An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics

Marshall S. Rich * and Mary Aiken

Posted Date: 12 December 2023

doi: 10.20944/preprints202312.0770.v1

Keywords: forensic cyberpsychology; cyberpsychology; predictive analytics; prophet model; behavioral-centric threat intelligence; ISPs; cyber behavioral analysis; cyber forensics; behavioral analysis; time-series analysis; cyber defense

Article

An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics

Marshall S. Rich * and Mary Aiken

Forensic Cyberpsychology, Capitol Technology University, Laurel, MD, USA
* Correspondence: mrich@captechu.edu

Abstract: A groundbreaking integrated predictive model, termed Cyber Forensics Behavioral Analysis (CFBA), has been developed in an environment characterized by rapidly evolving and increasingly sophisticated cyber threats. This model merges Cyber Behavioral Sciences with Digital Forensics to enhance the prediction accuracy and effectiveness of cyber threats originating from specific Autonomous System Numbers (ASNs). It has been observed that traditional cybersecurity strategies, predominantly focused on technical aspects, must be improved in addressing the complex landscape of cyber threats. Consequently, a novel approach has been proposed in this research, combining technical expertise with insights into the behavior of cybercriminals, thereby addressing a significant gap in existing methodologies. A mixed-methods approach has been employed in the study, integrating quantitative and qualitative research methods. This approach has created a comprehensive framework incorporating digital forensics, cybersecurity, computer science, forensic psychology, and the cyber behavioral sciences which incorporates disciplines scuch as cyberpsychology and forensic cyberpsychology. The study is anchored around four key concepts: (1) Forensic Cyberpsychology, which focuses on understanding psychological aspects of cybercriminal behavior; (2) Digital Forensics, involving the collection and analysis of digital evidence from cyber incidents; (3) Predictive Modeling, which utilizes historical data and patterns to anticipate potential cyber threats; and (4) the Cyber Behavioral Analysis Metric (CBAM) and Cyber Behavioral Score (CBS), tools designed for evaluating and scoring ASNs based on their behavior in terms of cybersecurity threat risks. Challenges encountered in the development of this integration have been significant. Initial setbacks included the misalignment of traditional cyber defense methods with the evolving nature of cyber threats and the absence of a holistic approach in pre-existing models. Through the narrative of these challenges and the subsequent development of the CFBA model, the research highlights the necessity for an interdisciplinary approach to cybersecurity. The outcomes of this study are not merely theoretical but provide practical, actionable tools and frameworks that markedly improve the precision of predicting cyber threats, especially from ASNs. The CFBA model represents a significant shift in cybersecurity strategies, highlighting the importance of integrating behavioral insights with technical knowledge. The study emphasizes the need for ongoing research and collaboration in cybersecurity, advocating for an approach that is as comprehensive and multifaceted as the cyber threats it seeks to mitigate. This research has been conducted to contribute significantly to cybersecurity, offering new perspectives and methodologies in a rapidly changing domain.

Keywords: forensic cyberpsychology; cyberpsychology; predictive analytics; prophet model; behavioral-centric threat intelligence; ISPs; Cyber behavioral analysis; cyber forensics; behavioral analysis; time-series analysis; cyber defense

 doi:10.20944/preprints202312.0770.v1

1. Introduction

1.1. Problem Overview

This study is dedicated to developing and implementing a pioneering integrated predictive model. This model synergistically fuses the insights of cyber behavioral sciences with the technical rigor of digital forensics. Its primary aim is to significantly elevate the accuracy and precision of cyber threat predictions linked to specific Autonomous System Numbers (ASNs).

At its core, cyber behavioral sciences represent an innovative interdisciplinary domain that merges psychology, cyberpsychology, information technology, cybersecurity, and digital forensics. This field is crucial in understanding the human elements inherent in cyber interactions. It provides deep insights into individuals' behaviors, motivations, and intentions in the digital world, thereby offering crucial insights into human factors in cybersecurity [1–3]. Cyberpsychology is the study of the impact of emerging technology on human behavior, covering areas such as human factors in cybersecurity, social technologies, and the psychology of virtual reality and artificial intelligence [4].

Forensic Cyberpsychology is a cutting-edge and emerging discipline, standing at the confluence of psychology and cybersecurity, focusing on psychological aspects of cybercriminal behavior, including offender profiling, motivations, and behaviors, as well as cyber deviancy and online victimology. It also involves developing methods for online investigative procedures to mitigate and prevent cybercrime, making it a specialized branch within the cyber behavioral sciences dedicated to understanding the psychological underpinnings of criminal cyber activities and threats [5].

In an era where digital landscapes are increasingly intertwined with our daily lives, the significance of the FBI's Internet Crime Complaint Center (IC3) has never been more pronounced [6]. As the frontline defense against the escalating threats of cyberattacks and cyber-enabled frauds, the IC3 not only represents our collective response to these prevalent dangers but also serves as a indicator of their evolving nature. Despite a 5% decrease in reported incidents in 2022, the alarming surge in potential financial losses—from $6.9 billion in 2021 to over $10.2 billion in 2022—underscores a troubling escalation in the severity and impact of cyber threats. This study delves into the complexities of this digital battleground [6].

Traditional cybersecurity strategies, predominantly grounded in technical methodologies, face significant challenges in accurately predicting these threats. The increasing sophistication of cybercriminal activities necessitates an approach that not only relies on technical defenses but also comprehensively understands the psychology of cybercriminals [1,7–10].

Cyber threats are no longer just a matter of technical vulnerabilities; they are intricately linked to the behaviors and motivations of the individuals, organizations, and nation-states behind these acts. Current cybersecurity strategies, while robust in their technical aspects, often need an approach that combines the psychological dimensions of cybercrime [10–13]. This gap highlights the limitations of traditional cybersecurity methods, which primarily focus on reactive measures rather than proactive threat prediction and prevention [14–16].

The evolving nature of cybercriminal activity, which often goes undetected by traditional technical approaches, highlights the importance of incorporating **cyber behavior sciences, which is defined and discussed in Section 1.**4.2.1**,** into cybersecurity practices [17–19]. As cybercriminals use more sophisticated techniques and psychological strategies, insights from this field become crucial for better understanding and predicting these complex threats [18–20].

Therefore, the problem in contemporary cybersecurity is characterized by the need to address the increasing complexity of cyber threats through a transdisciplinary approach. In a systematic review, **Martineau** et al. (2023)[2] establish a foundation for criminal profiling by a comprehensive framework referenced as "*Cyber Behavioral Analysis (CBA)*" [2], (p. 454). Initially, utilizing the CBA approach, this study will modify the CBA framework to add a *Forensic Sciences component* for this study, overarchingly named "*Cyber Forensics Behavioral Analysis (CFBA).*" Using the CFBA, this research will blend technical cybersecurity measures with an understanding of cybercriminal psychology to enhance the accuracy and effectiveness of threat prediction and prevention strategies [1,21–24].

 doi:10.20944/preprints202312.0770.v1

By adopting this integrated approach, cybersecurity strategies can evolve from being predominantly reactive to becoming more proactive and adaptive in the face of sophisticated and psychologically driven cyber threats.

1.2. Discipline Definitions and Knowledge Gaps

1.2.1. Definitions

For this study, "*Cyber Forensics Behavioral Analysis*" (CFBA) is a transdisciplinary overarching approach that combines elements from the cyber behavioral sciences, digital forensics, predictive modeling, and cyber threat intelligence [2]. Structured definitions incorporating the various aspects of CFBA:

Forensic Cyberpsychology (FCyberPsy)

An emergent discipline at the nexus of psychology and cyber forensics that is crucial for understanding and anticipating the behaviors and motivations of cybercriminals. It is vital in enhancing strategies to predict and counteract cyber threats, leveraging behavioral insights into cybercriminal activities [5,7,18].

Digital Forensics (DF)

Pertains to the technical side of investigating cybercrimes, which involves the collection, preservation, analysis, and presentation of evidence from digital devices. DF provides tangible, legal evidence from cyber incidents. This evidence is crucial in understanding the actions and methodologies of cybercriminals [10,25].

Psychology-Digital Forensic Analysis (PDFA)

PDFA, therefore, unifies the behavioral analysis from behavioral science with the technical evidence-based approach of DF. This holistic approach is vital in offering a more comprehensive understanding and method for addressing cyber threats. PDFA not only aids in profiling and understanding cybercriminals but also provides a robust, evidence-backed framework for legal proceedings and cybercrime investigations. The synergy of these disciplines under the umbrella of PDFA marks a significant step forward in enhancing cybersecurity measures and strategies [7,13].

Predictive Modeling (PM) Integration

PM in cybersecurity refers to creating models to anticipate potential cyber threats based on historical data and patterns. PM, which is technical dimension, employs various algorithms and machine learning techniques to predict future cyberattacks, enabling proactive cybersecurity measures. CFBA incorporates these predictive models to enhance threat detection and prevention [15,26].

Cyber Behavioral Analysis Metric (CBAM) and Cyber Behavioral Score (CBS)

CBAM is developed from Rich's (2023) research [25,27] and is a comprehensive analytical framework combining the methodologies of 'Malicious Threat Intelligence Feeds [27], (p. 624) and Association Rule Mining [25], (p. 400). This present study will combine the two to evaluate and score ASNs based on their cyber behavior as an output of CBAM; a CBS is derived, which is a quantifiable metric representing the behavioral dimension and patterns of an ASN in terms of cyber security threat risks, used to quantify and analyze ASN behavior to improve the accuracy of predicting cyber threats.

Interdisciplinary Predictive Model (IPM) and Advanced Tailored Predictive Tool (ATPT)

The IPM's central objective is to integrate cybercriminals' behavioral profiles and patterns into predictive algorithms [2,28,29] focusing on ASNs, as demonstrated by the introduction of CBAM. The ATPT outcome leverages strengths from cyberpsychology, digital forensics, cybersecurity modeling, and detailed behavioral analysis from CBAM and CBS. This tool is designed to predict cyber threats and provide insights into mitigation strategies, reflecting the complex dynamics of cybercriminal behavior.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

Final *Cyber Forensic Behavioral Analysis* (CFBA) Definition

Utilizing the previous combined definitions, CFBA is defined as an approach that combines psychological insights, digital evidence, predictive analytics, and detailed behavioral metrics to predict, understand, and mitigate cyber threats effectively. It represents a sophisticated understanding of cybercriminal behavior, utilizing diverse tools and methodologies to enhance cybersecurity measures.

Summary of Definitions

In summary, while CFBA is a more comprehensive and multidisciplinary approach that is informed by various research areas such as forensic cyberpsychology, digital forensics, predictive modeling, and behavioral analysis metrics. PDFA focuses explicitly on the integration of behavioral analysis with technical evidence. Both approaches aim to enhance the understanding and mitigation of cyber threats but differ in scope and specific methodologies.

Figure 1 is a flow diagram that represents the integrated CFBA model. The diagram illustrates the sequential phases and how they interconnect, starting from data collection to the final predictive tool, with feedback loops indicating the continuous improvement phase.

