è il terzo Stato al mondo, dopo Russia e Turchia, per numero di Forze di polizia in relazione alla popolazione¹ (467,2 agenti in servizio ogni 100 mila abitanti) e resta l'unico paese ad avere quattro forze dell'ordine a carattere nazionale (Polizia, Carabinieri, Guardia di Finanza e Polizia Penitenziaria), di cui due con competenze generali e due con competenze specifiche.

Ogni corpo ha naturalmente i suoi comandi, i suoi centri operativi, le sue caserme, i suoi generali che difendono il proprio status di potere. Questo comporta, oltre all'enorme spesa e alla sovrapposizione di materie e di competenze tra le diverse forze, anche un maggior ostacolo all'adozione di un sistema di *Intelligence-led policy* fondato sulla centralizzazione

1 Secondo quanto riportato nella relazione annuale dell' UNODC (United Nations Office on Drugs and Crime) 2013, (dati ripresi da altre organizzazioni come Eurostat) la Russia è il paese più militarizzato al mondo con 564,6 agenti ogni 100.000 abitanti, mentre la Turchia si piazza al secondo posto con 474,8 poliziotti (la statistica si riferisce a nazioni con una popolazione superiore a 50 milioni). Sebbene il numero di agenti di polizia nell'Unione Europea si sia lentamente ridotto negli ultimi anni, (tra il 2009 e il 2016 l'UE ha registrato una continua diminuzione del numero di agenti presenti sul territorio, con una riduzione del 3,4%) l'Italia resta in assoluto il paese più militarizzato della UE anche nel 2015 con 453 agenti ogni 100.000 abitanti (tuttavia l'analisi statistica Eurostat non considera la differenza della popolazione tra i diversi Stati collocandola al sesto posto dopo paesi che non hanno una popolazione superiore ai 11 milioni di abitanti). Cfr. Statistiche pubblicate dalla Commissione Europea, *1.6 million police officers in the EU*, in «Eurostat», Eurostat News, Product code: ddn-20190104-1, published on 04 - Jan-2019.

informativa, che sarebbe necessario per una più efficace analisi dei dati raccolti da tutte le forze armate e di polizia (fatta eccezione per il C.A.S.A.).

Mettendo da parte questo aspetto, che resta comunque centrale per qualunque attività di Intelligence si voglia svolgere (qui intesa come metodo di acquisizione delle informazioni)², sarebbe forse possibile utilizzare i numerosi agenti delle Forze di polizia, già disponibili e ben distribuite sul territorio, per monitorare, rilevare, acquisire informazioni utili alla Sicurezza Nazionale (attività terroristiche, attività eversive dell'ordine democratico) e al contrasto alla criminalità organizzata (in riferimento alle questioni indirette riguardanti la Sicurezza Nazionale) come fossero tanti sensori?

Non si tratta naturalmente di ribadire prerogative, obblighi, doveri e *modus operandi* a cui fanno già riferimento gli appartenenti alle Forze di polizia (attività distinte e diverse da quelle dell'Intelligence istituzionale), ma di meglio dotare i primi, per mezzo di una formazione *ad hoc*, di quella capacità di osservazione, elicitazione e sorveglianza del territorio e della gente, che spesso non tutti gli operatori di polizia posseggono³.

Più della metà degli appartenenti alle Forze di polizia, infatti, si occupa prevalentemente di attività burocratica o di attività funzionali alla propria organizzazione, mentre solo una piccola percentuale svolge regolarmente un lavoro investigativo o di controllo del territorio, attività queste capaci di predi-

2 Vedi tabella 2.3 – A.

3 «Il 60 % delle divise non è adibito alla sicurezza dei cittadini, ma lavora in ufficio e vigila stazioni e comandi sparsi per le nostre regioni». Dichiarazioni del Sap (Sindacato autonomo di polizia) nel 2015, riprese successivamente da diverse testate giornalistiche.

sporre e allenare l'operatore di polizia a cogliere e decifrare quei segnali che provengono dall'ambiente circostante.

«Il 60 % degli uomini in divisa, da Cuneo a Caltanissetta, lavora nell'apparato tecnico-logistico. Un esercito di colletti bianchi, segretari e impiegati: [ogni Forza di polizia] ha infatti le sue centrali operative, le sue caserme, gli uffici per le divise, quello per gli stipendi, il parco automezzi, i suoi apparati e le sue scuole di formazione. Una duplicazione pletorica che raggiunge, a Firenze, il suo apice: i 7 mila operatori in città fanno riferimento a 11 centrali diverse, mentre attorno all'Arno si contano quattro mense intitolate alla polizia, due in cui possono mangiare solo i carabinieri, una adibita ai pompieri e un'altra riservata alla municipale. A Firenze alcuni comandi sono distanti pochi metri, ma anche a Roma e Milano le sovrapposizioni sono clamorose: vicino al Duomo si contano una trentina tra commissariati, caserme dell'Arma, [...], dipartimenti di pubblica sicurezza e uffici della questura. [...]. Uno spreco di risorse che fa il paio con lo spreco di uomini impegnati nella vigilanza di troppi immobili affittati: se si accorpessero tutti gli uffici in un'unica questura avremmo ben 150 poliziotti in più a disposizione per attività di sicurezza sul territorio catanese. In Italia ci sono, attualmente, 1.850 centri di comando della Polizia di Stato, 6.140 dei carabinieri (di cui oltre 4 mila stazioni), oltre a una ventina di direzioni centrali, a cui vanno aggiunti i distaccamenti della Finanza. Un'enormità [...]»⁴.

4 Nell'inchiesta giornalistica del settimanale *L'Espresso* del 2015 si evince, oltre ad alcuni aspetti legati allo spreco di risorse economiche e alla sovrapposizione delle attività delle Forze di polizia, anche come il personale viene impiegato. Cfr. Fittipaldi Emiliano, *Troppo Divise*, in «L'Espresso», n° 2, anno LXI, 15 gennaio 2015, pp. 30 – 37.

Naturalmente non si può certo pensare di eliminare l'attività burocratica per inviare più Forze di polizia sulla strada come più volte dichiarato da politici improvvisati. E i motivi perché questo sia impossibile a farsi sono essenzialmente due: il primo sta nel fatto che la maggior parte delle attività burocratiche, essendo connesse alle attività di polizia, contengono per loro natura segreti professionali o d'ufficio, oppure informazioni classificate⁵ che ne impediscono la conoscenza a chiunque altro non appartenga a quella FF.pp. Quindi, la possibilità che una parte dell'attività burocratica possa essere svolta da impiegati civili, utile a sollevare i militari da tali incombenze, può riguardare solamente quegli ambiti amministrativi e contabili per i quali è possibile un tale impiego; il secondo, invece, sta nel fatto che contrariamente a quanto si possa pensare è proprio l'attività burocratica a rappresentare la reale ossatura dello Stato e quella che realmente ne detiene il potere (il cosiddetto *Stato Profondo*)⁶ e che, malgrado alcuni tentativi di razionalizzazione, risulta impossibile persino da ridurre. Infatti, come è stato dimostrato da un acuto studioso di sistemi organizzativi umani, Northcot Parkinson: qualsiasi organizzazione burocratica, per il sol fatto di esistere, tende a crescere annual-

5 Ogni dipendente pubblico è obbligato dalla legge a non rivelare segreti riguardanti la sua professione (Rivelazione di segreto professionale art. 622 C.P.) o il suo ufficio (Rivelazione ed utilizzazione di segreti di ufficio, art. 326 C.P.), e a garantire la protezione dei dati personali e la tutela della privacy. Inoltre, l'accesso ai documenti di polizia classificati è consentito solo a coloro che per funzione o ufficio ne hanno facoltà o diritto a conoscerla.

6 Con il termine *Stato Profondo* si intende quell'insieme di organizzazioni dello Stato (apparati militari, economici, burocratici, ecc. ecc), capaci di influenzare o far pesare la propria volontà nelle decisioni politiche; «davanti ad ogni stanza del potere diretto si forma una sorta di anticamera di influssi indiretti e di controlli, un ingresso verso l'orecchio del potente, un corridoio verso la sua anima. Non esiste nessun potere senza questa anticamera e senza questo corridoio». Cfr. Schmitt, Carl, *Dialogo sul potere*, Il Melangolo, Genova, 1990.

mente con un tasso non inferiore del 5%, e continuerà a espandersi anche nel caso che non abbia nulla da fare⁷.

In considerazione di quanto detto è possibile ritenere che se si integrasse la formazione degli appartenenti alle Forze di polizia (ogni anno è prevista un'attività di aggiornamento professionale per le FF.pp., sia nell'ambito giuridico – amministrativo e sia nell'ambito tecnico – operativo)⁸ con attività volte a migliorare quegli aspetti di OES utili ad intercettare i cosiddetti segnali deboli⁹, si disporrebbe di una enorme quantità di "sensori umani sul territorio", gli Human Sensors appunto, che sarebbero attivi non solo durante le ore lavorative, ma soprattutto quando sono fuori dal servizio¹⁰. La realizzazione di un simile sistema, che miri a prevedere con il maggior anticipo possibile l'evolversi di situazioni di pericolo sul territorio, diminuirebbe in modo sensibile l'efficacia di eventuali minacce all'Ordine Pubblico e alla Sicurezza Pubblica, e permette-

7 Cfr. Parkinson Cyril North, *La legge di Parkinson*, Monti & Ambrosini, Pescara, 2011. Cfr. pure, Aprile Pino, *Elogio dell'imbecille. Gli intelligenti hanno fatto il mondo, gli stupidi ci vivono alla grande*, Ed. Piemme, Milano, 2012. pp. 106-109.

8 Ad esempio per la Polizia di Stato sono programmate annualmente, sei giornate di aggiornamento professionale (nelle quali sono previste lezioni interdisciplinari tenute da funzionari della PdS o da esperti interni o esterni all'amministrazione), tre di tecniche operative e tre di addestramento al tiro. In alcune regioni, ad esempio, si sta sperimentando il sistema Sisfor (sistema di formazione on-line delle forze dell'ordine) per la formazione del personale nelle attività teoriche.

9 La sorveglianza non consiste semplicemente nello scrutare lo schermo di un radar, ma nell'adottare una visione proattiva dell'evoluzione dell'ambiente. In questa concezione si ritrova l'idea di un'Intelligence relativa – comprendere e agire prima dell'altro – e l'importanza centrale della comunicazione – i segnali deboli sono innanzitutto un pretesto per costruire una visione comune ed essere collettivamente attenti. Cfr. Ansoff Igor H., *Le risposte strategiche ai "segnali deboli"*, in «Sviluppo e organizzazione», fasc. 33, 1976.

10 È utile ricordare che numerosi e d'ogni genere sono gli esempi che hanno visto i diversi appartenenti alle Forze di polizia intervenire in situazioni di pericolo fuori dal servizio.

rebbe soprattutto di aumentare la capacità dei sistemi decisionali di fornire risposte immediate ed efficaci.

A questo riguardo, sono da considerarsi interessanti alcune iniziative adottate dai ministri dell'Interno (succedutosi tra il 2016 e il 2018) e dello stesso capo della Polizia in seguito ai tragici eventi terroristici che colpirono diverse città europee.

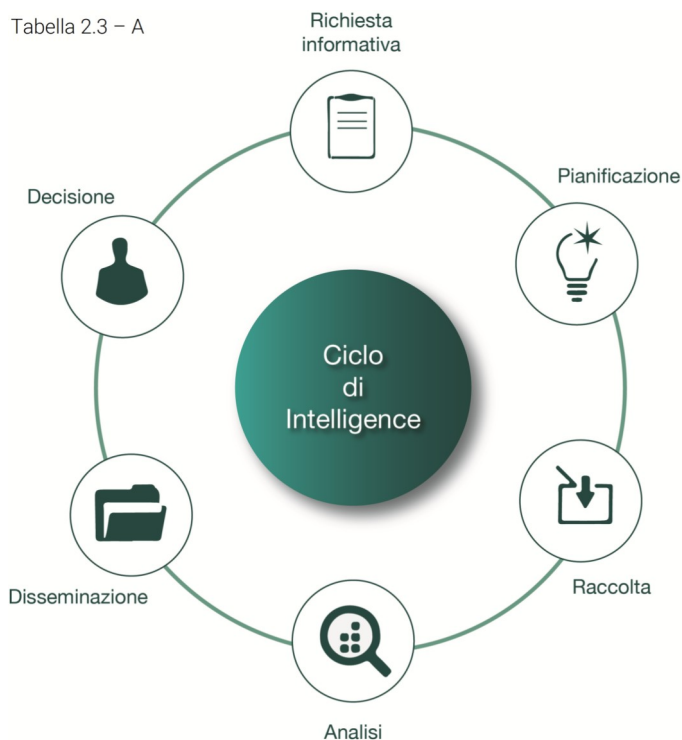
Pochi giorni dopo l'attentato terroristico di Nizza del 2016, ad esempio, una circolare del responsabile del Viminale inviata a prefetti e questori, invitava «tutti gli agenti a portare l'arma di ordinanza anche fuori dagli incarichi specifici e dall'orario di servizio, sollecitando alla vigilanza sempre». Una simile iniziativa è stata adottata l'anno successivo in seguito al vertice straordinario del Comitato di Analisi Strategica Antiterrorismo convocato dal ministro dell'Interno Marco Minniti, per decidere quali misure mettere in atto dopo l'attentato di Barcellona del 2017. Dalla riunione, alla quale hanno partecipato i vertici nazionali delle Forze di polizia e dei Servizi di Intelligence, fu ribadita la necessità che tutti i poliziotti portassero sempre con sé l'arma di ordinanza, anche quando non erano in servizio.

L'attentato di Berlino del 2016, invece, aveva già posto le basi per una nuova dottrina contro il terrorismo, ribattezzata dall'allora neo ministro Minniti come "prevenzione collaborativa", che in qualche modo estendeva a soggetti non appartenenti alle Forze di polizia, come amministratori locali, sindaci e corpi di polizia municipale delle città, affiancati da questori e prefetti, alcuni compiti di prevenzione del terrorismo, in modo da «rendere efficaci e capillari quelle forme di vigilanza attiva e di difesa passiva delle aree urbane di fronte alla minaccia del lupo solitario»¹¹.

11 Bonini Carlo, *Terrorismo, il nuovo schema di Minniti: "Sindaci e polizia locale ci*

Facendo affidamento, quindi, sull'elevato numero degli appartenenti alle forze di polizia, sulla loro diffusione su tutto il territorio e sul loro essere già uomini e donne militarmente addestrati (addestramento basico), si potrebbe presupporre con buona ragione che statisticamente questi *Human Sensors* potrebbero aumentare di gran lunga le *chance* sia dell'Intelligence istituzionale e sia dell'Intelligence di Polizia nell'acquisire informazioni utili concernenti la Sicurezza Nazionale e la criminalità organizzata.

Tabella 2.3 – A



aiuteranno a fermare i lupi solitari", in «Repubblica», 22 dicembre 2016.

2.4

L'ATTIVITÀ DI POLIZIA FUORI DAL SERVIZIO

Sebbene l'idea di poter disporre di un enorme "esercito" di *Human Sensors* disseminati su tutto il territorio per l'acquisizione di informazioni d'ambiente possa sollevare qualche dubbio circa la sua reale realizzazione ed efficacia (come attuare un programma formativo di questo genere, in che sistema raccogliere l'attività informativa proveniente dagli operatori delle Forze di polizia, chi e come dovrebbe gestire l'analisi dei dati, quanto costa un simile programma), c'è una questione che si impone su tutte le altre: perché mai un appartenente alle forze di polizia dovrebbe avere interesse a svolgere il proprio lavoro anche fuori dal servizio?

