Giuseppe Galetta

# Il modello Osint in ambito militare: dinamiche di open/closed access nel trattamento dell'informazione a fini strategici

**(doi: 10.53227/108474)**

Rivista di Digital Politics (ISSN 2785-0072)
Fascicolo 2, maggio-agosto 2023

**Ente di afferenza:**
*()*

Giuseppe Galetta

# Il modello Osint in ambito militare: dinamiche di *open/closed access* nel trattamento dell'informazione a fini strategici

**THE OSINT MODEL IN THE MILITARY CONTEXT: OPEN/CLOSED ACCESS DYNAMICS IN THE INFORMATION PROCESSING FOR STRATEGIC PURPOSES**

In this historical moment, characterized by a resurgence of conflicts throughout the world, the upheaval of geopolitical balances, but above all by the war in Ukraine, access to open sources is proving to be of absolute strategic importance for the military sector. The defense and national security needs of states, combined with rapid advancements in artificial intelligence, are reshaping the field of military intelligence, which now increasingly relies on advanced information analysis tools, with the aim of gaining a strategic advantage over the enemy. In a hybrid warfare scenario, where the war fought on the battlefield is accompanied by the information war, full control of information is fundamental to achieve informational supremacy over the adversary. The use of Open-source intelligence (Osint) in the military context is extremely varied: threat assessment, field operation planning, enemy movements analysis, data collection on their offensive and defensive capabilities, assessment of collateral damages, monitoring of activities of terrorist groups and international criminal organizations, forecasting sabotage actions on sensitive targets, peacekeeping operation planning. Since this is a highly complex scenario, but still without an adequate theoretical framework, this article aims to develop a reference model capable of illustrating the open sources processing dynamics by the military organizations, which exploit open data following specific procedures.

**KEYWORDS** *Osint, Cyberwarfare, Information Warfare, Military Intelligence.*

Giuseppe Galetta, Università degli Studi di Napoli Federico II – Area Risorse Umane – Via G. C. Cortese, 29 – 80133 Napoli, email: giuseppe.galetta@unina.it, orcid: 0000-0003-4780-1326.


ISSN 2785-0072

## 1. Introduzione

L'*Open source intelligence* (Osint) in ambito militare è una tecnica di raccolta di informazioni da fonti pubbliche a supporto dei processi decisionali delle catene di comando, in grado di determinare l'esito delle operazioni sul campo di battaglia (Akhgar *et al.* 2017). Dato l'attuale momento storico, caratterizzato dal riaccendersi di conflitti in ogni parte del mondo e dallo stravolgimento degli equilibri geopolitici internazionali, l'accesso alle fonti aperte si sta rivelando della massima importanza strategica per il settore militare (Ackerman 2006). Infatti, la necessità di difesa e sicurezza nazionale dei vari Paesi, unita ai rapidi progressi dell'Intelligenza artificiale (Ia), stanno riconfigurando il settore dell'*intelligence* militare (Bean 2011), che ora ha bisogno di nuovi analisti, capaci di filtrare e incrociare le informazioni, appurando l'attendibilità delle fonti allo scopo di tradurre i dati grezzi (*raw data*) in decisioni strategiche, in grado di salvare vite umane, confondere il nemico o decidere le sorti di un conflitto: «I conflitti futuri ruoteranno intorno alla ricerca di conoscenza. Con la crescente rapidità delle comunicazioni e dei flussi di dati a seguito dello sviluppo tecnologico, i conflitti futuri saranno decisi da coloro i quali avranno la capacità di raccogliere, analizzare e diffondere *intelligence* nella maniera più efficace ed efficiente» (Toffler 1980). Sin dal 1990, grazie ad una massiccia diffusione delle tecnologie digitali all'interno degli apparati militari di tutto il mondo, si è assistito ad uno spostamento delle guerre moderne dal *battlefield* al *cyberwarfare* e ad un incremento nell'utilizzo delle fonti aperte a supporto delle attività decisionali da parte delle catene di comando, allo scopo di acquisire la supremazia informativa sul nemico ed un vantaggio strategico sul campo di battaglia, come descritto in numerosi studi sull'evoluzione digitale dei sistemi d'*intelligence* militare (Arquilla e Ronfeldt 1993; Simmons 1995; Zarca 1995; Friedman 1998; Rapetto e Di Nunzio 2001; Davies 2005; Jeffson 2005; Glassman e Kang 2012; Gruters e Gruters 2018).

Poiché l'Osint militare presenta particolari caratteristiche distintive, si è cercato di sviluppare un modello teorico in grado illustrare le dinamiche di trattamento dell'informazione aperta da parte degli apparati militari, che sfruttano le fonti aperte seguendo particolari procedure, codificate in specifici manuali nel rispetto della dottrina militare e delle indicazioni degli stati maggiori (Taylor 2005; Johnson 2006; Smith *et al.* 2017; Connor *et al.* 2021). Per giungere all'elaborazione di un modello generale di Osint in ambito militare è stata utilizzata una metodologia di ricerca basata sullo studio di caso. Tuttavia, è bene precisare che, data la natura sensibile delle operazioni militari, i casi specifici di Osint militare sono spesso classificati o non resi pubblici, per cui un'analisi dei casi empirici può avvenire solo alla conclusione delle operazio-

ni militari o al momento della declassificazione delle fonti (Armistead 2004; Andrew *et al.* 2020), quando appare chiaro in che modo sono state utilizzate le informazioni e quale è stato l'impatto generato sul campo, ossia ripercorrendo il percorso compiuto dall'informazione attraverso vari punti nodali, identificati da diversi stadi (o sistemi) di trasformazione. Come si vedrà, si tratta di uno schema dinamico, di natura puramente informazionale e trasmissiva, dove l'informazione viene «spostata» dagli attori da un punto ad un altro all'interno di un circuito multisistemico integrato (Shannon 1948). Dato che il modello proposto si concentra unicamente sulle dinamiche di trasmissione dell'informazione, non si è affrontata un'analisi dei processi di significazione: infatti, l'attribuzione di senso alle fonti aperte è frutto del lavoro d'*intelligence* degli analisti militari, che determina le decisioni strategiche sul campo da parte delle catene di comando (Ziółkowska 2018).

Poiché i casi esaminati – ricavati da fonti ufficiali e verificate, da piattaforme Osint e dai bollettini di *intelligence* delle forze armate dei paesi coinvolti a vario titolo nella guerra in Ucraina – hanno evidenziato delle ricorrenze nelle modalità di gestione delle fonti aperte da parte dell'*intelligence* e delle catene di comando, si è deciso di analizzare il percorso dell'informazione all'interno dello specifico ecosistema informativo militare, a partire dalla selezione della fonte aperta da parte degli analisti sino all'utilizzo dell'informazione stessa a fini decisionali da parte dei comandi, con l'obiettivo di giungere all'elaborazione un modello teorico di riferimento in grado di spiegare le complesse dinamiche dell' Osint militare, ma anche di contribuire a tracciare un quadro di riferimento circa le opportunità e i rischi legati all'utilizzo delle fonti aperte in un ambito cruciale per l'esistenza degli Stati moderni, quello della difesa e della sicurezza militare, che, per quanto riguarda l'Italia, rappresenta uno dei pilastri tecnico-operativi della strategia di cybersicurezza nazionale (Clarke e Knake 2010; Acn 2022; Borriello e Fristachi 2022; Pdcm 2023).

Il modello teorico presentato in questo lavoro – che utilizza i principi del modello matematico della comunicazione di Shannon-Weaver (Shannon e Weaver 1949) – offre le basi per un'ingegnerizzazione epistemica dell'Osint militare, nel tentativo di chiarire i meccanismi di funzionamento dell'informazione nei moderni scenari di guerra ibrida, dove i dati provenienti da fonti aperte subiscono complessi processi di trattamento e trasformazione, ma anche una deliberata manipolazione, in base alle mutevoli strategie dei comandi militari (Mascella e Lattanzio 2008; Bazzell 2023). Si tratta di uno scenario molto complesso, ma ancora privo di un adeguato inquadramento teorico: data l'evoluzione tecnologica delle tecniche di estrazione dei dati da fonti aperte da parte degli addetti all'*intelligence*, una sistematizzazione delle varie fasi del processo in un modello integrato potrebbe rivelarsi utile per le scienze strategiche, con-

tribuendo ad una migliore comprensione di uno scenario che sta diventando sempre più complesso e rilevante per la difesa e la sicurezza degli Stati, considerato il crescente utilizzo della tecnologia Ia nell'analisi ed estrazione dei dati da fonti aperte in ambito militare (Best 2011; Casanovas 2017). Pertanto, le domande di ricerca cui si è cercato di rispondere attraverso l'elaborazione di un modello teorico di Osint militare sono le seguenti: è possibile tracciare il percorso dell'informazione dal momento della sua acquisizione da fonti aperte fino al suo utilizzo finale sul campo di battaglia? Quali sono le modalità di trattamento dei dati aperti in base alle finalità strategiche? Quali sono gli attori coinvolti nel processo informativo? Qual è il ruolo giocato dalle fonti aperte in uno scenario operativo per sua natura caratterizzato dalla chiusura e classificazione dei dati, quale quello militare? Quali sono le trasformazioni che l'informazione subisce nel corso del ciclo dell'*intelligence*? Ed infine, qual è il suo utilizzo pratico a fini strategici?

Per ottenere una risposta a tali domande, giungendo alla teorizzazione di un modello di Osint militare di riferimento, è stata utilizzata una metodologia di ricerca basata sull'analisi di casi empirici tratti direttamente dai teatri operativi in Ucraina, attraverso la consultazione di piattaforme di *Open source intelligence* (in particolare, la mappa interattiva *Eyes on Russia*), i report pubblicati da autorevoli fonti d'informazione (come i bollettini dei comandi militari), nonché i manuali di *Open source intelligence* ad uso della Nato, che evidenziano i processi di analisi e trattamento dell'informazione aperta a fini decisionali (fase di *intelligence*) ed il successivo utilizzo strategico sul campo di battaglia da parte dei centri di comando (fase operativa). Applicando il modello matematico della comunicazione di Shannon-Weaver al ciclo dell'*intelligence* delle fonti aperte, è possibile individuare il percorso compiuto dall'informazione dal momento dell'acquisizione da fonti aperte sino al suo utilizzo strategico sul campo: si è evidenziato che l'informazione passa attraverso una serie di stadi (o sistemi) di trasformazione, ciascuno dei quali caratterizzato da una specifica tipologia di trattamento dei dati. Alla fine, si è tradotto tale processo in un modello teorico di Osint militare, in grado di rispondere alle suddette domande di ricerca.

