RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0249 • articolo sottoposto a peer review • pubblicato in anteprima il 25 nov. 2025

Maria Vittoria Zucca

Mappare il *Crime-as-a-Service*: analisi delle strutture, dei ruoli e dei servizi nell'offerta criminale digitale

La presente ricerca si propone di indagare il fenomeno del *Crime-as-a-Service* (CaaS) quale modello consolidato di "industrializzazione" del crimine digitale. In risposta alle lacune individuate nella letteratura, lo studio segue un approccio metodologico lungo due direttrici: (i) l'analisi dell'ecosistema CaaS, nelle sue componenti strutturali, organizzative e sociali; (ii) la mappatura dei servizi offerti – di supporto diretto e indiretto – e dei modelli economici sottostanti. A seguire, i comuni denominatori ricavati verranno posti a confronto con le definizioni criminologiche tradizionali di criminalità organizzata e, attraverso la costruzione di un *network graph* concettuale, saranno messi in luce punti di convergenza, di divergenza e le aree di non-sovrapposizione tra i due paradigmi. L'obiettivo della ricerca è quello di fornire strumenti interpretativi utili alla comprensione teorico-criminologica, alla qualificazione giuridica e al più efficace contrasto del crimine digitale "organizzato".

Crime-as-a-Service – Mercati illeciti – Criminalità organizzata – Cybercrime – Criminologia digitale

Mapping Crime-as-a-Service: An analysis of structures, roles, and services in the digital criminal offering

This study investigates the phenomenon of Crime-as-a-Service (CaaS) as a consolidated model of digital crime "industrialization." In response to the gaps identified in the existing literature, the research adopts a methodological approach articulated along two main axes: (i) the analysis of the CaaS ecosystem in its structural, organizational and social dimensions; and (ii) the mapping of the services offered – both direct and indirect forms of support – and the underlying economic models. The common denominators emerging from this analysis are subsequently compared with the traditional criminological definitions of "organized crime" and, through the construction of a conceptual network graph, points of convergence, lines of divergence and areas of non-overlap between the two paradigms are highlighted. The aim of the study is to provide interpretative tools that can support theoretical-criminological understanding, legal qualification, and the more effective countering of digitally "organized" crime.

Crime-as-a-Service – Illicit markets – Organized crime – Cybercrime – Digital criminology

L'Autrice è dottoranda del Programma di Interesse Nazionale in Cybersecurity, affiliata presso la Scuola Superiore Sant'Anna di Pisa e la Scuola IMT Alti Studi di Lucca

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

1. Cenni introduttivi: la "mercificazione" del crimine digitale

Si premetta come le dinamiche che oggi contraddistinguono il crimine informatico[1] non rappresentano una rottura radicale rispetto ai paradigmi criminali "classici", bensì una loro trasposizione nell'ambiente digitale. Invero, già nel secolo scorso la teoria criminologica della scelta razionale[2], sulla scia degli studi economici di Becker[3], concepiva il comportamento criminale come il risultato di una valutazione utilitaristica del rapporto costi/benefici associati ad un'azione illecita rispetto a quella lecita. In tale prospettiva, l'agente criminale si comporta come un attore razionale, orientato a massimizzare i benefici (ad esempio, i profitti attesi da un'attività illecita) e, parallelamente, a minimizzare gli eventuali rischi (come l'identificazione, l'arresto e la condanna). Benché originariamente concepito per l'analisi della criminalità "terrestre", tale modello teorico risulta sorprendentemente attuale se traslato nel dominio digitale, ove le medesime logiche attoriali si ripresentano. La transizione verso l'ambiente cibernetico[4] ha infatti favorito un avvicinamento graduale alla carriera (cyber) criminale: una presa di coscienza delle potenzialità (quali versatilità, elusività e opportunità di guadagno) offerte dagli strumenti informatici, che ha indotto molti individui a valutare la convenienza dell'azione digitale illecita.

A ciò si sommi l'odierna facilità di accesso alle competenze necessarie per condurre attività cybercriminali: ciò che un tempo richiedeva elevate capacità tecnico-informatiche è oggi reso disponibile a un pubblico più ampio, grazie ai servizi offerti da reti criminali specializzate, attive sul

1. Sulla nozione di crimine informatico, qui richiamata in senso ampio, si vedano, *ex multis*, Fiorinelli 2023, Picotti 2011, Pecorella 2006.
2. Si v. Cornish–Clarke 1986, Clarke 1985, tra i primi a formalizzare in modo sistematico l'approccio della *rational choice* in ambito criminologico.
3. Si rimanda a Becker 1968, che, muovendo dal suo paradigma economico, re-interpreta il comportamento criminale.
4. Si rimanda a Gibson 1984, per la prima formulazione del concetto di "cyberspazio"; v. inoltre Castells 1996, per sviluppi socio-tecnologici del concetto stesso.

mercato illecito, che adottano modelli di business simili a quelli legittimi[5]. Si può affermare che la digitalizzazione abbia favorito una "industrializzazione" (e, al contempo, "democratizzazione"[6]) del crimine, tramite il fenomeno oggetto di questo studio: il c.d. *Crime-as-a-Service*[7] (da qui in poi, CaaS), espressione paradigmatica della mercificazione domanda-offerta del sapere criminale. Il CaaS consente infatti di esternalizzare competenze tecniche, offrendo servizi e/o strumenti (si pensi al noleggio di *botnet* o allo sviluppo di *malware*) a soggetti terzi, siano essi affiliati o semplici clienti[8], potenzialmente privi di specifiche abilità informatiche, ma parimenti con l'intento di accedere a profitti illeciti.

