사회과학연구 제37권 2호(2026) 충남대학교 사회과학연구소 pp. 123-155
http://dx.doi.org/10.16881/jss.2026.04.37.2.123

Toward an Integrated RAT-STT Framework for Understanding Cybercrime in the Age of AI

Vlademir T. Congo, Justin Jin-Hyuk Choi†

Graduate School of Police Studies, Korean National Police University

Artificial intelligence (AI) is transforming digital environments in ways that fundamentally alter the conditions under which cybercrime emerges. While existing scholarship has documented technological changes in offending techniques, less attention has been paid to how AI reshapes crime opportunity itself. This article addresses that gap by developing an integrated analytical framework combining Routine Activity Theory (RAT) and Space Transition Theory (STT) to explain how structural opportunity conditions and behavioral dynamics interact in AI-mediated environments. The framework conceptualizes AI not merely as a facilitative tool but as a systemic modulator that simultaneously expands offender capacity, algorithmically constructs target suitability, and reshapes guardianship and behavioral constraints. By synthesizing structural and behavioral perspectives, the study demonstrates that contemporary cybercrime should be understood as the outcome of dynamically reconfigured opportunity systems rather than as isolated technological offenses. The article contributes to criminological theory by clarifying the analytical relationship between technological change and crime causation and by providing a unified conceptual model capable of interpreting diverse forms of digitally mediated offending. This study is theoretical in orientation and does not propose a new crime typology, regulatory framework, or empirical measurement, but instead offers a conceptual foundation for future empirical, comparative, and interdisciplinary research on crime in the age of AI.

Keywords: Artificial Intelligence; Cybercrime; Crime Opportunity; Routine Activity Theory (RAT); Space Transition Theory (STT); Opportunity Structures; Theoretical Framework

† 교신저자(Corresponding Author) : Justin Jin-Hyuk Choi, Professor, The Department of Law, Korean National Police University [100-50 Hwangsan-gil, Shinchang-myeon, Asan City 31539, Republic of Korea] / Chair, The Department of Criminal Investigation, Graduate School of Police Studies, E-mail : thebestsecurity@me.com
Vlademir T. Congo, Ph.D. Student, The Department of Criminal Investigation, Graduate School of Police Studies / Criminal Investigator, The Criminal Investigation Service of Angola (SIC) (First Author)

■ 최초투고일 : 2026년 2월 20일 ■ 심사마감일 : 2026년 3월 28일 ■ 게재확정일 : 2026년 4월 15일

1. Introduction

The digital transformation of contemporary societies has generated unprecedented economic, social, and communicative opportunities, while simultaneously producing complex and rapidly evolving security challenges (Kolade et al., 2024; Saeed et al., 2023). Among these, online scams have emerged as one of the most pervasive and adaptive forms of crime within digital environments (Button & Cross, 2017; Kipngetich, 2025). Historically, such scams relied upon human-centered deception, interpersonal persuasion, and the manipulation of trust through direct or semi-direct interaction (Hancock, 2009; Norris, 2019).

The integration of Artificial Intelligence (hereafter 'AI'), however, has fundamentally altered this landscape. Technologies such as generative language models, conversational agents, deepfakes, and voice synthesis have enabled deception to be automated, personalized, and scaled, transforming scams from episodic interpersonal acts into industrialized, data-driven operations (Bociga & Lord, 2026; Schmitt & Flechais, 2024). In this sense, AI functions not merely as a new criminal tool, but as a structural condition that reshapes how crime opportunities are produced, distributed, and exploited (King et al., 2020; Rohozinski & Spirito, 2026; UNODC, 2025).

Existing scholarship across criminology, sociology, victimology, computer science, and law provides important insights into the evolution of scams and their harms. Early research focused on traditional fraud typologies, while later studies documented how digital connectivity expanded the reach and coordination of deceptive practices (Choo & Tan, 2008; Jahankhani et al., 2014; Koning et al., 2024). Victimological research has further demonstrated that susceptibility to scams is shaped not by individual gullibility, but by the strategic exploitation of trust, authority, urgency, and emotional need (Button et al., 2014; Norris, 2019; Shang et al., 2023; Whitty, 2019). Yet much of this literature remains grounded in human-mediated deception and does not fully account for AI-specific affordances such as synthetic interaction, adaptive persuasion, persistent conversational agents, and algorithmic targeting (Ho et al., 2025; Schmitt & Flechais, 2024; Velutharambath et al., 2025).

Notably, from a criminological perspective, these transformations cannot be adequately understood without attention to how AI restructures the conditions under which crime occurs. Routine Activity Theory (hereafter 'RAT') explains crime as the convergence of motivated offenders, suitable targets, and absence of capable guardianship (Cohen & Felson, 1979; Leukfeldt & Yar, 2016; Yar, 2005), whereas Space Transition Theory (hereafter 'STT') accounts for behavioral and normative shifts that occur when individuals move between physical and digital environments (Choi, 2025; Jaishankar, 2008; Zhou et al., 2024). Each framework captures important but partial dimensions of contemporary cybercrime. RAT in principle clarifies structural opportunity dynamics but under-specifies behavioral transformation (Felson & Clarke, 1998; Kigerl, 2012; Reyns, 2017; Vakhitova et al., 2015), while STT explains behavioral adaptation but remains less precise regarding technological restructuring of opportunity conditions (Al Shamsi et al., 2023; Assarut et al., 2019; Jaishankar, 2019).

The rise of AI renders this theoretical separation increasingly untenable. AI simultaneously expands offender capacity, algorithmically constructs target suitability, strains guardianship mechanisms, and intensifies identity fluidity and dissociative anonymity across digital spaces (Dobusch & Schoeneborn, 2015; Graham & Triplett, 2017; Weulen Kranenbarg et al., 2021). Understanding contemporary cybercrime thus requires a framework capable of explaining both structural opportunity transformation and behavioral transition within technologically mediated environments (Vakhitova, 2025; Završnik, 2021).

Against this backdrop, this study addresses the central question of how AI reconfigures crime opportunities and what this transformation implies for victimization and justice. Building upon prior work applying STT to digital offender profiling (Choi, 2025), this research integrates STT with RAT (Choi et al., 2025) into a unified analytical framework. This integrated RAT-STT model provides a dual-lens approach that simultaneously accounts for structural constraints and the process of behavioral transformations. Consequently, the analysis demonstrates how AI reshapes scam mechanisms, generates new victimization patterns, and exposes limitations in existing legal and institutional responses.

Accordingly, this article does not seek to introduce a new crime typology, nor does it aim to offer a regulatory analysis or provide empirical measurements of cybercrime trends. Instead, the study's primary contribution is theoretical: it develops an integrated RAT-STT framework that explains how AI reconfigures the mechanics of cybercrime opportunity and behavioral adaptation. By conceptualizing AI as a structural condition that simultaneously transforms opportunity structures and behavioral dynamics, the article offers a unified analytical lens for understanding cybercrime beyond offense-specific or technology-centered accounts.

2. Theoretical Foundations of Crime Opportunity in AI-Mediated Environments

Understanding cybercrime in the age of AI requires theoretical frameworks capable of explaining not only how crime is committed but how the conditions that make crime possible are structurally produced and dynamically transformed (Adewopo et al., 2025; Berk, 2021; Lavorgna & Ugwudike, 2021). In digitally mediated environments, opportunity is no longer a static situational configuration but an adaptive and technologically modulated system shaped by automation, data infrastructures, and algorithmic interaction (Brayne & Christin, 2021; Peeters & Schuilenburg, 2018). Conventional criminological approaches that treat crime as the outcome of individual motivation or deviant disposition are therefore insufficient for explaining contemporary AI-mediated offenses, which emerge within socio-technical environments that systematically organize exposure, vulnerability, and behavioral interaction (Opp, 2020; Sullivan, 2022; Wikstrom & Kroneberg, 2022).

Among existing criminological theories, RAT and STT, in particular, provide valuable analytical foundations because they examine complementary dimensions of crime causation. RAT conceptualizes crime as the product of structural convergence among motivated offenders, suitable targets, and

absent or ineffective guardianship (Brantingham & Brantingham, 2016; Felson, 2016; Hollis-Peel et al., 2011). Its core contribution hence lies in shifting explanatory emphasis away from offender pathology toward opportunity structure, demonstrating that crime rates fluctuate when environmental conditions alter the likelihood of such convergence (Clarke, 1995; Hipp, 2016; Kleemans et al., 2012; Schaefer & Mazerolle, 2017).

In contrast, STT elucidates the erosion of behavioral norms as individuals transition from physical to digital spaces. It posits that the interplay of anonymity, identity fluidity, and diminished social deterrence fundamentally alters moral constraints, thereby lowering the threshold for deviant conduct (Capurro et al., 2013; Jaishankar, 2010, 2018; Wen & Miura, 2025). While prior research has explored behavioral dynamics of digital offending through STT (Choi, 2025), the present study extends this approach by incorporating structural opportunity conditions through RAT (Choi et al., 2025), thereby developing an integrated explanatory framework. Collectively, these theories encompass both the structural and behavioral conditions shaping cybercrime. However, their divergent analytical emphases suggest the necessity for an integrated perspective that bridges opportunity structures with behavioral dynamics in technologically mediated environments.

1) Routine Activity Theory (RAT) and Opportunity as Structural Condition

RAT provides a foundational framework for analyzing technologically mediated crime because it treats criminal events as contingent upon situational configurations rather than individual predispositions (Cohen & Felson, 1979; Leukfeldt & Yar, 2005). In digital environments, these configurations are profoundly reshaped by AI. Continuous connectivity, platform integration, and automated communication expand target accessibility, while scalable digital infrastructures reduce offender effort and perceived risk (King et al., 2020; Lavorgna, 2014; Wall, 2024). As a result, the convergence of offenders, targets, and guardianship described by RAT becomes more frequent, more distributed, and less temporally constrained (Miller, 2013; Soudijn & Zegers, 2012; Vakhitova, 2025).

AI amplifies each element of the RAT triad. First of all, it lowers barriers to entry for offenders by providing user-friendly tools capable of generating persuasive content, impersonating identities, and automating interaction (Faqir, 2023; Hayward & Maas, 2020). Second, it transforms target suitability by enabling predictive profiling, allowing offenders to identify and tailor approaches to individuals based on behavioral data, social signals, and contextual cues (Brand, 2020; Huseynov & Ozdenizci Kose, 2022; Završnik, 2021). Third, it strains guardianship capacity by overwhelming detection systems with adaptive and rapidly generated content (Bossler & Holt, 2009; Ekundayo et al., 2024; Williams, 2016). As established in the theoretical integration section, AI accelerates opportunity convergence by reducing operational barriers, facilitating mass personalization, and outpacing traditional guardianship through its inherent speed and scale.

