forensic sciences

MDPI

Article

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

Marshall S. Rich * and Mary P. Aiken

Department of Cyberpsychology, Capitol Technology University, Laurel, MD 20708, USA; mpaiken@captechu.edu
* Correspondence: mrich@captechu.edu

Abstract: The Cyber Forensics Behavioral Analysis (CFBA) model merges Cyber Behavioral Sciences and Digital Forensics to improve the prediction and effectiveness of cyber threats from Autonomous System Numbers (ASNs). Traditional cybersecurity strategies, focused mainly on technical aspects, must be revised for the complex cyber threat landscape. This research proposes an approach combining technical expertise with cybercriminal behavior insights. The study utilizes a mixed-methods approach and integrates various disciplines, including digital forensics, cybersecurity, computer science, and forensic psychology. Central to the model are four key concepts: forensic cyberpsychology, digital forensics, predictive modeling, and the Cyber Behavioral Analysis Metric (CBAM) and Score (CBS) for evaluating ASNs. The CFBA model addresses initial challenges in traditional cyber defense methods and emphasizes the need for an interdisciplinary, comprehensive approach. This research offers practical tools and frameworks for accurately predicting cyber threats, advocating for ongoing collaboration in the ever-evolving field of cybersecurity.

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

Citation: Rich, M.S.; Aiken, M.P. An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sci.* **2024**, *4*, 110–151. https://doi.org/10.3390/forensicsci4010008

Academic Editors: Ricardo Jorge Dinis-Oliveira and Marcus Rogers

Received: 5 December 2023
Revised: 3 February 2024
Accepted: 24 February 2024
Published: 4 March 2024

1. Introduction

The fields of cyber behavioral sciences, integrating psychology, cyberpsychology, IT, cybersecurity, and digital forensics are pivotal for understanding human aspects in cyber interactions. Together they shed light on behavioral patterns, motivations, and intentions in cyberspace, contributing significantly to comprehending the human factors influencing cybersecurity [1–3].

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

This study's approach, which leverages live data from Internet Service Provider (ISP) customers to assess ASN predictive models, is a pivotal aspect, underscoring its substantial real-world applicability. The criticality of ASNs in the efficient routing of internet traffic and the overall management of the global internet infrastructure cannot be overstated, making this an essential point in substantiating the study's significance.

1.1. Problem Overview

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 behavior of cybercriminals [1,4–7].

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, robust in their technical aspects, require combining cybercrime's behavioral dimensions [7–10]. This gap highlights the limitations of traditional cybersecurity methods, which primarily focus on reactive measures rather than proactive threat prediction and prevention [11–13].

The evolving nature of cybercriminal activity, often undetected by traditional technical approaches, highlights the importance of incorporating cyber behavioral sciences into cybersecurity practices [14–16]. As cyber criminals use more sophisticated techniques and psychological strategies, insights from this field become crucial to developing a better understanding and predicting these complex threats [15–17].

Therefore, the problem of 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] established a foundation for criminal profiling using a comprehensive framework known 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 to this study, overarchingly named Cyber Forensics Behavioral Analysis (CFBA). Using the CFBA, this research will blend technical cybersecurity measures with understanding cybercriminal behavior to enhance the accuracy and effectiveness of threat prediction and prevention strategies [1,18–21].

By adopting this integrated approach, the study aims to pivot cybersecurity strategies from being predominantly reactive to becoming more proactive and adaptive. This shift is critical in effectively countering the sophisticated and psychologically driven cyber threats of today's digital landscape.

1.2. Structure of the Journal Article

This article begins with an introduction highlighting the need for an integrated model of cyber behavioral sciences, outlining the problem, defining disciplines, identifying knowledge gaps, and stating study objectives. It then details the materials and methods, describing the interdisciplinary approach, research framework, methods used, and data collection. The results section discusses empirical findings, addresses research questions, and analyzes data, including demographics and predictive modeling. The discussion interprets these results and notes the study's contributions, limitations, and future research directions. Finally, the paper summarizes key findings and underscores the importance of interdisciplinary methods in cybersecurity, suggesting future research areas.

1.3. Real-World Relevance of the Study: Integrating Cyber Behavioral Science and Forensics

The study uses real-world ISP customer data to evaluate the use of ASNs in predictive models relevant to cyber behavioral science and digital forensics. ASNs are vital for global internet traffic management, and inaccuracies in their prediction can lead to technical issues and security vulnerabilities. From a cyber behavioral standpoint, analyzing live data helps us understand behaviors, including those of cybercriminals, by observing patterns in internet traffic, which is supported by Lundie et al.'s (2024) [22] research on reversing social engineering in cyber defense. Their findings bolster the practical applicability of cyber behavioral science within the digital forensics domain.

This study's real-world data are critical for use in identifying and preventing malicious online activities. In digital forensics, focusing on ASNs aids in analyzing internet traffic flow, which is crucial for investigating cyberattacks and identifying vulnerabilities. Accurate ASN predictions enhance forensic capabilities to detect and respond to cyber incidents, improving network security. Overall, the study bridges theory and practice in cybersecurity and digital forensics, enhancing network behavioral understanding and applying forensic methods for better security. This study attempts to bridge the gap between theoretical

research and practical cybersecurity needs. This practical application underscores the study's commitment to addressing the evolving landscape of cyber threats with tangible, data-driven solutions.

