International Entrepreneurship and Management Journal (2026) 22:86
https://doi.org/10.1007/s11365-026-01212-x

Ecosystem-based framework for organized cybercrime

Pejvak Oghazi[1,2,3] · **Arash Kordestani**[1,3] · **Rana Mostaghel**[1,3]

Accepted: 10 March 2026 / Published online: 20 April 2026

Abstract

The increasing complexity of organized cybercrime, fueled by rapid technological advancements and global interconnectedness, challenges traditional criminological theories and fragmented policy responses. This study conducts a comprehensive literature review using both systematic and snowballing methods across two databases. From a review of 92 articles, the study identifies: (1) major journal publications in organized cybercrime, (2) major theoretical foundations employed by academic research in organized cybercrime, and (3) significant gaps in current theoretical frameworks and practical interventions, particularly concerning informal governance structures, ideological cohesion, and technological enablers that sustain cybercriminal ecosystems. The study proposes (4) an organized cybercrime ecosystem framework, drawing on criminology, institutional theory, technology adoption models, and socio-technical perspectives, and (5) targeted intervention strategies to disrupt the operational logic of organized cybercrime. Theoretical and managerial implications, along with important limitations and avenues for future empirical research, are discussed at the end of the paper.

Keywords Organized cybercrime · Ecosystem · Intervention strategies · Conceptual framework · Theory · Systematic literature review

✉ Pejvak Oghazi
Pejvak.oghazi@sh.se

Arash Kordestani
arash.kordestani@sh.se

Rana Mostaghel
rana.mostaghel@sbs.su.se

[1] School of Social Sciences, Södertörn University, Stockholm, Sweden

[2] School of Management, University of Vaasa, PO Box 700, Vaasa FI-65101, Finland

[3] University of Economics and Human Sciences, Warsaw, Poland

Introduction

The rise of complex and transnational cybercrime has intensified in recent years, with significant implications for national sovereignty, economic stability, and global security. According to Symantec's, 2024 report, ransomware operations (i.e., a sort of cybercrime) remained highly resilient despite intensified law enforcement actions (Symantec, 2024). Attacks escalated in late 2023, with incidents almost doubling in September and October compared to the previous year. Ransomware attacks increased from 2,859 in 2022 to 4,713 in 2023 and 4,873 in 2024, representing a 70% rise over the two-year period (Symantec, 2024). Similarly, the FBI's Internet Crime Complaint Center (IC3) reported 880,418 cybercrime complaints in 2023, representing a 10% increase from 2022 and resulting in financial losses exceeding $12.5 billion. Among the most financially damaging schemes were business email compromise and investment fraud, with cryptocurrency related scams alone accounting for over $3.96 billion (Federal Bureau of Investigation Internet Crime Complaint Center [IC3], 2024). Similarly, the National Institute of Standards and Technology (2020) estimated that cybercrime in the U.S. caused economic losses of up to $770 billion in 2016, equivalent to 4.1% of GDP with a considerable impact on the manufacturing sector.

These developments highlight an urgent need for conceptual frameworks that extend beyond technical or policy responses to explain how cybercriminal organizations emerge, establish trust, and adapt under conditions of anonymity and uncertainty (Lusthaus, 2013; Yip et al., 2013). While the Fourth Industrial Revolution has created technological conditions that enable cybercrime with increased connectivity, data centralization, and AI-driven tools (Whelan et al., 2024), questions remain about the organizational nature of cybercrime and the factors that allow it to evolve into complex, flexible networks (Lusthaus, 2013; Lavorgna, 2015).

Transnational organized crime has historically evolved in tandem with broader shifts in globalization, immigration, and advancements in communication technologies (Finckenauer, 2005). These breakthroughs have made controlling communications more challenging, giving rise to new forms of cybercrime (Finckenauer, 2005; Di Nicola, 2022). Organized cybercrime now extends beyond profit-seeking behavior, encompassing ideological, conspiratorial, and networked motivations that challenge existing criminological paradigms (Paquet-Clouston et al., 2018; Lavorgna, 2019; Di Nicola, 2022; Childs, 2023). As Di Nicola (2022) notes, the boundaries between digital and physical criminal environments have blurred, exposing gaps in existing frameworks that fail to fully reflect the hybrid nature of modern illicit activity.

However, many official efforts to address organized cybercrime continue to rely on conventional assumptions about hierarchy, centralization, or purely economic motives. For example, the Organization for Security and Co-operation in Europe (OSCE) identifies cybercrime as one of its top five security threats. Still, it primarily emphasizes cooperation, training, and legal harmonization as key tools (Lyzhenkov, 2018). These approaches, while valuable, may overlook how cybercriminal networks structure relationships and how broader societal and systemic forces shape these evolving ecosystems. Experimental evidence shows that social norms materi-

ally shape the impact of economic deterrents. When fraud is socially condemned, fines have stronger compliance effects, whereas enforcement-only strategies tend to be costly and insufficient (Cahyonowati et al., 2022). In this study, we define the term "ecosystem" as a complex, adaptive system of actors and technologies, drawing on its origins in biology and business studies (Stam & van de Ven, 2021; Moore, 2006). We use the term in an analytical (not merely metaphorical) sense to highlight interdependence and feedback effects, explaining how changes in platforms, enforcement, and security practices reshape incentives and coordination across the system over time. In the context of organized cybercrime, this ecosystem includes not only the economic actors and their interdependencies but also the technological infrastructures, governance gaps, and ideological drivers that enable criminal activities to flourish. By conceptualizing organized cybercrime as an ecosystem, we aim to move beyond linear or hierarchical models of criminal organization to capture the dynamic interactions and adaptive structures that sustain these illicit networks. This lens provides analytical leverage beyond static factor lists by explaining persistence and adaptation, including displacement and reconfiguration following interventions, rather than only describing drivers.

The literature on organized cybercrime is dispersed, and several research gaps can be identified. First, Di Nicola's (2022) theory of digital organized crime and Agrawal et al.'s (2022) critique of legal informatics both point to the inadequacy of existing legal and theoretical models. A holistic overview of organized cybercrime ecosystem remains limited in the current literature. Second, the necessary relationships for cybercriminal networks are not clearly identified in academic research (Paquet-Clouston et al., 2018). Yet, identifying these relationships is essential for disrupting the organized cybercrime ecosystem. Third, while academic research has identified organized cybercrime drivers, there are additional factors that have remained underexplored (Finckenauer, 2005; Lavorgna, 2019). Thus, the purpose of this study is threefold. First, it conceptualizes organized cybercrime as a complex ecosystem. Second, it explores how relationships are structured within the organized cybercrime ecosystems. Third, it examines how broader societal and systemic factors influence the organized cybercrime ecosystem. Drawing on a multidisciplinary framework, this study not only applies but also integrates theoretical perspectives, including transaction cost economics, institutional theory, conspiracy thinking, social network theory, and the securitization approach, to propose a hybrid and contextual approach to understanding and disrupting cybercrime networks.

Prior studies show that online criminal forums and illicit marketplaces rely on informal governance mechanisms to structure cooperation, reduce uncertainty, and build trust among otherwise anonymous participants. Yip et al. (2013) demonstrate that carding forums employ vendor review systems, escrow mechanisms, and hierarchical oversight to lower transaction risks. Similarly, Lusthaus et al. (2023) describe how the Gozi network balanced firm like internalization with market flexibility to sustain operations under high uncertainty. Yet, these studies remain case-specific and do not explain how such relational structures function more broadly across different cybercrime ecosystems. Moreover, Paquet-Clouston et al. (2018) highlight the passive role of law enforcement in these systems, but their analysis does not explore the relational architecture itself. This gap raises fundamental questions about how

relationships are organized, sustained, and scaled in cybercriminal environments. Accordingly, this study formulates the first research question as:

How do cybercriminal networks structure relationships within organized cybercrime ecosystems?

Research indicates that organized cybercrime cannot be understood in isolation from broader societal and systemic conditions. For instance, Finckenauer (2005) traces how globalization and technological innovation transformed organized crime, while Holt et al. (2018) show that political systems and democratic freedoms can inadvertently increase exposure to malware infections. Bui and Lee (2022) demonstrate how socialist and Western states adopt contrasting cybersecurity regimes, reflecting ideological and institutional differences, and cross-country evidence links governance quality to the size of illicit financial outflows. Stronger regulatory quality is associated with lower outflows, while corruption and weak government effectiveness increase them (Abotsi, 2018). Shad (2019) finds that the absence of securitization in Pakistan limits state-level responses. Di Nicola (2022) further argues that the digital and physical criminal worlds are increasingly intertwined, shaped by sociopolitical and institutional asymmetries. Despite these insights, the literature lacks a systematic account of how such societal and systemic drivers collectively influence the development and resilience of organized cybercrime ecosystems. To address this gap, the study formulates the second research question as:

What societal and systemic factors shape the organized cybercrime ecosystem?

While criminological theories such as Routine Activity Theory (Cohen & Felson, 1979; Yar, 2005) and Differential Association Theory (Sutherland et al., 1992; Dearden & Parti, 2021) explain offender behavior and learning processes, they provide only partial insights into cybercrime ecosystems. Economic perspectives such as Transaction Cost Economics (Williamson, 1991; Yip et al., 2013) and relational contracting (Walsh,2007) highlight governance under uncertainty but overlook ideological and sociopolitical dimensions. At the same time, conspiracy frameworks (Lavorgna, 2019; Childs, 2023) and securitization approaches (Buzan & Hansen, 2009; Shad,2019) emphasize narratives and state responses but neglect organizational structures and technological infrastructures. This fragmentation underscores the need for interdisciplinary integration that captures the relational, institutional, technological, and ideological dimensions of organized cybercrime. Therefore, this study formulates the third research question as:

How can interdisciplinary frameworks help explain and respond to the complexity of cybercrime ecosystems?

Taken together, these questions motivate an ecosystem perspective because they link micro-level relationship structuring, meso-level governance and infrastructures, and macro-level societal and institutional conditions into a single dynamic explanation of persistence and change.

