International Journal of Cybersecurity Intelligence & Cybercrime

Volume 7 | Issue 2 Article 4

9-16-2024

Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimization in the Digital Realm

Smith. (2024). *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(2), 54-70.

Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimization in the Digital Realm

Troy Smith*, Ph.D., Targeted Evidence-Based Research Solutions, Trinidad and Tobago.

Abstract:
This article introduces the Integrated Model of Cybercrime Dynamics (IMCD), a novel theoretical framework for examining the complex interplay between individual characteristics, online behavior, environmental factors, and outcomes related to cybercrime offending and victimization. The model incorporates key concepts from existing theories, empirical evidence, and interdisciplinary perspectives to provide a comprehensive framework. In contrast to traditional criminological theories, the proposed model integrates concepts from multiple disciplines to offer a holistic framework that captures the complexity of cybercrime and specifically caters to the uniqueness of cyberspace. The article will provide a detailed overview of the conceptual model, its theoretical underpinnings drawing from criminology and victimology, empirical support for the key components and relationships. The article will conclude by discussing the significance of the IMCD for advancing cybercrime theory, guiding future research, informing prevention/intervention efforts, and ultimately combating the growing challenge of cybercrime in the digital age.

Introduction

Cybercrime has emerged as a serious challenge for individuals, organizations and nations in the increasingly digital and interconnected contemporary world. However, traditional criminological theories, developed to explain offline or physical crimes, do not fully capture the unique characteristics and dynamics of cybercrime (Jaishankar, 2008). Scholars argue that cybercrime requires a distinct theoretical framework that can account for the online environment, technological advancements and the social and psychological factors at play (Bossler & Berenblum, 2019; Leukfeldt & Holt, 2019; Ngo & Jaishankar, 2017). Existing crime theories were generally crafted and adopted prior to the advent of cyberspace and while traditionally generalizable they have not been able to be fully adapted to the unique and ever-evolving nature of cybercrime. Applying traditional crime theories to cybercrime in some cases can be akin to using "Horse law" to govern automobiles, illustrating the mismatch between outdated theories and contemporary phenomena (Ngo & Jaishankar, 2017).

For instance, routine activities theory (RAT) is arguably one of the most influential criminological theories drawn upon in attempts to explain cybercrime over the last decade (Williams, 2016; Yar, 2005). Originally formulated by Cohen and Felson (1979), RAT focuses on how the spatiotemporal convergence of likely offenders, suitable targets and the absence of capable guardianship can create criminal opportunities. In cybercrime scholarship, RAT provides a starting point for considering how cybercrime events emerge from the online interactions, activities and interfaces that bring together offenders and victims in digital spaces where guardianship is lacking (Yar, 2005). However, critics argue that RAT fails to account for the unique characteristics of the virtual territory where cybercrime occurs, particularly its unique spatiotemporal dimensions (Bossler & Holt, 2010a; Smith & Stamatakis, 2020). Nor does it fully capture the power of anonymity and permanence to decentralize offenders and targets (Jaishankar, 2008; Williams, 2016). Additionally, the assumptions of ratio-

*Corresponding author
Troy Smith*, Ph.D., Department of Criminology & Public Safety, The University of Trinidad and Tobago, Tamana In-Tech Park, Wallerfield, Arima 301776, Trinidad and Tobago.
Email: troy.smith078@we.utt.edu.tt

nal decision-making and opportunity in RAT do not adequately capture the complexities of cybercriminal behavior (Ngo & Paternoster, 2011).

Furthermore, the premise of rational choice in individual decision-making and utility maximization by both offenders and victims does not fully encompass the social and environmental factors that influence cybercrime (van Wilsem, 2013). RAT gives inadequate attention to the personality traits, social learning, and motivations that give rise to offender decision-making. Social learning theory (SLT) addresses some gaps in RAT by emphasizing how social contexts, norms and modeled behaviors shape offending (Akers et al., 2021; Bandura, 1977). SLT highlights mechanisms of differential association, definitions favorable or unfavorable to crime, differential reinforcement for prosocial or antisocial conduct and imitation. In online settings, this helps explain how social media subcultures and online normalization of certain acts can increase cybercrime. However, SLT does not thoroughly address predispositions, individual gratifications, or situational drivers. Other theories, such as Differential Association Theory and Strain Theory, have been applied to cybercrime to some extent. However, they often focus on individual-level factors and may not sufficiently consider the unique characteristics of the online environment, including the role of technology, anonymity and the global interconnectedness of cybercrimes (Yar & Leukfeldt, 2016). These gaps in existing theories necessitate the development of a new cybercrime theory or framework that can offer a more comprehensive explanation of cybercriminal behavior.

Scholars engaging in empirical studies have elucidated not only concerns regarding traditional theories but potential paths to improving the assessment of cybercrime and online behaviors. Bossler and Berenblum (2019) explored individual and situational factors contributing to cybercrime victimization, emphasizing the importance of understanding online behavior and protective measures. Their work supported the inclusion of concepts such as online behavior and guardianship in the proposed theory. They argued that the application of traditional theories to cybercrime should be complemented by an understanding of the online context and the specific mechanisms that influence victimization. Yar and Leukfeldt (2016) discussed the challenges posed by cybercrime to criminology and advocated for a comprehensive approach to studying cybercrime. They highlighted the need to consider the role of technology, the global nature of cybercrimes, and the interplay between various factors in understanding cybercriminal behavior. These studies, along with others in the field, highlight the need for a theoretical framework that integrates personality, gratification, social norms, online behavior, guardianship and the type of cyberattack to provide a comprehensive understanding of cybercrime dynamics (Bossler & Berenblum, 2019; Bossler & Holt, 2010b; Holt & Bossler, 2014a; Leukfeldt & Holt, 2019; Ngo & Jaishankar, 2017; Ngo & Paternoster, 2011; Yar & Leukfeldt, 2016).