1.4. Knowledge Gaps

Despite the advancement of individual disciplines, a significant gap persists in effectively integrating the understanding of cybercriminal behavior and motivation with the technical aspects of threat prediction [3,9]. Insights from "Intention to Hack? Applying the Theory of Planned Behavior to Youth Criminal Hacking" [23] could be used to highlight the importance of understanding the behavioral aspects of cybercrime. This study's exploration of the motivations behind youth criminal hacking can inform this study's discussion on the "why" behind cybercrimes, complementing the technical "how" and "when" aspects of cyber threat prediction.

CFBA offers insights into the "why" behind cybercrimes; arguably, digital forensics and predictive modeling focus more on the "how" and "when". This disconnect hampers the understanding and prediction of cyber threats. For instance, predictive models can forecast potential cyberattacks, and understanding the behavioral triggers, drivers, and patterns of cybercriminal behavior could significantly refine these predictions [24]. Similarly, integrating cyberpsychological profiles into digital forensics investigations could enhance accuracy regarding attribution, that is, identifying potential cybercriminals (lone and organized) and understanding respective modus operandi [1,25,26].

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, showing the outcomes of the literature review, showcases interdisciplinary approaches, integrating specialized knowledge from various domains to enhance our understanding of cybersecurity and uncover overlooked critical factors [18,27]. References accompanying each approach offer additional context and support the role of transdisciplinarity in advancing cybersecurity practices [6].

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	[28,29]
Human-Centric Risk Assessment	Integrating cyber risk assessment with behavioral insights	Highlights gaps in risk assessment that overlook human factors	[9,30]
Cybersecurity Education and Training	Collaboration between cybersecurity and instructional design	Uncovers gaps in training effectiveness, guides learner-focused programs	[5,21]
Human-Centric Security Policies	Merging legal, cybersecurity, and behavioral science expertise	Exposes gaps in policies that disregard human behavior	[31,32]
User-Centered Security Design	Collaboration among cybersecurity, UX design, and HCI experts	Uncovers gaps in security designs that hinder usability	[19,22]
Cyber Threat Intelligence Analysis	Combining cybersecurity and social science expertise	Highlights gaps in threat intelligence that omit behavioral aspects	[6,15,23,24]

1.5. Glossary of Key Terms and Definitions for CFBA Framework

In this study, CFBA is a transdisciplinary overarching approach that combines elements from the cyber behavioral sciences, digital forensics, predictive modeling, and cyber threat intelligence [2].

1.5.1. Cyber Forensic Behavioral Analysis (CFBA) Framework

The CFBA framework, a predictive modeling approach, is part of a comprehensive research methodology combining various dimensions of digital forensics and cyber behavioral sciences to improve the accuracy of cyber threat predictions by integrating both technical and behavioral dimensions. Section 2.1 discusses in detail the technical and behavioral dimensions.

Figure 1 represents a high-level overview of the framework designed to predict cyber threats and provide insights into mitigation strategies, reflecting the complex dynamics of cybercriminal behavior. The Advanced Tailored Predictive Tool (ATPT) outcome leverages strengths from cyberpsychology, digital forensics, cybersecurity modeling, and detailed behavioral analysis from the Cyber Behavioral Analysis Metric (CBAM) and Cyber Behavioral Score (CBS).

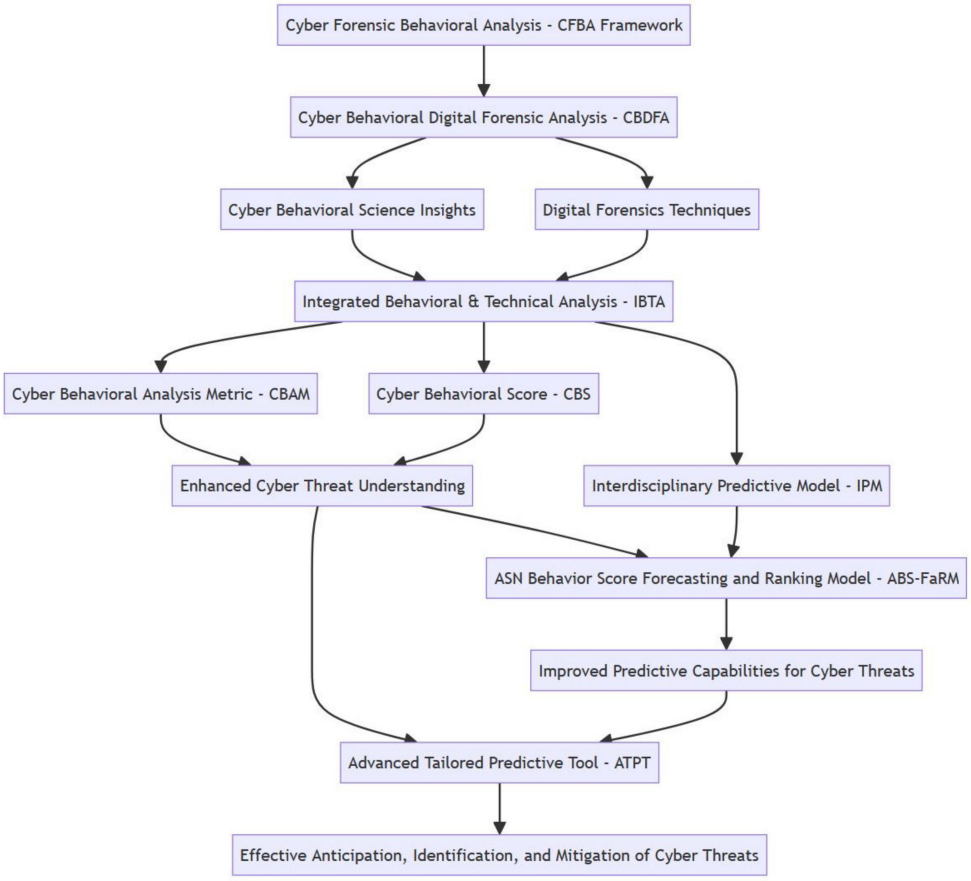

Figure 1. Cyber Forensic Behavioral Analysis (CFBA) framework.

