Article Analysis

Hailey Caram

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Matthew Umphlet

August 8, 2025

Rich and Aiken (2024) utilize an interdisciplinary approach to improve cyber threat prediction, relying on digital forensics and forensic cyberpsychology. The authors argue that the usual cybersecurity methods of relying on technology to secure systems are an insufficient response to the evolving cyber threats which are driven by human behavior. The study offers proactive solutions to the problem, such as machine learning algorithms.

The research combines social science principles with traditional cybersecurity knowledge to address the problem of cyber threat prediction. The authors heavily rely on real data provided by companies, weaving the social science principle of empiricism throughout technical discussion. The use of security logs and behavior profiles emphasize data and fact over speculation or assumption, which further emphasizes empiricism within the article. In addition to empiricism, objectivity is prioritized throughout the research to ask and answer questions with minimal bias or opinion. Instead, the research uses data to more effectively understand motivations and patterns. Objectivity also assists when assessing threats, providing a fuller and more clear picture of the threat or attack. The final social science principle relevant to this research article is determinism. The CFBA model assumes that cybercrime follows predictable patterns. This study supports the deterministic idea that actions are influenced or determined by causes.

The authors identified many knowledge gaps. One of the most significant gaps in research is an effective integration of the understanding of cybercriminal behavior and motivation with technical aspects of threat prediction. To address this knowledge gap, the researchers posed the following research question: How does integrating CBDFA with the Prophet model and CFBA improve the prediction of cyber threats from ASNs in modern cybersecurity?

To answer this research question, a three-part hypothesis was formulated. First, the researchers hypothesize that the Prophet model, which is well-renowned for its predictive capabilities, will significantly improve the accuracy of cyber threat predictions. Evidence to support this hypothesis include the model's notable and advanced analytical capabilities, which provide increasingly accurate predictions of cyber threats, especially from ASNs. Secondly, the researchers hypothesize that combining cyber incident data with CFBA will result in a more precise evaluation of cyber threats. The researchers assert that an integration of technical data, including logs and incident reports, and insights into cybercriminals' behavioral patterns and motivations will offer a fuller understanding of potential cyber threats. An integrated approach will likely lead to a more comprehensive comprehension of threats, resulting in more accurate threat evaluations and responses. The final piece of the hypothesis is that the IPM will greatly improve predictions of ASN-related cyber threats. Blending knowledge of human behavior and technical data within a single predictive model echoes the belief that a multidisciplinary approach provides a better understanding of cyber threats.

The authors utilized multi-method research approaches. The first approach featured within the article is archival research. The researchers dissected 638 days of historical security incident logs to attempt to answer the stated research question. Additionally, the researchers relied on case studies, focusing on three specific targets to properly test the CFBA model and Prophet forecasting. This research method helped to examine behavior patterns of cyber criminals, as well as the effectiveness of models.

Several types of data and analysis were present within the research article. Data types included cyber incident logs and reports, which can offer historical insight into past cyber threats and increase technical understanding, and GeoIP ASN data, which is essential for internet traffic

and cyber threat analysis, particularly for ASN-related threats. Additional data types within the research article included behavioral profiling techniques, which analyze cybercriminal psychology for greater insight into criminal motive and tactics, and cyber threat intelligence, which combines log data with threat intelligence to identify malicious or advanced threats. Ensuring that data sources are diverse deepens the understanding of both technical and behavioral aspects of cyber threat prediction. Analysis conducted within the research includes descriptive statistics, machine learning forecasting, behavior scoring, and ranking models. Analysis types were also varied and diverse.

This article demonstrates key class concepts, such as theories of cybercrime, human factors of cybersecurity, and cybersecurity subcultures. One important theory of cybercrime is neutralization theory, which asserts that individuals who engage in criminal acts find ways to justify their criminal behavior, allowing the individual to continue with criminal behaviors without guilt or moral constraints. The behavior profiling present in this study aligns with neutralization theory as researchers attempt to understand human behavior and criminal motivations. The human factor of cybersecurity, such as the increasing online presence of humans, emphasizes the need for more accurate threat prediction to provide effective cybersecurity. Finally, cybersecurity subcultures, such as hacking subculture, could influence hacker behavior and motivation, which is highly relevant to threat prediction. Accounting for subculture influence when predicting threats can increase accuracy.

The need for accurate threat prediction is especially critical for marginalized populations. Individuals in marginalized groups, such as those in low-income communities or rural areas, may lack access to advanced tools or education that increase digital literacy. Marginalized populations may be faced with under-resourced schools, contributing to decreased overall digital literacy.

This model can help identify potential threats which could be targeting these vulnerable groups who are experiencing under-resourced public systems and low digital literacy. Additionally, language and cultural barriers could contribute to behavior profiling. Forensic cyber investigations must consider cultural differences in online behavior, which may be overlooked in threat detection systems. Popular threat detection systems may rely on Western-centric behavior norms and language, which can fail to account for cultural differences and increase system vulnerability.

Overall, the study conducted by Rich and Aiken (2024) provided valuable contributions to society. Firstly, the study offers improved cybersecurity through CFBA, which enhances threat prediction and prevention measures. Law enforcement and forensics may also benefit from this study to aid investigations, especially the specific tools and models used for attribution of crimes. In addition, insights gleaned from this study can inform the educational sector, informing cybersecurity training and helping individuals understand the human element of cybersecurity. Finally, policy could be influenced by this study, and future policies could incorporate behavioral knowledge along with technical data.

References

Rich, M. S., & Aiken, M. P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sciences (Basel, Switzerland)*, *4*(1), 110–151. https://doi.org/10.3390/forensicsci4010008