This article notes the constraints inherent in conventional theories and puts forth an Integrated Model of Cybercrime Dynamics (IMCD) that accounts for the complex dynamics of offending and victimization in digital spaces. The model synthesizes concepts from across criminology, psychology and computer science to provide a holistic conceptualization of the determinants and outcomes related to diverse forms of cybercrime. These relationships are contextualized by the determinants of behavior and identified by personality, gratification, social norms, online behavior, guardianship and cyber-attacks. To justify and explain the model a systematic approach is taken. First, the theoretical origins of the model drawing from RAT, SLT and the criminology of personality development, motivation, space and opportunity are outlined. Second, each key component of the model including personality traits, gratifications, social norms, online be haviors, guardianship factors and cyber-attacks is explained in depth. Third, the relationships between the compon-

ents are described to map the interconnected pathways through which personal dispositions and social contexts coalesce situationally to enable cybercrime events when guardianship is lacking. Finally, testable propositions derived from the conceptual framework are presented along with implications for future research programs. Overall, this integrated model provides a comprehensive yet parsimonious framework for disentangling the complex sociotechnical dynamics underlying cybercrime.

Conceptual Framework

Cybercrime, characterized by illegal activities conducted in the digital realm, poses unique challenges for understanding offending, victimization, and the factors that contribute to criminal behavior in cyberspace. This section aims to provide a detailed conceptual framework that synthesizes relevant concepts from multiple theories into a comprehensive framework attuned to cybercrime.

Two theories lay the foundation of the model, namely the RAT and SLT. The model aligns with RAT (Cohen & Felson, 1979) by recognizing the importance of individual characteristics, such as vulnerability and guardianship, in cybercrime victimization. Thus, RAT provides the initial scaffolding but not a comprehensive framework by itself. SLT offers valuable insights into online socialization and cybercrime in its explanation of mechanisms of differential association with prosocial versus deviant groups, differential reinforcement for antisocial conduct and imitation of modeled behaviors in shaping offending (Holt, 2007).

For example, online normalization of piracy or hacking within deviant subcultures illustrates definitions favorable to cybercrime. Reinforcement from online peer interactions can encourage or discourage cyberbullying. Differential association with technical skill groups provides opportunities to learn tools later used to compromise target systems. However, SLT does not thoroughly address individual personality differences, motivations, or guardianship factors as additional contributors. Integrating SLT concepts is beneficial but insufficient alone to constitute a comprehensive cybercrime framework.

To address limitations of RAT and SLT, the integrated model draws upon and synthesizes additional theoretical concepts from criminology related to personality development, motivation, the role of space and opportunity. Essentially it introduces situational precipitators that shape criminal decision-making within crime opportunities. Thus, elucidating how cyber offending manifests from technical, social and psychological circumstances despite diversity in motives.

First, personality provides insight into stable individual differences in traits like impulsiveness, sensation-seeking, aggression, empathy, narcissism and self-control that empirically link to cybercrime involvement (Ševčíková, 2016; van Wilsem, 2013). Second, the model accounts for the importance of an offender's motivation in the determination of the method of attack, the target of attack and the specificity of who or what is targeted. Uses and gratification theory is used to explain behavior driven by the desire for needs affordance, where needs can be financial gain, sexual gratification, peer-esteem, notoriety or ideological goals that incentivize cybercrime (Holt, 2010). Third, criminological scholarship recognizes that the nature of online spaces empowers criminal decisions because of anonymity, lack of surveillance, interpersonal distancing and the asymmetric nature of cyber-attacks (Jaishankar, 2008; Yar & Leukfeldt, 2016). Finally, concepts of crime opportunity from situational action theory shed light on how motives, skills and tools converge to enable offenders to carry out attacks based on circumstances (Yar & Leukfeldt, 2016). It recognizes

that for a threat to exist an offender must have the required capabilities to exploit vulnerabilities in addition to intent for a crime event to occur.

In summary the proposed model underscores that cyber threat actors interact in a shared online dynamic space (virtual territory) which transcends geographical limitations. Consequently, investigating, preventing and addressing cybercrime requires understanding this complex global environment. The theory also acknowledges that technological infrastructure shapes cybercrime landscapes. Variations in connectivity, digital literacy and resource availability impact offenders' capabilities and the cyber-attacks/threat vectors they utilize. Recognizing the role of infrastructure enhances comprehension of contextual factors that enable cybercriminality. The following sections detail each component and relationship in this conceptual model and present the empirical support for the viability of this integration in explaining diverse forms of cybercrime offending and victimization.

Description of Model Components

Personality

A robust body of empirical research has found significant associations between personality traits and involvement in different forms of cybercrime, whether as offenders or victims (Craker & March, 2016; Ševčíková, 2016; van Wilsem, 2013). Personality represents relatively stable patterns of thoughts, emotions and behaviors that show consistency across situations and over the lifespan. Traits related to impulsivity, risk-taking, antisocial tendencies, negative emotionality, narcissism and low self-control are linked frequently to cybercrime through various pathways (Ševčíková, 2016; van Wilsem, 2013). For example, studies have demonstrated the influence of online behavior, such as self-disclosure and trust in unknown individuals, on an individual's vulnerability to cybercrime victimization (Bossler & Berenblum, 2019; Holt & Bossler, 2014a). This suggests that certain personality traits may predispose individuals to engage in deviant behaviors or seek gratification through illegal activities in cyberspace. Thus, the incorporation of personality as a central component of the cybercrime theory enhances the understanding of the individual-level factors that contribute to offending behavior.