1.5.2. Glossary of Conceptual and Theoretical Key Terms and Definitions

This glossary focuses on cyber behavior and forensics' conceptual and theoretical aspects. Understanding these terms is crucial for grasping the integrated approach of the CFBA model.

1. Behavioral analysis (BA): The study and interpretation of behavior, particularly in cybersecurity, to understand the actions and motivations of cybercriminals. It forms the basis for predicting and mitigating cyber threats [2,3].
2. Behavioral threat intelligence (BTI): A subset of cyber threat intelligence that focuses specifically on the behavior of cyber adversaries. It involves analyzing patterns, tactics, and motivations to effectively anticipate and respond to cyber threats [6,24].
3. Cyber behavioral analysis (CBA): A specific application of behavioral analysis in the cyber domain. It integrates the study of cybercriminal behavior with digital forensics to enhance threat prediction and response strategies [2].

4. Cyber defense (CD): The strategies, tools, and processes used to protect against cyberattacks and threats. It encompasses a range of activities, from technical defenses to behavioral analysis and threat intelligence [4,21].
5. Cyber Forensics Behavioral Analysis (CFBA): An interdisciplinary approach that integrates cyber forensics with behavioral analysis to enhance the understanding and prediction of cyber threats [2,3].
6. Cyberpsychology: The study of the human mind and behavior in cyberspace. It examines how psychological principles apply to online behaviors and the interactions between individuals and digital technologies [33].
7. Forensic cyberpsychology: An interdisciplinary field combining aspects of cyberpsychology and digital forensics. It focuses on understanding the psychological aspects of cybercriminals and applying this knowledge to forensic investigations [4,15,34].

1.5.3. Glossary of Technical and Operational Key Terms and Acronyms

This list of key terms is focused on including a broader range of terms and acronyms, extending beyond the CFBA model to encompass more technical and operational aspects of cybersecurity and network management.

1. Accuracy: A composite measure of how well the predictive models can correctly identify and categorize ASNs, emphasizing the correctness of predictions (precision) and the completeness of detecting relevant cases (recall), as synthesized in the F1 score [8,35].
2. Advanced Tailored Predictive Tool (ATPT): A specialized tool designed for advanced, customized prediction in the context of cybersecurity, utilizing specific algorithms and data analytics techniques [8,36].
3. Autonomous System Numbers (ASNs): Unique identifiers allocated to each autonomous system (AS) on the internet, used for routing traffic [21,37].
4. ASN Behavior Score Forecasting and Ranking Model (ABS-FaRM): A key component of the Interdisciplinary Predictive Model, ABS-FaRM focuses on forecasting and ranking ASN behaviors using advanced algorithms [8,38].
5. Cyber Behavioral Analysis Metric (CBAM): A metric used in cyber behavioral analysis to quantify and evaluate specific behaviors or trends in cyber environments [25,26].
6. Cyber Behavioral Digital Forensic Analysis (CBDFA): An approach that combines cyber behavioral analysis with digital forensic techniques to investigate cyber incidents more comprehensively [4,10].
7. Cyber Behavioral Score (CBS): A scoring system that quantifies cyber behavior, often used in predictive models and threat assessments [26].
8. Digital forensics (DF): Collecting, analyzing, and preserving digital evidence from cyber incidents. It is a crucial component of digital investigations and plays a significant role in the CFBA model [7,25].
9. Integrated Behavioral and Technical Analysis (IBTA): A methodology that combines behavioral science insights with technical data, providing a more complete view of cyber threats [2,27].
10. Interdisciplinary Predictive Model (IPM): A predictive model that integrates various disciplinary perspectives and methodologies for a comprehensive approach to prediction in a specific field [2,12,27,28,35]. IPM, a behavioral dimension, uses cybercriminals' behavioral profiles and patterns in predictive algorithms by utilizing the ABS-FaRM functions.
11. Internet Service Provider (ISP): A company that provides services for accessing, using, or participating online.
12. Predictive modeling (PM): A technical dimension, employs various algorithms and machine learning (ML) techniques to predict future cyberattacks based on historical data and patterns [12,35].

1.5.4. Summary of Definitions

In summary, CFBA is a more comprehensive mode of multidisciplinary approach informed by various research areas such as forensic cyberpsychology, digital forensics, predictive modeling, and behavioral analysis metrics. CBDFA 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.

1.6. Interdisciplinary CBDFA Approach

The conceptual foundation of the study is grounded in an integrated methodological approach incorporating CBDFA, as previously shown in Figure 1. This approach, informed by Kirwan's (2011) [4] exploration of cybercriminal psychology and techniques from cyber forensic psychology, facilitates a comprehensive understanding of the psychological principles underlying cybercrime and the details of digital forensics.