## 2. Tipologie e caratteristiche dell'Osint militare

In ambito militare, la definizione di Osint comunemente accettata in dottrina è quella di una metodologia di analisi strategica basata sulla individuazione (*discovery*), selezione (*discrimination*), distillazione (*distillation*) e diffusione (*dissemination*) di informazioni non classificate, ovvero liberamente

accessibili, utilizzate a supporto dell'attività di decision-making da parte delle catene di comando: si tratta delle cosiddette «four Ds», ossia le quattro fasi del ciclo dell'*intelligence* militare applicata alle fonti aperte, codificate dalla dottrina Nato (Nato Saclant 2001; 2002b; Jardines 2002; Minniti e Ciriello 2006; Steele 2006; Centoducati 2016). Tale metodologia, tuttora in costante evoluzione, dati i progressi dell'Ia e l'evolversi delle nuove tecnologie di analisi semantica ed inferenziale dei dati, sfrutta un'ampia varietà di fonti aperte (*all-source intelligence*), la cui numerosità richiede una rapida classificazione (Markowitz 2003; Teti 2015; 2020): fonti umane (Humint); social media (Socmint); intercettazione di comunicazioni e segnali (Sigint); immagini fotografiche acquisite tramite sensori ottici, a infrarosso, multi-spettro, radar e satellitari (Imint); misurazione, rilevazione, tracciamento e identificazione delle firme radar, chimiche, biologiche e radiologiche da fonti fisse o dinamiche, come la rilevazione della presenza di velivoli stealth (Masint); *intelligence* geospaziale (Geoint); *intelligence* elettronica e strumentale (Elint); *intelligence* nucleare (Nucint); *intelligence* degli infrarossi (Irint); *intelligence* del campo acustico, ossia di suoni, onde vibrazioni presenti nell'atmosfera (Acoustint) o nell'acqua (Acint); *intelligence* radar (Radint); *intelligence* telemetrica (Telint); *intelligence* delle comunicazioni (Comint); *intelligence* dei segnali delle strumentazioni avversarie (Fisint); *intelligence* dell'attività radiologica e nucleare non-intenzionale (Rint); identificazione degli obiettivi dell'avversario attraverso diverse metodologie di acquisizione dei dati sul campo, come l'impiego di droni, webcam, o le videocamere GoPro montate sui caschi dei soldati impegnati in azione (Tarint); informazioni di natura bio-scientifica, bio-medica, epidemiologica, ambientale utili alla salvaguardia della salute delle truppe (Medint).

L'utilizzo dell'Osint in ambito militare è, quindi, molto vario: valutazione delle minacce, pianificazione delle operazioni sul campo, analisi dei movimenti delle truppe del nemico e raccolta dei dati sulle sue capacità offensive e difensive, individuazione delle postazioni di tiro dell'artiglieria e dei veicoli militari sul campo, verifica dei bersagli colpiti, valutazione dei danni collaterali, monitoraggio delle attività di gruppi terroristici e delle organizzazioni criminali internazionali, previsione delle azioni di sabotaggio su obiettivi sensibili, pianificazione delle operazioni di peacekeeping, smascheramento di *false flag operations* (Turbeville *et al.* 1999; Williams e Blum 2018). In un simile scenario, caratterizzato da elevata complessità e rischiosità, l'utilizzo di fonti aperte (ovvero non classificate) in ambito militare potrebbe apparire alquanto contraddittorio, in quanto le necessità di segretezza e copertura delle operazioni sul campo, impongono che l'attività decisionale da parte delle catene di comando non possa essere basata su informazioni aperte, ossia liberamente accessibili da chiunque (Burke 2007; Hulnick 2002; 2010; Bazzell 2023). Infatti,

per poter raggiungere gli obiettivi militari, le informazioni acquisite da fonti aperte devono essere strategicamente manipolate, creando disinformazione e disseminando falsi indizi, con l'obiettivo di ingannare e depistare il nemico (Vero 2005; Bianchi 2009).

L'intensità crescente delle minacce a livello internazionale e le esigenze di coordinamento tra gli Stati, se da un lato richiedono l'accesso e la condivisione delle informazioni tra i paesi alleati – riducendo i livelli di *clearance* e la necessità di autorizzazioni e nulla osta di sicurezza (Nos) per l'accesso ai dati aperti (Osd, *Open source data*) – dall'altro implicano l'esigenza di proteggere le fonti da cui sono state ricavate informazioni cruciali per l'attività decisionale delle catene di comando (Madill 2005; Gill e Phythian 2006). Pertanto, è sulle dinamiche di *open/closed access* delle fonti aperte che si misura l'efficacia strategica del modello Osint in ambito militare: infatti, date le finalità strategiche del trattamento delle informazioni aperte, dopo aver raccolto e analizzato i dati utili alla presa di decisioni, è necessario proteggere il vantaggio acquisito chiudendo o oscurando l'accesso alle fonti aperte, alzando cortine fumogene allo scopo di confondere le analisi dell'avversario, spingendolo a commettere errori di valutazione o a prendere decisioni sbagliate. L'accesso alle fonti aperte deve essere quindi chiuso, secretato, classificato dagli stessi analisti che, ponendo barriere all'ingresso, fungono da *gatekeeper* del sistema informativo: i dati vengono deprivati del loro valore informativo, rendendoli inaffidabili e inutilizzabili per il nemico. Si tratta del gioco delle parti tipico dei servizi di *intelligence* e *counterintelligence* militari, una partita a scacchi dove è cruciale la manipolazione dell'informazione (Cia 1993; Barbato 1996; Vero 2005; Colonna Vilasi 2011), ma il contesto operativo è decisamente diverso rispetto al passato, in quanto mediato dalle nuove tecnologie e dalle potenzialità dei sistemi di Ia, in grado di simulare o costruire realtà virtuali e parallele, aventi lo stesso statuto di veridicità della realtà reale (Evangelista *et al.* 2020). Il pericolo delle false informazioni diffuse per ingannare, depistare o confondere il nemico, richiede massima cautela ed accurate verifiche: infatti, anche l'avversario sta raccogliendo informazioni da fonti aperte, mettendo in atto lo stesso gioco. Tutto ciò implica la rottura della blockchain informativa e la deliberata disseminazione di disinformazione a fini strategici o di propaganda (Chiais 2008; 2009).

La strategia dell'imprevedibilità, dell'ambiguità e dell'incertezza, tipica delle *Psyops* e delle operazioni di *intelligence* sotto copertura, impone la necessaria chiusura delle fonti aperte che hanno condotto ad una decisione strategica con effetti operativi sul campo, disseminando false tracce nella Rete a vari livelli di profondità (*surface*, *deep* e *dark web*) e modificando strategicamente la narrazione degli eventi (*data storytelling*) attraverso l'utilizzo di tecniche già sperimentate dall'*intelligence* tradizionale, quali la disseminazione coperta

e l'intossicazione ambientale (Gagliano 2012; Giannuli 2012; Pdcm 2013). Per depistare il nemico, le informazioni acquisite da fonti aperte devono essere offuscate e declassate allo status di disinformazione ai danni dell'avversario: i dati vengono manipolati per produrre strategicamente l'effetto desiderato, preservando il valore delle informazioni distillate dalle fonti aperte ed utilizzate nell'attività di decision-making da parte dei centri di comando, generando un effetto di spiazzamento semantico per l'avversario (decodifica aberrante): in altre parole, bisogna disinnescare il potere dell'informazione aperta corrompendola, rendendola incerta, evanescente, difficilmente rintracciabile e decifrabile, rompendo la catena di valore dei dati utili ai fini decisionali, confondendoli e inabissandoli nel *deep web*, dove però anche il nemico è attivo. In questa «zona grigia» e incerta, l'informazione si trasforma in una *smart weapon*, un'arma intelligente che, se ben gestita, può decretare le sorti di una guerra che sta diventando sempre più ibrida e disumanizzata: accanto alla guerra guerreggiata esiste infatti una *information warfare* (Libicky 1995; Waltz 1998; Rattray 2001), ossia una guerra tecnologica basata sulla manipolazione digitale delle informazioni, che procede parallelamente alla prima condizionandone le sorti.

## 3. Notizie dal fronte: quadro empirico e materiali di studio

Hostomel, oblast di Kiev, Ucraina: il 28 febbraio 2022, ad appena quattro giorni dall'inizio dell'«operazione militare speciale» da parte delle forze armate russe, un colpo sparato da un cecchino ucraino da ben 1500 metri di distanza uccide il generale russo Andrej Aleksandrovič Suchoveckij, un veterano pluridecorato con grande esperienza di guerra. L'errore del generale, il primo degli alti ufficiali russi uccisi dall'inizio della guerra, sarebbe stato quello di aver utilizzato il proprio telefono cellulare (una fonte aperta) per comunicare con i suoi ufficiali, esponendosi alla geolocalizzazione da parte dell'*intelligence* ucraina. L'evento, ampiamente notiziato sia dai media mainstream che sulla Rete, rappresenta un caso emblematico di Osint militare, ossia di utilizzo di informazioni provenienti da fonti aperte a fini strategici: l'*intelligence* ucraina, infatti, ha intercettato il numero di cellulare e geolocalizzato la posizione del chiamante, impartendo l'ordine di uccidere al cecchino sul campo. Appena ricevuta l'informazione, l'*intelligence* ucraina ha provveduto a «chiudere» la fonte per portare a termine la missione, in maniera che l'*intelligence* nemica non avesse il tempo di rintracciare la segnalazione ed avvisare il generale di essere stato localizzato dal nemico per essere eliminato. Il caso riportato evi-

denzia le modalità di trattamento dell'informazione aperta a fini strategici in un teatro di guerra.