Impulsivity reflects acting rashly based on the spur of the moment without deliberation regarding long-term consequences (Jones & Paulhus, 2011). Impulsive individuals seek immediate gratification and excitement while deficient in thinking through potential risks or harms before acting. This trait associates with more frequent online risk-taking such as sharing intimate photos, disclosing sensitive information, or downloading unknown files that can enable cybercrime victimization (van Wilsem, 2013). Impulsiveness also predicts greater perpetration of harassing social media posts, hacking behaviors and malicious online communications among adolescents and adults (Craker & March, 2016).

Sensation-seeking refers to a preference for novel and intense physical, social and emotional experiences even if illegal or dangerous (Jones & Paulhus, 2011). High sensation-seekers show diminished sensitivity to harm and pursue excitement and thrills through cyberstalking, trolling, hacking and viewing illicit content online. Such risk-taking is reinforced by online anonymity.

Antisocial tendencies include feelings of comfort when violating norms, manipulativeness, lack of empathy and aggression (Jones & Paulhus, 2011). These traits reflect deficits in self-regulation and conscience. A willingness to deceive, exploit and harm others online maps onto cyberbullying, fraud, property theft, and sexual predation. Antisocial individuals may also derive gratification from causing disruption through hacking, data theft, or spreading viruses.

Negative emotionality includes proneness to anxiety, irritability, and moodiness (Jones & Paulhus, 2011). These traits can increase susceptibilities to phishing, malware and monetary fraud by clouding judgment. Negative urgency reflecting impulsive reactions to distress is specifically predictive of cybercrime victimization (van Wilsem, 2013). Anger and hostility also link to aggressive (retaliatory) cybercrime.

Narcissism combines egocentrism, feelings of grandiosity, dominant behavior, exhibitionistic tendencies and exploitativeness in relating to others (Jones & Paulhus, 2011). Cyberbullying, sexual harassment, spreading false information, doxing and coercing others online can fulfill narcissistic desires for power, control and status. Narcissists may also post inappropriate content that increases vulnerability. Low self-control highlights deficits in regulating impulses, emotional reactions, desires and behaviors that can lead to criminality (Gottfredson & Hirschi, 1990). Reduced self-monitoring and willpower enable cyber misconduct ranging from compulsive gambling or shopping to hacking, harassment and pornography use. Low self-control also associates with risky online self-disclosure and financial behaviors that elevate victimization risks (van Wilsem, 2013).

This constellation of personality traits creates individual propensities for cybercrime involvement by shaping motives, goals, behavioral regulation and moral decision-making online. However, personality alone is not destiny. Contexts of online anonymity and social learning can enhance or inhibit the expression of these traits. Furthermore, personality interacts with gratifications to drive online activities, as discussed next.

Gratifications

Gratification theory explains human behavior as driven by the pursuit of desired psychological and material outcomes or 'needs affordance' (Holt, 2010; Smith, 2023a). Within criminology, this perspective helps account for the motives underlying crimes that bring status, excitement, peer-approval, sexual arousal, ideological purpose, financial gain or other valued rewards. In cyber contexts, gratifications help explain both offending and victimization.

The gratifications derived from cybercrime activities may be intrinsic, such as the thrill of successfully hacking into a system, or extrinsic, such as the monetary rewards obtained from identity theft. For offenders, power and dominance gratify by allowing control over victims and conferring status (Seigfried-Spellar & Treadway, 2014). Sexual gratification can motivate viewing pornography, cyberstalking, or harassment. Peer validation and recognition drive behaviors like hacktivism, trolling, and extremist content sharing. Retaliation fulfils desires for vengeance over grievances through aggressive actions like doxing, defacement, intimidation, or slander.

Financial gain also incentivizes various frauds, theft, ransomware and exploitation (Leukfeldt, 2017). Ideological gratifications inspire hacktivists and extremists to disrupt adversaries through data theft, hi ja-

cking, leaks or denial of service attacks. Escape provides relief from boredom or problems through immersive online gambling, gaming, or other compulsions. Thrill-seeking meets the need for novelty, risk and intensity through hacking, filtered access transgression and predation.

On the other hand, victims may also seek gratification through their online behavior, such as social validation, entertainment, or emotional support. The pursuit of gratification influences the types of behaviors individuals engage in online, ultimately shaping their vulnerability to cybercrime victimization (Holt & Bossler, 2014b). For victims, entertainment gratifications like gaming put them at risk to malware and monetary theft. Relationship seeking enables sexual extortion, catfishing and predation. Status pursuit fosters risky self-disclosure and friending that jeopardizes privacy and facilitates deception. Curiosity about illegal sites elevates exposure to viruses and coercion. Problem-solving through online queries and communities can increase vulnerability to phishing and technical support fraud during times of heightened distress or cognitive load (van Wilsem, 2013).

Integrating gratification theory into the conceptual framework allows for a comprehensive understanding of the motivations underlying cybercrime and victimization. This multitude of positive and negative drivers shapes online behaviors related to identity construction, self-disclosure, time spent online, communities frequented and relationships formed. Gratification illuminates the situational goals users pursue online that can increase risks.

Social Norms

Social norms, both offline and online, play a significant role in shaping behavior in cyberspace. Social norms refer to shared standards of conduct that delineate acceptable and permissible behavior within a group or community (Akers, 2017). Descriptive norms capture the behavioral patterns and prevalence of specific acts, while injunctive norms reflect the degree of approval or disapproval attributed to a behavior. Online platforms and digital communities develop their own unique set of social norms and expectations that influence individuals' actions and interactions (Brenner & Smith, 2019). These can range from appropriate etiquette for discussion forums to deviant subcultures that normalize and even glorify cybercrime. By considering the influence of social norms on online behavior, the conceptual framework acknowledges the contextual factors that shape cybercrime dynamics.

