ISSN 2421-4442

SicurezzaTerrorismoSocietà

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

18
2023

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

18

ISSUE 2/2023

Milano 2023

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 18/2023

Direttore Responsabile:

Matteo Vergani (Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou (Lecturer at National Security School – Atene)
Cristian Barna ("Mihai Viteazul" National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti (senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies – Roma)
Valerio de Divitiis (Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio (Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel (London School of Economics – London)
Rovshan Ibrahimov (Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler (German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš (Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi (Università Cattolica del Sacro Cuore – Milano)
Anita Perešin (University of Zagreb – Croatia)
Giovanni Pisapia (Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj (University of Ljubljana)
Eman Ragab (Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli (Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick (University of Aarhus – Denmark)
Arturo Varvelli (Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz (Independent Researcher – Turkish National Police)
Munir Zamir (Fida Management&C7 – London)
Sabina Zgaga (University of Maribor – Slovenia)
Ivo Veenkamp (Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni (Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa (Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini (Università Cattolica del Sacro Cuore – Milano)
Marco Maiolino (Università Cattolica del Sacro Cuore – Milano)
Davide Scotti (Università Cattolica del Sacro Cuore – Milano)

© 2023 EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 979-12-5535-198-6

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Terrorism & Digital Ecosystems

Federico Borgonovo, Giulia Porrino, Silvano Rizieri Lucini
Propaganda Hybridation: PMC Wagner Exploitation
of Islamic State Content 7

Ali Fisher
Time to be realistic about Swarmcast2.0:
How terrorists use WhatsApp 15

Francesco Balucani, Fabio Ottaviani
L'Italia alla prova del fondamentalismo radicale islamico 35

Evolving security issues & perspectives

Giacomo Buoncompagni
Within the informative-cultural chaos. Migration issue,
national politics and anti-Jewish conspiracy 59

Kamil Yilmaz
Hate speech predicts engagement on social media:
A case study from Turkey 79

Barbara Lucini
Medical Intelligence: definizione, metodi, prospettive
e gruppo nazionale Medint 113

Rene D. Kanayama
Dispute over the Nagorno-Karabakh – A Local Conflict
with Global Implications 131

Medical Intelligence: definizione, metodi, prospettive e gruppo nazionale Medint

Barbara Lucini

Barbara Lucini (phd in Sociology and Methodology of Social Research), is Researcher at the Faculty of Arts and Philosophy, Catholic University of Sacred Heart, Milan.
She is senior Researcher at the Italian Team for Security Terroristic issues and Managing Emergencies – ITSTIME. She is coordinating the research activities of the EU Project – H2020 – CounteR – Countering Radicalisation for a Safer World Privacy-first situational awareness platform for violent terrorism and crime prediction, counter radicalisation and citizen protection.
She is professor of Theories and Techniques of Media Communication Faculty of Arts and Philosophy, Catholic University of Sacred Heart, Milan.
She has been involved in the scientific coordination of several research projects (European and others) focused on crisis management, risk communication, risk perception, security, resilience, radicalisation and extremisms. Her research interests are oriented to sociology of disaster, disaster resilience, disaster management, extremisms and radicalisation. Further, the issue of the relation between terrorism and resilience as well as political extremism have been studied. She is the author of several publications and the Disaster Resilience from a Sociological Perspective Exploring Three Italian Earthquakes as Models for Disaster Resilience Planning, Springer International Publishing, 2014; The Other Side of Resilience to Terrorism A Portrait of a Resilient-Healthy City, Springer International Publishing, 2017

Abstract

This paper, for the first time in Italy, offers a reflection on the theme of Medical Intelligence which has become increasingly crucial over the last few years, due to the occurrence of events such as the Covid-19 pandemic in 2020, the Russian-Ukrainian war and the Israeli-Palestinian war; all events which possess characteristics of interdependence, mutual influence and high levels of uncertainty and complexity.
The focus of this paper concerns not only an innovative definition of Medical Intelligence and its specific areas of study, but also the consideration of the possibilities it offers in revising the intelligence process, in light of the impact of new technologies and the characteristics of emerging threats. Specific attention will then be devoted to the establishment and launch of the national Medical Intelligence group at the Università Cattolica del Sacro Cuore in Milan.
Finally, perspectives and lines of work that are already being developed to continue to expand the knowledge of Medical Intelligence in a rapidly changing world will be proposed.

Keywords

Medical Intelligence, Medint, Intelligence, Covid-19, pandemics

1. Introduzione

Gli ultimi anni sono stati caratterizzati da grandi cambiamenti presenti in tutto il mondo, con forti impatti sulle società coinvolte che stanno ridefinendo il rapporto fra i singoli ma anche fra le Nazioni.

Dall'inizio del 2020, la diffusione dell'epidemia da Covid-19 prima in Cina e poi in tutto il resto del mondo ha posto le persone e gli Stati nazionali di fronte a questioni fondamentali di sicurezza fisica personale e pubblica, variamente alimentati dai dibattiti sull'etica e sulla legalità delle misure poste per gestire e contenere le crisi.

La gestione della pandemia del 2020 e per gli anni a seguire è fonte inesauribile di riflessioni non solo sugli aspetti più specifici del crisis management ma anche per le tematiche relative alla sicurezza nazionale e alle pratiche di intelligence ad essa collegate.

La pandemia da Covid-19 ha mostrato, come sempre i disastri fanno, l'essenza di un mondo e di relazioni internazionali fragili, compromesse nel loro divenire perché collocate in una zona di limbo che ricade verso società ormai profondamente radicali (Lucini, 2023) e nelle quali le relazioni interpersonali fisiche e digitali appaiono polarizzate e senza possibilità di mediazione reciproca.