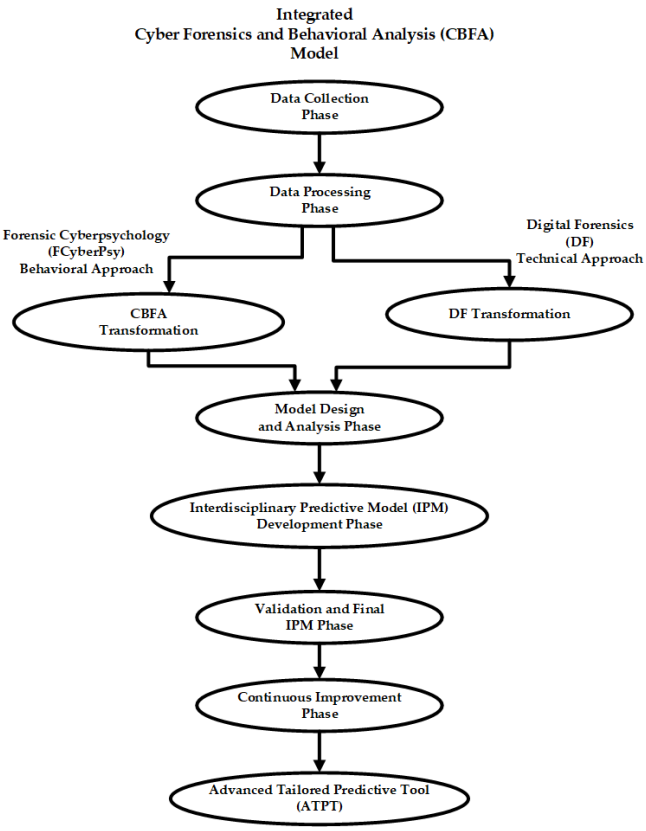

Figure 1. Integrated Cyber Forensic and Behavioral Analysis Model.

1.2.2. Knowledge Gaps

Despite the advancement of individual disciplines, a significant gap persists in effectively integrating the psychological understanding of cybercriminal behavior and motivation with the technical aspects of threat prediction [3,12]. While **PDFA (**Psychology-Digital Forensic Analysis**)** offers profound insights into the 'why' behind cybercrimes, arguably **DF (Digital Forensics)** and **PM (Predictive Modeling)** focus more on the 'how' and 'when.' This disconnect hampers the understanding and prediction of cyber threats. For instance, while predictive models can forecast potential cyberattacks, understanding the psychological triggers, drivers and patterns of cybercriminal behavior could significantly refine these predictions [30]. Similarly, the integration of cyberpsychological profiles into DF investigations could enhance accuracy with regard to attribution,

 doi:10.20944/preprints202312.0770.v1

that is, identifying potential cybercriminals (lone and organized) and understanding respective modus operandi [1,25,27].

Interdisciplinary cybersecurity research and practice approaches are essential for tackling multifaceted cyber threats. An interdisciplinary approach harnesses expertise from diverse fields, offers comprehensive insights, and reveals gaps in traditional methods to enable more effective strategic responses. Table 1, an outcome of the literature review, showcases interdisciplinary approaches, integrating specialized knowledge from various domains to enhance our understanding of cybersecurity and uncover overlooked critical factors [21,28]. References accompanying each approach offer additional context and support the role of interdisciplinarity in advancing cybersecurity practices [9].

Table 1. Interdisciplinary Approaches.

Examples	Interdisciplinary Approach	Exposing Gaps in Research	Reference(s)
Behavioral Threat Modeling	Combining cybersecurity, psychology, and human factors expertise	Reveals gaps in traditional threat modeling, emphasizing human behavior	[29,31]
Human-Centric Risk Assessment	Integrating cyber risk assessment with behavioral insights	Highlights gaps in risk assessment that overlook human factors	[12,32]
Cybersecurity Education and Training	Collaboration between cybersecurity and instructional design	Uncovers gaps in training effectiveness, guides learner-focused programs	[8,24]
Human-Centric Security Policies	Merging legal, cybersecurity, and behavioral science expertise	Exposes gaps in policies that disregard human behavior	[33,34]
User-Centered Security Design	Collaboration among cybersecurity, UX design, and HCI experts	Uncovers gaps in security designs that hinder usability	[22,30]
Cyber Threat Intelligence Analysis	Combining cybersecurity and social science expertise	Highlights gaps in threat intelligence that omit behavioral aspects	[9,18,25,27]

1.3. *Aim of the Study*

1.3.1. Overview

In this study, an integrated approach to Cyber Forensic Behavioral Analysis (CFBA) is proposed, aligning with the multidisciplinary nature of emerging cyber behavioral sciences. The core aim of developing an Interdisciplinary Predictive Model (IPM) is articulated by using the combined Psychology-Digital Forensic Analysis (**PDFA)** approach. The IPM is envisioned as a significant enhancement in cybersecurity, with a specific emphasis on the accuracy and precision in predicting cyber threats emerging from ASNs.

Incorporating the Cyber Behavioral Score into the IPM establishes a more comprehensive framework for cyber threat prediction. Connolly et al. (2016)[12] and Martineau et al. (2023)[2], outline that psychological underpinnings of cybercriminal behavior should be integrated with

 doi:10.20944/preprints202312.0770.v1

detailed examination of digital evidence in cyber incidents. This blend is considered pivotal in advancing the field of cyber threat detection and prevention.

1.3.2. Discussion of Interdisciplinary Approach

A notable shift in the cybersecurity approach has been observed, moving from a predominantly technical focus to one that includes behavioral aspects. For example; research by Ahmad et al. (2012)[8] and McAlaney et al. (2016)[21] highlights a trend toward technical advancements, with an emphasis on the behavioral science perspective in terms of addressing cyber vulnerabilities. The interdisciplinary approach advocated in the study underlines the significance of transcending purely technical solutions, by factoring in the human and thereby advocating for a more holistic perspective.

1.3.3. Primary Focus or Aim

As delineated, the study's primary aim is to refine the precision and accuracy of predicting cyber threats from ASNs [14]. It is observed that the IPM and Advanced Tailored Predictive Tool (ATPT) employs machine learning algorithms coupled with **PDFA**, offering more profound insights into the motivations behind cyber threats and scrutinizing digital footprints and behavioral patterns associated with these threats. Back and LaPrade (2019)[14] and Pollini et al. (2022)[28] support the enhanced predictive capabilities achieved through this integration.

The IPM is arguably a significant advancement in terms of integrating various disparate fields – ranging from cyberpsychology, to digital forensics, to cybersecurity modeling, and behavioral analysis. This comprehensive approach aims to gain a better understanding of the technical and human factors driving cybercriminal activities by measuring the IPMs' and the ATPTs' effectiveness in enhancing cyber threat prediction [15,29,32,35].

The study underscores the critical role of an interdisciplinary approach in developing strategic and effective strategies in the realm of cybersecurity [11,15,16]. This approach represents a significant step forward in the field of CFBA, emphasizing the integration of diverse expertise and a wider knowlege base to tackle the ever increasing complexities of cyber threats.

1.4. Literature Review

In response to the evolving cybersecurity landscape, this literature review explores existing research in cyber threat prediction and the diverse disciplines of PDFA. The primary focus of this study is to elevate the accuracy and precision of cyber threat prediction originating from ASNs by combining these disciplines using PDFA. This review underscores the critical need for a transdisciplinary approach, exposing gaps in the current body of knowledge and laying the foundation for future research endeavors to foster a more secure digital realm.

1.4.1. Research Methodology

For this comprehensive literature review, an extensive search was conducted across multiple databases, including the ACM Digital Library, EBSCOhost, Homeland Security Digital Library, Nexis Uni, ProQuest One Academic, and Wiley Online. The time frame for the literature selected spanned from 2000 to 2023. The inclusion criteria focused on academic sources such as Dissertations and theses, Scholarly Journals, Reports, Books, and Conference Papers and proceedings. Exclusion criteria were applied to filter out sources that did not offer full-text access, needed more relevance to the study's focus, fell short of academic rigor, or were redundant.

In conducting the research, a search strategy was employed using key subject-specific terms: 'Cyber Threat Prediction,' 'Cyberpsychology,' 'Digital Forensics,' 'Predictive Modeling,' and 'Interdisciplinary.' The process yielded a progressive accumulation of relevant articles. Initially, 47,241 articles were identified under 'Cyber Threat Prediction.' Incorporating 'Cyberpsychology' resulted in 2,757 additional articles. Further inclusion of 'Digital Forensics' led to 162 more articles.

 doi:10.20944/preprints202312.0770.v1

Considering 'Predictive Modeling' added 94 articles, the final criterion, 'Interdisciplinary,' contributed an additional 58 articles.

The next phase involved meticulous data extraction. The articles were systematically categorized according to their disciplinary focus and then subjected to a thematic analysis. This analysis aimed to distill recurrent themes, key concepts, and valuable insights. The findings were organized thematically to reflect the various disciplinary contributions to the field of cyber threat prediction, which are detailed in the subsequent sections.

1.4.2. Overview [9,13]

Traditionally, the emphasis in cyber-related endeavors has predominantly been on technical strategies and solutions. While invaluable, these technical approaches are founded on the principles of identifying, countering, and mitigating threats through technology. The recent initiative "ReSCIND," or Reimagining Security with Cyberpsychology-Informed Network Defenses, exemplifies the progressive shift towards leveraging human limitations in cybersecurity strategies [13]. The ReSCIND program aims to augment traditional defenses by exploiting cognitive biases and decision-making vulnerabilities inherent in cyber attackers [13] and notably is informed by the discipline of cyberpsychology.

However, cyber threats' sheer complexity and vitality underscore the need for a more comprehensive and human-centered approach. Spitaletta's (2021) work on "Operational Cyberpsychology" accentuates the transition from solely relying on technical tools to incorporating an understanding of psychological motivations and behaviors [9]. By adapting models from special operations, which historically emphasize precision, surprise, and specialized tactics, to combat operations, there is an opportunity to rebalance the asymmetric nature of cyber defense. This adaptation involves technical know-how and an in-depth grasp of the human psyche, including its susceptibilities, motivations, and behavioral patterns [9].

Cyber Behavioral Sciences [1,2,11–17,21,23]

Technical approaches [11,12] provide tangible defenses against cyber threats, however, understanding psychological and behavioral aspects of these threats is essential [2,13,21,23]. Combining these perspectives offers a view of the cyber threat landscape that encompasses various aspects [14–16,21]. Forensic Cyberpsychology an emerging subdiscipline of cyberpsychology, as highlighted in the Europol report, emphasizes this need [1]. Aiken & McMahon (2014)[1] propose an active defense strategy, focusing on understanding criminal behavior in cyberspace for more effective prediction and counteraction. Yan (2012)[17] also emphasizes the need for interdisciplinary collaboration in studying cybercrime and almost a decade ago predicted the exponential growth in, and importance of, the cyber behavioral sciences going forward.

Cyberpsychology and Human Factors [3,12,14,16,19–21,24,36]

Cyberpsychology explores the human aspect of cybercrime and cybersecurity. Aiken et al. (2022)[3] stress the importance of understanding human drivers in cybercrime for behavioral profiling. Connolly et al. (2016)[12] introduce the foundations of cyberpsychology and its significance in cybercrime prevention. Arguably, psychological perspective enhances predictive modeling efforts [14,16,19–21,24,36].