In this sense, AI does not merely assist or facilitate criminal conduct; it reconfigures the very landscape of criminal opportunity. Crime thereby is becoming

less dependent on physical proximity or prolonged effort, relying instead on automated, algorithmic coordination and digital vulnerability patterns (Homeland Security, 2024; Spyropoulos, 2024; UNODC, 2025; Wisnubroto & Tegnan, 2025). Opportunity is thus transformed from a localized situational condition into a distributed system characteristic of routine participation in digital life (Brenner, 2002; Romagna & Leukfeldt, 2024).

2) Space Transition Theory (STT) and Behavioral Dynamics in Digital Environments

Where RAT explains how opportunity structures emerge, STT demonstrates how individuals behave within them. STT posits that transitions between physical and virtual environments produce shifts in identity, moral restraint, and normative expectations. Digital environments—characterized by anonymity, dissociation (dissociative distance), and reduced deterrence—facilitate behaviors that are unlikely in offline settings (Chen et al., 2025; Cohen, 2007; Jaishankar, 2008, 2010). These shifts occur not because individuals become inherently deviant, but because environmental conditions alter perceptions of accountability, risk, and social feedback (Apene et al., 2024; Lapidot-Lefler & Barak, 2012).

AI intensifies these dynamics by introducing synthetic interaction, automated agents, and identity simulation into online environments. These features expand identity fluidity and create psychological distance between actors and consequences (Adler et al., 2024; Igba et al., 2025). Offenders may interact through avatars, generated personas, or bots, reducing emotional salience and moral inhibition. At the same time, AI systems can simulate empathy, memory, and conversational continuity, increasing victims' emotional engagement and compliance (Rosenberg, 2023; Rostami & Navabinejad, 2023). This results in a dangerous asymmetry: offenders remain detached while victims become deeply immersed in a fabricated relationship.

STT thus clarifies how technological mediation alters not only the structure of opportunity but also the psychological conditions under which deception becomes possible (Burrell, 2025; Ho et al., 2025; Velutharambath et al., 2025). As described in the discussion of identity and anonymity dynamics, digital environments enable individuals to maintain multiple synthetic identities and to shift between them rapidly, thereby distancing action from accountability (Arslan, 2023; Schmitt & Flechais, 2024). These processes demonstrate that cybercrime cannot be fully understood without accounting for the behavioral transformations associated with movement across digitally mediated spaces.

3) Limits of Single-Theory Explanations

Although both RAT and STT offer powerful insights, each theory is analytically incomplete when applied in isolation. RAT excels at explaining how opportunity structures expand or contract but does not fully specify how digital environments transform motivation, identity, or moral constraint (Vakhitova, 2025; Vakhitova et al., 2015; Willison & Backhouse, 2006). On the other hand, STT illustrates behavioral adaptation, but it offers limited insight into how technological infrastructures systematically create and

distribute criminal opportunities (Assarut et al., 2019; Choi, 2025; Salleh & Selamat, 2022). When used independently, each theory captures only part of the explanatory landscape.

This limitation becomes especially pronounced in AI-mediated contexts, where structural and behavioral transformations occur simultaneously. AI alters opportunity conditions through automation, scalability, and predictive targeting, while also reshaping behavioral dynamics through anonymity, simulation, and algorithmic interaction (Mokoena et al., 2023; Spyropoulos, 2024; Wall, 2024). Analytical approaches prioritizing exclusively structural or behavioral explanations fail to capture the reciprocal interaction between environment and action, which is fundamental to contemporary cybercrime (Hipp, 2010; Wikstrom & Kroneberg, 2022).

4) Toward a Unified Theoretical Perspective

The convergence of these insights points toward the necessity of theoretical integration (Kavish & Boutwell, 2018; Opp, 2020). AI functions as a systemic modulator that simultaneously reshapes opportunity structures and behavioral conditions (Schmitt & Flechais, 2024; Wisnubroto & Tegnan, 2025). By lowering effort thresholds, expanding target reach, and weakening guardianship, it reorganizes the structural conditions identified by RAT (Haley & Burrell, 2025; Reyns et al., 2011). By enabling identity fluidity, dissociative interaction, and norm displacement, it intensifies the behavioral mechanisms described by STT (Choi, 2025; Van der Wagen & Pieters, 2015). The explanatory power of each theory is therefore strengthened when considered together rather than separately.

This integrated perspective reframes AI-mediated crime as a phenomenon arising from dynamically reconfigured opportunity systems rather than isolated acts of deception (Bociga & Lord, 2026; Fiorinelli & Zucca, 2025). Crime becomes intelligible as the product of feedback processes linking technological infrastructure, human behavior, and institutional control (Aebi et al., 2025; Lewis & Lewis, 2011; Yeboah-Ofori & Opoku-Boateng, 2023). Such a perspective also clarifies why contemporary cybercrime is increasingly scalable, adaptive, and resistant to traditional forms of regulation: the conditions that enable it are embedded within routine digital interaction rather than confined to exceptional or abnormal situations (Dupont & Whelan, 2021; Katyal, 2002; Kipngetich, 2025).

5) Analytical Implications for the Present Study

Building on this theoretical foundation, the present study adopts an integrated RAT-STT approach to analyze how AI reconfigures crime opportunity in digitally mediated environments. This integrated model merges structural and behavioral dimensions, and provides a unified framework for analyzing the intricate dynamics of contemporary cybercrime (Ahmad & Thurasamy, 2022; Leukfeldt & Yar, 2016; Martineau et al., 2023). The sections that follow apply this framework to three related questions: (1) how AI generates new mechanisms of offending (Caldwell et al., 2020; Faqir, 2023; King et al., 2020), (2) how reconfigured opportunities produce observable outcomes (Lazarus et al., 2025; Porcedda

& Wall, 2019), and (3) what implications these transformations hold for legal, institutional, and policy responses (Goldsmith & Brewer, 2014; Kuziemski & Misuraca, 2020; Salehi et al., 2025). Importantly, this study does not propose a new standalone theory but develops an integrated explanatory framework in which structural opportunity and behavioral transition are analytically interdependent and jointly shape cybercrime in AI-mediated environments.

3. An Integrated RAT - STT Framework

The preceding discussion demonstrates that neither structural opportunity approach (RAT) nor behavioral transition model (STT) alone can adequately explain cybercrime in environments shaped by AI. Contemporary digital offending emerges from the simultaneous interaction of technologically produced opportunity structures and psychologically mediated behavioral dynamics (Akinbowale et al., 2025; Hughes & Hutchings, 2023). Building on the theoretical foundations, this section develops an integrated analytical framework that combines RAT and STT. Instead of treating the two theories as parallel or independent, the proposed framework conceptualizes them as analytically interdependent, linking structural opportunity conditions to behavioral transition dynamics within AI-mediated environments.

The framework is intended not as a standalone predictive model, but as a conceptual and analytical structure for understanding how cybercrime opportunity is reconfigured through the interaction of structural and behavioral processes. By positioning AI as a mediating condition that simultaneously reshapes opportunity structures and behavioral patterns, it provides a coherent basis for interpreting contemporary cybercrime beyond single-theory or offense-specific approaches. The analytical task, therefore, is not to choose between RAT and STT, but to integrate them into a unified framework that captures the reciprocal relationship between environmental conditions and human action in contemporary AI-mediated contexts.

1) Conceptual Logic of Integration

Notably, RAT and STT address different but interdependent explanatory domains. RAT specifies the structural conditions that make crime possible, emphasizing convergence among offenders, targets, and guardianship (Groff, 2007; Wortley & Townsley, 2016). In contrast, STT specifies the behavioral transformations that make crime more likely, emphasizing shifts in identity, norm perception, and deterrence across environments (Al Shamsi et al., 2023; Shetty et al., 2024). The theoretical limitation of treating these frameworks separately lies in the implicit assumption that opportunity structures and behavioral dynamics operate independently. In digitally mediated environments, however, they are mutually constitutive (Chiao, 2019; Fleetwood, 2016).

AI collapses the analytical boundary between these domains. Structural conditions increasingly shape behavior in real time through algorithmic interaction (Brand, 2020; Karunamurthy et al., 2023; Wilcox et al., 2018), while behavioral responses simultaneously reconfigure opportunity structures through data generation, adaptive targeting, and recursive feedback loops (Adanyin, 2024; Bello, 2025; Jabir

et al., 2025). Opportunity and behavior thus form a recursive system rather than sequential stages (Granic & Patterson, 2006; Mead & Neves, 2018). A theoretical model capable of explaining AI-mediated crime must therefore conceptualize structure and behavior as dynamically linked components of a single analytical architecture.

2) AI as Structural–Behavioral Modulator

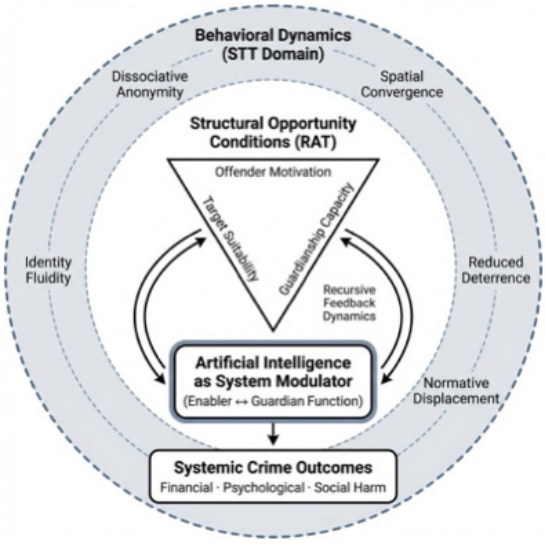
Within the integrated framework proposed here, AI is conceptualized not as an external tool used by offenders but as a central modulating condition that influences all components of the crime environment simultaneously (Caianiello, 2019; Smith, 2026). AI expands offender capacity by lowering technical barriers, automating engagement, and enabling deception at scale (Aebi et al., 2025; Bello, 2025; Pawar et al., 2021). It affects target suitability by transforming individuals into continuously profiled and algorithmically interpretable subjects (Al Fahdi et al., 2016; Büchi et al., 2023). In addition, AI influences guardianship by straining detection systems, complicating attribution, and generating adaptive adversarial behavior (Malatji & Tolah, 2025; Sudhakaran & Kshetri, 2026). At the same time, AI is reshaping behavioral conditions by enabling synthetic identities, persistent interaction, and emotional simulation, thereby altering human perceptions of risk, accountability, and authenticity (Pakina et al., 2023; Sharma et al., 2025).

