Reti criminali ad alto rischio e minacce ibride

Arije Antinori*, Stefano Ferracuti**

Ricevuto 20 aprile 2026 – Accettato 13 luglio 2026

Sommario

Il lavoro analizza l'evoluzione delle reti criminali, evidenziando il passaggio da strutture gerarchiche come precedentemente concepite a piattaforme tecnologiche e relazionali complesse. Le High-Risk Criminal Networks (HRCNs) non sono più semplici "bande", ma infrastrutture che operano come imprese di servizi, superando il modello organizzativo piramidale, acquisendo competenze specifiche, e infiltrando l'economia legale. L'AI non è solo un "tool", ma un acceleratore strategico che cambia il DNA del crimine, consentendo a soggetti con scarse competenze di gestire truffe complesse, automatizzando il phishing, i deepfakes, la clonazione di voci per frodi e favorendo il disimpegno emotivo. Gli attori di queste reti vanno valutati in relazione alla loro posizione funzionale. Gli HRCNs possono essere proxy per entità destabilizzanti tramite minacce ibride e l'uso delle reti come moltiplicatori di disordine. Per affrontare l'attuale situazione occorre un approccio che integri: Network Analysis Digital Forensics e Criminologia Clinica. Questo quadro trasforma la lotta al crimine da una semplice attività repressiva a una sfida di governance tecnologica e cooperazione internazionale, come indicato dall'EU AI Act.

Parole chiave: reti criminali ad alto rischio, criminalità organizzata, HRCN, minacce ibride, AI, MUAI, disinformazione, FIMI

* Sapienza Università di Roma. arije.antinori@uniroma1.it.
** Sapienza Università di Roma. stefano.ferracuti@uniroma1.it.

De Iustitia et Iure (ISSNe 3103-2761), 1/2026
DOI: 10.3280/ius2026oa22650

Abstract

This paper analyzes the evolution of criminal networks, highlighting the shift from previously conceived hierarchical structures to complex technological and relational platforms. High-Risk Criminal Networks (HRCNs) are no longer simple "gangs," but infrastructures that operate like service businesses, transcending the pyramid organizational model, acquiring specific skills, and infiltrating the legal economy. AI is not just a "tool," but a strategic accelerator that changes the DNA of crime, enabling individuals with low skills to manage complex scams, automating phishing, deepfakes, and fraudulent voice cloning, and promoting emotional disengagement. The actors in these networks must be assessed in relation to their functional position. HRCNs can function as proxies for destabilizing entities through hybrid threats and the use of networks as multipliers of disorder. Addressing the current situation requires an approach that integrates Network Analysis, Digital Forensics, and Clinical Criminology. This framework transforms the fight against crime from a simple repressive activity to a challenge of technological governance and international cooperation, as indicated by the EU AI Act.

Keywords: High-risk criminal networks, organized crime, HRCN, hybrid threats, AI, MUAI, disinformation, FIMI

1. Introduzione e definizioni operative[1]

La definizione di gruppo criminale organizzato come un gruppo strutturato di tre o più persone, esistente per un certo periodo di tempo e orientato alla commissione di reati gravi per ottenere un beneficio finanziario o materiale, elaborata nell'ambito della Convenzione delle Nazioni Unite contro la Criminalità Organizzata Transnazionale (UNODC, 2000) pur restando centrale dal punto di vista normativo, presenta dei limiti nel cogliere la complessità delle reti criminali contemporanee. Queste sono meglio inquadrabili come sistemi che interconnettono, tra l'altro, mercati illeciti, outsourcing criminale, mascheramento finanziario, attività lecite di copertura, asset tecnologici, competenze professionali e capacità sistemiche di corruzione.