Research method

This conceptual paper on organized cybercrime employs a comprehensive literature review, integrating both snowballing and systematic approaches to develop a thorough understanding of the subject. The research commenced with advanced keyword searches focusing on "organized cybercrime" to identify relevant initial literature. The first phase was a theory-driven forward-backward snowballing on Scopus database conducted between November 2024 and January 2025. To ensure a comprehensive search, the following search string was utilized: (organized OR organised) AND (cybercrime OR "cyber crime" OR "internet crime"). This search was conducted in the Scopus database to retrieve pertinent studies. Subsequently, a snowballing method was utilized, involving both backward and forward processes. Backward snowballing entailed reviewing the reference lists of selected papers to discover prior pertinent studies, while forward snowballing involved examining subsequent publications that have cited these key papers (Webster & Watson, 2002; Jalali & Wohlin, 2012). This phase identified 39 articles, of which 36 were retained as relevant and used in the review. This dual approach is recognized for its effectiveness in systematic literature reviews, as it helps to uncover a comprehensive set of relevant studies. Seven of the 36 snowballing retained papers later reappeared in the Systematic Literature Review (SLR) (see below), yielding 29 unique snowballed articles.

The second phase was an SLR conducted on ProQuest between February and the end of May 2025 to identify and synthesize scholarly research on organized cybercrime. The review was conducted using ProQuest, which aggregates content from major research databases. The review process followed four stages.

Stage 1) Initial search: An advanced search query was developed to identify relevant studies, using:

(abstract(organized OR organised) AND abstract(cybercrime OR (cyber crime) OR (internet crime))) AND (at.exact("Article" OR "Case Study") AND la.exact("ENG") AND PEER(yes)).

The focus was on articles mentioning organized or organised cybercrime and related terms within the abstract. Filters were applied to restrict results to peer-reviewed journal articles and case studies published in English. This search resulted in 170 articles.

Stage 2) Removal of duplicates: duplicate records across databases were identified and removed, reducing the number of articles to 130.

Stage 3) Title screening: titles and abstracts were screened to exclude studies that did not specifically address organized cybercrime. Following this stage, 92 articles remained.

Stage 4) Data extraction: the remaining 92 articles underwent a full text review in which bibliographic information, citation contexts, study purposes, theories, data collection and analysis techniques, and major findings were extracted. During this stage, we created a structured template to ensure consistency across the reviewed papers. For each article, the following measurement items were

collected: (1) bibliographic information, (2) number of citations, (3) journal of publication, (4) stated purpose of the study, (5) theoretical frameworks applied, (6) data gathering methods, (7) data analysis techniques, (8) major findings, and (9) the article abstract. These items served as the coding basis for our synthesis, allowing us to compare theoretical approaches, methodological choices, and empirical insights across the selected studies. Figure 1 depicts these stages. It should be noted that, while the search string is relatively generic, this was an intentional choice to ensure that relevant research was not prematurely excluded. Therefore, this review is best seen as an exploratory mapping of the field, identifying key trends, conceptual gaps, and future research directions, rather than a fully comprehensive review.

Literature review on organized cybercrime

Organized cybercrime covers a wide selection of illicit activities facilitated by digital technologies. While a comprehensive examination of all forms is beyond the scope of this section, several common types illustrate the diverse strategies employed by cybercriminals and the corresponding challenges for security and governance. These include ransomware attacks (Symantec, 2025), cyber fraud (Gilmour,2019), manipulation of collective behavior through digital platforms (Chowdhury & Ramadas, 2022), threats to Internet of Things (IoT) technologies (Aly et al., 2019) and transport systems (Tonn et al., 2019), as well as forms of exploitation such as sextortion and sex trafficking (Ray & Henry, 2024).

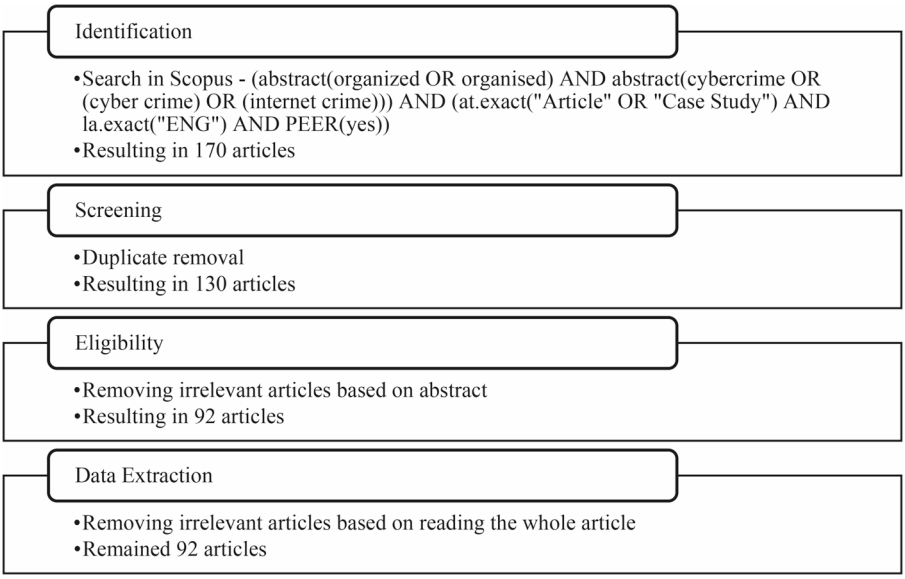

Fig. 1 Stages in systematic literature review

Ransomware has been ranked among the highest cyber threats by the United Kingdom's National Cyber Strategy and Europol's European Cybercrime Centre (Whelan et al., 2024) and is among the most common attacks orchestrated by organized cybercriminals. DarkSide's attack on the Colonial Pipeline (Russon, 2021, as cited in Whelan et al., 2024) and REvil's attack on JBS Foods (DiMaggio, 2022, as cited in Whelan et al., 2024) are notable examples of high-profile ransomware incidents. The attack on Colonial Pipeline severely disrupted fuel supplies across the United States, leading to temporary shortages and a spike in prices. To regain access to their systems, Colonial Pipeline paid a ransom of $4.4 million. Similarly, the ransomware attack on JBS Foods, one of the world's largest meat suppliers, caused significant disruption to the food supply chain and operations in Australia, Canada, and the United States. JBS ultimately paid $11 million to regain control of their systems and resume operations. Although some scholars (Lusthaus, 2013; Leukfeldt et al., 2017; Lavorgna, 2019) argue that cybercrimes are not committed by organized criminal groups, Whelan et al. (2024) contend that ransomware should be classified as organized crime when a current, adaptable framework is applied.

Fraud has evolved into one of the most prevalent types of cybercrime, including organized cross-border and international crime (Gilmour, 2019). Additionally, *hive minds* are another branch of cybercrime that is rooted in the manipulation and exploitation of collective behavior, particularly through social media and digital networks (Chowdhury & Ramadas, 2022). For instance, herd mentality, driven by robotics-based swarm intelligence and social media-based virtual reality games, can lead to new forms of control over individuals' free will and to more complex, organized cybercrimes (Chowdhury & Ramadas, 2022). Chowdhury and Ramadas highlight the importance of investigating cyber bioterrorism and the role of alternate reality games related to the spread of the SARS-CoV-2 virus. They argue for the development of laws and regulations to prevent ideology-driven manipulation, especially when alternate reality narratives merge with technological environments. Operation Tovar is a successful international collaboration in tackling cybercrime. This operation targeted the Gameover ZeuS botnet, a sophisticated network used for banking fraud and ransomware distribution. Law enforcement agencies from multiple countries, led by the US Department of Justice and the FBI, worked together to dismantle the botnet (Cartwright et al., 2019). The joint effort resulted in the disruption of the network and the prosecution of key individuals involved. Yet these successes are rare and highlight the complexity of dismantling distributed cybercriminal infrastructure.

De Liso and Zamparini (2022) reviewed the impact of transport security innovations on global supply chains, emphasizing how threats from organized crime and the need for cybersecurity have driven these advancements. They highlighted the importance of coordinated efforts among stakeholders to manage security challenges effectively while considering the tradeoffs between strict security measures and their effects on supply chain efficiency and costs. Another type of organized cybercrime targets the Internet of Things (IoT). These technologies often rely on multi-layered

services to enable interoperability between different IoT devices (Aly et al., 2019). However, these architectures are susceptible to a range of threats, including unauthorized access, malicious code, denial of service attacks, data breaches, privacy violations, service abuse, data security issues, and authorization problems. These vulnerabilities are often difficult to manage with conventional tools.

Other forms of organized cybercrime, such as sextortion and sex trafficking, highlight the human cost and the role of digital platforms in enabling coercion. Sextortion disproportionately affects youth and often occurs within peer relationships, yet it is severely underreported due to shame and fear (Ray & Henry, 2024). Similarly, sex trafficking has become more accessible through cyberspace, with offenders using encrypted platforms to facilitate recruitment, communication, and financial transactions. This lowers the barriers to entry and enables smaller offender groups to operate (Greiman & Bain, 2013). While technology also aids investigations, research suggests that advancing law enforcement capabilities is more effective than merely increasing traditional penalties (Raets & Janssens, 2021).

Table 1 provides definitions of the major concepts in this research. Because the extant literature is inconsistent in its terminology (Phillips et al., 2022; Whelan et al., 2024), we selected definitions that are most suitable for this study.

Table 1 Definitions

Concept	Definition	Reference
Cybercrime	"A broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target."	(European Commission, 2013, p. 3)
Organized Cybercrime	"Organized cybercrime refers to cybercriminal activities or groups that meet the defining features of organized crime. This means their operations and internal structures align with modern conceptions of organized crime, and they actively attempt to exert illicit governance, whether in physical spaces, digital environments, or both."	(Whelan et al., 2024)
Ransomware	"Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion. Ransomware is frequently delivered through spear-phishing emails. After the user has been locked out of the data or system, the cyber actor demands a ransom payment."	(United States Government Interagency Guidance Document, 2016, p. 2)
Cyber fraud	"Cyber frauds (also referred to as cyber scams) are any type of fraud that exploits mass communication technologies (e.g., email, Instant Messenger, social networking sites) to trick people out of money."	(Whitty, 2019, p. 277)
Ideological cyberattacks	"Cyberattacks by ideologically motivated offenders to cause harm and further their political and social agendas."	(Holt et al., 2017, p. 212)
Cybersex trafficking	Cybersex trafficking involves "non-consensual sexual acts conducted through technology-mediated environments, typically via live-streamed webcam sessions that may also be recorded and distributed. This form of trafficking is inherently criminal and characterized by coercion, manipulation, abuse, entrapment, and often extortion, disproportionately affecting vulnerable populations."	(Flanagan, 2022, abstract)

Descriptive statistics results

The systematic literature review of 92 articles reflects disciplinary and theoretical fragmentation. Journals that publish most frequently on organized cybercrime span criminology, security studies, financial regulation, and digital warfare, indicating broad concern but limited consolidation (see Fig. 2). *Crime, Law and Social Change* and *Global Crime* stand out with the highest number of contributions, each publishing five articles. Ranking next are *Trends in Organized Crime*, the *European Journal on Criminal Policy and Research*, and the *Journal of Information Warfare*, each contributing three papers. These journals reflect both the criminal justice perspective and the growing concern with cyber operations and warfare. Several other journals, including *Russian Education and Society*, *Studies in Conflict and Terrorism*, *Security and Human Rights*, *PLoS ONE*, *Journal of Financial Crime*, and *Journal of Money Laundering Control*, have each published two articles on the topic, underscoring the relevance of organized cybercrime across fields ranging from global security to education and financial integrity.

