INDIAN STREAMS RESEARCH JOURNAL
ISSN NO : 2230-7850
IMPACT FACTOR : 5.1651 (UIF)
VOLUME - 15 | ISSUE - 10 | NOVEMBER – 2025

THE PLATFORM AS A CRIME SCENE: SOCIAL MEDIA'S ENABLING ROLE IN THE ECOSYSTEM OF CYBERCRIME

Mr. Vijaya Kumara[1] and Dr. Padmanabha K.V.[2]
[1]Research Scholar, DOSR in Journalism and Mass Communication, Tumkur University-Tumkur.
[2]Associate Professor, DOSR in Journalism and Mass Communication, Tumkur University-Tumkur.

ABSTRACT:

While traditional media's reportingon cybercrime presents significant ethical dilemmas, a more profound transformation is occurring: the migration of cybercriminal activities directly onto media platforms. This research article argues that social media platforms are not merely channels for communication but have evolved into active, enabling environments for a wide spectrum of cybercrime. Through an analysis of platform architectures and business models, this paper investigates how the very design features of social media—connectivity, data aggregation, algorithmic amplification, and identity construction—are systematically weaponized by malicious actors. It examines three key areas: social media as an infrastructure for cybercrime operations, its role in facilitating new forms of digital fraud like influencer scams and romance fraud, and the creation of "crime-as-a-service" marketplaces within plain sight. The article concludes that combating this trend requires a fundamental re-evaluation of platform liability and a move beyond content moderation towards safety-by-design principles.

KEYWORDS: *Social Media, Cybercrime, Platform Governance, Digital Fraud, Business Model, Algorithmic Amplification, Crime-as-a-Service, Disinformation, Impersonation.*

1. INTRODUCTION

The discourse surrounding cybercrime and media has predominantly focused on how traditional and digital news outlets report on digital threats.However, this framing overlooks a more insidious and structurally embedded phenomenon: the metamorphosis of social media platforms from mere hosts of user-generated content into sophisticated ecosystems that inadvertently facilitate and amplify cybercrime. Platforms like Facebook, X (formerly Twitter), Instagram, Telegram, and TikTok are no longer just venues where crime is discussed; they have become the primary crime scenes themselves.

This article posits that the architecture and economic imperatives of social media platforms create inherent vulnerabilities that are exploited at scale. Unlike the isolated attacks on corporate firewalls or financial systems that often make the news, the cybercrime enabled by social media is diffuse, personalized, and integrated into the daily digital lives of billions. This paper will deconstruct the enabling role of social media by first analyzing its infrastructure as a tool for orchestration and reconnaissance. It will then explore how new genres of fraud have emerged directly from platform

dynamics, such as influencer culture and the pursuit of social validation. Finally, it will investigate the brazen operation of criminal marketplaces on these platforms, arguing that the line between harmful content and criminal conduct has been irreversibly blurred.

2. THE INFRASTRUCTURE OF EXPLOITATION: ORCHESTRATION AND RECONNAISSANCE

Social media platforms provide a ready-made,global infrastructure that cybercriminals leverage for free. This infrastructure serves two critical functions in the cybercrime lifecycle: orchestration and reconnaissance.

- **Orchestration:** Centralized platforms are ideal for commanding and controlling malicious campaigns. Disinformation operations, orchestrated by state and non-state actors, use networks of inauthentic accounts to sow discord, manipulate public opinion, and erode trust in institutions. These campaigns are launched directly from the platform, using its sharing and recommendation tools to achieve viral reach. Similarly, coordinated harassment campaigns ("brigading") are organized in closed groups or through coded public communications, using the platform's own connectivity features to mobilize participants and target victims en masse.
- **Reconnaissance:** Social media is a goldmine for open-source intelligence (OSINT) used to enable more targeted attacks. The culture of oversharing—posting vacation photos in real-time, detailing workplace frustrations, listing pet names and birthdays—provides a rich source of data for social engineering. Criminals scrape this information to:
- **Phish and Spear-phish:** Craft highly personalized emails or messages that appear legitimate because they contain verifiable personal details.
- **Guess Security Questions:** Derive answers to common security questions (e.g., "What is your mother's maiden name?" "What was your first school?").
- **Plan Physical or Digital Intrusions**: Identify when a user is away from home or gain insights into corporate structures for business email compromise (BEC) attacks.