Social norms also influence the boundaries of behavior, as individuals may feel compelled to conform to or deviate from prevailing norms. For instance, anonymity online can erode adherence to traditionally prosocial offline norms against deceit, cruelty and harming others (Jaishankar, 2008; Suler, 2004). Within deviant subcultures organized around hacking, gaming, pornography, extremism and other interests, descriptive norms reinforce cybercrime engagement by valorizing and modeling certain acts (Holt, 2007). For example, hacker subcultures may normalize unauthorized access, copyright piracy and dark web use as forms of exploration and resistance rather than criminality. The injunctive norms shift from condemning to validating these behaviors based on their perceived purposes or justifications within the subculture.

For victims, online norms can also encourage risky disclosures, interactions with unknown individuals, and sharing of provocative content that elevates dangers (Leukfeldt, 2017). Social norms contribute to victim culpability, or the perception they enabled or failed to prevent the crime. Unfortunately, this can reduce the perceived seriousness of cyber offending like harassment, further weakening norms against it. Ultimat-

ely norms affect cybercrime through their interactions with personality traits and gratifications in shaping online conduct.

Online Behaviors

The introduction of computer-mediated communication (CMC) transformed human relations by enabling new forms of interaction through text, audio, video and images largely devoid of in-person behavioral cues. Scholars highlight the importance of examining how the nature of online environments facilitates cybercrime through anonymity, absence of surveillance, interpersonal distancing and technical mediation (Jaishankar, 2008; Ngo & Paternoster, 2011). Online behavior encompasses the actions, interactions and representations of individuals in the digital realm. It includes various dimensions, such as disinhibition and online persona. Disinhibition refers to the reduction of social constraints and self-regulation that can occur in online environments (Joinson, 2007). The absence of eye contact, facial expressions, tone, gestures and shared situational context cultivate disinhibition online, allowing users to transgress social conventions and restraints more readily (Suler, 2004). Anonymity amplifies disinhibition by reducing accountability and consequences for online behaviors. Thus, cyber-disinhibition contributes to the normalization and enactment of deviance online that would face censure offline.

CMC also enables flexible self-presentation where identities become constructed through selective disclosure and socially desirable performances tailored for diverse audiences (Chester, 2004). Users construct online personas, which are defined as identities constructed and presented in virtual spaces (Goffman, 1959). Generally, these online personas or personalized profiles are geared towards highlighting attractive attributes and activities for social validation (Smith, 2022). These personas may deviate from individuals' true selves and can influence their engagement in criminal behavior or vulnerability to victimization. Frequent self-disclosure and sharing fosters connection but can jeopardize privacy and safety. Impression management motivates self-censorship while role-playing and experimenting with identities allow exploration of alternatives. This constructed sense of self shapes social networking, forum engagement and sharing behaviors that can increase vulnerability to deception, shaming and predation.

Together these dynamics of cyber-disinhibition and malleable self-construction online create behavioral patterns around identity, relationships, communication and information disclosure that are implicated in pathways to cybercrime. Both offenders and victims exhibit these psychosocial processes, interacting online in ways that often reflect personality traits and gratifications.

Guardianship

The conceptual framework emphasizes the importance of preventive measures and protective behaviors in combating cybercrime (guardianship) that reduce opportunities for crime (Cohen & Felson, 1979). It also notes that guardianship is situated across societal and individual levels and as such takes different forms.

In cyberspace, guardianship operates at multiple levels that span software, policies, education and individual precautions. At the individual level, strong password use, multi-factor authentication, avoiding location services, limiting personal disclosures, installing software updates promptly and maintaining bound-

ary settings for sharing all strengthen guardianship and contributes to reducing vulnerability to cybercrime (Bossler & Berenblum, 2019; Choi et al., 2017). Caution in downloading unknown applications and links reduces malware exposure. Seeking credible technical support protects against fraud. Encryption, biometric authentication, firewalls, antivirus programs and access controls institute technological guardianship against threats like hacking and theft. Overall, user precautionary behaviors (cybersafe culture) significantly lower cybercrime risks especially for interpersonal offenses like harassment or deception (van Wilsem, 2013).

Information security policies in organizations and website terms/conditions establish codified expectations online, which provide administrative guardianship. Education and campaigns improve awareness of risks and best practices for cyber safety. Additionally, the presence of effective guardianship measures, such as cybersecurity laws, enforcement agencies and technological safeguards implemented by companies, play a crucial role in deterring cybercriminals and protecting potential victims (Bossler & Holt, 2010a).

Cyber Attacks

Cyber-attacks represent purposeful actions by offenders abetted by technology to cause harm to data, information systems, individuals, groups, organizations or nations (Yar & Leukfeldt, 2016). Diverse types of cybercrimes flow from the situational convergence of motivated offenders with suitable targets made vulnerable by inadequate guardianship. Offenders require some combination of skills, tools and access to carry out attacks based on their motives and the nature of vulnerabilities detected. Further, the type of cybercrime committed, and the chosen threat vectors are influenced by the offenders' motivations, gratifications, capabilities, and the technical infrastructure of their location.

Offenders may engage in various cybercriminal activities, including hacking, phishing, malware distribution, identity theft and cyberstalking, among others (Holt & Bossler, 2014a). Their motivations can range from financial gain and ideological beliefs to personal vendettas or seeking social recognition (Brenner & Smith, 2019; Smith, 2023b). The offenders' capabilities, such as their level of technical skills and access to resources, play a critical role in determining the success and impact of their cyber-attacks (Holt & Bossler, 2014b). Moreover, the technical infrastructure of the location in which offenders reside can influence their opportunities and limitations in carrying out cybercrimes (Ngo & Jaishankar, 2017).

