Manuela Farinosi
Gian Luca Foresti
Francesco Zucconi
(a cura di)

L'INTELLIGENCE EMERGENTE TRA TECNOLOGIA E HUMINT

Applicazioni predittive e cognitive per i nuovi scenari nazionali e internazionali

FrancoAngeli

Manuela Farinosi
Gian Luca Foresti
Francesco Zucconi
(a cura di)

L'INTELLIGENCE EMERGENTE TRA TECNOLOGIA E HUMINT

Applicazioni predittive e cognitive per i nuovi scenari nazionali e internazionali

FrancoAngeli

Il presente volume è stato realizzato grazie al contributo del Dipartimento di Scienze Matematiche, Informatiche e Fisiche dell'Università degli Studi di Udine.

Progetto grafico di copertina: Alessandro Petrini

ISBN: 9788835183310

Indice

Sezione II – Innovazioni nell'intelligence e nella sicurezza pubblica

Sezione III – Rischi informativi e manipolazione cognitiva

Prefazione

Ammiraglio di Divisione Davide Berna

Il contesto geopolitico contemporaneo è attraversato da una trasformazione profonda, in cui le tradizionali distinzioni tra guerra e pace, sicurezza interna ed esterna, tecnologia civile e militare si stanno progressivamente dissolvendo. Le guerre moderne, seppur hanno mantenuto una forte combinazione con quelle tradizionali/convenzionali, come dimostra emblematicamente il conflitto nel Mar Nero, si configurano sempre più come scontri multi-dominio, dove capacità convenzionali si intrecciano con strumenti cibernetici, cognitivi e informativi, dando vita a una nuova morfologia del confronto strategico. In tale scenario, l'innovazione tecnologica – intelligenza artificiale, droni, piattaforme autonome e sistemi di fusione dati – non è più solo un moltiplicatore di potenza, ma un fattore strutturale che ridefinisce gli equilibri internazionali e le logiche di deterrenza. Il proliferare di strumenti a basso costo e alta efficacia ha facilitato l'accesso al potere militare, consentendo anche ad attori non statali di incidere profondamente sugli assetti di sicurezza globale.

Questa "ibridazione" del conflitto si riflette anche sul fronte interno, dove sicurezza pubblica, *governance* democratica e tutela dei diritti fondamentali si trovano a dover convivere con sistemi predittivi, sorveglianza intelligente e capacità di intervento in tempo reale. Progetti come Olympus, Hera Vision o Ares Guardian[1] testimoniano la necessità di costruire un ecosistema di

1. Olympus Project, Hera Vision e Ares Guardian rappresentano modelli prototipali di un ecosistema avanzato per la sicurezza pubblica e nazionale, in cui tecnologie come l'intelligenza artificiale, la sorveglianza intelligente e i sistemi predittivi convergono per supportare il *decision-making* umano in scenari complessi; Olympus Project simboleggia l'infrastruttura integrata di risposta e monitoraggio, Hera Vision ne costituisce il modulo di visione artificiale e analisi comportamentale in tempo reale, mentre Ares Guardian è concepito come componente difensivo

sicurezza fondato sull'integrazione uomo-macchina, in cui la figura dell'operatore umano non sia marginalizzata, bensì rafforzata da strumenti di supporto decisionale affidabili, trasparenti e regolati da un solido framework normativo. La centralità dell'essere umano (che non può e non deve essere sostituita) – come "*user* consapevole" – rappresenta non solo una scelta etica, ma una condizione imprescindibile per garantire un controllo responsabile della tecnologia in ambienti complessi e ad alto rischio.

Tuttavia, questa accelerazione tecnologica solleva interrogativi strategici e normativi di ampia portata: dalla vulnerabilità delle infrastrutture critiche agli attacchi informatici, dall'uso ostile dell'intelligenza artificiale al rischio di bias algoritmici, fino alla militarizzazione dello spazio cibernetico come nuovo teatro di scontro tra potenze globali. In parallelo, i grandi cambiamenti climatici, la crisi delle catene del valore, la crescente instabilità demografica e la corsa alle risorse in aree strategiche come l'Artico e l'Indo-Pacifico evidenziano l'interconnessione tra minacce tradizionali e sfide emergenti. Le grandi potenze – dagli Stati Uniti alla Cina, passando per Russia e attori emergenti del Sud globale – si contendono non solo territori e rotte, ma soprattutto capacità di influenza, superiorità informativa e dominio cognitivo.