Human Factors in Cybersecurity [3,20,27,29,32]

Understanding human factors in cybersecurity is crucial. Tennakoon (2011)[29] advocates for a holistic approach, that is, combining learnings from PDFA to enhance predictive modeling. Greitzer and Hohimer (2011)[20] support this assertion, highlighting the importance of modeling human behavior to anticipate insider attacks. Incorporating human factors may significantly improve cyber threat prediction [3,27,32].

 doi:10.20944/preprints202312.0770.v1

Cybercrime and Adversarial Tactics [1,27]

Understanding cyber adversaries' tactics is pivotal. Rich's (2023)[27] analysis provides insights into cyber adversarial tactics, while Aiken and McMahon's early work delves into the cyberpsychology of Internet-facilitated organized crime [1]. Recognizing psychological aspects is crucial for integrating advances in the cyber behavioral sciences into predictive modeling.

Psychology of Cybercrime [16,22]

Kirwan and Power (2013)[16] outline the psychology of online offenders, contributing to understanding aspects of cybercriminal motivation. Attrill-Smith and Wesson's work on "The Psychology of Cybercrime" [22] reinforces the importance of psychological factors in cybercrime, and the enhancement of predictive modeling for better threat identification.

Social and Psychological Impact of Cyber-Attacks [23,37]

Bada and Nurse (2019)[23] investigate the social and psychological impact of cyberattacks. Weems et al. (2018)[37] study susceptibility and resilience to cyber threats. Understanding these dynamics is crucial for merging the cyber behavioral sciences and specifically into predictive modeling.

Predictive Modeling (PM) and Machine Learning (ML) in Cybersecurity [11,38,39]

Section 1.4.2.7 discusses the role of PM and ML in cybersecurity, which has gained significant traction in recent research [11,38,39]. PM and ML are critical in addressing cybersecurity challenges, as noted by Sarker et al. (2020) [38], who emphasize the importance of ML in this domain. Alrowaily (2020) [11] focuses on the application of ML algorithms in network intrusion detection systems (IDS), highlighting their contribution to enhancing the accuracy of cyber threat prediction. Moreover, Abdullah et al. (2022) [39] examine the practical application of the Prophet model in intrusion detection within cloud computing environments. This collective work demonstrates the model's utility in predicting cyber threats and detecting intrusions and offers valuable methodological and interdisciplinary insights. These insights are particularly relevant to the aims and objectives of this study, underlining the increasing integration of PM and ML techniques in cybersecurity.

Cyber Behavioral Approaches to Cybersecurity [14,40]

Cyber behavioral approaches to cybersecurity consider human factors and emotional aspects. Back and LaPrade (2019)[14] discuss cybercrime prevention strategies, while Ferguson-Walter et al. (2021)[39] analyze affective states in cybersecurity. Cyber behavioral aspects effectively merge technology and psychology for cyber threat prediction. Table 2 presents the interplay between technology and psychology concerning cyber threat prediction, which is an output of the literature review.

Table 2. Cyber Behavioral Approachs and Examples.

Examples	Cyber Behavioral Aspects	Interplay	Reference(s)
Social Engineering Attacks	Exploiting human psychology through tactics like phishing.	Combining technical measures (e.g., email filtering) with understanding of psychological vulnerabilities.	[1,36]
Insider Threats	Motivations and behavioral anomalies in potential insider threats.	Integrating user behavioral analytics with technical monitoring.	[20]

 doi:10.20944/preprints202312.0770.v1

Behavioral Analysis for Anomaly Detection	Detecting deviations from typical behavior in cybersecurity systems.	Combining technical data (logs, network traffic) with psychological insights).	[2,25,27]
Phishing Awareness Training	Educating employees about the risks of phishing scams.	Merging technical awareness (recognizing phishing emails) with understanding of persuasive phishing & targeting tactics.	[21,41]
User-Centric Security Design	Designing security interfaces with consideration for human factors.	Balancing technical security measures with enhanced user behavior considerations.	[32]
Cognitive Biometrics	Analyzing user interactions for authentication.	Combining technology (capturing user interactions) with individual differences in cognitive behavior.	[13,30]
Threat Hunting	Proactively searching for signs of cyber threats that evade detection.	Utilizing both technical skills (e.g., analyzing network traffic) and understanding of attacker psychology.	[42]
User-Centric Risk Assessment	Assessing the likelihood of users falling victim to social engineering attacks.	Integrating technical risk assessments with insights into human behavior and vulnerabilities mediated by technology	[28]

Interdisciplinary Psychology-Digital Forensic Analysis (PDFA)

A methodological approach was conceptualizred with combined PDFA analysis [7,27,34], informed by Kirwan's "*The Psychology of Cyber Crime: Concepts and Principles*" to understand the psychological principles behind cybercriminal behaviors [7]. Concurrently, "*Introduction to Cyber Forensic Psychology: Understanding the Mind of Cyber Deviant Perpetrators*" [43] was consulted for digital forensic techniques. Additionally, methodologies from Pollini et al. (2022) in "*Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach*" were utilized to ensure a cyber behavioral understanding of human behavior and cybersecurity interplay [28].

Utilizing recent research, exemplified by the recent CC-Driver project a pan European study of the human and technical drivers of cybercrime (2022)[36], underscores the importance of considering both human and technical determinants in studying cybercrime. This interdisciplinary methodology includes an examination of human-induced and technology-driven aspects of cybercriminal activities is advocated.

- Human (Behavioral) Aspects: This facet explores the motivations, behaviors, and psychological profiles of individuals engaged in cybercrime. Studies seek to understand the reasons behind engagement in cybercriminal practices and the socio-psychological factors influencing such conduct. The role of online anonymity and societal norms within digital environments in cybercriminal activities is investigated [36].

 doi:10.20944/preprints202312.0770.v1

- Technical Aspects: This dimension involves an analysis of the tools, methodologies, and technologies cybercriminals use. The research includes an examination of software and hardware vulnerabilities, the creation and propagation of malware, hacking techniques, and emerging cyber threats. The utilization of cryptocurrencies and the Dark Web in cybercrime is also analyzed [36].

This human and technical "hybrid approach" deployed by the CC-Driver research project suggests that human and technical elements should be considered simultaneously for effective investigation and counteraction of cybercrime [36]. This methodology facilitates formulating strategies to preempt, identify, and counteract cybercriminal activities.

This approach aligns with research by Pollini et al. (2022) and Ferguson-Walter et al. (2021), which emphasizes the incorporation of human-centric factors in cybersecurity strategies [28,39]. Aiken and McMahon's (2014) work on Internet-enabled organized crime highlights the importance of understanding cyber behavioral dynamics from a forensic standpoint for effective investigation and mitigation of cybercrimes [1].

By combining insights into human motivations with technical knowledge of cyber threats, organizations, and law enforcement can develop robust cybersecurity measures and investigative techniques.

Summary of Literature Review

The literature review emphasizes the significance of contemporary disciplines such as cyberpsychology, the role of human factors, and predictive modeling in grasping the complexities of current cybersecurity issues. Merging these fields results in more accurate predictions of cyber threats. The study proposes a methodology that blends technical accuracy with broad principles from the behavioral sciences [17,20,23,30]. This study establishes the value of the Prophet model, as supported by Abdullah et al. (2022)[39] research, and how the prediction model effectively integrates with insights from cyber behavioral science to provide comprehensive threat predictions [9,22,34].

1.5. Research Question and Hypothesis

To address the knowledge gap, the study poses the following research question:

(RQ). How does integrating Psychology-Digital Forensic Analysis (PDFA) with the Prophet model and Cyber Forensic Behavioral Analysis (CFBA) improve the prediction of cyber threats from ASNs in modern cybersecurity?

The following hypotheses are formulated to address this research question:

(H1). The adaptation of "*the Prophet model [39], known for its robust predictive capabilities in various fields, will significantly enhance the accuracy of cyber threat predictions.*" This hypothesis is based on the premise that when applied to cybersecurity data, the Prophet model's advanced analytical capabilities will yield more accurate predictions of potential cyber threats, particularly from ASNs.

(H2). Proposes that a "*combination of cyber incident data with CFBA will result in a more precise evaluation of cyber threats.*" The rationale behind this hypothesis is that integrating technical data (such as logs and incident reports) with insights into cybercriminals' behavioral patterns and motivations will provide a more comprehensive understanding of potential threats. This integrated approach is anticipated to result in a deeper and more complete comprehension of threats, enabling more accurate threat evaluations and effective response strategies.

(H3). "T*he* Interdisciplinary Predictive Model (IPM) *will significantly improve predicting ASN-related cyber threats.*" This hypothesis extends the scope of the study to consider the synergistic effects of merging psychological insights and technical data analysis within a single predictive model. This hypothesis is anchored in the belief that a multidisciplinary approach [34,40], is crucial for a deeper and more accurate understanding of the complex landscape of cyber threats.

 doi:10.20944/preprints202312.0770.v1

1.6. Significance of the Research

This research holds significant importance in cybersecurity, addressing critical cyber threat prediction and management aspects. The study stands out for its innovative integration of **PDFA** with advanced predictive modeling techniques, particularly applying the Prophet model and CFBA.

- **Enhancing Cyber Threat Prediction Accuracy**: At its core, the research advances the precision and accuracy of predicting cyber threats, specifically from ASNs, in contemporary cybersecurity contexts. By effectively combining the technical data from DF (digital forensics) with the behavioral insights of cybercriminal psychology, the study introduces an approach to understanding and mitigating cyber threats.
- **Contribution**: The research significantly contributes to the field by demonstrating the practical application of psychological insights in predicting and preventing cyber threats. It provides a framework for understanding the motivations and behaviors of cybercriminals, thereby enriching the strategies for cyber threat management.
- **Development of the** IPM: A groundbreaking tool synthesizing diverse disciplinary perspectives. This model effectively enhances threat prediction and serves as a template for future cybersecurity research and practice, encouraging a more holistic and integrated approach.
- **Practical Implications for Cybersecurity**: For cybersecurity professionals, the research offers actionable insights and tools for improving defense mechanisms against cyber threats. The findings underscore the need for and benefits of integrating behavioral analysis into technical cybersecurity strategies, paving the way for more comprehensive and effective cyberdefense systems.
- **Future Research and Cybersecurity Strategy Development**: The study's findings lay the groundwork for future cybersecurity research, especially in exploring different predictive models and deepening the understanding of cybercriminal psychology. It advocates for interdisciplinary collaboration, pivotal in developing innovative and robust cybersecurity solutions.

In summary, this research is significant for its approach by combining **PDFA** with IPM. It offers a new perspective on cybersecurity, emphasizing the importance of understanding cyber threats' technical and behavioral dimensions. The study's insights and methodologies are poised to substantially impact the field, contributing to advancing cybersecurity strategies and safeguarding digital infrastructures.

2. Materials and Methods

2.1. Technical and Behavioral Dimensions

This study employs a comprehensive interdisciplinary research approach, bridging digital forensics, cybersecurity, computer science, and the cyber behavioral sciences. It blends quantitative and qualitative methods to tackle the complex challenges of cyber threat prediction in the evolving cybersecurity landscape, adapting to the interplay of technical and behavioral factors [34,40]. Utilizing both technical and behavioral dimensions, the study aims to improve cyber threat prediction accuracy and enhance proactive cybersecurity measures by drawing insights from this multifaceted perspective.