Tra le numerose piattaforme di Osint consultate ai fini dell'elaborazione del modello teorico proposto in questo lavoro, dalle quali è possibile rilevare decine di casi empirici simili a quello sopra descritto, una delle più importanti è Bellingcat[1], un sito di giornalismo investigativo con sede nei Paesi Bassi, guidato da un collettivo internazionale indipendente di ricercatori, giornalisti ed investigatori esperti di *Open source intelligence*, che riporta ogni giorno decine di casi di Osint militare. A seguito dell'invasione dell'Ucraina da parte della Russia, Bellingcat ha avviato un'importante collaborazione con il *Conflict intelligence team* (Cit)[2], un'organizzazione investigativa indipendente formata da oppositori russi e analisti militari (costretta a riparare in Georgia), che segue da vicino la guerra in Ucraina, conducendo indagini *open source* sul conflitto e fornendo informazioni tratte da fonti aperte di enorme rilevanza strategica per le forze armate ucraine e i suoi alleati. Le due organizzazioni, con il supporto di InformNapalm[3], una community internazionale di volontari esperti di *intelligence* degli *open data* e *fact checker*, conosciuta per aver pubblicato un database interattivo sull'aggressione russa che ha portato all'annessione della Crimea nel 2014 (Fig. 1)[4], hanno unito i loro sforzi in *crowdsourcing* per contribuire ad una mappatura della guerra in Ucraina basata sugli *open data*: il progetto è stato denominato *Eyes on Russia Map*[5], Si tratta di una mappa interattiva la cui supervisione scientifica è affidata al Centre for information resilience (Cir),[6] un ente sociale indipendente con sede a Londra, la cui mission è quella di mappare, individuare e documentare i crimini di guerra e la violazione dei diritti umani, potenziando l'integrità dell'ambiente informativo, contrastando la disinformazione e promuovendo la ricerca *open source*. In particolare, il

[1] Si ved, https://www.bellingcat.com/.

[2] Si ved, https://citeam.org/?lang=en.

[3] Si ved, https://informnapalm.org/en/.

[4] Nell'aprile 2018, InformNapalm ha pubblicato un database interattivo sull'aggressione russa all'Ucraina a partire dal 2014, anno dell'annessione della Crimea alla Russia all'indomani della rivoluzione dell'Euromaidan. Il database *Russian aggression* è il risultato di quattro anni di lavoro volontario. Più di 2500 indagini Osint sono state sistematizzate e divise in due gruppi: armi russe trovate nel Donbass; unità dell'esercito russo che hanno partecipato all'aggressione contro Ucraina, Georgia e Siria. Attraverso il database è possibile condurre ricerche per numero di unità militari e nome dell'unità. Le immagini degli stemmi delle unità militari o dell'equipaggiamento militare sono cliccabili e puntano ad un elenco di indagini non classificate, liberamente accessibili, che ha fornito all'intelligence ucraina preziose informazioni da utilizzare nell'elaborazione dei propri piani strategici, https://web.archive.org/web/20230629025953/https://informnapalm.org/db/russian-aggression/#lang=ua&page=m_unit.

[5] Si ved, https://eyesonrussia.org/.

[6] Si ved, https://www.info-res.org/.

ruolo del Cir è quello verificare l'attendibilità dei dati raccolti dalle suddette organizzazioni prima che vengano pubblicati sulla mappa sotto forma di *open data*, fornendo informazioni affidabili a giornalisti, politici, organi di giustizia, ma anche all'*intelligence* militare, che attraverso i propri analisti seleziona e distilla i dati utili ai fini decisionali, traducendoli in strategie d'azione sul campo.


Fig. 1. Il database interattivo di InformNapalm.

Ogni pin presente su *Eyes on Russia Map* rappresenta una costellazione di dati *open source*, visualizzabili sotto forma di foto, video o immagini satellitari corredate da metadati, come orari, date di rilevamento e coordinate geografiche (Fig. 2). Prima di essere utilizzati nei teatri operativi, gli *open data* vengono sottoposti ad un rigoroso processo di verifica da parte di analisti e investigatori Osint indipendenti attraverso strumenti di geolocalizzazione e cronolocalizzazione per individuare dove e quando sono stati rilevati: è da questo lavoro di verifica che dipende la vita dei soldati o il successo di un'operazione. Una volta raccolti e verificati, i dati vengono archiviati in un database centrale, dove è possibile ricercarli per tag o parole chiave. I segnaposto sulla mappa sono indicizzati per categorie (come movimenti militari russi, bombardamenti, scontri a fuoco, perdite militari, vittime civili, danni alle infrastrutture, incidenti, danni collaterali, etc.), nonché ordinati per data di pubblicazione, consentendo una ricerca per data, luogo, sistemi d'arma specifici o descrittori (come la lettera «Z» presente sui veicoli russi, diventata il simbolo dell'operazione speciale in Ucraina ed un meme diffuso da tutti i social media).

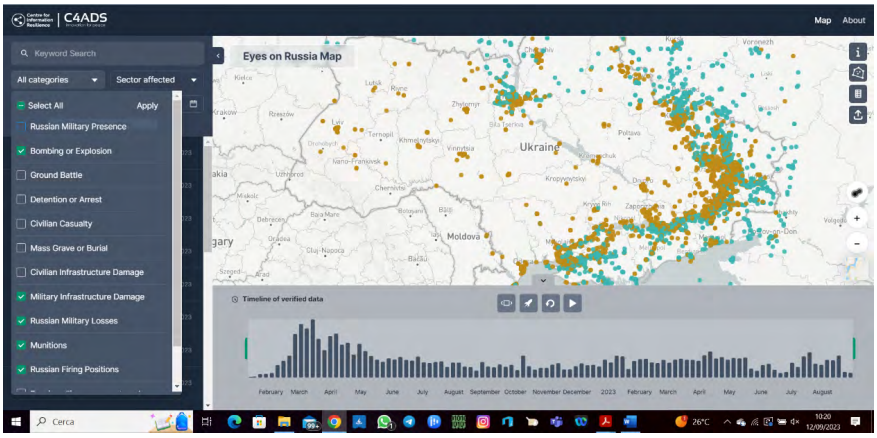


Fig. 2. La piattaforma Eyes on Russia Map.

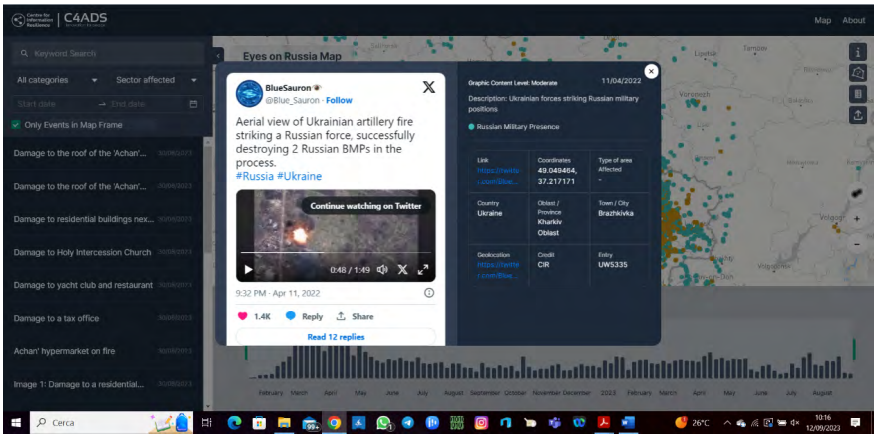


Fig. 3. Visualizzazione di un dato Osint sulla piattaforma Eyes on Russia Map.

Poiché le guerre ibride sono anche guerre di propaganda, non tutte le fonti aperte risultano affidabili, per cui è necessario verificare accuratamente le informazioni provenienti da fonti aperte per verificarne l'attendibilità (*fact checking*). Infatti, ai fini della teorizzazione del modello proposto, sono stati considerati i casi di operazioni militari effettivamente concluse sul campo, che hanno trovato preciso riscontro nelle informazioni pubblicate su *Eyes on Russia Map* (ad esempio, le postazioni bombardate o le trincee assaltate sulla base di precise coordinate geografiche o di immagini satellitari presenti sulla mappa) e che sono state confermate anche dai bollettini di guerra (Fig. 3). Inoltre, secondo la logica Osint, per appurare se le informazioni pubblicate dai comandi militari sono state manipolate, i casi confermati sono stati ulteriormente verificati attraverso la consultazione incrociata di altre piattaforme indipendenti di

*Open source intelligence* e giornalismo investigativo, come *Liveumap* (Fig. 4)[7], *GlobalSecurity*[8] e *War on Fakes*[9].

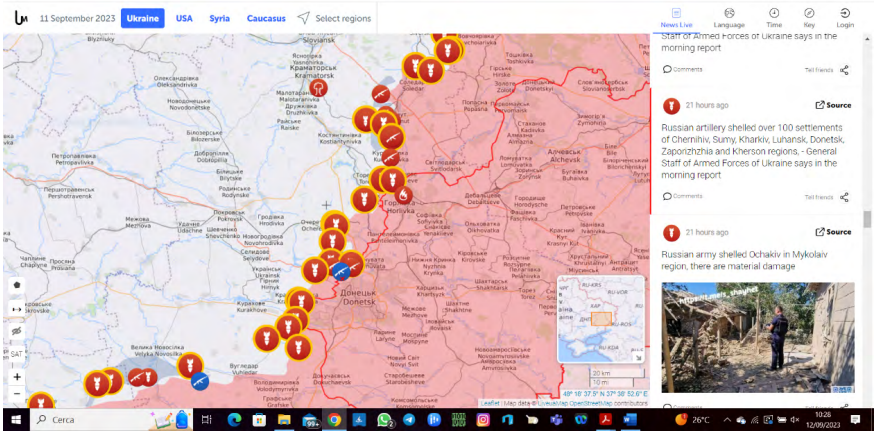


Fig. 4. La piattaforma *Liveumap*.

A completamento della metodologia d'indagine utilizzata in questo lavoro, al fine di avere una chiara comprensione delle procedure di analisi e trattamento delle informazioni acquisite da fonti aperte da parte degli analisti militari, ossia del percorso seguito dall'informazione prima di essere trasformata in decisione operativa, sono stati consultati: i manuali di Osint militare ad uso della Nato, che istruiscono gli analisti nel loro lavoro di analisi e trattamento degli *open data* (Nato Saclant 2001; 2002a; 2002b); il manuale in dotazione della *Us Defence intelligence* agency, redatto dal Joint military *intelligence* training center con sede a Reston, Virginia (Jmitc 2004)[10]; il rapporto di ricerca del National defence research institute (Nsrd), predisposto dalla Rand corporation per l'*Us Office of the secretary of defence* (Williams e Blum 2018)[11];

[7] *Liveumap* è una mappa interattiva aggiornata in tempo reale da *open source* sul campo di battaglia ed è liberamente consultabile al lin, https://liveuamap.com/.

[8] *GlobalSecurity* è una fonte affidabile di informazioni militari verificate sul campo da ricercatori indipendenti, https://www.globalsecurity.org/intell/index.html.

[9] *War on Fakes* è una piattaforma Osint indipendente nata da una costellazione di canali Telegram russi non politici, la cui mission è fornire informazioni verificate sulla guerra in Ucraina, https://waronfakes.com/.