This dual influence means that AI operates as both an environmental force and a behavioral catalyst. It thus reorganizes situational convergence while simultaneously modifying how actors perceive, interpret, and respond to that convergence (Ayling, 2011; Ekblom, 2017; Schiliro, 2024). In this sense, AI functions as a structural-behavioral bridge linking the explanatory domains of RAT and STT. The significance of this role is analytical rather than technological: it provides a conceptual mechanism through which structural and behavioral processes can be understood as co-evolving rather than independent.

As illustrated in <Figure 1>, the framework is organized as a layered analytical system. The inner RAT layer represents structural opportunity conditions defined by the convergence of offenders, targets, and guardianship, while the surrounding STT layer captures behavioral transformations associated with digitally mediated environments, including anonymity, identity fluidity, and norm conflict. AI hence is positioned beneath these layers as a systemic modulator, reflecting its role in simultaneously reshaping opportunity structures and behavioral conditions rather than operating as an independent causal factor. The bi-directional arrows indicate recursive feedback dynamics through which technological affordances, human behavior, and institutional constraints co-evolve. The resulting configuration demonstrates that AI-enabled online scams are best understood not as isolated deceptive acts but as emergent outcomes of dynamically reconfigured opportunity environments.

3) Opportunity Reconfiguration Mechanisms

Integrating RAT and STT highlights that AI-mediated crime represents a reconfiguration of opportunity rather than a mere expansion. This distinction is critical to better understand the evolving nature of digital offenses (Allah Rakha, 2024; Rossy & Ribaux, 2020;



<Figure 1> Conceptual Architecture of the Integrated RAT-STT Framework for AI-Mediated Cybercrime[1)]

Willison & Backhouse, 2006). Importantly, AI alters the spatial, temporal, relational, and informational dimensions of crime opportunity simultaneously (Butt et al., 2021; King et al., 2020; Zhou et al., 2024).

Spatially, digital environments erase physical borders, enabling offenders and targets to collide across global jurisdictions (Arnell & Faturoti, 2023; Lazarus, 2025; Mokoena et al., 2023). Temporally, automated systems allow continuous interaction, eliminating traditional limits on duration and/or frequency of contact (Bello, 2025; Van der Wagen & Pieters, 2015). Relationally, synthetic personas and simulated communication fundamentally reconfigures the landscape of interpersonal dynamics, facilitating deception to occur within seemingly authentic relationships (Čekić, 2024; George et al., 2023). Informationally, the convergence of predictive analytics and data aggregation transform inherent behavioral uncertainty

1) <Figure 1> illustrates the integrated RAT-STT framework, mapping how structural opportunities and behavioral dynamics converge within AI-mediated environments to drive modern cybercrime. This analytical framework was independently developed [and proposed] by the Author, drawing upon and synthesizing interdisciplinary scholarship on routine activity theory, space transition theory, situational action theory, AI-mediated crime environments, and cybercrime guardianship dynamics, including, inter alia [in alphabetical order]: Apene et al. (2025); Brewer et al. (2019); Caldwell et al. (2020); Chiao (2019); Choi (2025); Choi et al. (2025); Clarke (1995); Cohen & Felson (1979); Ekblom (2017); Faqir (2023); Felson (2016); Goldsmith & Brewer (2015); Holt & Bossler (2016); Jaishankar (2008, 2019); King et al. (2020); Leukfeldt & Yar (2016); Martineau et al. (2023); Reyns (2017); Schaefer & Mazerolle (2017); Vakhitova (2025); Vakhitova et al. (2015); Wall (2024); Wikstrom & Kroneberg (2022); Wilcox et al. (2018); Wortley & Townsley (2016); Yar (2005); Završnik (2021); Zhou et al. (2024).

into precise probabilistic targeting, thereby optimizing operational efficiency and reinforcing normative compliance (Arslan, 2023; Berk, 2021; Ekundayo et al., 2024).

These transformations indicate that opportunity is no longer a passive situational condition but an actively engineered environment. Digital offenders no longer merely encounter opportunities; they can design, replicate, and scale them (Broadhurst, 2021; Ekblom, 2017; Leukfeldt & Jansen, 2019). The result is a shift from situational opportunism to systemic opportunity production.

4) Feedback Dynamics Between Structure and Behavior

A central contribution of the integrated framework is its capacity to explain feedback dynamics linking structural opportunity and behavioral adaptation. In AI-mediated environments, structural changes alter behavioral incentives, and behavioral responses in turn reshape structural conditions (Groff, 2007; Hipp, 2016). For example, automated targeting increases victim exposure, generating additional data that refine predictive models and further enhance targeting accuracy (Ejjami, 2024; Haley & Burrell, 2025). Similarly, adaptive detection systems modify offender strategies, prompting iterative evasion techniques that reshape guardianship mechanisms (Gilbert et al., 2025; Quibell, 2024).

These recursive interactions give rise to an evolutionary dynamic resembling a co-adaptive system rather than a static environment. Crime opportunity becomes a moving equilibrium shaped by continuous interaction among offenders, targets, guardians, and technological infrastructures (Apene et al., 2024; Kigerl, 2012). This dynamic perspective helps explain why AI-mediated crime often appears resistant to traditional forms of prevention and control: interventions targeting one component of the system may trigger adaptive responses in another (Borgesano et al., 2025; Braithwaite, 2020; Selvadurai, 2025).

5) Analytical Value of the Integrated Model

The theoretical value of the integrated RAT-STT framework lies in its ability to unify previously fragmented explanations of cybercrime. Rather than treating contemporary digital offenses as anomalies requiring entirely new theoretical approach, the framework postulates how established criminological principles can be extended and recombined to account for technological transformation (Holt & Bossler, 2016; Maimon & Louderback, 2019; Opp, 2020; Leukfeldt & Yar, 2016). It therefore preserves the explanatory strengths of both theories while compensating for their respective limitations.

More specifically, the developed model shows that contemporary cybercrime should be understood not simply as technologically facilitated wrongdoing, but as the result of structurally produced opportunities interacting with behaviorally transformed actors (Aebi et al., 2025; Jaishankar, 2008; Smith, 2026). This reconceptualization shifts analytical attention from isolated incidents to systemic environments (Bello, 2025; Farrell & Pease, 2017; Wortley & Townsley, 2016), from individual culpability to situational configurations (Clarke, 1995; Leukfeldt & Jansen, 2019; Wilcox et al., 2018), and from static risk factors to dynamic interaction processes (Maimon

& Browning, 2012; McMillon et al., 2014). Such a perspective is especially useful for analyzing AI-mediated offenses, which are characterized by scalability, persistence, and adaptability.

6) Framework Implications for Subsequent Analysis

The proposed framework (Figure 1) provides the conceptual structure that guides the remainder of this study. It sets out three analytical propositions that organize the sections that follow. First, AI-mediated crime should be understood not as a collection of separate techniques, but as observable expressions of reconfigured opportunity. Second, outcomes such as victimization patterns and institutional strain are best understood as systemic consequences of these conditions. Third, legal and policy responses should be evaluated according to their ability to address both structural opportunity and behavioral dynamics.

These propositions are not empirical claims but analytical premises. Their purpose is to guide interpretation and clarify causal logic. By showing how structural and behavioral factors interact in digitally mediated environments, the framework offers a coherent lens for examining diverse cybercrime phenomena without fragmenting analysis into isolated explanatory models. Drawing upon those propositions, the following section examines the mechanisms of contemporary AI-mediated cybercrime as illustrative manifestations of the integrated framework, thereby demonstrating how reconfigured opportunity conditions are translated into observable patterns of offending.

4. Mechanisms of AI-Mediated Cybercrime

The mechanisms discussed in this section are presented not as discrete categories, but as illustrative manifestations of the integrated RAT-STT framework developed in Section 3. From this perspective, AI-mediated cybercrime is best understood not merely as technologically facilitated offending, but as the outcome of identifiable mechanisms through which reconfigured opportunity conditions are translated into actionable criminal behavior.

These mechanisms operate at the intersection of structural opportunity and behavioral transformation, linking technological affordances to observable patterns of offending (Bossler & Holt, 2009; Caldwell et al., 2020; Reyns, 2017; Wikstrom & Kroneberg, 2022). Rather than treating AI as a tool occasionally employed by offenders, this section conceptualizes it as an enabling infrastructure that systematically reorganizes how opportunities are generated, perceived, and exploited.

1) Automation of Offender Capacity

One of the most consequential mechanisms introduced by AI is the automation of offender activity Traditional forms of deception required sustained human effort, interpersonal skill, and temporal investment (Butt et al., 2021; Treleaven et al., 2023; Yar & Steinmetz, 2023). AI systems reduce these requirements by generating persuasive messages, synthesizing identities, and maintaining continuous interaction without direct human intervention (Bello, 2025; Jahan & Mell, 2024; Malatji & Tolah, 2024). When

less effort is needed, it becomes easier for even non-experts to commit sophisticated digital crimes. (Apene et al., 2024; Holt & Bossler, 2016; Leukfeldt et al., 2017). The resulting expansion of offender capacity does not merely increase crime volume; it alters the structural relationship between effort and reward, making cybercrime more scalable, persistent, and economically efficient (Bossler & Holt, 2009; Maimon & Louderback, 2019; Wall, 2024).

From a RAT perspective, automation increases the likelihood of offender-target convergence by enabling simultaneous engagement with multiple targets (Leukfeldt & Yar, 2016; Reyns, 2017). From an STT perspective, automation distances actors from the psychological consequences of their actions, reducing moral inhibition and facilitating norm displacement (Jaishankar, 2008; Williams, 2016; Zhuo et al., 2024). The same technological feature therefore operates simultaneously as a structural amplifier and a behavioral catalyst (Ekblom, 2017; Goldsmith & Brewer, 2015).

2) Algorithmic Construction of Target Suitability

AI also transforms the notion of target suitability (Büchi et al., 2023; Ekundayo et al., 2024). In traditional opportunity theory, suitable targets are those whose characteristics make victimization feasible or attractive (Cohen & Felson, 1979; Felson & Clarke, 1998; Miller, 2013). By contrast, in contemporary AI-mediated environments, target suitability is no longer passively encountered but actively constructed through algorithmic analysis (Al Fahdi et al., 2016; De Hert & Lammerant, 2016; Dzuba, 2025). Behavioral data, interaction patterns, and platform metadata allow digital offenders—or automated systems acting on their behalf—to identify individuals most likely to respond to specific forms of manipulation (Butkovic et al., 2018; Pakina et al., 2023; Schiliro, 2024).

This predictive targeting shifts the logic of crime from chance encounters to intentional selection. Offenders can now target individuals whose digital profiles indicate vulnerability, receptivity, or contextual susceptibility (Benbouzid, 2019; Ward & Durrant, 2011; Whitty, 2019). Such processes reduce uncertainty and increase efficiency, reinforcing the structural convergence conditions described by RAT (Pratt et al., 2010; Reyns, 2017; Williams, 2016). At the same time, personalized interaction enhances relational credibility and emotional immersion, intensifying the behavioral mechanisms identified by STT (Button et al., 2014; Suler, 2004; Buchanan & Whitty, 2014). Target suitability thus becomes a dynamic variable shaped through continuous data interpretation rather than a static attribute of individuals (Andrejevic & Gates, 2014; Zuboff, 2019).

