Review Article

Towards a Digital Sociology of Organized Crime: A Comprehensive Theoretical Synthesis

Joseph Murphy*

1. School of Inclusive and Special Education, DCU Institute of Education, St. Patrick's Campus, Dublin, Ireland

* Correspondence: Joseph.murphy@.dcu.ie

Abstract: Traditional paradigms of organized crime historically conceptualized around terrestrial hierarchies, physical territoriality, and the "Mafia mystique," are increasingly inadequate for capturing the complexities of contemporary criminal operations. This paper presents a theoretical synthesis establishing a digital sociology of organized crime, reframing illicit entities as dynamic sociotechnical assemblages rather than rigid, human-centric bureaucracies. Drawing on Actor–Network Theory (ANT) and concepts of "partial organization," the synthesis demonstrates how digital infrastructures, algorithms, and automated execution (such as botnets) act as non-human agents that reconfigure criminal agency, blur accountability, and foster hybrid "cyborg crime." The analysis explores the structural commodification of technical expertise through Crime-as-a-Service (CaaS) frameworks, illustrating how digital platforms reshape diverse illicit markets—including human smuggling, counterfeit pharmaceutical distribution, and wildlife trafficking—by lowering technical barriers, scaling reach, and weaponizing platform affordances. Furthermore, the paper addresses the "fraudogenic" horizon driven by artificial intelligence and synthetic media (deepfakes), which automate deception and undermine traditional evidentiary standards. Methodologically, the study advocates for "digital realism" and Crime Script Analysis to map procedural vulnerabilities while recognizing how traditional subcultural trust persists within digital co-offending networks. Examining the COVID-19 pandemic as a catalytic shock, the synthesis highlights how global disruptions accelerate digital adaptation in illicit supply chains while simultaneously fostering citizen-led "digilantism." Ultimately, this paper argues that digital infrastructures must be understood not as neutral conduits, but as foundational layers of criminal reality, calling for an adaptive, relational, and methodologically pluralist research agenda for future criminological and sociological inquiry.

Keywords: organized crime, mafia mystique, actor–network theory, surveillant assemblage

1. INTRODUCTION

For much of the twentieth century, organized crime was predominantly theorized through the lens of the "Mafia mystique" or conceptualized as a rational, bureaucratic enterprise characterized by stable hierarchies, centralized authority, and clearly delineated chains of command [1]. Such models presupposed organizational coherence, territorial embeddedness, and human-centric coordination. However, the advent and diffusion of the internet have fundamentally destabilized these assumptions, functioning as a catalyst for the "dis-organization" of crime by displacing monolithic structures with flexible, decentralized, and transient networks of actors [2]. Within the digital milieu, contemporary forms of criminal organization are more productively understood through Actor–

Network Theory (ANT). ANT challenges instrumentalist conceptions of technology by foregrounding the agency of non-human actors, thereby reframing digital infrastructures, algorithms, and platforms as constitutive elements of criminal assemblages rather than neutral tools [3]. From the perspective, online criminality operates within a broader “surveillant assemblage” in whom human and technological actors are recursively entangled in processes of coordination, control, and visibility [4]. First, the proliferation of botnets exemplifies the emergence of “cyborg crime,” wherein hybrid criminal actor-networks blur the distinction between human intentionality and automated execution [4]. In such configurations, scripts, malware, and machine-driven decision-making function alongside human operators, rendering authorship, accountability, and agency increasingly opaque [6]. Second, these developments underscore the sociometrical nature of contemporary criminal organization. Organizational boundaries are no longer anchored in physical territory or stable membership but are instead constituted through dynamic “socio material” entanglements of code, hardware, platforms, and social relations [7]. Finally, many digitally mediated criminal group’s exhibit characteristics of “partial organization,” selectively deploying elements such as hierarchy, rule enforcement, or surveillance while eschewing the administrative burdens and visibility associated with fully formalized institutions [8]. Collectively, these shifts signal a profound reconfiguration of organized crime, in which organizational form, agency, and governance are increasingly contingent, distributed, and technologically mediated [9].