In uno scenario mondiale, caratterizzato da eventi con un impatto trasformativo dei più alti nella storia post-moderna è essenziale poter comprendere il ruolo che le informazioni raccolte possono giocare nel monitoraggio della situazione, nella comprensione e definizione della minaccia e da ultimo, nella possibilità di prevenire fatti avversi.

A questo riguardo, sia la guerra russo – ucraina iniziata nel 2022 sia quella israelo- palestinese nel 2023 pongono l'attenzione sulla necessità di implementare le modalità di raccolta delle fonti e della loro analisi interpretativa, così da poter successivamente adeguare politiche di sicurezza efficaci nel loro scopo, considerando le caratteristiche della minaccia e il contesto di sviluppo.

In questo scritto, preso atto del contesto mondiale profondamente conflittuale, interconnesso e interdipendente nel quale tutti viviamo e di un Uomo nuovo digitale, si vuole proporre una analisi sistematica della Medical Intelligence come attività fondante una nuova visione dell'uomo e della sicurezza considerata nella sua multidimensionalità.

Un primo elemento da considerare, in un'ottica più ampia ma con ricadute specifiche nella definizione di Medical Intelligence, è la definizione di Uomo che, partendo dalla tradizione specificatamente umanista che ha accompagnato per secoli una certa parte del mondo, si scopre essere in rela-

zione con un contesto sempre più digitale e dal quale viene profondamente influenzato in ogni sua attività.

L'emergere dell'Uomo Digitale, le cui azioni e relazioni si collocano inevitabilmente al crocevia fra la dimensione off-line e quella on-line è un dato caratteristico da considerare nell'ambito della Medical Intelligence per cui il fattore umano deve essere ricollocato al centro delle riflessioni.

Questa visione apre alla necessità di considerare i rapporti fra gli uomini e le tecnologie, il loro ruolo nella definizione e nella formazione di relazioni interpersonali che contano nel settore dell'intelligence ma anche nelle più ampie esperienze di vita generale.

A questo riguardo è importante non dimenticare le parole dell'archeologo Ranuccio Bianchi Bandinelli citato da Broccoli (2019): "*Il mondo costruito su un modello di civiltà prevalentemente tecnica, che non ha il coraggio di essere storicizzato, è retto, in realtà, dalle forze politiche che governano la tecnica.*"

Questa prospettiva pone in luce due elementi essenziali nella riflessione più ampia sulla Medical Intelligence: da un lato si riconosce l'avanzare del ruolo delle tecnologie nelle società moderne e post- moderne, spesso però vissuto come fatto ineluttabile, per il quale si può agire con poche azioni autonome e determinate; dall'altro lato si apre alla questione precipua ovvero la considerazione che la mancanza di contestualizzazione storica, spesso così presente nelle nostre società, porta inevitabilmente non tanto alla predominanza della tecnica, quanto alla prevalenza delle scelte politiche che governano proprie le tecnologie.

È questa una differenza sostanziale nella definizione dell'Uomo digitale e delle sue possibilità concrete e reali affinché le sue azioni svolgano un ruolo centrale nell'orientare le relazioni sociali e con esse dare forma al mondo che si vive.

L'apertura alla Medical Intelligence e ad una sua innovativa visione ha come obiettivo quello di scandagliare le dinamiche uomo – contesto con particolare attenzione ai dati che sono propri degli uomini, quelli sanitari e quelli tipici degli ambienti fisici e digitali.

La presente riflessione si contestualizza non solo per la sua rilevanza nella definizione di un ambito di studi, metodologico e operativo essenziale per la sicurezza nazionale e internazionale ma anche per la considerazione delle minacce emergenti che interessano e intersecano la Medical Intelligence, fra cui:

- le relazioni internazionali sempre più conflittuali e destabilizzanti che si esplicitano in ecosistemi sociali sempre più interdipendenti ma anche estremamente fragili e vulnerabili;

- la dimensione cyber che mostra un mondo sempre più sotto attacco e i dati sanitari esposti e vulnerabili all'uso malevolo da parte di hacker, gruppi criminali e terroristici;
- le possibili nuove epidemie e pandemie che possono svilupparsi alla luce di un mondo interconnesso e con continui scambi quotidiani, considerando anche il ruolo del cambiamento climatico;
- tematiche relative ai dati di persone transgender legate alla stereotipizzazione e discriminazione di certe comunità;
- lo sfruttamento di dati da parte di gruppi criminali appartenenti a persone e comunità affette da malattie mentali.

Da queste minacce così multiformi e presenti contemporaneamente nel mondo digitale ovvero quello che allo stato attuale include sia la dimensione off-line sia quella on-line virtuale diventa essenziale, proprio per il raggiungimento dello scopo generale ovvero la sicurezza nazionale e internazionale in un'epoca di grandi cambiamenti, analizzare il tema della Medical Intelligence proponendone una visione differenti e contestualizzata all'attualità.

2. Medical Intelligence: definizioni e prospettive

Fin dalle sue origini la storia della Medical Intelligence si colloca in ambito militare e muove i primi sviluppi proprio considerando i dati sanitari degli eserciti impegnati nei vari conflitti.

Ciò non stupisce, in quanto, molto spesso, nel corso della storia umana le grandi scoperte e invenzioni sono avvenute proprio durante le guerre e prendendo spunto dalle riflessioni che emergevano in contesti così deprivanti ed estremamente ostili.

Un iniziale dato storico relativo alla Medical Intelligence viene proposto da Marble (2020) che riporta la prima definizione di Medical Intelligence durante la Seconda Guerra Mondiale ovvero: "*la collezione, analisi e diffusione di informazioni mediche di importanza per le nostre truppe che operano in tutte le parti del mondo.*"[1]

Il focus era quindi orientato alla conoscenza di dati sanitari delle truppe impegnate al fronte e alla loro sicurezza fisica nazionale.