The study employs interdisciplinary methodologies that integrate human factors in cybersecurity, as advocated by Pollini et al. (2022) [27]. This approach ensures a thorough understanding of how human behavior intersects with cybersecurity. Additionally, the significance of analyzing both human and technical elements in cybercrime is emphasized, drawing on insights from the CC-Driver project (2022) [39].

A "hybrid approach" that concurrently addresses human and technical factors, as recommended by the CC-Driver project, is essential for effectively investigating and countering cybercrime [36].

The CBDFA approach aligns with Ferguson-Walter et al. (2021) [40] and Aiken and McMahon (2014) [1], underscoring the importance of including human-centric factors in cybersecurity strategies and the significance of understanding cyber behavioral dynamics from a forensic perspective.

Critical Aspects of the Approach:

- Behavioral (human) aspects—Investigations into cybercriminals' motivations, behaviors, and psychological profiles. The influence of online anonymity and societal norms in digital environments on cybercriminal activities is explored [39];
- Technical aspects—Analyses of the tools and methodologies used by cybercriminals, focusing on software and hardware vulnerabilities, malware propagation, hacking techniques, and emerging threats [39].

1.7. Expanding the CBDFA Approach with IPM

The study's approach merges the interdisciplinary CBDFA approach with the introduction of IPM within CFBA. In line with the multidisciplinary nature of cyber behavioral sciences, this approach leverages CBDFA to enhance cybersecurity, particularly in accurately predicting cyber threats from ASNs [9,11]. It represents a significant advancement in CFBA by combining technical analysis with a deep understanding of cybercriminal behavior.

The IPM, incorporating CBS, creates a comprehensive framework for threat prediction, as supported by Connolly et al. (2016) [9] and Martineau et al. (2023) [2]. This approach signifies a shift in cybersecurity strategies, integrating cyber behavioral science aspects as noted by Ahmad et al. (2012) [5] and McAlaney et al. (2016) [18], and focuses on refining ASN threat prediction accuracy, as supported by Back and LaPrade (2019) [11] and Pollini et al. (2022) [27]. The primary aim of IPM is to improve the precision and accuracy of predictions from ASNs, utilizing ML algorithms and CBDFA [11,27]. This integration of cyberpsychology, digital forensics, and behavioral analysis marks a significant advancement in CFBA [8,12,13,28,30,36], emphasizing the use of diverse expertise to address complex cyber threats.

Building on Figure 1, Figure 2 provides a structured overview that maps out the interconnected components of the modeling system. It details the process flow from CBDFA, through quantifying and analyzing cybercriminal behavior to applying these

insights for comprehensive threat mitigation solutions. The narrative in Sections 1.6 and 1.7 aligns with the visual representation in Figure 2, ensuring a comprehensive understanding of the CFBA framework and its components.

