**Article Review 2: The Integrated Model of Cybercrime Dynamics, Cyber Offenders, and Victimization**

David R. Allen

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 6, 2024

**Introduction**

Psychology plays a huge role in how cyber offenders and victims interact with each other. It can consist of many different theories. Some of these theories can include the routine activities theory or social learning theory. This paper will review an article that talks about previously known theories to create a framework to understand how cyber offenders and their victims interact and how this information can contribute to future studies about cybercrime and preventing victimization.

**Social Science Principles**

The first principle of social science this article covers is relativism. This article talks about how many different characteristics of a person that could contribute to the chances of someone becoming a cyber offender or continuing cybercrime activities (Smith, 2024, pp. 64-65). It’s a representation of how social systems can change behavior and how we interact with technology. For example, someone with personality traits such as narcissism or aggression correlate to committing cybercrime (Smith, 2024, p. 64). The second principle of social science this article relates to is determinism. It talks about how personality, gratification, social norms affect online behavior and how they may lead to committing cybercrime (Smith, 2024, pp. 57-60). It answers the question of why cybercrime is committed among cyber offenders. Another principle is parsimony. The author keeps explanations simple about previous theories involved with the IMCD framework. For example, the author explains that the social learning theory helps provide more depth of why cyber offenders commit crime using specific social contexts compared to routine activities theory that covers less about personality, social learning, and motivation and more about how crime starts based on the presence of other offenders, victims, and the lack of guardianship (Smith, 2024, pp. 54-55). Guardianship is described as protective or preventive behavior in this instance (Smith, 2024, p. 60).

**Research Question and Hypotheses**

This article looks to utilize the IMCD to provide a greater understanding of how victims and cyber offenders interact and what causes offenders to commit crime (Smith, 2024, p. 54). This model takes from various theories that involve personality and other social aspects to provide context to this understanding (Smith, 2024, p. 54). They are then used to build the IMCD model, which can then help provide information to future researchers so that they can advance cybercrime studies and look into psychological and social concepts to fight cybercrime (Smith, 2024, p. 54).

**Research Methods**

This article utilizes archival research based on psychological and social theories related to criminology and victimology (Smith, 2024, p. 54). Multiple academic journals and various studies are used to gather information about RAT, SLT, and their components (Smith, 2024, p. 67-70). It takes both the RAT and SLT to use as a foundation for the IMCD model (Smith, 2024, p. 56). The SLT makes up for what RAT lacks; they depend on each other to make up the IMCD model (Smith, 2024, p. 56). A visual model is created to show the relationship between online behavior, guardianship, and cyber-attacks relate back to both the victim and offender (Smith, 2024, p. 62)

**Data Analysis**

The model shown presents many interrelationships between the components (Smith, 2024, p. 62). The first relationship is about how personality, gratification, and social norms influence online behavior (Smith, 2024, pp. 62-63). The second relationship is about online behavior contributing to potential crime (Smith, 2024, p. 63). The third relationship is about how cyber-attacks are determined through the offender (Smith, 2024, pp. 63-64). The final relationship is about guardianship constraining cybercrime (Smith, 2024, p. 64). Based on all of these put together, it’s like a domino effect where one trait can affect the other. Personality shapes gratification, social norms can affect perception, while both combined affects online behavior (Smith, 2024, p. 64). If there’s no protection for the victims, offenders will strike based on the evaluation of their target and determined approach (Smith, 2024, p. 64).

This analysis gives rise to some propositions based on individual characteristics, social context, motivation and behavior, and guardianship (Smith, 2024, pp. 64-65). Cybercrime has links towards character traits such as low self-control, narcissism, and aggression (Smith, 2024, p. 64-65). Social contexts that include anti-social conduct or deviance can normalize hacking and promote cyberbullying (Smith, 2024, p. 65). Those motivated by thrill, dominance, escapism, and sexual arousal will more likely commit acts of cybercrime related to predation or viewing illegal content (Smith, 2024, p. 65) With guardianship, efficient training programs within organizations, efficient laws and regulations within a nation, and social media platforms that greatly harden their security on privacy and sharing can decrease the amount of victimization (Smith, 2024, p. 65).