Prima di tutto è opportuno ricordare che nella storia delle Forze di polizia e nelle cronache ci sono moltissimi esempi di agenti fuori servizio (nell'esercizio delle proprie funzioni) che sono intervenuti in situazioni di estremo pericolo, mettendo a rischio la propria incolumità per salvare quella di altre persone¹. Fortunatamente non tutte le attività svolte fuori dall'orario di lavoro avvengono in modi così drammatici. Tuttavia, la maggior parte di queste situazioni, proprio per gli innumerevoli scenari che si potrebbero verificare, viene gestita pre-

1 Se si potesse disporre di tutti i dati riguardanti il profilo degli appartenenti alle Forze di polizia che hanno operato fuori dal servizio (background di polizia, formazione, conoscenza, esperienza, ecc.) si potrebbero analizzare le caratteristiche comuni e ripetitive che diventano determinanti in simili contesti.

valentemente in due modi: o con un'azione immediata, volta ad impedire il compimento di un reato, nel prestare un soccorso pubblico e via dicendo; oppure con una azione differita, dando informazioni ai propri centri di comando riguardo a luoghi, persone e fatti concernenti attività criminose o potenzialmente tali.

Pur riconoscendo l'esistenza di fatto di un'attività di polizia fuori dall'orario di servizio, sebbene principalmente limitata a situazioni di pericolo, resta il dubbio che tutti gli agenti delle Forze di polizia si adoperino in tal senso o che si presentino, come qui si sostiene, facendo attività di OES.

Per meglio affrontare la questione appena posta è necessario valutare due ulteriori aspetti concernenti l'attività delle forze dell'ordine in un simile contesto: l'obbligo giuridico a intervenire in presenza di un reato penale (in particolare quando c'è la procedibilità d'ufficio) e il compenso economico per l'attività svolta. Il primo riguarda alcune disposizioni di legge che di fatto obbligano gli appartenenti alle Forze di polizia a osservare i doveri inerenti la loro funzione anche fuori dal servizio². Il secondo, invece, riguarda alcune questioni di carattere meramente economico-amministrativo che prevedono il riconoscimento agli appartenenti delle Forze di polizia che operano fuori dal servizio di un compenso remunerativo in ore straordinarie, che per consuetudine poi

2 Gli ufficiali e gli agenti di polizia giudiziaria (c.p.p. art. 57), o come nel caso degli appartenenti alla Polizia di Stato, avendo contratto un obbligo giuridico con lo Stato, nella fattispecie in riferimento all'ordinamento della pubblica sicurezza, sono tenuti ad osservare i doveri inerenti la propria funzione anche fuori dalle ore lavorative (art. 68 della legge n° 121 del 01.04.81) e pertanto sono da considerarsi in servizio permanente anche nei periodi di permesso e di licenza. Cfr. pure art. 55, 330 e 347 c.p.p.

il personale non richiede mai³.

Proprio in riferimento a quest'ultimo aspetto, ci si potrebbe domandare se scelte differenti (ad esempio, maggiori incentivi premiali) possano incentivare l'attività di OES fuori dal servizio⁴.

Ad ogni modo, non è questo l'argomento centrale che spiega il perché un operatore di polizia dovrebbe svolgere fuori dal servizio attività di OES: a determinare il successo di una simile progetto (Human Sensors) sono piuttosto gli aspetti psicologici (in riferimento alle condotte umane altruistiche e prosociali) e quelli statistici (in riferimento a un numero significativo di Forze di polizia sul territorio nazionale che se debitamente formate potrebbero implementare una simile attività).

3 L'indennità delle ore straordinarie per gli operatori di polizia sono suddivise per fasce in riferimento al grado, ma non rappresenta un importo particolarmente attrattivo.

4 Un determinato comportamento umano si verifica tanto più spesso quanto più ad esso è associato una ricompensa. A questo proposito vedi il principio base della teoria dell'apprendimento di Thorndike: La *legge dell'effetto* (una risposta che definisce un effetto piacevole tende a ripetersi, viceversa un effetto spiacevole fa sì che la risposta non si ripeta); E la *legge dell'esercizio* (l'apprendimento è graduale e migliora con la ripetizione delle prove e tanto più spesso viene ripetuta una risposta, tanto più diventa probabile).

2.5

IMPLEMENTAZIONE DEL MODELLO OES NELL'ATTIVITÀ DI HUMAN SENSORS: UNA QUESTIONE DI PSICOLOGIA SOCIALE E DI STATISTICA

Quali sono le ragioni per cui un soggetto, nel nostro caso un appartenente alle Forze di polizia, è portato a comportarsi in modo altruistico fuori dal servizio?

Per poter rispondere a questa domanda, occorre guardare oltre gli aspetti "meccanicistici" legati all'esistenza di una norma giuridica che impone al soggetto un determinato comportamento, e cercare nella psicologia sociale e nella sociobiologia gli elementi più profondi per la comprensione di questa caratteristica umana.

Secondo autorevoli studiosi, sono le *motivazioni* a spingere una persona a comportarsi in modo *prosociale* o in modo *altruistico*.

La condotta prosociale, ovvero quei comportamenti che mirano a portare sollievo o aiuto ad altri, non può definirsi necessariamente altruistica, proprio perché le motivazioni che spingono un soggetto ad adottare simili comportamenti potrebbero essere determinate dall'aspettativa di ricavarne un vantaggio.

Anche in riferimento all'altruismo, le cose non sono molto diverse da quel che comunemente si pensa. Se consideriamo l'altruismo alla luce di alcuni aspetti della teoria evuzionistica di Charles Darwin, come la selezione naturale e la lotta dell'individuo per la sopravvivenza, sembra esserci piena contraddizione con tale principio. Lo scienziato britannico non

riuscì mai a spiegare questa contraddizione, tanto da dubitare egli stesso della fondatezza della sua teoria, semplicemente perché partiva da un errato postulato che non distingueva tra specie che hanno elaborato strutture sociali e specie che non l'hanno fatto.

Nelle specie sociali il vantaggio competitivo per la trasmissione del proprio corredo cromosomico non dipende esclusivamente dal singolo individuo ma è legato alla sopravvivenza del nucleo familiare, del gruppo o dell'intero branco¹.

Guardando la questione da un'altra prospettiva, quindi, si comprende come la selezione non avviene più in riferimento all'individuo, ma al sistema sociale, e che la maggior parte degli atteggiamenti solidali non è generata dall'amore per il prossimo, quanto piuttosto, come spiega la sociobiologia, da una qualche forma di interesse.

Nella teoria della selezione del gruppo dell'ecologo scozzese Vero Copner Wynne-Edwards, ad esempio, si sostiene che gli individui che sono disposti a sacrificare se stessi per la sopravvivenza della specie hanno meno probabilità di estinguersi di un gruppo rivale i cui membri mettono davanti a tutto il proprio interesse egoistico².

Un'altra prospettiva più convincente venne fornita più tardi da

-
- 1 Cfr. Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, Il Mulino, Bologna, 2010, p. 249.
 - 2 Wynne-Edwards V. C., *Animal dispersion in relation to social behavior*, Oliver and Boyd, Edinburgh 1962.

William Hamilton con il concetto di *selezione parentale*³ [1964], che venne poi integrata dalla teoria del *gene egoista* del biologo evolutivo Richard Dawkins⁴ [1976], il quale spiegò che i comportamenti altruistici, persino quelli che sembrano compiere un puro atto di amore, sono determinati dai propri geni per perpetuare se stessi⁵.

Tuttavia si deve alla teoria dell'*altruismo reciproco* del biologo Robert Trivers [1971] la spiegazione del perché gli individui si comportano altruisticamente anche verso membri non consanguinei. Questa teoria si basa sul concetto di scambio (io faccio un favore a te perché mi aspetto che tu ne faccia uno a me): in definitiva, un individuo mette in atto un comportamento altruistico nei riguardi di un estraneo se i potenziali benefici dell'azione superano il costo⁶.

-
- 3 Sia per gli uomini che per gli animali il comportamento altruistico verso figli, nipoti, cugini avviene perché così facendo aumenta la probabilità di sopravvivenza dei propri geni o di un insieme genetico che contiene comunque molto del proprio DNA. In questo modo, l'evoluzione non promuove il successo riproduttivo dell'individuo ma quello del gene. Cfr. Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, op. cit. p. 250.
 - 4 Nel suo celebre libro lo studioso riduce tutte le dinamiche evolutive a una competizione tra geni, liquidando la questione dei comportamenti altruisti e cooperativi esistenti in natura sostenendo come essi non siano altro che una forma sottile di egoismo mascherato, in cui chi si comporta altruisticamente in realtà lo fa per favorire i propri parenti più stretti (che condividono una buona percentuale degli stessi geni) o in vista di un qualche altro vantaggio o beneficio per sé stesso. Cfr. Dawkins Richard, *Il gene egoista. La parte immortale di ogni essere vivente*, Arnoldo Mondadori Editore, Milano, 2011.
 - 5 Una madre che si butta nel fuoco per salvare un figlio in pericolo lo fa immaginando di compiere un genuino atto di amore ma, in realtà, in lei questo tipo di comportamenti è programmato a livello genetico e nel suo DNA è codificato un imperativo categorico: fai qualunque cosa, anche a costo della tua stessa vita, per garantire e salvaguardare la trasmissione dei tuoi cromosomi. S. Boca, P. Bocchiaro, C. Scaffidi Abbate, *Introduzione alla psicologia sociale*, op. cit., p. 250.
 - 6 Cfr. Hauser Marc D., *Menti Morali. Le origini naturali del bene e del male*, Il Saggiatore, Milano, 2007, p. 252 – 253.

Dal punto di vista evolutivo, quindi, l'altruismo rappresenta un meccanismo con cui gli individui e i gruppi sociali aumentano le probabilità di far sopravvivere i propri geni e cooperano per massimizzare i benefici individuali ricavabili in futuro.

Alcuni ricercatori hanno condotto degli esperimenti allo scopo di definire l'area neuronale dell'altruismo reciproco registrando i segnali più forti in presenza di alleanze e mutua collaborazione nelle medesime zone cerebrali che rispondono positivamente a un numero indefinito di piaceri⁷. Quindi l'istinto alla collaborazione, portando ad una piacevole sensazione di benessere, rinforza ulteriormente i comportamenti altruistici.

Sebbene le diverse ipotesi sociobiologiche considerino l'altruismo dal punto di vista della genetica, è necessario esaminare anche quegli studi che considerano la questione in relazione alla *selezione culturale*, leggendo l'altruismo come un valore e una norma sociale da interiorizzare mediante l'apprendimento.

L'assunto principale di un modello teorico riferito alla selezione culturale evidenzia come gli individui, vivendo all'interno di una società e sviluppando il senso di appartenenza a gruppi sociali che per loro sono significativi, sono influenzati dai valori e dalle norme che condividono con gli altri membri del gruppo.

Spesso, in modo semplicistico, si è indotti a ritenere una persona altruista o egoista, coraggiosa o pavida, a seconda

7 Rilling J., Gutman D., Zeh T., Pagnoni G., Berns G., Kilts C., *A neural basis for social cooperation*, in «National Center for Biotechnology Information, U.S. National Library of Medicine», Atlanta, 2002.

del suo atteggiamento in relazione ad una medesima azione, ma questo giudizio non aiuta a spiegare gli aspetti più profondi di tali comportamenti. Per gli psicologi sociali, invece, la questione va posta in altri termini per essere compresa. E per far questo bisogna partire da una domanda: quando le persone aiutano?

Negli anni settanta fu elaborato un *modello stadiale di intervento*⁸ in grado di rispondere a questa domanda. Prima che un soggetto intraprenda comportamenti di aiuto in una situazione di emergenza, occorre che si verifichino cinque distinte condizioni:

1. accorgersi dell'evento
2. interpretare l'evento come emergenza
3. assumersi la responsabilità
4. sapere cosa fare
5. decidere di intervenire

Naturalmente è essenziale che il soggetto si accorga di quello che sta accadendo. Spesso circostanze banali come l'andare di fretta possono impedire la percezione di allarme⁹. Oltre ad accorgersi della condizione di emergenza, è necessario che il soggetto la interpreti come tale. In alcuni contesti, ad esempio, l'individuo può non accorgersi immediatamente della situazione di emergenza, e per superare questa condizione di incertezza e confusione tende ad affidarsi a

8 Cfr. Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, op. cit., pp. 255 – 257.

9 Confronta a questo riguardo il un famoso studio del 1973 chiamato del «Buon Samaritano», di Darley e Batson.

quanto fanno le altre persone presenti.

Tuttavia, l'aver compreso di trovarsi in una situazione di emergenza non è sufficiente a far decidere il soggetto a intervenire, ma occorre un ulteriore passaggio: l'assunzione di responsabilità.

Studi intrapresi in tal senso hanno evidenziato in modo inquietante come la disponibilità a prestare soccorso diminuisca nelle situazioni di pericolo all'aumentare del numero delle persone presenti¹⁰, accertando che il numero dei testimoni genera nei partecipanti un effetto di suddivisione di responsabilità, dove ciascuno pensa e spera che sarà l'altro ad intervenire¹¹.

Infine, una condizione di fondamentale importanza, per poter intervenire in situazioni di pericolo o di emergenza, è sapere cosa fare.

La mancanza di conoscenza, di competenze ed esperienza pone il soggetto in una condizione di cecità, di inadeguatezza e di timore di fronte al pericolo, proprio perché non è in grado di prefigurarsi quali possibili scenari potrebbero delinearsi. Avere contezza della situazione e sapere come gestirla sono determinanti nel far decidere un soggetto ad intervenire o meno, presupposti senza i quali non è possibile offrire un aiuto adeguato.

Pur ritenendo valido il modello stadiale sopra citato, non rappresenta in modo esaustivo tutte le diverse situazioni che

10 Ci si riferisce al dramma di Kitty Genovese del 1964. La giovane donna americana venne aggredita e uccisa in strada davanti ad una quarantina di persone che nonostante le urla e le violenze non intervenne a dare soccorso. Cfr. Bocchiaro Pietro, *Psicologia del male*, Editori Laterza, Bari, 2010, pp. 47 – 67

11 Questo comportamento sociale è conosciuto come “diffusione della responsabilità”. Ivi, p. 55

si possono determinare. Ad esempio, ci sono circostanze in cui i soggetti, pur essendo consapevoli del bisogno di aiuto della vittima e di essere chiamati alle proprie responsabilità, preferiscono non intromettersi per non rischiare. Per chiarire queste situazioni è stato sviluppato un altro modello teorico, verificato sperimentalmente, che spiega in termini di costi-benefici quali fattori entrano in gioco.

Nella teoria dello *scambio sociale*, le interazioni umane sono guidate da una sorta di economia sociale per cui gli individui scambiano non solo beni materiali, ma anche beni sociali quali amore, assistenza, informazioni, status, mirando, come avviene in ambito economico (secondo la teoria "mini-max" del matematico ungherese John von Neumann), al massimo piacere con il minimo costo. Secondo questo principio, gli individui agiscono in modo razionale e nel proprio interesse valutando in termini di vantaggio e svantaggio la decisione di prestare o meno aiuto.

Persino nel caso dell'altruismo, quindi, l'uomo pensa in termini di costi e benefici. Ragionando in termini di reciprocità, ad esempio, può essere conveniente prestare il proprio aiuto perché ci si attende che venga restituito il favore in futuro. Anche l'approvazione sociale, e di conseguenza l'innalzamento dell'autostima che in questo modo genera una sensazione di benessere, è una condizione che favorisce i comportamenti altruistici.

In definitiva è possibile dire che la massimizzazione dei benefici, come si è accennato, non riguarda solamente la sfera di beni materiali, ma anche, e forse soprattutto, quella di beni sociali come l'autostima, la stima, l'amore, l'approva-

zione o la gratitudine¹².

Pur considerando valide le considerazioni fin qui poste, importanti nel farci comprendere la vastità dei meccanismi e delle motivazioni psicologiche che possono indurre un soggetto a comportarsi altruisticamente, è necessario mettere in luce anche quelle condizioni che non tengono conto del modello decisionale costi-benefici. Una di queste è la *percezione di similarità*¹³.

E' stato dimostrato, infatti, che le persone sono tanto più disposte ad aiutare gli altri quanto più quest'ultimi sono percepiti come propri simili. La ragione principale sta proprio nella percezione di somiglianza che aumenta l'attrazione tra i soggetti accrescendo così la disponibilità ad aiutare.

Questo breve percorso fatto nel campo della psicologia sociale e della sociobiologia, ci spiega quali sono i meccanismi comportamentali per cui un individuo possa decidere di intraprendere un'attività apparentemente senza benefici, chiedendo così quegli aspetti che hanno indotto a dubitare della possibilità che un appartenente delle Forze di polizia possa in modo deliberato e partecipativo (se messo nelle condizioni di saper cosa fare e come svolgere il ruolo di Human Sensor) iniziare una simile attività fuori dal servizio a prescindere dei suoi obblighi giuridici.