[10] Il manuale è disponibile sul sito dell'Ooda Network, una rete costituita da esperti ed analisti di intelligence a supporto dell'attività di decision-making, al lin, https://www.oodaloop.com/wp-content/uploads/2015/02/osint_handbook_apr_04_edition.pdf.

[11] Il rapporto di ricerca del Ndri predisposto dalla Rand corporation è disponibile al lin, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf.

il manuale rilasciato dall'*Us Department of the army, directorate of doctrine*[12]; ed infine, per quanto attiene all' Osint militare in Italia, la ricerca condotta dal CeMiSS (Centro militare di studi strategici), pubblicata dal Ministero della Difesa (Minniti e Ceriello 2006)[13]. Come evidenziato nei suddetti manuali e rapporti, dove la procedura dell' Osint militare è dettagliatamente codificata, l'informazione passa attraverso vari stadi (o sistemi) di trattamento o trasformazione, dalla fase di acquisizione dei dati aperti, a quella dell'*intelligence*, a quella decisionale, fino al suo utilizzo strategico sul campo di battaglia: in sintesi, una volta processata all'interno di un sistema, l'informazione passa allo stadio successivo, fino al completamento del ciclo d'*intelligence*.

## 4. Risultati: dinamiche di *open/closed access* e *gatekeeping*

Attraverso l'analisi di un numero rilevante di casi in cui le operazioni militari ucraine sono state condotte utilizzando i dati aperti ricavati dalla mappa *Eyes on Russia* (ad esempio, selezionando dal menu la categoria «postazioni di tiro russe», è possibile accedere alle coordinate delle postazioni nemiche, essenziali per effettuare attacchi di precisione per mezzo di droni o dirigere il fuoco dell'artiglieria), è emerso uno schema ripetitivo nel trattamento dell'informazione da parte degli analisti d'*intelligence*, a partire dall'acquisizione dei dati da fonti aperte, alla fase decisionale, fino all'utilizzo strategico sul campo di battaglia. Ma il dato più interessante che è stato rilevato è la funzione di *gatekeeping* esercitata dall'*intelligence*: l'analisi del percorso compiuto dall'informazione, nel corso del suo viaggio dalla fonte aperta al campo di battaglia, ha evidenziato dinamiche di apertura/chiusura delle fonti a seconda delle strategie adottate dai comandi militari per raggiungere i propri obiettivi: la fonte aperta selezionata, una volta utilizzata, viene «chiusa» (ossia segretata) per evitare di fornire informazioni di ritorno al nemico, allertandolo ad esempio sui preparativi di attacco sulla conduzione di una specifica missione, compromettendo il vantaggio acquisito attraverso il lavoro d'*intelligence* (Nacci 2016; Carroll 2001), proprio come avvenuto nel caso dell'uccisione del generale Suchoveckij, dove le informazioni relative all'individuazione del bersaglio sono

[12] Il manuale dell'Us Department of the army è disponibile sul sito dell'Intelligence resource program appositamente predisposto dalla Federation of american scientists al lin, https://irp.fas.org/doddir/army/fmi2-22-9.pdf.

[13] La ricerca del CeMi.SS è consultabile sul sito del Ministero della difesa al lin, https://www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/42175_Minniti_0pdf.pdf.

state segretate prima di essere inviate allo *sniper team* che ha compiuto la missione, in modo da non poter essere rintracciate dal nemico.

Come già anticipato, la chiusura di una fonte aperta viene messa in atto erigendo «barricate digitali», rendendo il sistema informativo impenetrabile, o manipolando i dati aperti allo scopo di ingannare il nemico. Ovviamente il processo di chiusura è molto più complesso: infatti non si tratta semplicemente di spegnere un segnale (come disattivare il transponder di un aereo in volo o ordinare il silenzio radio alle truppe sul campo), ma di confondere le fonti aperte utilizzando tecniche di manipolazione digitale (*hacking*) e *cover-up*, sempre più spesso assistite dall'Ia, in grado di falsificare metadati, tracciati, immagini satellitari, riprese sul campo, suoni, voci, coordinate geografiche, disseminando falsi indizi per confondere e depistare il nemico: una guerra d'*intelligence* iper-tecnologizzata e immateriale, ma con enormi ripercussioni sul campo di battaglia (Hughes-Wilson 2004; Labanca e Zadra 2011). Si è notato, infatti, che molte delle notizie diffuse dai social media, data la loro sensibilità, vengono poi rimosse o oscurate e non sono più visualizzabili: le informazioni, una volta acquisite, vengono nascoste nel *deep* e *dark web*, spesso sotto forma di falsi dati, in modo da ingannare il nemico proprio dove pensa di poter scovare informazioni veritiere sotto forma di dati criptati (Ju *et al.* 2020).

L'analisi del processo di apertura/chiusura delle fonti, sopra descritto, ha quindi consentito di tracciare i contorni di un modello teorico in grado di evidenziare il percorso dell'informazione, dalla fase di selezione da fonti aperte fino alla sua trasformazione in decisioni strategiche sul campo: come si vedrà dall'illustrazione finale del modello, che si presenta come una struttura multisistemica all'interno della quale circolano i dati oggetto del ciclo dell'*intelligence*, l'informazione transita attraverso vari stadi (o sistemi), subendo diverse trasformazioni.

## 5. Discussione dei risultati: l'asimmetria informativa come strumento di *intelligence* e *smart weapon*

Nelle guerre ibride e asimmetriche, dove la tecnologia impatta profondamente le modalità di conduzione delle operazioni militari sul campo, determinando l'adozione di strategie operative non convenzionali, assume un'importanza decisiva il concetto di supremazia informativa: vince chi possiede maggiori informazioni rispetto all'avversario, o chi è in grado di manipolarle riducendo il valore informativo ai danni del nemico. Un concetto già espresso da Sun Tzu secoli fa nel suo trattato sull'arte della guerra (Sunzi Bingfa): «Se conosci il nemico e te stesso, la tua vittoria è sicura. Se conosci te stesso

ma non il nemico, le tue probabilità di vincere e perdere sono uguali. Se non conosci il nemico e nemmeno te stesso, soccomberai in ogni battaglia» (Tsu 2013, 96). Il sistema delle fonti Osint è estremamente complesso, in quanto gli analisti militari, prima di sottoporre i risultati alla catena di comando, cui compete la definizione dei requisiti essenziali di informazione (Ir, *Intelligence requirement*) e l'attività di decision-making, devono essere in grado di selezionare, tra milioni di dati disponibili da fonti aperte, le informazioni realmente utili e rilevanti, verificandone il grado di attendibilità e credibilità (*due diligence*) o, al contrario, il livello di disinformazione, al fine di sfuggire a possibili operazioni di *counterintelligence* da parte dell'avversario (*deception*). Una volta completata l'attività di *data mining*, ovvero di estrazione delle informazioni dalle fonti aperte, i dati vengono distillati e smistati ai centri decisionali e si trasformano nella matrice dell'attività di decision-making da parte della catena di comando, creando uno specifico asset informativo (ovvero informazione di valore, tecnicamente definita *payload* o carico pagante). Tale asset, dopo essere stata utilizzato per elaborare una decisione strategica, deve essere protetto e occultato o, al contrario, sfruttato ai danni del nemico attraverso operazioni di disinformazione, rendendo difficile o impossibile all'avversario attribuire il reale significato ai dati aperti disponibili. Per ottenere un simile vantaggio strategico, bisogna quindi indurre uno stato di asimmetria informativa a svantaggio del nemico, ovvero generare una situazione di scarsezza/ambiguità informativa, rendendo difficile, confusa, rischiosa o del tutto impossibile la presa di decisioni da parte della catena di comando avversaria. Ciò è reso possibile reimmettendo i dati strategicamente manipolati all'interno del circuito informativo, ma solo dopo aver confuso o occultato le informazioni reali, ovvero producendo disinformazione seppur in un contesto di fonti aperte e accessibili, oppure nascondendo le informazioni ai vari livelli di profondità del web. Ma, dato che anche il nemico sta facendo lo stesso gioco, gli analisti devono essere in grado di distinguere la vera informazione da quella manipolata. In un contesto di *information warfare* la Rete non può rimanere neutrale: infatti, si sta assistendo ad una frammentazione del web in varie partizioni, strategicamente controllate dai contendenti in gioco (*player*). Il fenomeno dello *splinternet* (o cyberbalcanizzazione) è indicativo della tendenza alla frammentazione della rete globale, operata da vari governi (in particolar modo da Cina, Russia e Corea del Nord) al fine di delimitare i confini geopolitici a livello digitale, attuando una divisione in blocchi geopolitici e militari contrapposti: lo spazio aperto si sta progressivamente chiudendo in nome degli interessi di difesa e sicurezza nazionali (Messa 2018). Infatti, i tecnonazionalismi e lo *sharp power* emergenti, ricalcano le attuali divisioni e rivalità tra gli Stati, soprattutto se questi sono direttamente impegnati in conflitti militari: il web si è trasformato nel nuovo

campo di battaglia di guerre combattute a livello globale (*weaponization*), dove si staglia uno scenario digitale iper-sorvegliato e ad elevata conflittualità, caratterizzato da «giochi di guerra» sempre più complessi ed iper-tecnologizzati (Calise e Musella 2019; Santaniello 2022). La stessa sovranità digitale dei singoli Stati pone enormi barriere alla libera fruizione di un'unica Rete globale e la guerra in Ucraina sta accelerando tale processo di frammentazione, creando reti contrapposte e barriere digitali, incrementando la tendenza ad un utilizzo «ristretto» e al tempo stesso multipolare della Rete da parte dei paesi in conflitto (*narrowcasting*). Ecco perché il fenomeno dello *splinternet* sta avendo un enorme impatto sulla definizione stessa di fonti aperte, riconfigurando paradossalmente l'Osint militare come *intelligence* delle «fonti occulte» ed evidenziando i meccanismi manipolatori alla base dello sfruttamento degli *open data*, che vengono gestiti secondo le logiche strategiche degli apparati militari (Miller 2018).

Generare asimmetria informativa, in ambito militare, significa dunque proteggere il valore dell'informazione distillata da fonti aperte, utilizzata per prendere decisioni aventi un impatto diretto sul campo di battaglia, creando un vantaggio strategico rispetto all'avversario attraverso le dinamiche di *open/closed access* delle fonti informative, in grado di creare supremazia informativa: sfruttando le nuove tecnologie generative e trasformative (Ia, motori di ricerca semantici, etc.) è possibile manipolare le informazioni, secretando, classificando o oscurando le fonti aperte (*cripting*); oppure confondendo o camuffando le fonti stesse attraverso operazioni di disinformazione e depistaggio, con l'obiettivo di renderle inaffidabili e, quindi, inutilizzabili per il nemico. Un modello di *intelligence* funzionale a tali dinamiche di manipolazione informativa è quello dell'Osint «a strati», nel quale l'informazione di valore strategico (*payload*) può essere occultata tra vari strati di informazione, dando luogo a molteplici e differenti combinazioni, secondo la metafora dei mattoncini Lego, che possono essere assemblati seguendo vari percorsi progettuali (Nacci 2017).