Citation data reveals a mix of conceptual, technical, and empirically grounded works. Among the most cited works on organized cybercrime, Broadhurst (2006) stands out with 332 citations (citation counts reported as of May 2025), providing a general review of international responses to the rapid expansion of computer crime. The study emphasizes that cybercrime frequently mirrors traditional forms of criminality, such as fraud, while introducing new challenges for global enforcement. Abdul-Ghani et al. (2018), with 267 citations, propose a four-layered IoT security reference architecture, taking a literature-based approach to address the vulnerabilities that make cyber infrastructures susceptible to organized cyber threats. Yar (2012), a conceptual and widely cited paper with 232 citations, critically explores the ontological and criminological challenges in defining and understanding cybercrime, particularly in its organized forms. Leukfeldt and Yar (2016), with 175 citations, base their analysis on 18 police investigation files and show that, although cybercriminal networks exhibit signs of structural organization, they often rely

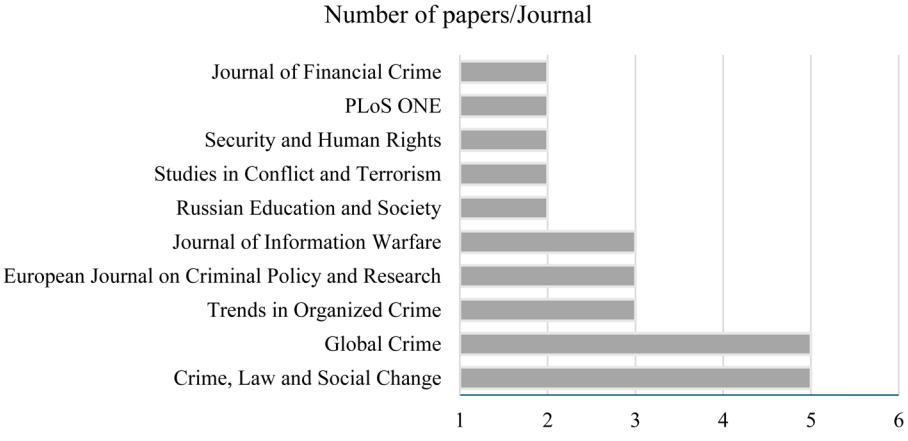

Fig. 2 Top 10 journals with the highest number of publications (counts retrieved May 2025)

on temporary and loosely connected collaborations. In addition, Yip et al. (2013) analyze actual conversations from cybercriminal forums, revealing how carding communities facilitate the functioning and maintenance of organized cybercrime structures. Other influential themes that continue to shape the scholarly debate on cybercrime include the transformation of traditional organized crime groups into fully fledged cybercriminal networks (McCusker, 2006), the question of whether cybercrime is organized (Lusthaus, 2013), the reasons why cybercrime takes place (Frank & Odunayo, 2013), internet exploitation by organized cybercrime groups (Lavorgna,2015), and the wide spectrum of cybercrimes (Lin, 2012). Figure 3 illustrates the ten most cited articles.

A review of the theoretical frameworks applied in studies on organized cybercrime reveals a diverse and multidisciplinary landscape, reflecting the complexity of the phenomenon (see Table 2). The most frequently used theory is Transaction Cost Economics (4 occurrences), which emphasizes the costs of exchanges and governance structures in illicit online environments. Securitization approach and Routine Activity Theory each appeared twice, highlighting the role of perceived threats and the convergence of motivated offenders, suitable targets, and the absence of capable guardians in cyberspace. Several studies also employed criminological perspectives, such as Conspiracy Thinking, Differential Association Theory, Deterrence Theory, and Strain Theory, alongside more sociologically grounded models, including moral panic theory, Social Learning and Peer Influence, and Chicago School Theory. Interestingly, some studies adopted more contemporary lenses, Actor Network Theory, Network Society Theory, and Technological Self-Efficacy Theory, which focus on the interplay between technology, actors, and social structure. The use of Institutional Theory, Instrumental Theories of Compliance, and Rational Choice Theory further reflects the integration of organizational and deci-

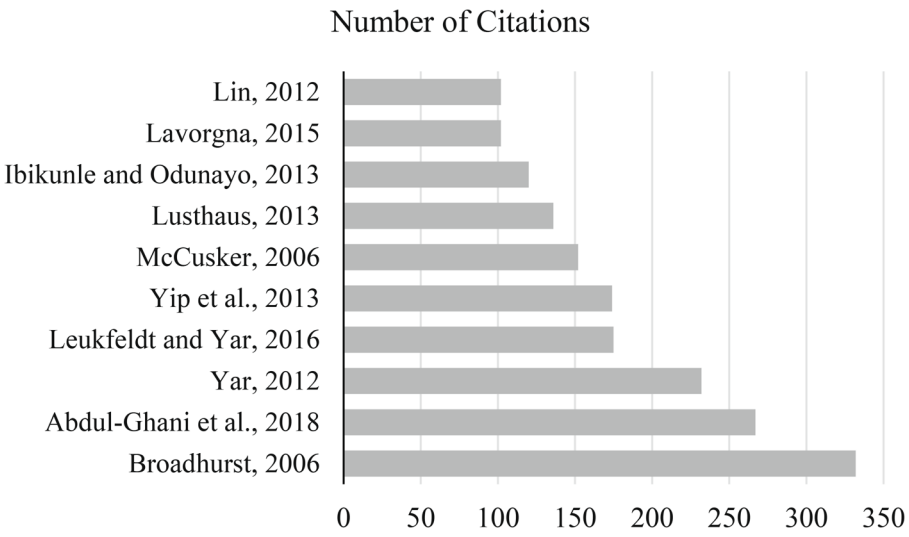

Fig. 3 Top 10 most cited articles (counts retrieved May 2025)

Table 2 Theoretical framework of the papers

Number of articles	Frameworks
65	No specific theory
4	Transaction Cost Economics
2	Securitization Approach
2	Routine Activity Theory (RAT)
2	Conspiracy Thinking
2	Institutional Theory
1	Situational Crime Prevention
1	Differential Association Theory
1	Moral Panic
1	Merged Actor-Network Theory & Social Network Theory
1	Deterrence Theory
1	Instrumental Theories of Compliance
1	Sutherland's Theory of Behavior Systems in Crime
1	Strain Theory
1	Actor Network Theory
1	Technological Self-Efficacy
1	Network Society
1	Social Network Theory
1	Social Learning and Peer Influence
1	Restrictive Deterrence
1	Rational Choice Theory
1	Cressey's Criminal Organization
1	Mary McIntosh's The Organization of Crime
1	Chicago School Theory[†,††]

There are some articles with several theoretical frameworks

[†]By "Chicago School," we refer to the early urban ecology & social disorganization tradition in sociology and criminology associated with the University of Chicago, especially Park & Burgess's The City (University of Chicago Press, 1967). *Cited in Chen, A. (2005). Secret societies and organized crime in contemporary China. Modern Asian Studies, 39(1), 77–107*

[††]Shaw & McKay's Juvenile Delinquency and Urban Areas (University of Chicago Press, 1969)

sion-making perspectives in understanding the strategic behavior of cybercriminal networks. It should be noted, however, that 65 papers in the dataset lack any explicit theoretical foundation, indicating that a sizable portion of the literature is still largely descriptive or empirically driven. This absence limits explanatory depth, particularly when addressing coordination, trust, or adaptation within cybercriminal networks.

The literature offers rich descriptions and introduces multiple theoretical perspectives, but it lacks an integrated framework that can account for governance structures, ideological cohesion, and institutional asymmetries within digital criminal ecosystems. Themes such as informal trust mechanisms, regulatory gaps, and the symbolic or conspiratorial dimensions of cybercrime are examined in isolation but rarely synthesized. This diversity of frameworks reinforces the fragmented nature of theorizing in the field and points to the need for a synthesized, ecosystem-oriented approach. This study addresses that gap by conceptualizing organized cybercrime as a dynamic ecosystem and proposing a hybrid theoretical model that integrates governance, network logic, and sociopolitical framing.

Unresolved policy and governance challenges in combating organized cybercrime

Earlier studies have identified theoretical shortcomings; however, many practical and governance challenges remain unresolved and continue to complicate efforts to counter organized cybercrime. Current approaches struggle to keep pace with the speed of technological innovation and the transnational nature of cybercriminal operations. Legal systems are constrained by jurisdictional boundaries, regulatory bodies face coordination challenges, and law enforcement agencies often lack the technological capabilities required to effectively disrupt cybercriminal ecosystems. This section critically examines these practical and institutional limitations, highlighting the need for solutions that are not only technically effective but also informed by a deeper understanding of how cybercrime operates across policy, governance, and technological domains.

Cyberspace challenges traditional notions of jurisdiction, sovereignty, and state boundaries. Existing debates question how political concepts originally rooted in the physical world apply to the borderless nature of the internet and cyber warfare (Chatinakrob, 2024). These disagreements stem from both the complexity of global digital networks and the evolving definitions of sovereignty and governance. The metaphors and language used to describe cyberspace further shape how these issues are framed, influencing both policy and enforcement responses.

Cybercrimes entail direct, indirect, and prevention costs for states and organizations (Matsaung & Masiloane, 2024). In South Africa, defensive expenditures include significant investments in firewalls, antivirus programs, and other cybersecurity technologies. In Latin America and the Caribbean (LAC), cybersecurity investments have grown by 8% annually since the COVID-19 pandemic. However, ransomware attack costs have surged to an estimated $15 million, with incidents increasing by 200%. This suggests that rising expenditures are not yet translating into effective deterrence (Kosevich, 2023).