Le Reti Criminali ad Alto Rischio (HRCNs) costituiscono oggi una delle principali minacce alla sicurezza, soprattutto all'interno dello spazio

[1] Il contributo è frutto di una comune riflessione degli autori. Ai fini dell'attribuzione sono da ascrivere ad Arije Antinori i paragrafi 1, 2, 3, 4, e 7, e a Stefano Ferracuti i paragrafi 5, 6 e 8.

dell'Unione Europea (EU). Tali entità criminali si caratterizzano per configurazioni organizzative a carattere reticolare capaci di combinare transnazionalità, elevato adattamento strutturale, infiltrazione dell'economia legale, uso di corruzione e/o violenza, disponibilità di facilitatori specialistici e potenziale di produrre effetti sistemici. Nel 2024 Europol ha pubblicato una mappatura comparata delle reti ritenute più minacciose per l'Unione, affermando che la loro pericolosità non dipende soltanto dal numero di reati commessi, ma dalla capacità di interconnettere funzioni e ambienti diversi (Europol, 2024). Un anno dopo la medesima Agenzia evidenzia come la criminalità organizzata stia mutando il proprio "DNA" attraverso l'accelerazione digitale, l'uso dell'Intelligenza Artificiale (AI), la professionalizzazione dei servizi criminali, nonché una crescente attitudine nel destabilizzare le democrazie anche attraverso alla possibilità di rappresentare una minaccia ibrida (Europol, 2025). Sul piano concettuale, tale tipo di minaccia costituisce una unicità in quanto non coincide con una minaccia militare in senso stretto, ma designa una modalità di aggressione composita nella quale pratiche criminali, disinformazione, cyber-intrusione, finanza illecita, corruzione, sabotaggio e pressione sociale si combinano con l'obiettivo di erodere fiducia, istituzioni, mercati e processi decisionali. Risulta interessante la lettura strategica che ne fanno le istituzioni francesi, nel descrivere l'aumento del ricorso a strategie/modalità ibride, tra cui in particolare la sistematizzazione della manipolazione informativa e l'uso crescente dell'AI nel dominio cyber (Secrétariat général de la défense et de la sécurité nationale, 2025). Alla luce di ciò, si segnala come le entità criminali organizzate non rappresentino sempre l'attore primario della minaccia ibrida, ma possano divenire rispettivamente dei facilitatori, dei partner criminali, dei proxy e/o moltiplicatori di efficacia operativa. È perciò evidente che le Reti Criminali ad Alto Rischio debbano essere studiate non come associazioni di soli autori di reato, ma come vere e proprie infrastrutture di relazione, capaci di organizzare protezione, potere, circolazione di risorse, adattamento e opacità. Pertanto, una lettura criminologica centrata sulla sola fattispecie di reato e/o sul singolo gruppo non risulta più sufficiente a coglierne la portata strategica, soprattutto in prospettiva, considerando la crescente complessità dello scenario tanto europeo quanto globale sul piano della sicurezza sia interna che nazionale e internazionale. Diventa quindi necessaria la costruzione di un framework analitico integrato che tenga insieme struttura, funzione, ambiente, tecnologia e attori.

2. Architettura organizzativa delle reti criminali ad alto rischio

Uno degli aspetti più interessanti dell'evoluzione criminale organizzata degli ultimi anni consiste nel superamento della rete criminale quale tipica struttura piramidale unica e rigidamente gerarchica. Il dataset Europol del 2024 include 821 reti e oltre 25.000 individui; al suo interno coesistono strutture gerarchiche, reti a nucleo centrale, gruppi loose, configurazioni modulari e reti decentralizzate (Europol, 2024). Ciò significa che la pericolosità non dipende da una sola forma, ma dalla combinazione tra stabilità, capacità di adattamento, ampiezza delle connessioni e controllo di risorse strategiche.

Il dato più significativo è che una leadership forte e una struttura organizzativa fluida non si escludono reciprocamente. Molte reti mantengono un vertice difficilmente sostituibile, pur interconnettendosi a cerchi esterni, collaboratori occasionali e provider di servizi criminali. Ne è la conferma il fatto che diversi leader possono continuare a esercitare controllo anche dalla detenzione, attraverso delega, comunicazioni criptate e intermediazione fiduciaria (Europol, 2024). Pertanto, le reti criminali ad alto rischio appaiono come organizzazioni di "potere distribuito", in cui la centralità non coincide necessariamente con la presenza fisica, bensì con il controllo strategico attraverso decisioni, logistica e monetizzazione.