12 A questo riguardo sarebbe utile approfondire anche quegli aspetti riguardanti il *senso di colpa* generato da un non intervento in situazioni di emergenza e i suoi effetti sulla psiche sul comportamento umano necessario per ripristinare la propria immagine di sé. Cfr. Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, op. cit., p. 254.

13 Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, op. cit., p. 259.

Dotare gli appartenenti delle Forze di polizia di un modello di OES utile nell'attività di Human Sensor significa semplicemente disporre, o predisporre, di personale già qualificato e disseminato su tutto il territorio pronto ad attivarsi in modo autonomo quando le circostanze lo richiedono allo scopo di raccogliere informazioni di contesto.

L'idea di utilizzare in modo indistinto tutte le Forze di polizia per implementare un più ampia collezione informativa si basa principalmente sulle probabilità con cui un operatore di polizia, se formato nell'attività di OES, possa contribuire ad aumentare sensibilmente le *chance* di raccolta di notizie utili all'attività di Intelligence o a impedire che situazioni di emergenza diventino un pericolo per la Sicurezza Nazionale o per la Sicurezza Pubblica.




A questo scopo ci si servirà di un piccolo esempio per riferirsi a quegli aspetti statistici sopra richiamati partendo però da una domanda: Quanto inciderebbe nella raccolta informativa la somministrazione a tutto il personale delle FF.pp. di un corso formativo o addestrativo per il potenziamento delle capacità di OES?

Per poter rispondere a questo quesito è necessario partire da alcune premesse.

Consideriamo, come popolazione oggetto di questa analisi (vedi tab. 2.5 - A), l'insieme delle Forze di polizia "Fp", di cui il 40% pratica principalmente attività investigativa e di prevenzione (propedeutiche all'attività informativa) che chiameremo "Fi", mentre il restante 60% pratica un'attività esclusivamente

tecnico – burocratica (con una modesta capacità di raccolta informativa) che chiameremo “ F_t ”¹⁴.


Tabella 2.5 - A

<i>Forze di polizia</i> 	F_p	40%	Operatori di polizia che svolgono prevalentemente attività investigativa, di prevenzione e del controllo del territorio		F_i
		60%	Operatori di polizia che svolgono prevalentemente attività tecnico – burocratiche		F_t

Introduciamo il parametro ICI (Indice di Capacità Investigativa) ad esprimere la capacità di raccolta di informazioni utili nell'attività di Intelligence con un range compreso tra 0 e 1, dove 0 è il valore nullo e 1 è il valore massimo (quindi si considereranno tutti i valori intermedi: 0,1; 0,2; ..., 0,5; ecc.).

Ipotizziamo (vedi tab. 2.5 – B) che le Forze investigative (F_i) abbiano un ICI di 0.6 – 0.7, mentre le Forze tecnico - burocratiche (F_t) ne abbiano uno di 0,2 - 0,25¹⁵.

Tabella 2.5 - B

F_p	Capacità di raccolta di informazioni da 0  1	
F_i	0,6	0,7
F_t	0,2	0,25

14 Questa indicazione fa riferimento alle dichiarazioni del sindacato di polizia Sap (vedi § 2.3) riguardo alle percentuali degli operatori della Polizia di Stato impiegati in attività investigative e tecnico-burocratiche. È possibile supporre con buona ragione che anche le altre FF.pp. abbiano come tendenza un numero inferiore di addetti alle attività investigative.

15 L'ipotesi fa riferimento ai dati percentuali medi rilevati dai questionari somministrati agli investigatori delle FF.pp. (vedi § 3.2)

A questo punto occorre valutare di quanto, un corso di formazione o di addestramento, possa incidere nel migliorare quelle abilità necessarie a ciascun operatore di polizia (nelle attività di OES), al fine di implementare le capacità di raccolta informativa.

Alcuni studi di John Barron (1987) e John Bishop (1994) hanno esaminato una stretta correlazione tra la formazione e la produttività, stabilendo quale impatto determini l'aggiornamento professionale del capitale umano sugli aumenti della produttività del lavoro¹. Barron, ad esempio, evidenzia come l'indice di produttività, in seguito ad una attività formativa, porti ad una sostanziale crescita della produttività: «un aumento del 10 % della formazione aumenta la produttività del 2 % durante i primi tre mesi di lavoro»². Secondo Bishop, invece, l'entità del beneficio dello *spillover*³ nei primi tre mesi è stimata intorno al 16% della produttività al netto dei costi di formazione⁴.

Anche diversi report economici italiani ed europei evidenziano l'effetto positivo della formazione professionale nell'ambito della produttività aziendale⁵.

1 Black Sandra E., Lynch Lisa M., *Human - Capital Investments and Productivity*, in «The American Economic Review», Vol. 86, No. 2, Papers and Proceedings of the Hundredth and Eighth Annual Meeting of the American Economic Association San Francisco, CA, January 5-7, 1996 (May, 1996), pp. 263-267

2 Barron John M., Berger Mark C., Black Dan A., *On-the-Job Training*, W.E. Upjohn Institute for Employment Research, Kalamazoo, Michigan, 1997, p. 185.

3 In italiano "traboccamento", la «situazione in cui una spesa pubblica, sostenuta per produrre benefici per i residenti di un ambito territoriale o amministrativo, genera benefici anche fuori di tale ambito. Cfr. VV.AA., *Enciclopedia dell'Economia Garzanti*, Garzanti Editori, Cernusco, 1997, p. 1120.

4 Lynch Lisa M., *Training and the Private Sector*, University of Chicago Press, 1994. Si veda in particolare il capitolo 6 di John Bishop, *The Impact of Previous Training on Productivity and Wages*, pp. 161 – 200.

5 «Si stima infatti che per ogni ora di formazione per addetto i ricavi corrispon-

Tuttavia, al pari di altre attività intangibili, la possibilità di stabilire un valore dell'incidenza di un corso di formazione sulla produttività in modo univoco risulta di non facile determinazione poiché dipendente da molte variabili, come ad esempio, le modalità con le quali vengono somministrati i corsi di aggiornamento, la qualità della formazione, se l'attività formativa è svolta con risorse interne o esterne⁶ all'azienda, le ore pro-capite di formazione, il background e l'istruzione di ciascun lavoratore, e via dicendo.

Presupponiamo che un corso di formazione ben strutturato, allo scopo di migliorare le capacità di OES di ciascun operatore nella raccolta informativa di alto valore, incida di appena il 10% in più sull' ICI rispetto al valore precedente, una percentuale assai più bassa rispetto a quelle emerse dai diversi studi⁷. In questo caso il 60% delle FF.pp. che non svolge attività propedeutiche alla raccolta informativa, aumenterebbe la propria capacità di raccolta informativa totale dello 0,275%, portando ad un aumento totale delle Capacità Informative (CI) dell'1 % in più.

denti aumentino di oltre un euro». Cfr. Isfol (Istituto per lo sviluppo della formazione professionale dei lavoratori), *XVI Rapporto sulla Formazione continua Annualità 2014 - 2015*, commissionato dal Ministero del Lavoro e delle politiche sociali (Direzione generale per le politiche attive, i servizi per il lavoro e la formazione), dicembre 2015, pp. 27 - 28.

6 Alcuni studi hanno mostrato una diversa incidenza dei corsi di formazione sulla produttività a seconda del fatto che la formazione venga svolta all'interno dell'azienda con proprio personale esperto oppure all'esterno. Nel secondo caso si registra un sensibile aumento.

7 Bartel, ad esempio, evidenzia come quelle aziende che implementato nuovi programmi di formazione per specifici gruppi di dipendenti registrano significativi aumenti di produttività (in media del 19%). Cfr. Bartel, P. Ann, *Productivity gains from the implementation of employee training programs*. Industrial Relations, Vol. 33(4), 1994, pp. 411-425. Cfr. pure, de Kok Jan M.P., *The Impact of Firm - provided training on production: testing for firm - size effects*, Tinbergen Institute Discussion Paper, Netherlands, 2000, p. 5

Tabella 2.5 - C

FF.pp. Fp % numerica	(ICI) Indice di Capacità di raccolta delle informazioni da 0 a 1 (valore medio)	Valore totale della (CI) Capacità Informativ a prima di un corso di formazion e %	Ipotetico Incremento % dell'ICI dopo un corso di formazione	Increment o parziale dell'ICI	Valore complessi vo dell'ICI dopo corso di formazion e	Valore totale della (CI) Capacità informativa dopo un corso di formazione %
Fi 40%	0,7	28	10%	0,07	0,77	31
			15%	0,105	0,80	32
			20%	0,14	0,84	34
Ft 60%	0,25	15	10%	0,025	0,275	16
			15%	0,0375	0,288	17
			20%	0,05	0,30	18

A questo riguardo è stato valutato un diverso impatto dei corsi di formazione se rivolto ad un personale specializzato o non specializzato. Nel 2008, infatti, è stato condotto uno studio che ha analizzato gli effetti della formazione sulla produttività del lavoro utilizzando un gruppo omogeneo e rappresentativo di aziende e dimostrando come all'interno dei gruppi professionali l'effetto della formazione sulla produttività sia più grande e significativo per i "colletti blu" che non per i "colletti bianchi"⁸. Questo elemento potrebbe essere utile per valutare con maggiore attenzione l'utilità che un corso di aggiornamento avrebbe sugli appartenenti alle FF.pp. che normalmente non svolgono attività informativa.

8 Colombo Emilio, *Stanca Luca, The Impact of Training on Productivity: Evidence from a Large Panel of Firms*, Working Papers from University of Milano – Bicocca, No 134, Department of Economics, Milano, 2008, p. 1

Quindi valutando un maggior impatto per quegli operatori di polizia che non svolgono regolarmente attività investigativa o di prevenzione è possibile considerare un maggior impatto sull'aumento delle CI (vedi tab. 2.5 – D).

Tabella 2.5 - D

FF.pp. Fp % numerica	(ICI) Indice di Capacità di raccolta delle informazioni da 0 a 1 (valore medio)	Valore totale della (CI) Capacità Informativ a prima di un corso di formazion e %	Ipotetico Incremento % dell'ICI dopo un corso di formazione		Incremento parziale dell'ICI		Valore complessivo dell'ICI dopo corso di formazione		Valore totale della (CI) Capacità informativa dopo un corso di formazione %	
Fi 40%	0,7	28	10%		0,07		0,77		31	
			15%		0,105		0,80		32	
			20%		0,14		0,84		34	
Ft 60%	0,25	15	10%	20%	0,025	0,05	0,275	0,30	16	18
			15%	25%	0,0375	0,063	0,288	0,54	17	32,4
			20%	30%	0,05	0,075	0,30	0,55	18	33

In considerazione di quanto detto è possibile ritenere che un diffuso addestramento o aggiornamento delle FF.pp. migliorerebbe in modo sensibile la raccolta informativa d'ambiente aumentando le *chance* dell'Intelligence di intercettare quei famosi segnali deboli sempre più difficili da cogliere.

Ma quanto costerebbe allo Stato l'attivazione di un simile programma? Secondo alcune stime il costo di un corso di aggiornamento per un dipendente di aziende si aggira mediamente intorno ai 50 euro. Tuttavia occorre considerare, come

già detto, che le FF.pp. hanno già a bilancio il costo per l'aggiornamento professionale che annualmente sono tenuti a frequentare, quindi, si tratterebbe principalmente di predisporre un programma addestrativo/formativo e di un corpo docente esperto nelle attività di OES.

Se si considerano i drammatici eventi terroristici che dal 2001 in poi hanno colpito le diverse città del mondo e le interconnessioni che sempre più spesso vede terrorismo, criminalità organizzata e corruzione agire assieme⁹, allora forse occorre domandarsi se non sia il caso di considerare lo Human Sensor nell'Intelligence di polizia un utile strumento per la raccolta informativa di contesto.

9 Maronta Fabrizio, Caracciolo Lucio, *Criminalità e terrorismo sono due facce della stessa medaglia. Conversazione con Louise Shelley, professoressa e direttrice del Terrorism, Transnational Crime and Corruption Center alla George Mason University (Virginia, Usa)*, in «Limes», n° 11, dicembre 2015.

CAPITOLO 3

LO HUMAN SENSOR NELL'ATTIVITÀ DI INTELLIGENCE DI POLIZIA

3.1

INTELLIGENCE DI POLIZIA E SICUREZZA NAZIONALE

Come accennato, *l'Intelligence di polizia* è l'attività con cui le forze dell'ordine, raccolgono, analizzano e diffondono le informazioni, indirizzandole verso i diversi livelli di competenza in base alla loro natura.

Un processo informativo, questo, in cui l'attività di Intelligence può sia riguardare la prevenzione e la repressione dei reati (sempre più spesso questo avviene grazie all'utilizzo di potenti software e di dispositivi tecnologicamente avanzati in grado di catalogare, aggregare e processare un'infinità di dati e informazioni)¹, sia a far nascere e sia a sostenere un processo investigativo. A questo scopo, due sono le colonne portanti su cui poggia l'efficacia di qualsiasi attività di Intelligence: una buona raccolta informativa e un'ottima capacità di analisi². La mancanza o la debolezza di uno dei due mo-

1 La possibilità di poter disporre di potenti sistemi tecnologicamente all'avanguardia, come quello in uso al Comando Generale dei Carabinieri (SI.CO.TE. - *Sistema di Controllo del Territorio*, un programma compreso tra quelli di specifico rilievo per la difesa e la Sicurezza Nazionale) per elaborare e processare dati strutturati e non, interni ed esterni con formati eterogenei, permette di poter assicurare un più elevato supporto alle attività di prevenzione generale e controllo del territorio. Questo sistema ha permesso di ampliare le capacità di analisi e operative dei reparti dedicati alle attività informative e di contrasto al terrorismo e alla criminalità organizzata.

2 Naturalmente anche gli altri elementi del ciclo d'Intelligence sono indispensabili per poter ottenere una informazione utile al decisore: porre un obiettivo informativo non necessario porta a distrarre risorse e tempo prezioso da attività che invece sarebbero più importanti; la mancanza di un sistema capace di elaborare l'enorme quantità di dati a disposizione avrebbe conseguenze certe sulla tempestività e sull'accuratezza dell'analisi; l'assenza di archivi correttamente orga-

menti influiscono notevolmente sui risultati di conoscenza e di previsione che si vogliono raggiungere.

Sebbene le FF.pp. hanno funzioni e compiti distinti da quelli dei Servizi di Informazione per la Sicurezza, i rivolgimenti geopolitici, sociali, tecnologici, economici, militari degli ultimi decenni hanno portato - stanno portando - questi due mondi ad una sempre maggiore convergenza.

Sino al 1991, la collaborazione tra le Forze di polizia e le Agenzie dell'Intelligence in Italia riguardava, almeno ufficialmente, in prevalenza i delitti contro lo Stato (propaganda eversiva, attività terroristiche ed eversive dell'ordine democratico e così via) di matrice politica o criminale (estremisti di destra, di sinistra e criminalità organizzata). Basti pensare all'attività terroristica e alle stragi che dal secondo dopoguerra in poi, a cominciare dall'eccidio di Portella della Ginestra del 1947, insanguinarono il Paese.

Come conseguenza degli "anni di piombo", caratterizzati da un'estremizzazione della dialettica politica e da una recrudescenza degli scontri di piazza sino alla lotta armata e terroristica, l'Italia si è dotata di una legislazione innovativa³ e all'avanguardia nel contrasto al terrorismo. In questo contesto fu necessario sia dare alle FF.pp. maggiori poteri, sia chiarire quale fosse la posizione dei Servizi di Intelligence nel quadro costituzionale e democratico dello Stato, regolamentando giuridicamente per la prima volta le sua attività⁴. La

nizzati limiterebbe le capacità di ricerca.

3 Furono introdotte una serie di misure repressive che rafforzavano i poteri della polizia. Vennero istituiti dei corpi speciali (GIS, NOCS) con finalità antiterrorismo ed emanate pene più severe. Cfr. Legge n. 15 del 6 febbraio 1980.