In questo scenario, il concetto di sicurezza va ripensato in modo sistemico e trasversale: non è più sufficiente proteggere i confini, occorre salvaguardare le infrastrutture digitali, la coesione sociale, l'autonomia tecnologica e la resilienza istituzionale. L'adozione di tecnologie avanzate deve avvenire all'interno di un framework strategico che coniughi efficacia operativa, sostenibilità etica e sovranità decisionale. Il futuro della sicurezza – nazionale e collettiva – non sarà garantito solo dalla superiorità dei mezzi, ma dalla capacità di orchestrare risorse umane e tecnologiche in un'architettura coerente, adattiva e inclusiva, capace di prevenire, gestire e trasformare le crisi in opportunità di stabilità.

In definitiva, il mondo che ci attende sarà dominato da attori in grado di integrare informazione, potenza tecnologica e resilienza strategica. Per affrontarlo con successo, occorre superare l'approccio emergenziale e costruire visioni lungimiranti che coniughino sicurezza, libertà e innovazione sotto un unico paradigma: quello della responsabilità democratica nel governo della complessità.

per la protezione attiva di aree sensibili e infrastrutture critiche, incarnando così un approccio multi-dominio alla sicurezza che combina efficacia operativa, controllo umano e tutela dei diritti fondamentali.

Introduzione. Formare all'intelligence in un mondo complesso

di Manuela Farinosi, Gian Luca Foresti, Gianluigi Sechi, Francesco Zucconi

Il presente volume raccoglie una selezione dei migliori elaborati prodotti dai discenti della quarta e quinta edizione del Master universitario di primo e secondo livello in Intelligence and Emerging Technologies, promosso dal Dipartimento di Scienze Matematiche, Informatiche e Fisiche (DMIF) dell'Università degli Studi di Udine, in convenzione con il Centro Alti Studi Difesa – Scuola Superiore Universitaria (CASD-SSU). Tali contributi sono frutto del lavoro individuale dei corsisti, svolto sotto la supervisione di esperti e docenti del Master.

Il Master, giunto ormai alla soglia della sua settima edizione, privilegia una didattica laboratoriale senza trascurare di presentare le basi di quelle sistemazione concettuali necessarie per l'analisi dei profondi mutamenti che l'innovazione tecnologica impone al mondo dell'intelligence, della sicurezza – in tutte le sue declinazioni – e dell'attività informativa in senso lato, con particolare attenzione alla componente umana (HUMINT) che rimane il fondamento di ogni processo informativo efficace di raccolta e analisi delle informazioni.

Tra le sfide poste dal presente, quelle che riguardano una reale e operativa difesa della pace, fondata sui principi universali e non negoziabili di giustizia sanciti dalla Dichiarazione dei Diritti dell'Uomo, sono affrontate con un approccio analitico scevro da pregiudizi ideologici o narrazioni precostituite, disancorate dal contesto storico.

Il lavoro di analisi che viene proposto nel Master mira, per mezzo di esercitazioni pratiche appositamente progettate all'uopo, a promuovere una comprensione critica e pragmatica del reale, sottolineando come errori di impostazione, approssimazioni e pregiudizi cognitivi (*bias*) possano minare fin dall'origine qualsiasi strategia di risposta efficace alle crisi in atto, finendo col favorire – talvolta inconsapevolmente – ottuse dinamiche di cruda sopraffazione.