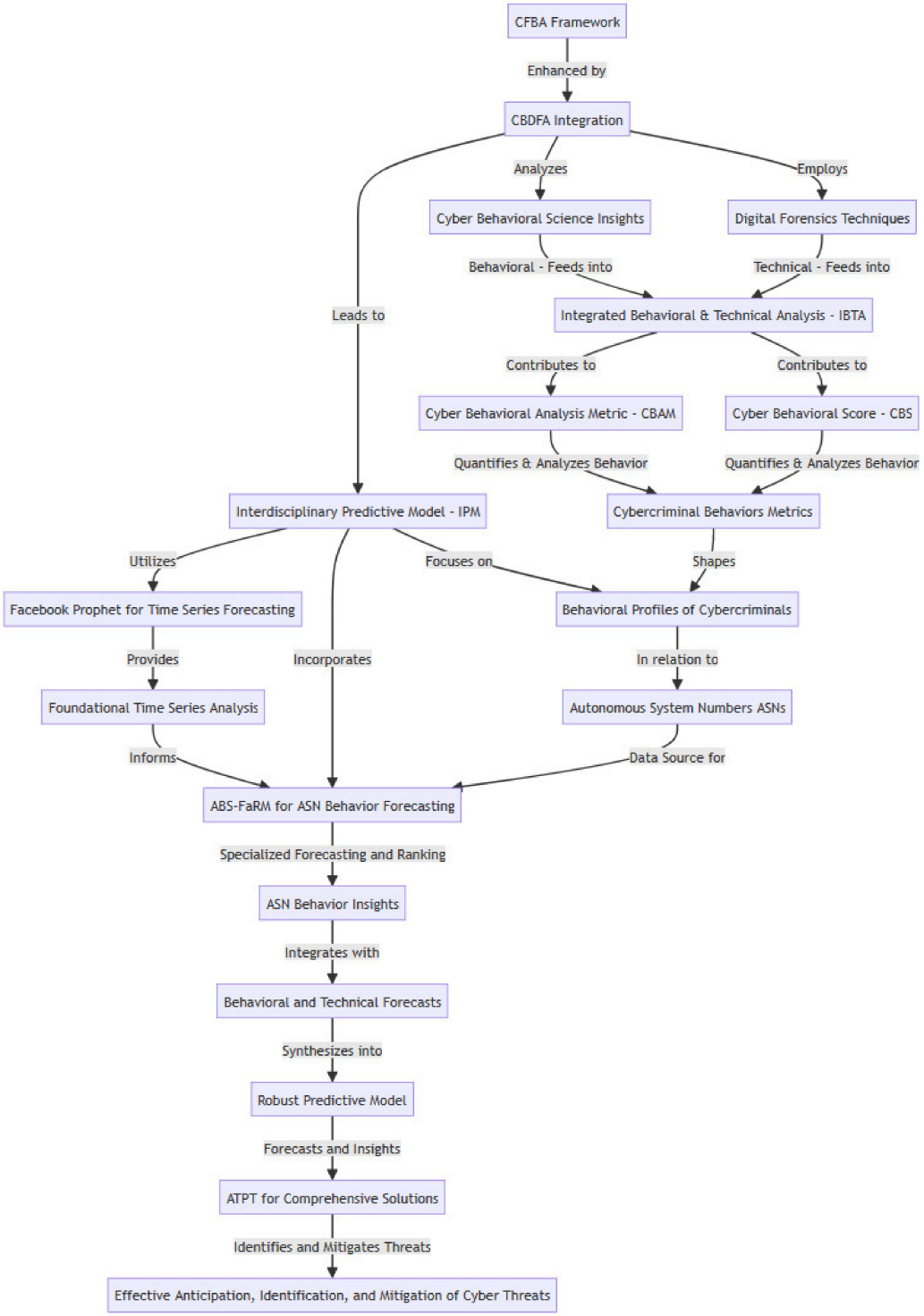

Figure 2. Structured CFBA framework outline.

1.8. Literature Review

In response to the evolving cybersecurity landscape, this literature review explores existing research in cyber threat prediction and the diverse disciplines of CBDFA. The primary focus of this study is to elevate the accuracy and precision of cyber threat pre-

diction originating from ASNs by combining these disciplines using CBDFA. 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.

1.8.1. Research Methodology

For this comprehensive literature review, 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, 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 needed to be more varied.

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 2757 additional articles. The further inclusion of "Digital Forensics" led to 162 more articles. Considering "Predictive Modeling" added 94 articles, while 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.

1.8.2. Overview [6,10]

Traditionally, the emphasis in cyber-related endeavors has predominantly been on technical strategies and solutions. These technical approaches are founded on 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 [10]. The ReSCIND program aims to augment traditional defenses by exploiting cognitive biases and decision-making vulnerabilities inherent in cyberattackers [10], and is notably informed by the discipline of cyberpsychology.

However, the sheer complexity and vitality of cyber threats underscore the need for a more comprehensive and human-centered approach. Spitaletta's (2021) [6] work on "Operational Cyberpsychology" accentuates the transition from solely relying on technical tools to incorporating an understanding of behaviors and motivations. 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 and behavioral and motivational patterns [6].

Cyber Behavioral Sciences [1,2,8–14,18,20]

Technical approaches [8,9] provide tangible defenses against cyber threats; however, understanding these threats' psychological and behavioral aspects is essential [2,10,18,20]. Combining these perspectives offers a view of the cyber threat landscape that encompasses various aspects [11–13,18]. Forensic cyberpsychology, an emerging subdiscipline of cyberpsychology, as highlighted in the Europol report, emphasizes this need [1]. Aiken and McMahon (2014) [1] proposed an active defense strategy, focusing on understanding criminal behavior in cyberspace for more effective prediction and counteraction. Yan (2012) [14]

also emphasized 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 [3,9,11,13,16–18,21,39]

Cyberpsychology explores the human aspect of cybercrime and cybersecurity. Aiken et al. (2022) [3] stressed the importance of understanding human drivers in cybercrime for behavioral profiling. Connolly et al. (2016) [9] introduced the foundations of cyberpsychology and its significance in cybercrime prevention. Arguably, the psychological perspective enhances predictive modeling efforts [11,13,16–18,21,39].

Human Factors in Cybersecurity [3,17,26,28,30]

Understanding human factors in cybersecurity is crucial. Tennakoon (2011) [28] advocated for a holistic approach, combining learnings from CBDFA to enhance predictive modeling. Greitzer and Hohimer (2011) [17] supported this assertion, highlighting the importance of modeling human behavior to anticipate insider attacks. Incorporating human factors may significantly improve cyber threat prediction [3,26,30].

Cybercrime and Adversarial Tactics [1,26,39]

Understanding cyber adversaries' tactics is pivotal. Rich's (2023) [26] analysis provides insights into cyber adversarial tactics. Aiken and McMahon's (2014) [1] early work delves into the cyberpsychology of internet-facilitated organized crime. Recognizing psychological aspects is crucial for integrating advances in the cyber behavioral sciences into predictive modeling. The recent CC-Driver Project (2022) [39] underscores the importance of considering human and technical determinants in studying cybercrime.

Psychology of Cybercrime [13,19]

Kirwan and Power (2013) [13] outlined the psychology of online offenders, contributing to understanding cybercriminal motivation. Attrill-Smith and Wesson's work on "The Psychology of Cybercrime" [19] reinforced the importance of psychological factors in cybercrime and the enhancement of predictive modeling for better threat identification.

Social and Psychological Impact of Cyberattacks [20,41]

Bada and Nurse (2019) [20] investigated the social and psychological impacts of cyberattacks. Weems et al. (2018) [41] studied susceptibility and resilience to cyber threats. Understanding these dynamics is crucial for merging the cyber behavioral sciences, specifically into predictive modeling.

PM and ML in Cybersecurity [8,38,42]

PM and ML in cybersecurity have gained significant traction in recent research [11,38,42]. PM and ML are critical in addressing cybersecurity challenges, as noted by Sarker et al. (2020) [38], who emphasized the importance of ML in this domain. Alrowaily (2020) [8] focused 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) [42] examined 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.