3) Synthetic Identity and Interaction Simulation

A further mechanism linking structural and behavioral dynamics is the capacity of AI systems to generate synthetic identities and simulate interaction (Chesney & Citron, 2019; Jahan & Mell, 2024). Digital personas can be constructed rapidly, modified continuously, and deployed across multiple platforms, allowing offenders to operate through layers of mediated representation (Capurro et al., 2013;

Hancock & Bailenson, 2021; Paris, 2021). These synthetic identities facilitate deception not only by obscuring attribution but by producing the appearance of authenticity, familiarity, or authority (Alder et al., 2024; Tolosana et al., 2020).

From a structural standpoint, identity simulation reduces the risks associated with exposure, thereby weakening guardianship effectiveness (Caldwell et al., 2020; Karnouskos, 2020). From a behavioral standpoint, simulated interaction reshapes social perception, enabling targets to interpret automated communication as genuine interpersonal engagement (Cheng, 2023; Rashid et al., 2025). Emotional cues, conversational continuity, and contextual adaptation can create the impression of a stable relational partner, increasing trust and compliance (McKay & Macintosh, 2024; Rosenberg, 2023; Whitty, 2019). This mechanism demonstrates how technological affordances concurrently alter situational opportunity and cognitive interpretation, thereby reinforcing the analytical necessity of integrating RAT and STT (Choi, 2025; Choi et al., 2025; Ekblom, 2017; Goldsmith & Brewer, 2015; Jaishankar, 2008).

4) Temporal Persistence and Interaction Continuity

AI also introduces a temporal dimension that distinguishes contemporary cybercrime from earlier forms of digital deception (Allah Rakha, 2024; Čekić, 2024). Automated agents can maintain continuous interaction across extended periods, eliminating the temporal constraints that traditionally limited offender activity (Bello, 2025; Hughes & Hutchings, 2023). Persistence increases exposure probability, allowing repeated engagement attempts and adaptive message refinement based on recipient response patterns (Buchanan & Whitty, 2014; Rohozinski & Spirito, 2026).

This persistence affects both opportunity structure and behavioral response (Cohen & Felson, 1979; Granic & Patterson, 2006; Wikstrom & Kroneberg, 2022). Structurally, extended interaction duration increases the likelihood of convergence between offender and target (Ilievski, 2016; Reyns et al., 2011; Yar & Steinmetz, 2023). Behaviorally, repeated communication fosters familiarity and reduces skepticism, gradually normalizing interaction that might initially appear suspicious (Michael & Brewer, 2025; Vakhitova, 2025) Over time, targets may reinterpret the interaction as routine rather than exceptional, a shift that lowers psychological resistance (Modic & Anderson, 2015; Stajano & Wilson, 2011). Temporal continuity thus operates as a mechanism through which digital environments reshape perception and decision-making processes.

5) Distributed and Scalable Opportunity Production

Perhaps the most significant transformation introduced by AI-mediated environments is the shift from opportunistic offending to systemic opportunity production (Brayne & Christin, 2021; King et al., 2020). In physical settings, opportunities arise sporadically and are constrained by proximity, timing, and effort (Felson & Clarke, 1998; Wortley & Townsley, 2016). In AI-mediated environments, opportunities can be designed, replicated, and distributed across networks at scale (Apene et al., 2024;

Kipngetich, 2025). Automated scripts, adaptive algorithms, and platform infrastructures enable offenders to generate large numbers of interaction scenarios simultaneously (Broadhurst, 2021; Haley & Burrell, 2025; Huseynov & Ozdenizci Kose, 2022).

As Felson observed in his 2016 work, such capacity fundamentally transforms the ontology of opportunity itself. Opportunity is no longer a situational condition awaiting discovery; it becomes an engineered resource subject to optimization (Faqir, 2023; Felson, 2016; Maimon & Louderback, 2019; Wisnubroto & Tegnan, 2025). Structural convergence is therefore no longer contingent on chance but can be strategically orchestrated. As a result, the distinction between opportunity and strategy collapses, producing a system in which criminal activity resembles a coordinated process rather than isolated events (Leukfeldt et al., 2017; Lavorgna, 2014; Schiliro, 2024).

6) Adaptive Feedback and Evolutionary Dynamics

The mechanisms described above do not operate independently. They interact through feedback processes that produce adaptive system behavior. Automated targeting generates data; these data refine predictive models, and refined models further enhance targeting accuracy (Ekundayo et al., 2024; Granic & Patterson, 2006; Haley & Burrell, 2025). Meanwhile, detection efforts provoke evasion strategies, which in turn reshape detection systems. Together, this resulting dynamic constitutes a co-evolutionary environment characterized by continual adjustment among offenders, targets, guardians, and technological infrastructures (Cable et al., 2024; Do & Selvadurai, 2025).

These feedback dynamics help explain why AI-mediated cybercrime often appears resilient to traditional prevention approaches. Interventions that target one mechanism may trigger adaptive responses in another, thereby sustaining the overall system equilibrium (Apene et al., 2024; Braithwaite, 2020; Hayward & Maas, 2021; Van Elteren et al., 2024). Understanding cybercrime as a dynamic system rather than a static phenomenon therefore becomes essential for accurate analysis (Opp, 2020; Smith, 2026; Wikstrom & Kroneberg, 2022). The integrated RAT-STT framework provides the conceptual tools necessary to interpret these processes because it captures both the structural conditions enabling adaptation and the behavioral processes through which adaptation occurs (Cullen et al., 2008; Dzuba, 2025; Goldsmith & Brewer, 2014; Ilievski, 2016).

Taken together, the mechanisms identified in this section demonstrate how AI translates reconfigured opportunity conditions into operational forms of cybercrime. The next section then examines the observable consequences of these processes, showing how systemic opportunity transformation manifests in patterns of harm, victimization, and institutional strain.

5. Outcomes of Reconfigured Opportunity

As the preceding analysis shows, AI not only expands cybercrime opportunities but fundamentally reconfigures the conditions that produce them (Caldwell et al., 2020; King et al., 2020). If the

integrated RAT-STT framework is analytically robust, these transformations should generate observable effects (consequences) extending beyond individual incidents of offending (Farrell & Pease, 2017; Leukfeldt & Yar, 2016; Quibell, 2024; Spyropoulos, 2024). Such consequences are not incidental by-products of technological misuse; they are structural outcomes generated by the interaction between altered opportunity environments and behaviorally transformed actors (Leukfeldt et al., 2017; Maimon & Louderback, 2019). This section therefore analyzes the structural implications of those reconfigured opportunity conditions as they become visible in observable distributions of injury, exposure, and institutional pressure.

1) Victimization as a Structural Outcome

In traditional criminological analysis, victimization is often treated as a contingent outcome resulting from individual exposure or misfortune (Finkelhor & Asdigian, 1996; Schreck et al., 2002; Vakhitova et al., 2015). Under AI-mediated conditions, however, victimization increasingly reflects the systemic properties of digital environments rather than isolated situational encounters (Büchi et al., 2023; Ilievski, 2016; Reyns, 2017; Smith, 2026). Automated targeting, predictive profiling, and persistent interaction mechanisms reshape the distribution of risk across populations, producing patterns of exposure that are structured rather than random (Benbouzid, 2019; De Hert & Lammerant, 2016; Modic & Anderson, 2014; Whitty, 2019).

Interpreted within the RAT framework, these developments intensify the convergence of offenders and suitable targets while simultaneously weakening guardianship capacity (Cohen & Felson, 1979; Pratt et al., 2010; Yar, 2005). AI increases the likelihood of such convergence not only by expanding offender reach but by continuously recalculating target suitability through data analysis (Butkovic et al., 2018; Ekundayo et al., 2024; Pakina et al., 2023). From the perspective of STT, the same conditions reshape behavioral responses, reducing skepticism, increasing compliance, and fostering emotional engagement (Choi, 2025; Jaishankar, 2008; Suler, 2004). Victimization thus emerges as a systemic effect of interacting structural and behavioral processes rather than a function of individual vulnerability alone (Holt & Bossler, 2016; Leukfeldt & Yar, 2016; Van Wilsem, 2011).

2) Expansion and Differentiation of Harm

The reconfiguration of opportunity conditions also alters the nature and distribution of harm (Button & Cross, 2017; Whitty, 2019). AI-mediated offenses frequently produce multidimensional consequences that extend beyond immediate financial loss (Ho et al., 2025; Modic & Anderson, 2015). Psychological distress, reputational damage, relational disruption, and prolonged uncertainty may accompany or even exceed material harms (Buchanan & Whitty, 2014; Gilbert et al., 2025; Kipngetich, 2025). These effects arise in part because technologically mediated interactions blur boundaries between authentic and simulated communication, complicating individuals' ability to assess credibility and intent (Assarut et al., 2019; Sudhakaran & Kshetri, 2026).

More importantly, the scale and persistence of

AI-enabled interactions can amplify these harms. Automated systems may maintain contact over extended periods, increasing emotional investment and deepening perceived relational ties (Button et al., 2014; Pawar et al., 2021; Whitty, 2019). When deception is later revealed, the resulting sense of betrayal or manipulation may be experienced as personally directed rather than structurally produced (Akinbowale et al., 2025; Stajano & Wilson, 2011; Buchanan & Whitty, 2014). This phenomenon illustrates how behavioral mechanisms identified by STT interact with opportunity structures identified by RAT to produce consequences that are both materially and psychologically significant (Ahmad & Thurasamy, 2022; Choi, 2025b; Goldsmith & Brewer, 2014; Jaishankar, 2008; Leukfeldt & Yar, 2016).

3) Redistribution of Risk and Exposure

Another consequence of reconfigured opportunity environments is the redistribution of victimization risk across demographic, social, and situational contexts. Rather than selecting targets at random, AI-enabled systems can identify and prioritize specific user categories based on behavioral indicators, platform activity, or contextual signals (Büchi et al., 2023; De Hert & Lammerant, 2016; Jahan & Mell, 2024). As a result, exposure to cybercrime may become patterned according to algorithmically inferred characteristics rather than traditional criminogenic factors such as geographic proximity or routine physical activities (Benbouzid, 2019; Butkovic et al., 2018; Hayward & Maas, 2020).