Ciò comporta una forte riduzione dei costi d'ingresso al "mercato" criminale (in termini di risorse, competenze e rischio) e, parallelamente, una minimizzazione dell'esposizione personale. La vendita di *tool* illeciti, infatti, invece del loro utilizzo "diretto" da parte dello sviluppatore, consente di diluire la responsabilità lungo la catena criminale e di aumentare l'opacità delle operazioni, riducendo la tracciabilità. Si assiste così a una prosecuzione delle logiche razionali di matrice beckeriana e cornishiana da cui si è partiti, per cui l'agire cyber-criminale assume ad oggi i tratti di un'impresa orientata alla convenienza, alla replicabilità e all'efficienza. In questa prospettiva, lo studio si propone di indagare il fenomeno del CaaS, analizzandone *in primis* le strutture organizzative e i servizi offerti, così da, *in secundis*, identificarne i tratti comuni e metterli a confronto con i caratteri della criminalità organizzata tradizionale, al fine di evidenziare convergenze, divergenze (nonché, zone d'ombra) tra i due paradigmi teorico-definitori.

2. Una mappatura del *Crime-as-a-Service*

L'immediato proseguo della trattazione prende atto dalla consapevolezza di una lacuna nella letteratura esistente, derivante dalla mancanza di un approccio sistematico alle diverse tipologie di servizi offerti nell'ambito del CaaS. Gli studi attuali, infatti, tendono a focalizzarsi su alcune forme particolarmente note, come il *Ransomware-as-a-Service* (RaaS)[9], inserito nella famiglia dei *Malware-as-a-Service* (MaaS), trascurandone altre parimenti significative. A ciò si sommi una seconda criticità: la mancanza di studi interdisciplinari in grado di integrare, in un'unica cornice analitica, gli aspetti tecnici e i profili socio-criminologici che caratterizzano i gruppi CaaS. Una comprensione più articolata del fenomeno risulta dunque necessaria per ricavare i comuni denominatori tra le varianti di CaaS e per costruirne una "mappatura" strutturata. Alla luce dei più recenti report istituzionali[10] e degli studi di settore, l'analisi procederà seguendo un duplice binario: (i) l'esame della struttura organizzativa del CaaS, comprensiva dei ruoli professionali coinvolti e delle connessioni sociali; (ii) l'analisi dei principali servizi offerti e dei modelli economico-commerciali ad essi associati.

5. Sul ruolo delle comunità online e dei *marketplace* nel facilitare l'ingresso nel cybercrime, si v. in particolare Lusthaus 2013, che analizza i "mercati delle competenze" nell'ecosistema del cybercrime.
6. Il ruolo delle tecnologie ICT come motori della "democratizzazione" del crimine è stato evidenziato, in termini generali, da Wall 2007.
7. Si adotta qui il termine *Crime-as-a-Service* (sintetizzato, CaaS), in allineamento con i più recenti report istituzionali di settore (v. EUROPOL 2017; EUROPOL 2023).
8. Per "affiliati" si intendono i soggetti terzi che partecipano attivamente a un *network* di CaaS, contribuendo alla diffusione o esecuzione di attività illecite in cambio di incentivi, come percentuali sui profitti generati. Per "clienti", invece, si intendono coloro che acquistano semplicemente i servizi e/o gli strumenti messi a disposizione, senza entrare a far parte di un programma collaborativo strutturato (come avviene tipicamente nei modelli di *Ransomware-as-a-Service* - RaaS).
9. In tema di RaaS, si rimanda per approfondire, ai recenti studi tecnici di Alwashali–Abd Rahman–Ismail 2021; Karapapas–Pittaras–Fotiou–Polyzos 2020; e Meland–Bayoumy–Sindre 2020.
10. Si rimanderà in tal senso ai recenti report periodici pubblicati da Europol, come il SOCTA (*Serious and Organised Crime Threat Assessment*) e l'IOCTA (*Internet Organised Crime Threat Assessment*), poiché offrono una panoramica aggiornata circa le tendenze del crimine organizzato e delle minacce cibernetiche, inclusi fenomeni come il CaaS; cfr. EUROPOL 2017; EUROPOL 2023.

2.1. Architettura socio-organizzativa

Un primo interrogativo centrale nell'analisi delle fenomenologie criminali riguarda la loro morfologia strutturale. Le evidenze empiriche suggeriscono che il CaaS non corrisponda né a una gerarchia criminale rigida tradizionale né a una rete totalmente decentralizzata, ma che si configuri piuttosto come una struttura, si potrebbe dire, "ibrida". Ossia, da un lato paiono prevalere dinamiche orizzontali, nelle quali attori iper-specializzati (come sviluppatori di *malware*, *broker*, affiliati, amministratori di *marketplace*) cooperano, dall'altro, in alcuni segmenti della catena criminale, sembrano emergere elementi verticali, come figure di coordinamento, intermediari dominanti o leader tecnici, che svolgono un ruolo di supervisione delle attività[11]. Questa natura "ibrida" riflette, in parte, la logica imprenditoriale sottostante al modello CaaS, che, in analogia ai modelli leciti (si pensi al *Software-as-a-Service*), riproduce ecosistemi composti da venditori, fornitori e gestori dotati di ampia autonomia, ma sostenuti da nodi centrali che coordinano o facilitano specifiche operazioni[12]. Pertanto, ne emerge, a livello complessivo, un'organizzazione caratterizzata da: flessibilità (nell'assetto interno), specializzazione professionale, relazioni di durata variabile (alle volte configurate quali collaborazioni "a progetto", in funzione delle esigenze del "mercato") e una forte dipendenza da meccanismi di affidabilità e coordinamento reciproco, più che da una rigida catena di comando, punto su cui si tornerà a breve[13].