Come già accennato, il ciclo di *intelligence* delle fonti aperte in ambito militare prevede una fase di osservazione ed individuazione dei dati all'interno di uno specifico contesto di analisi (*discovery*); una fase di selezione dei dati maggiormente significativi, liberamente accessibili o comunque acquisibili attraverso l'utilizzo di opportuni protocolli di identificazione (*discrimination*); una fase di estrazione dei dati, sia osservati che percepiti, utili al raggiungimento degli obiettivi dell'analisi (*distillation*); infine, una fase di identificazione e rapida trasmissione alle catene di comando degli input informativi utili alla presa di decisioni o, in caso di operazioni di disinformazione e *counterintelligence*, la manipolazione dei dati da reimmettere nel circuito informativo (*dissemination*), in grado di produrre effetti prevedibili nello scenario di analisi

del nemico, secondo le intenzioni strategiche dell'emittente. Si parla di «dinamiche informative ambientali» per descrivere la complessità delle variabili in gioco nell'ambito dell'*intelligence* delle fonti aperte, capaci di produrre effetti diretti sui processi decisionali delle catene di comando, o sulle analisi d'*intelligence* da parte dell'avversario: questo processo di apertura/chiusura delle fonti (*open/closed access*) rende l' Osint militare simile ad una «macchina di trasformazione» che, come evidenziato dal modello teorico proposto, è in grado di reimmettere nell'ambiente informativo (infosfera) un'informazione manipolata e corrotta, producendo disinformazione. Quello che emerge è la trasformazione dell'informatività dei dati (ossia della loro valenza informativa a fini decisionali) sulla base di un preciso disegno strategico che mira a corrompere il significato dei dati stessi, secondo una strategia di *intelligence* deliberatamente pianificata ai danni dell'avversario: è possibile costruire una narrativa funzionale agli obiettivi militari, rendendo visibile al nemico una costruzione della realtà diversa da quella reale.

L'*intelligence* delle fonti aperte in ambito militare si basa su un approccio interdisciplinare, in quanto prevede il ricorso alle scienze cognitive (logica, linguistica, psicologia cognitiva, psicolinguistica, filosofia della mente e del linguaggio, neuroscienze), nonché all'Ia, alla teoria dei giochi e alla crittografia, determinando un nuovo tipo di guerra, la *cognitive warfare*, che è tuttora oggetto di studio da parte dei comandi militari (Ministero della difesa 2023). Compito dell'analista è dunque quello di estrarre i dati rilevanti dalle fonti aperte utilizzando tutti i tools a sua disposizione, per poi trasferirli ai centri di comando che li utilizzeranno nel processo decisionale strategico. Ma affinché l'Osint abbia una reale valenza strategica, trasformandosi in una *smart weapon*, è necessaria la manipolazione delle variabili del sistema, riducendo il «carico pagante» dei dati ed inducendo scarsità informativa o disinformazione ai danni dell'avversario (*anti-data*). È proprio in questo momento che il sistema delle fonti aperte si chiude, offuscando la valenza informativa dei dati e sgretolandone l'affidabilità a fini strategici: l'obiettivo è quello di confondere il nemico, inducendolo a prendere decisioni sbagliate o a commettere errori di valutazione, secondo gli intenti dell'apparato emittente che, esercitando la propria supremazia informativa, sarà in grado di produrre un vantaggio strategico sul campo di battaglia, ottenendo così il pieno controllo sul circuito informativo.

Se è compito dell'*intelligence* quello di individuare, analizzare e validare le informazioni utili alla presa di decisioni, per poi manipolarle e deprivarle del loro valore ai danni del nemico (reimmettendole nel circuito informativo sotto forma di falsi dati), compito della *counterintelligence* delle fonti aperte è quello di scoprire gli eventuali tentativi d'inganno orditi dal nemico, che è in grado di utilizzare le stesse tecniche di analisi informativa. Secondo il model-

lo di *intelligence* «a strati», cui si è accennato prima, è possibile manipolare l'informazione aperta stratificandola e occultandola tra le pieghe del tessuto informativo, ovvero combinando i dati in maniera coerente con le finalità strategiche alla base dell'analisi, oppure lasciando filtrare le informazioni volute, in base al livello di astrazione strategicamente pianificato dai vertici militari (Floridi 2012; 2014), facendo in modo che la realtà percepita dall'avversario corrisponda a quella voluta dall'emittente, secondo una precisa strategia informativa. Una delle tecniche di *data analysis* più utilizzate dall'*intelligence* delle fonti aperte è l'analisi semantica, effettuata attraverso sistemi di Ia (*text mining*) che, sulla base di specifiche istruzioni (*intelligence requirement*), operano automaticamente l'individuazione l'analisi, il riconoscimento, la comprensione, la comparazione, la categorizzazione e l'indicizzazione dei dati provenienti dalle varie fonti (*all-source intelligence*), identificandone le ricorrenze: il motore inferenziale dell'Ia, infatti, oltre ad avere capacità di disambiguazione e contestualizzazione, è in grado di trarre conclusioni sia di tipo deduttivo (*forward chaining*) che induttivo (*backward chaining*) attraverso il cosiddetto «rafforzatore di consistenza», che testa la veridicità delle ipotesi ricavate attraverso la comparazione dei dati. Nel caso di un'analisi Socmint (Social media *intelligence*), l'analisi semantica del contenuto condotta dall'Ia può essere applicata ai contenuti, alle *sensation* e al *sentiment* emergenti dai social network (Charania 2016), individuando la frequenza delle argomentazioni o la descrizione di stati d'animo che possono far prevedere il comportamento del nemico: consultare i profili Instagram e Facebook dei soldati impegnati in battaglia permette di comprendere la reale situazione sul campo di battaglia, il morale delle truppe, le perdite subite, gli spostamenti in corso, anticipandone i piani e indirizzando in maniera efficace le operazioni attraverso l'elaborazione di un modello predittivo (Noubours *et al.* 2013).

Un altro aspetto cruciale dell'Osint in ambito militare è il livello di attendibilità e affidabilità dei dati acquisiti dalle fonti aperte. Infatti, l'informatività dei dati, ossia il carico informativo utile o informazione pagante (*payload*), in grado di orientare l'attività di decision-making delle catene di comando, può essere acquisito attraverso molteplici canali, che implicano attività di osservazione, percezione, registrazione e trasmissione di dati. Ma non tutti i contenuti che la funzione di *intelligence* è chiamata a processare sono veri o reali; infatti, qualora i dati siano stati già distillati e reimmessi nell'ambiente informativo dall'*intelligence* avversaria, i contenuti potrebbero essere stati deliberatamente falsificati (*deception*) o, a un più basso livello di intensità, potrebbero essere stati involontariamente falsati, come nel caso della misinformazione, ossia l'informazione non accurata e inattendibile veicolata dai mass media generalisti. Il *payload*, nella maggior parte dei casi, non è costituito da ciò che è direttamente

visibile o percepibile ma, trattandosi dell'analisi di enormi masse di dati (big data), è frutto di estrazioni operate automaticamente dai motori inferenziali su cui si basano i sistemi di Ia utilizzati nel ciclo di *intelligence*, anche se spetta all'analista umano individuare i dati di valore attraverso opportune comparazioni: l'attività di *intelligence* sulle fonti aperte non può essere solo *machine-driven*, ma deve essere necessariamente *analyst-driven*.

La tipologia di informazioni offerte dall'analisi automatica è costituita da dati appartenenti alle classi dei metadati (dati che descrivono le proprietà di altri dati), dei dati operazionali (dati che descrivono operazioni che si svolgono all'interno di un sistema di dati o che riguardano il funzionamento e l'organizzazione di altri dati) e dei dati derivati (dati estratti da altri dati attraverso inferenze, comparazioni o rapporti di relazione con altri dati). L'analista che interroga le fonti aperte si muove in un sistema informativo reticolare in cui le fonti sono in qualche modo collegate da rapporti di relazione diretta, indiretta o occulta: il carico informativo utile «punta» sempre ad altre fonti, ed i *raw data* sono sempre suscettibili di sviluppo o trasformazione attraverso processi di linking semantico. Una volta individuata l'informazione utile, diventa strategico ridurre il *payload*, creando asimmetria informativa ai danni dell'avversario. Vengono quindi messi in atto processi di classificazione delle informazioni (ovvero di limitazione della disponibilità dell'informazione o di occultamento dei dati di valore), oppure di falsificazione più o meno estesa dei dati allo scopo di produrre disinformazione o fake news per ingannare il nemico: limitare la disponibilità dell'informazione equivale a chiudere l'accesso alla fonte. Se la fonte primaria è quella di cui si ha diretta percezione (ad es. la ripresa delle operazioni sul campo di battaglia da parte di un drone), questa può essere manipolata occultando i dati essenziali alla comprensione del contesto di analisi (ad esempio eliminando alcuni frame della ripresa o falsificando le coordinate geografiche), costruendo un'altra narrativa, in modo da indurre in errore l'analista avversario. Infatti, grazie alle nuove tecnologie, è possibile manipolare le informazioni, inquinando l'ambiente informativo allo scopo di produrre disinformazione (Hughes-Wilson 2004; Chiais 2009): manipolare i dati significa modificare la narrazione dei fatti veicolati dai dati (storytelling), rendendola ambigua, imprecisa e incerta, trasformando i fatti in fattoidi a fini strategici. La conoscenza che l'Osint militare acquisisce dalle fonti aperte è, nella maggior parte dei casi, indiretta, ovvero procede per comparazioni tra dati provenienti da diverse fonti, sussistendo sempre il sospetto che la fonte possa essere già stata corrotta dal nemico. È dunque essenziale procedere alla validazione delle fonti attraverso controlli incrociati e ulteriori verifiche (*fact checking*). Infatti, caratteristica della *information warfare* è quella di scatenare guerre semantiche tra gli avversari (Waltz 1998), dove l'obiettivo del gioco è

individuare il reale significato dei dati analizzati, distillando l'informazione utile ai fini decisionali, evitando mistificazioni e inganni.