In relazione a questo e alla rilevanza sia del dato storico sia della Medical Intelligence in ambito militare, è bene ricordare che l'epidemia di influenza Spagnola che ha imperversato nel mondo fra il 1918 e il 1920 e i cui primi

[1] In lingua inglese nel testo originale: "*The collection, analysis, and dissemination of medical information of importance to our troops operating in all and any parts of the world. —World War II definition of medical intelligence*." (Marble, 2020).

casi si ebbero presso il campo di addestramento statunitense di Camp Funston, nel Kansas dove da qui poi si propagò attraverso i soldati che tornavano a casa dal fronte.

L'ambiente militare è quindi storicamente il primo ambito sistematico nel quale vengono condotte analisi e studi relativi ai dati sanitari raccolti e dove prende avvio la Medical Intelligence.

Per molti autori la Medical Intelligence ha a che fare quindi con la raccolta di informazioni e dati sanitari mentre per esempio Jarcho (1991) focalizza la sua definizione sullo scopo delle attività di Medical Intelligence ovvero: "*l'applicazione di conoscenze mediche e biologiche per la difesa nazionale.*"[2]

Il periodo storico nel quale questa definizione si sviluppa è interessante per comprendere la specificità dello scopo della difesa nazionale. Infatti, emerge da qui la prospettiva di difesa che è stata tipica di una visione tradizionale e militare della Medical Intelligence per la quale lo scopo di tale attività era la stretta difesa della sicurezza nazionale e dei suoi interessi. L'ambito nazionale, contestualizzando gli eventi nella contemporaneità non risulta più l'unico da considerare bensì è il livello internazionale e transnazionale ad avere preso il posto della definitezza nazionale.

Nel corso degli anni, le definizioni di Medical Intelligence si fanno via via più articolate, considerando la crescente complessità delle relazioni sociali e del mondo in generale.

A questo riguardo, la definizione proposta da La Gioia (2015): "*un processo sistematico di collezione e analisi di pericoli per la salute, minacce per la salute, rischi per la salute e capacità mediche in una specifica area*"[3] ha il merito di porre in risalto tre dimensioni fondamentali per la comprensione di fenomeni che possono minare la sicurezza nazionale e internazionale: pericoli, minacce e rischi che affondano la loro epistemologia sul versante informativo, di collezione di dati e di definizione degli eventi tipici delle pratiche di intelligence.

Nel corso degli anni, sempre più maggiore attenzione viene posta alle questioni mediche e ai loro risvolti per la sicurezza nazionale e internazionale. Un'ulteriore definizione che concentra l'attenzione sulla pratica di intelligence prima e successivamente sulla tipologia di informazioni è quella proposta dal Military Committee Terminology Board – NATO: "*l'intelligence*

[2] In lingua inglese nel testo originale: "*the application of medical and biological knowledge to national defence*" *(Jarcho, 1991).*

[3] In lingua inglese nel testo originale: "*a systematic process of collection and analysis of health hazards, health threats, health risks and medical capabilities in a specific area*" *(La Gioia, 2015).*

derivata da informazioni mediche, bio-scientifiche, epidemiologiche, ambientali e altre informazioni relative alla salute umana e animale (2021)."[4]

Attraverso questa definizione l'attenzione è rivolta al processo di intelligence e poi ad una serie di informazioni che possono essere molteplici sia per tipologia sia per ambiti considerati, con il fine ultimo di riguardare tutte la salute umana e animale. Tale definizione è stata proposta nel 2021 ma manca completamente un riferimento, anche minimo, al contesto di sviluppo di tali pratiche. Infatti, non viene menzionato né l'ambiente naturale o artificiale né la dimensione digitale della vita contemporanea: due elementi questi che, a parere di chi scrive, risultano invece essenziali se mediante l'apporto della Medical Intelligence, lo scopo finale sia la sicurezza nazionale e internazionale.

Infine, ancora più attuale risulta la definizione di Medical Intelligence proposta dall' Office of the Chairman of the Joint Chiefs of Staff: "*quella categoria di intelligence risultante dalla raccolta, valutazione, analisi e interpretazione di informazioni mediche, bio-scientifiche e ambientali straniere che che siano di interesse per la pianificazione strategica e per la pianificazione e le operazioni medico-militari per la conservazione della forza di combattimento delle forze amiche e per la formazione di una valutazione delle capacità mediche straniere sia nel settore militare che in quello civile.*"[5]

In questo senso, la Medical Intelligence appare essere considerata una delle varie tipologie di intelligence con due novità di interesse: l'utilizzo delle risultanze per fini di pianificazione strategica e per la conservazione delle proprie risorse personali; l'apertura verso il settore civile delle capacità mediche interessate.

Quelle fino ad ora considerate sono le più utilizzate e conosciute definizioni di Medical Intelligence sia da una prospettiva storica sia concettuale che risultano essere al momento limitate o mancanti di una visione che possa includere gli elementi innovativi emersi con l'impatto della pandemia da Covid-19 e con la sua gestione. Evento questo che ha promosso enormi cambiamenti in relazione a diverse dimensioni della vita sociale delle persone e alla loro sicurezza percepita e agita. Tutti questi mutamenti si sono tradotti in nuove minacce – altre pandemie, guerre, conflitti urbani, violenza diffu-

[4] In lingua inglese nel testo originale: *"intelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health" (Military Committee Terminology Board, NATO, 2021).*

[5] In lingua inglese nel testo originale: *"that category of intelligence resulting from collection, evaluation, analysis, and in-terpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors."(Office of the Chairman of the Joint Chiefs of Staff, 2022).*

sa – che necessitano di essere compresi come scenario all'interno del quale si vuole promuovere una definizione di Medical Intelligence funzionale e adeguata alla contemporaneità.