Sul versante delle connessioni sociali, uno snodo cruciale del CaaS riguarda il ruolo dei canali di comunicazione attraverso cui gli attori criminali entrano in contatto, si coordinano e costruiscono relazioni di fiducia. I *marketplace* e i forum illeciti (spesso ospitati sul *dark web*, ma presenti anche sulla *surface*[14]) rappresentano i principali spazi in cui i potenziali partecipanti vengono reclutati e in cui vengono ricercate competenze specifiche. In tali ambienti digitali, tuttavia, le preoccupazioni legate all'anonimato generano un senso di incertezza circa la qualità dei beni e dei servizi offerti, rendendo fiducia e reputazione risorse preziose per la cooperazione criminale. Invero, per ridurre il rischio di truffe, prodotti di scarsa qualità o infiltrazioni delle forze dell'ordine, le comunità criminali legate al CaaS fanno ricorso a specifici meccanismi reputazionali[15]. L'accesso ai forum può essere infatti regolato da verifiche preliminari, quote di adesione o sistemi *invite-only*[16] e, in alcuni casi, agli aspiranti membri può venire richiesto di dimostrare le proprie capacità tramite prove

11. Sul punto si veda Patsakis–Arroyo–Casino 2024, per una ampia disamina circa l'iper-specializzazione professionale all'interno delle dinamiche criminali di CaaS.
12. Per approfondire le funzionalità (lecite) del *Software-as-a-Service*, Tsai–Bai–Huang 2014.
13. Per esemplificare, si consideri il modello del *Malware-as-a-Service* (MaaS). La dimensione orizzontale emerge nella presenza di una pluralità di attori iper-specializzati che cooperano tra loro: gli sviluppatori di *malware*, gli *exploit developers*, i *reverse engineers* che forniscono servizi tecnici complementari, mentre gli affiliati, gli *initial access brokers*, i *traffer* e i *phisher* operano come unità incaricate della diffusione e monetizzazione del *malware*. All'interno di questo ecosistema si osservano, tuttavia, anche ruoli verticali che introducono elementi di direzione (o coordinamento). Tra questi, i *core maintainers* (o *lead developers*) definiscono il piano di sviluppo tecnico del *malware* e ne stabiliscono gli standard operativi; gli *infrastructure coordinators* prendono decisioni sull'architettura di comando; i *negotiators* centralizzano le trattative con le vittime (si pensi al RaaS) determinando gli importi dei riscatti; e i *financial controllers* sovraintendono alla gestione dei proventi. Completano il quadro i *recruiters* e i *PR managers*, che contribuiscono alla coesione organizzativa attraverso il reclutamento, la gestione dell'immagine pubblica e il mantenimento della reputazione del "brand" criminale. Per approfondire sul punto, Patsakis–Arroyo–Casino 2024.
14. A questi si affiancano anche canali di comunicazione, come gruppi Telegram e server Discord, utilizzati da individui e gruppi per pubblicizzare i servizi, rivendicare capacità tecniche o vendere prodotti malevoli, cfr. Lykousas–Koutsokostas–Casino–Patsakis 2023.
15. Sul punto, Huang–Siegel–Madnick 2017, che analizzano il CaaS come una vera e propria *supply chain* criminale, individuando nei *criminal marketplace* i principali punti di controllo dell'intero ecosistema.
16. Cfr. Yip–Shadbolt–Webber 2013.

pratiche, come di "hackerare un sito web entro x mesi" per mantenere l'iscrizione[17]. In questo contesto, la reputazione assume il valore di un vero e proprio capitale economico: costituisce la principale forma di "moneta" fiduciaria che abilita la cooperazione tra sconosciuti, influenza la capacità di attirare potenziali affiliati, orienta la fissazione dei prezzi e condiziona l'ingresso nei *marketplace* più ricercati.

Nel complesso, tali caratteristiche socio-organizzative delineano il CaaS come un modello industriale del crimine, fondato su reti associative adattabili, ruoli specializzati e meccanismi reputazionali che fungono da "infrastruttura di fiducia", dando luogo a un ecosistema al tempo stesso stabile (nell'operatività) e volatile (nella capacità di mutare forma), nonché fortemente scalabile sul piano economico.