## 6. Verso un modello teorico di Osint militare

In ambito militare, la raccolta di informazioni da fonti aperte (*open access*) si configura tecnicamente come un'attività offensiva, finalizzata ad individuare il *payload* necessario a supportare le attività decisionali dei centri di comando, prima di chiudere l'accesso al sistema informativo, mettendolo in sicurezza; al contrario, la «chiusura» del sistema informativo (*closed access*) rappresenta un'attività difensiva, che mira a proteggere il vantaggio informativo acquisito. Quest'ultima attività diventa a sua volta offensiva nel momento in cui l'informazione acquisita da fonti aperte viene trasformata in disinformazione o informazione occulta, che viene reimmessa nel circuito producendo di fatto una situazione di asimmetria informativa ai danni del nemico: proprio per questo, oggi assistiamo ad una guerra ibrida e immateriale (*information warfare*). Questo nuovo tipo di guerra viene combattuta proprio attraverso le dinamiche di *open/closed access* delle fonti informative, che sono in grado di determinare le sorti di un conflitto sul campo di battaglia.

Il ciclo dell' Osint militare, infatti, si svolge all'interno di un circuito informativo costituito da vari sistemi, all'interno dei quali avvengono i processi di trattamento dell'informazione aperta, dalla fase di selezione dei dati da parte dell'*intelligence*, all'utilizzazione da parte dei decisori, all'utilizzo sul campo da parte dei comandi militari, fino alla manipolazione e reimmissione dei dati nel circuito informativo sotto forma di disinformazione, misinformazione, informazione occulta o informazione classificata da parte della stessa *intelligence*. Come è possibile rilevare dal modello teorico proposto (Fig. 5), il processo di trasmissione dell'informazione da un sistema all'altro si svolge in maniera ciclica: l'analisi delle informazioni raccolte può richiedere ulteriori ricerche puntando ad altri dati, per cui il ciclo può riprendere senza dover necessariamente giungere alla fase finale di disseminazione, ovvero di trasmissione in tempi rapidi delle informazioni di valore ai centri decisionali (Minniti e Ciriello 2006, 18-24). L'acquisizione di dati da fonti aperte si basa su una valutazione strategica di *intelligence* da parte dei vertici militari, tecnicamente definita Ir, mentre il sistema di analisi utilizzato è chiamato Ibp (*Intelligence preparation of the battlefield*), una metodologia di raccolta, analisi e processamento dei dati informativi finalizzata a supportare il processo decisionale in ambito militare o Mdmp (*Military decision making process*), in grado di effet-

tuare una valutazione delle minacce orientando il Coa (*Course of action*) sul campo di battaglia (Nato Saclant 2001).

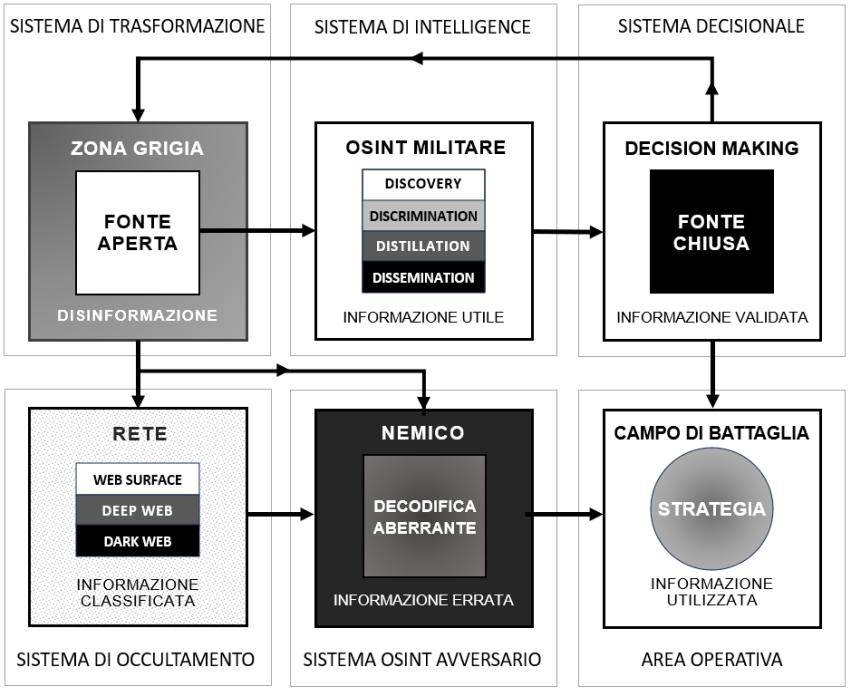


Fig. 5. Modello teorico dell'Osint militare.
*Fonte:* elaborazioni proprie.

Il modello teorico presentato in questo lavoro ha l'obiettivo di illustrare il percorso dell'informazione all'interno del circuito informativo nel quale si muove l'analista di Osint militare, senza scendere nel dettaglio sulle modalità di distillazione e validazione dei dati acquisiti da fonti aperte, che interessano i processi di significazione dei dati e che attengono alle mutevoli strategie da utilizzare sul campo. Il modello proposto sintetizza i risultati della ricerca che, come già detto, ha evidenziato precise ricorrenze nel trattamento dei dati aperti da parte dell'*intelligence*. Tuttavia, è necessario precisare che si tratta di un modello informazionale di tipo trasmissivo, in quanto evidenzia i flussi e le traiettorie dell'informazione che viene trasmessa dall'emittente (l'analista) al ricevente (il nemico), nonché i nodi-sistemici all'interno dei quali il processo di trasformazione dei dati avviene, ma senza invadere il campo semantico: il problema della costruzione dei significati ricavati dagli *open data* riguarda il lavoro di *intelligence* degli analisti e le valutazioni strategiche dei vertici militari, che

non è possibile racchiudere in tale modello, essendo connotati dall'imprevedibilità e incertezza dei valori da assegnare ai dati stessi. I percorsi di significazione attengono infatti ai disegni di *intelligence* militare, che vanno adeguati agli obiettivi da raggiungere e alle valutazioni di scenario: è così che l'informazione tratta da fonti aperte si trasforma in *intelligence*, ovvero in informazione contestualizzata, validata e finalizzata a produrre decisioni operative sul campo.

Ciò che viene evidenziato nel modello teorico proposto (che si presenta come un circuito multisistemico integrato) è il percorso/direzione del dato informativo a partire dall'accesso alle fonti aperte, nonché il processo di trasformazione dell'informazione in disinformazione o informazione occulta a fini strategici da parte dell'emittente ai danni dell'avversario, ovvero la chiusura della fonte aperta dopo l'utilizzazione dei dati utili ad orientare il processo decisionale, finalizzato ad avere effetti operativi sul campo di battaglia. Come si nota, esiste una somiglianza con il concetto del «rumore» presente nel modello matematico della comunicazione di Shannon-Weaver (Shannon e Weaver 1949; Wolf 1997), ovvero gli elementi di disturbo che impediscono la corretta ricezione del messaggio, producendo una perdita di informazione all'interno del sistema informativo (entropia) o una decodifica aberrante dei dati (*derailment of understanding*). Ma nel caso dell'Osint militare il rumore non è esterno alla fonte dell'informazione e non interessa unicamente il canale di comunicazione, poiché ingloba l'emittente stesso nel sistema di trasformazione dell'informazione disponibile: l'analista agisce sui dati, manipolandoli strategicamente, mettendo in atto un'attività offensiva. Infatti, obiettivo dell'emittente è quello di indurre deliberatamente uno stato di scarsezza informativa ai danni del nemico, ottenendo la supremazia informativa sull'avversario; per far ciò è necessario ampliare l'area del «rumore», sino ad inglobare le fonti stesse del messaggio, creando cortine fumogene o disinformazione allo scopo di proteggere i dati utili acquisiti, strategicamente funzionali alla presa di decisioni, e chiudendo l'accesso alle fonti. La «zona grigia» di informazione, visibile nel modello teorico elaborato, rappresenta l'area di protezione dei dati delle fonti aperte che sono stati già processati e trasformati dall'emittente attraverso il ciclo dell'*intelligence* basato sulle «four Ds» (*discovery*, *discrimination*, *distillation*, *dissemination*): si tratta di una zona d'interdizione posta tra la fonte del messaggio e il destinatario della comunicazione, ossia l'*intelligence* nemica. È proprio nel momento in cui i dati vengono manipolati all'interno del «sistema di trasformazione», predisposto e guidato dall'emittente, che la fonte aperta si chiude, alzando barriere all'ingresso o rilasciando false informazioni nel circuito comunicativo, allo scopo di confondere gli analisti avversari. Infatti, l'Osint militare non è solo *intelligence* che raccoglie informazioni da fonti aperte, ma anche *intelligence* che comunica con il nemico attraverso tali fonti, o meglio,

le manipola per comunicare con l'avversario sulla base di precise strategie informative: più è alto il livello di classificazione richiesto dalla strategia, minore è la quantità di informazione che può essere diffusa nel circuito. In base all'Ir, molte informazioni, oltre a subire una manipolazione prima di essere reimmesse nel circuito informativo sotto forma di disinformazione o misinformazione, possono anche essere occultate o classificate, inabissandole nel web a vari livelli di profondità (*surface*, *deep* o *dark web*). Sapendo che il nemico è attivo anche a questi livelli, è possibile pianificare operazioni di *counterintelligence*, *undercovering* o *deception*, manipolando e, al tempo stesso, occultando l'informazione, allo scopo di ingannare l'avversario che, scandagliando il web, potrebbe credere di aver scoperto un'informazione importante, ritenendola genuina per il solo fatto di essere stata nascosta in profondità. Causare la perdita intenzionale di informazione (e quindi di attendibilità dei dati), o pianificare la classificazione controllata dei dati, ha l'obiettivo ingenerare confusione nella sfera informativa analizzata dall'avversario, il quale rischia di mettere in atto un processo di «decodifica aberrante» dei dati, ossia un'errata interpretazione dell'informazione (Eco 1975; Volli 2014), producendo decisioni sbagliate con esiti infausti sul campo di battaglia: diffondere disinformazione nel sistema significa creare una cortina fumogena in grado di offuscare i dati utili alla presa di decisioni da parte del nemico.