Il Master è impostato sulla distinzione tra tecnologie dirompenti (*disruptive technologies*) e tecnologie emergenti (*emerging technologies*). Riprendendo quanto già evidenziato nell'introduzione al secondo volume della serie (*Intelligence e tecnologie emergenti. Per la pace, per la sicurezza informatica, per la lotta alla criminalità*, FrancoAngeli, 2024), si può ricordare che per tecnologie dirompenti si intendono quelle innovazioni destinate a modificare radicalmente l'interoperabilità di sistemi complessi – quali entità statuali o organizzazioni sovranazionali (ONU, Commissione Europea, NATO, European Defence Agency). Le tecnologie emergenti, invece, sono applicazioni tecnologiche basate su teorie scientifiche parzialmente consolidate, le cui potenzialità sono ancora in fase sperimentale ma che si prevede possano maturare entro il 2040. L'intelligenza artificiale (IA) è un classico esempio di tecnologia dirompente, mentre il quantum computing, con le sue applicazioni nella crittografia e nelle comunicazioni, rappresenta emblematicamente una tecnologia emergente.

Uno degli obiettivi formativi centrali del Master è quello di rafforzare le capacità predittive e analitiche dei discenti, affinché siano in grado di delineare, almeno in parte, gli scenari possibili che saranno dischiusi dalle tecnologie sopra ricordate, particolarmente nell'ambito della sicurezza informatica e della sicurezza delle persone. A tal fine, si valorizza un approccio didattico fondato sull'"imparare facendo" (*learning by doing*), grazie al quale i partecipanti sono guidati in esercitazioni pratiche complesse, mirate alla comprensione e all'applicazione concreta delle conoscenze acquisite.

Il programma integra competenze accademiche e operative, offrendo ai corsisti la possibilità di acquisire l'uso corretto e appropriato di alcune pratiche di raccolta di informazioni, quali, ad esempio, quelle di OSINT, GEOINT, SOCINT ed anche, per quanto possibile, di HUMINT. Il percorso è inoltre affiancato da una solida base concettuale, che comprende elementi teorici fondamentali relativi al funzionamento dell'intelligenza artificiale, della sicurezza cibernetica e delle strutture matematiche sottese a tali tecnologie. L'obiettivo è duplice: da un lato, consolidare le competenze tecniche dei discenti; dall'altro, rafforzarne la fiducia nell'utilizzo critico e consapevole degli strumenti informatici avanzati.

Il quadro formativo è completato dall'introduzione ai principi fondamentali della geopolitica e del diritto, indispensabili per una lettura critica del contesto internazionale e per l'assunzione di responsabilità decisionale in scenari complessi. Il raccordo tra le cosiddette "due culture" – scientifica e umanistica – è reso possibile grazie a tre elementi chiave: il modulo dedicato alle soft skills, gestito dai consulenti del ForMad (Consiglio per la Forma-

zione Organizzativa e Manageriale), in cui si trattano tematiche relative alla neuro-leadership, al problem solving e al decision making; i moduli di intelligence e intelligence economica, volti a integrare competenze tecnico-operative e capacità di analisi strategica; e infine l'elaborazione e presentazione finale di un report, curato con la supervisione di esperti del settore.

I dieci contributi qui raccolti sono articolati in tre sezioni tematiche:

1. tecnologie emergenti in contesti operativi;
2. innovazione nell'intelligence e nella sicurezza pubblica;
3. rischi informativi e manipolazione cognitiva.

La prima sezione si apre con un approfondito studio di Niccolò Cecchinato, dedicato all'integrazione di UAV (Unmanned Aerial Vehicles) e UUV (Unmanned Underwater Vehicles) per operazioni multidominio in ambito ISTAR (Intelligence, Surveillance, Target Acquisition, Reconnaissance). Il lavoro propone un'architettura di comunicazione sicura tra UAV e UUV, con specifico focus sulla cifratura dei dati sensibili mediante algoritmi AES e sulla sincronizzazione tra nodi in scenari operativi complessi.

Segue il contributo di Giuseppe Vincenzo Giugno, che analizza la strategia asimmetrica adottata dall'Ucraina nel confronto navale sul Mar Nero, con particolare attenzione al ruolo dell'innovazione tecnologica, dell'intelligence avanzata e del coordinamento con le forze occidentali nel controbilanciare la disparità navale con la Russia.

Il terzo contributo, elaborato da Alberto Celestino Monici, esplora invece l'applicazione di tecnologie quantistiche per la difesa dei satelliti in orbita LEO. Il lavoro propone un sistema innovativo basato su quantum dots (particelle di materiale semiconduttore della dimensione di pochi nanometri, le cui proprietà elettroniche e ottiche differiscono da quelle di particelle più grandi a causa di effetti quantistici) e radar quantistici per la protezione attiva contro vettori ostili, delineando uno scenario operativo di frontiera.