2.2. Servizi offerti *à la carte*

Come evidenziato sino ad ora, il mercato del CaaS offre una gamma estremamente articolata di servizi, strumenti e competenze, che in letteratura risultano spesso privi di una sistematizzazione comune. In questa sede si propone, a tal fine, di suddividerli in due macrocategorie: i servizi di supporto "diretto", cioè che consentono materialmente di eseguire un attacco informatico o di ottenere un accesso tecnico iniziale al sistema target, e i servizi di supporto "indiretto", comprendenti le attività (ancillari) dirette a sfruttare, monetizzare e/o sostenere l'operazione criminale nel tempo[18]. La prima categoria include tutte le offerte che permettono di condurre un attacco in senso stretto o di stabilire un punto d'ingresso: tra queste rientrano il *botnet-as-a-service*, ovverosia il noleggio di reti di dispositivi compromessi; il *traffic/DDoS-as-a-service*, volto alla generazione di traffico ostile o di attacchi di saturazione (DDoS); il *payload-as-a-service*, che mette a disposizione file malevoli già configurati; l'*exploit-as-a-service*, dedicato alla fornitura o licenza di vulnerabilità; il *bulletproof-as-a-service*, ossia infrastrutture di *hosting* progettate per resistere a *takedown* e investigazioni; e, ancora, le varie forme di *phishing-*, *dropper/delivery-* e *proxy-as-a-service*, incaricate rispettivamente di predisporre campagne di *phishing*, distribuire *malware* attraverso vettori affidabili (o automatizzati) e fornire accessi remoti o instradamenti tramite server compromessi per garantire anonimato ed esecuzione sicura dell'attacco[19].

La seconda categoria, invece, comprende tutte quelle funzioni necessarie per sfruttare economicamente gli attacchi, occultarne le tracce o sostenerne l'operatività. Vi appartengono il *laundering-as-a-service*, che comprende servizi di riciclaggio e il reclutamento di *money mules* per la gestione dei flussi finanziari illeciti; il *marketplace-as-a-service*, che fornisce licenze, infrastrutture e strumenti per la gestione di piattaforme di scambio-offerta criminale; l'*obfuscation-as-a-service* e il *security-checker-as-a-service*, volti rispettivamente a rendere un malware più difficile da rilevare e a verificare la qualità tecnica di un cyberattacco; infine, il *training-as-a-service* e il *recruiting-as-a-service*, che permettono di alimentare l'ecosistema favorendo formazione, specializzazione, ricambio e continuità professionale[20].

I modelli economici maggiormente diffusi tra i venditori paiono essere[21]: (i) le formule in abbonamento, tipiche dei servizi continuativi, che prevedono un pagamento ricorrente in cambio dell'accesso stabile a risorse come *botnet*, servizi di *hosting* o strumenti di offuscamento: si tratta di modelli che garantiscono al fornitore entrate costanti e all'acquirente continuità e aggiornamenti tecnici; (ii) le vendite *one-shot*, che riguardano invece l'acquisto singolo di *tool*, accessi iniziali o *exploit*, spesso senza supporto successivo: sono modalità adatte a prodotti che non richiedono

17. Cfr. Holland 2016, che descrive come forum, *marketplace* e canali di scambio diventino luoghi di "*talent scouting*", nei quali la reputazione tecnica costituisce un asset per attrarre collaboratori affidabili.
18. Per un'analisi longitudinale circa l'evoluzione dell'offerta e della domanda di CaaS all'interno dei forum cybercriminali, si veda Akyazi–van Eeten–Hernández Gañán 2021, che esaminano undici anni di attività su *HackForums*, uno dei più grandi e longevi forum di *cybercrime* in lingua inglese presenti sul *surface web*.
19. *Ibidem*.
20. *Ibidem*, ma si v. anche Huang–Siegel–Madnick 2017.
21. Per approfondire il versante economico-commerciale si rimanda a Huang–Siegel–Madnick 2017.

manutenzione prolungata e che possono essere monetizzati tramite transazioni isolate; (iii) modelli di affiliazione o di *revenue-share*, nei quali l'operatore principale mette a disposizione l'infrastruttura e l'affiliato riceve una percentuale dei profitti, schema particolarmente comune nel RaaS[22].

Si noti ancora come le dinamiche di prezzo e di funzionamento del mercato CaaS risultino fortemente condizionate sia da fattori di offerta (ad esempio i costi di sviluppo, di manutenzione e il livello di rischio percepito dal venditore) sia da fattori di domanda (quali il numero di acquirenti potenziali e il valore dell'obiettivo), ricalcando, ancora una volta, le logiche di business rinvenibili dei mercati leciti. L'evidenza empirica raccolta da Akyazi, van Eeten e Gañán nel 2021[23] relativa a undici anni di dati provenienti da *HackForums*, uno dei principali forum di cybercrime, mostra a tal proposito una diversificazione delle fasce di prezzo e una segmentazione dell'offerta. La parte "bassa" del mercato risulta costituita da servizi automatizzati – come traffico web fraudolento (TRaaS; 7-15 dollari per 1.000 visitatori) o installazioni malware (PLaaS; 0,02-0,1 dollari per installazione) – caratterizzati da un'elevata omogeneità dell'offerta e da margini contenuti, contribuendo alla c.d. democratizzazione dell'accesso al cybercrime. All'estremo opposto si colloca la parte "alta" del mercato, che comprende infrastrutture *zero-day* ed *exploit-as-a-service*, con prezzi che possono superare i 250.000 dollari per licenza o raggiungere 150.000 dollari al mese per pacchetti avanzati. Invece, servizi intermedi, come *botnet-as-a-service* o *bulletproof-as-a-service*, adottano tariffe più contenute, ma regolari (circa 40 dollari/mese per *botnet*, 300 dollari/mese per *hosting*). Nel complesso pare emergere un mercato a doppia velocità: da un lato, servizi a basso costo e facilmente accessibili; dall'altro, un settore altamente specializzato con prezzi elevati e relazioni più stabili, dove reputazione e fiducia fungono da meccanismi di regolazione economica.