Nel corso del processo di trasformazione che avviene all'interno del sistema descritto nel modello, l'informazione aperta, ovvero non soggetta a classificazione o a specifici profili di *clearance* (potenzialmente accessibile senza violare alcun vincolo di riservatezza), può transitare attraverso vari gradi di accessibilità, secondo le strategie dell'emittente. I livelli assegnati all'informazione sono i seguenti: *open*, *official*, *twilight*, *classified* e *closed*. Lo stato definito *twilight* information rappresenta la «zona grigia» e manipolabile dell'informazione, uno stato altamente sensibile che viene definito sulla base delle strategie pianificate dalle catene di comando, che possono prevedere l'offuscamento o occultamento dei dati a fini strategici (*deception*) o la disinformazione per confondere il nemico, ponendolo in uno stato di vulnerabilità sul campo a causa dell'asimmetria informativa. Prima di giungere a tale stato, l'informazione viene distillata all'interno di un «sistema di trasformazione» che altera la valenza informativa dei dati, trasformandone la catena di significati che li lega alla realtà: in tale stato le fonti sono ancora aperte ma ambigue e ingannevoli e, proprio per questo, pericolose. Ciò che ne risulta è un'informazione disinnescata e depotenziata alla fonte: una vera e propria trappola semantica per i comandanti nemici, su cui grava il rischio di fondare le proprie decisioni operative su dati fallaci e ingannevoli, che possono comportare gravi perdite sul campo di battaglia (azzardo morale). Infatti, nel momento in cui l'avversario

intercetta questo tipo di informazione (falsa) utilizzando a sua volta il ciclo dell'*intelligence* sopra descritto (ossia il modello delle «four Ds»), rischia di orientare le proprie decisioni secondo la volontà dell'emittente, che ha strategicamente pianificato l'inganno manipolando le fonti aperte. L'euristica delle fonti aperte è dunque una parte essenziale del lavoro di *intelligence*, dove l'informazione aperta deve essere accuratamente verificata e validata dagli analisti militari prima di poter influenzare i processi decisionali di vertice, giungendo al livello Osint-v (*Open source of intelligence validated*), il più alto livello di codifica, prima che l'informazione stessa venga trasmessa (disseminata) ai centri di comando per l'attività di decision-making sul campo, o per essere riutilizzata in operazioni di depistaggio o *counterintelligence* (Jmitc 2004; Gagliano 2012).

Data l'ampia varietà di fonti aperte, è necessario standardizzare le metodologie di estrazione e analisi dei dati, fissando precisi e rigorosi protocolli di validazione dei dati (Hassan e Hijazi 2018; Lapi 2021). Infatti, il concetto di affidabilità delle fonti è di vitale importanza affinché i dati analizzati possano acquisire lo status di informazione di valore (*payload*) ed essere tempestivamente trasmessi ai vertici militari per le opportune decisioni sul campo (la fase finale del ciclo d'*intelligence*, o *dissemination*). Un'informazione di valore, per essere tale, deve essere generativa di senso, ossia deve innovare lo stato conoscitivo del ricevente riducendone lo stato di incertezza: è questo il senso del lavoro degli analisti militari, che devono riuscire a verificare, testare, validare e rafforzare le ipotesi deducibili dai dati acquisiti da fonti aperte per permettere ai centri di comando di prendere le giuste decisioni. Il lavoro dell'analista, di norma, si concretizza anche in un oggetto fisico, ossia un documento registrato su supporto analogico o digitale atto a garantire la persistenza del dato, consentendone la trasmissione/diffusione in sicurezza ai vertici militari nella fase finale del ciclo d'*intelligence* (Ferraris 2009; Nacci 2016). Ai comandi spetta, infine, il compito di decidere quale statuto assegnare alle informazioni acquisite, mantenendo il vantaggio acquisito attraverso lo sfruttamento delle fonti aperte: decisioni operative sul campo, disinformazione o occultamento dei dati a fini strategici.

## 7. Conclusioni

Nell'intento di offrire una migliore comprensione dell'utilizzo dell'Osint in ambito militare e delle modalità di sfruttamento delle fonti aperte da parte degli analisti militari, si è tentato di costruire un modello in grado di spiegare i processi di trasformazione dell'informazione da parte degli apparati d'*intelligence* militare, colmando l'attuale mancanza di un inquadramento

teorico di riferimento per l'Osint militare. In sintesi, i risultati più rilevanti emersi dallo studio dello scenario empirico, che ha condotto alla realizzazione del modello teorico proposto, sono i seguenti: l'individuazione di specifiche dinamiche di apertura/chiusura delle fonti aperte a fini strategici; la funzione di *gatekeeping* esercitata dall'*intelligence* militare.

Si spera che il modello teorico presentato in questo lavoro possa essere approfondito da ulteriori studi che tengano in considerazione nuove modalità di sfruttamento delle fonti aperte, anche alla luce dei progressi dell'Ia, diventando uno strumento di utilità pratica a disposizione degli analisti militari e degli studiosi di scienze strategiche, aggiungendo un ulteriore tassello alla comprensione del processo di *weaponization* della Rete e di militarizzazione dell'Ia a scopi strategici da parte degli apparati militari (Mezza 2022). Se le minacce alla pace e alla sicurezza mondiali stanno aumentando i livelli di incertezza e vulnerabilità dei vari paesi, la creazione di un sistema integrato e reticolare di interscambio delle informazioni tra gli alleati occidentali (Nato e Aukus), basato su una più ampia accessibilità delle fonti aperte attraverso protocolli condivisi, potrebbe consentire un più efficace coordinamento degli sforzi militari congiunti, ma bisogna contemperare le esigenze di condivisione dei dati con quelle di protezione delle informazioni sensibili: l'*intelligence* delle fonti aperte rappresenta sicuramente una risposta efficace alle richieste di dati da parte degli Stati belligeranti, ma è necessario applicare ad essa i metodi di trattamento delle informazioni propri dell'*intelligence* tradizionale, allo scopo di accrescere i livelli di sicurezza e proteggere l'attività di decision-making dei centri di comando in base alle esigenze di difesa dei singoli Stati.

## Riferimenti bibliografici

Ackerman, R. K. (2006), *Intelligence Center Mines Open Sources*, in «Signal», 60(7), pp. 60-66.

Agenzia per la Cybersicurezza Nazionale-Acn (2022) (a cura di), *Strategia Nazionale di Cybersicurezza 2022-2026*, https://www.acn.gov.it/ACN_Strategia.pdf. Consultato il 6 settembre 2023.

Akhgar, B., Saskia Bayerl, P. e Sampson, F. (2017) (a cura di), *Open Source Intelligence Investigation: From Strategy to Implementation*, Basilea, Springer.

Andrew, C., Aldrich, R, J. e Wark. W. K. (2020) (a cura di), *Secret Intelligence: A Reader*, New York, Routledge.

Armistead, L. (2004) (a cura di), *Information Operations: Warfare and The Hard Reality of Soft Power*, Washington, DC, Brassey's.

Arquilla, J. e Ronfeldt, D. (1993), *Cyberwar is Coming!*, in «Comparative Strategy», 12(2), pp. 141-165.

Barbato, A. (1996), *Come si manipola l'informazione*, Roma, Editori Riuniti.
Bazzell, M. (2023), *OSINT Techniques: Resources for Uncovering Online Information*, London, Amazon Publishing.
Bean, H. (2011), *No More Secrets: Open Source Information and the Reshaping of US Intelligence*, Westport, Praeger Security International.
Best, C. (2011), *Challenges in Open Source Intelligence, paper presentato alla 2011 European Intelligence and Security Informatics Conference*, Atene, Grecia, 12-14 settembre.
Bianchi, A. (2009), *Pragmatica cognitiva. I meccanismi della comunicazione*, Roma-Bari, Laterza.
Borriello, G. e Fristachi, G. (2022), *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in «Rivista di Digital Politics», 2 (1-2), pp. 157-178.
Burke, C. (2007), *Freeing Knowledge, Telling Secrets: Open Source Intelligence and Development*, in «Research paper series: Centre for East-West Cultural & Economic Studies», 13, Goald Coast, Bond University.
Calise, M. e Musella, F. (2019), *Il Principe digitale*, Roma-Bari, Laterza.
Casanovas, P. (2017), *Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT)*, in M. Taddeo e L. Glorioso (a cura di), *Ethics and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, Cham, Springer, pp. 139-167.
Carroll, T.P. (2001), *The Case Against Intelligence Openness*, in «International Journal of Intelligence and CounterIntelligence», 14(4), pp. 559-574.
Centoducati, C. (2006), *Open Source Intelligence. Cenni sulla dottrina alleata*, in «Informazioni della Difesa», 1, pp. 26-31.
Charania, S. (2016), *Social Media's Potential in Intelligence Collection*, in «Intelligence in Peace and War», 33(2), pp. 94-100.
Chiais, M. (2008), *Menzogna e propaganda. Armi di (dis)informazione di massa*, Milano, Lupetti.
Chiais, M. (2009) (a cura di), *Propaganda, disinformazione e manipolazione dell'informazione*, Roma, Aracne Editrice.
Cia-U.S. Central Intelligence Agency (1993), *Preparing U.S. Intelligence for the Information Age: Coping with the Information Overload*, Washington D.C.
Clarke, R. e Knake, R. (2010), *Cyber War: The Next Threat to National Security and What to Do About It*, New York, Harper.
Colonna Vilasi, A. (2011), *Manuale d'Intelligence*, Reggio Calabria, Città del Sole Edizioni.
Connor, B., Medina, D., Silvers, J., Steinhaus, N. e DuBois, P. (2021), *Integrating Open Source Intelligence into the Brigade Combat Team at Combat Training Centers*, in «Industrial and Systems Engineering Review», 8(1), pp. 24-30.
Coom, H. L. (1969), *The Exploitation of Foreign Open Sources*, in «Studies in Intelligence: Journal of the American Intelligence Professional», 13(2), pp. 129-136.
Davies, P. H. (2005), *Intelligence, Information Technology and Information Warfare*, in «Annual Review of Information Science and Technology», 36, pp. 313-352.

Eco, U. (1975), *Trattato di semiotica generale*, Milano, Bompiani.

Evangelista, J. R. G., Sassi, R. J., Romero, M. e Napolitano, D. (2020), *Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence*, in «Journal of Applied Security Research», 16(3), pp. 1-25.

Ferraris, M. (2009), *Documentalità. Perché è necessario lasciare tracce*, Roma-Bari, Laterza.

Floridi, L. (2012), *La rivoluzione dell'informazione*, Torino, Codice Edizioni.

Floridi, L. (2014), *The 4th Revolution. How Infosphere is Reshaping Human Reality*, Oxford, Oxford University Press.

Friedman, R. S. (1998), *Open Source Intelligence*, in «Parameters», 2, pp. 6-12.

Gagliano, G. (2012), *Guerra psicologica. Saggio sulle moderne tecniche militari di guerra cognitiva e di disinformazione*, Roma, Fuoco Edizioni.