Table 3 presents six critical dimensions for cyber threat prediction, categorized into Technical (quantitative) and Behavioral aspects (qualitative). Table 3 is an output of the literature review and integrates insights from digital forensics, cybersecurity, computer science, forensic psychology, and the cyber behavioral sciences. It highlights the significance of combining technical and behavioral approaches in developing effective cybersecurity strategies.

 doi:10.20944/preprints202312.0770.v1

Table 3. Technical and Behavioral Dimensions.

Dimensions	Description	Key Components and Insights	Supporting References
Technical Dimensions (3) - Quantitative Methods			
Digital Forensics	Systematic examination of digital devices and data to uncover evidence within ASNs.	Trace origin and trajectory of cyber threats.	[26,44]
Cybersecurity	Emphasis on protecting digital assets and systems. Offers tools for securing digital environments.	Designing safeguards informed by behavioral insights.	[6,18,24]
Computer Science	Provides technical foundations for predictive modeling and data analysis. Empowers predictive capabilities.	Employs advanced algorithms and machine learning techniques.	[11,35,38]
Behavioral Dimensions (3) - Qualitative Methods			
Real-world Forensic Psychology	Applies criminal profiling and investigative techniques to digital realm. Understands threat actors' psychological triggers and motivations.	Valuable in predicting cyber threats based on human behavior.	[7,13,45]
Cyber Behavioral Sciences of Cyberpsychology	Focuses on human behavior in digital environments, exploring online interactions, motivations, and responses.	Provides behavioral analysis tools for understanding threat actors.	[9,15,32,46]
Forensic Cyberpsychology	Extends forensic psychology principles to digital domain. Examines behavioral aspects of cybercrime.	Understands and profiles cybercriminals within threat prediction.	[1–3,12,46]

2.2. Description

Figure 2 outlines the research methodology process, encompassing data collection, analysis techniques, data sources, and ethical considerations.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

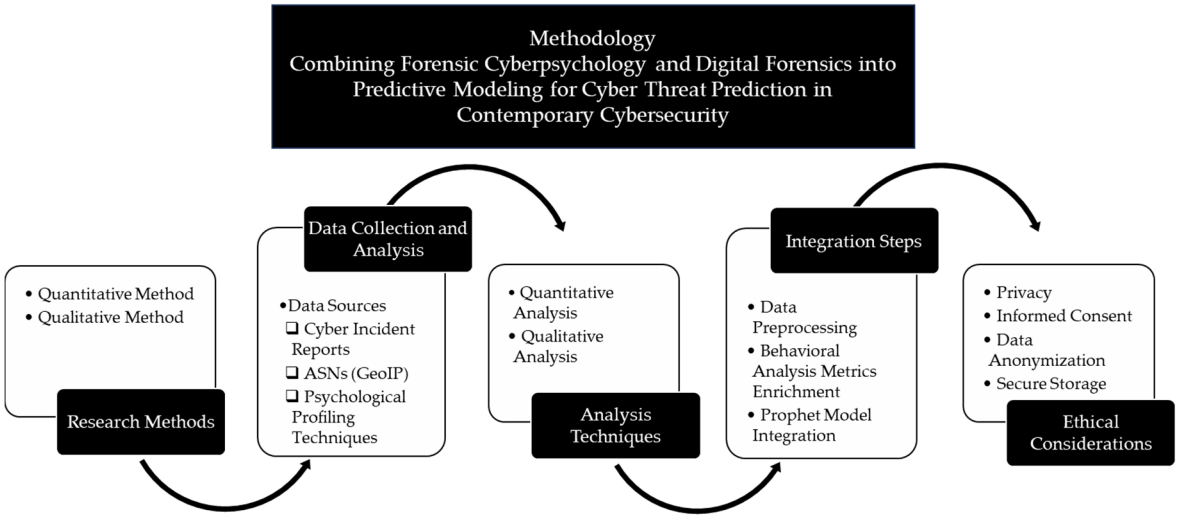

Figure 2. Methodology.

2.2.1. Research Methods

This study employs a mixed-methods approach, combining quantitative and qualitative research methods.

- Quantitative Methods (Technical Dimensions): Utilized statistical analysis, data modeling, and machine learning techniques to explore technical dimensions within Table 3, including digital forensics, cybersecurity, and computer science's roles in proactive threat prediction.
- Qualitative Methods (Behavioral Dimensions): Encompassing a thorough examination of cyber incident data and utilizing psychological techniques to explore the behavioral aspects outlined in Table 3.

This mixed-methods approach aligns with the interdisciplinary nature of cybersecurity research [37,41,45]. It integrates insights from prior research in the field, such as Aiken and McMahon [1] and Kirwan and Power [16], to understand criminal behaviors in cyberspace and techniques used in digital forensic analysis.

2.2.2. Data Collection Data Sources Include:

- Cyber Incident Logs and Reports: Offering historical data on cyber threats and incidents, these provide insights into past attacks and patterns, essential for understanding the technical aspects of cyber threats.
- ASNs: Pertinent to Internet traffic routing and cyber threat propagation, these are critical for identifying the origins and pathways of cyber threats in alignment with the study's focus on ASNs.
- Behavioral Profiling Techniques: Utilized for comprehending the psychological and behavioral dimensions of cybercriminals, aiding in understanding motivations and methods behind cyber threats.

These diverse data sources facilitate an interdisciplinary approach to investigating both technical and behavioral dimensions in cyber threat prediction, aligning with the methodologies discussed by Pollini et al. [28].

2.2.3. Data Analysis

Quantitative Analysis (Technical Dimensions):

- Statistical Analysis: Applied to historical cyber incident data to identify significant patterns, trends, and anomalies.
- Machine Learning Algorithms: Utilized for advanced predictive modeling, enhancing the precision of threat forecasts.

 doi:10.20944/preprints202312.0770.v1

- Prophet Model: Employed to refine predictive capabilities, especially at capturing seasonal trends and recurring patterns in cyber threat data.

Qualitative Analysis (Behavioral Dimensions):

- Cyber Incident Log Analysis: Focused on extracting behavioral insights from cyber incidents, delving into the methods and motivations underlying cyber-attacks.
- Cyber Behavioral Analysis Metric (CBAM): Applied to analyze and score ASNs based on their cyber behavior, identifying behavioral and motivational factors driving cyber threats.
- Interdisciplinary Predictive Model (IPM): Utilizes machine learning algorithms for predictive modeling, integrating Cyber Behavioral Score (CBS) to enrich the Advanced Tailored Predictive Tool (ATPT).

This combined quantitative and qualitative approach enables a comprehensive exploration of both technical and behavioral dimensions, aligning with the interdisciplinary nature of the study and integrating insights from Aiken and McMahon [1].

2.2.4. Interdisciplinary Approach (Steps)

The integration of Cyber Forensic Behavioral Analysis (CFBA) into predictive modeling involves several key steps:

- Data Preprocessing: This involves data cleaning and preparation, crucial for maintaining high data quality and reliability.
- CBAM/CBS Enrichment: Enhances predictive accuracy by incorporating behavioral analysis metrics.
- IPM Model Development: Central to predictive modeling, IPM incorporates historical incident data, ASN information, and CBS insights.
- Prophet ATPT Model Integration: Seamlessly integrates daily observations and behavioral analysis, bolstering prediction precision.

These steps emphasize the interdisciplinary nature of the research, combining technical and behavioral elements to advance the accuracy and effectiveness of cyber threat prediction, as suggested by Kirwan and Power [16].

Figure 3 is a graphical flow diagram of the approach that combines CBFA with DF (Digital Forensics) to create an ATPT for a 45-day prediction model.

- Throughout the process, a feedback loop is present between the CBAM and the CBS, indicating a dynamic and iterative approach to refining the behavioral metrics used within the model.
- The model represents a cutting-edge approach in the field of cybersecurity, where understanding the human element behind cyber threats is as crucial as the technical traces left by such activities.
- The ATPT can be a powerful asset for proactive cyber defense strategies, enabling organizations to anticipate and potentially thwart cyber threats well in advance.

2.2.5. Ethical Considerations (Interdisciplinary Approach)

Ethical principles guiding the research include:

- Handling Sensitive Data: Emphasizes the secure and ethical handling of sensitive cyber incident data, ensuring privacy and confidentiality.
- Informed Consent: Ensuring informed consent is obtained in organizational information cases, emphasizing participants' understanding of research objectives and methods while maintaining anonymity.
- Data Anonymization: Rigorous practices are employed, including the removal or encryption of identifiers, to prevent re-identification.
- Data Security: Robust security measures such as encryption, access controls, and secure storage are implemented to protect sensitive information.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

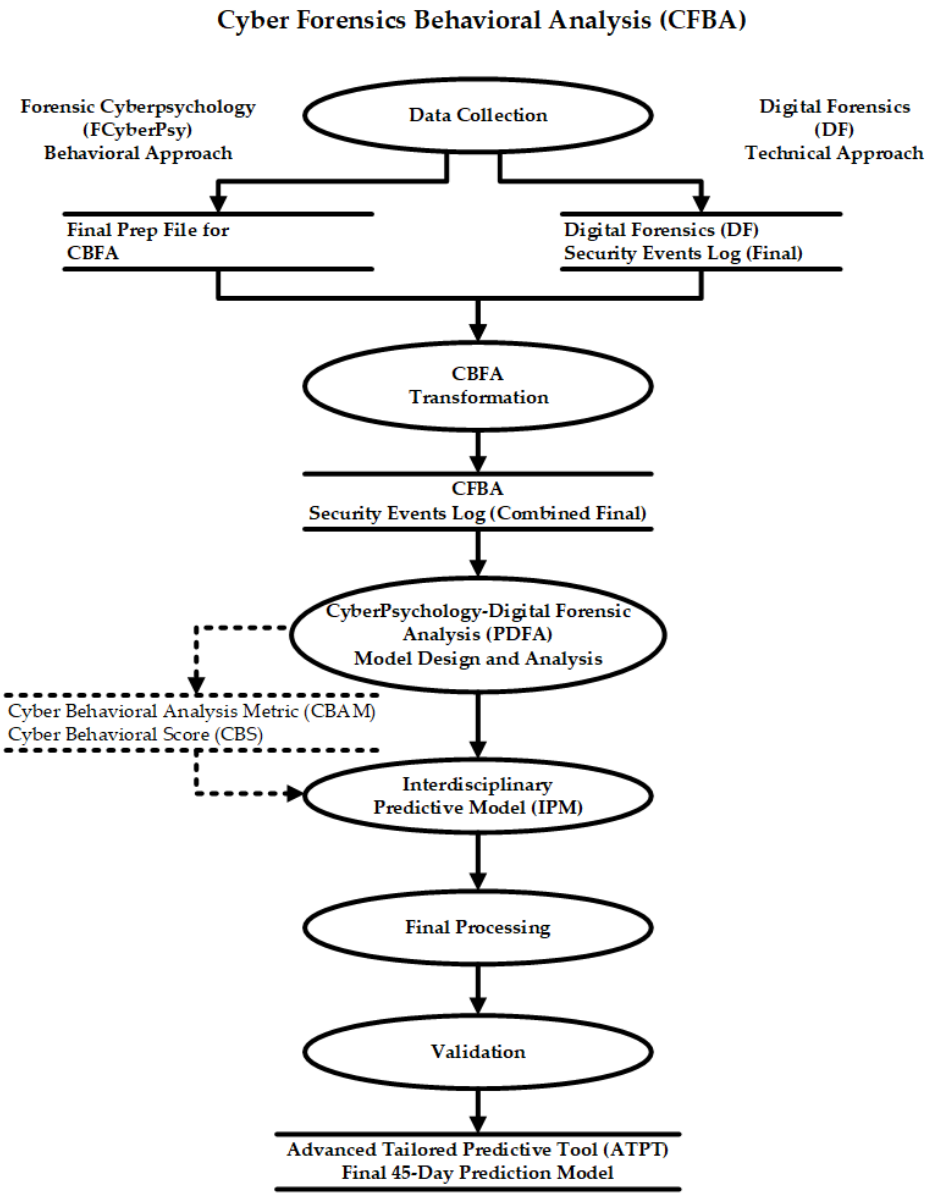

Figure 3. Cyber Forensic Behavioral Analysis (CFBA) Predictive Modeling.