3. CaaS e *organized crime* a confronto: convergenze e divergenze

L'analisi condotta nella sezione precedente, indirizzata all'individuazione dei tratti-chiave del CaaS, consente ora di affrontare il passaggio successivo, e conclusivo, dello studio: una comparazione tra il modello CaaS e le principali definizioni criminologiche di criminalità organizzata[24]. Tale confronto permette di interrogarsi se, e in quale misura, gli attori del CaaS possano ricondursi a forme "classiche" di *organized crime*, se il digitale abbia (ri) configurato i tratti-chiave di tali gruppi o se, di conseguenza, emerga l'esigenza di rivedere o integrare le maglie definitorie tradizionali sul tema. Seguendo un approccio metodologico adottato dagli studi criminologici in tema di cybercrime[25], il CaaS può essere messo, in questa sede, in relazione con i quindici elementi costitutivi della criminalità organizzata, tratti dalla letteratura di riferimento[26]. Per ragioni di sistema, tali elementi sono ivi distribuiti in cinque macrocategorie, all'interno delle quali vengono ri-allocati, come segue:

22. Il modello "affiliazione" trova una delle sue espressioni più strutturate nel caso di LockBit, gruppo RaaS tra i più attivi fino al 2024: l'operatore centrale forniva infrastruttura, pannelli di gestione, strumenti di cifratura e supporto tecnico, mentre gli affiliati conducevano gli attacchi *ransomware* e trattenevano una quota significativa dei profitti, secondo un sistema di *revenue sharing* altamente organizzato e supportato da meccanismi reputazionali, cfr. El Emary–Yaghi 2024.
23. Cfr. Akyazi–van Eeten–Hernández Gañán 2021.
24. Sul tema della ri-configurazione delle forme digitali di criminalità organizzata, la letteratura criminologica recente converge sulla necessità di adottare approcci analitici flessibili e non rigidamente dicotomici. Si citi sul punto Picarella 2025, che critica la contrapposizione binaria del "*to be or not to be*" e propone modelli definitori elastici capaci di cogliere la natura ibrida e fluida dei gruppi cybercriminali odierni.
25. L'approccio metodologico richiama quello adottato da Di Nicola–Baratto–Vettori 2025, che ricostruiscono la griglia dei quindici elementi definitori dell'*organized crime*, per poi successivamente applicarli a un corpus di 71 casi giudiziari tratti dal database UNODC SHERLOC, selezionati in quanto caratterizzati da una duplice qualificazione come "cybercrime" e come "partecipazione a un gruppo criminale organizzato".
26. Si rimanda per tale operazione a Varese 2010; Von Lampe 2016.

a) La prima macrocategoria, "strutturale", comprende la presenza di un gruppo composto da almeno tre persone che collaborano stabilmente nella commissione di reati (*group/collaboration*), la durata nel tempo dell'associazione criminale (*duration*), l'esistenza di una catena di comando gerarchica (*hierarchy*) e, più in generale, la presenza di una struttura organizzativa, semplice o complessa che sia (*structure*).
b) La seconda, di natura "economico-funzionale", riguarda l'orientamento primario al profitto economico (*economic profit*), il funzionamento secondo una logica strettamente imprenditoriale (*enterprise*) e l'offerta sistematica di beni o servizi illeciti (*provision of illegal goods/services*).
c) Segue una dimensione "socioculturale", che include l'aspirazione al potere e al controllo sociale o politico (*desire for power*), il radicamento in identità etniche o culturali, spesso territorialmente definite (*ethnicity/subculture*), nonché il ricorso a reti sociali estese e legami relazionali come risorsa operativa (*network*).
d) La quarta categoria concerne aspetti di "governance e coercizione", quali l'impiego di violenza come strumento di gestione interna ed esterna (*corruption/violence*), la ricerca di posizioni monopolistiche in mercati illegali (*monopoly*) e l'esistenza di regole interne e meccanismi di enforcement che disciplinano il comportamento dei membri (*internal regulation and enforcement*).
e) Infine, la quinta macrocategoria, di carattere "operativo", richiama la commissione di reati gravi (*illegal organized activities*) e la capacità del gruppo di generare danni significativi, diretti o indiretti, a individui, istituzioni o sistemi (*harm*).

L'obiettivo della seguente comparazione è, si ribadisce, quello di individuare le aree di invarianza, varianza e assenza rispetto ai modelli tradizionali di *organized crime*, al fine di verificare se e in quale misura l'ambiente digitale agisca come fattore di ri-configurazione adattiva delle dinamiche criminali "organizzate". L'analisi è stata condotta tramite l'elaborazione di un *Network Graph* (Fig. 1), che visualizza per ciascun elemento costitutivo-chiave le tre condizioni analitiche di: invarianza (in verde), varianza (in giallo) e assenza (in grigio) all'interno del modello CaaS, in rapporto alle caratteristiche del crimine organizzato tradizionale.