**Concepts**

Most of the concepts mentioned in this article relate to criminology and victimization, focusing on different theories and various psychological aspects within the two. The first concept this article relates to is the Reinforcement Sensitivity Theory when mentioning personality (Smith, 2024, p. 57-58). This article supports this theory by suggesting those who are highly impulsive and seek gratification are more likely to be involved with cybercrime or similar behaviors, such as online harassment or hacking (Smith, 2024, p. 57). The second concept this article talks about is behavior and risk. A criminological theory related to behavior and risk, such as RAT, suggests that routines can increase the level of risk someone may face. With the case of RAT, those that engage in behaviors that lack guardianship could have an increased risk since it’s used to determine how cybercrime events may start (Smith, 2024, p. 54). The third concept this article relates to are psychological consequences of victimization, specifically support. Psychological consequences are affected by the degree of support victims receive. This article offers great solutions to help victims and get them the support they need, which includes discussing personality tendencies, mentioning unhealthy motivations, learning how to be safer online, and therapy to help that person’s personality grow all help the victim (Smith, 2024, p. 67). Lastly, when mentioned in the online behavior section, there’s a relationship between identity creation and the concept of peer networks (Smith, 2024, p. 60). With peer networks, those whose peers engage in cybersecurity are more likely to engage in cybersecurity themselves. Many people online use social media to create a profile and gain attraction, thus building a peer network online, and if they tend to deviate from being themselves, potentially one that engages in cybercrime, they may influence others within the network to do the same (Smith, 2024, p. 60).

**Challenges, Concerns, and Contributions**

The groups mentioned in this article refer to cyber offenders and victims. Victims can often be involved with the challenge of cyberbullying, which is mentioned throughout the article in different aspects. For example, reinforcement from online peer interaction can either encourage or discourage cyberbullying (Smith, 2024, p. 56). This could mean that victims of cyberbullying could include communities, such as LQBTQ, and is something that they have to keep fighting as online interactions and our reliance upon technology and the internet evolve. Another concern that these victims may face are cyber-attacks, where activities that cybercriminals may engage in include hacking, phishing, distribution of malware, identity theft, and cyberstalking (Smith, 2024, p. 61). Victims must find ways to protect themselves online in order to overcome evolving attacks in the domain of cybersecurity.

**Societal Contributions**

Contributions to this study involve various applications where the IMCD model can be applied (Smith, 2024, pp. 66-67). These applications and solutions include research applications, policy applications, victim interventions, and offender management (Smith, 2024, pp. 66-67). This model can provide empirical researchers a framework for investigation of psycho-social determinants, provide predictive time association for longitudinal studies, and give depth about personality, social context, and online behavior for qualitative studies when referring to research applications (Smith, 2024, p. 66). Referring to policy applications, this model could be used to prevent victimization online by providing interventions for each element, such as cognitive behavioral therapy solutions for personality and skills training programs for those that are highly impulsive (Smith, 2024, p. 66). With victim intervention, the model can be used as a template for understanding victims and their many traits involving their victimization in order to get them the proper help, which involves therapy and protective change (Smith, 2024, pp. 66-67). Lastly, the model can be used for offender management, where a criminal’s personality, social learning history, motivations, and online behavior can be analyzed (Smith, 2024, p. 67). Solutions used with this involve therapy and technological controls to combat cyber offenders (Smith, 2024, p. 67).

**Conclusion**

Overall, this article discusses a model that is meant as a guide for future contributions in cybercrime research. It provides greater understanding of various aspects of cyber offenders and victims, including behavior, personality, and their environment of their situation. This article also provides solutions for fighting cybercrime in both a psychological and technical perspective. This article was overall well done with a model that can be used to supplement further research involving cybercrime and cybervictimization.

**Works Cited**

Smith, T. (2024). Integrated Model of Cybercrime Dynamics: a comprehensive framework for understanding offending and victimization in the digital realm. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2), 53-70. <https://doi.org/10.52306/2578-3289.1163>