Per raggiungere tale scopo, si ritiene utile proporre un modello di analisi dell'attuale concettualizzazione della Medical Intelligence e, dopo avere declinato alcune riflessioni specifiche per la componente Medical e quella Intelligence, lo stesso modello verrà considerato per la proposta di una nuova definizione.

Gli elementi che costituiscono il modello di analisi delle maggiori prospettive di Medical Intelligence considerante fino ad ora sono i seguenti:

1. Focus tematico;
2. Ambito (scenario organizzativo da una prospettiva più operativa)
3. Dimensione legata all'ambito;
4. Funzione e scopo;
5. Metodi e tecniche.

Applicando tale modello alle definizioni considerate emerge quanto segue:

1. Focus tematico: prevalentemente orientato all'aspetto medico meno alle pratiche di intelligence e al suo processo di raccolta e analisi delle informazioni;
2. Ambito (scenario organizzativo da una prospettiva più operativa): militare in modo preponderante, con la considerazione di attività di peacekeeping e un'apertura verso gli ultimi anni al settore civile coinvolto al principale ambito militare;
3. Dimensione legata all'ambito: prevalentemente operativa – tattica;
4. Funzione e scopo: difesa degli interessi nazionali e sicurezza militare;
5. Metodi e tecniche: Humint e Virtual Humint (Teti, 2019)

3. L'aspetto "Medical" della Medical Intelligence: prospettive e implicazioni

Dall'avvento della pandemia nel 2020 sono stati chiari a tutti i cambiamenti che l'impatto di una simile crisi avrebbe causato nella vita di tutte le persone, nessuno escluso.

Riferendosi alla Medical Intelligence emergono alcuni orientamenti che supporteranno la definizione che si darà al termine dell'analisi.

Un primo aspetto concerne l'elemento della corporeità: come dimenticare l'esposizione mediatica delle prime vittime da Covid-19, intubate o ventilate tramite i caschi, immobile nell'impossibilità di combattere contro un agente che ancora non si conosceva?

Corpi esposti, resi simbolo di una battaglia che si stava combattendo senza conoscere il nemico che invece si palesava in tutta la forza di stremare le persone colpite.

Gli stessi corpi oggetti di dibattito pubblico nei pezzi delle varie guerre contemporanee che si stanno combattendo, nemmeno così lontano dalla propria casa: il massacro di Buča a Marzo 2022 così come altre violazioni e massacri di altri conflitti combattuti in varie parti del mondo.

Un corpo che è oggetto di riflessioni sociologiche (Featherstone et al, 1991) perché, in modo primario, è attraverso di esso che entriamo in relazione con gli altri e si definiscono gli spazi vitali di ognuno, a volte infranti, a volte abusati.

Questa corporeità è in diretta relazione con le questioni legate ai dati medici e sanitari che costituiscono la prima parte dell'elemento di Medical Intelligence e che caratterizzano le prospettive epidemiologiche che spesso sono associate come le prioritarie per questo ambito di studi.

Nonostante ciò, il corpo assume ulteriore valenza nella relazione fisica che si esplicita fra corpo e ambiente naturale: un dato questo emerso per esempio mediante i tentativi di comprensione dell'inizio della pandemia da Covid-19 per la quale si supponeva un contatto diretto fra animali infetti e persone.

Questo rappresenta un secondo aspetto chiave nella presente riflessione poiché pone in evidenza il sistema relazione fra uomo e la sua dimensione fisica esplicitata dagli ecosistemi naturali.

In questo modo è possibile argomentare la necessità di includere sia la dimensione medica, strettamente riferita al dato medico per sé, sia la dimensione di salute che racchiude la relazione fra persone ed ecosistemi.

Questa prospettiva significa sviluppare la definizione di Medical Intelligence considerando tutte le aree e le tematiche che sono trasversali ai due principali orientamenti (medico e di salute).

Infatti, diventa essenziale in accordo allo scenario prima descritto considerare le intersezioni e la trasversalità delle aree tematiche che si pongono in relazione alla Medical Intelligence.

Per anni, per esempio, si è trattato del tema della Medical Intelligence in relazione al rischio CBRN considerando le caratteristiche specifiche di questa tipologia di rischio e le sue correlate implicazioni.

Ad oggi, però comprendiamo che il rischio CBRN non può essere considerato unicamente nella sua espressione di rischio verso la vita umana, animale o la sopravvivenza di infrastrutture critiche, quanto devono essere rilevate anche le dimensioni più ampie che esso abbraccia come quella tecnologia nella sua dimensione digitale.

Emerge quindi da questa riflessione la necessità di riconsiderare il concetto Medical secondo un'accezione più ampia, atta ad includere elementi che, sebbene non specificatamente medici o relativi ad aspetti di salute umana o animale, giocano un ruolo rilevante di interconnessione fra aspetti molteplici della più ampia Medical Intelligence.

Guardando alla struttura eco-sistemica di queste relazioni emerge come ciò che deve interessare nella definizione e identificazione degli aspetti Medical, non siano più i singoli punti che connettono due ambiti, per esempio Medical e rischio epidemiologico, ma la relazione fra quei punti, sviluppando un'ottica policentrica e non di relazione diretta tra un punto e l'altro di un eco-sistema.

Il policentrismo, considerato in relazione ad uno o più contesti eco-sistemici considerati è lo strumento metodologico che permette di considerare argomenti trasversali a quello strettamente Medical ma comunque rilevanti per gli scopo più ampi della Medical Intelligence.