A seguire i risultati emersi, riportati secondo le cinque macrocategorie sistematiche precedentemente delineate:

a) *Strutturale*: il CaaS presenta alcuni elementi di continuità con la criminalità organizzata tradizionale, in particolare per quanto riguarda la presenza di gruppi composti da più soggetti che cooperano stabilmente e l'esistenza di una struttura organizzativa che, per quanto flessibile, risulta essere riconoscibile (*group, structure*). Invero, nei contesti CaaS è possibile trovare nuclei cooperativi relativamente stabili, reti di affiliati, ruoli differenziati e coordinamento operativo. Tuttavia, altri elementi "classici" – quali la durata nel tempo e la gerarchia (*duration, hierarchy*) – mostrano una varianza. Le organizzazioni CaaS tendono infatti a configurarsi come aggregazioni fluide e a volte temporanee, costituite per il perseguimento di obiettivi specifici (come campagne di attacco, operazioni RaaS) e successivamente disgregate o ri-configurate in funzione delle opportunità di mercato. Ne risulta un assetto che non corrisponde né a una rigida piramide gerarchica né a una rete totalmente dispersa, ma a una configurazione composita (o "ibrida", cfr. par. 2.1). La struttura complessiva alterna così elementi reticolari e momenti di verticalizzazione, riflettendo una adattabilità tipica ai contesti digitali (per loro natura, altamente mutevoli).
b) *Economico-funzionale*: si riscontra una forte invarianza rispetto al modello "classico" dell'impresa criminale. Il CaaS conserva infatti un orientamento esplicito al profitto economico (*economic profit*), adottando logiche di efficienza, scalabilità e mitigazione del rischio tipiche delle organizzazioni imprenditoriali (*enterprise*)[27]. Tale continuità trasla il paradigma dell'impresa criminale in chiave meramente tecnologica: il mercato dei servizi – digitali – illeciti (*provision*) si struttura secondo dinamiche di domanda-offerta, segmentazione,

27. Si v. Schelling 1967, che già proponeva una lettura economica dell'impresa criminale, sostenendo che molte dinamiche di mercato, incentivi e strutturazione organizzativa presenti nelle attività illecite non andavano a differire profondamente da quelle delle imprese legali.

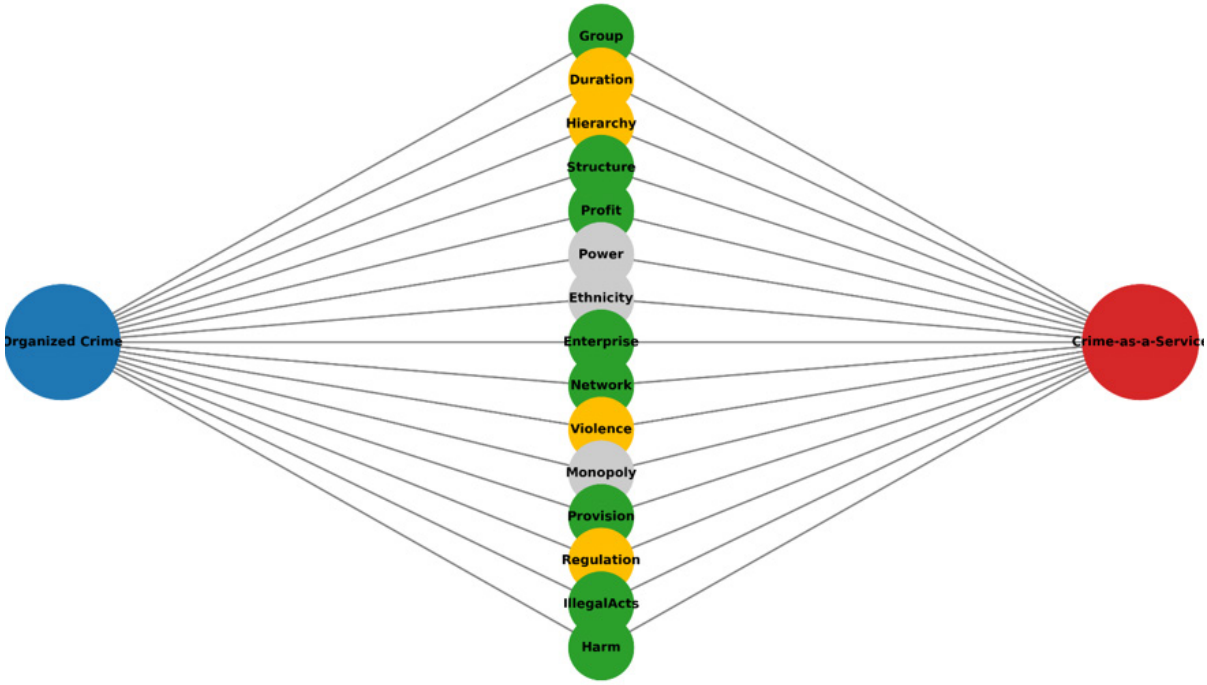

Fig. 1 — *Network Graph elaborato dall'autrice, sui 15 elementi costitutivi dell'organized crime, cfr. Von Lampe 2016 e Varese 2010*

specializzazione funzionale e diversificazione dei prodotti, specularmente a quanto avviene nei mercati leciti.