Chiude la prima sezione il saggio di Antonio Maccari, che esamina l'impiego dell'intelligenza artificiale nei processi di intelligence finalizzati al targeting in contesti critici. L'analisi mette in luce le potenzialità dell'intelligenza artificiale nell'automatizzazione delle decisioni tattiche, senza trascurare le implicazioni critiche in termini di accountability e governance algoritmica.

La seconda sezione si apre con una proposta, redatta da Marco Ternavasio, di un sistema integrato di sicurezza pubblica che sfrutta sinergicamente le potenzialità dell'intelligenza artificiale e degli UAV per attività di sorveglianza, riconoscimento e supporto operativo in contesti urbani ad alto rischio. Il progetto dimostra la possibilità di integrare una piattaforma di

intelligenza artificiale avanzata per l'analisi automatica di immagini da videosorveglianza con una flotta di droni da ricognizione aerea per acquisizione dati in situazioni critiche e supporto alle unità di difesa interna, fino all'impiego, in operazioni ad altissimo rischio, di UAV tattici.

Segue il contributo di Alessia Penge, incentrato sull'uso di algoritmi di machine learning per la *predictive policing*. L'elaborato offre una riflessione articolata sulle potenzialità predittive dell'intelligenza artificiale nella prevenzione del crimine, problematizzando gli aspetti etici e metodologici.

Il terzo contributo, di Salvatore Recano, presenta uno strumento gestionale già testato in contesto operativo, volto al rafforzamento delle capacità predittive e di controllo nei flussi doganali, attraverso analisi incrociate e validazioni in tempo reale.

Chiude la sezione il contributo di Paolo Nadal, che propone un'analisi dettagliata dell'ecosistema informativo del Dipartimento della Protezione Civile, evidenziando – anche alla luce delle più recenti disposizioni normative – la necessità di una maggior condivisione informativa tra il comparto intelligence e quello della comunicazione di emergenza.

La terza e ultima sezione è interamente dedicata alle tecniche malevole legate alla manipolazione della voce e ai rischi significativi ad esse associati. Il primo lavoro, redatto da Beatrice Di Stasio, analizza le vulnerabilità degli smart speaker, partendo da esperienze maturate durante il tirocinio formativo del Master. L'elaborato combina osservazione sul campo e riflessione teorica in merito alla sicurezza degli assistenti vocali.

Conclude il volume il saggio di Loris Silverio, che propone una disamina tecnica sull'impiego dell'intelligenza artificiale nella clonazione vocale, offrendo al contempo uno spunto critico sulle implicazioni di tale tecnologia in ambito informativo, sociale e giuridico.

La somma di questi contributi offre una riflessione che va oltre l'ambito tecnico-operativo per toccare il cuore stesso della formazione nel campo dell'intelligence: il rapporto tra sapere, potere e responsabilità in un'epoca sempre più segnata dalla pervasività delle tecnologie emergenti.

L'eterogeneità dei capitoli raccolti nel volume non rappresenta soltanto la pluralità delle competenze acquisite dai discenti, ma riflette anche la complessità sistemica del presente, in cui le tecnologie dell'informazione e della comunicazione ridefiniscono i confini stessi dell'agire umano. In tale contesto, il rischio principale non è tanto quello di un uso malevolo delle tecnologie – pur concreto e ben documentato in letteratura – quanto quello, più sottile e insidioso, di una deresponsabilizzazione generalizzata, che spinga a

delegare alle macchine, agli algoritmi o alle narrative semplificanti, il compito di interpretare la realtà.

In un simile scenario, una maggiore consapevolezza dei rischi diventa indispensabile premessa per costituire una cittadinanza più vigile e autonoma. In questo senso, la formazione all'intelligence non può più essere considerata un sapere specialistico riservato a contesti ristretti, ma rappresenta un patrimonio epistemico e civico essenziale, in grado di fornire strumenti critici per interpretare i complessi fenomeni del presente e del futuro prossimo. Educare all'intelligence significa formare menti capaci di cogliere la complessità, di discernere tra dato e informazione, tra informazione e conoscenza, tra conoscenza e decisione. Significa, inoltre, coltivare una postura epistemica fondata sulla razionalità critica, sull'attenzione etica e sul senso della misura.