A livello funzionale, infatti, tali reti operano come vere e proprie piattaforme criminali ove i membri effettivi sono affiancati da: avvocati, fiscalisti, consulenti, facilitatori, esperti cyber, esperti di riciclaggio, logistici, operatori portuali, falsari, prestanome, sanitari e broker. Dal punto di vista strutturale dette entità possono essere fortemente strutturate, attraverso catene di comando e controllo vincolanti, o più modularmente autonome, ma si sorreggono sempre più spesso su servizi esterni, in particolare per quanto concerne il Cybercrime_as_a_Service e il Money-Laundering_as_a_Service (INTERPOL, 2024, 2026), che rendono le reti più resilienti e al contempo decisamente più opache agli occhi delle istituzioni.

La coesione interna non è soltanto di tipo economico, ma può fondarsi su nazionalità condivisa, origine territoriale, legami familiari, lingua, subcultura, esperienza comune e/o precedente cooperazione criminale (Europol, 2024). In tal senso, la rete criminale è al contempo impresa, comunità e infrastruttura socio-relazionale. La sua capacità di sopravvivere alla repressione dipende spesso proprio dalla stratificazione multilivello dei legami, ossia una rete è tanto più resistente quanto più riesce a rendere interscambiabili alcuni ruoli senza perdere i propri nodi fiduciari centrali.

3. Violenza, corruzione, imprese legali e convergenza con le minacce ibride

Secondo i report istituzionali più recenti, corruzione e violenza non sono repertori comportamentali alternativi, ma complementari. Europol, in particolare, rileva che un ampio numero delle reti più minacciose utilizza la corruzione, una quota altrettanto rilevante ricorre alla violenza, e una parte significativa usa in modo proattivo entrambe le risorse come strumenti integrati di governo criminale (Europol, 2024). Tuttavia, il dato davvero importante è che l'assenza di violenza manifesta non riduce necessariamente la pericolosità della rete in termini di profonda "contaminazione criminale", operando soprattutto attraverso frodi, infiltrazione, manipolazione economica, controllo logistico, intimidazione latente e abuso di competenze specialistiche. L'infiltrazione dell'economia legale è un fattore decisivo in questo contesto. Le imprese legali non hanno soltanto una funzione di riciclaggio, ma anche di facilitare il reato, ottenere rispettabilità, acquistare accesso a informazioni e generare dipendenza sociale, attraverso in particolare costruzioni, trasporti, ospitalità e logistica (Europol, 2024b). La penetrazione criminale non va quindi letta solo come presenza nel mercato, ma come capacità di modellare opportunità, nascondere flussi, controllare nodi infrastrutturali e soprattutto condizionare ambienti a livello locale.

Il caso italiano è particolarmente interessante in tal senso, evidenziando un uso sempre più sofisticato di operatori compiacenti nei porti, di dispositivi criptati, di canali radio separati e di gruppi specializzati nell'estrazione di cocaina dai container (Direzione Centrale per i Servizi Antidroga, 2024, 2025). Qui la rete criminale assume la forma di filiera logistica diffusa: non un gruppo chiuso, ma un sistema aperto che integra complicità amministrative, conoscenze tecniche, segmentazione dei compiti, outsourcing e "subappalti" criminali.

In tale scenario, la convergenza con le minacce ibride diventa più chiara. In Francia, Germania e Spagna i documenti strategici recenti collocano la criminalità organizzata dentro il perimetro della sicurezza nazionale, sottolineando il rapporto fra cybercriminalità, destabilizzazione, disinformazione, riciclaggio e aggressione alle istituzioni (Bundeskriminalamt, 2025; Departamento de Seguridad Nacional, 2025; Ministère de l'Intérieur, 2025; SGDSN, 2025). Le reti criminali possono offrire ad attori ostili: servizi, canali, finanziamenti, opacità e capacità di negazione plausibile, ma possono anche utilizzare tattiche ibride ai fini della massimizzazione di profitto, pressione e immunità.