This redistribution does not necessarily imply that certain groups are inherently more vulnerable. Instead, it reflects the logic of predictive targeting, in which algorithmic processes generate probabilistic assessments of responsiveness (Arslan, 2023; Berk, 2021; Finkelhor & Asdigian, 1996; Schreck et al., 2002). The implication is that risk is increasingly assigned through technological interpretation rather than determined solely by individual traits. Understanding victimization patterns therefore requires attention to how digital infrastructures classify, sort, and prioritize users within data-driven systems (Eubanks, 2018; Pasquale, 2015, 2019).

4) Institutional Strain and Enforcement Asymmetry

Shifts in opportunity conditions also carry institutional implications, as law enforcement agencies, regulatory authorities, and platform face asymmetries in speed, scale, and adaptability when responding to AI-mediated crime (Brewer et al., 2019; Maimon & Louderback, 2019; Wall, 2024). Automated systems can generate deceptive content more rapidly than detection mechanisms can analyze it, while cross-jurisdictional digital interactions may further complicate attribution and enforcement. (Arnell & Faturoti, 2023; Schaefer & Mazerolle, 2017). These structural asymmetries do not merely hinder criminal investigation; they alter the strategic environment in which both offenders and guardians operate (Dupong & Whelan, 2021; Ekblom, 2017; Lavorgna, 2014).

Within the integrated analytical framework, such asymmetries can be interpreted as manifestations of weakened guardianship capacity (Bossler & Holt, 2009; Reyns, 2017; Williams, 2016). When detection systems struggle to match the pace of automated

offending, the structural balance described by RAT shifts in favor of offenders (Felson & Clarke, 1998; Pratt et al., 2010; Van Wilsem, 2011). At the same time, the behavioral dynamics emphasized by STT may reduce perceived deterrence, as actors interpret enforcement limitations as signals of reduced risk (Al Shamsi et al., 2023; Assarut et al., 2019; Jaishankar, 2008; Suler, 2004). Institutional strain therefore constitutes a systemic outcome of reconfigured opportunity conditions rather than an administrative shortcoming alone.

5) Normalization and Environmental Embedding

AI-mediated opportunity environments also foster the gradual normalization of deceptive interaction. As automated communication becomes more prevalent in digital spaces, distinguishing authentic from artificial engagement may become harder (Hancock & Bailenson, 2021; Varol et al., 2017). Over time, this ambiguity can alter expectations about online interaction, making manipulative or deceptive practices appear less anomalous. When deception becomes embedded within routine digital experience, it may be interpreted as an ordinary feature of the environment rather than as an exceptional event (Comes, 2025; Natale, 2024).

This normalization reflects the interplay of structural and behavioral dynamics. Extensive exposure to automated interaction reshapes how credibility is perceived and assessed (Goldsmith & Brewer, 2014; Stajano & Wilson, 2011), while altered perceptions expand the effectiveness of deceptive strategies (Modic & Anderson, 2015; Wikstrom & Kroneberg, 2022). The resulting feedback loop demonstrates that opportunity environments are not static contexts but evolving systems shaped by technological change and human adaptation (Broadhurst et al., 2021; Leukfeldt et al., 2017).

6) Systemic Interpretation of Cybercrime Outcomes

Taken together, the patterns described above suggest that contemporary cybercrime outcomes are best understood as systemic manifestations of reconfigured opportunity environments (Ekblom, 2017; Romagna & Leukfeldt, 2024; Wilcox et al., 2018). AI modifies the structural conditions under which crime occurs and simultaneously reshapes the behavioral responses of actors within those conditions (Caldwell et al., 2020; Fiorinelli & Zucca, 2025; Fleetwood, 2016; King et al., 2020). The observable consequences—patterns of victimization, differentiated harms, redistributed risk, institutional strain, and normalization of deception—reflect this dual transformation (Aebi et al., 2025; Farrell & Pease, 2017; Leukfeldt & Yar, 2016; Smith, 2026).

This interpretation shifts analytical focus away from individual incidents toward the broader environments in which those incidents become possible (Clarke, 1995; Cohen & Felson, 1979; Lee, 2010; Wortley & Townsley, 2016). It highlights that the significance of AI-mediated cybercrime lies not only in its technological novelty but in its capacity to reorganize the fundamental relationship between opportunity, behavior, and harm (Borgesano et al., 2025; Dupong & Whelan, 2021; Martineau et al., 2023; Miller, 2013). Such a perspective provides the con-

ceptual foundation for assessing the implications of these transformations for theory, governance, and institutional response.

The outcomes examined here demonstrate that AI reshapes cybercrime not only at the level of technique but at the level of systemic consequence. The final section considers the broader theoretical and practical implications of this transformation, including what the integrated framework contributes to criminological analysis and how it may inform responses to digitally mediated crime.

6. Implications and Conclusion

The analysis advanced in this study has argued that AI does not simply introduce new tools for cybercrime but fundamentally transforms the conditions under which such crime becomes possible. Integrating RAT and STT into a single analytical framework shows that contemporary cybercrime is better understood as the product of dynamically reconfigured opportunity environments than as a mere collection of isolated technological offenses. This reconceptualization shifts cybercrime from an incident-centered phenomenon to a systemic one, highlighting the interplay between structural conditions and behavioral processes within digitally mediated environments.

1) Theoretical Implications

The primary contribution of this study is conceptual. Existing criminological approaches to cybercrime have largely adopted single-theory frameworks that foreground either structural opportunity or behavioral transformation at the expense of their interaction (Holt & Bossler, 2016; Maimon & Louderback, 2019; Yar, 2005). While each approach captures important dimensions of digital offending, neither alone adequately explains the co-evolving relationship between technological infrastructure and human action characteristic of AI-mediated environments (Goldsmith & Brewer, 2015; Leukfeldt & Yar, 2016; Wall, 2024). The integrated RAT-STT framework developed here illustrates that structural opportunity and behavioral dynamics should be treated as mutually constitutive rather than analytically separable.

The implications of this reconceptualization extend beyond the present study to criminological theory more broadly. It suggests that technological change should not be approached as an external variable applied to existing models but as a condition capable of reshaping the explanatory architecture of those models themselves (Brantingham & Brantingham, 2018; Felson, 2016; Wikstrom & Kroneberg, 2022). In this sense, AI functions not merely as a contextual factor but as a structural-behavioral modulator that reorganizes the relationship between opportunity, agency, and constraint (Brewer et al., 2019; Opp, 2020; Cullen et al., 2008; Schaefer & Mazerolle, 2017). Recognizing this role allows established theories to be extended rather than replaced, preserving theoretical continuity while accommodating technological transformation.

2) Analytical Implications

Beyond its theoretical contribution, the integrated RAT-STT framework provides a systematic lens for interpreting diverse forms of cybercrime within a sin-

gle analytical structure. Conceptualizing crime as a recursive interaction among offenders, targets, guardians, and technological systems helps explain why AI-mediated offenses often appear scalable, adaptive, and resistant to traditional controls (Caldwell et al., 2020; King et al., 2020; Lee, 2010; McKay & Macintosh, 2024). These characteristics are not anomalies requiring entirely new categories of explanation; they are predictable consequences of environments in which opportunity conditions and behavioral dynamics are continuously reshaped by automated processes.

This perspective also highlights the importance of examining crime at the level of systems rather than incidents (Farrell & Pease, 2017). Individual cases may appear idiosyncratic or technologically novel, yet when analyzed within the integrated framework they reveal common underlying mechanisms (Holt & Bossler, 2016; Maimon & Louderback, 2019). Such an approach encourages comparative analysis across offense types and technological contexts, facilitating cumulative theoretical development as opposed to fragmented case-specific interpretation.

3) Institutional and Policy Implications

Although the present study is conceptual rather than prescriptive, its findings carry important implications for institutional and policy responses to contemporary cybercrime. Above of all, if digital offenses arise from reconfigured opportunity environments, interventions that focus exclusively on individual offenders or isolated incidents are unlikely to address their underlying causes. Effective responses must instead consider how technological infrastructures, platform architectures, and governance arrangements shape opportunity conditions (Dupong & Whelan, 2021; Wall, 2024). Measures that strengthen guardianship capacity, reduce structural asymmetries, or limit exploitability of digital environments may therefore be more effective than strategies oriented solely toward post hoc enforcement (Wortley & Townsley, 2016).

At the same time, the framework suggests that institutional responses should account for behavioral dynamics as well as structural conditions. Efforts to enhance user awareness, reduce susceptibility to manipulation, or increase perceived accountability can complement structural interventions by altering the behavioral context in which opportunities are interpreted and acted upon (Modic & Anderson, 2015; Reyns et al., 2011; Whitty, 2019). Approaches that address only one dimension risk producing adaptive responses in the other, underscoring the need for strategies that engage both simultaneously.

4) Limitations

Several limitations should be acknowledged. First, the framework developed here is theoretical in orientation and is not empirically tested within this article. While this conceptual focus allows the model to remain generalizable across technological contexts, empirical validation will be necessary to assess its explanatory scope and boundary conditions. Second, the analysis centers primarily on digitally mediated environments and therefore does not address how the integrated framework might apply to hybrid forms of crime that combine online and offline components. Third, the rapid evolution of AI tech-

nologies means that specific mechanisms discussed here may change over time, requiring ongoing refinement of theoretical models.

These limitations, however, reflect deliberate analytical choices rather than methodological shortcomings. The central aim of this study has been to clarify underlying conceptual relationships and to advance a framework capable of structuring future inquiry. Empirical research, comparative analysis, and domain-specific applications therefore represent logical extensions of this theoretical foundation.

5) Directions for Future Research

The integrated RAT-STT framework opens several avenues for future research. Empirical studies could examine how specific AI-mediated environments alter opportunity convergence or behavioral response patterns. Comparative analyses might investigate whether different technological architectures produce distinct configurations of structural and behavioral dynamics. Longitudinal research could explore how feedback processes between offenders, guardians, and technological systems evolve over time. Such work would not only test the propositions advanced here but also refine understanding of how digital environments shape crime more broadly. Future research may incorporate case-based, comparative, or data-driven analyses to empirically assess the applicability of the proposed framework across diverse cybercrime contexts.

Interdisciplinary collaboration will be particularly important in this regard. Because AI-mediated crime operates at the intersection of technological design, social interaction, and institutional governance, its analysis benefits from perspectives drawn from criminology, computer science, sociology, police science, law, psychology, and information studies. The framework proposed in this article is intended to support such dialogue by providing a shared conceptual vocabulary for analyzing technologically mediated offending.

7. Conclusion

This article has argued that AI marks not merely a technological development but a structural transformation in the ecology of crime. By integrating Routine Activity Theory and Space Transition Theory, it has demonstrated that contemporary cybercrime can be understood as an emergent outcome of dynamically reconfigured opportunity systems shaped by the interaction of technological infrastructure and human behavior. This perspective clarifies why AI-mediated offenses are increasingly scalable, adaptive, and resistant to traditional control mechanisms, and it highlights the need for analytical approaches that capture the systemic nature of digitally mediated crime.