c) *Socioculturale*: evidenzia i mutamenti più profondi. Nelle reti CaaS, elementi quali il desiderio di potere radicato territorialmente (*power*) e l'appartenenza etnica o subculturale (*ethnicity/subculture*), centrali nei modelli tradizionali di criminalità organizzata, risultano pressoché assenti. Le logiche identitarie e territoriali lasciano infatti il posto a una comunità digitale transnazionale (ma anche, a-territoriale), legata non tanto da vincoli culturali, ma da meccanismi reputazionali e da interessi economici condivisi. La coesione sociale interna (*network*) permane, ma si trasforma: non si fonda più su appartenenze precostituite, bensì su forme di fiducia costruite attraverso i *marketplace* criminali, basate su affidabilità tecnica e capacità di onorare gli impegni. Questa de-territorializzazione determina una vera e propria de-culturalizzazione del legame criminale, in cui il capitale sociale risulta definito dalla reputazione operativa più che dall'identità (o sottocultura) condivisa.

d) *Governance e coercizione*: la governance criminale nel CaaS si esercita attraverso forme di regolazione e coercizione digitali. La violenza, centrale nell'*organized crime* tradizionale (*violence*), viene ricodificata in modalità tecnologiche: si pensi al RaaS, in cui l'estorsione "informatica" sostituisce quella fisica come strumento di intimidazione e pressione sulle vittime. Analogamente, la regolazione interna (*internal regulation and enforcement*) si manifesta tramite programmi di affiliazione online, regole di condotta e sistemi di reputazione condivisi nei *marketplace*, che definiscono in modo vincolante ciò che è consentito e proibito all'interno del gruppo[28]. Quanto al monopolio

28. Si vedano, ad esempio, le *rules of conduct* pubblicate da gruppi RaaS come REvil, LockBit e Conti, che prevedono divieti espliciti (quali di colpire infrastrutture sanitarie o organizzazioni non profit), obblighi operativi (tempistiche di consegna, standard minimi di qualità del *malware*, procedure di negoziazione) e sanzioni in caso di violazione. Tali regole sono spesso integrate da sistemi reputazionali su *marketplace* come *Exploit* o

(*monopoly*), le dinamiche appaiono differenti: il mercato CaaS è infatti aperto, frammentato e altamente competitivo, il che rende improbabile la formazione di posizioni di dominio duraturo o la concentrazione stabile del potere.

e) *Operativa*: Le gravi attività illecite (*illegal activities*) proprie delle reti CaaS, insieme alla loro capacità di ingenerare danni significativi (*harm*), mostrano una sostanziale invarianza rispetto ai modelli tradizionali. Sebbene cambino, digitalmente, gli strumenti e le modalità di esecuzione, il CaaS continua infatti a porre in essere forme di attività criminale coordinate ad alto impatto (si pensi agli attacchi *ransomware* su larga scala), mantenendo un significativo potere lesivo nei confronti di individui, imprese e istituzioni, con impatti sulla sicurezza economica, informativa e, più in generale, sulla stabilità dei sistemi digitali.

4. Prospettive teoriche e giuridiche emergenti

Tirando le fila dell'analisi, il confronto tra il modello CaaS e le definizioni criminologiche di *organized crime* rivela: il passaggio dalle forme di controllo territorializzato a gruppi reticolari e a-spaziali; dalla coercizione fisica a quella tecnologica; dalle gerarchie stabili a strutture "ibride" e fluide. Ne emerge un paradigma in cui il nucleo economico-organizzativo dell'impresa criminale resta pressoché invariato, mentre mutano – digitalizzandosi – i *modi operandi* e le dinamiche relazionali. Tale evidenza richiama la necessità di un'integrazione più stretta tra teoria criminologica e prospettiva giuridico-penale, così da poter inquadrare normativamente la natura organizzata, seppur digitalmente riconfigurata, delle economie del crimine basate sul modello CaaS[29].

In questa direzione, la ricerca criminologica futura dovrebbe approfondire ulteriormente la struttura dei *network* CaaS, le loro dinamiche collaborative e, soprattutto, i meccanismi motivazionali e di affiliazione che guidano la partecipazione degli attori, ancora poco indagati. Comprendere perché e come gli affiliati entrino, permangano o abbandonino tali ecosistemi costituirebbe un passaggio essenziale per formulare strategie preventive realmente efficaci. Parimenti, meriterebbe maggiore attenzione la ricostruzione dei sistemi di regolazione interna e delle modalità di governance criminale, elementi decisivi per spiegare la resilienza di queste reti.

Sul versante normativo, risulta indispensabile una qualificazione giuridica coerente delle forme "organizzate" di CaaS, necessitante di categorie giuridiche flessibili e sensibili alle specificità singole dei modelli *as-a-service*, assieme alla previsione di strumenti investigativi aggiornati – dalla *digital forensics* alle tecniche di *blockchain analytics* – utili per tracciare pagamenti, mappare reti finanziarie e identificare le connessioni operative tra gli attori coinvolti. L'attuale quadro legislativo rimane infatti, in parte, lacunoso (si pensi agli interventi della legge n. 90/2024), e richiederebbe un ripensamento capace di cogliere la natura dei modelli CaaS. In definitiva, una sinergia effettiva tra studi tecnici, criminologia e diritto, fondata su strumenti – teorico/definitori e operativi – adeguati e aggiornati, consentirebbe di comprendere appieno la complessità del CaaS e di elaborare relative strategie di prevenzione e contrasto idonee a fronteggiare tali fenomeni criminali. Il presupposto di fondo di questo studio è il seguente: le definizioni modellano le risposte; e nell'era digitale, solo definizioni capaci di evolvere possono garantire interventi realmente efficaci.