At the policy level, international conventions such as the United Nations Convention against Transnational Organized Crime have proposed stronger legislative measures to combat organized cybercrime (Apenov et al., 2021). However, enforcement gaps remain. Using Kazakhstan as a case study, Apenov et al. (2021) highlight that legal frameworks often lack effective mechanisms for implementation despite formal agreements. Fragmented and inconsistent regulatory systems further hinder efforts to combat cybercrime, as criminal actors exploit jurisdictional loopholes and the slow harmonization of cross-border legal processes (Broadhurst, 2006; Doig, 2018; Mugarura & Ssali, 2021).

These challenges are compounded by emerging technologies, which introduce new complexities for law enforcement. As Whelan et al. (2024) emphasize, understanding the internal dynamics of ransomware groups, including their governance structures, conflict resolution methods, and financial management practices, is critical for effective intervention. Di Nicola (2022) critiques existing cyber criminology frameworks for failing to address the organizational sophistication of digital criminal enterprises. He advocates developing new criminological theories that explain the causes of digital organized crime, explore its relationship with Industry 4.0 technolo-

gies, and foster interdisciplinary dialogue between criminology, information technology, and policy research.

Although these studies identify critical challenges (see Table 3), they often lack integrated theoretical frameworks that explain how organized cybercrime networks sustain themselves in fragmented regulatory environments and rapidly evolving technological landscapes. Addressing these gaps requires not only practical solutions but also conceptual models capable of capturing the complex interplay between technology, informal governance structures, ideological cohesion, and institutional gaps. The following section explores existing solutions and evaluates their effectiveness in addressing these multifaceted challenges.

These persistent governance and enforcement limitations highlight the need for a comprehensive conceptual framework capable of addressing the systemic complexity of organized cybercrime. The following section explores this in greater detail.

Theories and approaches

Understanding organized cybercrime requires a multidisciplinary theoretical foundation that accounts for its complex, adaptive, and decentralized nature. Existing theories offer valuable but partial insights into how cybercriminal networks establish trust, sustain cooperation, and evolve in environments characterized by high uncertainty and limited formal governance (Yar, (Yar 2005) ; Leukfeldt & Yar, (Leukfeldt and Yar 2016)). Classical criminological approaches, such as Routine Activity Theory (RAT) and Differential Association Theory (DAT), explain offender behavior, target selection, and the social learning processes in cybercriminal activity (Cohen &

Table 3 Challenges and limitations highlighting the need for a new conceptual framework

Core Challenge Area	Specific Limitation or Gap	Key References
Governance and Jurisdictional Gaps	Jurisdictional complexity; sovereignty concepts poorly applied to cyberspace.	Chatinakrob (2024)
	Law enforcement gaps despite international agreements.	Apenov et al. (2021)
	Fragmented and inconsistent regulatory systems.	Broadhurst (2006); Mugarura and Ssali (2021); Doig (2018)
Economic and Resource Constraints	High defensive costs with limited effectiveness.	Matsaung and Masiloane (2024)
	Ransomware surge despite increased cybersecurity investments.	Kosevich (2023)
Technological Complexity	Emerging technologies outpace policy and enforcement capabilities.	Whelan et al. (2024)
Theoretical and Conceptual Gaps	Existing theories are inadequate to explain digital organized crime.	Di Nicola (2022)
	Lack of interdisciplinary dialogue and new theory development.	Di Nicola (2022)
Implication for Research	Highlights the need for integrated theoretical frameworks to address the interplay of governance, economics, technology, and ideology in organized cybercrime ecosystems.	Current study

Felson, (Cohen and Felson 1979) ; Sutherland et al., 1992). However, these theories and approaches alone are insufficient to fully capture the organizational dynamics, governance structures, and ideological drivers of modern cybercrime ecosystems (Paquet-Clouston et al., (Paquet-Clouston et al. 2018) ; Di Nicola, 2022). To address these gaps, this study integrates perspectives from economic governance theories, including Transaction Cost Economics and relational contracting (Williamson, 1991; Walsh, 2007). It also incorporates technology adoption models and sociotechnical frameworks such as Actor-Network Theory and Social Network Theory (Callon, 1999; Haas, 2023). In addition, lay theories and approaches of conspiracy thinking, moral panic, and securitization help illuminate how ideological narratives and political structures shape both cybercriminal behavior and state-level responses (Lavorgna, 2019; Shad, 2019; Childs, 2023). Together, these theories and approaches provide the conceptual foundation to analyze organized cybercrime not only as a series of isolated criminal acts but as a dynamic and evolving ecosystem shaped by institutional gaps, digital infrastructures, and sociopolitical forces.

RAT, which is built upon three key elements of motivated offenders, a suitable target, and the absence of capable guardianship (Cohen & Felson, 1979), has been used extensively to explain the convergence of crime. Yar's (2005) study frames cybercrime as an ecosystem, structured by key elements adapted from RAT. In this ecosystem, predators (motivated offenders) include hackers, fraudsters, and cyberstalkers who seek out targets online. Prey (suitable targets) consists of personal data, financial information, and online services, all vulnerable to unauthorized access. Defenders (capable guardians) are both human, such as network administrators and vigilant users, and automated, such as firewalls and antivirus systems. Although it seems that cybercrimes can be analyzed using conventional criminology theories, there are significant differences between cybercrimes and traditional crimes. As Yar (2005) explains, the differences lie in the target's value, properties, exposability, and accessibility. In cyberspace: (i) value attaches to data, information, or asset; (ii) properties are often related to the services, making them weightless; (iii) exposability indicates the ease with which valuable properties can be found; and (iv) accessibility refers to the ease of access to the target. This online ecosystem mirrors the terrestrial crime environment, with dynamic interactions among offenders, targets, and guardians shaping cybercrime patterns. However, cyberspace is fundamentally different from the physical environment in that the distance between predators and prey is irrelevant (Leukfeldt & Yar, 2016). In relation to RQ1, RAT provides a baseline explanation of how networked offending becomes possible when targets and guardianship conditions align in the digital environment, while also clarifying the role of technological and institutional guardians, which may vary across contexts (RQ2).

Drawing on RAT, Holt et al. (2018) emphasized the role of technological infrastructure, political systems, attackers' strategies, and the challenges of detection and removal, alongside the function of Computer Emergency Response Teams (CERTs), in addressing malware infections. They observed that democratic nations, with their robust technological resources and greater political freedoms, are more likely to experience malware infections. However, these same factors – including higher numbers of web hosts and internet users – also make detection and mitigation efforts more challenging. But the presence of CERTs in these countries was found to have a mini-

mal impact on reducing infection rates or improving reporting processes in the fight against organized cybercrime. It is worth noting that applying existing cybercrime theories to the digital world poses significant challenges (Diamond & Bachmann, 2015). While RAT in its traditional form emphasizes the convergence of offenders and victims in the absence of capable guardians (Cohen & Felson, 1979), Yar, (2005) argues that the framework's core elements, motivated offenders, suitable targets, and the lack of guardianship, remain relevant and applicable in the virtual realm. This strengthens the RQ2 link by showing how national-level institutional capacity and infrastructural features condition guardianship effectiveness in practice.

DAT, also known as Sutherland's theory of behavior systems, argues that individuals learn criminal behavior through social interactions (Sutherland et al., 1992). Building on this foundation, Dearden and Parti (2021) explored the impact of both online and offline social learning on self-reported cybercrimes, using a national sample of 1,109 participants. Their findings revealed significant correlations between social learning and cybercrimes, with lower self-control further amplifying the likelihood of cyber offending when combined with social learning. Thus, these findings, highlight social learning and low self-control as key predictors of cybercrime, both independently and together. Expanding on this perspective, Paquet-Clouston et al. (2018) argued that cybercrimes emerge from the behaviors of all system actors, highlighting the passive role of law enforcement due to the lack of direct victims, the international nature of cybercrimes, and the high costs of investigations. For RQ1, DAT is particularly useful for explaining how participation, norms, and know-how circulate through social ties and online communities, which in turn shapes the relational structure and continuity of cybercriminal networks.

Integrating RAT and DAT provides valuable insights into organized cybercrime and offers strategies for prevention and enforcement. RAT suggests that cybercrimes occur when a motivated offender identifies a suitable target lacking adequate cybersecurity measures (Leukfeldt & Yar, 2016). For example, individuals engaging in online activities without proper safeguards might fall into phishing traps. DAT asserts that individuals learn criminal behaviors through interactions with others (Sutherland et al., 1992). In cyberspace, this can involve learning hacking techniques or engaging in cybercriminal activities through online communities that encourage such behaviors (Dearden & Parti, 2021). Considering the borderless nature of cybercrime, effective responses require coordinated efforts at governmental, national, and international levels (Alweqyan, 2024). Collaborative actions enhance the ability to detect, prevent, and respond to cybercrimes. Taken together, RAT and DAT serve as the criminological anchor for RQ1, but they leave open the question of how large-scale, repeated cooperation is governed under anonymity and high uncertainty. This issue is addressed by the governance-oriented lenses below.

In addition to explaining offender behavior and target selection, it is also important to consider how cybercriminal markets are structured to enable repeated, large-scale collaboration. Transaction Cost Economics (TCE) offers a useful framework by interpreting uncertainty as a transaction cost that actors aim to minimize through governance mechanisms (Williamson, 1991). Yip et al. (2013) apply this perspective to carding forums, which they describe as environments where participants face uncertainty about both the quality of goods being exchanged and the true identity of

those involved in transactions. To mitigate these risks, forums develop hybrid organizational structures that blend market features with hierarchical oversight. According to Yip et al. (2013), mechanisms such as vendor reviews, escrow services, and role-based trust hierarchies reduce the likelihood of opportunism and facilitate institution-based trust among anonymous participants. These structural features support initial trust formation and enable scalable and sustained criminal exchanges. As Yip et al. (2013) demonstrate, carding forums function as markets where transaction costs are actively managed to support illegal collaboration under high uncertainty. This directly advances RQ1 by specifying which governance mechanisms enable trust and cooperation when formal enforcement is absent.