The significance of this contribution lies not in proposing a new typology or regulatory framework but in offering a conceptual model (framework) capable of explaining how technological change reshapes the fundamental conditions of criminal activity. In doing so, the study seeks to advance criminological understanding of cybercrime while providing a foundation for future theoretical, empirical, and policy-oriented inquiry into crime in the age of AI.

References

Adanyin, A. (2024). AI-Driven Feedback Loops In Digital Technologies: Psychological Impacts On User Behaviour And Well-Being. *ArXiv: Computers and Society*, arXiv: 2411.09706 [cs.CY], 1-14.

Adewopo, V. A. et al. (2025). Comprehensive analytical review of cybercrime and cyber policy in West Africa. *Journal of Electrical Systems and Information Technology*, 12(20), 1-23.

Aebi, M. F. et al. (eds.) (2025). *Understanding Crime Trends in a Hybrid Society: The Digital Draft.* Cham, Switzerland: Springer (SpringerBriefs in Criminology).

Ahmad, R., & Thurasamy, R. (2022). A Systematic Literature Review Of Routine Activity Theory's Applicability In Cybercrimes. *JCSANDM (Journal of Cyber Security and Mobility)*, 11(3), 405-432.

Akinbowale, O. E. et al. (2025). Emerging technologies as a mediating factor between causes of cyberfraud and cyberfraud perpetration in the South African banking industry. *International Journal of Cyber Behavior, Psychology and Learning*, 15(1), 1-19.

Al Fahdi, M. et al. (2016). A suspect-oriented intelligent and automated computer forensic analysis. *Digital Investigation*, 18, 65-76.

Al Shamsi, M. et al. (2023). Space Transition and the Vulnerabilities of the NFT Market to Financial Crime. *Journal of Financial Crime*, 30(6), 1664-1673.

Alder, S. et al. (2024). Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. *ArXiv: Computers and Society*, arXiv: 2408.07892 [cs.CY], 1-63.

Allah Rakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 16(2), 23-54.

Andrejevic. Mark, & Gates, K. (2014). Big Data Surveillance: Introduction. *Surveillance & Society*, 12(2), 185-196.

Apene, O. Z. et al. (2024). Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions. *European Journal of Applied Science, Engineering and Technology*, 2(2), 285-297.

Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime: Why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 37(1), 29-51.

Arslan, S. (2023). The Legal Implications of Predictive Policing Algorithms: Bias, Oversight, and Public Accountability. *Legal Studies in Digital Age*, 2(3), 49-63.

Assarut, Nuttapol et al. (2019). Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. *International Journal of Cyber Criminology*, 13(1), 84-100.

Ayling, Julie. (2011). Criminalizing Organizations: Towards Deliberative Law-making. *Law & Policy*,

33(2), 149-178.

Bello, H. O. (2025). Integrating Behavioral Biometrics And Machine Learning To Combat Evolving Cybercrime Tactics In Financial Systems. *International Journal of Computer Applications Technology & Research*, 14(1), 121-133.

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the U.S. *Big Data & Society*, 6(1), 1-13.

Berk, R. A. (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement. *Annual Review of Criminology*, 4(1), 209-237.

Bociga, D., & Lord, N. (2026). AI and the organisation and control of fraud. In: Smith, R. G. (ed.). *Research Handbook on Fraud and Society*, Chapter 16 (pp. 266-283), Cheltenham, U.K.: Edward Elgar Publishing.

Borgesano, Francesco et al. (2025). AI & Justice: A Systematic Literature Review And Future Research Perspectives On Justice 5.0. *European Journal of Innovation Management*, 28(11), 349-378.

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3(1), 400-420.

Braithwaite, J. (2020). Crime as a Cascade Phenomenon. *International Journal of Comparative and Applied Criminal Justice*, 44(3), 137-169.

Brand, D. (2020). Algorithmic Decision-making and the Law. *JeDEM (e-Journal of e-Democracy and Open Government)*, 12(1), 115-132.

Brantingham, P. L., & Brantingham, P. J. (2018). Environment, Routine, and Situation: Toward a Pattern Theory of Crime. In: Clarke, R. V., & Felson, M. (eds.). *Routine Activity and Rational Choice (Advances in Criminological Theory: Vol. 5)* (1st edn.), Chapter 11 (pp. 259-294), New York: Routledge.

Brayne, S., & Christin, Angèle (2021). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social Problems*, 68(3), 608-624.

Brenner, Susan W. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law and Technology*, 4(1), 1-50.

Brewer, Russell et al. (2019). *Cybercrime Prevention: Theory and Applications*. Cham, Switzerland: Palgrave Macmillan.

Broadhurst, R. (2021). Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace. In: Cornish, P. (ed.). *The Oxford Handbook of Cybersecurity*, Chapter 6 (pp. 89-108), Oxford University Press.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime and Law*, 20(3), 261-283.

Büchi, M. et al. (2023). Making sense of algorithmic profiling: User perceptions on Facebook. *Information, Communication & Society*, 26(4), 809-825.

Burrell, D. N. (2025). The Cyber-psychology and Criminal Psychology of Cyber Identity Theft and Criminal Reach in the Digital Era. *RAIS Journal for Social Sciences*, 9(2), 343-360.

Butkovic, Asmir et al. (2018). Geographic Profiling for Serial Cybercrime Investigation. *Digital Investigation*, 28(4), 176-182.

Butt, U. et al. (2021). Spatio-Temporal Crime Predictions by Leveraging Artificial Intelligence for Citizens Security in Smart Cities. *IEEE Access*, 9, 47516-47529.

Button, M. et al. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, 27(1), 36-54.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. London: Routledge.

Cable, J. et al. (2024). Showing the Receipts: Understanding the Modern Ransomware Ecosystem. *2024 APWG Symposium on Electronic Crime Research* (eCrime), 149-161.

Caianiello, M. (2019). Criminal process faced with the challenges of scientific and technological development. *European Journal of Crime, Criminal Law and Criminal Justice*, 27(4), 267-291.

Caldwell, M. et al. (2020). AI-enabled future crime. *Crime Science*, 9(1), 14-26.

Capurro, R. et al. (2013). *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*. New Jersey (USA) & Lancaster (U.K.): Ontos Verlag.

Čekić, E. (2024). The Impact of AI Tools on Criminal Psychological Profiling. *International Journal of Academic Research in Psychology*, 11(1), 1-13.

Chen, X. et al. (2025). Online Moral Deviance: An Integrative Review of Digital Behaviors. *Frontiers in Psychology*, 16, 1-19.

Cheng, Y. (2023). The Impact of Social Media on Deviance and Crime. *Journal of Education, Humanities and Social Sciences*, 22, 873-877.

Chesney, R., & Citron, D. (2019). Deepfakes and the New Disinformation War. *Foreign Affairs*, 98(1), 147-155.

Chiao, V. (2019). Fairness, Accountability and Transparency: Notes on Algorithmic Decision-Making in Criminal Justice. *International Journal of Law in Context*, 15(2), 126-139.

Choi, Justin Jin-Hyuk (2025). A Study On Profiling Frameworks For Digital Offenders In Transition: Applying Space-Transition Theory (STT). *The Korean Association of Police Science Review* (KAPS), 27(6), 185-222.

Choi, Justin Jin-Hyuk et al. (2025). Applying Routine Activity Theory To Cybercrime: Revisiting 'VIVA' Model. *The Korean Association of Police Science Review* (KAPS), 27(1), 61-90.

Choo, F., & Tan, K. B. (2008). The effect of fraud triangle factors on students' cheating behaviors. In: Schwartz, B. N., & Catanach, A. H. (eds.). *Advances in Accounting Education* (pp. 205-220), Bingley, England: Emerald Group Publishing.

Clarke, R. V. (1995). Situational Crime Prevention. In: Tonry, M. H., & Farrington, D. P. (eds.). *Crime*

and Justice, Vol. 19: Building a Safer Society: Strategic Approaches to Crime Prevention, 91-150, Chicago, IL (USA): The University of Chicago Press.

Cohen, Julie E. (2007). Cyberspace As/And Space. *Columbia Law Review*, 107(1), 210-255.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588-608.

Comes, B. (2025). Blurring the Line: Digital Anonymity, Deception, and the Crisis of Online Authenticity. *Advances in Social Sciences Research Journal*, 12(10), 131-135.

Cullen, F. T. et al. (2008). Gender, Bullying Victimization, and Juvenile Delinquency: A Test of General Strain Theory. *Victims and Offenders*, 3(4), 346-364.

De Hert, P., & Lammerant, H. (2016). Predictive Profiling and its Legal Limits: Effectiveness Gone Forever? In: Van der Sloot, B. et al. (eds.). *Exploring the Boundaries of Big Data* (1st edn.), Chapter 6 (pp. 145-174), London: Routledge.

Do, T. H., & Selvadurai, N. (2025). Future crime: A theoretical foundation for designing effective cybercrime laws in the age of AI and ransomware. *North Carolina Journal of Law and Technology*, 27(1), 91-164.

Dobusch, Leonhard, & Schoeneborn, D. (2015). Fluidity, Identity, and Organizationality: The Communicative Constitution of Anonymous. *Journal of Management Studies*, 52(8), 1005-1035.

Dupong, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, 54(1), 76-92.

Dzuba, C. (2025). Artificial intelligence in social engineering: A literature review through the lens of routine activity theory. *Issues in Information Systems*, 26(2), 452-465.

Ejjami, R. (2024). AI-driven justice: Evaluating the impact of artificial intelligence on legal systems. *International Journal for Multidisciplinary Research*, 6(3), 145-168.

Ekblom, Paul. (2017). Technology, Opportunity, Crime and Crime Prevention - Current and Evolutionary Perspectives. In: Leclerc, B., & Savona, E. U. (eds.). *Crime Prevention in the 21st Century: Insightful Approaches for Crime Prevention Initiatives*, Chapter 19 (pp. 319-344), New York: Springer.

Ekundayo, F. et al. (2024). Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. *International Journal of Research Publication and Reviews*, 5(11), 5934-5948.

Eubanks, Virginia. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St Martin's Press.

Faqir, R. S. A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, 17(2), 77-94.

Farrell, G., & Pease, K. (2017). Preventing repeat and near repeat crime concentrations. In: Tilley, N., & Sidebottom, A, (eds.). *The Handbook of Crime Prevention and Community* (2nd edn.). Chapter

7 (pp. 319-344), London: Routledge.

Felson, M. (2016). The Routine Activity Approach. In: Wortley, R., & Townsley, M. (eds.). *Environmental Criminology and Crime Analysis* (2nd edn.), Chapter 4 (pp. 87-97), London: Routledge.