2. THE DIGITAL MARKETPLACE: "CRIME-AS-A-SERVICE" (CAAS)

The digitalization of illicit trade has given rise to what has been described as a “hackers’ bazaar”: a globally networked, decentralized marketplace in which stolen data, malware, and exploit kits are exchanged with relative anonymity and minimal barriers to entry [10]. Within the environment, criminal expertise itself has been commodified, enabling low-skill or novice actors to acquire advanced technical capabilities that were previously confined to highly specialized offenders. As a result, digital infrastructures function not merely as facilitators of illicit exchange but as mechanisms for the standardization, scaling, and diffusion of criminal competencies. The expansion of digitally mediated organized crime extends across a wide range of illicit markets, reshaping both their organizational forms and operational logics [11]. First, in the context of human smuggling and trafficking, digital platforms have increasingly supplanted physical recruitment sites and face-to-face intermediaries. So-called “social smugglers” exploit encrypted messaging applications and social media platforms to coordinate movement, negotiate fees, and manage financial transactions, thereby reducing exposure to law enforcement while expanding their transnational reach [12] These practices blur the boundaries between social networking, commercial exchange, and criminal facilitation. Second, the online distribution of counterfeit and illicit pharmaceuticals—particularly via social media platforms—constitutes a significant and growing public health risk. Such markets leverage sophisticated branding strategies, platform affordances, and situational crime prevention bypasses to enhance legitimacy and evade regulatory scrutiny. The migration of pharmaceutical crime into digital spaces thus reflects not only technological adaptation but also the strategic exploitation of consumer trust and algorithmic visibility. Finally, wildlife and environmental crimes have undergone a comparable digital transformation [13]. The illicit trade in exotic pets, including endangered species such as slow lorises and Asian otters, has been amplified through visually oriented platforms such as Instagram, which provide access to vast, largely unregulated audiences. Here, affective appeal, aesthetic presentation, and platform virality operate as key drivers of demand, complicating traditional enforcement approaches grounded in border control and physical markets. Collectively, these cases illustrate how digital technologies have diversified illicit commodities while simultaneously reconfiguring the spatial, organizational, and normative dimensions of organized crime. Rather than constituting a discrete category of “cybercrime,” these developments point to the

hybridization of online and offline criminal economies, in which digital infrastructures are integral to market expansion, coordination, and concealment [14].

3. DISRUPTIVE TECHNOLOGIES: AI AND THE "FRAUDOGENIC" HORIZON

The so-called “Internet Revolution” has been widely characterized as inherently “fraudogenic,” insofar as it has produced socio-technical conditions in which deception can be readily automated, replicated, and scaled across populations with minimal marginal cost [15]. Digital infrastructures not only lower barriers to fraudulent activity but also normalize impersonation, obfuscation, and asymmetries of information, thereby embedding fraud as a routine and systemic feature of contemporary online environments. Within the context, recent developments signal intensification rather than a departure from earlier patterns, most notably through the malicious deployment of artificial intelligence [16]. Advances in machine learning have enabled the production of deepfakes and the operation of semi-autonomous agents capable of convincingly simulating human identity, intent, and trustworthiness, effectively weaponizing authenticity itself. The emergence of deepfake technologies poses a particularly acute challenge for governance and enforcement institutions. As [17] observes, the capacity to generate hyper-realistic synthetic audio and video content precipitates a “facing reality” crisis for law enforcement, undermining traditional evidentiary standards and eroding the reliability of sensory verification. These technologies significantly enhance the effectiveness of advanced social engineering attacks, facilitate large-scale impersonation fraud, and enable the manipulation of public opinion through highly targeted and persuasive disinformation campaigns. Consequently, the deepfake phenomenon exemplifies a broader shift in the political economy of crime, wherein the distinction between the authentic and the fabricated becomes increasingly unstable, complicating efforts to regulate trust, accountability, and truth in digital societies [18].