4 L'offensiva sferrata al cuore dello Stato da parte del terrorismo interno portò

lunga storia di lotta al crimine organizzato e al terrorismo interno ha forgiato una cultura dell'antiterrorismo assente in altri Stati del mondo che non hanno conosciuto stagioni eversive paragonabili a quella italiana.

Se si considerano i dati riguardanti gli attentati terroristici che dalla seconda metà del XX sec. sino agli anni Novanta hanno colpito l'Europa, si noterà come questo fenomeno sia legato principalmente a movimenti nazionalisti e separatisti o a estremismi politici di destra e di sinistra. Dal 2001, invece, si assiste ad un aumento significativo degli attacchi di natura pseudo religiosa⁵ (fenomeno della radicalizzazione religiosa; appartenenza a gruppi estremisti jihadisti)⁶ o legati al disagio sociale.

Quest'ultimo fenomeno in particolare è forse oggi poco considerato come una reale e costante minaccia alla Sicurezza Nazionale. Nell'interessante analisi di Mario Caligiuri⁷, il di-

unitariamente le forze politiche a legiferare in materia di sicurezza come mai era accaduto prima d'allora. Con la legge del 24 ottobre 1977, n. 801, si introduce per la prima volta il Diritto nel campo dei Servizi di Informazione per la Sicurezza. Viene attribuita una precisa responsabilità politica delle attività che viene svolta nel mondo dell'Intelligence con a capo il Presidente del Consiglio, e per competenze il Ministro dell'Interno (a capo della struttura operativa SISDe - Servizio civile) e il Ministro della Difesa (a capo della struttura operativa Sismi - Servizio militare). Viene inoltre creato il COPACO (Comitato parlamentare di controllo sui Servizi di Intelligence) per il controllo dell'attività dei due organismi di sicurezza.

- 5 Dal 2006 l'Europol pubblica ogni anno una relazione statistica sugli attentati terroristici e sugli arresti collegati. Cfr. EUROPOL – European Union Agency for Law Enforcement Cooperation, EU Terrorism situation & trend report (TE – SAT).
- 6 In occidente, alla parola *Jihad* viene spesso attribuito un'accezione negativa del suo significato traducendolo in "guerra santa". In realtà il termine significa "sforzo, impegno" e può riguardare una pluralità di significati.
- 7 Cfr. Caligiuri Mario, *Il disagio sociale digitale: da problema di Ordine Pubblico a questione di Sicurezza Nazionale*, in «Formiche», n. 154, dicembre 2019 :« Il cyber spazio è sempre più centrale nella vita sociale, rappresentando, in una certa misura, l'ambito economico prevalente, così come quello politico, comunicativo,

sagio sociale è posto al centro di una articolata analisi sulla sua pericolosità verso la società e le istituzioni democratiche di un paese⁸. E mentre da una parte l'aumento delle diseguglianze sociali, la crisi della democrazia, la precarietà lavorativa, la bassa scolarizzazione, la povertà sono solo alcune delle condizioni che generano e alimentano questo malessere, dall'altra l'utilizzo di internet ne propaga e amplifica a dismisura i suoi effetti più nefasti e disastrosi. Troppo presto, infatti, si è magnificata la grandezza del nuovo mondo – il *cyber space* – dove tutto è libero, tutto è gratis, tutto è democratico. Oggi sappiamo che le cose non sono così semplici e che c'è un prezzo da dover pagare⁹. L'aumento sensibile dei casi di minaccia alla Sicurezza Nazionale legati al disagio sociale¹⁰ dimostra come il problema necessiti di essere affrontato in un modo organico e ampio, non solo monitorando il *cyber space*, dove spesso le attività terroristiche trovano terreno

informativo e finanche educativo. È quindi diventata l'area decisiva dei conflitti, che sono sempre più di natura economica e culturale, combattuti attraverso la guerra delle informazioni sul web».

- 8 Cfr. Caligiuri Mario, *L'avanzata del disagio sociale (e quali rimedi)*, in «Formiche», n. 146, aprile 2019, pp. 38-39.
- 9 Caligiuri Mario, *Il disagio sociale digitale: da problema di ordine pubblico a questione di Sicurezza Nazionale*, op. cit.
- 10 Le analisi condotte dal Council of Europe (2016) si soffermano particolarmente su quegli «individui che si sentono emarginati, maltrattati, socialmente esclusi e cercano disperatamente un senso della vita e un senso di appartenenza sono ad alto rischio di essere radicalizzati, indottrinati dalla propaganda estremista, anche tramite Internet e le reti sociali, e reclutati da gruppi terroristici» e designano un profilo piuttosto definito del soggetto radicalizzato: giovani maschi (anche se la quota femminile è in crescita) con basso livello di istruzione e scarsa conoscenza della religione islamica, disoccupati o con lavori non qualificati, spesso provenienti da famiglie poco abbienti. Cfr. Parliamentary Assembly, - Assembly debate on 27 January 2016 (6th Sitting) (see Doc. 13937, report of the Committee on Political Affairs and Democracy, rapporteur: Mr Dirk Van der Maelen; Doc. 13959, opinion of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Pieter Omtzigt). Text adopted by the Assembly on 27 January 2016 (6th Sitting). See also Recommendation 2084 (2016).

fertile, ma anche individuando gli elementi di pericolosità nei soggetti che possono considerarsi in astratto pericolosi (i disagiati sociali, per stile di vita o per tratti caratteristici della personalità)¹¹ e negli ambienti che ne favoriscono la tendenza criminale (i cosiddetti “luoghi devianti”)¹².

Dagli eventi dell'11 settembre 2001 in poi, gli attentati terroristici sono diventati via via sempre più mediatici ed eclatanti. Cambiano le motivazioni, gli obiettivi e gli antagonisti degli scontri. Le cellule degli attentatori si fanno sempre più piccole, compiono attentati a bassa capacità tecnologica, usano ordigni esplosivi improvvisati (*Improvised Explosive Device* - IED) veicoli lanciati a gran velocità sulla folla, aggressioni fatte con armi leggere o da taglio, attività terroristiche che talvolta sono addirittura realizzate da singoli squilibrati¹³.

11 A questo riguardo ci si può riferire alla classificazione fatta dalla Legge n. 1423 del 27 dicembre 1956 in materia di misure di prevenzione che individua alcune tipologie di persone pericolose per la sicurezza e la pubblica moralità: «vagabondi e oziosi; soggetti dediti a traffici illeciti; soggetti proclivi a delinquere; sospetti sfruttatori di prostitute, contrabbandieri o trafficanti di sostanze stupefacenti; soggetti abitualmente dediti ad attività contrarie al buon costume o alla morale pubblica». Successivamente viene introdotta una legislazione riguardante la pericolosità di soggetti criminali legati alla mafia e al terrorismo. Negli anni '80, una nuova normativa (art. 2 della L. 327/1988) interviene sui criteri di valutazione inerenti il profilo dei soggetti da ritenersi pericolosi: «coloro che sono abitualmente dediti a traffici delittuosi; coloro che vivono abitualmente, anche in parte, con i proventi di attività delittuose; coloro che mettono in pericolo l'integrità fisica o morale dei minorenni, la società, la sicurezza o la tranquillità pubblica». Ulteriori classificazione hanno riguardato le categorie legate alle violenze sportive e alle violenze a sfondo razziale.

12 Secondo la teoria dell'*Ecology Crime* di Rodney Stark ci sono cinque fattori che incidono sulla devianza criminale: la densità della popolazione, la povertà, uso misto (aree urbane dove le zone residenziali sono adiacenti agli spazi commerciali delle città), la transitorietà dei residenti, la disgregazione sociale. Cfr. Stark R., *A Theory of the Ecology of Crime*, in «Criminology», 25 (1987), pp. 891 – 907. Cfr. pure, Saitta Pietro – Rinaldi Cirus, *Devianze e crimine: antologia ragionata di teorie classiche e contemporanee*, PM Edizioni, Varranze (SV), 2017, pp. 145 – 152.

13 Vedi ad esempio: l'attentatore di Oslo, Anders Behring Breivik che nel luglio

La presa di coscienza, da parte di ciascuno Stato, della propria vulnerabilità di fronte a simili attacchi, ha portato ciascun paese ad implementare diverse misure di sicurezza e protezione del proprio territorio, favorendo la creazione di centri di coordinamento e di scambio informativo tra diversi organismi di polizia e di sicurezza. Il fulcro della collaborazione tra le Agenzie di Intelligence e le FF.pp. riguarderà sempre più la minaccia terroristica di matrice pseudo-religiosa.

All'indomani degli attacchi alle *Twin Towers*, anche l'Italia ha adottato una serie di misure urgenti volte a garantire una maggior sicurezza dello Stato e dei cittadini¹⁴. Ma è solo nel 2003 (dopo l'attentato terroristico al contingente italiano a Nassirya) che è nata una struttura unificata contro il terrorismo che prevede una più stretta collaborazione informativa tra Forze di polizia e Servizi di Intelligence, il C.A.S.A. appunto.

Recenti studi del fenomeno terroristico hanno mostrato come le sue diramazioni e le interconnessioni non sono confinate a determinati soggetti e specifiche attività, ma trovano legami più ampi e pericolosi nel mondo della corruzione e della criminalità¹⁵.

Analizzando gli attentati terroristici degli ultimi anni, viene fuori come il mondo del terrorismo sia fortemente collegato a

2011 mise in atto due attacchi terroristici volti a colpire il governo norvegese, o l'attacco di Marsiglia dell'ottobre 2017 nel quale un tunisino irregolare accolteffò fatalmente due giovani studentesse presso la stazione di Saint-Charles.

- 14 Uno dei primi atti intrapresi dallo Stato italiano contro il terrorismo è stato l'approvazione della Legge 438/2001, volta ad adeguare la normativa italiana (revisione dell'art. 270 bis c.p.), sino ad allora orientata alla minaccia del terrorismo interno, alla grave emergenza del terrorismo internazionale.
- 15 Cfr. Shelley L. I., *Dirty Entanglements Corruption, Crime, and Terrorism*, Cambridge University Press, 2014, p.5.

quello della criminalità¹⁶. Non solo alla più feroce criminalità organizzata, fatta di grandi traffici di droga e armi, ma anche - e sempre di più - alla piccola delinquenza urbana (che si nutre di spaccio, contrabbando, contraffazione), alla quale gli apparati di sicurezza occidentali non rivolgono grande attenzione.

Generalmente il legame tra terrorismo e criminalità organizzata viene affrontato erroneamente, come fossero due fattispecie criminali distinte ed indipendenti l'uno dall'altra. Dal dopoguerra ad oggi, invece, ci si è resi conto di quanto il confine tra queste due realtà sia sempre più sottile, sfociando in una pericolosa commistione di attività economiche e obiettivi politici al fine di destabilizzare gli Stati, dando luogo a quelle che alcuni studiosi hanno definito *hybrid threats*¹⁷.

Questa natura sempre più promiscua e pericolosa tra le organizzazioni criminali e terroristiche è stata evidenziata già nel 2009 dal direttore esecutivo dell'UNODC (*United Nations Office on Drugs and Crime*):

oggi il traffico di droga è diventato la causa principale di un altro problema: il finanziamento del terrorismo. È diventato sempre più difficile distinguere chiaramente i gruppi terroristici dalle comuni organizzazioni criminali perché le loro strategie tendono sempre più a sovrapp-

16 Mentre in passato il terrorismo era principalmente finanziato dagli Stati o da potenti organizzazioni politiche, negli ultimi anni questa fonte di finanziamento sembra andare via via erodendosi facendo sorgere la necessità di trovare fonti alternative di sostentamento. Il finanziamento avviene attraverso vari canali, tra cui il traffico di droga, di armi, di reperti archeologici, di sequestri a fini di riscatto e la tratta di esseri umani. Cfr. Maronta F., Caracciolo L., *Criminalità e terrorismo sono due facce della stessa medaglia. Conversazione con Louise Shelley, professoressa e direttrice del Terrorism, Transnational Crime and Corruption Center alla George Mason University (Virginia, Usa)*, op. cit., 2015.

17 Raufer Xavier., *New World Disorder, New Terrorism: New Threats for Europe and Western World*, in «Terrorism and Political Violence» 11, n° 4, 1999, p. 35.

porsi. Se non recidiamo il legame tra crimine, droga e terrorismo, il mondo assisterà alla nascita di un ibrido e cioè di organizzazioni terroristiche della criminalità organizzata¹⁸.

Come l'avvento della guerra asimmetrica ha cambiato lo scenario dello scontro, richiedendo una nuova presa di coscienza per non soccombere alla nuova realtà che si parava dinanzi, così queste nuove minacce ibride, dovute a una mescolanza di relazioni tra corruzione, terrorismo e criminalità¹⁹, richiedono un approccio pragmatico per essere limitate. Al nuovo scenario criminale va ad aggiungersi, come è stato accennato, la minaccia altrettanto insidiosa e pericolosa per la Sicurezza Nazionale che deriva dal disagio sociale, che in un prossimo futuro potrebbe divenire incontenibile.

In un simile contesto non si può pensare di concentrarsi solo su singoli obiettivi. Le minacce sono sempre più numerose ed imprevedibili. Ecco perché una raccolta informativa maggiormente estesa nel campo delle fonti umane ad opera delle FF.pp. potrebbe rivelarsi determinante per intercettare quei famosi "segnali deboli" che spesso non sono riconoscibili dai, seppur potentissimi, sistemi tecnologici.

18 Cfr. Innocenti Piero, Caradonna Mirna, *Il narcotraffico internazionale è il "bancomat" privilegiato dai terroristi: Dalle Farc a Hezbollah, da al Qaida a Boko Haram: dove c'è una lotta armata, c'è il commercio di droga a finanziare il conflitto*, in «Limes», n° 6, luglio, 2015.

19 Cfr. Relazione OCSE: *Terrorism, corruption and the criminal exploitation of natural resources*, Parigi, 2016. Vedi pure Shelley L., *Dirty entanglements: Corruption, crime and terrorism*, op. cit. 2014.

3.2

IL MODELLO INVESTIGATIVO E INFORMATIVO NELL'ATTIVITÀ PRATICA DELLE FF.PP.

Per comprendere se la costruzione del modello teorico ipotizzato possa funzionare, ovvero trasformare ogni operatore delle forze dell'ordine in uno Human Sensor nell'attività di Intelligence di polizia, occorre individuare uno schema di riferimento che tenga conto della prassi e dall'osservazione della realtà come linee guida su cui strutturare un programma formativo indispensabile per implementare le capacità di OES.

A tal fine è stata svolta un'indagine ricognitiva¹ per individuare quali sono gli elementi ripetitivi e significativi in grado di identificare un buon investigatore delle FF.pp., e ricercare quale sia il percorso formativo più efficace per ottenerli. I risultati del sondaggio non solo hanno fornito notizie utili allo scopo, ma hanno permesso di rilevare alcune importanti sfumature riguardanti sia l'esperienza e la pratica investigativa, sia l'attività informativa.

Il modello di studio ha riguardato un campione statistico a *scelta ragionata* concernente alcuni appartenenti delle FF.pp. che svolgono regolarmente e da lungo tempo attività investigative. La somministrazione dei quesiti ha previsto alcune domande aperte volte a raccogliere dati e informazioni

1 Il campione utilizzato ha riguardato un numero di appartenenti alle Forze di polizia suddivisi per area geografica (sud, centro e nord Italia) non particolarmente significativo, ma sufficiente a poter determinare una tendenza.

derivanti dall'esperienza personale di ciascuno.

L'analisi dei report ha descritto intorno a quali caratteristiche (in riferimento a quelle che gli stessi operatori di polizia ritengono essenziali per essere un buon investigatore) si sia maggiormente concentrata la distribuzione di frequenza dei cosiddetti *markers* osservati, indipendentemente dalla provenienza geografica e dall'esperienza di ciascun agente. Gli elementi emersi ci permettono quindi di individuare quali siano gli aspetti fondamentali da dover favorire e da dover ricercare in ogni singolo operatore.

Secondo quanto dichiarato dalla maggior parte degli investigatori, tutti potrebbero assolvere a compiti di OES se debitamente formati, anche i soggetti che non hanno alcuna esperienza o nozione di attività investigativa e informativa. Anzi, la possibilità di poter acquisire questo tipo di capacità tecniche porterebbe addirittura a incentivare una buona parte degli operatori di polizia a svolgere con più entusiasmo il proprio lavoro.