Relational contracting and institutional theories provide additional insights into cooperation in high-risk environments such as organized cybercrime. Institutionalist work (e.g. Keohane, 2005) explains how cooperation can emerge under anarchy through shared norms, reciprocity and mutual monitoring, while transaction-cost economics shows how long-term, incomplete contracts and hierarchical governance structures can be designed to manage uncertainty, bilateral dependency and opportunism (Williamson, 1985, 1991). Walsh (2007) applies these concepts to international intelligence sharing, arguing that dominant states create hierarchical structures to reduce transaction costs and ensure compliance by offering oversight and selective material benefits. Although institutional theory assumes trust-based cooperation, relational contracting argues that trust is not always necessary when power and incentives can be structured to reduce opportunism. In the context of organized cybercrime, these theories offer insights into how informal, yet stable governance arrangements can emerge to establish sustained coordination despite anonymity and legal risk. This perspective is supported by Lusthaus et al. (2023), who examine the Gozi cybercriminal network and discuss how core functions such as malware development and administration were internalized to reduce transaction costs. Their findings illustrate how cybercriminal groups operate as hybrid organizations that strategically balance firm-like control and market flexibility. The study also highlights how these groups are shaped by broader institutional environments, including corruption, jurisdictional differences, and informal norms, which influence how such networks are structured and maintained. The contribution is twofold: these lenses extend RQ1 by explaining how cooperation is stabilized through hybrid market-firm designs, and they extend RQ2 by demonstrating how broader institutional environments, including corruption and jurisdictional variation, constrain and enable governance arrangements.

These perspectives demonstrate how cybercriminal networks sustain cooperation through hybrid structures, yet they lack a systematic account of how such relationships are organized within broader ecosystems; a gap addressed by this study in its first research question. Accordingly, in this study they are used narrowly and purposefully to clarify the governance micro-foundations of network relationships (RQ1), which are then assembled into an ecosystem-level explanation in RQ3.

Prior studies have largely applied adoption theories, including the technology acceptance model (TAM), innovation diffusion, and the Unified Theory of Acceptance and Use of Technology (UTAUT) to study financial technology solutions (Jafri et al., 2024). Given the importance of trust and security, prior studies have combined these factors into adoption theories. For instance, in the banking industry, various

models have been applied: cloud computing in Malaysia (TAM-Dual Process Theory Model), smartphone banking in South Korea (TAM), mobile banking in India (TAM-Social Response Theory-UTAUT), and Egypt (TAM with Service Dominant Logic) (see Jafri et al., 2024). While trust and security issues have been studied in the context of mobile and online banking in developing countries, limited research exists on digital-only banking (Saif et al., 2022) and cloud computing (Asadi et al., 2017). This research gap, along with the increasing occurrence of organized cybercrime, underscores the need for focused attention from the research community and a supervisory framework in fintech to address this issue (Jafri et al., 2024). Building interdisciplinary connections among criminology, cybersecurity, and technology adoption, Alqahtani and Braun (2021) explored how technology adoption constructs relate to cybersecurity compliance. They identified factors such as performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habits as significant drivers of users' intentions and behaviors toward cybersecurity compliance. These adoption-oriented perspectives are incorporated to illuminate a specific part of RQ2: how organizational and user-level adoption and compliance conditions shape systemic exposure or resilience. They also support RQ3 by linking criminological explanations to practical levers for prevention and response.

In response to cyberattacks, Hasani et al. (2023) proposed a framework integrating the Technology-Organization-Environment (TOE) framework, the Technology Acceptance Model (TAM), Diffusion of Innovations theory (DOI), and the Balanced Scorecard. Their study highlighted that the perceived usefulness and ease of use of cybersecurity technologies strongly influence SMEs' adoption in the UK, ultimately enhancing organizational performance. The role of forensic photography and advanced imaging techniques has been emphasized in the investigation and documentation of fraud (Gilmour, 2019). This type of organized cybercrime often demands complex digital and financial elements to capture detailed, accurate, and objective images that can be analyzed and used as evidence in court. Building on social network theory, Haas (2023) proposed a cybersecurity-based solution to identify and eliminate wildlife traffickers, with the aim of disrupting their organized illegal activities. Collectively, these studies are used to operationalize the response side of RQ3 by showing how sociotechnical and organizational frameworks translate into concrete investigative and prevention capabilities.

Similarly, Di Nicola (2022), drawing on Actor-Network Theory (Callon, 1999; Latour, 2005), emphasizes the interconnectedness of the digital and physical worlds. He argues that human and non-human actors are not disconnected but rather deeply intertwined. Di Nicola further asserts that the sociology of crime is crucial for understanding digital organized crime, as these crimes operate in both digital and offline environments. Consequently, he proposes the spectrum theory of digital organized crimes, conceptualizing criminal behavior as existing on a continuum that blends online and offline territories. This is particularly relevant for RQ3 because it supports the ecosystem premise that infrastructures, platforms, and human actors co-produce criminal opportunity and coordination, complementing the relational focus of RQ1 with a sociotechnical account of what participates in networked offending.

Conspiracy thinking and moral panic offer complementary perspectives for understanding the ideological dimensions and public narratives surrounding organized cybercrime. Rather than purely economic motivations, some cybercriminal networks operate within a framework shaped by distrust in government, opposition to perceived surveillance, and libertarian ideologies. Childs (2023), in his study of fake vaccine certificate distribution on the alt-tech platform Gab, highlights how anti-surveillance sentiment and conspiracy beliefs about global control and global tyranny shaped both the motivation and structure of this illicit community. These networks operated not only through transactional exchanges but were also bonded by a shared narrative of resistance, making ideological cohesion a critical component of their longevity. In parallel, Lavorgna (2019) examines how media and political actors construct organized cybercrime as a public threat through moral panic, exaggerating the organizational features of online offenders and invoking the language of organized crime to justify surveillance, policing powers, and policy responses. In both cases, organized cybercrime is not just a technical or financial phenomenon but also a socio-political one, shaped by shared belief systems and media-driven threats. Together, these perspectives expand the understanding of cybercriminal coordination beyond structure and strategy by highlighting the affective and rhetorical forces that legitimize and mobilize action within and around digital criminal communities. This section contributes to RQ2, showing how societal narratives and ideological alignment can act as a binding force within the ecosystem, sustaining communities over time and shaping both the intensity and form of external responses.

A nation's political structure significantly influences its approach to cybersecurity and its vulnerability to cyber threats. In socialist economies, the state often centralizes cybersecurity efforts, prioritizing ideological stability and regime security. This centralized approach can lead to challenges in bureaucratic efficiency and resource allocation. For instance, China's cybersecurity strategy emphasizes controlling information flow to preserve social harmony and political stability, utilizing extensive internet regulations and infrastructure such as the Great Firewall to monitor and restrict online content. This model of internet regulation is deeply integrated with China's specific technological and political context and may not be easily transferable to other nations lacking similar infrastructure (Bui & Lee, 2022). These institutional differences are included to address RQ2 by clarifying how governance models and political priorities condition both vulnerabilities and available countermeasures.

In contrast, Western nations typically perceive cybersecurity through the lens of technical threats, emphasizing the protection of data, privacy, and the integrity of information systems. This perspective leads to a focus on safeguarding individual rights and maintaining open internet access. However, greater online freedom and a larger number of potential targets can increase susceptibility to cyber threats. Research indicates that democratic governments often experience higher rates of active cyber infections due to extended attack lifespans and the hackers' opportunistic exploitation of these freedoms (Holt et al., 2018). This further supports RQ2 by linking macro-level political conditions to ecosystem exposure and guardianship capacity.

These differing approaches reflect broader ideological distinctions: socialist systems prioritize regime stability and ideological control, leading to stringent internet regulations and centralized oversight, while Western systems value individual freedoms and open access, implementing cybersecurity measures that balance security with personal privacy and freedom of expression. Consequently, each system faces unique challenges and vulnerabilities in managing cyber threats.

Building on the role of political systems in shaping cybersecurity approaches, the securitization approach (Buzan & Hansen, 2009) helps explain how governments define and prioritize cyber threats within national security discourse. According to Buzan and Hansen (2009), securitization involves framing a topic as an existential threat that demands exceptional political or legal measures. Shad (2019) applies this approach to Pakistan's cyber threat landscape, arguing that, despite growing digital vulnerability, Pakistan has not effectively securitized its exposure to threats from hacking, cybercrime, and cyberwarfare. Drawing on the work of Hansen and Nissenbaum (2009), Shad identifies three key modalities of cyber securitization: hypersecuritization, everyday security practices, and technification, which remain largely absent in Pakistan. As a result, cyber threats in the country are politicized but not elevated to the level of urgent national security concerns. This gap between recognition and response illustrates how the absence of securitization can hinder policy action and institutional readiness in the face of organized cybercrime. These insights indicate that institutional and political contexts decisively shape vulnerabilities and resilience in organized cybercrime, yet the combined impact of these societal and systemic factors remains underexplored, a gap that we explore in the second research question. Here, securitization is used specifically to support RQ2 by explaining variation in political prioritization and its influence on institutional readiness, rather than serving as an additional general-purpose theory of cybercrime.

Theoretical insights from criminology, economics, sociology, and political science collectively illustrate that organized cybercrime cannot be fully understood through isolated disciplinary lenses. Instead, it must be conceptualized as a dynamic ecosystem in which informal governance mechanisms, ideological cohesion, and technological infrastructure interact to sustain criminal activity amid anonymity and institutional gaps. While classical theories and approaches explain patterns of offender behavior and target selection, newer frameworks shed light on how cybercriminal networks build and maintain trust, adapt to evolving technological environments, and leverage ideological narratives to legitimize their actions. Each lens is retained here only to the extent that it advances one of the study's research questions: RQ1 (networked relationships and governance), RQ2 (societal and systemic shaping conditions), and RQ3 (interdisciplinary integration to explain and respond to ecosystem complexity). This integrated perspective provides a foundation for addressing the research questions posed in this study, offering a holistic understanding of how organized cybercrime emerges, evolves, and persists within increasingly complex ecosystems (see Table 4).