Recent Research Trends and Predictive Models in Cybersecurity [37,43,44]

Recent scholarly contributions have significantly enriched the understanding of CBDFA in cybersecurity. Kia et al.'s (2024) [37] research exemplifies the integration of

data-driven models, using CVE data and supervised ML algorithms, in enhancing cyber threat predictions. This approach aligns with CBDFA's aim to combine technical precision with behavioral insights.

Furthermore, the bibliometric review by Wu et al. (2023) [43] expands the understanding of the field's evolution. This review highlights the growing depth and scope of research, reinforcing the necessity for a transdisciplinary approach in CBDFA, integrating psychology, forensics, and data analytics.

Additionally, Samtani et al. (2020) [44] emphasized the critical role of AI in cybersecurity, particularly in analyzing diverse data for threat detection and management. This article aligns with CBDFA's objective by combining advanced AI methods with an understanding of human factors, furthering the efficacy of cyber threat prediction.

These recent studies contribute valuable insights, emphasizing the integration of multidisciplinary approaches and advanced technologies in cybersecurity, thus enhancing the foundations of CBDFA.

Cyber Behavioral Approaches to Cybersecurity [11,40]

Cyber behavioral approaches to cybersecurity consider human factors and emotional aspects. Back and LaPrade (2019) [11] discussed cybercrime prevention strategies, while Ferguson-Walter et al. (2021) [40] analyzed 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, an output of the literature review.

Table 2. Cyber behavioral approaches 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.	[1,39]
Insider Threats	Motivations and behavioral anomalies in potential insider threats.	Integrating user behavioral analytics with technical monitoring.	[17]
Behavioral Analysis for Anomaly Detection	Detecting deviations from typical behavior in cybersecurity systems.	Combining technical data (logs, network traffic) with psychological insights.	[2,25,26]
Phishing Awareness Training	Educating employees about the risks of phishing scams.	Merging technical awareness (recognizing phishing emails) with understanding of persuasive phishing and targeting tactics.	[18,45]
User-Centric Security Design	Designing security interfaces with consideration of human factors.	Balancing technical security measures with enhanced user behavior considerations.	[30]
Cognitive Biometrics	Analyzing user interactions for authentication.	Combining technology (capturing user interactions) with individual differences in cognitive behavior.	[10,24]
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.	[46]
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.	[27]

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 [14,17,20,24]. This study establishes the value of the Prophet model, as supported by Abdullah et al.'s (2022) [42] research, and how the prediction model effectively integrates insights from cyber behavioral science to provide comprehensive threat predictions [6,19,32].

1.9. Research Question and Hypothesis

This study poses the following research question to address the knowledge gap.

RQ. *How does integrating CBDFA with the Prophet model and CFBA improve the prediction of cyber threats from ASNs in modern cybersecurity?*

The following hypotheses are formulated to address this research question:

H1. *The Prophet model [42], 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. *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. *The IPM will significantly improve predictions of ASN-related cyber threats.*

This hypothesis extends the scope of the study to consider the synergistic effects of merging behavioral insights and technical data analysis within a single predictive model. This hypothesis is anchored in the belief that a multidisciplinary approach [32,40] is crucial for a deeper and more accurate understanding of the complex landscape of cyber threats.

1.10. 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 CBDFA 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 digital forensics (DF) with the behavioral insights of the cybercriminal, the study introduces an approach to understanding and mitigating cyber threats [8,25].
- Contribution: The research significantly contributes to the field by demonstrating the practical application of cyber behavioral 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 [3,27].

- Development of the IPM: A 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 [2,36].
- 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 cyber defense systems [21,30].
- 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, which is pivotal in developing innovative and robust cybersecurity solutions [13,44].

In summary, this research is significant for its approach in combining CBDFA 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

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 [32,40]. The study aims to improve cyber threat prediction accuracy and enhance proactive cybersecurity by drawing insights from technical and behavioral dimensions.

2.1. Technical and Behavioral Dimensions

Table 3 presents six critical dimensions for cyber threat prediction, categorized into technical (quantitative) and behavioral aspects (qualitative). Table 3 is the 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.

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.	[35,47]
Cybersecurity	Emphasis on protecting digital assets and systems. Offers tools for securing digital environments.	Designing safeguards informed by behavioral insights.	[15,21,48]
Computer Science	Provides technical foundations for predictive modeling and data analysis. Empowers predictive capabilities.	Employs advanced algorithms and ML techniques.	[8,36,38]

Table 3. *Cont.*

Dimensions	Description	Key Components and Insights	Supporting References
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.	[4,10,49]
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.	[6,12,30,50]
Forensic Cyberpsychology	Extends forensic psychology principles to digital domain. Examines behavioral aspects of cybercrime.	Understands and profiles cybercriminals within threat prediction.	[1–3,9,50]

By integrating these dimensions, the study presents a unique transdisciplinary approach. For example, insights from digital forensics enhance the behavioral profiling techniques used in forensic cyberpsychology, leading to more precise predictions of cyber threats. This synthesis improves accuracy and enriches the understanding of the complex interplay between technological vulnerabilities and human behaviors. The practical application of this approach is evident in scenarios where combined technical and behavioral analyses have successfully preempted sophisticated cyberattacks, demonstrating its efficacy in real-world cybersecurity challenges [3,25].