4. AI e MUAI nella dimensione strategico-organizzativa

L'Uso Malevolo dell'Intelligenza Artificiale (MUAI) per condurre attacchi diretti o indiretti, sabotaggio, manipolazione, interferenza e destabilizzazione (Antinori, 2025) rappresenta un'importante risorsa a disposizione di una serie ampia di categorie di attori ed entità criminali. Questa nozione è utile perché consente di superare una lettura riduttiva dell'AI come semplice strumento di efficienza criminale; oggi il MUAI deve essere considerato come infrastruttura di accelerazione, trasformazione e ibridazione criminale, mentre dal punto di vista organizzativo, l'AI come generale ecosistema trasformativo, riduce i costi di coordinamento e amplia la scala delle possibili configurazioni e di *modus operandi*. Ad esempio, i Large Language Models (LLMs) possono rendere il phishing più credibile, adattabile, multilingue e accessibile anche a soggetti con competenze informatiche limitate (Europol, 2023a). INTERPOL descrive l'AI come force multiplier della frode finanziaria, capace di aumentare profilazione, social engineering, impersonazione e automazione (INTERPOL, 2024, 2026). Si determina così una trasformazione strutturale: la rete criminale ha bisogno di meno competenze diffuse e può acquistare e/o integrare servizi AI-ready in modo modulare, in un ecosistema criminale sempre più caratterizzato dal MUAI_as_a_Service. Nel Sud-Est Asiatico si registra un ulteriore salto di qualità, identificato dagli scam compounds che combinano chatbot, voice cloning, deepfakes, synthetic identities, outreach automatizzato, mule accounts e lavoro coartato (UNODC, 2025). Si evince come in tali scenari l'AI non è soltanto supporto tecnico, ma diviene, anche grazie al MUAI, il tessuto connettivo che integra sfruttamento umano, frode, riciclaggio, gestione delle vittime e moltiplicazione dei punti di attacco. Ciò comporta che, per le istituzioni, la risposta non possa essere soltanto repressiva, ma sempre più integrata – nell'ottica di prevenzione e anticipazione dell'evoluzione criminale –, includendo capacità analitiche, cooperazione transnazionale, strumenti di intelligence finanziaria, partnership pubblico-private e una governance dell'AI coerente con standard europei di legalità e diritti fondamentali. L'AI Act dell'EU mostra la direzione di intervento sulla base di un approccio risk-based, divieti per gli usi a rischio non accettabile, e disciplina stringente per applicazioni ad alto rischio, inclusi alcuni ambiti rilevanti per il Law Enforcement (European Parliament & Council of the European Union, 2024).

5. Profili attoriali, ruoli e funzioni criminali

Non esiste un profilo psicologico tipico del membro delle reti criminali ad alto rischio, come emerge dall'analisi di cinquantadue studi sui fattori individuali legati al reclutamento nella criminalità organizzata, seppure alcuni elementi ricorrano con maggiore frequenza, tra cui: sesso maschile, precedenti attività criminali e/o violente, relazioni con soggetti già coinvolti e contesti familiari problematici (Calderoni et al., 2022). Pertanto, più del tipo criminale, ciò che appare più rilevante è il concetto di posizione funzionale, ossia la funzione che svolge un determinato attore all'interno della rete, con quanti/quali margini di scelta, in quale contesto socio-relazionale, nonché attraverso quali mediazioni tecnologiche. Questa prospettiva consente di individuare al contempo: intenzionalità, adattamento, coercizione, moral disengagement e differenziazione dei compiti. Se si abbandona la ricerca del profilo unico, emerge una costellazione di figure attoriali. Le fonti istituzionali consentono, infatti, di distinguere almeno le seguenti figure: leader, broker, facilitatori, specialisti ed esecutori fungibili, a cui vanno oggi aggiunte, quelle dell'attore coartato e/o trafficato, particolarmente visibili nei sistemi di frode online e negli scam compounds (Europol, 2024; INTERPOL, 2026; UNODC, 2025), come di seguito specificato:

Il leader non coincide necessariamente con l'attore più violento o più esposto. Spesso è il soggetto che controlla le relazioni chiave, seleziona i partner, decide la distribuzione del rischio e presidia i canali di monetizzazione. Le sue qualità psicologicamente rilevanti sono riconducibili a una combinazione di dominio situazionale, capacità di gestire fiducia e minaccia, tolleranza al rischio e visione strategica.

Il broker opera come mediatore di mondi, collegando ambienti criminali e leciti, piazze fisiche e piattaforme digitali, competenze tecniche e bisogni operativi, gruppi locali e mercati transnazionali. È una figura cruciale in quanto la sua forza risiede nel capitale socio-relazionale e nella traducibilità tra codici sociali differenti.

I facilitatori comprendono professionisti, consulenti, operatori compiacenti, logistici e figure amministrative che, senza apparire come membri ordinari del gruppo, rendono possibile il funzionamento della rete.

Gli specialisti offrono competenze specifiche (come hacking, falsificazione, crittografia, chimica, gestione di wallet, analisi dati e creazione/gestione di identità sintetiche), e per questo occupano una posizione considerata ad alto valore, ma non sempre di leadership.

Gli esecutori fungibili sono gli attori più facilmente sostituibili, quali: corrieri, vedette, addetti all'estrazione di merci, mule accounts, operatori di

prossimità con le vittime, figure di presidio territoriale e/o digitale. La loro fungibilità organizzativa non significa irrilevanza psicologica, proprio il carattere sostituibile del ruolo favorisce spesso meccanismi di de-responsabilizzazione e adattamento rapido.

Una lettura criminologica di questi profili suggerisce che l'elemento centrale risulta essere la funzionalizzazione dell'individuo. La rete premia capacità differenti a seconda della posizione: dominio e calcolo nei vertici, mediazione nei broker, specializzazione tecnica nei facilitatori e specialisti, affidabilità e obbedienza negli esecutori. Ciò che appare come profilo è spesso l'esito della relazione tra individuo e compito assegnato. In questo senso, la rete criminale non si limita a selezionare persone già predisposte, ma contribuisce a produrre e stabilizzare identità funzionali alla propria conformazione esistenziale.

6. Reclutamento, appartenenza e coercizione

Il reclutamento nelle reti criminali ad alto rischio va concepito come processo dinamico che non si sostanzia quindi in un unico atto d'ingresso. Dal punto di vista attoriale, emerge l'importanza di un vissuto caratterizzato da legami sociali con membri già coinvolti, contesti familiari problematici e ambienti di socializzazione devianti, ma il peso di queste variabili cambia profondamente secondo il tipo di rete, il mercato criminale e la posizione occupata (Calderoni et al., 2022). In alcuni indotti criminali il reclutamento è fortemente relazionale e territoriale, mentre in altri è opportunistico e task-based. In altre ancora è parzialmente o totalmente coercitivo.

Il caso italiano mette in luce la dimensione emulativa e ambientale, caratterizzata dall'uso crescente di giovani e giovanissimi nei mercati della droga, spesso dotati di capacità relazionali, logistiche, comunicative e finanziarie non banali; l'ostentazione di ricchezza, *status* e visibilità funziona, in alcuni contesti, da meccanismo di attrazione e normalizzazione (DCSA, 2024). Da questo punto di vista, la socializzazione criminale è meno simile ad un reclutamento formalizzato e più simile a un percorso di apprendimento funzionale attraverso il quale si entra progressivamente nella rete attraverso fiducia, compiti minori, prove di affidabilità e condivisione di codici simbolici.