Offenders make rational choices within crime opportunities but not always with perfect calculations since cyber tools empower impulsive and emotionally-driven strikes (Levick & Moon, 2010). Group offenders are often empowered by the diffusion of responsibility. Still, different types of cybercrimes stem broadly from financial, power assertion, sexual, ideological or entertainment motivations (Seigfried-Spellar & Treadway, 2014). Victim responses like reporting, support-seeking and resilience strategies can shape the degree of psychological, financial and productivity harms from attacks. By considering the situated interaction of offenders, victims/targets and guardians within a criminal opportunity framework, the model accounts for the manifestation of diverse cyber-attacks.

Relationships Between Components

The strength of the model lies in its recognition of the interplay between individual characteristics, online behavior, environmental factors, and victimization outcomes. The conceptual framework pins cybercri-

me events to the convergence in time and cyber-space of persons with criminogenic personality traits and gratifications seeking situations online to fulfill goals shaped by conducive social norms and online behavioral patterns, eventually taking advantage of low target guardianship to carry out a specific attack using some tool or method to achieve their ends based on the circumstances. However, preventive actions at any phase can disrupt this pathway. Guardianship mechanisms that match offense motivations, target vulnerabilities and attack vectors can stop cybercrimes. This section details relationships between model components, which is visually captured in Figure 1.

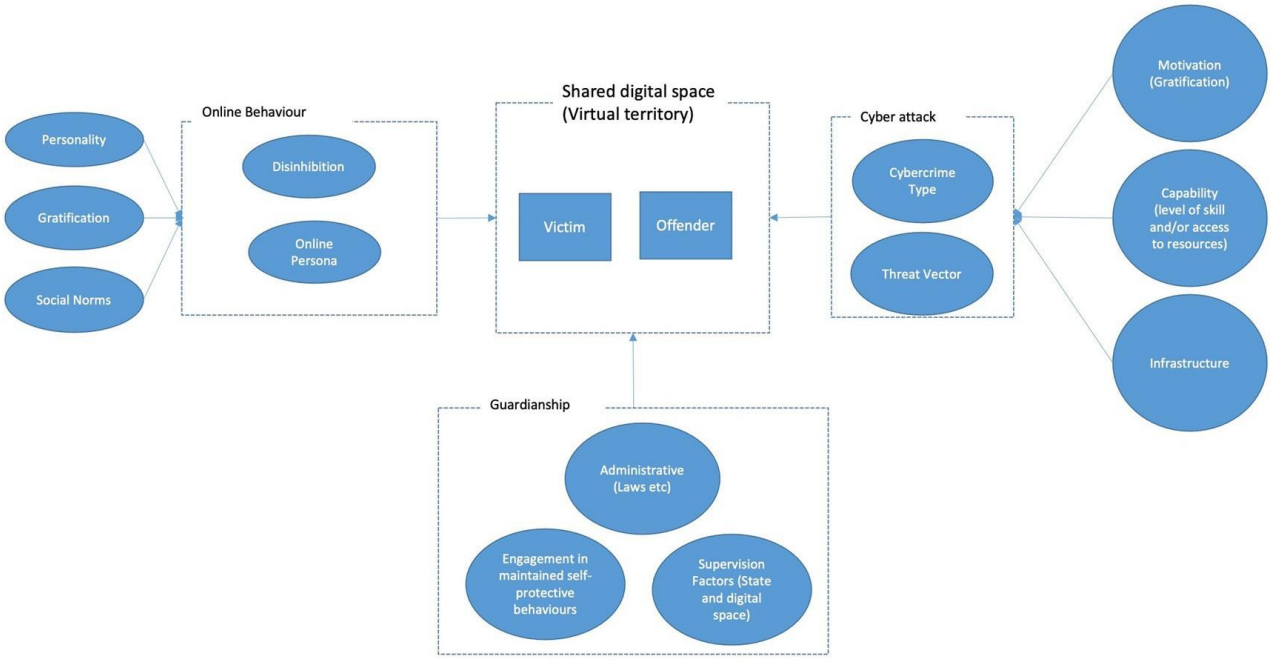

Figure 1. Proposed structure of the Integrated Model of Cybercrime Dynamics

Interrelationship 1: Personality, Gratification, and Social Norms Determine Online Behavior:

The first relationship posits that personality traits, gratification-seeking motives and social norms significantly influence an individual's online behavior. The theoretical reasoning behind this postulate is grou nded in the understanding that individuals with certain personality traits (such as impulsivity, sensation-seeking, lack of empathy, and narcissism) may be more inclined to seek gratification through illegal activities in the online realm. Empirical evidence supports this notion, demonstrating associations between specific personality traits and engagement in cybercrime (Holt & Bossler, 2014a). Additionally, social norms, both offline and online, shape an individuals' behavior in cyberspace, influencing the boundaries of acceptable and deviant actions (Brenner & Smith, 2019). These relationships are broken down and formulated and summarized below:

• Personality → Gratifications: Traits like sensation-seeking, impulsiveness, aggression, empathy deficits, and narcissism generate desires for excitement, power, status, revenge, sexual arousal, escape and ideological purpose. Gratifications represent manifestations of personality in motivation.
• Personality + Gratifications → Online Behavior: Personality and gratifications jointly shape patterns of online activity, disclosure, relationships and interactions linked to cybercrime involvement. Impulsiveness facilitates disinhibited actions. Attention-seeking fosters excessive disclosure. Antisocial behavior reduces caution with unknown partners. Sensation-seeking drives transgressive site use.
• Social Norms → Online Behavior: Social norms delineate the boundaries of acceptable conduct online. Descriptive norms normalize risky self-promotion. Deviant norms valorize hacking. Injunctive norms condone or condemn behaviors like fraud. Norm adherence depends partly on personality.