4. Intelligence: riportare l'informazione al centro della Medical Intelligence

Nell'attuale scenario critico, contraddistinto da crescenti conflitti interdipendenti, le attività di intelligence assumono un ruolo centrale per orientare decisioni politiche e seguenti pratiche operative.

Nel corso dei decenni si è andato sempre più riflettendo sulla definizione di intelligence e sulle sue implicazioni metodologiche ed etico -legali sia per chi la pratica sia per tutti i cittadini (Antiseri e Soi, 2013).

Nell'immaginario collettivo e spesso non solo in quello, l'intelligence sconta la percezione di considerare quasi unicamente come attività di intelligence quelle di spionaggio alle quali sono state dedicate grandi film e idealizzazione di personaggi per il grande pubblico.

Le attività di intelligence sono invece un sistema complesso di azioni che hanno al loro centro le informazioni: dalla raccolta, alla sistematizzazione, all'analisi e alla interpretazione.

Lavoro complesso che richiede necessariamente conoscenze ampie ma allo stesso tempo approfondite sia dei fenomeni sia delle tecniche per il monitoraggio e la previsione.

L'informazione è elemento distintivo e assume un ruolo fondamentale per identificare l'ambito di studi specifico al quale l'intelligence può appartenere: *"Per disegnare un possibile ambito scientifico per l'intelligence un primo settore include certamente le scienze dell'informazione, con particolare riguardo a temi emergenti di fondamentale importanza per il trattamento dell'informazione, come data science, big data analytics e intelligenza artificiale. La*

raccolta, l'analisi, il trattamento, la diffusione e l'utilizzo dell'informazione è un'area sempre più decisiva della società." (Caligiuri e Pili, 2020)

Inoltre, l'informazione è elemento centrale nel processo di intelligence perché attraverso di essa si crea la conoscenza necessaria del fenomeno e si sviluppa la cognizione di fenomeni che possono minare la sicurezza nazionale e internazionale, Caligiuri (2016) a questo riguardo ricorda che: "*L'intelligence è un metodo efficiente di raccolta e gestione delle informazioni, uno strumento fondamentale per fornire elementi utili all'assunzione di decisioni, adoperato dagli Stati nazionali e dalle imprese private.*"

Un'altra definizione interessante di intelligence è quella proposta da Capezzani (2023) che sottolinea la duplice natura di metodo e processo nonché la natura scientifica delle attività: "*[…] l'intelligence come metodo di trattazione delle informazioni necessarie a soddisfare il fabbisogno informativo dei decisori, statuali e non statuali, e a tutelare i loro interessi, non è una mera raccolta di informazioni ma un'attività scientifica guidata da prassi ipotetica-interpretativa. Si tratta di un metodo e un processo che da indizi pre-conoscitivi e nella formulazione di un'ipotesi di ricerca indirizza la raccolta, la selezione, l'analisi, l'interpretazione delle informazioni e che nella valutazione delle interpretazioni stesse genera conoscenza.*"

Figueroa et al. (2021) riportano la definizione di Sherman Kent il quale aggiunge alla dimensione di processo, quella di prodotto e di identificazione di una organizzazione che conduce attività di intelligence:

> *Uno dei primi a definire l'attività di intelligence è stato Sherman Kent 10 nel campo della sicurezza nazionale, dove ha identificato tre componenti importanti:*
> *a) Il prodotto derivante dalla gestione e dalla trasformazione di informazioni e conoscenze;*
> *b) l'organizzazione che svolge questa attività;*
> *c) I processi attraverso i quali viene svolta.*[6]

Questa definizione risulta utile per approfondire anche gli ambiti e i contesti all'interno dei quali il processo e le attività di intelligence prendono forma.

Sherman Kent prima citato da Figueroa et al. (2021) pone in evidenza come l'intelligence così identificata si colloca essenzialmente nel dominio

[6] In lingua inglese nel testo originale: "*One of the first to define intelligence activity was Sherman Kent 10 in the field of national security where he identified three important components:*
a) The product derived from the management and transformation of information and knowledge
b) The organization that carries out this activit
c) The processes through which it is carried out" Figueroa et al. (2021)

della Humint, per il quale la dimensione di riferimento è quella del mondo fisico – reale e il tempo quello presente.

Questa unicità della dimensione spaziale fisica è considerata da Sironi (2022) come un limite rispetto alla caratteristiche degli scenari e delle minacce contemporanee: *"La Humint sconta il limite principale della sua dimensione fisica, con la necessità di interfacciarsi direttamente con il soggetto da cui si intende elicitare quanto necessario." (Sironi (2022).* Altre argomentazioni per la definizione di Humint pongono in risalto la sua valenza nel definire il quadro cognitivo all'interno del quale ci si muove attraverso la raccolta delle informazioni: *"Si precisa che "la Humint è la tecnica di intelligence, tra le altre, che può fornire un quadro cognitivo più attendibile e verificabile, perché si basa essenzialmente su contatti diretti e reali con le fonti, utilizzando risorse umane sul campo, ed eliminando tutte le possibili intossicazioni derivanti dalla distanza geografica, dall'assenza del contatto fisico e dall'elemento temporale."[…]" Teti (2019).*

La Humint così intesa è stata però ampiamente superata dall'avvento dei social network, i quali hanno spostato l'attenzione verso le relazioni virtuali, creando quelle che Tosoni (2004) ha definito *"identità virtuali"* portatrici di nuovi sistemi relazionali, comunicativi, culturali e che hanno visto una forte espansione che nel corso dei decenni, assumendo forme sempre più diverse: dai primi forum e community online alle chat di Telegram o ai gruppi di WhasApp solo per fare alcuni esempi.