Una teoria del reclutamento oggi non può ignorare la coercizione. La crescita di scam centres e fraud compounds vede oggi la presenza crescente di soggetti, attirati con false offerte di lavoro, che vengono manipolati, privati dei documenti e costretti a partecipare a truffe online, sextortion, romance baiting e altre frodi seriali (INTERPOL, 2026; UNODC, 2025). In tali casi

emerge una figura liminare, essenziale, ossia il soggetto che è insieme autore materiale di condotte illecite e vittima di coercizione criminale. Pertanto, in questo contesto la tradizionale dicotomia offender/victim, come framework interpretativo appare insufficiente, rivelando una prospettiva di complessità interpretativa, soprattutto in ordine all'elaborazione di strategie e tattiche di prevenzione, relativamente ad un fenomeno criminale come quello genericamente definito scam in crescente e rapida diffusione a livello globale. Inoltre, si evidenzia come la protezione delle vulnerabilità sociali, economiche, migratorie e cyber-sociali risulti essere parte integrante del contrasto alle reti, non attività accessoria.

Inoltre, la continuità vittima-autore ha implicazioni importanti. Sul piano teorico, mostrando che il comportamento criminale può essere il risultato non soltanto di scelta opportunistica, ma di assoggettamento, intimidazione, paura, dipendenza e/o concreta mancanza di alternative di vita. Ciò impone, sul piano criminologico, una valutazione più profonda in ordine alla volontarietà, consapevolezza e margine di autodeterminazione del soggetto.

7. AI e MUAI nella dimensione attoriale, socio-cognitiva e relazionale

Se in precedenza l'AI è apparsa come moltiplicatore organizzativo, funzionale, qui interessa il suo effetto sulla soggettività criminale. L'AI riduce innanzitutto la soglia di competenza necessaria per entrare in attività fraudolente, estorsive e/o manipolative. LLM e strumenti su base di Generative AI (GenAI), permettono a soggetti con limitate competenze linguistiche e/o tecniche, di produrre messaggi credibili, imitare stili, strutturare conversazioni persuasive, creare identità sintetiche e adattare al profilo della vittima i contenuti mediali sviluppati (Europol, 2023a; INTERPOL, 2026). Ne deriva una trasformazione sostanziale dell'ingresso nell'indotto criminale specifico e nel contesto criminale, in senso più generico, meno dipendente da lunghi "apprendistati", ma più dipendente dalla capacità di gestire la capacità criminale degli strumenti disponibili. AI, tra l'altro, può determinare nel tempo una ridefinizione del rapporto ruolo gerarchico/funzione, con impatti trasformativi in merito allo sviluppo di entità criminali sempre più flessibili, adattive, riposizionabili e modularmente rigenerabili.

L'AI modifica anche la natura della relazione con la vittima. Deepfakes, voice cloning, chatbot e sistemi di profiling consentono di aumentare il realismo dell'inganno e, al tempo stesso, di accrescere la distanza morale dell'autore. Chi agisce attraverso interfacce automatizzate può percepire la

propria condotta come tecnica, frammentata, impersonale. La mediazione algoritmica, sommata alla divisione del lavoro, facilita processi di disimpegno morale, poiché ciascun attore vedendo una parte minima del danno complessivo, tende a leggere la propria azione come mera procedura funzionale e non come attività violenta eterodiretta (INTERPOL, 2026). Questo non elimina la responsabilità, ma può contribuire a spiegare perché alcune forme di "ferocia" economica, come nel caso delle scam, e manipolativa possano essere esercitate con apparente freddezza.

Sul piano relazionale, l'AI altera la stessa nozione di presenza. Le reti criminali possono moltiplicare i propri "Sé operativi", in termini di account, identità sintetiche, voci, volti, e personae persuasive. Ciò consente di aumentare i punti di contatto con le vittime, saturare lo spazio informativo, frammentare l'attribuzione e intensificare la capacità di grooming. L'Agentic AI sta rapidamente ampliando le possibilità di automatizzare parti consistenti delle campagne fraudolente, dalla ricognizione iniziale alla selezione delle vittime, fino all'interazione persuasiva (INTERPOL, 2026). In tale contesto, il profilo attoriale diventa sempre più ibrido, meno centrato sul soggetto agente, ma più "distribuito" tra esso, interfaccia, script e automazione.