Naturalmente dire che tutti possano implementare capacità di OES nell'attività di Human Sensor dell'Intelligence di Polizia non significa certo che tutti vogliano farlo (specie se si tratta di farlo fuori dal servizio) o che tutti siano in grado di farlo allo stesso modo (e non certo affidandosi soltanto ad un corso di formazione). Ci sono, infatti, molte variabili che concorrono a determinare l'efficacia di un intervento di questo tipo, più volte ribadite dagli stessi intervistati: la validità del corso di formazione, il bagaglio culturale personale, il *background* professionale, l'attitudine a simili attività, le motivazioni, la curiosità, la capacità del sistema di stimolare e di inglobare in modo organico le nuove figure.

Tuttavia, facendo affidamento sulla teoria dei grandi numeri, proprio in considerazione del numero significativo degli appartenenti alle FF.pp., si può affermare che una diffusa formazione in tal senso aumenterebbe di molto le probabilità di poter acquisire informazioni utili non altrimenti acquisibili.

Se si passa, invece, a considerare quali sono le modalità con le quali gli investigatori si sono formati, e quali tra queste abbia maggiormente contribuito a plasmare le loro capacità investigative, la questione diventa davvero interessante.

Il percorso formativo si basa su metodi classici di apprendimento: uno teorico (corsi di formazione; seminari; dispense, codificazioni delle leggi, testi specifici; studio di precedenti attività di indagine); l'altro empirico (esperienza diretta; confronto con altri operatori del settore investigativo/informativo e dell'autorità giudiziaria; condivisione di esperienze).

Ma è la seconda modalità ad essere ritenuta determinante per acquisire competenze e professionalità nel settore. Pur esistendo un'ampia letteratura riguardo il *modus operandi* delle tecniche investigative e informative di polizia, è la conoscenza pratica trasmessa dagli stessi operatori più esperti a fornire gli strumenti più importanti. Una conoscenza pratica che non può essere trasferita in altro modo se non ascoltando, osservando e comprendendo come gli investigatori più abili pensano, agiscono e risolvono le diverse situazioni.

E, come avviene nei *cluster industriali*², più questa cono-

2 In economia con il termine *cluster industriale* si intende una concentrazione di imprese, fornitori e istituzioni strettamente interconnesse in un'area geografica determinata. Il principale *cluster* di innovazione oggi conosciuto è la Silicon Valley. Secondo l'economista Michael E. Porter il *cluster* è «un'agglomerazione geografica di imprese interconnesse, fornitori specializzati, imprese di servizi, imprese in settori collegati e organizzazioni associate che operano tutti in un

scienza è ampia (estesa a diversi ambiti e discipline), profonda (figlia di una grande esperienza maturata nel tempo) e concentrata (racchiusa in un luogo ristretto e tra molti soggetti che ne aumentano di gran lunga le opportunità), più la formazione e l'innovazione garantiranno un vantaggio competitivo.

I *cluster*, infatti, tendono a realizzarsi attraverso agglomerazioni di diversi soggetti in un determinato luogo fisico e consentono l'accesso al massimo flusso di informazioni e idee, opportunità di collaborazione, disponibilità di specialisti e conoscenze. Inoltre, permettono la massima efficienza nell'attività lavorativa, lo sviluppo di *team* specializzati, la riduzione dell'esposizione al rischio degli stessi appartenenti alle FF.pp. e di maggiori opzioni di scelta.

A questo riguardo ci si può riferire allo studio dell'economista Harmaakorpi Vesa³ per comprendere perché alcune

particolare campo, e caratterizzata dalla contemporanea presenza di competizione e cooperazione tra imprese». Cfr. Porter Michael E., *Il vantaggio competitivo delle nazioni*, Einaudi, Torino, 2011.

- 3 Adattando il modello di Harmaakorpi nell'ambito delle FF.pp. è possibile comprendere perché alcuni ambienti lavorativi, a parità di risorse, hanno una maggior capacità informativa, di indagine, di prevenzione, operativa, ecc. Lo studio dell'economista è rivolto allo sviluppo e innovazione dei sistemi regionali partendo dall'analisi degli aspetti tecno-economici e socio-istituzionali di cui il territorio è fatto. «La competitività di una regione si basa sulle configurazioni delle risorse regionali. In un mondo turbolento, queste configurazioni di risorse devono essere rinnovate nel tempo, imponendo richieste di capacità dinamiche regionali. Questo studio sottolinea cinque capacità dinamiche regionali: capacità di leadership, capacità visionaria, capacità di apprendimento, capacità di rete e capacità innovativa. Lo studio assume un punto di vista olistico nella valutazione dell'ambiente di innovazione regionale. Questo ambiente è visto come un sistema di reti e istituzioni di innovazione situate all'interno di una regione, con interazioni interne regolari e forti che promuovono l'innovatività ed è caratterizzato da integrazione. Le innovazioni sono sempre più viste come il risultato di processi non lineari profondamente radicati nelle normali attività sociali ed economiche. La natura non lineare e interattiva dei processi di innovazione pone nuo-

realtà lavorative sono più efficienti, efficaci e innovative di altre. Come i *cluster* industriali fanno scaturire la propria forza dall'efficienza collettiva, ossia dal «vantaggio competitivo che deriva dalla presenza di economie esterne locali e di azioni congiunte»⁴, così i *cluster* culturali⁵ nell'ambito dell'attività investigativa e informativa di polizia, derivano la propria forza dall'efficienza collettiva determinata dall'esistenza *in loco* di un *background* investigativo e da azioni congiunte dei diversi operatori.

Nel quadro delle conoscenze empiriche, ad esempio, uno degli aspetti più rilevanti nel trasferimento di conoscenze ai soggetti neofiti nelle attività informative, riguarda le raccomandazioni sulle modalità di acquisizione di informazioni da fonte umana (vedi tab. 3.2 – A).

Tuttavia, se per comprendere l'importanza del trasferi-

ve richieste di coesione sociale nel sistema di innovazione regionale». Cfr. Harmaakorpi Vesa, *Building a competitive regional innovation environment : the regional development platform method as a tool for regional innovation policy*, Doctoral dissertations series 2004/1, Helsinki University of Technology, Lahti Center, 2004.

- 4 Schmitz J. Hubert, Collective efficiency and increasing returns, in «Cambridge Journal Economic», Oxford University Press, vol. 23(4), July 1999, pages 465-483. Con "economie esterne" ci si riferisce a quei vantaggi al di fuori della singola impresa ma interni al *cluster*, come ad esempio: la presenza in loco di manodopera e fornitori specializzati e la rapida diffusione di conoscenza; con "azioni congiunte", invece, si fa riferimento a quelle forme di collaborazione sia tra singole aziende o gruppi di imprese concorrenti sia con fornitori o clienti. Nella traslitterazione dal modello economico al modello investigativo si può intendere, per economie esterne l'insieme di investigatori di un determinato ufficio e di altri settori e operatori del sistema; per azioni congiunte l'interazione collaborativa tra operatori di uno stesso ufficio, tra più uffici e tra questi ed altre istituzioni dello Stato.
- 5 Qui inteso come la concentrazione di uomini, risorse, competenze professionali e dotazioni culturali che, singolarmente o a sistema, possono essere dirette nel processo di valorizzazione dell'attività investigativa e informativa di polizia.

mento delle conoscenze pratiche si guarda al campo di studi dell'etologia e della gnoseologia, si noterà come gli animali non solo si comportano per istinti e comportamenti innati, ma anche per condizionamenti ambientali e processi di apprendimento. L'etologo austriaco Konrad Lorenz, infatti, riteneva che le performance della conoscenza umana si determinano allo stesso modo del processo evolutivo per la conservazione della specie, ovvero sia in riferimento a «un sistema reale, formatosi in seguito ad un processo naturale» evoluzionistico, sia «in un rapporto interattivo con un altrettanto reale mondo circostante»⁶. Allo stesso modo la stretta interazione tra gli operatori di polizia nel trasferimento della conoscenza pratica può servire a capire come gli individui e gli ambienti siano in grado di influenzarsi reciprocamente.

Ciononostante occorre tener presente che la mancanza di percorsi strutturati e specifici sulla materia, dovuta alla carenza di sufficienti risorse tecniche, logistiche ed economiche, possa aver paradossalmente avvantaggiato oltre misura la formazione del personale investigativo, compensando l'esigenza di acquisizione delle conoscenze e competenze con la più semplice, economica ed efficace modalità disponibile: affiancando operatori esperti e facendo esperienza sul campo.

L'analisi dell'indagine ricognitiva ha evidenziato un altro aspetto fondamentale, riguardo l'attività Humint di Polizia nell'acquisizione di informazioni: rispetto alle diverse attività di raccolta informativa delle FF.pp.⁷, le notizie da fonte uma-

6 Cfr. Konrad Lorenz, *L'altra faccia dello specchio: per una storia naturale della conoscenza*, Adelphi, Milano, 2007.

7 Si fa riferimento alle principali fonti informative delle FF.pp. Vedi tabella 3.2 – B.

na risultano essere decisive. Secondo gli intervistati, infatti, sono proprio le *fonti umane* le principali e più importanti *fonti informative*. Spesso, infatti, le svolte nelle indagini o nuove ipotesi investigative arrivano da informatori, confidenti, testimoni e collaboratori. Naturalmente quando ci si riferisce a questa tipologia di fonte informativa occorre valutarne l'attendibilità e la veridicità⁸.

Sebbene l'utilizzo delle tecnologie moderne abbia permesso un'analisi sempre più elaborata dei dati disponibili, aumentando di gran lunga le capacità di ricerca, aggregazione e catalogazione delle informazioni sino a divenire uno strumento formidabile per comprendere, prevenire, pianificare e reprimere i diversi fenomeni criminali e le possibili connessioni con altri soggetti sociali, l'attività Humint di Polizia resta insostituibile e fondamentale nella raccolta informativa.

8 La valutazione, la gradazione e la disseminazione dell'informazione, si effettuano tramite diversi sistemi di *cross evaluation*. A questo riguardo sia le FF.pp. che i Servizi di Intelligence utilizzano alcuni modelli per la valutazione e comprensione dell'affidabilità della fonte informativa e la veridicità delle notizie raccolte. Vedi tabella 3.2 – C / 3.2 – D sul metodo di valutazione delle informazioni: *Sistema 4x4 Europol*; *Sistema 6x6 DEA*.

Tabella 3.2 – A

ALCUNE INDICAZIONI SULLE MODALITÀ DI ACQUISIZIONE DI INFORMAZIONI DA FONTE UMANA E GESTIONE DELLA RISORSA PIÙ VOLTE RIBADITE DAGLI STESSI INVESTIGATORI DI POLIZIA	
1	<i>Mettere a proprio agio la fonte in modo da infondere fiducia</i>
2	<i>Attendibilità della fonte</i>
3	<i>Riscontro delle informazioni</i>
4	<i>Non fidarsi delle prime informazioni</i>
5	<i>Valutare quale sia il tornaconto della fonte e perchè rivela una determinata informazione</i>
6	<i>Annotazione delle informazioni su un taccuino</i>
7	<i>Incontro con la risorsa in coppia</i>
8	<i>Parlare poco e lasciar parlare la fonte</i>
9	<i>Dire meno di quello che si sa</i>
10	<i>Condurre la conversazione</i>
11	<i>Non rendersi ricattabili</i>
12	<i>Non farsi coinvolgere emotivamente</i>
13	<i>Non cercare di raggiungere un obiettivo a tutti i costi</i>
14	<i>Non influenzare la fonte dandogli informazioni</i>
15	<i>Assicurare la riservatezza della fonte non rivelando l'identità a terzi</i>
16	<i>Dare riscontro formale (relazionando) i propri superiori</i>

Tabella 3.2 – B

FONTI INFORMATIVE delle FF.pp.	
FONTI	TIPOLOGIA
Aperte	OSINT – open source intelligence
Tecnologiche	SIGINT – signals Intelligence; IMINT – imagery Intelligence COMINT – communications Intelligence; ELINT – electronic Intelligence CYBINT – cyber Intelligence
Umane	HUMINT – human source intelligence: Informatore; confidenti; testimoni; collaboratori; agente sotto copertura; persona interposta.
Documentali	-BANCHE DATI - ATTI FF.pp. ATTI PROCESSUALI
Chiuse	Fonti documentali subordinate a vincoli di riservatezza.

VALUTAZIONE DELLE INFORMAZIONI
Sistema 4x4 (Europol)

Tabella 3.2 – C

ATTENDIBILITÀ FONTE	A	Sempre affidabile
	B	Quasi sempre affidabile
	C	Quasi mai affidabile
	D	Affidabilità non verificata
VERIDICITÀ DELL'INFORMAZIONE	1	Accuratezza indubbia
	2	Notizia nota solo alla fonte
	3	Non nota alla fonte ma riscontrata da esterno
	4	Notizia non verificabile

FONTE

- A Fonte per la quale non sussistono dubbi circa l'autenticità, l'affidabilità o la competenza, oppure informazione fornita da una fonte che, in passato, ha dimostrato di essere affidabile in tutti i casi.
- B Fonte dalla quale l'informazione pervenuta si è dimostrata affidabile nella maggior parte dei casi.
- C Fonte dalla quale l'informazione pervenuta non si è dimostrata affidabile nella maggior parte dei casi.
- D Fonte la cui affidabilità non può essere valutata.

INFORMAZIONE

- 1 L'informazione è ritenuta sicura senza alcuna riserva.
- 2 L'informazione è conosciuta personalmente dalla fonte, ma non conosciuta personalmente dall'agente che la fornisce.
- 3 L'informazione non è conosciuta personalmente dalla fonte, ma è avallata da altre informazioni già registrate.
- 4 L'informazione non è conosciuta personalmente dalla fonte e non può essere avallata in alcun modo

VALUTAZIONE DELLE INFORMAZIONI
Sistema 6x6 (DEA – *Drug Enforcement Administration*)

Tabella 3.2 – D

ATTENDIBILITÀ FONTE	A	Completamente affidabile.
	B	Normalmente affidabile.
	C	Abbastanza affidabile.
	D	Di solito non affidabile.
	E	Non affidabile.
	F	Non Classificabile.
VERIDICITÀ INFORMAZIONE	1	Confermata.
	2	Probabilmente vera.
	3	Possibile.
	4	Poco attendibile.
	5	Improbabile.
	6	Non classificabile.

FONTE

- A Assoluta mancanza di dubbi circa l'autenticità della fonte. Rivelatasi completamente affidabile.
- B Esiste qualche dubbio sull'autenticità, affidabilità e competenza della fonte anche se, in passato si è rivelata nella maggior parte dei casi affidabile.
- C Di solito da adito a dubbi sull'autenticità, affidabilità e competenza della fonte. In passato alcune informazioni si sono dimostrate affidabili.
- D Sussistono dubbi sulla autenticità, affidabilità e competenza della fonte. Occasionalmente affidabile in passato.
- E Esistono grossi dubbi sull'autenticità, affidabilità e competenza della fonte. In passato ha fornito informazioni non affidabili.
- F Non è possibile esprimere alcun giudizio perché la fonte non è conosciuta.

INFORMAZIONE

- 1 Confermata da altre fonti. Logica di per sé. Concorda con altre informazioni qualificate sullo stesso argomento.
- 2 Non confermata. Logica di per sé. Concorda con altre informazioni qualificate sullo stesso argomento.
- 3 Non confermata. Logica nel ragionamento. Concorda in qualche punto, con altre informazioni sull'argomento.
- 4 Non confermata. Non illogica. Non creduta al momento della valutazione sebbene possibile.
- 5 È confermato il contrario. Illogica. Contraddetta da altre informazioni sull'argomento.
- 6 Non è possibile giudicare l'informazione.

Nota esplicativa

Mentre la valutazione e la gradazione dell'informazione serve a stabilire il livello della sua attendibilità (ad esempio, nel sistema 4x4, il livello A1 indica un'altissima affidabilità della notizia), per la disseminazione dell'informazione, invece, ci si serve di un sistema che attribuisce un codice a seconda del destinatario partendo dalla meno riservata 1 sino ad arrivare a quella più riservata 6 (ad esempio, un'informazione con codice 1 potrebbe essere disponibile per tutti gli operatori di Polizia, mentre una valutata 6, solo per gli operatori che si occupano di un tipo particolare d'investigazioni).