Interrelationship 2: Online Behavior Contributes to the Potential Criminal Event:

The second relationship posits that an individuals' online behavior directly contributes to the potential occurrence of a criminal event between the victim and the offender in a shared virtual territory. Online behavior encompassing disinhibition and the construction of online personas, plays a critical role in shaping individuals' vulnerability to cybercrime victimization or their engagement in cybercriminal activities. Disinhibition resulting from factors such as anonymity and reduced social constraints online can lead individuals to engage in deviant behaviors that they may not exhibit in offline settings (Joinson, 2007; Suler, 2004). The construction of online personas allows individuals to adopt different identities, which may influence their involvement in cybercriminal behavior or make them susceptible to victimization (Goffman, 1959). This is supported by empirical studies that have explored the relationships between online behavior and cybercrime involvement or victimization (Holt & Bossler, 2014a). This relationship is formulated and summarized below:

• Online Behavior → Cybercrime: Disinhibition, constructed personas and social networking influence risks of cybercrime offending or victimization through increased visibility, disclosure of personal data and development of unsafe relationships online. Online behaviors reflect personality, gratifications and norms.

Interrelationship 3: Cyber Attacks are Determined by Offenders' Motivation, Capability, and Technical Infrastructure:

The third interrelationship posits that the nature and success of cyber-attacks are determined by offenders' motivation and gratification, their capability in terms of technical skills and access to resources,and the technical infrastructure of the location in which the offender resides. The theoretical reasoning behind this relationship is grounded in the understanding that an offender's motivation drives the choice of cybercrime types and threat vectors. The offender's capabilities, including technical skills and access to resources influence the ability to carry out cyber-attacks effectively (Holt & Bossler, 2014a). Additionally, the technical infrastructure of the location in which offenders reside impacts their opportunities and limitations in conducting cybercrimes (Ngo & Jaishankar, 2017). This relationship is formulated and summarized below:

• Cybercrime → Harms: Cyber-attacks perpetrate financial, psychological, dignity and productivity harms on individuals, groups and organizations. However, target resilience and post-victimization responses can mitigate degree of damage suffered.

Interrelationship 4: Guardianship Constrains the Likelihood of Cybercrime:

The fourth relationship asserts that guardianship, defined by existing administrative measures and laws, as well as the engagement and maintenance of protective behaviors by victims and supervision factors, constrains the likelihood of cybercrime events. The theoretical reasoning behind this relationship aligns with RAT, which emphasizes the importance of capable guardians in preventing criminal events (Cohen & Felson, 1979). These relationships are formulated and summarized below:

• Personality + Gratifications + Norms + Online Behavior → Guardianship: Precautionary cybersecurity behaviors represent behavioral guardianship. Personality traits like impulsiveness undermine guardianship while conscientiousness promotes it. Awareness of norms also affects guardianship adoption.
• Guardianship → Cybercrime: Capable guardianship prevents successful attacks by blocking opportunities to offend. Encryption foils data theft. Antivirus stops malware. Strong passwords prevent account hijacking. Care in connections limits deception. Guardianship matches offense behaviors, contexts and tools.

Based on these linkages, cybercrime manifests as the outcome of several interacting pathways. Personality provides foundational dispositions shaping gratifications. Social contexts and norms frame perceptions. Together personality and social forces drive online behaviors that increase visibility and develop situations. In the absence of precautions, motivated offenders locate and take advantage of unguarded victims. However, capable guardianship mechanisms that match the specific offense, target and method disrupt this roadmap for studying offenders and victims in ways that inspire novel interventions. This conceptual model can orient future empirical research programs using diverse methods and data sources to quantify relationships and test propositions about the origins and drivers of cybercrime.

Propositions

This integrated model gives rise to numerous testable propositions regarding the relationships between key determinants highlighted. This section itemizes these testable relationships giving a clear path to the development of empirical studies to test the framework and the proposed interactions. Testing propositions empirically will refine understanding of how model components interrelate and the relative predictive strength of each element. Results can guide resource allocation to most potent intervention opportunities.

Some propositions reflect individual characteristics:

- Personality traits like impulsiveness, sensation-seeking, narcissism, aggression, and negative emotionality will positively correlate with engagement in cybercrime offenses.
- Deficits in self-control and empathy will enable cyber bullying/harassment by reducing restraint against harming others online.

- Individuals exhibiting narcissism and Machiavellianism will be more likely to engage in doxing, reputation attacks, privacy violations and coercion.
- High impulsiveness will associate with greater susceptibility to phishing attempts and social engineering cybercrimes that leverage urgency.
- Neuroticism will predict likelihood of compulsive oversharing online that jeopardizes privacy and enables extortion victimization.

Other propositions relate to social contexts:

- Strong presence of deviant online subcultures valorizing unauthorized access will normalize hacking among members.
- Offline peer associations supportive of anti-social conduct will encourage cyberbullying perpetration through differential reinforcement.
- Areas with high cybercrime rates will experience diffusion of descriptive norms condoning identity theft and sharing of attack methods through online networks.

Some propositions address motivation and behavior:

- Persons motivated by thrill, dominance, escapism and sexual arousal will show greater frequency of transgressive cybercrime acts like filtered access, predation, and viewing illegal content.
- Individuals exhibiting excessive reassurance and approval-seeking in online communications will face increased risks of grooming, deception and extortion victimization.
- Social media users with large networks of superficial contacts will encounter more incidents of photo appropriation, location tagging threats, and reputation attacks.

Propositions also relate to guardianship:

- Organizations that implement employee cybersecurity training programs will experience significantly lower rates of data breaches, malware incidents and policy violations.
- Nations with comprehensive privacy laws, cybercrime regulations, and investment in enforcement capabilities will report reduced levels of citizen victimization and cyber-attacks originating within their borders.
- Social media platform features that limit sharing, tighten default privacy settings, and surface friendship network commonalities will decrease peer deception victimization.