Per quanto concerne la psicologia forense e la criminologia clinica, questo cambiamento risulta assai rilevante, poiché non si tratta solo di aggiornare il catalogo dei mezzi impiegati – tra l'altro nell'ottica di una tendenza di crescente presenza degli asset tecnologici –, ma si tratta di comprendere come l'AI (ri-)imodelli percezione del rischio, distanza dalla vittima, senso di autoefficacia criminale, modalità di identificazione con il ruolo e possibilità di dissociazione morale. L'introiezione ingegnerizzata del MUAI nelle reti criminali ad alto rischio, in prospettiva, non costituisce un semplice quanto impattante valore aggiunto, ma una trasformazione dell'ecologia socio-cognitiva e relazionale entro cui il comportamento criminale prende forma, si modella, evolvendosi nel tempo in un'ottica di mutamento tecnodiretto, tra l'altro decisamente in linea con le necessità operative delle minacce ibride.

8. Conclusioni

L'analisi svolta consente almeno due riflessioni che riteniamo rilevanti. La prima è che le reti criminali ad alto rischio vanno comprese come sistemi adattivi plurifunzionali: non semplici gruppi orientati al profitto, ma infrastrutture in grado di connettere mercati illeciti, economia legale, corruzione, servizi criminali esterni, piattaforme cyber-sociali e, in alcuni casi, obiettivi destabilizzanti (Europol, 2024, 2025). La seconda è che il profilo attoriale

non può essere ricondotto a un tipo psicologico, ma la sua partecipazione criminale è funzione di ruolo, traiettoria, contesto, vulnerabilità e posizione nella rete (Calderoni et al., 2022; INTERPOL, 2026). Pertanto, AI e MUAI, sul piano organizzativo, aumentano scala, automazione, modularità e convergenza con minacce ibride. Mentre dal punto di vista attoriale, riducono le barriere di accesso, amplificano impersonazione e inganno e accrescono la distanza morale dalla vittima. Infine, per quanto concerne la prospettiva istituzionale, esse impongono una risposta che tenga insieme capacità tecnica, cooperazione transnazionale e globale, intelligence finanziaria, network analysis, digital forensics e governance democratica dell'AI (European Parliament & Council of the European Union, 2024; Europol, 2023b).

Da qui la necessità di sviluppare un approccio criminologico ad hoc per lo studio delle reti criminali, capace di leggere sia funzioni e interdipendenze offline/online, che le traiettorie, coercizione, continuità vittima-autore e mediazione tecnologica. Ciò attraverso un'analisi integrata tra criminalità organizzata, cybercrime, estremismi, disinformazione, FIMI e hybrid threats. Occorre, infine, una profonda riflessione normativa ed etica sugli strumenti di AI adottati tanto nella prevenzione quanto nel contrasto delle reti criminali ad alto rischio in un mondo sempre più ibrido.

Riferimenti bibliografici

Antinori A. (2025). *Malicious use of Artificial Intelligence (MUAI): l'uso malevolo dell'intelligenza artificiale nell'ecosistema cyber-sociale. Sicurezza e Scienze Sociali*, 2025(2). Testo disponibile al sito: https://siss.terni.unipg.it/ojs/index.php/siss/article/view/151. DOI: 10.5281/zenodo.17297557.

Bundeskriminalamt (2025). *Bundeslagebild Organisierte Kriminalität 2024*. Testo disponibile al sito: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2024.pdf?__blob=publicationFile&v=8.

Calderoni F., Berlusconi G., Bianchi I., Favarin S. & Dugato M. (2022). *Organized crime groups: A systematic review of individual-level risk factors related to recruitment*. *Campbell Systematic Reviews, 18*(1). Testo disponibile al sito: https://pmc.ncbi.nlm.nih.gov/articles/PMC8833286/. DOI: 10.1002/cl2.1218.