4. METHODOLOGICAL INNOVATIONS: SCRIPTING AND DIGITAL REALISM

Analyzing these complex, transnational, and technologically mediated criminal activities necessitates a shift toward what [19] terms “digital realism,” alongside the adoption of robust data-driven analytical approaches capable of capturing both online and offline dynamics. Such perspectives reject technological determinism while simultaneously acknowledging the constitutive role of digital infrastructures in shaping criminal opportunity structures. Within the methodological landscape, Crime Script Analysis has emerged as a particularly effective tool in the digital sociologist’s analytical repertoire [20]. By disaggregating criminal activities into sequential stages—ranging from initial preparation and coordination to execution and eventual “cashing out”—that approach enables the systematic identification of situational vulnerabilities and intervention points across the criminal process. Applied to cyber-enabled offenses, Crime Script Analysis facilitates granular examination of the “social networks of malware writers,” allowing study to trace how information and communication technology (ICT) expertise is acquired, circulated, and operationalized within illicit online environments [21]. Such analyses reveal that, notwithstanding the digital character of these crimes, the underlying social architectures frequently depend on conventional mechanisms of trust formation, reputation signaling, and subcultural socialization. Indeed, co-offending networks within the digital underground often evolve through processes analogous to those observed in offline criminal milieus, underscoring the persistence of established social dynamics even within highly technologized criminal contexts [22].

5. GLOBAL SHOCKS: COVID-19 AS A DIGITAL ACCELERATOR

The COVID-19 pandemic functioned as a critical catalyst for criminal innovation, accelerating pre-existing trends toward digitalization and organizational flexibility within illicit economies [23]. As restrictions on physical mobility disrupted established routes and face-to-face interactions, organized crime groups exhibited a high degree of adaptive capacity by shifting operational, communicative, and logistical practices to what has been described as the "busy internet". Rather than producing a temporary suspension of criminal activity, the pandemic reconfigured opportunity structures, compelling criminal actors to experiment with novel digital modalities. One significant adaptation involved a strategic pivot within illicit supply chains [24]. Traditional drug trafficking organizations adjusted their behavioral patterns in response to border closures, heightened surveillance, and volatile pricing by increasing their reliance on digitally mediated coordination, including encrypted communications and platform-based logistics. These shifts underscore the resilience of transnational criminal markets and highlight the extent to which digital infrastructures have become integral to maintaining continuity under conditions of acute disruption. Concurrently, the pandemic period witnessed an intensification of digitally mediated forms of vigilantism. Practices of "digilantism" and crowd-sourced policing expanded as citizens mobilized social media platforms to publicly identify, shame, and sanction individuals perceived to be violating public health regulations or social norms [26]. While often framed as participatory governance or civic responsibility, such practices raise significant concerns regarding due process, misidentification, and the privatization of surveillance. Taken together, these developments illustrate how crisis conditions not only reshape organized crime but also transform the broader ecology of control, blurring the boundaries between formal enforcement, informal social regulation, and digital participation [26].

6. CONCLUSION

The future trajectory of study on African and global organized crime increasingly depends on the development of an integrated digital sociology attentive to the "entanglements of humans and things" that constitute contemporary social and criminal life. Such an approach requires a decisive departure from conceptualizations of the internet as a neutral or instrumental "conduit" for criminal activity and instead demands its recognition as a foundational layer of social reality—one that actively structures interaction, organization, and meaning-making. In that sense, digital infrastructures are not external to organized crime but are intrinsic to its contemporary forms, logics, and trajectories. Empirically, the shift is evident across diverse contexts and modalities. From the "surf and turf wars" characterizing online gang rivalries and territorial signaling, to the exploitation of peer-to-peer lending platforms for money laundering within Chinese financial ecosystems, organized crime increasingly operates in a natively digital register. These phenomena underscore the inadequacy of analytical frameworks that treat online dimensions as ancillary or derivative of offline criminality. Instead, they point to the need for theoretical models capable of capturing the co-evolution of digital platforms, economic infrastructures, and illicit social networks. The central challenge for the next generation of scholars, therefore, lies in sustaining intellectual rigor amid the epistemic pressures of the "big data" era. The entails balancing methodological innovation with critical reflexivity, and ensuring that criminological theories remain sufficiently agile, relational, and adaptive to account for criminal networks whose forms are fluid, distributed, and continuously reassembled. Only through such theoretically informed and methodologically plural approaches can organized crime study remain analytically relevant in an increasingly data-saturated and digitally entangled world.

REFERENCES

[1] Baratto, G., & Vettori, B. (2025). Criminological definitions of organized crime on the digital test bench: towards a physical–digital framework. Trends in Organized Crime, 1-17.

[2] Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in organized crime*, 1-20.

[3] Brada, A., & Dahmani, F. (2025). Criminal Behavior in the Digital Environment: Historical Foundations and a Sociological Perspective. *Revista Universitară de Sociologie*, *21*(2), 10.