This fragmentation emphasizes the importance of an interdisciplinary synthesis that integrates criminological, economic, sociological, and political perspectives into a unified framework, which is the focus of the third research question. Building

Table 4 Strengths and weaknesses

Theory	Key Explanations	Limitations	This Study's Conceptual Focus
Routine Activity Theory (RAT)	Explains convergence of offenders and targets (Yar, 2005).	Ignores role of digital infrastructure and irrelevance of distance; underdeveloped concept of guardianship (Holt et al., 2018).	Expands guardianship to include digital infrastructures and CERTs; integrates ecosystem thinking to address borderless crime patterns.
Differential Association Theory (DAT)	Highlights social learning of criminal behaviors (Dearden & Parti, 2021.	Does not address network governance or community maintenance (Paquet-Clouston et al., 2018).	Explores how informal online communities facilitate sustained criminal behavior, using Social Network Theory.
Transaction Cost Economics (TCE)	Explains how uncertainty is managed in illegal markets (Yip et al., 2013).	Overemphasizes rationality; ignores bounded rationality and informal trust.	Adds relational and social dimensions of trust formation, beyond economic transactions.
Institutional Theory & Relational Contracting	Explains cooperation under risk through hierarchy or shared norms (Walsh, 2007).	Difficult to apply to decentralized cybercrime ecosystems (Lusthaus et al., 2023).	Frames cybercrime networks as hybrid organizations using flexible governance under uncertainty.
Conspiracy Thinking	Explains ideological cohesion and policy responses (Childs, 2023; Lavorgna,2019).	Focuses on ideology but overlooks organizational structures.	Highlights how ideological narratives both sustain criminal networks and shape state securitization.
Securitization Theory	Explains how cyber threats are framed in national discourse (Shad, 2019).	Discursive focus; securitization does not guarantee policy action.	Emphasizes the gap between securitization rhetoric and actual cybersecurity capacity.

on the identified strengths and limitations of existing theories and approaches, this study proposes a conceptually organized cybercrime ecosystem framework that integrates these perspectives to offer a more comprehensive understanding of organized cybercrime. Rather than viewing cybercrime through isolated theoretical lenses, the ecosystem model captures how diverse actors, trust-based relationships, enabling infrastructures, and ideological motivations interact dynamically to sustain criminal networks in digital environments. As a result, the framework consolidates the targeted contributions of RAT and DAT for RQ1, governance theories that bridge RQ1 and RQ2, and sociotechnical and narrative lenses that link RQ2 and RQ3 into a single explanatory structure designed for analytical coherence rather than theoretical completeness. This integrated framework is presented below through a structured analytical table and a conceptual figure.

Toward an integrated ecosystem framework for organized cybercrime

Table 5 outlines the key components of the organized cybercrime ecosystem, offering a structured view of the actors, their relationships, enabling conditions, and the resulting criminal outputs.

Figure 4 synthesizes the ecosystem model, illustrating the dynamic interactions among actors, governance structures, trust mechanisms, technological infrastruc-

Table 5 Conceptualizing the cybercrime ecosystem: actors, relationships, antecedents, and theoretical foundations

Ecosystem Component	Description	Examples	Theoretical Foundations
Cybercriminal Actors	Diverse networks or individuals that plan, execute, or facilitate cybercrime activities at various levels	Hackers, carding groups, malware developers, botnet operators	Routine Activity Theory (RAT), Social Network Theory
Trust and Cooperative Relationships	Informal or semi-structured mechanisms for coordination, trust-building, or enforcement among offenders	Escrow systems, vendor review systems, admin-enforced rules in forums	Transaction Cost Economics (TCE), Relational Contracting
Enabling Infrastructures	Technological platforms and tools that support criminal activity or reduce traceability	VPNs, anonymizing browsers, IoT vulnerabilities, blockchain-based markets	Technology Adoption Models, Actor-Network Theory
Institutional, Ideological, and Political Antecedents	Structural conditions that foster organized cybercrime by creating regulatory gaps or ideological motivation	Weak regulations, under-securitization of cybercrime, conspiratorial narratives, anti-surveillance ideology	Institutional Theory, Securitization Theory, Conspiracy Theory

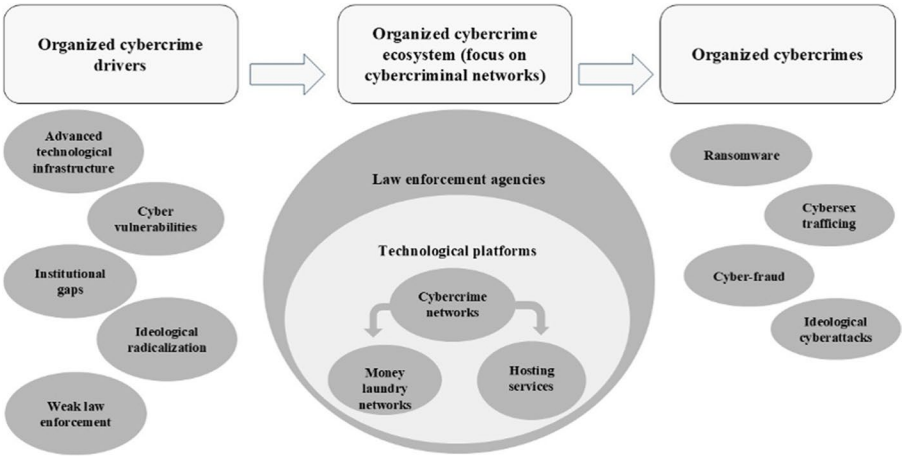

Fig. 4 Organized cybercrime as an evolving ecosystem

ture, and ideological drivers. This framework focuses on the initial steps, namely, the organized cybercrime drivers, the organized cybercrime ecosystem (with a focus on cybercriminal networks), and the organized cybercrimes. It does not investigate the victims and their disaster management and recovery phases. The aim of this research is to identify the drivers of organized cybercrime and to examine how cybercriminal networks take shape.

While the proposed ecosystem framework offers a conceptual understanding of how organized cybercrime operates, effectively addressing this phenomenon also requires targeted practical and policy interventions. The following section reviews existing responses and identifies areas for further development.

Discussion

Although various technological, policy, and law enforcement solutions have been proposed to combat organized cybercrime, these efforts often remain fragmented and fail to address the complex interdependencies between governance, technology, and ideology. Technological solutions primarily focus on securing digital infrastructures, while policy frameworks emphasize regulatory harmonization and transnational cooperation. However, few approaches fully consider how trust, cooperation, and governance emerge within decentralized ecosystems or how ideological narratives and institutional gaps shape cybercriminal networks. This section reviews existing solutions, organized around the key thematic challenges identified in this study, and assesses their effectiveness in addressing the governance, institutional, and ideological dimensions of organized cybercrime. It also outlines the theoretical contributions and implications for practice, demonstrating how an ecosystem perspective adds value beyond existing approaches.

To begin with, technological and infrastructural solutions have expanded rapidly, particularly in relation to IOT and cloud-based environments. Advances in machine learning (ML) and deep learning (DL) have introduced a range of tools to mitigate threats to IoT and cloud-based technologies. These include intrusion detection systems, cryptographic techniques, privacy-preserving models, blockchain applications, and hypervisor-based protections (Aly et al., 2019). Blockchain technology has been promoted for its potential to strengthen trust in digital environments through immutability, transparency, and decentralization (Jafri et al.,2024). However, these technologies also introduce new vulnerabilities, such as the misuse of ML models, blockchain transparency that creates privacy risks, and the challenges of securing multi-layered IoT environments. Despite these innovations, solutions remain focused on defending infrastructure rather than addressing the broader governance and trust mechanisms that sustain cybercriminal ecosystems. Concepts such as Computer Emergency Response Teams (CERTs) have been introduced to strengthen collective guardianship (Holt et al., 2018), yet their effectiveness is limited by fragmented institutional support and inconsistent international coordination.

Beyond technical defenses, governance and institutional responses remain central, particularly given the cross-border character of cybercrime. National and international regulatory frameworks continue to face challenges in managing the cross-border nature of cybercrime. Efforts at legal harmonization, such as the UN Convention against Transnational Organized Crime and mutual legal assistance treaties, have aimed to strengthen international cooperation (Broadhurst, 2006; Clough, 2015). However, practical enforcement remains inconsistent due to jurisdictional complexities, varying national capabilities, and bureaucratic inefficiencies (Doig, 2018; Mugarura & Ssali, 2021). At the institutional level, organizations such as Europol and the OECD play a critical role in facilitating information exchange and developing policy guidelines (Al Azzam, 2019). Successful national models, such as Taiwan's inter-agency collaboration between the National Police Agency (NPA) and the Ministry of Justice Investigation Bureau (MJIB), demonstrate the importance of clearly defined mandates and integrated governance structures (Wang et al.,2021). Similarly, OSCE's Police Academies Network (PAN) has advanced capacity building among

member states to improve coordination and operational readiness (Lyzhenkov,2018). Yet, these efforts often fall short in addressing the informal and hybrid governance structures that dominate cybercriminal ecosystems, where trust and cooperation are maintained through decentralized forums, escrow systems, and reputation mechanisms rather than formal institutional arrangements (Yip et al.,2013; Lusthaus et al., 2023).

At the same time, these governance gaps interact with ideological and social drivers that shape how cybercriminal communities form and persist. Beyond structural governance challenges, organized cybercrime is increasingly shaped by ideological motivations and conspiracy-driven narratives. Platforms within the alt-tech ecosystem have enabled the formation of cybercriminal communities bonded not just by profit motives but by shared ideological opposition to state surveillance and global governance structures (Childs, 2023). Efforts to counter these dynamics remain limited and often rely on over-securitization or moral panic narratives that risk amplifying the visibility of these networks rather than dismantling them (Lavorgna, 2019). Some targeted interventions have emerged, such as online reporting tools and in-system detection algorithms aimed at preventing sextortion (Ray & Henry, 2024), as well as networked investigative models aimed to combat wildlife trafficking (Haas, 2023). However, these solutions tend to address specific offenses without considering the broader ideological frameworks that facilitate group cohesion and long-term survival.

While these existing solutions address important aspects of organized cybercrime, they often remain fragmented and reactive. To move from this assessment toward a more integrated response, building on the proposed ecosystem framework, this study outlines additional strategic interventions aimed at disrupting the key relational, technological, and ideological mechanisms that sustain cybercriminal activity. These proposed strategies highlight the importance of coordinated, interdisciplinary efforts to disrupt and dismantle the evolving ecosystems that sustain organized cybercrime.

In practical terms, Table 6 presents strategic policy and intervention recommendations derived from the ecosystem-based conceptual framework proposed in this

Table 6 Intervention strategies aligned with the organized cybercrime ecosystem framework

Intervention Area	Proposed Strategies
Governance Structures	Enhance cross-border legal harmonization; establish specialized international task forces focused on dismantling hybrid governance models in cybercrime forums.
Trust and Cooperation Mechanisms	Target and disrupt informal trust-building tools, such as vendor review systems and escrow services on dark web markets. Promote digital misinformation campaigns that undermine trust in criminal platforms.
Technological Infrastructure	Strengthening digital guardianship through expanded CERT capabilities and AI-driven threat detection systems. Promote mandatory security-by-design principles in IoT devices to reduce vulnerabilities.
Ideological Cohesion	Develop counter-narratives to disrupt extremist and conspiratorial ideologies on alt-tech platforms. Support content moderation partnerships between governments and tech firms to reduce the spread of radicalizing materials.
Institutional Readiness	Apply securitization theory to elevate cybercrime threats in national security agendas, ensuring adequate policy action and resource allocation. Invest in capacity building for law enforcement agencies to address the evolving digital landscape.

study. These strategies aim to address the systemic enablers of organized cybercrime and provide actionable pathways to disrupt its technological, relational, and ideological foundations.