These ethical considerations uphold the integrity and responsibility of the research, safeguarding individual and organizational privacy, as endorsed by Attrill-Smith and Wesson [20].

2.3. *Summary*

In summary, this research methodology [7,8,21,23,29] demonstrates the necessity of a holistic and interdisciplinary approach in addressing the intricate challenges posed by cyber threats. By integrating insights from digital forensics, cybersecurity, computer science, forensic psychology, cyberpsychology, and forensic cyberpsychology, this study offers a comprehensive framework for advancing cyber threat prediction. Ethical considerations, including the secure handling of sensitive data and adherence to ethical guidelines for psychological profiling, underscore the commitment to conducting responsible and impactful research [23]. As cyber threats evolve in complexity, this methodology is a robust foundation for proactive cybersecurity measures, bridging the gap between technical insights, behavioral understanding, and advanced analytical techniques to achieve more precise predictions and enhanced security strategies.

 doi:10.20944/preprints202312.0770.v1

3. Results

3.1. Introduction to Results

This section presents the empirical findings from the Cyber Forensic Behavioral Analysis (CFBA). The focus is enhancing precision and accuracy in predicting cyber threats, particularly from specific ASNs.

- **RQ.** Initially, the study poses a critical question: "How does the integration of Psychology-Digital Forensic Analysis (PDFA) with predictive modeling, particularly using the Prophet model and CFBA, enhance the accuracy and precision of predicting cyber threats from ASNs in contemporary cybersecurity contexts?" This question sets the foundation for the investigation.
- **H1.** The adapted Prophet model demonstrated its effectiveness in accurately forecasting threats from ASNs, thereby substantiating H1. This result highlights the model's utility in enhancing cyber threat prediction accuracy.
- **H2.** Integrating the Cyber Behavioral Analysis Metric (CBAM) and Cyber Behavioral Score (CBS) into the predictive model led to significant improvements in threat prediction accuracy, supporting H2.
- **H3.** The effectiveness of the Interdisciplinary Predictive Model (IPM), by combining CFBA, is confirmed. H3 indicated substantial improvement in predicting ASN-related cyber threats.

In summary, the research demonstrates a significant advancement in cybersecurity by effectively integrating CFBA modeling.

- The interdisciplinary approach has proven pivotal in enhancing cyber threat predictions' accuracy, precision, and reliability.
- Comparative analysis further evidenced the accuracy of the Prophet model in predicting ASN behaviors, aligning with the study's RQ and hypotheses.
- The study underscores the significance of a multidisciplinary approach in cybersecurity, indicating a trend towards more targeted and personalized measures for predicting and mitigating potential cyber threats.

3.2. Definition of Targets and Their Relationship with Internet Service Providers (ISPs)

For this study, three targets represent distinct and separate business sectors, each with its inherent vulnerabilities in the modern digital landscape:

- Target1: An agribusiness leveraging digital systems to oversee a significant livestock count and daily milk production. The reliance on digital tools brings to light potential cybersecurity challenges pertinent to agribusiness. A breach in its network could lead to catastrophic economic losses and supply chain disruption.
- Target2: A financial institution entrusted with vast amounts of sensitive data, thus spotlighting its heightened risk profile and the broader cybersecurity demands within the financial domain.
- Target3: An innovative firm in augmented and virtual reality. The nature of its proprietary data underscores potential vulnerabilities, emphasizing the intricate cybersecurity landscape for technology-focused entities. A cybersecurity breach could expose cutting-edge data to insider threats and corporate espionage risks.

In the context of Internet connectivity, each target entity exclusively utilizes the services of a distinct ISP. These ISPs are substantial and independent entities, operating without any business affiliations among them. Consequently, Target1's internet connectivity is provisioned by ISP1, while Target2 and Target3 are independently serviced by ISP2 and ISP3, respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

3.2. Data Collection and Processing Results

3.2.1. Demographics (Preprocessing)

Data was collected from three ISP customers (Target) over 638 days, data collection yielded no zero-count days for any of the selected Targets. Target3 had the highest average daily entries at 8,598, with a peak daily count reaching 17,245 events, notably different from Target1 and Target2. There were significant daily count variations among the targets, especially with Target3 showing the most fluctuations in attack numbers. Temporal daily patterns for each ISP-Target are displayed in Figure 4, with detailed demographic data in Table 4.

Table 4. Summarized Demographic Data for each ISP-Target.

Parameter	ISP-Target1	ISP-Target2	ISP-Target3
Total number of days	638	638	638
Total number of log entries processed	4,248,365	3,632,477	5,485,828
Total number of days with zero count	0	0	0
Date with the highest number of attacks	2021-11-05 (Count: 11,033)	2023-01-09 (Count: 14,240)	2023-05-22 (Count: 17,245)
Date with the lowest number of attacks	2022-06-18 (Count: 3,180)	2021-12-20 (Count: 3,571)	2022-06-18 (Count: 1,994)
Mean	6,659	5,694	8,598
Standard deviation (std)	1,190	1,237	1,928
Minimum (min) Number of Attacks per Day	3,180	3,571	1,994
25th Percentile (25%)	5,888	4,865.25	7,279
Median (50%)	6,480	5,460	8,427
75th Percentile (75%)	7,204	6,289	9,588
Maximum (max) Number of Attacks per Day	11,033	14,240	17,245
Number of Unique Source IPs	228,954	194,289	233,892
Number of Unique Source Continents	9	8	6
Number of Unique Countries	198	199	195
Number of Unique Source-AS-Number	8,596	8,577	7,618
Number of Unique Source-AS-Org-Names	8,063	8,055	7,141
Number of Unique Destination IP Ports	65,532	65,536	65,531
Number of Unique Destination IP Services	263	265	261

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

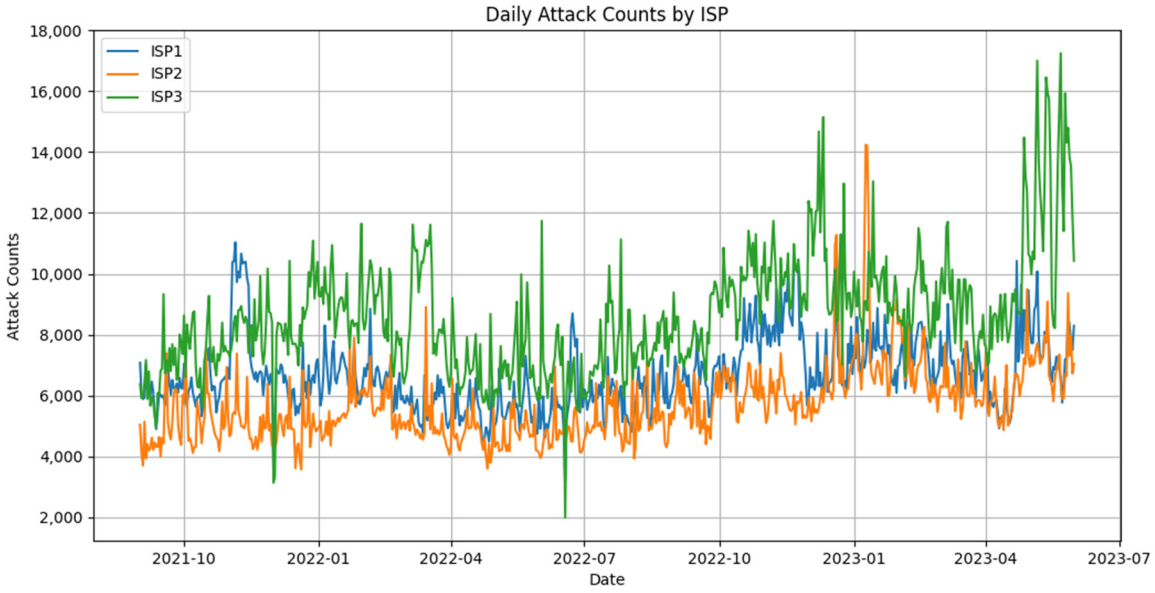

Figure 4. Temporal Daily Patterns.

3.2.2. Observations

Key insights drawn from the dataset are:

- Internet Traffic Volume: The highest internet traffic volume was observed in Target3, while Target2 had the lowest.
- Unique Source IPs: Target3 had the highest number of unique source IPs, whereas Target2 had the fewest.
- IP and AS Organizational Name: Recurring ASN '202425,' associated with the AS Organizational Name 'IP Volume Inc,' was identified across all ISPs, indicating significant Internet activity or events originating from this source. Further exploration of this organization's role and activities is warranted.
- Geographical Origin: Most traffic originated from Europe, closely followed by North America. The United States was the top source country across all targets.
- Data Variations: Disparities were observed in the number of unique countries and continents, most-contacted ports, and services. Variations were also noted in the source ASN and Organizations.

Target3 encountered a notably greater volume of attacks and variability than the other two targets. This observation underscores the need for further investigation to identify specific vulnerabilities or threats responsible for this heightened malicious activity, which will be the primary focus for the remainder of this study.

3.3. H1 - PM (Predictive Modeling) Results (Technical Approach)

The prediction process, spanning a 45-day interval for the three targets, conducted a single-model analysis using the Prophet model to provide insights into the daily occurrences of security events. The derived insights have been organized into categories: accuracy, agreement, analysis, and visualization, facilitating a structured approach toward interpreting and comparative analysis of the prediction results.

Table 5 details the means and standard deviations of the correct predictions and the accuracy percentage for the three targets. It furnishes an initial quantitative insight into the Prophet model's performance.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

Table 5. Means and Standard Deviations.

Metric	Target1 Means	Target1 Standard Deviations	Target2 Means	Target2 Standard Deviations	Target3 Means	Target3 Standard Deviations
Prophet Correct Predictions	5.96	0.87	6.13	0.96	7.04	1.26
Prophet Accuracy	59.56	8.68	61.33	9.57	70.44	12.64

The evaluation over the 45-day prediction interval provides essential insights into the inherent behavior and consistency of the forecasting model across the different targets. These findings set the groundwork for more detailed discussions and interpretations in the subsequent sections of this study. Table 6 contrasts the Prophet model's accuracy and moving averages (MA) across targets, highlighting Target3's significant accuracy.

Table 6. Accuracy and Moving Averages.