[4] Brada, A., & Dahmani, F. (2025). Criminal Behavior in the Digital Environment: Historical Foundations and a Sociological Perspective. *Revista Universitară de Sociologie*, *21*(2), 10.

[5] Schneider, S. (2024). *An ontology of organized crime: A meta-analytical framework and enforcement implications*. Taylor & Francis.

[6] Darabseh, R. S., & Alkhatib, A. J. (2025). The Sociology of Cybercrime: Causes and Prevention. *Pakistan Journal of Life & Social Sciences*, *23*(1), 4014.

[7] Oghazi, P., Kordestani, A., & Mostaghel, R. (2026). Ecosystem-based framework for organized cybercrime. *International Entrepreneurship and Management Journal*, *22*(2), 86.

[8] Toprak, K. (2026). The Control-Opportunity Nexus: Synthesizing Frameworks for Digital Crime. In *Crypto-Assets & Crime: Exploiting Opportunities and Exercising Control in Fraud, Ransomware Attacks, and Money Laundering* (pp. 19-34). Cham: Springer Nature Switzerland.

[9] Nicaso, A., & Danesi, M. (2023). *The dark mafia: organized crime in the age of the internet*. Taylor & Francis.

[10] Sguotti, G. (2025). Web and SNS, the digital evolution of organized crimes. *Social Justice and Organized Crime*, *1*, 191-210.

[11] L'Hoiry, X., Moretti, A., & Antonopoulos, G. A. (2024). Human trafficking, sexual exploitation and digital technologies. *Trends in organized crime*, *27*(1), 1-9.

[12] Kamden, A., Bouché, V., Silver, B., Freeman, N., & Euteneier, J. (2026). Behind the Screen: Online Sex Buyer Networks and the Organized Criminal Promotion of Exploitation. *Dignity: A Journal of Analysis of Exploitation and Violence*, *11*(2), 9.

[13] Muhammad, G. R., Marwiyah, S., Paramitha, V. N., & Hamdani, F. (2026). Combating Digital Transnational Organized Crime: Assessing the Effectiveness of Mutual Legal Assistance for Indonesia. *Begawan Abioso*, *17*(2), 253-276.

[14] Pereda, V. (2022). Why Global North criminology fails to explain organized crime in Mexico. *Theoretical Criminology*, *26*(4), 620-640.

[15] Lazarus, S. (2026). *Cybercriminals (yahoo boys) and society: Hustle kingdoms, occult economies, and the colonial politics of digital fraud*. Taylor & Francis.

[16] Luong, H. T., Kraus, F., Nožina, M., & Silverstone, D. (2026). Vietnamese Organised Crime Overseas: The International Dimension of the Problem. In *Vietnamese Organized Crime in its International Dimension* (pp. 1-15). Routledge.

[17] Gately, H. (2023). *Russian organised crime and Ransomware as a Service: state cultivated cybercrime* (Doctoral dissertation, Macquarie University).

[18] Housley, W., Fitzgerald, R., Beneito-Montagut, R., & Edwards, A. (2022). The SAGE handbook of digital society.

[19] Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2024). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, *27*(3), 364-387.

[20]Okoli, A. C., & Nwangwu, C. (2023). Organized crime–terror nexus: Interrogating the linkage between banditry and terrorism in Northern Nigeria. *Journal of Asian and African Studies*, *58*(5), 766-778.

[21]Lord, N., & Levi, M. (2023). Economic crime, economic criminology, and serious crimes for economic gain: On the conceptual and disciplinary (dis) order of the object of study. *Journal of Economic Criminology*, *1*, 100014.

[22]PAVLIDIS, G. (2026). Twenty years of Europol strategic analysis and the harmonisation of EU criminal justice: A meta-analysis. *Open Research Europe*, *6*, 279.

[23]Andreasson, J., & Henning, A. (2023). *Online doping: The digital ecosystem and cyborgification of drug cultures*. Springer Nature.

[24]Lusthaus, J. (2024). Reconsidering crime and technology: What is this thing we call cybercrime?. *Annual Review of Law and Social Science*, *20*(1), 369-385.

[25]Leese, M. (2023). Enacting criminal futures: data practices and crime prevention. *Policing and Society*, *33*(3), 333-347.

[26]Forberg, P., & Schilt, K. (2023). What is ethnographic about digital ethnography? A sociological perspective. *Frontiers in Sociology*, *8*, 1156776.

