Chapter 6
Forensic-Centric Human Threat Intelligence:
An Integrated Framework for Modern Cybercrime Investigation

J. V. P. Udaya Deepika
https://orcid.org/0000-0001-6593-4443
Sreenidhi Institute of Science and Technology, India

T. Venkat Narayana Rao
https://orcid.org/0000-0002-1996-1819
Sreenidhi Institute of Science and Technology, India

G. Seshu Kumari
Sreenidhi Institute of Science and Technology, India

ABSTRACT

Cyber threats today are increasingly driven by human intent, showing greater sophistication and stealth that traditional forensic models, focused mainly on digital traces, struggle to address. "Cyber Forensic Framework: Forensic-Centric Human Threat Intelligence Analysis" introduces an innovative framework that integrates behavioral science, cyber forensics, artificial intelligence, and human threat intelligence. This structured, forensic-centric approach empowers investigators, analysts, and cybersecurity professionals to detect, attribute, and mitigate threats from insiders, hacktivists, cybercriminals, and nation-state actors. By combining technical evidence with behavioral insights and threat intelligence, the book offers a comprehensive view of modern cybercrime. Through real-world case studies and

DOI: 10.4018/979-8-3373-4898-8.ch006

applied examples, it equips experts in academia, law enforcement, and cybersecurity with practical strategies to prevent and respond to complex threats across civilian domains and critical infrastructure environments.

1.INTRODUCTION

Cybercrime has become one of the most significant worldwide threats in the era of hyperconnected society, affecting both individuals and corporations, as well as national governments. Conventional solutions to cybersecurity which place their emphasis on technical security like firewalls, antivirus programs and intrusion identifications systems do not always serve to prevent the current high stakes of sophistication of cyber criminals.

Due to this, there is an urgent need of a more broad based approach where the human aspect of causing such attacks is taken under consideration. An approach that enables such combination can be referred to as a forensic-centric human threat intelligence (HTI) framework and focuses on digital forensics and human behavioral analysis to provide law enforcement with a tool to investigate and predict cyber threats more successfully.

Whereas the traditional threat intelligence is focused on determining evil artifacts such as malicious IP addresses or malware signatures, a forensic-centric HTI model goes deeper, addressing the behavioral, psychological, and social views of the threat actors. It will establish not only a way of how an attack was carried out, but (Williams & Lee, 2022) also a reason of why and who did it. The collected information by examining communication records, social media patterns, darknet communications, and previous attack trends can be used by the investigators to construct threat actor profiles with very complex data including their motives, alliances, and what they might do next.

Digital forensics is the key in this framework since it is able to gather and maintain a legally acceptable form of digital evidence. When used along with threat intelligence, this kind of data proves to be an effective source of mapping (Chen & Zhao, 2024) cyberattacks and knowing how and why a certain attacker does what they do. Instead of relying on post-attack investigations only, this combined response can enable the proactive detection and prevention of the attack before it happens.

Human aspect of cybercrime, which is normally ignored in technical defensive systems, consists of insiders and discontented employees, hacktivists and state-based attackers. The intentions can be seen through the understanding of the psychological traits and linguistic patterns, as well as through the observation of the social behavior that the technical signs would be no longer able to reflect. Such human intelligence

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