Departamento de Seguridad Nacional (2025). *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2025*. Testo disponibile al sito: https://www.dsn.gob.es/sites/default/files/202510/Estrategia%20Nacional%20contra%20el%20CO%20y%20la%20DG%202025.pdf.

Direzione Centrale per i Servizi Antidroga (2024). *Relazione annuale 2024*. Ministero dell'Interno. Testo disponibile al sito: https://antidroga.interno.gov.it/wp-content/uploads/2024/10/RelazioneAnnuale 2024.pdf.

Direzione Centrale per i Servizi Antidroga (2025). *Relazione annuale 2025*. Ministero

dell'Interno. Testo disponibile al sito: https://antidroga.interno.gov.it/wp-content/uploads/2025/10/Relazione-Annuale-2025.pdf.
Drewer S. & Ellermann A. (2012). *Key future trends in organised crime from a law enforcement perspective. European Police Science and Research Bulletin.* Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/drewer_ellermann_article_0.pdf
European Parliament, & Council of the European Union (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Testo disponibile al sito: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.
Europol (2017). *SOCTA 2017: Serious and organised crime threat assessment*. Testo disponibile al sito: https://www.europol.europa.eu/sites/default/files/documents/socta2017_0.pdf.
Europol (2023a). *The impact of large language models on law enforcement*. Europol Innovation Lab. Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf. DOI: 10.2813/255453.
Europol (2023b). *AI and policing: The benefits and challenges of AI in policing from an ethical and fundamental rights perspective*. Publications Office of the European Union. Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and policing.pdf. DOI: 10.2813/0321023.
Europol (2024a). *Decoding the EU's most threatening criminal networks*. Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EUs%20most%20threatening%20criminal%20networks.pdf. DOI: 10.2813/811566.
Europol (2024b). *Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures.* Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_report__Leveraging_legitimacy__How_the_EU_most_threatening_crim_networks_abuse_legal_business_structures.pdf.
Europol (2025). *EU-SOCTA 2025: The changing DNA of serious and organised crime*. Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
Europol & European Union Intellectual Property Office (2020). *IP crime and its link to other serious crimes: Focus on poly-criminality*. Testo disponibile al sito: https://www.europol.europa.eu/cms/sites/default/files/documents/europol-euipo_polycriminality_report_2.pdf.
INTERPOL (2024). *Global financial fraud assessment*. Testo disponibile al sito: https://www.interpol.int/ar/content/download/21077/file/24COM00556301%20%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03%20v2.pdf.
INTERPOL (2026). *Global financial fraud threat assessment*. Testo disponibile al sito: https://www.interpol.int/Media/Documents/Publications/FinancialCrime/INTERPOL-Global-Financial-Fraud-Threat-Assessment-March-2026
Ministère de l'Intérieur (2025, May 30). *Une stratégie nationale pour lutter contre la cybercriminalité*. Testo disponibile al sito: https://www.interieur.gouv.fr/actualites/actualites-du-ministere/strategie-nationale-pour-lutter-contre-cybercriminalite.

Secrétariat général de la défense et de la sécurité nationale (2025). *Revue nationale stratégique 2025*. Testo disponibile al sito: https://www.sgdsn.gouv.fr/files/2025-08/20250713_NP_SGDSN_Actualisation_2025_RNS_FR.pdf.

United Nations Office on Drugs and Crime (2000). *Definition in the organized crime convention*. Testo disponibile al sito: https://www.unodc.org/e4j/zh/organized-crime/module-1/key-issues/definition-in-convention.html.

United Nations Office on Drugs and Crime (2025, September 29). *Emerging threats in Southeast Asia – Exploitation of AI and automation in the regional cybercrime landscape*. Testo disponibile al sito: https://www.unodc.org/unodc/frontpage/2025/September/emerging-threats-in-southeast-asia--exploitation-of-ai-and-automation-in-the-regional-cybercrime-landscape.html.