Giannuli, A. (2012), *Come i servizi segreti usano i media*, Pioltello, Adriano Salani Editore.

Gill, P. e Phythian, M. (2006), *Intelligence in an Insecure World*, Cambridge, Polity Press.

Glassman, M. e Kang, M. J. (2012), *Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)*, in «Computers in Human Behavior», 28(2), pp. 673-682.

Glorioso, L. e Taddeo, M. (2016) (a cura di), *Ethics and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, New York, Springer.

Gruters, P. C. e Gruters, K. T. (2018), *Publicly Available Information: Modernizing Defense Open Source Intelligence*, in «Special Operations Journal», 4(1), pp. 97-102.

Hassan, N. A. e Hijazi, R. (2018), *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, Berkeley, Apress.

Herman, M. (1996), *Intelligence Power in Peace and War*, Cambridge, Royal Institute of International Affair.

Herman, M. (2001), *Intelligence Services in the Information Age*, London, Frank Cass.

Hughes-Wilson, J. (2004), *Military Intelligence Blunders and Cover-ups*, London, Robinson.

Hulnick, A. S. (2002), *The Downside of Open Source Intelligence*, in «International Journal of Intelligence and CounterIntelligence», 15(4), pp. 565-579.

Hulnick, A. S. (2010), *The Dilemma of Open Source Intelligence: Is Osint Really Intelligence?*, in L. K. Johnson (a cura di), *The Oxford Handbook of National Security Intelligence*, Oxford, Oxford University Press, pp. 229-241.

Jardines, E. A. (2002), *Understanding Open Sources, in Supreme Allied Commander Atlantic-Saclant, Intelligence Branch, Intelligence Exploitation of the Internet*, Norfolk, VA, pp. 9-11.

Jeffson, J. (2005), *Creating an Open Source Capability*, in «Military Intelligence Professional Bulletin», https//www.thefreelibrary.com/Creating+an+open+source+capability.-a0146354021</a>. Consultato il 10 settembre 2023.

Johnson, L. K. (2006) (a cura di), *Handbook of Intelligence Studies*, Abingdon, Routledge.

Joint Military Intelligence Training Center-Jmitc (2004), *Open Source Exploitation: A Guide For Intelligence Analysts*, Reston, Open Source Publishing Inc.

Labanca, N. e Zadra, C. (2011) (a cura di), *Costruire un nemico. Studi di storia della propaganda di guerra*, Milano, Edizioni Unicopli.

Lapi, M. (2021), *Open Source Intelligence. Metodologie e strumenti per investigare il web*, Roma, Edizioni Themis.

Libicky, M. C. (1995), *What Is Information Warfare?*, Washington D.C., National Defence University.

Madill, D. L. (2005), *Producing Intelligence from Open Sources*, in «Military Intelligence Professional Bulletin», 31(4), pp. 19-26.

Markowitz, J. (2003), *Open Source: In Support of All-Source Intelligence*, Washington D.C., Open Source Solutions.

Mascella, R. e Lattanzio, P. (2008), *Teoria e strutture dell'informazione*, Roma, Aracne Editrice.

Messa, P. (2018), *L'era dello sharp power. La guerra (cyber) al potere*, Milano, Bocconi University Press.

Mezza, M. (2022), *Net-war. Ucraina: come il giornalismo sta cambiando la guerra*, Roma, Donzelli Editore.

Miller, B. H. (2018), *Open Source Intelligence (OSINT): An Oxymoron?*, in «International Journal of Intelligence and CounterIntelligence», 31, pp. 702-719.

Ministero della Difesa-Stato Maggiore della Difesa (2023) (a cura di), *Cognitive Warfare. La competizione nella dimensione cognitiva*, Roma, https://www.difesa.it/SMD_/Staff/Sottocapo/UGID/Dottrina/Documents/Cognitive_Warfare_Ed.2023.pdf. Consultato il 10 settembre 2023.

Minniti, F. e Ciriello, S. (2006), *Le Fonti Informative e l'Open Source Intelligence*, Ricerca CeMiSS C8/Z (Centro Militare di Studi Strategici), Roma, Centro Alti Studi per la Difesa (CASD).

Monahan, T. (2006) (a cura di), *Surveillance and Security: Technological Politics and Power in Everyday Life*, New York, Routledge.

Mulgan, G., Steinberg, T. e Salem, O. (2005), *Wide Open: Open Source Methods and Their Future Potential*, London, Demos.

Nacci, G. (2016), *Vietato lasciare le fonti aperte*, Novi Ligure, Edizioni Epoké.

Nacci, G. (2017), *Open Source Intelligence Application Layer. Proposta per una Teoria Generale dell'Intelligence delle Fonti aperte*, Novi Ligure, Edizioni Epoké.

Nato Saclant – Supreme Allied Commander Atlantic, Intelligence Branch (2001), *NATO Open Source Intelligence Handbook*, Norfolk, VA.

Nato Saclant – Supreme Allied Commander Atlantic, Intelligence Branch (2002a), *Intelligence Exploitation of the Internet*, Norfolk, VA.

Nato Saclant – Supreme Allied Commander Atlantic, Intelligence Branch (2002b), *NATO Open Source Intelligence Reader*, Norfolk, VA.

Norton, R. A. (2011), *Guide to Open Source Intelligence. A Growing Window into the World*, in «Journal of U.S. Intelligence Studies», 18(2), pp. 65-67.

Noubours, S., Pritzkau, A. e Schade, U. (2013), *NLP as an Essential Ingredient of Effective OSINT Frameworks, paper presentato alla 2013 Military Communications and Information Systems Conference*, Saint-Malo, Francia, 7-9 ottobre.

Office of the Director of National Intelligence – United States of America (2011), *U.S. National Intelligence. An Overview 2011*, https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf. Consultato il 10 giugno 2023.

Pdcm – Presidenza del Consiglio dei Ministri, Sistema di informazione per la sicurezza della Repubblica, Dipartimento delle Informazioni per la Sicurezza (2013) (a cura di), *Il linguaggio degli organismi informativi. Glossario Intelligence*, Roma, De Luca Editori.

Pdcm– Presidenza del Consiglio dei Ministri, Sistema di informazione per la sicurezza della Repubblica, Dipartimento delle Informazioni per la Sicurezza (2023) (a cura di), *Relazione Annuale sulla Politica dell'Informazione per la Sicurezza 2022*, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2023/02/Relazione_annuale_2022_interattiva.pdf. Consultato il 6 settembre 2023.

Rapetto, U. e Di Nunzio, R. (2001), *Le nuove guerre*, Milano, Rizzoli.

Rattray, G. J. (2001), *Strategic Warfare in Cyberspace*, Cambridge, MIT Press.

Santaniello, M. (2022), *Live Chat con Michele Mezza su Net-war Ucraina: come il giornalismo sta cambiando la guerra*, in «Rivista di Digital Politics», 2(3), pp. 539-548.

Scott, L. e Jackson, P. (2004), *The Study of Intelligence in Theory and Practice*, in «Intelligence and National Security», 19(2), pp. 139-169.

Schaurer, F. e Störger J. (2013), *The Evolution of Open Source Intelligence (OSINT)*, in «Journal of U.S. Intelligence Studies», 19(3), pp. 53-56.

Shannon, C. E. (1948), *A Mathematical Theory of Communication*, in «The Bell System Technical Journal», 27(3), 379-423.

Shannon, C. E. e Weaver, W. (1949), *The Mathematical Theory of Communication*, Urbana, University of Illinois Press.

Shpiro, S. (2001), *The Media Strategies of Intelligence Services*, in «International Journal of Intelligence and CounterIntelligence», 14(4), pp. 486-502.

Shulsky, A. N. e Schmitt, G. J. (2002), *Silent Warfare: Understanding the World of Intelligence*, Dulles, Brassey's Inc.

Simmons, R. M. (1995), *Open source intelligence: an examination of its exploitation in the defense intelligence community*, Washington D.C., Defense Intelligence College.

Smith, T., Revell, Q. e Stacey, R. (2017), *Tools for Osint-based Investigations*, in B. Akhgar, P., Saskia Bayerl e F. Sampson (a cura di), *Open Source Intelligence Investigation: From Strategy to Implementation*, Basilea, Springer, pp. 153-166.

Steele, R. D. (2006), *The Open Source Intelligence Cycle*, in L. K. Johnson (a cura di), *Handbook of Intelligence Studies*, Abingdon, Routledge, pp. 139-146.

Steele, R. D. (1995), *The Importance of Open Source Intelligence to the Military*, in «International Journal of Intelligence and CounterIntelligence», 8(4), pp. 457-470.

Taylor, M. C. (2005), *Open Source Intelligence Doctrine*, in «Military Intelligence Professional Bulletin», 4, pp. 12-14.

Tekir, S. (2009), *Open Source Intelligence Analysis. A Methodological Approach*, Riga, VDM Verlag.

Teti, A. (2015), *Open Source Intelligence & Cyberspace. La nuova frontiera della conoscenza*, Soveria Mannelli, Rubbettino.

Teti, A. (2020), *Virtual Humint. La nuova frontiera dell'Intelligence*, Soveria Mannelli, Rubbettino.

Toffler, A. (1980), *The Third Wave*, New York, Morrow.

Tsu, Z. (2013), *L'arte della guerra*, Milano, Feltrinelli.

Turbeville Jr, G. H., Prinslow, K. E. e Waller, R. E. (1999), *Assessing Emerging Threats Through Open Sources*, in «Military Review», 5, pp. 72-75.

Vero, S. (2005), *Le strutture profonde della comunicazione*, Acireale, Bonanno Editore.

Volli, U. (2014), *Il nuovo libro della comunicazione*, Milano, Il Saggiatore.

Waltz, E. (1998), *Information Warfare: Principles and Operations*, Boston, Artech House.

Williams, H. J. e Blum, I. (2018), *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Santa Monica, Rand Corporation Publishing.

Wolf, M. (1997), *Teorie delle comunicazioni di massa*, Milano, Bompiani.

Ju, Y., Li, Q., Liu, H. Y., Cui, X. M. e Wang, Z. H. (2020), *Study On Application Of Open Source Intelligence From Social Media In The Military*, in «Journal of Physics: Conference Series», doi:10.1088/1742-6596/1507/5/052017

Zarca, P. (1995), *Le fonti aperte: uno strumento essenziale dell'attività di intelligence*, in «Per Aspera Ad Veritatem», SISDE, 1, pp. 237-238.

Ziółkowska, A. (2018), *Open Source Intelligence (OSINT) as an element of military recon*, in «Security and Defence Quarterly», 19(2), pp. 65-77.