2.2. Description of the Research Approach

Figure 3 presents the sequential steps and methodologies involved in a mixed methods research approach combining quantitative and qualitative methods for complex data analysis. It starts with extensive data collection and thorough preprocessing for quality assurance. The analysis uses advanced statistical and machine learning techniques and behavioral models to extract technical and behavioral insights. This process culminates in a 45-day dynamic predictive model featuring iterative feedback loops and prioritizing ethical data management and security, showcasing a contemporary, adaptable approach to data-driven research [29,31,32].

2.2.1. Research Methods

This study employs a mixed-methods approach.
Quantitative analysis (technical dimensions):

- Statistical analysis—Used historical cyber incident data to find critical patterns and anomalies;
- ML algorithms—For enhanced predictive modeling and accurate threat forecasting;
- Prophet model—Refines predictions, capturing trends in cyber threat data;
- Involvement of digital forensics, cybersecurity, and computer science in threat prediction.

Qualitative analysis (behavioral dimensions):

- Cyber Incident Log Analysis—Extracts behavioral insights from cyber incidents, exploring attackers' methods and motives;
- CBAM—Assesses ASNs based on cyber behavior to identify underlying behavioral drivers of threats;
- IPM—Integrates ML and cyber behavioral science for predictive modeling;
- Uses cyber behavioral science to study behavioral aspects of cyber incidents.

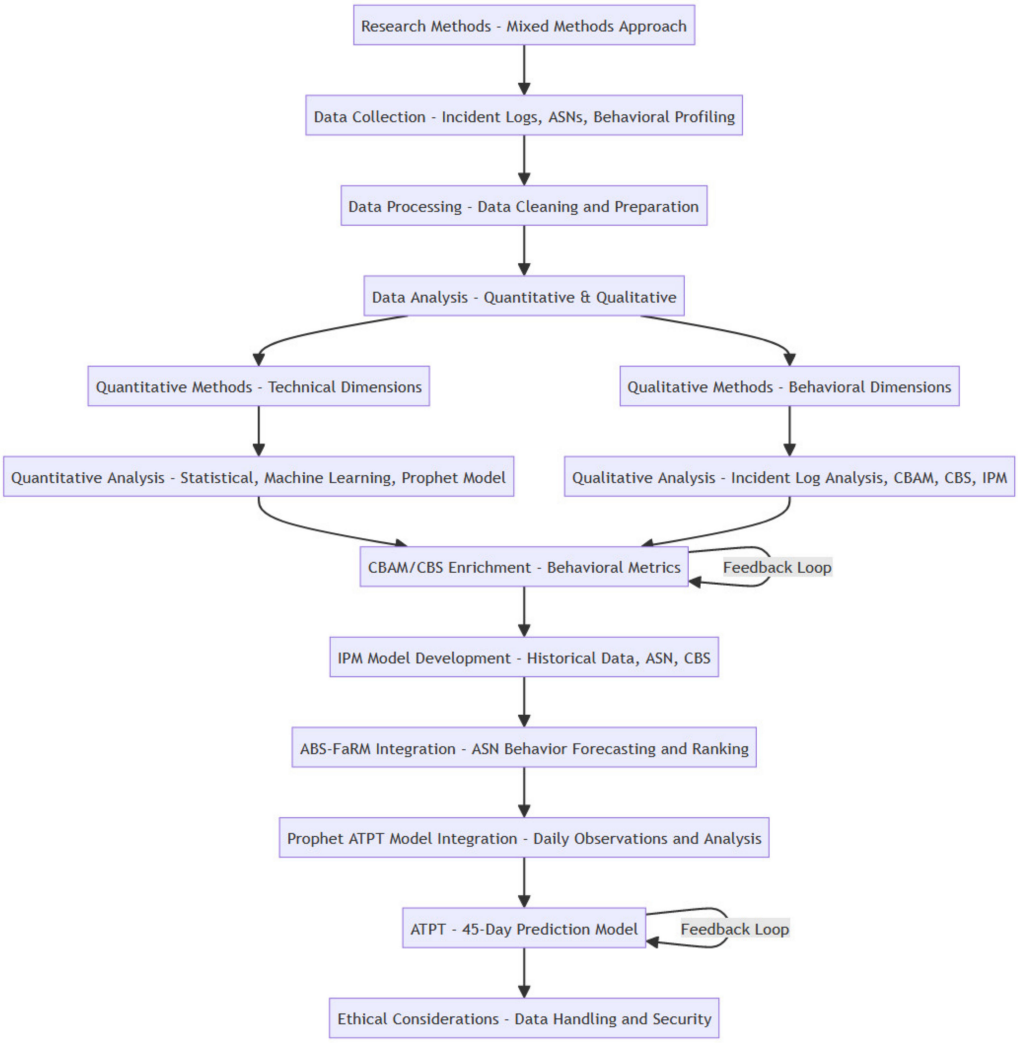

Figure 3. Research workflow and methodology.

This approach aligns with the interdisciplinary nature of cybersecurity research [41,50,51] by combining quantitative and qualitative methods to adhere to cybersecurity research's interdisciplinary essence. It builds on the prior work of Aiken and McMahon [1] and Kirwan and Power [13] to understand criminal behaviors in cyberspace and digital forensics, thoroughly exploring both technical and behavioral aspects of cyber threats.