Un livello di attendibilità A2 - 1 sta a significare che la fonte è sempre affidabile, l'informazione sperimentata e conosciuta dalla fonte ma non dall'operatore e può essere disseminata a tutte le agenzie di Polizia.

3.3

L'IMPORTANZA DELLO HUMAN SENSOR NEI NUOVI SCENARI DEMOGRAFICI E TECNOLOGICI

Nei prossimi decenni, due saranno i fattori che agiranno con maggior forza nei cambiamenti sociali, economici e politici del pianeta: l'aumento della popolazione mondiale; la pervasività della tecnologia in tutti gli ambiti della vita umana.

L'ultimo rapporto delle Nazioni Unite del 2019 ha confermato le stime di crescita della popolazione mondiale che passeranno dagli attuali 7,7 miliardi agli 8,5 miliardi del 2030 e ai 9,7 miliardi del 2050, per arrivare, entro la fine del secolo, a quasi 11 miliardi di abitanti (10,9 miliardi nel 2100)¹.

E mentre i paesi occidentali avranno una decrescita sempre più marcata e costante, con un incremento sostanziale degli over 65², continenti come l'Asia, in parte l'America Latina

1 United Nations, Department of Economic and Social Affairs, Population Division (2019). *World Population Prospects 2019: Highlights* (ST/ESA/SER.A/423), New York, 2019.

2 La popolazione del globo sta invecchiando rapidamente. Mentre nel 2019 la percentuale degli ultra sessantacinquenni è del 9%, nel 2050 sarà pari al 16%. Cfr. Morgan Steve, *Come sarà la Terra quando saremo 10 miliardi*, in «Limes», n° 10, agosto, 2019.

ed in particolare l'Africa vedranno un aumento significativo della propria popolazione con un'età media di gran lunga inferiore. La sola Nigeria, ad esempio, nel 2050 avrà una popolazione di circa 411 milioni di abitanti (più del doppio di quella attuale), laddove l'intera Europa non supererà i 716 milioni³ (un numero addirittura inferiore a quello censito oggi). La demografia del XXI secolo, quindi, segnerà il progressivo declino del Vecchio Continente. Uno scenario, questo, che determinerà uno stravolgimento degli assetti economici, politici e sociali di molti paesi.

L'aumento demografico della popolazione mondiale, i cambiamenti climatici, le guerre e le carestie, porteranno inevitabilmente masse sempre più consistenti di esseri umani a spostarsi dalle campagne alle città e da un paese ad un altro in cerca di migliori condizioni di vita. Per di più, l'idea di poter raggiungere l'agognata "terra promessa" viene ulteriormente alimentata dall'utilizzo, sempre più diffuso nei paesi del terzo e del quarto mondo⁴, della rete internet che, facendo rimbal-

3 United Nations, Department of Economic and Social Affairs, Population Division (2017). *World Population Prospects: The 2017 Revision, Key Findings and Advance Tables*. Working Paper No. ESA/P/WP/248, New York, 2017, pp. 23; 26. (per le stime di crescita vedi tabella 3.3 – A1/A2/A3)

4 Simoncelli Lorenzo, *Internet in Africa: i giganti del web alla guerra dei cavi*, in «la Repubblica - Affari e Finanza», 3 agosto 2019: «Dal 2000 ad oggi, l'Africa è il Continente che è cresciuto di più per numero di connessioni ad Internet. In

zare in ogni computer e in ogni *smartphone* immagini e filmati dell'opulenza delle grandi città, ne aumenta la portata.

Basti ricordare l'effetto che ebbero gli spot pubblicitari trasmessi dalla televisione italiana sulla popolazione albanese all'indomani del crollo del regime comunista. L'8 agosto del 1991, la nave da carico *Vlora*, con 20.000 profughi a bordo ammassati come fossero formiche, entrò nelle acque territoriali italiane attraccando al porto di Bari⁵. Il collasso economico del paese, la grave penuria di cibo e una diffusa incertezza politica e sociale indussero molti albanesi, sino ad allora isolati dal resto del mondo, a fuggire e tentare la sorte in altri paesi, alcuni per sottrarsi alla fame altri inseguendo la libertà.

La maggior parte di loro aveva come meta l'Italia non solo perché poco distante, ma anche per le molte aspettative che creava, alimentate da quegli spot pubblicitari che inducevano a credere, erroneamente, di poter arrivare in un paese ricco e felice, dove la gente comprava addirittura del cibo per i propri animali domestici, mentre loro dall'altra parte dell'Adriatico non avevano nulla di che sfamarsi. Se una semplice trasmissione

vent'anni è passata da 4,5 milioni di utenti a 525 milioni, quasi tutti giovani under 35 che si collegano alla Rete più con gli *smartphone* che con i pc. Nonostante la crescita, in Africa, il tasso di penetrazione di Internet tra la popolazione è ancora il più basso al mondo».

5 Cfr. Redazione, *Invasione – Senza speranze: ponte aeronavale per rimpatriarli*, in «Gazzetta del Mezzogiorno», anno CIV – n. 198, 9 agosto 1991.

televisiva ha potuto infondere queste prospettive, bisogna immaginare cosa può determinare l'accesso alla rete internet nei molti paesi in via di sviluppo.

Lo studio dei fenomeni migratori degli ultimi decenni ha evidenziato uno spostamento consistente di popolazioni che dalle campagne si sono riversate nelle città. E sono proprio queste ultime a dover subire un cambiamento radicale nel proprio aspetto e nella loro stessa identità, divenendo sempre più una enorme periferia, una *non-città*. Secondo alcuni studiosi,

«le *megacities* sono destinate a succedere agli Stati quali soggetti geopolitici principali. Megalopoli che detengono una quota decisiva del Pil nazionale e si profilano come *hub* globali grazie al peso economico, alla capacità di attrarre investimenti, alla connessione con i centri omologhi [...] Oggi nel mondo ci sono molte più città funzionali di quanti siano gli Stati effettivi. Tali città sono spesso isole di *governance* e ordine in Stati molto più deboli. Le megacittà sono indifferenti ai fragili Stati che le circondano»⁶.

Le città tradizionali sembrano lentamente sprofondare in

6 Barile Alessandro, *Indagine sulle periferie*, in «Limes» n°4, maggio, 2016.

una sterminata e disordinata periferia generata dalla sua natura abusiva (da una parte si edifica abusivamente, dall'altra i piani regolatori servono ormai solo a ratificare quanto già costruito) divenendo così uno smisurato insediamento urbano che separa la "città legittima" (quella storica) e la "città funzionale" (quella dove si concentrano le attività economiche più importanti, dove ci si incontra, si studia e si lavora) dagli immensi sobborghi, che emarginati dai processi di valorizzazione pubblica si trasformano in ghetti sociali, sempre più meticcici e sempre meno integrabili e rappresentabili politicamente.

«In Italia la metamorfosi urbanistica della città di Roma serve bene come modello negativo di riferimento. La capitale è infatti una città abnorme, sproporzionata alle sue necessità e alla sua popolazione: 1287 kmq, contro i 105 kmq di Parigi o i 785 kmq di New York. Una città dove vivono meno di tre milioni di persone, facendone una delle grandi città meno densamente popolate del mondo. Una contraddizione generata dalla natura abusiva della sua espansione: un terzo del territorio comunale è nato illegalmente, un territorio più grande dell'intero comune di Napoli è di fatto abusivo, ma è anche quella porzione di territorio dove oggi risiede la maggior parte della popolazione romana. E allora, Roma può definirsi ancora una città? La realtà dei fatti mette in relazione piuttosto due città, antitetiche e ostili tra loro: un centro storico quantitativamente minuscolo rispetto al resto del territorio amministrato dal Comune, ma dove si concentrano tutti i flussi economici cittadini, dai proventi del turismo globale alle funzioni di rappresentanza econo-

miche e amministrative comunali, a cui va aggiunta la prima cintura (semi)periferica nel frattempo integrata nella città legittima; e una sterminata periferia che inizia ai margini del Grande raccordo anulare (un tempo vero e proprio *limes* cittadino) e prosegue per chilometri oltre, in pieno ex agro romano oggi completamente cementificato e (sub)urbanizzato. Una periferia che però non detiene alcuna compattezza o unità, se non derivata sociologicamente dalla sua marginalizzazione economica, culturale e politica. Bisognerebbe parlare allora di periferie, al plurale, perché questi insediamenti urbani non comunicano reciprocamente, sono distanti dal centro tanto quanto fra di loro»⁷.

Periferie senza frontiere etniche, che inglobano mescolanze di identità spurie, dove sono i residenti autoctoni ad avvicinarsi alle condizioni di vita dei migranti e non viceversa. La difficoltà ad integrarsi di milioni di abitanti delle periferie produrrà forme autonome di integrazione, spingendo una parte di questi emarginati o disadattati sociali a trovare un senso di appartenenza e di riscatto nel radicalismo religioso o nelle organizzazioni criminali.

In questi ultimi anni, oltre alla questione migratoria, si è verificato un altro fenomeno importante: l'avvento di internet che, con i suoi innumerevoli riflessi in molti ambiti della vita

7 Barile Alessandro, *Indagine sulle periferie*, Op. Cit.

umana, ha prodotto un profondo e radicale cambiamento della società, stravolgendo ogni concetto sin qui conosciuto riguardante le interazioni dell'uomo con se stesso e con il mondo circostante.

Un aumento consistente e pervasivo delle tecnologie (in particolare di quelle informatiche e digitali) che investono sempre più non solo la sfera militare, economica e politica di molti paesi, ma anche quella privata delle persone. Basti pensare, ad esempio, all'IoT (*Internet of Things*)⁸, dove tutto è collegato ed interconnesso in rete, pronto a inviare e ricevere dati utili ad analizzare, gestire e controllare intere città, aziende, trasporti, amministrazioni di pubblica utilità, edifici o qualsiasi cosa si voglia connettere⁹. Un'enorme quantità di dati (i *Big Data*)¹⁰ che dematerializza il mondo fisico riconducendolo

8 Il termine "*Internet of Things*" (IoT) è stato proposto nel 1999 dall'ingegnere inglese Kevin Ashton per descrivere un sistema in cui gli oggetti nel mondo fisico possono essere connessi a Internet attraverso sensori.

9 IoT è solo una parte dell'IoE (*Internet of Everything*). Quest'ultima, infatti, collega persone, processi, dati e cose in modo da rendere le connessioni in rete più pertinenti e preziose che mai, trasformando le informazioni in azioni che creano nuove capacità, esperienze più ricche e opportunità economiche senza precedenti per le aziende, individui e paesi (Cisco, 2013).

10 «I *Big Data* sono l'asset informativo caratterizzato da un volume, una velocità e una varietà così elevati da richiedere specifici metodi analitici e tecnologici per la sua trasformazione in valore». De Mauro A., Greco M., Grimaldi M., *A formal definition of Big Data based on its essential features*, in «Library Review», Vol. 65 n° 3, 2016, pp. 122 - 135.

in forme computabili dai quali è possibile estrapolare e conoscere ogni genere di informazione. Un volume di dati che aumenta anno per anno in modo esponenziale¹¹ sollevando così numerosi dubbi su chi materialmente dispone di questi dati e su come decide di servirsene o di renderli disponibili ad altri. Una questione questa di non poco conto¹².

Le possibili applicazioni dall'evoluzione dell'IoT sono davvero innumerevoli e di grande importanza, in particolare modo se le si riferisce alla Sicurezza Nazionale e alla lotta alla criminalità organizzata. Ad esempio, la possibilità di poter acquisire una quantità e una varietà enorme di dati provenienti dalle cosiddette *smart city* (a partire dal controllo e gestione del trasporto pubblico, dall'identificazione di animali domestici e persone, dall'autenticazione, dal monitoraggio del traffico, ecc.) permette sia ai Servizi di Sicurezza e sia alle Forze di polizia di poter predisporre di informazioni di conte-

11 Vedi tabella 3.3 – B

12 «Un'indagine del New York Times e del Guardian, dopo mesi di verifiche e trattative con le fonti, ha scoperto che Cambridge Analytica – una società di analisi dei dati che ha collaborato con il team elettorale di Donald Trump e con altre campagne controverse come quella a favore della Brexit – ha raccolto i dati personali di oltre 50 milioni di utenti di Facebook (soprattutto americani) in una delle più grandi violazioni della *policy* del gigante tecnologico. Questi dati sarebbero stati utilizzati per costruire un potente software che sarebbe in grado di prevedere e influenzare le scelte all'urna. Per quanto non sia del tutto sorprendente (è da tempo che si parla dei social network come un rischio potenziale per le democrazie) il caso ha sollevato un grande dibattito». Cfr. *Cos'è il caso Cambridge Analytica?*, in «Il Foglio» 19 Marzo 2018.

sto utili ad un'analisi delle questioni sempre più dettagliata, ampia ed efficace.

Un esempio estremo di simili sistemi è dato dall'utilizzo dell'intelligenza artificiale adottata dalla Cina. Nei data base del governo cinese, infatti, finiscono ogni genere di dati: immagini e filmati delle telecamere sparse per le città e dotate di sistemi di riconoscimento facciale, transazioni delle carte di pagamento, spostamenti in auto, tracciati telefonici, carte fedeltà dei supermercati, dati catastali delle abitazioni, sino alle cartelle cliniche dei pazienti. Uno dei maggior investimenti ha riguardato proprio l'uso dell'intelligenza artificiale per il riconoscimento facciale. Già nel 2016 erano presenti sul territorio 176 milioni di telecamere di sorveglianza ed entro il 2020 si stima che ne verranno installate altre 450 milioni¹³. Un sistema talmente efficace da poter ricostruire con notevole precisione gli spostamenti e le attività svolte di chiunque negli ultimi sette giorni e localizzare un uomo tra una folla di sessantamila persone¹⁴.

Naturalmente si comprende bene la portata di queste nuove tecnologie nell'ambito della sorveglianza e del control-

13 Cfr. Tremolada L., *Cina, quando la sorveglianza è globale: sotto controllo 1,3 miliardi di persone*, in «lsole24ore», 15 aprile 2018.

14 Notizia riportata nell'articolo: *Chinese man caught by facial recognition at pop concert*, in «BBC News» del 13 aprile 2018.

lo del territorio e, allo stesso tempo, la necessità di intelligenze umane in grado di predisporre questi potenti software per processare e analizzare i dati e le informazioni raccolte.

Tuttavia occorre considerare che, nonostante la prospettiva di una società sempre più tecnologica e artificiale tenda addirittura a determinare in modo predittivo i comportamenti umani, l'uomo sarà sempre in grado di sottrarsi e aggirare i diversi sistemi di controllo, come più volte dimostrato. Anzi, proprio l'estrema pervasività della tecnologia con la quale stiamo fasciando il mondo reale potrebbe rivelarsi alla fine un *boomerang* dal quale dover trovare riparo. Un mondo tecnologico dominato da una raccolta dati incredibilmente grande e impossibile da gestire se non con potenti microprocessori e complessi software, dove la memoria storica è sempre più orwelliana¹⁵, le informazioni manipolabili, i dati non verificabili, le relazioni umane surrogate, dove tutto è immagine e la "cultura scritta" una breve ed effimera citazione.

15 Nel racconto di George Orwell, *1984*, un impiegato del Partito Esterno che lavora presso gli uffici del Ministero della Verità, è incaricato di "correggere" i libri e gli articoli di giornale già pubblicati, modificandoli in modo da rendere riscontrabili e veritiere le previsioni fatte dallo stesso Partito. Egli inoltre si occupa di modificare la storia scritta, contribuendo così ad alimentare la fama di infallibilità del Partito stesso, applicare le *damnatio memoriae* verso dissidenti "mai esistiti". «Chi controlla il passato controlla il futuro. Chi controlla il presente controlla il passato». Orwell G., *1984*, Mondadori, Milano, 2004, p. 38.

