


# Chapter 8


## A Forensic Intelligence Approach for Profiling and Investigating Human-Driven Cyber Threats

**Vikas Sharma**

 <https://orcid.org/0000-0001-8173-4548>


*Department of Computer Applications,  
SRM Institute of Science and  
Technology, Delhi, India*

**Puneet Chauhan**

 <https://orcid.org/0009-0000-1652-8764>

*Swami Vivekanand Subharti University,  
Meerut, India*

**Tarun Kumar Vashishth**

 <https://orcid.org/0000-0001-9916-9575>

*IIMT University, Meerut, India*

**Sanjukta Vidyant**

*Shobhit University, Meerut, India*

**Kewal Krishan Sharma**

 <https://orcid.org/0009-0001-2504-9607>

*IIMT University, Meerut, India*

**Kajal Chaudhary**

 <https://orcid.org/0009-0000-6713-6509>

*IIMT University, Meerut, India*

**Pushendra Kumar Verma**

 <https://orcid.org/0000-0003-2777-5626>

*School of Computer Science and  
Applications, IIMT University, Meerut,  
India*

### ABSTRACT

*In this day and age, cyberspace is rife with exposures generated by people - insider attacks, clever social engineering phishing schemes, and lurking advanced persistent threats, and each event not only tests company defences but also challenges the broader security framework of a nation. This chapter draws on an intersection*

DOI: 10.4018/979-8-3373-4898-8.ch008

*of cyber forensics and human intelligence threat, with a forensic-first approach to provide a foundation to profile, investigate and pursue the people undertaking attacks. You'll observe how behavioural analytics, raw digital evidence, and advanced artificial intelligence work in concert to depict motivation, strategies, and actions intruders will employ, as well as their electronic footprints. Here are the sequential techniques to identify, pin blame, and mitigate these impacts and threats, which rely on forensic toolkits, network traffic examinations, and digital poison extraction, aka malware reverse engineering.*

## **1. INTRODUCTION**

In a world where cyberspace is dominated by human creativity and psychological intent, cyber threat attacks diligently contain a human component, and no longer just automated scripts or malware. Today's most harmful threat activity is human-driven, either from malicious insider risks with well-developed access, social engineers with an understanding of human psychology, or advanced persistent threat (APT) groups with long-term intent. Threats may impede or avert operations for organizations and can ultimately compromise national security and critical infrastructure. Generally, cybersecurity capabilities cannot easily defeat potentially sophisticated human-enabled threats. This chapter articulates a forensic intelligence approach through the development of a structured framework for investigating human-enabled cyber threats as a combination of cyber and human-centric threat intelligence that addresses the research problem, which is outlined below.

### **1.1. Overview of Human-Driven Cyber Threats**

Human-enabled cyber threats fall into an increasingly sophisticated and generally more dangerous class of cyber threats. Actions taken by individuals or groups can include thought, targeted actions, and consideration of surrounding conditions. These threats depend on the human adversary's cognitive capacity, social engineering skills, and the planning that goes into the attack (considered as time) within a set timeframe. Human-enabled cyber threats may include but are not limited to: insider threats (whether active insider or passive insider), phishing attacks, business email compromises, and advanced persistent threats (APTs). Each of these threats includes steps taken by human adversaries to maintain covert access to networks over long-timeline engagements. Human-enabled cyber-attacks are not designed simply to gain unauthorized access to systems; they often seek to avoid detection, to manipulate human behavior patterns, extract sensitive data, serve as a strategic disruption to operations. One of the most substantive challenges of human-enabled

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/a-forensic-intelligence-approach-for-profiling-and-investigating-human-driven-cyber-threats/401295](http://www.igi-global.com/chapter/a-forensic-intelligence-approach-for-profiling-and-investigating-human-driven-cyber-threats/401295)

## Related Content

---

### Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulz and 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](http://www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186)

### Advancing Agriculture With Industry 5.0-Enabled Crop-Type Prediction

Abhikalp Mishra, Pushkar Praveen, Ananya Subudhi, Somil Majila and Sachin Negi (2024). *Infrastructure Possibilities and Human-Centered Approaches With Industry 5.0* (pp. 20-35).

[www.irma-international.org/chapter/advancing-agriculture-with-industry-50-enabled-crop-type-prediction/337805](http://www.irma-international.org/chapter/advancing-agriculture-with-industry-50-enabled-crop-type-prediction/337805)

### Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulz and 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](http://www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186)

### Futuristic Chatbots: Expectations and Directions for Accomplishment

Nitin Sharma and Pawan Bhakuni (2024). *Design and Development of Emerging Chatbot Technology* (pp. 317-345).

[www.irma-international.org/chapter/futuristic-chatbots/344265](http://www.irma-international.org/chapter/futuristic-chatbots/344265)

### Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulz and 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](http://www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186)