These intervention strategies are designed to disrupt the organized cybercrime ecosystem, thereby impeding and mitigating cybercrimes. To clarify how these measures relate within the framework, Fig. 5 illustrates these strategies.

Building on these findings, this study offers both theoretical contributions and practical implications that together extend the current understanding of organized cybercrime and inform strategies to address it. In theoretical terms, this study advances theory by integrating criminological, economic, sociological, and political perspectives into a unified ecosystem-based framework. Whereas prior research has often applied isolated theories such as Routine Activity Theory (Yar, 2005), Differential Association Theory (Dearden & Parti, 2021), or Transaction Cost Economics (Yip et al., 2013) in narrow contexts, our framework highlights how technological infrastructures, governance gaps, and ideological narratives interact dynamically to sustain organized cybercrime. By bridging these perspectives, the study moves beyond single theory explanations, offering a holistic conceptualization that more accurately captures the hybrid, adaptive, and transnational character of cybercriminal ecosystems. From a practical standpoint, the proposed ecosystem-based framework has clear implications for practitioners. For policymakers, it underscores the need to complement regulatory harmonization with targeted disruption of informal governance mechanisms such as escrow systems and reputation tools that sustain cybercriminal markets (Yip et al., 2013; Lusthaus et al., 2023). For law enforcement, the findings highlight the value of expanding CERT capabilities, adopting AI-driven detection, and applying networked investigative models drawn from other transnational crimes (Holt et al., 2018; Aly et al., 2019; Haas, 2023). For industry actors,

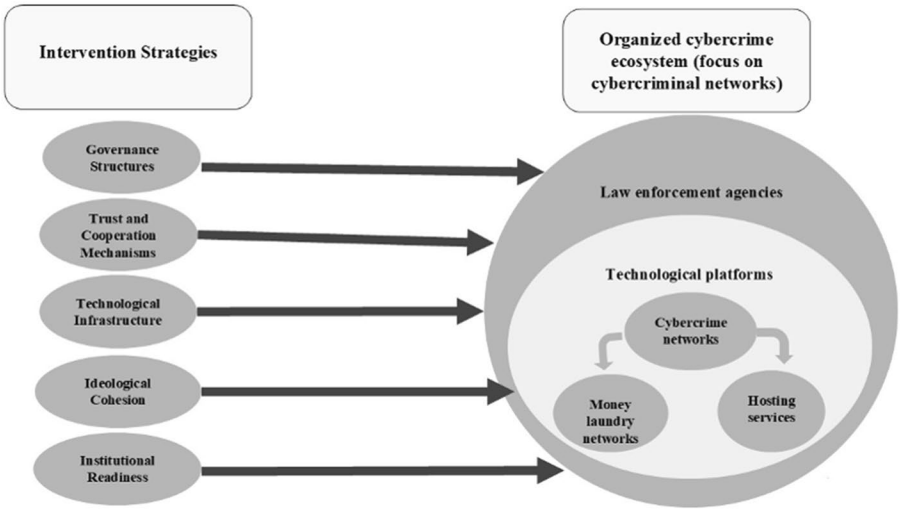

Fig. 5 Intervention strategies aligned with the organized cybercrime ecosystem framework

particularly in the IoT and cloud domains, the study underscores the importance of embedding security-by-design principles and proactive vulnerability reduction (Aly et al., 2019). In parallel, collaboration with governments on counter-narratives and content moderation can help reduce the ideological cohesion that sustains cybercriminal communities (Lavorgna, 2019; Childs, 2023). Taken together, these insights suggest that only coordinated, cross-sector interventions can effectively weaken the resilience of organized cybercrime ecosystems. Overall, the study underscores how an ecosystem perspective advances theory while also informing practice, with the final section reflecting on its limitations and outlining avenues for future research.

Conclusion

This study arrives at four key conclusions. First, while existing criminological and economic theories such as Routine Activity Theory (Cohen & Felson, 1979), Differential Association Theory (Sutherland et al., 1992), and Transaction Cost Economics (Williamson, 1991; Yip et al., 2013) offer important insights into certain aspects of cybercrime, their explanatory power is limited when applied in isolation. By bringing these perspectives into dialogue with institutional and sociopolitical approaches, this study demonstrates that an ecosystem perspective offers a more comprehensive and dynamic framework for understanding how organized cybercrime operates. Second, a central finding is that hybrid governance arrangements where market-based coordination, informal trust systems, and hierarchical controls coexist are not only present but foundational to sustaining cybercriminal networks. These forms of governance, while well documented in political science and organizational theory, have been insufficiently recognized in mainstream criminological accounts of cybercrime. Third, ideological narratives, including conspiracy-driven worldviews and resistance to state surveillance (Lavorgna, 2019; Childs, 2023), emerge as crucial mechanisms of cohesion and resilience. Far from being peripheral, they sustain trust, facilitate recruitment, and complicate law enforcement responses by framing criminal activity within larger political or cultural projects. Finally, although significant progress has been made in technological and institutional responses such as AI-based threat detection, blockchain-supported protections (Aly et al., 2019; Hasani et al., 2023), and cross-border law-enforcement coordination (Broadhurst, 2006; Lyzhenkov, 2018; Wang et al., 2021) these remain fragmented and reactive. Effective counter-cybercrime interventions must employ an integrated approach across governance, technological, and ideological dimensions to avoid merely addressing symptoms instead of tackling the ecosystemic foundations of organized cybercrime.

Limitations

Several limitations of this study should be acknowledged. The most fundamental challenge lies in the rapidly evolving nature of organized cybercrime, which means that new threats may quickly emerge that are not captured by the frameworks proposed here. This temporal limitation affects all literature-based studies but is particularly acute in domains shaped by fast-moving technological innovations. Another

limitation concerns the difficulties of interdisciplinary synthesis: criminology, political science, sociology, and economics approach cybercrime through distinct conceptual vocabularies and methodological traditions. Integrating these perspectives risks both oversimplification and conceptual stretching, even as it enables new insights. A further limitation relates to the scope of the literature review. Although an initial theory driven forward backward snowballing on Scopus yielded 29 unique sources, the subsequent systematic review on ProQuest identified 92 articles. Despite this two-stage process, the review excludes non-English studies, practitioner reports, and other grey literature that may contain valuable insights. Moreover, publication patterns in the reviewed literature show a strong emphasis on cyber-dependent and financial offenses, particularly ransomware and market-related fraud (Yip et al.,2013; Leukfeldt et al., 2017; Cartwright et al., 2019; IC3, 2024; Symantec, 2024; Whelan et al., 2024; Symantec, 2025), whereas ideologically motivated attacks and environmental or wildlife-related cybercrimes are examined primarily in a smaller set of specialized studies (Holt et al., 2017; Childs,2023; Haas, 2023). Finally, while ecosystem thinking provides a unifying framework, it remains primarily conceptual in this paper; empirical validation will be required to assess its applicability across different contexts.

Future research directions

Building on these limitations, future research should advance in four main directions. First, at the theoretical level, classical frameworks such as RAT and DAT require further adaptation to account for digital infrastructures, decentralized governance, and ideological drivers. Their integration with institutionalism and securitization should also be developed more systematically (Keohane, 2005; Buzan & Hansen, 2009; Shad, 2019). Second, methodological innovation is needed. Empirical studies should test the ecosystem framework using tools such as social network analysis to map trust relations, simulation modeling to capture adaptive behaviors, and comparative case studies across sectors such as finance, healthcare, and maritime security. Mixed method designs that combine qualitative and quantitative insights would help overcome the current fragmentation of empirical evidence. Third, future work should engage more directly with the technological dimension. Emerging technologies such as artificial intelligence, blockchain, and the Internet of Things should be examined as dual use infrastructures. On the one hand, they provide new opportunities for criminal exploitation. On the other hand, they hold potential for disruption and prevention if integrated into security and governance frameworks (Aly et al., 2019; Hasani et al., 2023). Finally, research should evaluate the effectiveness of international cooperation mechanisms and policy interventions, from Europol-style task forces to OSCE capacity building programs (Lyzhenkov,2018), to identify which governance strategies most effectively weaken the relational, institutional, and ideological foundations of organized cybercrime. In conclusion, this study demonstrates that organized cybercrime is best understood as an evolving ecosystem sustained by interlocking technological infrastructures, hybrid governance mechanisms, and ideological narratives. Addressing it requires both theoretical innovation and empirical robustness,

as well as cross-sectoral and international collaboration. By adopting an ecosystem perspective, scholars, policymakers, and practitioners can better anticipate emerging threats, design more integrated interventions, and ultimately disrupt the systemic foundations of organized cybercrime.

Funding Open access funding provided by Södertörn University.

References

Abdul-Ghani, H. A., Konstantas, D., Mahyoub, M., Agrawal, S., Sahu, A., & Kumar, G. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications*, *9*(3), 355–373. https://doi.org/10.14569/IJACSA.2018.090349

Abotsi, A. K. (2018). Influence of governance indicators on illicit financial outflow from developing countries. *Contemporary Economics*, *12*(2), 139–151. https://www.ceeol.com/search/article-detail?id=732588

Agrawal, S., Sahu, A., & Kumar, G. (2022). A conceptual framework for the implementation of Industry 4.0 in legal informatics. *Sustainable Computing: Informatics and Systems*, *33*, 100650. https://doi.org/10.1016/j.suscom.2021.100650.