Felson, M., & Clarke, R. V. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. Police Research Series: Paper 98. Home Office, U.K.

Finkelhor, D., & Asdigian, N. (1996). Risk Factors for Youth Victimization: Beyond a Lifestyles/Routine Activities Theory Approach. *Violence and Victims*, 11(1), 3-19.

Fiorinelli, G., & Zucca, M. V. (2025). Regulating AI to Combat Tech-Crimes: Fighting the Misuse of Generative AI for Cyber Attacks & Digital Offenses. *Technology and Regulation*, TILTing 2024 Special Issue, 247-262.

Fleetwood, J. (2016). Narrative habitus: Thinking through structure/agency in the narratives of offenders. *Crime, Media, Culture: An International Journal*, 12(2), 173-192.

George, M. M. et al. (2023). When "who I am" is under threat: Measures of threat to identity value, meanings, and enactment. *Journal of Applied Psychology*, 108(12), 1952-1978.

Gilbert, C. et al. (2025). Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity. *International Journal of Multidisciplinary Research and Publications* (IJMRAP), 7(10), 87-104.

Goldsmith, A., & Brewer, R. (2014). Digital Drift and the Criminal Interaction Order. *Theoretical Criminology*, 19(1), 112-130.

Graham, R., & Triplett, R. (2017). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, 38(12), 1371-1382.

Granic, I., & Patterson, G. R. (2006). Toward a comprehensive model of antisocial development: A dynamic systems approach. *Psychological Review*, 113(1), 101-131.

Groff, E. R. (2007). 'Situating' Simulation to Model Human Spatio-Temporal Interactions: An Example Using Crime Events. *Journal Transactions in GIS*, 11(4), 507-530.

Haley, P., & Burrell, D. N. (2025). Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety. *Law, Economics and Society*, 1(1), 46-59.

Hancock, J. T., & Bailenson, J. N. (2021). The Social Impact of Deepfakes. *Cyberpsychology, Behavior, and Social Networking*, 24(3), 149-152.

Hancock, Jeffrey T. (2009). Digital deception: Why, when and how people lie online. In: Joinson, A. et al. (eds). *Oxford Handbook of Internet Psychology*, Oxford Handbooks Online: Oxford University Press.

Hayward, K. J., & Maas, M. M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture: An International Journal*, 17(2), 209-233.

Hipp, John R. (2016). General Theory of Spatial Crime Patterns. *Criminology*, 54(4), 653-679.

Ho, Shuyuan M. et al. (2025). Synthetic Lies, Digital Truths: A Systematic Review of Computer-Mediated Deception Research in the Era of AI and Deepfakes. *The 46th International Conference on Information*

Systems (ICIS) Proceedings, 1-17.

Hollis-Peel, M. E. et al. (2011). Guardianship for Crime Prevention: A Critical Review of the Literature. *Crime Law and Social Change*, 56(1), 53-70.

Holt, T. J., & Bossler, A. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses* (1st edn.). London: Routledge.

Homeland Security. (2024). *Impact of Artificial Intelligence (AI) on Criminal and Illicit Activities*. The 2024 Public-Private Analytic Exchange Program. The Department of Homeland Security, USA.

Hughes, J., & Hutchings, A. (2023). Digital Drift and the Evolution of a Large Cybercrime Forum. *2023 IEEE European Symposium on Security and Privacy Workshops*, 1-11.

Huseynov, F., & Ozdenizci Kose, B. (2022). Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development*, 40(2), 298-318.

Igba, E. et al. (2025). Synthetic Data Generation Using Generative AI to Combat Identity Fraud and Enhance Global Financial Cybersecurity Frameworks. *International Journal of Scientific Research and Modern Technology* (IJSRMT), 4(2), 1-19.

Ilievski, A. (2016). An Explanation of the Cybercrime Victimisation: Self-control & Lifestyle/Routine Activity Theory. *Innovative Issues and Approaches in Social Sciences*, 9(1), 30-47.

Jabir, R. et al. (2025). Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. *AI*, 6(8), 1-29.

Jahan, N., & Mell, J. (2024). Unraveling the Tapestry of Deception and Personality: A Deep Dive into Multi-Issue Human-Agent Negotiation Dynamics. In: *Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems*, 916-925.

Jahankhani, H. et al. (2014). Cyber crime Classification and Characteristics. In: Akhgar, B. et al. (eds). *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Chapter 12 (pp. 149-164), Waltham, MA (USA): Syngress.

Jaishankar, K. (2008), Space Transition Theory of Cyber Crimes. In: Schmalleger, F., & Pittaro, M. (eds.). *Crimes of the Internet*, Chapter 14 (pp. 283-301), New Jersey: Prentice Hall/Pearcon.

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities 1. *International Journal of Cyber Criminology*, 4(1/2), 26-31.

Jaishankar, K. (2019). Cyber Criminology and Space Transition Theory: Contribution and Impact. *The 6th International Report on Crime Prevention and Community Safety: Preventing Cybercrime,* 100-110, Montral, Quebec (Canada): International Centre for the Prevention of Crime.

Karnouskos, S. (2020). Artificial Intelligence in Digital Media: The Era of Deepfakes. *IEEE Transactions on Technology and Society*, 1(3), 138-147.

Karunamurthy, A. et al. (2023). Human-in-the-Loop Intelligence: Advancing AI-Centric Cybersecurity

for the Future. *Quing International Journal of Multidisciplinary Scientific Research & Development,* 2(3), 20-43.

Katyal, N. K. (2002). Architecture as crime control. *The Yale Law Journal*, 111(5), 1039-1139.

Kavish, N., & Boutwell, B. (2018). The unified crime theory and the social correlates of crime and violence: Problems and solutions. *Journal of Criminal Psychology*, 8(4), 287-301.

Kigerl, Alex. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), 470-486.

King, T. C. et al. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, 26(1), 89-120.

Kipngetich, A. (2025). A review of online scams and financial frauds in the digital age. *GSC Advanced Research and Reviews*, 22(01), 302-329.

Kleemans, E. R. et al. (2012). Organized crime, situational crime prevention and routine activity theory. *Trends in Organized Crime*, 15, 87-92.

Kolade, T. M. et al. (2024). Artificial Intelligence and Information Governance: Strengthening Global Security, Through Compliance Frameworks, and Data Security. *Asian Journal of Research in Computer Science*, 17(12), 36-57.

Koning, Luka et al. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, 30(3), 443-479.

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, 44(6), 1-13.

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior*, 28(2), 434-443.

Lavorgna, A. (2014). Internet-mediated drug trafficking: Towards a better understanding of new criminal dynamics. *Trends in Organized Crime*, 17(4), 250-270.

Lavorgna, A., & Ugwudike, P. (2021). Datafication Revolution in Criminal Justice: An Empirical Exploration of Frames Portraying Data-Driven Technologies for Crime Prevention and Control. *Big Data & Society*, 8(2), 1-15.

Lazarus, S. et al. (2025). Cybercrime against senior citizens: Exploring ageism, ideal victimhood, and the pivotal role of socioeconomics. *Security Journal*, 38(1), 1-23.

Lee, Daniel R. (2010). Understanding and Applying Situational Crime Prevention Strategies. *Criminal Justice Policy Review*, 21(3), 263-268.

Leukfeldt, E. R. et al. (2017). Origin, Growth and Criminal Capabilities of Cybercriminal Networks: An International Empirical Analysis. *Crime, Law and Social Change*, 67(1), 39-53.

Leukfeldt, E. R., & Jansen, J. (2019). Financial cybercrimes and situational crime prevention. In: Leukfeldt,

E. R., & Holt, T. J. (eds.). *The Human Factor of Cybercrime*, Chapter 10 (pp. 216-239), London: Routledge.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263-280.

Lewis, S. & Lewis, D. A. (2011). Digitalizing Crime Prevention Theories: How Technology Affects Victim & Offender Behavior. *International Journal of Criminology and Sociological Theory*, 4(2), 756-769.

Maimon, D., & Browning, C. R. (2012). Adolescents' Violent Victimization in the Neighbourhood: Situational and Contextual Determinants. *The British Journal of Criminology*, 52(4), 808-833.

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, 2(1), 191-216.

Malatji, M., & Tolah, A. (2024). Artificial intelligence cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*, 5(2), 883-910.

Martineau, M. et al. (2023). A Comprehensive Framework For Cyber Behavioral Analysis Based On A Systematic Review Of Cyber Profiling Literature. *Forensic Sciences*, 3(3), 452-477.

McKay, C., & Macintosh, K. (2024). Remote Criminal Justice and Vulnerable Individuals: Blunting Emotion and Empathy? *Tilburg Law Review*, 29(2), 125-143.

McMillon, D. et al. (2014). Modeling the Underlying Dynamics of the Spread of Crime. *PLoS ONE,* 9(4), 1-22.

Mead, G., & Neves, B. B. (2018). Recursive Approaches to Technology Adoption, Families, and the Life Course: Actor Network Theory and Strong Structuration Theory. In: Neves, B. B., & Casimiro, C. (eds.). *Connecting Families?: Information & Communication Technologies, Generations, and the Life Course*. Chapter 3 (pp. 41-57), Bristol, U.K.: Polity.

Michael, Z., & Brewer, N. (2025). Detecting criminal intent in social interactions: The influence of autism and theory of mind. *Law and Human Behavior*, 49(1), 89-107.

Miller, J. (2013). Individual Offending, Routine Activities, and Activity Settings: Revisiting the Routine Activity Theory of General Deviance. *Journal of Research in Crime and Delinquency*, 50(3), 390-416.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy*, 13(5), 99-103.

Mokoena, Thabo et al. (2023). Cybercrime Prosecution in the Metaverse: Evidentiary and Jurisdictional Challenges. *Legal Studies in Digital Age*, 2(1), 53-67.

Natale, S. (2024). Digital media and the banalization of deception. *Convergence: The International Journal of Research into New Media Technologies*, 31(2), 1-18.

Norouzi, Y. (2022). Spatial, Temporal, and Semantic Crime Analysis Using Information Extraction From

Online News. *The 8th International Conference on Web Research* (ICWR), 40-46.

Norris, G. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, 34(3), 231-245.

Opp, Karl-Dieter. (2020). *Analytical Criminology: Integrating Explanations of Crime and Deviant Behavior* (1st edn.). London: Routledge.

Pakina, A. K. et al. (2023). AI-Generated Synthetic Identities in Fin Tech: Detecting Deep fakes KYC Fraud Using Behavioral Biometrics. *IOSR Journal of Computer Engineering*, 25(3), 26-37.

Paris, B. (2021). Configuring Fakes: Digitized Bodies, the Politics of Evidence, and Agency. *Social Media + Society*, 7(4), 1-13.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard University Press.