Il sovraccarico di informazioni, ad esempio, resta uno dei problemi di non poco conto che potrebbe determinare il fallimento dell'attività di Intelligence, come accadde alle agenzie americane nel 2001: pur disponendo di diversi elementi per prevenire il complotto non furono in grado di "congiungere i diversi punti" che avrebbero creato il quadro di insieme dell'attentato terroristico.

Robert David Steel, uno dei maggiori esperti mondiali del sistema di Informazione e Sicurezza americana, aveva previsto il fallimento dell'Intelligence strategica internazionale anni prima dei fatti dell'11 settembre, elencando e motivando le ragioni che avrebbero portato a questo risultato: l'eccesso di tecnologia nella raccolta dei dati è il primo punto¹⁶.

In un simile panorama quindi, il riporre una cieca fiducia nei sistemi tecnologici per garantire la Sicurezza Nazionale e nella lotta alla criminalità organizzata potrebbe significare ancora una volta¹⁷ non tener conto della natura estremamente

16 I sei punti di debolezza dell'Intelligence internazionale indicati da Steel sono: «1) eccesso di tecnologia nella raccolta dei dati; 2) inadeguata raccolta clandestina, fondamentalmente limitata alle fonti aperte; 3) gravi inadeguatezze nella gestione delle risorse; 4) inerzia mentale aggravata da inerzia organizzativa; 5) mancanza di credibilità del direttore dell'acquisizione se risulta non essere adeguatamente informato sulle tecnologie e le contromisure; 6) nessun coinvolgimento nei confronti della popolazione». Cfr. Steel Robert David, *Intelligence – Spie e segreti in un mondo aperto*, Rubbettino Editore, Soveria Mannelli, 2002, p. 81.

17 Prima dell'attacco alle *Twin Towers*, le agenzie di Intelligence di mezzo mondo, in particolare quelle americane, avevano destinato gli sforzi e le risorse maggiori ad implementare sistemi tecnologici SIGINT (vedi lo sviluppo del programma

complessa dell'uomo e della sua capacità di adattarsi ai mutamenti che lo circondano, pronto a mettere in atto misure e contromisure per essere fuori dalla portata e dal controllo di una società sempre più tecnologica.

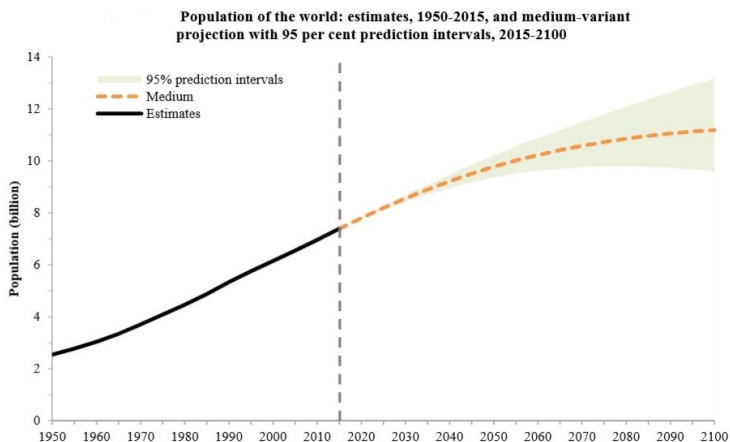
E' in questo contesto che l'attività di Human Sensor, rivolto alla salvaguardia della Sicurezza Nazionale e alla lotta alla criminalità organizzata, trova la sua ragion d'essere. Un esercito di sensori umani sparsi su tutto il territorio e capaci di attivarsi autonomamente, muoversi, vedere e ascoltare in città sempre più grandi e sovrappopolate, dove le tecnologie più sofisticate non potranno interpretare le numerose e complesse sfumature dei comportamenti umani.

AUSCANNZUKUS conosciuto dal grande pubblico come "Echelon" sviluppato da una cordata di 5 paesi: Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti) incentrati sull'intercettazione e la raccolta delle comunicazioni private e pubbliche.

Tabella 3.3 - A1				
POPULATION OF THE WORLD AND REGIONS, 2017, 2030, 2050 AND 2100 ACCORDING TO THE MEDIUM-VARIANT PROJECTION				
<i>Population (millions)</i>				
<i>Region</i>	<i>2017</i>	<i>2030</i>	<i>2050</i>	<i>2100</i>
World	7 550	8 551	9 772	11 184
Africa	1 256	1 704	2 528	4 468
Asia	4 504	4 947	5 257	4 780
Europe	742	739	716	653
Latin America and the Caribbean	646	718	780	712
Northern America	361	395	435	499
Oceania	41	48	57	72

Source: United Nations, Department of Economic and Social Affairs, Population Division (2017).
World Population Prospects: The 2017 Revision. New York: United Nations

Tabella 3.3 – A2

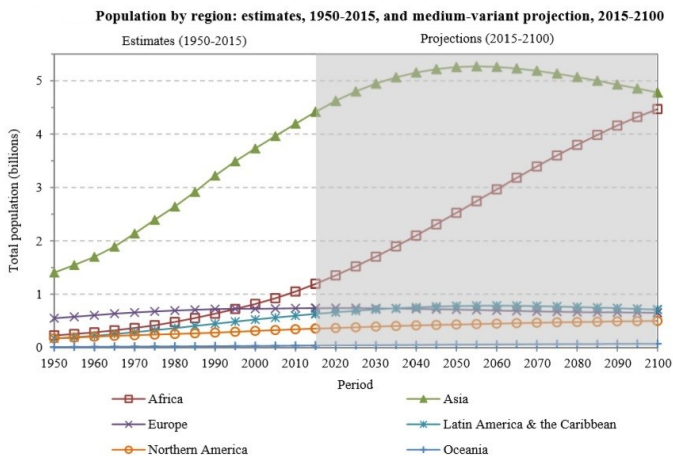


Source: United Nations, Department of Economic and Social Affairs, Population Division (2017).
 World Population Prospects: The 2017 Revision. New York: United Nations.

United Nations Department of Economic and Social Affairs/Population Division
 World Population Prospects: The 2017 Revision, Key Findings and Advance Tables

Tabella 3.3 – A3

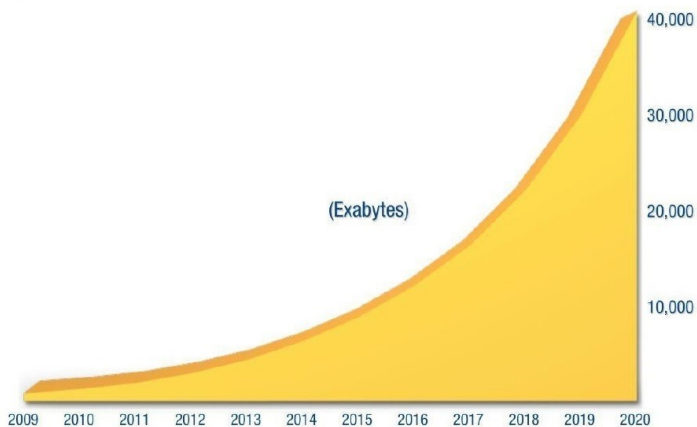
2050 than in 2017. Beyond 2050, Africa will be the main contributor to global population growth.



Source: United Nations, Department of Economic and Social Affairs, Population Division (2017).
 World Population Prospects: The 2017 Revision. New York: United Nations.

Tabella 3.3 – B

Tendenza dei Dati creati dal 2009 al 2020



Questo grafico mostra la crescita esponenziale dei *dati globali* partendo dai circa 3 zettabyte del 2013 sino ai circa 40 zettabyte previsti entro la fine del 2020. Un exabyte equivale a 1.000.000.000.000.000.000 byte, e 1.000 exabyte equivalgono a 1 zettabyte. Fonte: Digital Universe Study – IDC.

CONCLUSIONI

I mutamenti politici, economici e sociali degli ultimi trent'anni hanno prodotto profondi e rapidi cambiamenti nelle vite delle persone e degli Stati. La fine della divisione del mondo in due blocchi, la Guerra del Golfo, l'11 settembre 2001, la globalizzazione, l'avvento di internet e delle nuove tecnologie di comunicazione, la destabilizzazione politica di molti paesi, la crisi delle democrazie, l'ascesa economica e commerciale cinese, la rinascita militare russa, i cambiamenti climatici, le carestie, l'aumento della popolazione mondiale, i fenomeni migratori di massa, le sconfiniate periferie cittadine estranee ad ogni possibile integrazione: un mondo, il nostro, che sembra sfuggire ad ogni governabilità e controllo possibili.

Oggi sembra si stiano ripetendo gli stessi errori che nel recente passato hanno portato gli apparati di Intelligence internazionale a fallire le previsioni fatte a causa dell'eccessiva fiducia riposta nei sistemi tecnologici.

Secondo alcuni addetti ai lavori, la falla principale dei Servizi di Intelligence internazionale degli ultimi anni consiste nella scarsa capacità di interpretare e decifrare i cosiddetti "segnali deboli", causata dalla mancanza di bravi analisti in grado di collegare i famosi puntini. Questo in parte potrebbe essere vero. Nella società moderna, infatti, la cultura sembra sempre più orientata all'iper-specializzazione, in cui

ciascuno sa tutto di un determinato settore o materia, ma nulla di tutto il resto: in tal modo, è diventato arduo il compito di decifrare la complessità del mondo, di saper guardare lontano e a largo campo, proprio perché siamo abituati a vedere in solo punto e da vicino le cose.

Il problema principale, tuttavia, potrebbe trovarsi altrove. La capacità di catalogazione, aggregazione e analisi dei dati disponibili (una quantità ormai impressionante da dover gestire) non è sempre sufficiente a poter determinare una corretta previsione o predizione degli scenari che si vogliono comprendere, se non si dispone di una buona raccolta informativa. Spesso, infatti, mancano proprio quelle informazioni di contesto che sfuggono ai sofisticati sistemi tecnologici, come più volte dimostrato, ponendo la necessità di dover essere acquisite con l'attività *Humint* direttamente sul campo, come aveva già fatto notare Robert David Steel.

Se da una parte l'attività di Intelligence è - e sarà - rivolta ad implementare l'utilizzo di potenti software che raccolgono e analizzano l'enorme massa di dati inviati da un mondo sempre più connesso in rete, dall'altra ci sarà bisogno di presidiare quelle periferie, quelle zone d'ombra, quegli ambienti o quegli individui che tenderanno ad escludere la tecnologia dalle proprie attività criminali e terroristiche. Luoghi, questi, dove potrebbero più facilmente annidarsi pericoli alla Sicurezza Nazionale o alla Sicurezza Pubblica.

Naturalmente non è possibile monitorare, controllare o sorvegliare un ambito così esteso e disordinato sia per le scarse risorse finanziarie e sia per il numero elevato di obiet-

tivi. Una possibile soluzione, invece, potrebbe venire proprio da una diversa visione dell'impiego delle FF.pp., addestrandole come Human Sensors alla raccolta di informazioni di contesto provenienti dai molteplici scenari locali nei quali ciascun operatore è quotidianamente e naturalmente immerso.

Si disporrebbe in questo modo di una formidabile forza nell'attività informativa. Un esercito già addestrato, numeroso, disseminato su tutto il territorio e senza costi da dover sostenere, pronto ad attivarsi autonomamente. Un'attività, questa, che aumenterebbe di molto le *chance* dell'Intelligence di polizia e dell'Intelligence Istituzionale di poter acquisire informazioni utili al contrasto della criminalità organizzata e alla salvaguardia della Sicurezza Nazionale.

GLOSSARIO

GLOSSARIO

Humint (Istituzionale)	Human Intelligence – È la disciplina di Intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione.
Humint di polizia	È quell'attività svolta dalle FF.pp. che si occupa principalmente di trovare tutte le informazioni e le fonti di prova possibili su fatti penalmente rilevanti. È costituita da quel flusso informativo che include le notizie dei confidenti, degli informatori e degli stessi poliziotti, le dichiarazioni spontanee su fatti e persone di gente comune, le attività di sorveglianza, i rapporti e i verbali delle attività di sicurezza.
Human Sensor (ES2)	È un metodo di raccolta informativa adottata in contesti operativi estremamente cangianti e imprevedibili fatta da soldati non particolarmente addestrati nell'attività di Intelligence ma pronti a servire, oltre che come combattenti, anche come "sensori umani" per rilevare qualsiasi notizia utile del contesto tattico in cui si opera.
Intelligence led policy	Polizia diretta dai metodi di Intelligence o polizia dell'informazione. E' un modello di polizia che inquadra tutte le principali attività di polizia (contrasto della criminalità organizzata, terrorismo, traffici di droga, dell'immigrazione, controllo del territorio) in modo più efficiente (in termini di ottimizzazione delle risorse impiegate) e più efficace (in termine di risultati) grazie ad una adeguata analisi preventiva dei fenomeni criminali. Un approccio, quindi, che postula una stretta integrazione tra attività di Intelligence e attività di polizia in cui l'analisi dei dati, sono fondamentali per un quadro decisionale.
Intelligence (Istituzionale)	È lo strumento con cui lo Stato, per mezzo dei suoi Servizi di Informazione per la Sicurezza, raccoglie, analizza, custodisce e dissemina (ai soggetti interessati) informazioni e dati utili al processo decisionale del governo in tema di Sicurezza Nazionale e Interesse Nazionale.
Intelligence di polizia	È l'attività con cui, le forze dell'ordine, raccolgono, analizzano e diffondono le informazioni ai livelli superiori o all'autorità giudiziaria o di governo. Si tratta del processo informativo declinato attraverso le tre fasi principali in funzione di una triplice direzione, in base alla natura delle informazioni elaborate o richieste (organi superiori interni, autorità giudiziaria, autorità politica).
OES (Osservazione, Elicitazione, Sorveglianza)	È quell'attività umana propedeutica alla raccolta di notizie e informazioni utili all'attività di Intelligence, investigativa e di controllo del territorio.

BIBLIOGRAFIA

- Aprile Pino, *Elogio dell'imbecille. Gli intelligenti hanno fatto il mondo, gli stupidi ci vivono alla grande*, Ed. Piemme, Milano, 2012.
- Barron John M., Berger Mark C., Black Dan A., *On-the-Job Training*, W.E. Upjohn Institute for Employment Research, Kalamazoo, Michigan, 1997.
- Bartel, A.P. *Productivity gains from the implementation of employee training programs*. *Industrial Relations*, Vol. 33(4), 1994.
- Bauman Zygmunt, *La solitudine del cittadino globale*, Feltrinelli Editore, Milano, 2004.
- Bertaccini Davide, *Polizia professionale – Polizia di comunità – Polizia dei problemi – Polizia dell'ordine – Polizia di prossimità*, Maggioli Editore, Santarcangelo di Romagna, 2011.
- Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, Il Mulino, Bologna, 2010.
- Bocchiaro Pietro, *Psicologia del male*, Editori Laterza, Bari, 2010.
- Chabris Christopher, Simons Daniel, *Il gorilla invisibile. E altri modi in cui le nostre intenzioni ci ingannano*, Gruppo 24 ore, Milano, 2012.
- Chomsky Noam, *Capire il potere*, Marco Tropea Editore, Milano, 2002.
- Chomsky Noam, *Egemonia americana e "Stati fuorilegge"*, Edizioni Dedalo, Bari, 2001.
- Chomsky Noam, Herman Edward S., *La fabbrica del consenso, ovvero la politica dei mass media*, Marco Tropea Editore, Milano, 1998.
- Clausewitz Karl von, *Della Guerra*, Arnoldo Mondadori, Milano, 2000.
- Colombo Emilio, *Stanca Luca, The Impact of Training on Productivity: Evidence from a Large Panel of Firms*, Working Papers from University of Milano – Bicocca, No 134, Department of Economics, Milano, 2008.