L'impatto delle tecnologie virtuali nella vita quotidiana di miliari di persone ha avuto anche l'esito di incrementare la relazionalità e la comunicazione di gruppi criminali e terroristi, eliminando i vincoli e le distanze spaziali e temporali e portando alla nascita di quella che è stata chiamata la Virtual Humint.

Il concetto di Virtual Humint appare per la prima volta, come ricorda Teti (2019), nella pubblicazione *Countering the New Terrorism* pubblicata da Ian Lesser e colleghi. per RAND Corporation nel 1998 e prende avvio proprio attraverso il monitoraggio dei primi Forum online per monitorare attività legate a possibili azioni terroristiche.

A questo riguardo, una definizione generale di Virtual Humint è quella proposta da Teti (2019), il quale concentra poi la sua attenzione sulle possibili tecniche di applicazione della Virtual Humint: *"La virtual human intelligence, o virtual humint, al pari della human intelligence, focalizza la sua attenzione sulla ricerca, l'identificazione, il reclutamento e la gestione di fonti umane, ma a differenza di quella tradizionale, utilizza tecniche e metodologie all'interno dei social media."*

Nel corso degli anni si è reso però sempre più evidente che la relazione fra Humint e contesto, come per esempio quello virtuale, assumesse un valore

informativo completamente diverso da quello immaginato, in quanto, lo stesso contesto online è un elemento di produzione di identità virtuali (Tosoni, 2004) che sono altro da una mera applicazione delle identità fisiche ad un contesto online.

Quest'ultimo, come è emerso anche da ricerche condotte in ambito europeo (Lombardi et al., 2020), è costituito da un insieme di funzioni e possibilità che portano alla creazione di identità sociali differenti in interazione fra loro fautrici di informazioni "altre" rispetto a quelle che potrebbero emergere se questo processo avvenisse nell'unico spazio fisico.

Da ciò si desume che il contesto online e le sue caratteristiche possiedano capacità trasformative in grado di influire sia sul processo relazionale online sia su quello informativo di tutti coloro che ne sono coinvolti e, ovviamente, da questa diffusione di informazioni emergono differenti capacità e di percezione e di interpretazione dei fenomeni oggetto di attenzione.

A fronte di questa capacità di mutamento e di influenza nella definizione delle identità sociali online, il passaggio successivo per adeguare il processo di intelligence ad un contesto in forte mutamento è stato quello della Digital Humint definita da Lombardi et al. (2015) come un: "*[…] connubio fruttuoso tra la pratica della Humint (Human Intelligence), parte costituente a pieno titolo e sin dalla sua origine del ciclo di intelligence, e l'approccio legato alle nuove fonti social.*"

La Digital Humint diventa, ad oggi, l'approccio e la prospettiva più adeguata per comprendere i fenomeni attuali e per leggere cognitivamente le informazioni che vengono considerate (Lucini, 2022): essa infatti porta con sé le pratiche tipiche della Humint tradizionale, in particolare ricordando il ruolo centrale del fattore umano nella sua fisicità, come la Medical Intelligence e gli approcci specifici agli ambienti digitali che permettono di focalizzare l'attenzione sulla tipologia di informazione e sul quadro cognitivo – relazionale all'interno del quale essa viene prodotta e diffusa.

Dall'evoluzione della Humint applicata ai nuovi contesti digitali e alle future possibilità offerte dalle nuove tecnologie come, per esempio, l'intelligenza artificiale e il Metaverso emergono alcuni elementi che per lo sviluppo futuro dell'Intelligence correlata alla parte "Medical" risultano essere di fondamentale importanza:

1. La rilevanza del fattore umano nell'approccio informativo alla Medical Intelligence, considerando le istanze etico – legate che si stanno delineando con la costituzione dell'Uomo Digitale;
2. La necessità di focalizzarsi sulle caratteristiche del contesto (digitale) dal quale le informazioni vengono raccolte. Ciò anche per implementare nella pratica di intelligence la consapevolezza della situazione socio-relazionale e tecnica- cognitiva all'interno del quale le informa-

zioni vengono identificare e raccolte (U.S. Department of Defence, 2023);

3. Comprendere l'importanza delle relazioni sociali digitali che si vanno a creare fra i vari attori che costituiscono un processo di intelligence e il ruolo che esse hanno nel ciclo dell'informazione, dalla identificazione all'interpretazione;
4. La Digital Humint assume valore metodologico per l'approfondimento della Medical Intelligence, in quanto racchiude in sé gli elementi tecnologici e cognitivi-informativi che possono meglio orientare la comprensione di minacce emergenti più direttamente connesse al settore medico-sanitario, senza dimenticarne la trasversalità con altri settori.

5. Il gruppo nazionale di lavoro Medint – Università Cattolica, Milano

Per riflettere sulle tematiche della Medical Intelligence e sviluppare questa tematica con le opportune considerazioni teoriche, metodologiche e operativa, tenendo conto delle implicazioni etiche e legali che tale materia prevede, è stato istituito con comunicazione del 18 Marzo 2023[7] presso l'Università Cattolica di Milano, il primo gruppo nazionale di Medical Intelligence (email: medint@unicatt.it).

Tale gruppo è costituito da una cinquantina di esperti che coprono differenti ambiti trasversali alla Medical Intelligence, quali:

- nuove tecnologie e sviluppo di intelligenza artificiale in ambito medico – sanitario;
- rischi sanitari e correlati (epidemie, CBRN, ecc.);
- metodologie osint e metodologie di intelligence.

