Chapter 1
The Two-Sided Reality of Cyber Threat Actors: A Sociological MLA of Forensic Intelligence

M. M. Abdullah Al Mamun Sony
https://orcid.org/0000-0001-8169-2851
ChangeMaker Nexus Ltd., Bangladesh

ABSTRACT

This chapter introduces the Theory of Two-Sided Fact (TSF) and its operationalization through Multiple-Lens Analysis (MLA) as a transformative framework for cyber forensic intelligence. While traditional methods like anomaly detection, machine learning, and rational-choice models capture patterns, they often neglect symbolic, ideological, and affective dynamics. TSF addresses this by emphasizing the inseparability of objective structures and subjective meanings, situating cyber events as sociotechnical phenomena. Through MLA's structural, symbolic, historical, affective, and ideological lenses, analysts gain multidimensional insight into causality, escalation, and intervention. Ethical reflexivity remains central, ensuring balanced interpretation and enabling socially informed, contextually grounded responses to contemporary cyber threats.

1 INTRODUCTION

In recent decades, the accelerating complexity of digital technologies and the expansion of transnational cybercrime have posed unprecedented challenges to forensic intelligence. Investigators, analysts, and intelligence communities are confronted with vast flows of technical data, new forms of organized criminality

DOI: 10.4018/979-8-3373-4898-8.ch001

(Di Nicola, 2022), and the persistence of cyber-enabled ideological movements that resist conventional profiling (Lavorgna, 2023). The dominant response to this landscape has been to intensify the technical sophistication of forensic tools: more refined anomaly detection systems, advanced machine learning classifiers, and highly formalized models of risk assessment (Chen & Yuan, 2022; Liu et al., 2024). While these developments undeniably extend investigative capacity, they also reveal an enduring limitation—an epistemic bias that privileges technical artifacts and rational-choice assumptions while marginalizing the symbolic, cultural, and ideological dimensions of cyber behavior (Chen & Yuan, 2022). The consequence is an intelligence paradigm that excels at describing *how* certain actions occur within networks but remains less effective at explaining *why* actors mobilize, persist, or innovate in the ways they do.

This problem can be characterized as the persistence of technical bias in forensic intelligence. Analysts often rely on algorithmic models designed to process massive quantities of data with high statistical accuracy (Galante et al., 2023; Galyashina et al., 2025). Yet the epistemology of such models is oriented toward correlation rather than interpretation (Galante et al., 2023), treating behavior as a calculable function of rational incentives and system vulnerabilities (Oatley et al., 2020). In this sense, many forensic approaches remain tethered to a form of rational-choice reductionism: the assumption that cybercriminals, hackers, and digital activists act primarily as strategic calculators of risk and reward (Mushtaq & Shah, 2025; Oatley et al., 2020). While this model may capture some elements of cybercrime economics, it falls short when confronted with phenomena such as ransomware groups invoking geopolitical symbolism, hacktivist collectives animated by ideological grievances, or insider threats driven by resentment, alienation, or identity conflicts (Galyashina et al., 2025). Here, motivations are not reducible to utility-maximization; they are entangled with narratives of injustice, communal belonging, or symbolic recognition (Tyagi et al., 2024). Without adequate theoretical tools to integrate these dimensions, forensic intelligence risks constructing partial and misleading portraits of the actors it seeks to understand.

The inadequacy of this paradigm, however, becomes clearer when forensic intelligence is situated in the broader history of criminology and sociology. Criminological theories rooted in rational-choice and deterrence logics have long dominated policy frameworks, emphasizing calculation, opportunity, and risk environments (Ramadhan, 2024). In parallel, the technical disciplines that contribute to cyber forensics—computer science, data analytics, network engineering—naturally emphasize quantifiable evidence, traceable patterns, and computational modeling (Galyashina et al., 2025; Mushtaq & Shah, 2025). Yet the sociological insight, first articulated by classical thinkers such as Émile Durkheim, Max Weber, and Karl Marx, is that social action cannot be adequately understood without reference to shared

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186