Al Azzam, F. A. F. (2019). The adequacy of the international cooperation means for combating cybercrime and ways to modernize it. *JANUS NET e-journal of International Relations*, *10*, 64–81. https://doi.org/10.26619/1647-7251.10.1.5

Alqahtani, M., & Braun, R. (2021). Reviewing influence of UTAUT2 factors on cyber security compliance: a literature review. *Journal of Information Assurance & Cyber Security*. https://doi.org/10.5171/2021.666987

Alweqyan, D. (2024). Cyberattacks in the context of international law enforcement. *Journal of Financial Crime*, *31*(5), 1052–1066. https://doi.org/10.1108/JFC-07-2023-0164

Aly, M., Khomh, F., Haoues, M., Quintero, A., & Yacout, S. (2019). Enforcing security in Internet of Things frameworks: A systematic literature review. *Internet of Things*, *6*, 100050. https://doi.org/10.1016/j.iot.2019.100050

Apenov, S. M., Jetibayev, N. S., Makisheva, M. K., Kuanalieva, G. A., & Kussainov, S. (2021). International crime as a threat to global socio-economic security. *International Journal of Electronic Security and Digital Forensics*, *13*(2), 133–154. https://doi.org/10.1504/IJESDF.2021.113387

Asadi, S., Nilashi, M., Husin, A. R. C., & Yadegaridehkordi, E. (2017). Customers perspectives on adoption of cloud computing in banking sector. *Information Technology and Management*, *18*, 305–330. https://doi.org/10.1007/s10799-016-0270-8

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408–433. https://doi.org/10.1108/13639510610684674

Bui, T. X., & Lee, J. (2022). Comparative cybersecurity law in Socialist Asia. *Vanderbilt Journal of Transnational Law*, *55*(3), 631–680. https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss3/2

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Cahyonowati, N., Ratmono, D., & Juliarto, A. (2022). The Moderating Role of Social Norms on Tax Compliance Model: A Laboratory Experimental Evidence in Indonesia. *Contemporary Economics*, *16*(4), 410–423. https://www.ceeol.com/search/article-detail?id=1120760

Callon, M. (1999). Actor-network theory-the market test. *Sociological Review*, *47*(S1), 181–195. https://doi.org/10.1111/j.1467-954X.1999.tb03488.x

Cartwright, E., Castro, H., J., & Cartwright, A. (2019). To pay or not: game theoretic models of ransomware. *Journal of Cybersecurity*, *5*(1), 1–12. https://doi.org/10.1093/cybsec/tyz009

Chatinakrob, T. (2024). Interplay of international law and cyberspace: State sovereignty violation, extraterritorial effects, and the paradigm of cyber sovereignty. *Chinese Journal of International Law*, *23*(1), 25–72. https://doi.org/10.1093/chinesejil/jmae005

Childs, A. (2023). The distribution of fake Australian vaccine digital certificates on an alt-tech platform. *Trends in Organized Crime*, *26*(2), 136–155. https://doi.org/10.1007/s12117-022-09466-x

Chowdhury, A., & Ramadas, R. (2022). Cybernetic Hive Minds: A Review. *AI*, *3*(2), 465–492. https://doi.org/10.3390/ai3020027

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime*, *22*(4), 492–512. https://doi.org/10.1108/JFC-11-2014-0056

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588–608.

De Liso, N., & Zamparini, L. (2022). Innovation, transport security and supply chains: a review. *Transport Reviews*, *42*(6), 725–738. https://doi.org/10.1080/01441647.2022.2105415

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice*, *46*(6), 935–955. https://doi.org/10.1007/s12103-021-09655-4

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*, 1–20. https://doi.org/10.1007/s12117-022-09457-y

Diamond, B., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology*, *9*(1), 24–34. https://doi.org/10.5281/zenodo.22196

Doig, A. (2018). Implementing national policing agendas and strategies for fraud at local level. *Journal of Financial Crime*, *25*(4), 984–996. https://doi.org/10.1108/JFC-04-2017-0027

European Commission (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; *European Commission: Brussels, Belgium*, 2013. Retrieved August 19, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=join:JOIN_2013_071

Federal Bureau of Investigation Internet Crime Complaint Center (IC3) (2024). *2023 Internet Crime Report*. Retrieved August 19, 2025, from https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Finckenauer, J. O. (2005). Problems of definition: what is organized crime? *Trends in Organized Crime*, *8*(3), 63–83. https://doi.org/10.1007/s12117-005-1038-4

Flanagan, P. (2022). Cybersex trafficking: The insidious side of the Internet. *Handbook of Research on Present and Future Paradigms in Human Trafficking* (pp. 362–372). IGI Global. Scientific Publishing.

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in Science Engineering and Education*, *1*(1), 100–110.

Gilmour, P. M. (2019). The application of photography in investigating fraud. *The Imaging Science Journal*, *67*(4), 215–223. https://doi.org/10.1080/13682199.2019.1600254

Greiman, V., & Bain, C. (2013). The emergence of cyber activity as a gateway to human trafficking. *Journal of Information Warfare*, *12*(2), 41–49. https://www.jstor.org/stable/26486854

Haas, T. C. (2023). Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity*, *9*(1), tyad004. https://doi.org/10.1093/cybsec/tyad004

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 97. https://doi.org/10.1007/s43546-023-00477-6

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice*, *33*(3), 212–233. https://doi.org/10.1177/1043986217699100

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, *62*(6), 1720–1741. https://doi.org/10.1177/0306624X16679162

Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2024). A systematic literature review of the role of trust and security on Fintech adoption in banking. *Heliyon*, *10*(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e

Jalali, S., & Wohlin, C. (2012, September). Systematic literature studies: database searches vs. backward snowballing. In *Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement* (pp. 29–38). https://doi.org/10.1145/2372251.2372257

Keohane, R. O. (2005). *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.

Kosevich, E. (2023). Cybersecurity, cyberspace and cyberthreats at the beginning of the 21st century: a Latin America typology and review. *Area Development and Policy*, *9*(1), 86–107. https://doi.org/10.1080/23792949.2023.2259972

Latour, B. (2005). *Reassembling the social: An introduction to Actor-Network-Theory*. Oxford University Press.

Lavorgna, A. (2015). Organised crime goes online: realities and challenges. *Journal of Money Laundering Control*, *18*(2), 153–168. https://doi.org/10.1108/JMLC-10-2014-0035

Lavorgna, A. (2019). Cyber-organised crime. A case of moral panic? *Trends in Organized Crime*, *22*(4), 357–374. https://doi.org/10.1007/s12117-018-9342-y

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*, 287–300. https://doi.org/10.1007/s10610-016-9332-z

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, *94*(886), 515–531. https://doi.org/10.1017/S1816383112000811

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60. https://doi.org/10.1080/17440572.2012.759508

Lusthaus, J., Van Oss, J., & Amann, P. (2023). The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology*, *20*(5), 1701–1718. https://doi.org/10.1177/14773708221077615

Lyzhenkov, A. L. (2018). OSCE addresses organized crime through police co-operation. *Security and Human Rights*, *28*(1–4), 49–61. https://doi.org/10.1163/18750230-02801005

Matsaung, P., & Masiloane, D. T. (2024). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *African Security Review*, 1–16. https://doi.org/10.1080/10246029.2024.2421225

McCusker, R. (2006). Transnational organised cyber crime: distinguishing threat from reality. *Crime Law and Social Change*, *46*(4–5), 257–273. https://doi.org/10.1007/s10611-007-9059-3

Moore, J. W. (2006). Animal ecosystem engineers in streams. *BioScience*, *56*(3), 237–246. https://doi.org/10.1641/0006-3568(2006)056[0237:AEEIS]2.0.CO;2.

Mugarura, N., & Ssali, E. (2021). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28. https://doi.org/10.1108/JMLC-11-2019-0092

National Institute of Standards and Technology (2020). *Cybercrime losses: An Examination of U.S. Manufacturing and the Total Economy (NIST AMS 100–32)*. U.S. Department of Commerce. Retrieved August 19, 2025, from https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.100-32.pdf

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, *19*(1), 1–21. https://doi.org/10.1080/17440572.2017.1411807

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Raets, S., & Janssens, J. (2021). Trafficking and technology: Exploring the role of digital communication technologies in the Belgian human trafficking business. *European Journal on Criminal Policy and Research*, *27*, 215–238. https://doi.org/10.1007/s10610-019-09429-z

Ray, A., & Henry, N. (2024). Sextortion: A scoping review. *Trauma Violence & Abuse*, 15248380241277271. https://doi.org/10.1177/15248380241277271

Saif, M. A., Hussin, N., Husin, M. M., Alwadain, A., & Chakraborty, A. (2022). Determinants of the intention to adopt digital-only banks in Malaysia: The extension of environmental concern. *Sustainability*, *14*(17), 11043. https://doi.org/10.3390/su141711043

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, *39*(1), 1–19. https://www.jstor.org/stable/48544285

Stam, E., & Van de Ven, A. (2021). Entrepreneurial ecosystem elements. *Small Business Economics*, *56*(2), 809–832. https://doi.org/10.1007/s11187-019-00270-6

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of Criminology*. Bloomsbury Publishing PLC.

Symantec (2024). The 2024 ransomware threat landscape: An analysis from the Symantec Threat Hunter Team, Retrieved August 19, 2025, from https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf

Symantec (2025). Ransomware 2025: A resilient and persistent threat: An analysis from the Symantec Threat Hunter Team, Retrieved August 19, 2025, from https://www.security.com/sites/default/files/2025-02/2025_02_Ransomware_2025.pdf

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, *79*, 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

United States Government Interagency Guidance Document (2016). *How to Protect Your Networks from Ransomware*. Retrieved August 19, 2025, from https://www.justice.gov/criminal-ccips/file/872771/download

Walsh, J. I. (2007). Defection and hierarchy in international intelligence sharing. *Journal of Public Policy*, *27*(2), 151–181. https://doi.org/10.1017/S0143814X07000682

Wang, S. Y. K., Hsieh, M. L., Chang, C. K. M., Jiang, P. S., & Dallier, D. J. (2021). Collaboration between law enforcement agencies in combating cybercrime: implications of a Taiwanese case study about ATM hacking. *International Journal of Offender Therapy and Comparative Criminology*, *65*(4), 390–408. https://doi.org/10.1177/0306624X20952391

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii-xxiii. https://www.jstor.org/stable/4132319

Whelan, C., Bright, D., & Martin, J. (2024). Reconceptualising organised (cyber) crime: The case of ransomware. *Journal of Criminology*, *57*(1), 45–61. https://doi.org/10.1177/26338076231199793

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Williamson, O. E. (1985). *The Economic Implications of Capitalism: Firms, Markets, and Relational Contracting*. In Das summa Summarum des Management: Die 25 wichtigsten Werke fur Strategie, Fuhrung und Veränderung (pp. 61-75) Wiesbaden: Gabler.

Williamson, O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. *Administrative Science Quarterly*, *36*(2), 269–296. https://www.jstor.org/stable/2393356

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime Media Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516–539. https://doi.org/10.1080/10439463.2013.780227