Riferimenti bibliografici

U. Akyazi, M. van Eeten, C. Hernández Gañán (2021), *Measuring Cybercrime-as-a-Service (CaaS) Offerings in a Cybercrime Forum*, in "Proceedings of the Workshop on the Economics of Information Security (WEIS 2021)", 2021

BreachForums, in cui i membri vengono classificati tramite *rating*, *feedback* e *ban list*, strumenti cruciali per garantire affidabilità e disciplina interna. Per approfondire, Hägvall–Valverde 2024.

29. Così anche Whelan–Bright–Martin 2023.

A.A.M.A. Alwashali, N.A. Abd Rahman, N. Ismail (2021), *A Survey of Ransomware-as-a-Service (RaaS) and Methods to Mitigate the Attack*, in "Proceedings of the 14th International Conference on Developments in eSystems Engineering (DeSE 2021)", IEEE, 2021

G.S. Becker (1968), *Crime and Punishment: An Economic Approach*, in "Journal of Political Economy", 1968

M. Castells (1996), *The Rise of the Network Society*, Blackwell, 1996

R. Clarke, D. Cornish (1985), *Rational Choice Theory*, in "Crime and Justice", 1985

D. Cornish, R. Clarke (1986), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer, 1986

A. Di Nicola, G. Baratto, B. Vettori (2025), *Criminological definitions of organized crime on the digital test bench: towards a physical-digital framework*, in "Trends in Organized Crime", 2025

I.M.M. El Emary, K.A. Yaghi (2024), *Machine Learning Classifier Algorithms for Ransomware LockBit Prediction*, in "Journal of Applied Data Sciences", vol. 5, 2024, n. 1

EUROPOL (2023), *Cyber-attacks: the apex of crime-as-a-service (IOCTA 2023)*, 2023

EUROPOL (2017), *European Union Serious and Organised Crime Threat Assessment Report (SOCTA) 2017*, in www.europol.europa.eu/, 2017

G. Fiorinelli (2023), *Nomina nuda tenemus? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in "Discrimen.it", 2023

W. Gibson (1984), *Neuromancer*, Ace Books, 1984

J. Hägvall, G. Valverde, (2024), *A Case Study of DarkDock Marketplace: Seller-Buyer Trust & Reputation in Cybercrime Services*, Linnaeus University, disponibile su DiVA Portal, 2024

R. Holland (2016), *The Hacker Talent Shortage: What Organizations Can Learn from the Recruitment Efforts of Their Attackers*, in "Digital Shadows", 2016

K. Huang, M. Siegel, S. Madnick (2017), *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*, CISL Working Paper n. 2017-17, Massachusetts Institute of Technology, 2017

C. Karapapas, I. Pittaras, N. Fotiou, G.C. Polyzos (2020), *Ransomware-as-a-Service Using Smart Contracts and IPFS*, in "2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)", IEEE, 2020

J. Lusthaus (2013), *How organized is organised cybercrime?*, in "Global Crime", vol. 14, 2013

N. Lykousas, V. Koutsokostas, F. Casino, C. Patsakis (2023), *The Cynicism of Modern Cybercrime: Automating the Analysis of Surface Web Marketplaces*, in "2023 IEEE International Conference on Service-Oriented System Engineering (SOSE)", IEEE, 2023

P.H. Meland, Y.F.F. Bayoumy, G. Sindre (2020), *The Ransomware-as-a-Service economy within the darknet*, in "Computers & Security", vol. 92, 2020

C. Patsakis, D. Arroyo, F. Casino (2024), *The malware as a service ecosystem*, in "Malware: Handbook of Prevention and Detection", Springer Nature, 2024

C. Pecorella (2006), *Il diritto penale dell'informatica*, CEDAM, 2006

L. Picarella (2025), *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, Donzelli, 2025

L. Picotti (2011), *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in "Rivista trimestrale di diritto penale dell'economia", 2011, n. 4

T.C. Schelling (1967), *Economics and Criminal Enterprise*, in "The Public Interest", 1967, n. 7

W. Tsai, X. Bai, Y. Huang (2014), *Software-as-a-Service (SaaS): Perspectives and Challenges*, in "Science China Information Sciences", vol. 57, 2014, n. 5

F. Varese (2010), *What is Organized Crime?*, in F. Varese (a cura di), "Organized Crime", Routledge, 2010

K. Von Lampe (2016), *Organized crime: Analyzing illegal activities, criminal structures, and extra-legal governance*, SAGE Publications, 2016

D.S. Wall (2015), *Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, in "The European Review of Organised Crime", vol. 2, 2015, n. 2

D.S. Wall (2007), *The Transformation of Crime in the Information Age*, Polity Press, 2007

C. Whelan, D. Bright, J. Martin (2023) *Reconceptualising organised (cyber)crime: the case of ransomware*, in "Journal of Criminology", vol. 56, 2023, n. 4

M. Yip, N. Shadbolt, C. Webber (2013), *Why forums?: An Empirical Analysis into the Facilitating Factors of Carding Forums*, in "Proceedings of the 5th Annual ACM Web Science Conference", 2013