In this context, the platform is not a passive bystander but an active provider of the tools—the messaging systems, the group functionalities, the data-rich profiles—that lower the barrier to entry for sophisticated cyber-operations.

3. The New Face of Fraud: Weaponizing Social Validation and Influence

The social dynamics unique to these platforms have given rise to novel forms of cyber-fraud that exploit human psychology and the quest for social capital.

- Influencer-Led and Impersonation Scams: The rise of the "influencer economy" has created new vectors for fraud. Followers often develop parasocial relationships with influencers, perceiving them as trusted friends. Criminals exploit this trust in two ways. First, they may compromise a legitimate influencer's account to promote crypto "pump-and-dump" schemes or fake giveaway scams. Second, and more commonly, they create deepfake videos or sophisticated impersonator accounts of public figures like Elon Musk or Warren Buffett to endorse fraudulent investment platforms. The platform's algorithmic promotion of trending topics and verified-looking accounts lends an air of credibility that these scams ruthlessly exploit.
- Romance Fraud 2.0: While romance scams predate the internet, social media has industrialized them. Platforms like Facebook Dating and Instagram provide a target-rich environment where criminals can create fake, appealing identities (a process known as "catfishing"). They use the platform to build emotional rapport over time before introducing a fabricated crisis that requires financial assistance. The integration of instant messaging and story features allows for constant, intimate communication that accelerates the trust-building process, making the eventual fraud more devastating.

- Fake Merchandise and E-commerce Scams: The seamless integration of social media and e-commerce has been a boon for fraudsters. They use targeted ads—leveraging the platform's sophisticated profiling capabilities—to promote counterfeit goods or non-existent products from fake online stores. The ad platform ensures the scam reaches the most susceptible demographics, and the transactional nature of the in-app purchase creates a facade of legitimacy.

4. Crime-as-a-Service in Plain Sight: The Brazen Marketplaces

Perhaps the most startling development is the open operation of"crime-as-a-service" (CaaS) marketplaces on mainstream and niche social platforms. Cybercrime has been democratized, with specialized actors offering their services for hire to less technically skilled "clients."

Platforms like Telegram and Discord have become notorious hubs for this activity. In these semi-public or private channels, one can readily find offers for:

- DDoS-for-Hire: Services that will take down a website or online service for a fee.
- Phishing Kits: Pre-packaged software and templates that allow anyone to launch a phishing campaign.
- Stolen Data Dumps: Databases of usernames, passwords, and personal information leaked from previous breaches.
- Ransomware-as-a-Service (RaaS): Where developers lease their ransomware code to affiliates in exchange for a cut of the profits.

The persistence of these marketplaces highlights the failure of a content-moderation-centric approach. These are not just discussions about crime; they are the direct facilitation of criminal transactions. The end-to-end encryption and privacy-focused branding of some platforms, while beneficial for user rights, create significant challenges for law enforcement and platform governance, allowing these ecosystems to thrive with relative impunity.

5. CONCLUSION: RE-EVALUATING LIABILITY AND DESIGNING FOR SAFETY

The evidence is clear:social media platforms are critical enablers of the modern cybercrime ecosystem. Their design, which optimizes for engagement, data collection, and connectivity, creates systemic risks that are weaponized by malicious actors. The traditional view of media as a narrator of crime is insufficient; we must now confront the reality of media as an active, if unwilling, accomplice.

Addressing this crisis requires a paradigm shift. Policymakers and regulators must move beyond the current debate over content moderation and grapple with the more fundamental issue of platform design and liability. Treating cybercrime on social media as a series of discrete, violative "posts" to be removed is a losing battle. Instead, a "safety-by-design" approach must be mandated, requiring platforms to proactively assess how their features could be misused and build in mitigations before harm occurs. This could include:

- Defaulting to stronger privacy settings to limit OSINT harvesting.
- Implementing more robust identity verification for accounts running high-reach advertising.
- De-prioritizing algorithmic amplification for unverified accounts promoting financial schemes.
- Investing in more sophisticated detection of coordinated inauthentic behavior and CaaS advertisements.

The era of considering cybercrime and social media as separate entities is over. The platform is the crime scene, and its architects must be held accountable for making it a harder target.

REFERENCES

1. Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114-133.
2. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
3. Bradshaw, S., & Howard, P. N. (2018). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute.
4. Pace, J., & Shilling, L. (2021). The Social Media Murder Factory: How Tech Giants Enable Cybercrime. Journal of Cyber Policy, 6(2), 145-162.
5. Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.