Pasquale, F. (2019). A Rule Of Persons, Not Machines: The Limits Of Legal Automation. *The George Washington Law Review*, 87(1), 1-55.

Pawar, S. et al. (2021). Cyber Crime, Cyber Space and Effects of Cyber Crime. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 7(1), 210-241.

Peeters, R., & Schuilenburg, M. (2018). Machine justice: Governing security through the bureaucracy of algorithms. *Information Polity*, 23(3), 267-280.

Porcedda, M. G., & Wall, D. S. (2019). Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk Hack. *Proceedings of 2019 IEEE European Symposium on Security and Privacy Workshops: WACCO 2019 (1st Workshop on Attackers and Cyber-Crime Operations)*, 443-452.

Pratt, Travis C. et al. (2010). The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly*, 27(6), 765-802.

Quibell, J. (2024). Towards 'in-situ' Psychological Profiling of Cybercriminals Using Dynamically Generated Deception Environments. *ArXiv,* arXiv: 2405.11497, 1-16.

Rashid, M. et al. (2025). The Influence of Social Media on Criminal Behaviour and Public Perception of Crime. *Journal for Social Science Archives*, 3(4), 309-325.

Reyns, B. W. (2017). Routine Activity Theory and Cybercrime: A Theoretical Appraisal and Literature Review. In: Steinmetz, K., & Nobles, M. R. (eds.). *Technocrime and Criminological Theory*, Chapter 3 (pp. 35-54), New York: Routledge.

Reyns, Bradford W. et al. (2011). Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, 38(11), 1149-1169.

Rohozinski, R., & Spirito, C. (2026). Weaponising AI: The New Cyber Attack Surface. *Survival*, 68(1), 7-18.

Romagna, M., & Leukfeldt, R. E. (2024). Social Opportunity Structures in Hacktivism: Exploring Online

and Offline Social Ties and the Role of Offender Convergence Settings in Hacktivist Networks. *Victims & Offenders*, 19, 1-23.

Rosenberg, L. (2023). Generative AI as a dangerous new form of media. *Proceedings of the 17th International Multi-Conference on Society, Cybernetics and Informatics* (IMSCI 2023), 165-170.

Rossy, Q., & Ribaux, O. (2020). Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. *European Journal on Criminal Policy and Research*, 26(3), 335-356.

Rostami, M., & Navabinejad, S. (2023). Artificial empathy: User experiences with emotionally intelligent chatbots. *AI and Tech in Behavioral and Social Sciences*, 1(3), 19-27.

Saeed, S. et al. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, 23(15), 1-20.

Salehi, K. et al. (2025). Artificial Intelligence and the Future of International Law and Power. *Journal of World Sociopolitical Studies*, 9(4), 923-958.

Schaefer, L., & Mazerolle, L. (2017). Putting process into routine activity theory: Variations in the control of crime opportunities. *Security Journal*, 30(1), 1-24.

Schiliro, F. (2024). From Crime to Hypercrime: Evolving Threats and Law Enforcement's New Mandate in the AI Age. *ArXiv: Computers and Society*, arXiv: 2411.10995 [cs.CY], 1-28.

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(324), 1-23.

Schreck, C. J. et al. (2002). A Study of Individual and Situational Antecedents of Violent Victimization. *Justice Quarterly*, 19(1), 159-180.

Selvadurai, N. (2025). Advancing Lawful AI through Compliance by Design. *Computer & Telecommunications Law Review*, 31(2), 35-38.

Shang Y. et al. (2023). Theoretical Basis and Occurrence of Internet Fraud Victimisation: Based on Two Systems in Decision-Making and Reasoning. *Frontiers in Psychology*, 14, 1-14.

Sharma, A. et al. (2025). The Rise of AI-Generated Synthetic Identities: A New Frontier in Social Media. *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*, 13(2), 1-11.

Shetty, Sanaika et al. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. *International Journal of Cybersecurity Intelligence & Cybercrime*, 7(2), 28-53.

Smith, R. G. (ed.) (2026). *Research Handbook on Fraud and Society*. Cheltenham, U.K.: Edward Elgar Publishing.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and Virtual Offender Convergence Settings. *Trends in Organized Crime*, 15(2-3), 111-129.

Spyropoulos, F. (2024). New Approaches to Researching AI Crime: Institutionalization of Digital

Criminology. *Journal of Digital Technologies and Law*, 2(3), 636-656.

Stajano, Frank, & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, 54(3), 70-75.

Sudhakaran, S., & Kshetri, N. (2026). AI Agents vs. Human Investigators: Balancing Automation, Security, and Expertise in Cyber Forensic Analysis. *The 21st International Conference on Cyber Warfare and Security* (ICCWS 2026). arXiv: 2601.14544 [cs.CR], 1-10.

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, 7(3), 321-326.

Sullivan, G. (2022). Law, technology, and data-driven security: Infra-legalities as method assemblage. *Journal of Law & Society*, 49(S1), S31-S50.

Tolosana, Ruben et al. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, 64, 131-148.

Treleaven, Philip et al. (2023). The Future of Cybercrime: AI and Emerging Technologies Are Creating a Cybercrime Tsunami. SSRN Electronic Journal (https://ssrn.com/abstract=4507244).

United Nations Office on Drugs and Crime (UNODC). (2025). *Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence (AI) in the cybercrime landscape of Southeast Asia*. Cybercrime Technical Brief Series. Bangkok, Thailand: Regional Office for Southeast Asia and the Pacific, UNODC.

Vakhitova, Z. I. (2025). Cyber-Routine Activity Theory. In: Pontell, H. N. (ed.). *Oxford Research Encyclopedia of Criminology and Criminal Justice in 2025*, New York & Oxford: Oxford University Press.

Vakhitova, Z. I. et al. (2015). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice,* 32(2), 169-188.

Van der Wagen, W., & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *The British Journal of Criminology*, 55(3), 578-595.

Van Elteren, Casper et al. (2024). Criminal organizations exhibit hysteresis, resilience, and robustness by balancing security and efficiency. *Scientific Reports*, 14, 1-11.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, 8(2), 115-127.

Varol, Onur et al. (2017). Online Human-Bot Interactions: Detection, Estimation, and Characterization. *Proceedings of the International AAAI Conference on Web and Social Media*, 1-11.

Velutharambath, A. et al. (2025). What if Deception Cannot be Detected? A Cross-Linguistic Study on the Limits of Deception Detection from Text. *Computer Linguistics*, arXiv: 2505.13147 [cs.CL], 1-53.

Wall, D. S. (2024). *Cybercrime: The Transformation of Crime in the Information Age* (2nd edn.).

Hoboken, NJ (USA): Polity.

Ward, T., & Durrant, R. (2011). Evolutionary psychology and the rehabilitation of offenders: Constraints and consequences. *Aggression and Violent Behavior*, 16(5), 444-452.

Wen, R., & Miura, A. (2025). Online disinhibition is not a master key: An examination of online disinhibition mechanisms. *Internet Research*, 35(7), 52-70.

Weulen Kranenbarg, M. et al. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology*, 18(3), 386-406.

Whitty, Monica T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277-292.

Wikstrom, Per-Olof H., & Kroneberg, C. (2022). Analytic Criminology: Mechanisms and Methods in the Explanation of Crime and its Causes. *Annual Review of Criminology*, 5, 179-203.

Wilcox, Pamela et al. (2018). *Criminal Circumstance: A Dynamic Multicontextual Criminal Opportunity Theory* (2nd edn.). New York: Routledge.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *The British Journal of Criminology*, 56(1), 21-48.

Willison, R. A., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, 15(4), 403-414.

Wisnubroto, A., & Tegnan, H. (2025). Preventing AI Crime Towards A New Legal Paradigm:: Lessons From United States. *Journal of Human Rights, Culture and Legal System*, 5(2), 630-658.

Wortley, R. K., & Townsley, M. (2016). Environmental Criminology and Crime Analysis: Situating the Theory, Analytic Approach and Application. In: Wortley, R. K., & Townsley, M. (eds). *Environmental Criminology and Crime Analysis* (2nd edn.). Chapter 1 (pp. 1-26), London: Routledge.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407-427.

Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and Society* (4th edn.). London: SAGE Publications.

Yeboah-Ofori, Abel, & Opoku-Boateng, F. (2023). Mitigating Cybercrimes In An Evolving Organizational Landscape. *Continuity & Resilience Review*, 5(1), 53-78.

Završnik, A. (2021). Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings. *European Journal of Criminology*, 18(5), 623-642.

Zhou, Y. et al. (2024). Meta-crime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, 19(3), 419-439.

Zuboff, Shoshana. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

인공지능 시대의 사이버범죄 분석을 위한 RAT-STT(일상활동이론-공간전이이론) 통합 이론 모형

블라데미르 콩고,
최 진 혁

치안대학원 수사학과 박사과정 / 앙골라 경찰,
경찰대학교 법학과 교수 / 치안대학원 수사학과장

인공지능(AI) 기술의 확산은 디지털 환경을 근본적으로 변화시키며, 범죄가 발생하는 조건 자체를 재구성하고 있다. 기존 연구는 기술의 발전이 범죄 수법에 미치는 영향에 주로 주목해 왔으나, 인공지능이 범죄 기회 구조 자체를 어떻게 변화시키는지에 대한 이론적 분석은 상대적으로 부족하였다. 이에 주목하여 이 연구는 일상활동이론(Routine Activity Theory)과 공간전이이론(Space Transition Theory)을 통합한 분석 틀(Framework)을 제시하여, 인공지능 매개 환경에서 구조적 기회 조건과 행태적 역동성이 어떻게 상호작용하는지를 설명한다. 여기서 제안된 통합 프레임워크는 인공지능을 단순히 범죄에 활용되는 도구가 아니라 범죄의 기회 구조와 행위 조건을 동시에 변화시키는 체계적 조절 요인으로 개념화한다. 이를 통해 현대 사이버범죄는 개별 기술 집약적인 범죄의 양태(樣態)가 아니라 동적으로 재구성된 기회 환경의 산물로 이해되어야 함을 논증한다. 이 연구는 기술 변화와 범죄 발생 간의 분석적 관계를 명확히 하려는 동시에, 다양한 디지털 범죄 현상을 설명할 수 있는 통합 개념 모형을 제시함으로써 사이버범죄 관련 학술 분야의 발전에 기여하려는 것이다. 이 논문은 실증 분석이나 규범적 정책 제안을 목적으로 하지는 않으며, 인공지능 시대에서 사이버범죄 연구를 위한 개념적 토대를 제공하는 데 그 궁극적 목표가 있다.

주요어: 인공지능(AI), 사이버범죄, 범죄 기회, 일상활동이론(RAT), 공간전이이론(STT), 기회 구조, 통합 개념 모형(프레임워크)