Target	Prophet (%)	Prophet MA (%)
Target1	59.56	63.64
Target2	61.33	63.79
Target3	70.44	63.78

3.4. H2 - CBAM (Cyber Behavioral Analysis Metric) (Behavioral Approach)

This study represents a significant advancement in Forensic Science by combining techniques from Rich's research, [25,27] as outlined in Section "1.2.1. Definitions." The CBAM process assigns a final CBS (Cyber Behavioral Score) to each ASN. CBS quantifies ASN behaviors, which facilitates a detailed and precise assignment of a final CBS, significantly improving the accuracy of threat prediction. This method effectively validates H2, which suggests a correlation between predefined behavioral patterns and threat levels. By combining these methodologies, the study reinforces the IPM (Interdisciplinary Predictive Model) and ATPT (Advanced Tailored Predictive Tool) process's effectiveness and marks a notable progression in predicting and understanding cyber threats from ASNs.

3.4.1. CBS Accuracy

Table 7 provides a detailed summary of the performance metrics for the three Targets using the IPM methodology. The table demonstrates the alignment of actual CBS with the expected outcomes, categorizing the results into matching and non-matching CBS. Figure 5 visually compares the matches and non-matches by day for Target3.

Table 7. Percent of Matching Behavior Scores.

n = 450	Matching CBS	Non-Matching CBS	% Matching CBS
Target1-Predicted-ASN-Prophet-BehaviorScore	268	182	59.56%
Target2-Predicted-ASN-Prophet-BehaviorScore	276	174	61.33%
Target3-Predicted-ASN-Prophet-BehaviorScore	317	133	70.44%

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

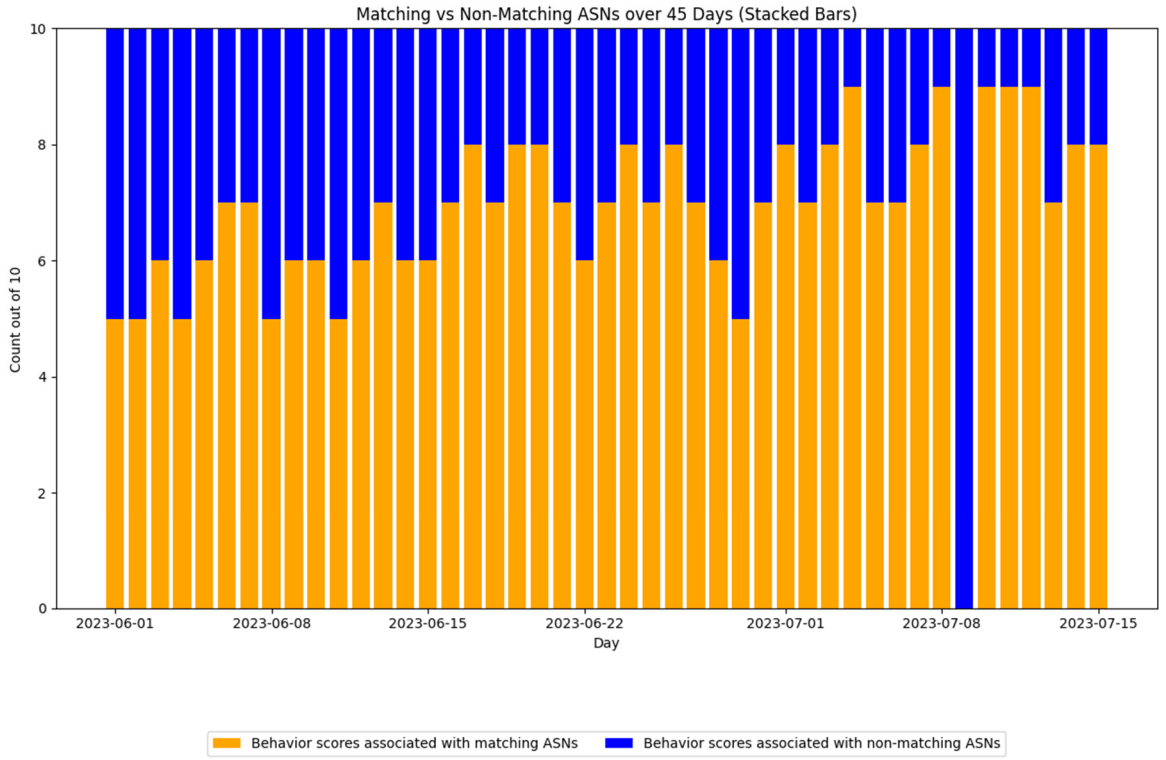

Figure 5. Target3 45-Day Prophet Cyberbehavioral Score Accuracy.

3.4.2. CBS Evaluation

A comparative evaluation of the 45-day predictive period of Target3's CBS was conducted to understand the IPM performance. A sample of this assessment is illustrated in Table 8, which offers insights from two distinct days. Using observed sample data for specific dates, notably 6/1/2023 and 6/15/2023, encompassed predicted and actual ASN CBS. Variations in these scores were observed, indicating potential discrepancies between expected and observed cyber activities.

Table 8. Comparative Evaluation of Behavior Scores.

Day	ISP3 Predicted ASN Prophet	ISP3 Predicted BehaviorScore	ISP3 Actual ASN	ISP3 Actual BehaviorScore
6/1/2023	202425	465	14061	946
6/1/2023	396982	276	202425	465
6/1/2023	49943	171	57523	351
6/1/2023	50867	105	50360	276
6/1/2023	14618	66	396982	276
6/1/2023	16509	55	398324	190
6/1/2023	400161	45	50867	105
6/1/2023	40244	28	204428	91
6/1/2023	209559	28	14618	66
6/1/2023	19750	3	16509	55
6/15/2023	202425	465	202425	465
6/15/2023	49943	171	50360	276

 doi:10.20944/preprints202312.0770.v1

6/15/2023	14618	66	396982	276
6/15/2023	396982	276	57523	351
6/15/2023	19750	3	204428	91
6/15/2023	16509	55	14061	946
6/15/2023	400161	45	14618	66
6/15/2023	57523	351	16509	55
6/15/2023	209559	28	209605	253
6/15/2023	14061	946	398324	190

Consider the data from June 15, 2023, presented in Table 8. The top 10 predicted malicious ASNs had a 60% positive match rate (identified by orange), leaving a 40% discrepancy (identified by blue). Actual CBS thresholds were applied to the missed ASNs (red and yellow), categorizing them based on their associated threat risks. A predetermined threshold of 250 was used for this analysis; it was observed that there were two high-risk (identified by red) and two medium-risk (identified by yellow) threats among the discrepancies. This percentage demonstrates the model's accuracy in predicting potential threats.

4. Discussion

4.1. Overview

This study investigates cyber-attack dynamics within a digital environment, utilizing an interdisciplinary framework that blends technical and behavioral perspectives. It employs predictive modeling, digital forensics, and data analysis to decode network behaviors and strategies employed by cyber threat actors. Concurrently, it integrates insights and learnings from cyber behavioral sciences, as defined in Table 3 and elaborated in Section **1**.4.2.1. This aspect of the study is crucial for understanding cybercriminals' behavioral patterns and motivations, forming a comprehensive approach to predicting cyber threats.

As detailed in Table 3 and Section **1**.4.2.1, the cyber behavioral sciences focus on human interactions and behaviors within digital environments. This area explores online behaviors and responses and provides crucial tools for analyzing the actions of threat actors in cyber contexts. The study utilizes these insights, especially in applying the ATPT (Advanced Tailored Predictive Tool), to better understand cybercriminal activities.

The core of this research lies in the effective combination of technical methods with cyber behavioral scientific insights. By merging technical indicators with insights into the psychology of cybercriminal' behavior, the IPM (Interdisciplinary Predictive Model) achieves greater accuracy in predicting threats. This dual approach not only pinpoints observable network behaviors but also explores the deeper behavioral profiles of threat actors, aiding in early detection and efficient allocation of cybersecurity resources.

The study combines predictive modeling and digital forensics with the cyber behavioral sciences to gain a comprehensive understanding of cyber threats, highlighting the importance of an interdisciplinary methodology. It also points out the need for further investigation into specific vulnerabilities, particularly those observed in 'Target3', which showed a higher frequency and variability of attacks. This method enhances proactive detection and mitigation of cyber threats, offering improved accuracy and depth in analyzing and addressing cyber-attacks.

4.2. Interpretation of Results

The comprehensive investigation into the integration of PDFA (Psychology-Digital Forensic Analysis) with predictive modeling in cyber threat analysis, as evidenced by the application of the IPM, has provided transformative insights.

 doi:10.20944/preprints202312.0770.v1

4.2.1. Research Question**:**

Using the Prophet model, alongside CFBA (Cyber Forensic Behavioral Analysis), allowed for a more comprehensive assessment of potential threats from ASNs and significantly improves the accuracy and precision of cyber threat predictions. This approach is critical for the field of cyber behavioral sciences, specifically the discipline of forensic cyberpsychology, as it emphasizes the importance of understanding psychological aspects of cybercriminal behavior in predicting and mitigating cyber threats. These insights are essential for developing targeted interventions and preventive measures in cybersecurity.

4.2.2. H1 - Prediction

The application of the Prophet model demonstrates the effectiveness of the IPM in enhancing predictive models. The data in Tables 7 and 8 and Figure 5 show the model's accuracy in predicting cyber threats over 45 days, with Target3 exhibiting greater accuracy than Targets 1 and 2, thus confirming H1.

These results underscore the importance of the Prophet model in improving cyber threat prediction [3,17,18,20,39]. The findings have crucial implications for strengthening network security protocols and deepening the understanding of cyber behavioral patterns, highlighting the need for future research to enhance technological defenses and contribute to the theoretical development of the cyber behavioral sciences.

4.2.3. H2 - Cyber Behavioral Scoring

The integration of malicious CBS (Cyber Behavioral Score) with predictive analytics, as evidenced by Target3's 70.44% match rate with real-world behaviors, endorses H2. This result validates the combined threat assessment approach's accuracy, as indicated in Tables 7 and 8 and Figure 5 [8,14,19,24,36].

The study aligns with the frameworks of Rich (2023)[27] and Martineau (2023)[2] and draws on insights from Attrill and Fullwood [45], balancing technological vulnerabilities with CFBA. The predictive vs. actual behavior comparison for Target3 suggests areas for further model refinement.

4.2.4. H3 - Synergistic Effect of the IPM

The research also explores the impact of the synergistic integration of **PDFA** within the IPM. The results showed notable improvement in predicting ASN-related cyber threats, supporting H3.

4.2.5. RQ

These findings highlight the crucial role of integrating **PDFA** in predictive modeling. The development of the IPM and the ATPT represents a successful interdisciplinary approach, substantiating the study's RQ and hypotheses and significantly advancing the understanding and prediction of cyber threats. This research underscores the importance of an integrated approach in cybersecurity, providing essential theoretical and practical insights contributing to developing more sophisticated and effective strategies for managing cyber threats.

 doi:10.20944/preprints202312.0770.v1

4.3. Practical Implications and Recommendations

The study's findings offer substantial implications for cybersecurity professionals and researchers in cyber behavioral sciences. Integrating PDFA with predictive modeling, as demonstrated by the IPM and the Prophet model, significantly enhances the capacity to forecast and mitigate cyber threats.