La conoscenza delle potenzialità – ma anche delle vulnerabilità – associate alle tecnologie digitali deve diventare uno strumento di autodifesa intellettuale e culturale, in grado di contrastare le derive manipolative, i fenomeni di disinformazione e l'involuzione cognitiva favorita da ecosistemi comunicativi sempre più opachi. In questo senso, l'intelligence si configura come un sapere strategico al servizio della pace e della libertà, come una disciplina che, se ben orientata, può contribuire a una socialità più libera, perché più auto-consapevole.

Saper leggere le intersezioni tra tecnologia, potere e narrazione è oggi una condizione necessaria non solo per prevenire minacce, ma anche per progettare scenari di convivenza meno vulnerabili e più giusti. È in questa prospettiva che la formazione all'intelligence deve porsi come un laboratorio permanente di esercizio critico, capace di tenere insieme analisi operativa, profondità storica e immaginazione politica.

In definitiva, riteniamo che solo una conoscenza che non rifugge dalla complessità, ma che anzi la assuma come costitutiva della realtà, possa costituire un autentico presidio di pace, giustizia e libertà nell'era delle tecnologie emergenti.

Sezione I

Tecnologie emergenti nei contesti operativi

Sistemi autonomi distribuiti e intelligenti. La comunicazione sicura e coordinata nelle operazioni tattiche di droni

di *Niccolò Cecchinato*

Introduzione

L'evoluzione attuale del panorama bellico internazionale segna l'inizio di una nuova fase, caratterizzata da una trasformazione radicale tanto sotto il profilo geopolitico quanto sotto quello tecnologico. I conflitti moderni si sviluppano in uno scenario multi-dominio, che integra dimensioni fisiche e digitali: alla guerra convenzionale si affiancano oggi la cyberwarfare e le forme di guerra ibrida.

Il progresso tecnologico ha reso accessibili strumenti bellici avanzati – come droni, intelligenza artificiale e sistemi autonomi – anche a Paesi instabili o in via di sviluppo, alterando gli equilibri strategici tradizionali. Tali tecnologie, grazie ad un favorevole rapporto costo-efficacia, operano non solo nel dominio per cui sono state progettate, ma sono in grado di comunicare e cooperare trasversalmente tra domini bellici diversi.

L'integrazione tra UAV e intelligenza artificiale ha dato origine a nuovi strumenti per missioni ISTAR (Intelligence, Surveillance, Target Acquisition, Reconnaissance), oltre che per operazioni di addestramento, simulazione di minacce, interventi umanitari e ricerca e soccorso. Sistemi modulari e scalabili, sono impiegati in missioni critiche come, ad esempio, lo sminamento e l'evacuazione da aree ad alto rischio (Leonardo, 2022).

Gli UAV, dotati di unità computazionali e sistemi multi-sensore, svolgono compiti eterogenei: dal monitoraggio di infrastrutture strategiche all'intercettazione di segnali, fino al contrasto di intrusioni in zone sensibili (Cecchinato *et al*., 2023a). Tali piattaforme sono oggi utilizzate principalmente per attività di SIGINT (Signal Intelligence), IMINT (Image Intelligence) e MASINT (Measurement and Signature Intelli-

gence), grazie all'elaborazione intelligente di segnali, immagini e firme caratterizzanti.

Innovativa risulta anche l'integrazione di sensori acustici a bordo UAV, come evidenziato da (Toma, 2021a) e (Salvati *et al*., 2020a), che abilita, su questi sistemi, capacità di ACINT (Acoustic Intelligence) per l'identificazione e classificazione di fonti sonore, amiche o ostili, contribuendo ad una nuova dimensione dello spionaggio tattico.

Le tecnologie emergenti – droni, intelligenza artificiale, cyberspazio – non solo cambiano la natura del conflitto, ma ridefiniscono anche i soggetti coinvolti, ampliando lo spettro delle minacce oltre gli attori statuali tradizionali.