- Cossiga Francesco, *Abecedario per principianti, politici e militari, civili e gente comune*, Rubettino Editore, Soveria Mannelli, 2002.
- Dawkins Richard, *Il gene egoista. La parte immortale di ogni essere vivente*, Arnoldo Mondadori Editore, Milano, 2011.
- de Kok Jan M.P., *The Impact of Firm - provided training on production: testing for firm - size effects*, Tinbergen Institute Discussion Paper, Netherlands, 2000.
- Gagliano Giuseppe, *Guerra psicologica – Saggio sulle moderne tecniche militari cognitive e di disinformazione*, Fuoco Edizioni, Rende, 2013.
- Giannulli Aldo, *Come funzionano i servizi segreti*, Ponte alle Grazie, Milano, 2013.
- Giupponi T. F., *Servizi di informazione e forze di polizia dopo la legge n. 124/2007 – contributo per il Gruppo di lavoro di Astrid*, 20 maggio 2009.
- Harmaakorpi Vesa, *Building a competitive regional innovation environment: the regional development platform method as a tool for regional innovation policy*, Doctoral dissertations series 2004/1, Helsinki University of Technology, Lahti Center, 2004.
- Hauser Marc D., *Menti Morali. Le origini naturali del bene e del male*, Il Saggiatore, Milano, 2007.
- Hobsbawm Eric J., *Il secolo breve, 1914-1991: l'era dei grandi cataclismi*, Rizzoli Editore, Milano, 2000.
- Illuminati G., *Nuovi profili del segreto di Stato e dell'attività di Intelligence*, G. Giampichelli Editore, Torino, 2010.
- Izzi S., *Intelligence e gestione delle informazioni – Attività preventiva contro i traffici illeciti*, Ed. Franco Angeli, Milano, 2011.
- Jean Carlo, *Manuale di studi strategici*, CSGE, Ed. Franco Angeli, Milano, 2017.
- Kautilya, *Il codice del potere. L'arte della guerra e della strategia indiana*, Ed. Il Punto d'Incontro, Vicenza, 2011.
- Konings Jozef, Vanormelingen Stijn, *The Impact of Training on Productivity and Wages: Firm Level Evidence*, The Institute for the Study of Labor, Discussion Paper No. 4731, Bonn, 2010.

- Konrad Lorenz, *L'altra faccia dello specchio: per una storia naturale della conoscenza*, Adelphi, Milano, 2007.
- Lynch Lisa M., *Training and the Private Sector*, University of Chicago Press, 1994.
- Macchiavelli Niccolò, *Il Principe*, Biblioteca Universale Rizzoli, Milano, 1995.
- Major Jeffrey C. Schrick, *Effective Intelligence In Urban Environments*, Edit. Tannenber Pickle Partners Publishing, 2015.
- Montanelli Indro, Cervi Mario, *L'Italia degli anni di piombo, 1965 – 1978*, Rizzoli - Corriere della Sera, Milano, 2011.
- Mosca C., Gambacurta S., Scandone G., Valentini M., *I Servizi di Informazione e il Segreto di Stato (Legge 3 agosto 2007, n.124)*, Giuffrè Editore, Milano, 2008.
- Orwell G., *1984*, Mondadori, Cles, 2004
- Parkinson Cyril North, *La legge di Parkinson*, Monti & Ambrosini, Pescara, 2011.
- Pisani Vittorio, *Informatori, notizie confidenziali e segreto di polizia*, Giuffrè Editore, Milano, 2007.
- Popper R. Karl, *Cattiva maestra televisione*, Marsilio Editori, Venezia, 2006. Cfr. pure Sartori Giovanni, *Homo videns*, Editori Laterza, Bari, 2007.
- Qiao Liang, Wang Xiangsui, *Guerra senza limiti – L'arte della guerra asimmetrica tra terrorismo e globalizzazione*, LEG Edizioni, Gorizia, 2002.
- Ratcliffe Jerry H., *Intelligence-Led Policing*, Willan Publishing, Cullompton – UK, 2008
- Saitta Pietro – Rinaldi Cirus, *Devianze e crimine: antologia ragionata di teorie classiche e contemporanee*, PM Edizioni, Varrazze (SV), 2017.
- Sawyer Ralph D. (a cura di), *Cento strategie non ortodosse*, Neri Pozza Editore, Vicenza, 2000.
- Schmitt, Carl, *Dialogo sul potere*, Il Melangolo, Genova, 1990.
- Singh Simon, *Codici & Segreti – La storia affascinante dei messaggi segreti dall'antico Egitto a Internet*, RCS Bur saggi, Milano, 2015.

Steel Robert David, *Intelligence – Spie e segreti in un mondo aperto*, Rubbettino Editore, Soveria Mannelli, 2002.

Sun Tzu, *L'arte della Guerra*, Oscar Mondadori, Milano, 2008.

Wynne-Edwards V. C., *Animal dispersion in relation to social behavior*, Oliver and Boyd, Edinburgh 1962.

Altre Fonti

Ansoff I.H., Le risposte strategiche ai "segnali deboli", in «Sviluppo e organizzazione», fasc. 33, 1976.

Barile A., Indagine sulle periferie, in «Limes» n. 4, maggio 2016.

Black S. E., Lynch L. M., Human. Capital Investments and Productivity, in «The American Economic Review», vol. 86, n. 2, Papers and Proceedings of the Hundredth and Eighth Annual Meeting of the American Economic Association San Francisco, CA, January 5-7, 1996 (May, 1996).

Bonini C., Terrorismo, il nuovo schema di Minniti: "Sindaci e polizia locale ci aiuteranno a fermare i lupi solitari", in «la Repubblica», 22 dicembre 2016.

Caligiuri M., L'avanzata del disagio sociale (e quali rimedi), in «Formiche», n. 146, aprile 2019.

Caligiuri M., Predictive Policing. Il futuro della sicurezza è nei modelli di prevenzione, convegno regionale, Napoli, 24 maggio 2019.

Caligiuri M., La rivoluzione che verrà. Come il disagio sociale digitale minaccia la sicurezza nazionale, allegato, in «Formiche», n. 153, dicembre 2019.

Charbonnier A., L'Intelligence Service apre gli archivi del MI5, in «GNOSIS. Rivista italiana di Intelligence», aprile 2009.

De Mauro A., Greco M., Grimaldi M., A formal definition of Big Data based on its essential features, in «Library Review», Vol. 65 n. 3, 2016.

Fittipaldi E., Troppo Divise, in «L'Espresso», n° 2, anno LXI, 15 gennaio 2015.

Giansoldati F., Papa Francesco: Il comunismo ci ha rubato la bandiera, in «Il Messaggero», 29 giugno 2014.

Innocenti P., Caradonna M., Il narcotraffico internazionale è il "bancomat" privilegiato dai terroristi: Dalle Farc a Hezbollah, da al Qaida a Boko Haram: dove c'è una lotta armata, c'è il commercio di droga a finanziare il conflitto, in «Limes», n° 6, luglio, 2015.

- Kfir I., Israel's Approach to Counterterrorism, in «The Strategist (ASPI - The Australian Strategic Policy Institute)», 27 settembre, 2018.
- Loeb V., Instead of Force, Friendly Persuasion, in «The Washington Post», 5 Novembre 2003.
- Maronta F., Caracciolo L., Criminalità e terrorismo sono due facce della stessa medaglia, Conversazione con Louise Shelley, professoressa e direttrice del Terrorism, Transnational Crime and Corruption Center alla George Mason University (Virginia, Usa), in «Limes», n. 11, dicembre 2015.
- Morgan S., Come sarà la Terra quando saremo 10 miliardi, in «Limes», n. 10, agosto, 2019.
- Raufur X., New World Disorder, New Terrorism: New Threats for Europe and Western World, in «Terrorism and Political Violence» 11, n° 4, 1999.
- Redazione, Bush: finiti i combattimenti in Iraq, in «Corriere della Sera», 2 maggio, 2003.
- Redazione, Cos'è il caso Cambridge Analytica?, in «Il Foglio» 19 Marzo 2018.
- Redazione, Invasione. Senza speranze: ponte aeronavale per rimpatriarli, in «Gazzetta del Mezzogiorno», anno CIV, n. 198, 9 agosto 1991.
- Rilling J., Gutman D., Zeh T., Pagnoni G., Berns G., Kilts C., A neural basis for social cooperation, in «National Center for Biotechnology Information, U.S. National Library of Medicine», Atlanta 2002.
- Schmitt E., Shanker T., Bombings in London: Hearts and Minds. U.S. Officials Retool Slogan for Terror War, in «The New York Time». 26, July, 2005.
- Schmitz J.H., Collective efficiency and increasing returns, in «Cambridge Journal Economic», Oxford University Press, vol. 23(4), July 1999.
- Shelley L.I., Dirty Entanglements Corruption, Crime, and Terrorism, in «Cambridge University Press», 2014.
- Simoncelli L., Internet in Africa: i giganti del web alla guerra dei cavi, in «la Repubblica. Affari e Finanza», 3 agosto 2019.
- Stark R., A Theory of the Ecology of Crime, in «Criminology», 25 (1987).
- Tremolada L., Cina, quando la sorveglianza è globale: sotto controllo 1,3 miliardi di persone, in «la Repubblica», 15 aprile 2018.

INDICE DEI NOMI

Africa, 104, 105, 115, 116
America, 13, 22, 103, 115, 116
America Latina, 103, 116
Ansoff H. Igor, 61
Aprile Pino, 61
Aristotele, 52
Ashton Kevin, 109
Asia, 103, 115, 116
Australia, 114
Azzolini Giulio, 12
Baghdad, 29, 40
Balacava, 51
Barcellona, 62
Bari, 105
Bartel P. Ann, 78
Batson Daniel, 71
Barile Alessandro, 106, 108
Barron John, 77
Bauman Zygmunt, 11
Beane Billy, 26
Beck Ulrich, 9
Berger Mark C., 77
Berlino, 32, 62
Berns Gregory S., 70
Bishop John, 77
Black Dan A., 77
Black Sandra, 77
Boca Stefano, 68, 69, 71, 74
Bocchiaro Piero, 68, 69, 71, 72, 74
Bonini Carlo, 62

Brand Peter, 26
Breivik Anders Behring, 87
Brooker Charlie, 23
Buchanan Lyn, 13
Bush George, 38
Caligiuri Mario, 10, 11, 12, 13, 17, 48
85, 86
Caltanissetta, 59
Camilleri Andrea, 16
Canada, 114
Caracciolo Lucio, 81, 89
Caradonna Mirna, 90
Caraibi, 115, 116
Chabris Christopher, 23
Chicago, 12
Cina, 111
Colombo Emilio, 79
Crimea, 51
Cuneo, 59
Darley John, 71
Darwin Charles, 67
Dawkins Richard, 69
De Mauro Andrea, 109
Dick Philip K., 12
Europa, 85, 104, 115, 116
Faverzani Camillo, 16
Fiore Paolo, 11
Firenze, 59
Fittipaldi Emiliano, 59
Gagliano Giuseppe, 11
Galli Giorgio, 11
Gambacurta Stefano, 47
Genovese Kitty, 72

Germani Luigi Sergio, 10
Germania, 9, 12
Gerusalemme, 36
Giansoldati Franca, 22
Gori Umberto, 10
Greco Marco, 109
Grimaldi Michele, 109
Gromyko Andrej, 52
Gutman David A., 70
Hamilton William, 69
Harari Yuval Noah, 16
Harmaakorpi Vesa, 94, 95
Hauser Marc D., 69
Heslov Grant, 13
Innocenti Piero, 90
Iraq, 37, 38
Israele, 34, 35
Italia, 7, 9, 10, 12, 27, 47, 57, 59
84, 88, 91, 105, 107
Izzi S, 49
Jean Carlo, 32
Kane Chris, 39, 40
Kautilya, 52
keith Alexander, 10
Kfir Isaac, 35
Kilts Clinton D. , 70
Kissinger Henry, 52
Lanfranca Dario, 16
Lawrence Wright, 9
Lewis Monroe Michael, 26
Lissoni Alfredo, 13
Lombardo Elia, 12
Londra, 12

Lorenz Konrad, 96
Los Angeles, 12
Lynch Lisa M., 77
Lyon David, 11
Macchiavelli, 52
Magi Gianluca, 52
Maronta Fabrizio, 81, 89
Marsiglia, 88
Mc Kiernan J. Brian, 40
Metternich W. N. L. Klemens, 52
Milano, 12, 59
Mini Fabio, 31
Minniti Marco, 62
Monti Mario, 11
Morgan Steve, 103
Mosca Carlo, 47
Naim Moisés, 16
Napoli, 12, 107
Nassiriya, 27, 88
Nehru Jawaharlal, 52
Neumann John von, 73
New York, 107
Nigeria, 104
Nizza, 62
Nuova zelanda, 114
Oceania, 115, 116
Omtzigt Pietre, 86
Orwell George, 112
Oslo, 87
Ostrander Sheila, 13
Pagnoni Giuseppe, 70
Papa Francesco, 22

Parigi, 107
Parkinson Northcot, 60, 61
Patton Michael S., 37
Popper Karl R., 22
Porter Michael E., 93, 94
Qiao Liang, 31, 38
Ratcliffe Jerry H, 28
Reglan Fitzroy Somerset, 51
Regno Unito, 114
Reimer Dennis J., 42, 44
Rilling James K., 70
Rinaldi Cirus, 87
Roma, 59, 107
Rosling Hans, 15
Russia, 13, 27, 57
Saddam Hussein, 37, 40
Saitta Pietro, 87
Sartori Giovanni, 22
Scaffidi-Abbate Costanza, 68, 69, 71, 74
Scandone Giuseppe, 47
Schmitt Carl, 60
Schmitt Eric, 33
Schmitz J. Hubert, 95
Schroeder Lynn, 13
Shanker Thom, 33
Shelley Louise I., 81, 88, 89, 90
Simoncelli Lorenzo, 104
Simons Daniel, 23
Spagna, 47
Spielberg Steven, 12
Stanca Luca, 79
Stark Rodney, 87

Stati Uniti d'america, 32, 37, 38, 39, 43, 52, 114
Steel Robert David, 113, 119
Sun Tze, 52
Terzi di Sant'Agata Giulio, 11
Teti Antonio, 13
Thorndike Edward Lee, 66
Tremolada Luca, 111
Trento, 12
Trisolini Marcello, 13, 17
Trump Donald, 110
Turchia, 27, 57
Unione Europea, 57
Unione Sovietica, 52
Valentini Marco, 13, 47
Van der Maelen Dirk Leo, 86
Venezia, 12
Vernon Loeb, 37, 40
Vlora, 105
Walsingham Francis, 51
Wang Xiangsui, 31, 38
Wertherbach Eckart, 15
West Poit, 39
WYNNE-EDWARDS VERO COPNER, 68
XAVIER RAUFER, 89
Zeh Thorsten R., 70
ZUBOFF SHOSHANA, 11

Ringraziamenti

Questa pubblicazione non sarebbe stata possibile senza la disponibilità ed il contributo di conoscenza ricevuto dai numerosi appartenenti alle Forze di polizia, esperti in investigazione e controllo del territorio, che hanno prestato il proprio tempo nel rispondere ai diversi quesiti posti, utili sia all'indagine statistica e sia alla comprensione della realtà che li circonda.

Si ringrazia il Prefetto dott. Marco Valentini per la cortese disponibilità dimostrata nel seguire tutte le fasi della ricerca, dando numerosi suggerimenti e spunti di approfondimento.

Un particolare ringraziamento, va ai miei cari amici Prof. Marco Mottola e il Dott. Egisto Scalini per la preziosa collaborazione fornita durante la preparazione e lo sviluppo del presente lavoro.

Si ringraziano, infine, tutti coloro che a vario titolo non hanno mai fatto mancare il proprio sostegno.

Publicato nel mese di dicembre 2020
SOCINT *Press*
c/o Università della Calabria, Cubo 18-b, 7° piano via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia

L'Intelligence ha bisogno di competenze umane, perché esercita la logica, la razionalità, il pensiero. In questa originale e argomentata pubblicazione si delinea la figura dello Human Sensor nell'attività di Intelligence di polizia. La proposta di questa professionalità può essere considerata la nuova frontiera nella raccolta delle informazioni, come sperimentato con successo dall'esercito americano nella seconda Guerra del Golfo. Si tratta, infatti, di intercettare i "segnali deboli" che poi possono diventare travolgenti non solo per l'ordine pubblico ma anche per la sicurezza nazionale. Pertanto, potrebbe risultare decisiva una formazione specifica che sviluppi le tecniche di osservazione e sorveglianza delle Forze di polizia. Con questi strumenti umani si possono affrontare sia i problemi vecchi, come la criminalità organizzata, che quelli nuovi, come il disagio sociale.

(dalla prefazione di Mario Caligiuri)



9 791280 111135