Implications and Applications

The IMCD outlines key components and relationships validated by research, which can lead to significant implications for advancing theory, guiding future studies, and informing prevention initiatives, interventions, education and policies related to combating cybercrime. This section details potential applications across these domains.

Theoretical Implications

For researchers, the integrated model offers a preliminary conceptual map of relevant domains based on

the current state of cybercrime scholarship. It provides value by distilling and organizing constructs investigated presently in a way that reveals their interconnectedness. However, more theoretical refinement is needed. In particular, the relative explanatory power and predictive validity of each component requires examination. Statistical tests can shed light on the most salient drivers of offending versus victimization and which mechanisms exhibit only indirect relationships versus direct effects. Exploring whether certain components such as personality or social norms moderate links between other elements will further elaborate the framework. Evaluating differences in model dynamics across types of cybercrime like interpersonal harassment, property offending, or sexual predation is also warranted (Smith & Haines, 2023). Additionally, theoretically validating the sequencing of effects in the model can guide resource allocation in interventions by identifying the most pivotal leverage points.

Research Applications

For empirical researchers, the conceptual model provides a framework to systematically investigate relationships between psycho-social determinants highlighted across disciplines. Quantitative correlational designs can evaluate linkages proposed between personality variables, gratifications sought, aspects of online behavior, guardianship adoption and offending patterns.

Longitudinal analyses can examine predictive associations over time and establish temporal precedence. Qualitative studies can elicit in-depth perspectives from offenders and victims regarding how personality, social contexts, online behaviors and precautions intersected in their cybercrime experiences. Mixed methods that combine surveys, experiments, observation of online behavior and interviews can provide richer understanding of model dynamics. The model guides selection of constructs as testable predictors, mediators and moderators. Findings will refine the explanatory scope of the model and build knowledge on pathways linking cybercrime involvement to broader psychosocial determinants.

Policy Applications

The integrated model also has implications for prevention policy initiatives seeking to reduce cybercrime victimization and offending through education, deterrence, opportunity reduction, and encouraging protective actions. By delineating multiple determinants, the model points to tailored interventions across each element. For example, personality research indicates cognitive behavioral therapies and skills training programs can strengthen impulse control and self-regulation among youth prone to risk-taking, a common cybercrime correlate (Roberts et al., 2017). Online safety education in schools can increase awareness of victimization risks associated with identity construction, relationships and information disclosure online. Trainings for organizations can spotlight the role of gratifications in motivating offenses and necessitating controls against financial, power and sexual motivations. Promoting adoption of layered guardianship matching known technical and social engineering attack methods is vital. The model supports multidimensional policies spanning psychological, social, educational, technological and criminal justice responses tailored to salient risks and drivers rather than one-size-fits-all solutions.

Victim Interventions

For victim services, the model provides a conceptual template for assessing cybercrime victims' broader

psychosocial situation based on personality traits, social contexts, online behaviors, and precautions. Rather than treating victimization as discrete incidents, practitioners can identify patterns of vulnerability rooted in personality tendencies like impulsiveness, social norms that justify risk-taking, motivation to find intimacy online after relationship loss, and low technical guardianship (Choi et al., 2017). Discussing these circumstances underlying victimization can enhance coping efficacy, help-seeking behaviors and protective changes. Support plans can address unhealthy motivations, build capabilities for more cautious online conduct, expand social connections offline, and adopt technical precautions. Therapies focusing on personality development, emotional regulation and esteem, social skills, and motivation enhancement can facilitate growth. The model maps out intervention opportunities not just after but before victimization by pinpointing psychosocial risk factors.

Offender Management

For offender management, the model similarly provides a framework for contextualizing crimes in patterns of personality traits, social learning histories, motivations and online behaviors that require redirection to prevent recidivism (Craker & March, 2016). Assessment tools guided by the model can identify specific drivers like narcissism, peer influences favorable to cybercrime, sexual motivations, and low self-control risks to address through supervision plans, therapy referrals and skills development programs. Comments from offenders themselves often lament how poor impulse control, anger, isolation or depressive tendencies contributed to cyber offending. The model suggests tailored management strategies based on the constellation of determinants for each offender. Technological controls like computer monitoring, internet use conditions and approved device specifications can supplement self-regulation challenges with external guardianship.

Conclusion

This conceptual model offers significant advancements in the interdisciplinary field of cyber criminology addressing the need for fresh perspectives tailored specifically to cybercrime. It integrates principles from criminology, psychology, and computer science to form a contemporary framework that encapsulates the complexity of cybercrime, ranging from individual differences to broader social contexts. By mapping interconnected pathways from personality traits and social norms to online behaviors and cybercrime events, the model enables a nuanced understanding of both cyber offenders and victims, acknowledging the fluidity of roles in cyberspace. Its multidimensionality and flexibility allow for the examination of various forms of cyber offending, from hacking to sexual predation. Importantly, the model's practical utility extends to informing prevention policies, education programs, and strategies for both victim intervention and offender management across individual, social, and technical levels. This integrated approach not only synthesizes current evidence and theories in cybercrime but also lays a foundation for ongoing empirical refinement, ensuring its relevance and effectiveness in advancing cybercrime research and practice.

References

Akers, R. L. (2017). Social learning theory and crime and deviance. *The Handbook of Criminological Theory, 4*(3), 245–266.

Akers, R. L., Sellers, C. S., & Jennings, W. G. (2021). *Criminological theories: Introduction, evaluation, and application* (Eighth edition). Oxford University Press.

Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: Prentice-Hall.

Bossler, A. M., & Berenblum, G. M. (2019). Cybercrime victimization: An examination of individual and situational level factors. *The Oxford Handbook of Cybercrime,* 69-94. Oxford University Press.