- **Enhanced Cybersecurity through Predictive Modeling**: The effectiveness of the Prophet model in predicting cyber threats, particularly evident in the accurate forecasting of activities from ASNs, underscores its value in enhancing digital infrastructure security [12,38]. When combined with CFBA, this predictive capability leads to a more comprehensive evaluation of threat landscapes. Such a holistic approach is vital for proactive and reactive cyber defense strategies [3,8,12,19,24,26,28,47].
- **Contribution**: Incorporating behavioral sciences into cyber threat analysis moves beyond technical aspects, offering more profound insights into cybercriminals' psychological behaviors and motivations [1,9,11,13,19,21,48]. This enhanced understanding allows organizations to anticipate vulnerabilities and tailor their defense strategies based on distinct cybercriminal profiles, thereby mitigating cyber-attack risk more effectively [7,11].
- **Dual-Layered Defense Strategy**: An interdisciplinary approach, merging technical defenses with behavioral insights, creates a more robust defense mechanism. This strategy leads to a more detailed and proactive defense approach and ensures efficient resource allocation in cybersecurity measures.

Based on these insights, the following key recommendations are proposed:

- **Implementation of Holistic Predictive Tools**: Cybersecurity strategies should employ predictive modeling tools like the Prophet model in conjunction with behavioral analysis. This integrated approach enables a more holistic threat assessment, identifying both technical vulnerabilities and behavioral patterns [2,15,17,33,42].
- **Ongoing Training in Cyber Attack Psychology**: Cybersecurity teams should receive continuous training focusing on cyber-attack psychology. Such training will equip them with the necessary skills to understand and respond to the evolving nature of cyber threats [13,20,23,30].
- **Collaborative Interdisciplinary Research**: There should be an emphasis on fostering collaboration between technical experts and behavioral scientists. This interdisciplinary research approach will lead to more informed and effective cyber defense strategies [8,28,31,49].
- **Focus on Cyber Behavioral Science Research**: Prioritizing research in the cyber behavioral sciences is essential to bridge the gap between technical and behavioral aspects of cyber threat mitigation. This research will contribute to a better understanding of the human elements in cybersecurity and enhance overall defense capabilities [1,27,28].

In summary, blending technical and cyber behavioral insights is fundamental in addressing the complexities of contemporary cybersecurity. As cyber threats evolve and become more sophisticated, integrating these diverse fields is crucial for ensuring robust digital infrastructure protection and a comprehensive understanding of human behaviors associated with cyber threats [3,12,14,17,31,42].

4.4. Limitations and Future Research

While this study successfully demonstrated the effectiveness of the Prophet model and the IPM in predicting cyber threats, it recognizes certain inherent limitations. Addressing these limitations opens avenues for future research:

- Exploration of Additional Predictive Models: Future research should extend to investigating other predictive models to encompass the evolving nature of cyber threats better. Diversifying the range of models beyond the Prophet model is crucial for adapting to the dynamic nature of cyber threats [14,37,42].
- Deeper Analysis of Cybercriminal Psychology: Further examination of cybercriminals' behavioral patterns and motivations is needed. Although this study incorporated elements of cyber behavioral sciences, a more thorough exploration of cybercriminal behavior's

 doi:10.20944/preprints202312.0770.v1

psychological aspects mediated by technology would enhance understanding and prediction accuracy [10,17,19].

- Broadening the Behavioral Analysis Database: Expanding the database to include a more comprehensive array of cybercriminal behaviors and motivations is recommended. This recommendation would provide a richer and more comprehensive dataset for more precise predictive modeling [9,23,40].
- Differentiating Cyberpsychology and Forensic Cyberpsychology: This differentiation will deepen the understanding ofbehavioral aspects within cybersecurity, providing a more apparent distinction between these overlapping fields [10,18,49].
- Interdisciplinary Collaboration Enhancement: Promoting interdisciplinary collaboration among cybersecurity experts, behavioral scientists, and cyberpsychologists is vital. Such collaboration is critical to developing comprehensive solutions that combine technical robustness with behavioral insights, leading to more effective cyber threat management strategies [12,31,48].

These directions for future research seek to address the current study's limitations and enrich the cyber threat prediction and management field, acknowledging the ever-changing landscape of cyber threats and the complex interplay of human behavior in digital environments.

5. Conclusions

5.1. Summary of Main Findings

This interdisciplinary study successfully predicted cyber threats by combining technical accuracy with behavioral insights [14,42]. It verified the Prophet model's capability to predict threats from specific ASNs using varied data sets [9,14,37,42]. CBSs (Cyber Behavioral Score) were crucial, linking technical forecasts with CFBA (Cyber Forensic Behavioral Analysis), aligned with a cyber behavioral science approach, thus improving understanding of threats [2,10,17,19,25,27].

The study underscored the importance of precise predictive tools that integrate technical defenses with insights into human behaviors in cyber threats [12,50]. Acknowledging the human element's dual role as both a potential threat and a defense mechanism is vital in contemporary cybersecurity [12,31,39,48].

5.2. Contributions to the Field

This research integrates technical methodologies with the cyber behavioral sciences to enhance cybersecurity practices. It confirms the effectiveness of the Prophet model in accurately predicting threats from specific ASNs, making it an asset for cybersecurity professionals [11,14,37,42].

Critical aspects of the study include:

- The pivotal role of CBS is to bridge the gap between predictive analytics and the emerging disciplines of behavioral sciences. These scores improve threat prediction accuracy and provide deeper insights into the motivations of attackers, informing the development of future predictive models [10,12,48].
- Establishing a crucial synergy between **PDFA (**Psychology-Digital Forensic Analysis) highlights the importance of interdisciplinary methods in cybersecurity [10,17,19].

Overall, the research underscores the necessity of comprehending technical and behavioral dimensions in cyber threat scenarios. Its insights are instrumental in guiding future research and forming comprehensive defense strategies against increasingly sophisticated threats [12,31,48].

5.3. Practical Implications

This research offers several practical implications listed below and in Table 9 for enhancing cybersecurity:

- Prophet Model Application: The study validates the Prophet model as a valuable tool in cybersecurity, demonstrating its utility in threat prediction [11,14,37,41].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0770.v1

- Integration of Behavioral Insights: CBS is instrumental in understanding attackers' motivations. This understanding aids in developing proactive defense strategies and targeted training programs [10,17,48].
- Interdisciplinary Approach: The effectiveness of cybersecurity is heightened by merging **PDFA**, offering a more comprehensive strategy for addressing cyber threats [17,19].

Overall, the research advocates for a comprehensive approach that combines technical tools with behavioral insights, significantly improving cyber defense mechanisms in the face of increasingly complex threats.

Table 9. Practical Implications and Contributions.

Dimensions	Description	Key Components and Insights	Supporting References
Potential Contributions to Threat Prediction			
Enhance Behavioral Profiling	Refines behavioral profiling techniques for more accurate cybercriminal profiles.	Improves precision in identifying cybercriminal activities.	[2,3,49]
Analyze Psychological Triggers	Examines psychological triggers and motivations behind cybercriminal behavior.	Provides insights into the "why" behind cyber threats.	[7,15,22]
Utilize Digital Footprints	Analyzes digital footprints left by cyber adversaries, understanding their tactics and techniques.	Enables deeper understanding of cyber adversaries' activities.	[11,47,51]
Detect Patterns	Uses temporal analysis to detect patterns in cyber activities, facilitating proactive threat prediction.	Enhances the ability to identify emerging threats.	[25,35,43,50,52]
Prioritize Threats	Develops risk assessments based on historical data and vulnerabilities, aiding in threat prioritization.	Assists in focusing resources on the most critical threats.	[18,33]
Overall Approach			
Interdisciplinary Lens	Synergizes technical and behavioral dimensions to enhance cyber threat prediction.	Fortifies cybersecurity strategies in an interconnected world.	[9,28,30,34,51]

5.4. Future Research Directions

This study lays the foundation for several future research directions in the field of cyber threat understanding and prediction:

- Enhanced Behavioral Analysis: Investigating cyber attackers' motivations and triggers offers deeper insights [10,17,47].

 doi:10.20944/preprints202312.0770.v1

- Advancement in Predictive Models: Assessing new predictive models and established ones like the Prophet model to refine threat prediction capabilities [14,30,31,39,42].
- Sector-Specific Threat Identification: Applying CBSs across different industries and organizations of varying sizes could uncover unique sector-specific threats, aiding in developing customized cybersecurity measures [3,17,25,26,47].
- Greater Interdisciplinary Integration: Strengthening the integration of real-world behavioral sciences with cyber behavioral sciences to enrich threat analysis [18,28,49].
- Ongoing Model Optimization: Continuously evaluating and updating predictive models ensures they remain effective against evolving cyber threats [11,14,37,42].

Ultimately, this study marks a significant step forward in integrated cyber threat assessment, yet it underscores the necessity for ongoing research that merges technical intelligence with CFBA insights. It provides an important contribution to the general area of the cyber behavioral sciences and the discipline of forensic cyberpsychology in particular.

5.5. Final Thoughts

This study concludes by emphasizing the importance of an interdisciplinary approach in understanding the evolving landscape of cybersecurity [15,44]. Integrating a **PDFA** approach with advanced predictive models like Prophet has deepened the understanding of cyber threats, particularly their human elements, contributing to developing proactive cyber defense strategies [14,17,32,39,42,48,50].

The research highlights the growing significance of the cyber behavioral sciences in understanding and predicting online behaviors, particularly regarding cybercriminals and cyber threat actors. This field extends beyond threat assessment to include various aspects of online interactions, offering potential applications for improving online security and digital user experiences [27,28].

This study underscores the critical role of interdisciplinary collaboration in cybersecurity. Such teamwork is vital for effectively understanding, predicting, and mitigating cyber threats, contributing to a more secure and cohesive online environment, thereby enhancing trust and confidence among digital users [10,49].

In conclusion, facing the challenges of the digital era requires an innovative combination of technical expertise and behavioral insights. This study contributes valuable knowledge to cybersecurity and sets the groundwork for ongoing exploration and innovation. The synergy of **PDFA** and predictive modeling resulting in the development of an adapted IPM and ATPT model that represents a significant advancement in our collective efforts to understand and counteract cyber threats, providing a more secure and resilient digital future [44].

Author Contributions: M.R. has contributed to all aspects of the article. M.A. has contributed substantially to conceptualization; methodology; validation; formal analysis; academic resources; review and editing; and supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The author incurred all costs.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Access to the study data and associated code can be granted upon request to the corresponding author. Public availability is not provided in order to maintain controlled access and to protect the integrity of both the data and the code.

Acknowledgments: The authors wish to sincerely thank Dr. Derex O. Griffin and LTC(R) Bobby G. Rich for their invaluable contributions during the review and refinement of the final draft. Their expert insights and detailed feedback were instrumental in enhancing the quality of this work.

Conflicts of Interest: The author declares no conflicts of interest related to the research.