Gli ambiti disciplinari che caratterizzano questo gruppo di lavoro sono militare, medico-sanitario, ingegneria, psicologia, sociologia, politiche per la sicurezza e la prospettiva alla quale si tende è quella multidisciplinare, così da poter fare emergere la necessità di lavorare per uno sviluppo della Medical Intelligence, settore sempre più strategico per la sicurezza nazionale e internazionale, contestualizzato nel presente ma con visioni aperte al futuro.

Il gruppo di lavoro nasce da due incontri sul tema della Medical Intelligence che si sono tenuti presso l'Università Cattolica del Sacro Cuore – Milano.

[7] https://news.socint.org/intelligence-costituito-nella-societa-italiana-di-intelligence-il-gruppo-di-lavoro-dedicato-alla-medical-intelligence.

Il primo intitolato "Medical Technical Intelligence", il 23 Giugno 2022, il cui scopo è stato di riunire esperti e professionisti per riflettere circa le attuali definizioni di Medical Intelligence e gli ambiti tecnici – operativi all'interno dei quali si stava sviluppando.

Il secondo incontro invece è stata la prima conferenza internazionale "Medical Intelligence", il 26 Gennaio 2023, che aveva come finalità quella di discutere insieme ad un panel di esperti, anche internazionali e con esperienze professionali variegate, il tema della Medical Intelligence e le sue molteplici declinazioni.

I prossimi passi del gruppo nazionale sono quelli di definire i contorni di una disciplina che si interseca con molteplici tematiche di attualità e che richiede una riflessione continua sulle metodologie da utilizzare e le valenze etiche e legali che possono interessare.

In particolare, si evincono alcuni temi di sviluppo di immediato futuro per la loro importanza strategica sui quali già si sta lavorando:

- MedInt e pandemie
- MedInt e rischi medico – sanitari
- MedInt e guerre
- MedInt e nuove tecnologie
- MedInt e attività di vari gruppi criminali

A questo riguardo, un tema che merita particolare attenzione e approfondimento è quello della Medical Intelligence applicata ai grandi eventi e ciò per varie ragioni di sicurezza nazionale, internazionale, logistica, infrastrutturale.

Dal 06 al 22 Febbraio 2026 a Milano e Cortina si terranno le prossime Olimpiadi e paraolimpiadi invernali che rappresentano un primo grande evento importante come valutazione per misure di sicurezza e di intelligence che coinvolgono la dimensione digitale e durante le quali, il dato sanitario e le informazioni ad esso riferite avranno un ruolo chiave per lo svolgimento stesso dell'evento.

In particolare, sarà questa l'occasione per testare la lezione appresa dalla gestione della pandemia da Covid- 19 e da importanti esperienze internazionale come quella approfondita da Zumla et al. (2022) in riferimento a grandi eventi religiosi tenutisi negli ultimi anni.

Il tema della diffusione di epidemie durante i grandi eventi non è nuovo ma già considerato in anni passati come per esempio emerge dal lavoro svolto da Friedman e colleghi nel 2009.

La prospettiva degli Autori è estremamente interessante poiché definisce i grandi eventi intendendo anche i cambiamenti politici ed economici di un Paese che possono influenzare i rischi epidemici e i loro andamenti. In pre-

parazione delle prossime Olimpiadi invernali nel 2026 è quindi utile approfondire questi aspetti oltre che quelli legati per esempio a possibili attacchi cyber per rubare informazioni sanitarie relative allo stato di salute degli atleti.

Un'eventualità questa non remota ma che ripercorre la storia delle Olimpiadi di Pyeongchang nel 2018 e dell'attacco informatico che aveva attaccato i loro sistemi informatici, rendendo difficile la gestione dell'evento (Greenberg, 2018; 2019).

6. Conclusioni

Al termine di questa riflessione emerge la possibilità, nonché la necessità epistemologica, di identificare quello che può essere definito un modello delle future prospettive della Medical Intelligence, fondato sugli elementi considerati nell'analisi precedente.

Tale modello risulta essere costituito dai seguenti elementi:

1. Focus tematico: intelligence e informazioni considerate all'interno di un ecosistema digitale di relazioni sociali e culturali;
2. Ambito (scenario organizzativo da una prospettiva più operativa): civile, industriale, sociale, organizzativo;
3. Dimensione legata all'ambito: strategica;
4. Funzione e scopo: proattività per sicurezza nazionale, internazionale e cyber security;
5. Metodi e tecniche: privilegio di Digital Humint con apertura al mondo delle nuove tecnologie e dell'intelligenza artificiale.

Tale modello racchiude ed esplicita le caratteristiche sociali, culturali e tecnologiche tipiche dello scenario del mondo attuale ad elevata minaccia, interpretando i bisogni cognitivi per organizzarli e sistematizzarli al fine di produrre una conoscenza per ridurre la vulnerabilità nazionale e internazionale.

In particolare, il modello in questione si fa carico di una visione nuova della Medical Intelligence, proiettata al futuro, radicata in una dimensione strategica e orientata alla proattività.

L'apertura determinata dall'ambito di riferimento, non più specificatamente militare, è un altro tratto distintivo del passo in avanti necessario per comprendere le istanze di Medical Intelligence che includono anche settori quali quello civile, industriale e sociale.

La figura che segue sintetizza i modelli di Med Int discussi.