Bossler, A. M., & Holt, T. J. (2010a). The effect of self-control and perceived opportunity on a variety of property crimes: A county-level analysis. *Journal of Criminal Justice, 38*(5), 1034-1042.

Bossler, A. M., & Holt, T. J. (2010b). Theoretical explanations of cybercrime. *The Handbook of Internet crime,* 39-52. Routledge.

Brenner, S. W., & Smith, J. R. (2019). Cybersecurity law and policy: A comprehensive overview. *The Oxford Handbook of Cybercrime*, 3-28. Oxford University Press.

Chester, A. (2004). Presenting the self in cyberspace: Identity play in MOOs. [Doctoral dissertation, The University of Melbourne]. Department of Psychology, The University of Melbourne. Retrieved from https://www.academia.edu/110569058/Presenting_the_self_in_cyberspace_identity_play_in_MOOS?ucsb-sw=11420876.

Choi, I., Milne, D., Glozier, N., Peters, D., Harvey, S., & Calvo, R. (2017). Using different Facebook advertisements to recruit men for an online mental health study: Engagement and selection bias. *Internet Interventions, 8*, 27–34.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Craker, N., & March, E. (2016). The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours. *Personality and Individual Differences, 102*, 79–84. Retrieved from https://doi.org/10.1016/j.paid.2016.06.043

Goffman, E. (1959). The presentation of self in everyday life. Anchor Books.

Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Stanford University Press.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*, 171–198.

Holt, T. J. (2010). Examining the Role of Technology in the Formation of Deviant Subcultures. *Social Science Computer Review, 28*(4), 466–481. Retrieved from https://doi.org/10.1177/0894439309351344

Holt, T. J., & Bossler, A. M. (2014a). Cybercrime in the digital age: Defining and analyzing computer-facilitated offenses. *The Oxford Handbook of Cybercrime*, 29-47. Oxford University Press.

Holt, T. J., & Bossler, A. M. (2014b). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 35*(4), 263-287.

Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology, 1*(2), 7–9.

Joinson, A. N. (2007). Disinhibition and the internet. In *The Oxford Handbook of Internet Psychology*, 75-85. Oxford University Press.

Jones, D. N., & Paulhus, D. L. (2011). Differentiating the Dark Triad within the interpersonal circumplex. In L. M. Horowitz & S. Strack (Eds.), *Handbook of interpersonal psychology: Theory, research, assessment, and therapeutic interventions*, 249–267. John Wiley & Sons, Inc.

Leukfeldt, E. R. (2017). Cybercriminal networks, communities, and forums: An exploratory study. *The Oxford Handbook of Cybercrime*, 31-48. Oxford University Press.

Leukfeldt, E. R., & Holt, T. J. (2019). Routine activity theory and cybercrime: Applications and extensions. *The Oxford Handbook of Cybercrime,* 135-152. Oxford University Press.

Levick, M., & Moon, K. (2010). Prosecuting sexting as child pornography. *Valparaiso University Law Review, 44* (4), 1035. Retrieved from https://scholar.valpo.edu/vulr/vol44/iss4/2

Ngo, F. T., & Jaishankar, K. (2017). Introduction to cybercriminology: Exploring Internet crimes and criminal behavior. *Cybercriminology,* 1–14. CRC Press.

Ngo, F. T., & Paternoster, R. (2011). Online privacy and consumer victimization: A review of online privacy literature through the perspective of routine activities theory. *Crime and the Internet*, 177-210. Routledge.

Roberts, B. W., Luo, J., Briley, D. A., Chow, P. I., Su, R., & Hill, P. L. (2017). A systematic review of personality trait change through intervention. *Psychological Bulletin, 143*(2), 117–141. https://doi.org/10.1037/bul0000088

Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. *Deviant Behavior, 35*(10), 782–803. Retrieved from https://doi.org/10.1080/01639625.2014.884333

Ševčíková, A. (2016). Girls' and boys' experience with teen sexting in early and late adolescence. *Journal of Ado lescence, 51*(1), 156–162. Retrieved from https://doi.org/10.1016/j.adolescence.2016.06.007

Smith, T. (2022). An exploratory analysis of the relationship of problematic Facebook use with loneliness and self-esteem: The mediating roles of extraversion and self-presentation. *Current Psychology*. Retrieved from https://doi.org/10.1007/s12144-022-03505-0

Smith, T. (2023a). An exploratory investigation into social media use in Trinidad and Tobago: A comparison of Facebook and TikTok. *Caribbean Journal of Multidisciplinary Studies, 2*(1), 88–112.

Smith, T. (2023b). Threat actors in cyberspace: An examination of motivations for cybercrime. *Contemporary Issues & Challenges in International Law: An Asian Perspective*, 121-135. Satyam Law International.

Smith, T., & Haines, K. (2023). Examining the Etiology of Cybercrime: Comparing the utility of the Routine Activities Theory using a model-comparison approach. *Caribbean Journal of Multidisciplinary Studies, 2*(1), 1–24.

Smith, T., & Stamatakis, N. (2020). Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns. *International of Cyber Criminology, 14*(2), 433–459. Retrieved from https://dx.doi.org/10.5281/zenodo.4769989

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321-326.

Wilsem, J. (2013). Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437–453. Retrieved from https://doi.org/10.1177/1043986213507402

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. *British Journal of Criminology, 56*(1), 21–48. Retrieved from https://doi.org/10.1093/bjc/azv011

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407–427. Retrieved from https://doi.org/10.1177/147737080556056

Yar, M., & Leukfeldt, E. R. (2016). The "cyber" in the "crime": A challenge for criminology. *Cybercrime and its victims*, 21-37. Routledge.