References

1. Aiken, M.P.; McMahon, C. The Cyberpsychology of Internet Facilitated Organized Crime. Europol Organized Crime Threat Assessment Report (iOCTA). 2014. Available online: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2014 (accessed on [9/23/2023]).
2. Martineau, M.; Spiridon, E.; Aiken, M. A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sci.* **2023**, *3*, 452–477. Available online: https://www.mdpi.com/2673-6756/3/3/32 (accessed on [9/23/2023]).
3. Aiken, M.P.; Davidson, J.C.; Kirichenko, A.; Markatos, E.P. Human Drivers of Cybercrime: A Forensic Cyberpsychology Approach to Behavioral Profiling. [Manuscript in preparation]. 2023.
4. Capitol Technology University. Doctor of Philosophy (PhD) in Cyberpsychology. Capitol Technology University. Available online: https://www.captechu.edu/degrees-and-programs/doctoral-degrees/cyberpsychology-phd (accessed on [10/23/2023]).
5. Capitol Technology University. Doctor of Philosophy (PhD) in Forensic Cyberpsychology. Capitol Technology University. Available online: https://www.captechu.edu/degrees-and-programs/doctoral-degrees/forensic-cyberpsychology-phd (accessed on [10/23/2023]).
6. FBI. Internet Crime Complaint Center Releases 2022 Statistics. Available online: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics (accessed on [11/27/2023]).
7. Kirwan, G. *The Psychology of Cyber Crime: Concepts and Principles*. IGI Global, 2011.
8. Ahmad, A., Hadgkiss, J., & Ruighaver, A. (2012). Incident response teams – challenges in supporting the organisational security function. *Computers Security, 31(5),* 643–652. https://doi.org/10.1016/j.cose.2012.04.001
9. Spitaletta, J.A. Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations. Johns Hopkins University Applied Physics Laboratory, 2021. Available online: https://nsiteam.com/social/wp-content/uploads/2021/07/Invited-Perspective-Operational-Cyber-Psych_FINAL.pdf (accessed on [9/23/2023]).
10. Donalds, C.; Osei-Bryson, K.M. Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach. *Comput. Hum. Behav.* **2019**, 92, 403–418. https://doi.org/10.1016/j.chb.2018.11.039
11. Alrowaily, M. Investigation of Machine Learning Algorithms for Improving Network Intrusion Detection System in Cybersecurity. Ph.D. Dissertation, University of South Florida, Tampa, FL, USA, 2020.
12. Connolly, I.; Palmer, M.; Barton, H.; Kirwan, G. An Introduction to Cyberpsychology; Routledge: Abingdon, UK, 2016.
13. ReSCIND. "Reimagining Security with Cyberpsychology-Informed Network Defenses." Office of the Director of National Intelligence; Intelligence Advanced Research Projects Activity (IARPA). [Online]. Available: https://www.iarpa.gov/research-programs/rescind. Accessed on 10/12/2023.
14. Back, S.; LaPrade, J. The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *Int. J. Cybersec. Intell. Cybercrime* **2019**, *2*(2), 1–4.
15. Aiken, M.P.; Farr, R.; Witschi, D. Cyberchondria, Coronavirus and Cybercrime: A Perfect Storm. In *Handbook of Cyberchondria, Health Literacy, and the Role of Media in Society's Perception of Medical Information*; Aker, H., Aiken, M.P., Eds.; IGI Global: Hershey, PA, USA, 2022a; pp. ch002. https://doi.org/10.4018/978-1-7998-8630-3
16. Kirwan, G.; Power, A. *Cybercrime: The Psychology of Online Offenders*. Cambridge University Press: Cambridge, UK, 2013.
17. Yan, Z. 2012. "Encyclopedia of Cyber Behavior (Volume 1)." IGI Global. ISBN-10: 1668425475.
18. INTERPOL. 2022. "Cybercrime." [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime
19. Gillam, A. R. Technology Threat Avoidance Factors as Predictors of Risky Cybersecurity Behavior Within the Enterprise. Indiana State University, ProQuest Dissertations Publishing. 2019.
20. Greitzer, F. L.; Hohimer, R. E. Modeling human behavior to anticipate insider attacks. *J. Strateg. Secur.* **2011**, *4*(2), 25–48. Available online: https://digitalcommons.usf.edu/jss/vol4/iss2/3/. (accessed on [9/23/2023])
21. McAlaney, J., Thackray, H., & Taylor, J. (2016). The social psychology of cybersecurity. https://www.bps.org.uk / psychologist / social - psychology - cybersecurity (accessed: 06.12.2023)
22. Attrill-Smith, A.; Wesson, C. The Psychology of Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T., Bossler, A., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 653–678. https://doi.org/10.1007/978-3-319-78440-3_25
23. Bada, M.; Nurse, J. R. C. The social and psychological impact of cyber-attacks. arXiv.org, **2019**. [Online]. Available: https://doi.org/10.1016/B978-0-12-816203-3.00004-6. (accessed on [10/17/2023]).
24. Stallings, W. *Network Security Essentials: Applications and Standards*. Pearson, 2017. **ISBN-13:** 978-0134527338.
25. Rich, M.S. Enhancing Microsoft 365 Security: Integrating Digital Forensics Analysis to Detect and Mitigate Adversarial Behavior Patterns. *Forensic*. Sci. 2023, 3, x. https://doi.org/10.3390/forensicsci3030030.

26. Ahsan, M.; Nygard, K. E.; Gomes, R.; Chowdhury, M. M.; Rifat, N.; Connolly, J. F. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. J. Cybersecur. Privacy 2022, 2, N/A, doi:10.3390/jcp2030027.
27. Rich, M.S. Cyberpsychology: A Longitudinal Analysis of Cyber Adversarial Tactics and Techniques. *Analytics* 2023, 2, 618–655. https://doi.org/10.3390/analytics2030035.
28. Pollini, A.; Callari, T. C.; Tedeschi, A.; Ruscio, D.; Save, L.; et al. Leveraging human factors in cybersecurity: An integrated methodological approach. *Cogn. Technol. Work* **2022**, *24*(2), 371–390. Available online: https://link.springer.com/article/10.1007/s10111-021-00683-y. (accessed on [9/23/2023])
29. Tennakoon, H. The Need for a Comprehensive Methodology for Profiling Cyber-Criminals. 2011. Available online: https://scholar.google.com/citations?user=tFdcybAAAAAJ&hl=en. (accessed on [9/23/2023]).
30. Benson, V.; McAlaney, J. *Cyber Influence and Cognitive Threats*. Academic Press, 2019.
31. Braun V. and Clarke, V. (2006) *'Using thematic analysis in psychology.'* Qualitative Research in Psychology, 3(2), pp. 77-101.
32. Parsons, K.; McCormac, A.; Butavicius, M.; Ferguson, L. Human factors and information security: Individual, culture and security environment. Defense Science and Technology Organization, Commonwealth of Australia. **2010**.
33. Plachkinova, M.; Vo, A. A Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure (TRACI). *Communications of the Association for Information Systems* **2022**, 52, e-ISSN:1529-3181.
34. Rohan, R.; Funilkul, S.; Pal, D.; Chutimaskul, W. Understanding of Human Factors in Cybersecurity: A Systematic Literature Review. In International Conference on Computational Performance Evaluation (ComPE) **2021**, 133–140. IEEE. pp. 133-140, Available online: https://ieeexplore-ieee-org.captechu.idm.oclc.org/document/9752358. (accessed on [9/23/2023])
35. Tufail, S.; Riggs, H.; Tariq, M.; Sarwat, A. I. Advancements and Challenges in Machine Learning: A Comprehensive Review of Models, Libraries, Applications, and Algorithms. Electronics 2023, 12, N/A, doi:10.3390/electronics12081789.
36. CC-Driver. Human and Technical Drivers of Cybercrime. 2022. Available online: https://www.ccdriver-h2020.com/project (accessed on 26 September 2022).
37. Weems, C. F.; Ahmed, I.; Golden III, G. R.; Russell, J. D.; Neill, E. L. Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behavior. *PLoS One* **2018**, *13*(12), e0207408. Available online: Link. (accessed on [9/23/2023])
38. Sarker, I. H.; Kayes, A. S. M.; Shahriar, B.; Hamed, A.; Watters, P.; Ng, A. Cybersecurity Data Science: An Overview from Machine Learning Perspective. J. Big Data 2020, 7, N/A, doi:10.1186/s40537-020-00318-5.
39. Abdullah, M. M., Ahmed, H., Hasan, A. A., Ali, D. B., Al-Maeeni, M. K. A., et al. (2022). Designing Predictive Models for Cybercrime Investigation in Iraq. International Journal of Cyber Criminology, 16(2), 47-60. https://doi.org/10.5281/zenodo.4766566
40. Ferguson-Walter, K. J.; Gutzwiller, R. S.; Scott, D. D.; Johnson, C. J. Oppositional human factors in cybersecurity: A preliminary analysis of affective states. In Proceedings of the IEEE Conference 2021, 153–158.
41. Pouani Tientcheu, P. Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals. *D.I.T. Dissertation*, Walden University, Minneapolis, MN, USA, **2021**.
42. Bhardwaj, A.; Kaushik, K.; Alomari, A.; Alsirhani, A.; Alshahrani, M. M.; et al. BTH: Behavior-Based Structured Threat Hunting Framework to Analyze and Detect Advanced Adversaries. *Electronics* **2022**, *11*(19), 2992. Available online: https://www.mdpi.com/2079-9292/11/19/2992. (accessed on [9/23/2023])
43. Khader, M.; et al. *Introduction to Cyber Forensic Psychology: Understanding the Mind of the Cyber Deviant Perpetrators*. World Scientific, 2021.
44. Sites, A. L., Sr. Thinking Like a Cyber Adversary: Exploring the Impact of Language Fluency for Cyber Security. Northcentral University, ProQuest Dissertations Publishing. **2019**. (27663379).
45. Attrill, A.; Fullwood, C. *Applied Cyberpsychology: Practical Applications of Cyberpsychological Theory and Research*. Palgrave Macmillan: New York, NY, USA, 2016.
46. Rohan, R.; Funilkul, S.; Pal, D.; Chutimaskul, W. Understanding of Human Factors in Cybersecurity: A Systematic Literature Review. In International Conference on Computational Performance Evaluation (ComPE) **2021**, 133–140. IEEE. pp. 133-140, Available online: https://ieeexplore-ieee-org.captechu.idm.oclc.org/document/9752358. (accessed on [9/23/2023])
47. Fernandez, G.C. Deep Learning Approaches for Network Intrusion Detection. M.S. Dissertation, The University of Texas at San Antonio, San Antonio, TX, USA, 2019.
48. Kaye, L.K. *Issues and Debates in Cyberpsychology*. Open University Press, 2022.
49. Sutter, O. W. The cyber profile: Determining human behavior through cyber-actions. Capitol Technology University, ProQuest Dissertations Publishing. **2020**. (29257172).
50. Burgio, D.A. Reduction of False Positives in Intrusion Detection Based on Extreme Learning Machine with Situation Awareness. Ph.D. Dissertation, Nova Southeastern University, Fort Lauderdale, FL, USA, 2020.

 doi:10.20944/preprints202312.0770.v1

51. Withers, K. L. A Psychosocial Behavioral Attribution Model: Examining the relationship between the "Dark Triad" and cyber-criminal behaviors impacting social networking sites. Nova Southeastern University, ProQuest Dissertations Publishing. **2019**. (13856408).
52. Roy, K. C. Towards modeling host-based data for cyber-psychological assessment in cyber threat detection. Ph.D. Thesis, The University of Texas at San Antonio, San Antonio, TX, USA, **2022**; ProQuest Dissertations Publishing, p. 29261425.