Figura 2 - *Modelli di Medical Intelligence a confronto*

Elementi	Modello tradizionale	Modello innovativo
Focus Tematico	Medico – sanitario	Intelligence e medico -sanitario
Ambito	Militare	Civile, industriale, sociale, organizzativo
Dimensione	Operativa-tattica	Strategica
Funzione e scopo	Difesa degli interessi nazionali e sicurezza militare	Proattività per sicurezza nazionale, internazionale e cyber security
Metodi e tecniche	Humint e Virtual Humint	Digital Humint

Una prima definizione, dunque, di Medical Intelligence da porre in discussione può essere quella che descrive *un processo informativo relativo a questioni biologiche, sanitarie e mediche interconnesse e interdipendenti a contesti socio-tecnici che si avvale di fonti informative presenti in ecosistemi sociali digitali con lo scopo di supportare decisioni per preservare la sicurezza nazionale e internazionale nel rispetto dei principi etici e legali.*

Tale definizione considera le prospettive emerse dalle analisi dei modelli di Medical Intelligence e le possibilità di sviluppare percorsi di Medical Intelligence che considerino, non solo i cambiamenti sociali in atto, ma anche la rilevanza dell'approccio informativo e del ruolo del fattore umano nella dimensione digitale attuale.

Bibliografia

Antiseri, D., Soi, A., (2013), *Intelligence e metodo scientifico*, Rubettino Editore, Soveria Mannelli.

Broccoli, U. (2019), Il mito di Ulisse ovvero il fattore umano chiave dell'intelligence, in *Limes Rivista Italiana di Geopolitica*, Vol. 8, GEDI Gruppo Editoriale SpA, Roma.

Caligiuri, M. (a cura di), (2016), *Intelligence e scienze umane*, Rubbettino Editore, Soverìa Mannelli.

Caligiuri, M. e Pili, G. (2020), *Intelligence studies Un'analisi comparata fra l'Italia e il mondo anglo-americano*, Rubbettino Editore, Soverìa Mannelli.

Capezzani, L. (2023), Funzioni intelligence della psicologia: un "anello mancante della mente sociale?", Società Italiana di Intelligence, SOCINT Press, Cosenza.

Featherstone, M., Hepworth, M., Turner, B. S. (1991), *The Body. Social Process and Cultural Theory*, Sage Publications, London.

Figueroa Uribe, Augusto F.; Hernández Ramírez, Julia; and Flores del Razo, Jorge O. (2021) "Intelligence in health: A critical analysis strategy for decision-making

in the health area," *Revista de la Facultad de Medicina Humana*, Vol. 22: Iss. 2, Article 21. Available at: https://inicib.urp.edu.pe/rfmh/vol22/iss2/21.

Friedman, S.R., Rossi, D. e Braine, N. (2009), Theorizing "Big Events" as a potential risk environment for drug use, drug-related harm and HIV epidemic outbreaks, *International Journal of Drug Policy*, Vol. 20, Issue 3, Science Direct, Elsevier.

Greenberg, A. (2018), The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, 22 Agosto 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

Greenberg, A. (2019), Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday, New York.

Jarcho, S. (1991). Historical perspectives of medical intelligence. Bulletin of the New York Academy of Medicine, 67 (5), 501.

La Gioia, V. (2015, November 5). Medical Intelligence in Biological Issues (PowerPoint).

Annual International Symposium on Biosafety, Biosecurity: Future Trends, and Solutions. Milan.

Lesser, I.O. et al. (1998), *Countering the New Terrorism*, RAND Corporation, https://www.rand.org/pubs/monograph_reports/MR989.html.

Lombardi, M. Burato, A., Maiolino, M. (2015), Dalla SOCMINT alla Digital HumInt. Ricomprendere l'uso dei Social nel ciclo di intelligence, Sicurezza Terrorismo Società, EDUCATT, Unicatt, Milano.

Lombardi, M., Maiolino, *M.* Lucini, B. (2020), Beyond counter- and alternative narratives to tackle extremism: the new Format model, in *Sicurezza Terrorismo Società - Security Terrorism Society, International Journal Italian Team for Security, Terroristic Issues & Managing Emergencies*, Educatt, Università Cattolica del Sacro Cuore, Milano. Vol. 11, Issue 1.

Lucini, B. (2022), *Social Network, la sicurezza e l'intelligence: prospettive metodologiche*, in Intelligence C4 Conoscenza, Comprensione, Consapevolezza, Comunicazione, BTT Editori, Lomazzo (CO).

Lucini, B. (2023), Società Radicali: dalla Francia alla guerra russo – ucraina, Itstime, Disponibile online: https://www.itstime.it/w/societa-radicali-dalla-francia-alla-guerra-russo-ucraina-by-barbara-lucini.

Marble, S. (2020), Medical Intelligence: Historical Background and Current Capabilities, *Military Intelligence Professional Bulletin*, Ft. Huachuca Vol. 46, Fasc. 1.

Military Committee Terminology Board. (2021, December 15). Medical intelligence. In.

NATO glossary of terms and definitions (english and french) (p. 298). North At-lantic Treaty Organization.

Office of the Chairman of the Joint Chiefs of Staff. (2022, May). Medical intelligence. In.

DOD dictionary of military and associated terms (p. 359). The Joint StaffSironi, M. (2022), La Digital Humint alla prova della guerra in Ucraina, Formiche, https://formiche.net/2022/03/digital-humint-ucraina-matteo-sironi.

Teti, A. (2019), *Virtual Humint La nuova frontiera dell'intelligence*, Rubbettino Editore, Soverìa Mannelli.

Tosoni, S. (2004), *Identità Virtuali: Comunicazione mediata da computer e processi di costruzione dell'identità personale*, Franco Angeli, Milano.

U.S. Department of Defence, (2023), Biodefence Posture Review, https://media.defense.gov/2023/Aug/17/2003282337/-1/-1/1/2023_BIODEFENSE_POSTURE_REVIEW.PDF.

Zumla, A. et al., (2022), Reducing the threat of epidemic-prone infections at mass gathering religious events, *The Lancet*, https://www.thelancet.com/action/showPdf?pii=S0140-6736%2822%2901194-1.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 979-12-5535-198-6

9 791255 351986