Il presente lavoro si focalizza sugli aspetti tecnologici di queste soluzioni, con particolare attenzione all'impiego sicuro e coordinato dei sistemi UAV/UUV per missioni di intelligence e sorveglianza. Verranno inoltre introdotte un'architettura di streaming sicuro per la cifratura in tempo reale dei dati sensibili acquisiti e una piattaforma collaborativa multi-dominio che integra veicoli aerei e subacquei senza equipaggio.

Protezione delle comunicazioni dei droni

Questo capitolo è un estratto dell'articolo scritto da (Cecchinato *et al*., 2023a), pubblicato su *IEEE Communications Magazine* per il numero dedicato a "Military Communications and Networks" e realizzato nell'ambito del Master in Intelligence and Emerging Technologies. Esso sottolinea l'importanza della cifratura e della protezione dei dati sensibili acquisiti da droni e sistemi autonomi.

Descrizione dello studio svolto

L'utilizzo dei droni, equipaggiati con sensori multimodali, come telecamere e array microfonici, permette di aumentare le capacità di identificazione delle minacce del drone, non solo a livello visivo, ma anche grazie all'identificazione della firma sonora della sorgente e alla sua direzione d'arrivo (Direction of Arrival – DoA) (Salvati *et al*., 2020b). I dati raccolti a bordo vengono parzialmente elaborati dal processore/computer di bordo e poi inviati in tempo reale a terra per un'analisi più approfondita; in questo caso la protezione della sicurezza dei dati emerge come una preoccupazione critica. È fondamentale garantire l'integrità della sicurezza dei dati durante l'intero

processo di trasmissione, a partire dal momento dell'acquisizione a bordo dei droni fino alla consegna finale al nodo di destinazione o alla stazione di terra (Ground Control, GC), specialmente quando il dato da trasmettere è sensibile e deve essere segregato.

Il presente studio descrive l'implementazione di un framework che utilizza l'algoritmo di cifratura Advanced Encryption Standard (AES) a livello applicativo, in tempo reale e a basso impatto computazionale, per la protezione dei dati multimediali acquisiti a bordo dei droni e trasmessi al GC. Questo schema di cifratura è progettato per essere eseguito sui Single Board Computers (SBCs) installati a bordo delle entità remote, le quali possono disporre di risorse computazionali ed energetiche limitate, ma in grado, con il sistema che verrà descritto, di acquisire, cifrare e trasmettere il dato.

L'indagine proposta nell'articolo dimostra significativi progressi nello sviluppo di un'applicazione di streaming all'interno di un framework di trasmissione, concepito per scenari militari di contrasto agli UAV (counter-UAV). Tale applicazione si distingue per efficacia, sicurezza, velocità e affidabilità nella gestione simultanea di segnali audio e video. Inoltre, viene introdotta una sperimentazione di cifratura con gestione sincrona di chiavi multiple. Le sperimentazioni condotte confermano l'efficacia dei processi di cifratura e decifrazione, anche in condizioni difficili del canale radio.

Trasmissione sicura in tempo reale di dati multimediali da UAV mediante crittografia AES

In missioni ISTAR, che prevedono la compresenza di diversi attori e sistemi dotati di sensori eterogenei e multimodali, è frequentemente necessaria la trasmissione di dati raccolti in modo confidenziale in tempo reale attraverso reti wireless, garantendo una latenza minima e una fedeltà adeguata, verso unità interconnesse o una stazione di terra centralizzata. Questa unità centrale è in grado di ricevere i flussi di dati, condurre l'elaborazione necessaria ed emettere istruzioni di comando e controllo (C_2) verso i nodi remoti.

Nel nostro studio, impieghiamo una rete di Unmanned Aerial Vehicles (UAV) in contesti operativi militari, che richiede misure rigorose per proteggere l'integrità delle informazioni scambiate tra i droni e la Ground Station (GS). Il nostro obiettivo principale riguarda la garanzia della riservatezza dei flussi multimediali, attraverso l'adozione di un algoritmo di cifratura dei dati rapido, affidabile e certificato, caratterizzato da un carico computazionale minimo, rendendolo adatto per il deployment su Single-Board Computers