2.2.2. Data Sources

- Cyber Incident Logs and Reports: Offer historical insights into past cyber threats, essential for technical understanding.
- GeoIP ASN data: Key for internet traffic and cyber threat analysis, especially for ASN-related threats.
- Behavioral profiling techniques: Analyze cybercriminal psychology and behavior to understand their motives and tactics.
- Cyber threat intelligence: Combines log data with threat intelligence for identifying malicious and advanced threats.

These diverse data sources enable a thorough study of both technical and behavioral facets of cyber threat prediction, aligning with the methodologies of Pollini et al. (2022) [27].

2.2.3. Interdisciplinary Approach (Steps)

The integration of CFBA into predictive modeling involves key steps:

- Data preprocessing—Essential for data quality and reliability;
- CBAM/CBS enrichment—Adds behavioral analysis metrics for better prediction accuracy;
- IPM model development—Utilizes historical data, ASN information, and CBS insights for core predictive modeling;
- ABS-FaRM—Focuses on forecasting and ranking ASN behaviors using advanced algorithms;
- Prophet ATPT model integration—Merges daily observations with behavioral analysis to enhance prediction precision;
- A continuous feedback loop between CBAM and CBS ensures the dynamic refinement of behavioral metrics.

These steps highlight the research's interdisciplinary approach, merging technical and behavioral aspects to improve cyber threat prediction accuracy, following the guidelines of Aiken and McMahon [1] and Kirwan and Power [13].

2.2.4. Ethical Considerations (Interdisciplinary Approach)

Ethical principles guiding the research include:

- Secure data handling—Stresses secure and ethical management of sensitive cyber incident data, ensuring privacy and confidentiality;
- Informed consent—Prioritizes obtaining consent in organizational studies, clarifying research aims and methods while maintaining anonymity;
- Data anonymization—Applies strict methods like removing or encrypting identifiers to prevent re-identification;
- Data security—Enforces strong protections like encryption, access controls, and secure storage for data safety.

These ethical guidelines ensure responsible research conduct, protecting individual and organizational privacy, in line with Attrill-Smith and Wesson [19].

2.3. Initial Data Collection and Preprocessing Procedures

The initial data collection process gathered security incident logs from Cisco Firewalls, using nineteen log files from real-world customers across six ISP IP subnets from four ISPs, including both Tier-1 and Tier-2 providers. A Python script was created to standardize the date range across all ISP logs for comparative analysis and forensic reporting, reducing manual errors and saving time. This standardization was crucial for aligning datasets with overlapping dates.

Preprocessing showed data from three ISP customers over 638 days (1 September 2021, to 31 May 2023), with no zero-count days. The Python script focused on data extraction, transformation, and loading (ETL) [8,25], leading to consistent CSV files [31] corresponding to each original file but limited to the standard date range. Preprocessing ensured uniformity across datasets and reduced data size by excluding irrelevant records [38], streamlining further data handling, and emphasizing advanced data processing in forensic science [25].

2.4. Initial Data Preparation and Analysis Procedures

The "Security Log Preprocessing and IP Address Extraction Workflow" is a structured process for handling security log files. It involves sanitization, field extraction, normalization, and data transformation to refine and improve the log files. Key steps include:

- Addressing missing values, eliminating duplicates, and converting data to a categorical format;
- Anonymizing confidential information;
- Creating structured new fields.

This methodical approach results in a final log file that is clean, organized, and secure, making it suitable for further security analysis and investigative work.

2.5. ML and Statistical Analysis Methods

ML and statistical methods were used to analyze demographic data from the final log files for each Target, leveraging Python's data science and ML capabilities [31,35].

The process included:

- Applying descriptive statistics such as mean, median, standard deviation, and percentiles to gain insights into data trends and variations [8];
- ML techniques, including classification algorithms and Facebook Prophet for time series forecasting, offer a specialized approach to handling data variations [38].

Python automated this analysis, utilizing libraries such as Pandas for data manipulation, NumPy for numerical computations, and Scikit-learn for ML [25,36]. This process led to a detailed demographic summary, as presented in Section 3.2.2. Demographics (Preprocessing).

2.6. ASN Behavior Score Forecasting and Ranking Model (ABS-FaRM) Workflow

The ABS-FaRM model, integrated with the CFBA model in cybersecurity, uses the Prophet technique from Facebook Prophet to predict future network activities of ASNs and rank them based on activity and behavior scores. This approach enhances the CFBA's predictive and behavioral analysis capabilities in relation to cyber threats, especially from different ASNs [35,38].

The model functions in phases: data ingestion via Python script, detailed ASN analysis, forecasting with the Prophet algorithm, and aggregating and ranking ASNs based on activity and behavior scores. Implementing the phases complements the CFBA's focus on understanding cybercriminal behavior and digital evidence analysis [8,25].

ABS-FaRM's inclusion improves cybersecurity predictive modeling by blending technical tools like Prophet with insights into cybercriminal behavior, boosting the effectiveness of cybersecurity strategies [3,27]. The methodology of the Python script, crucial for this process, is detailed in stages in Figure 4, providing clarity on its procedural steps within this study [25,31,36,38].

Let D be the dataset containing ASN records with fields 'GeoIP ASN', 'Date', 'Count', and 'Behavior Score'.

1. **Unique ASN Extraction**:
   $\text{Unique ASNs} = \{\text{ASN}_1, \text{ASN}_2, \ldots, \text{ASN}_n\} \subseteq D(\text{'GeoIP ASN'})$
2. **Individual ASN Forecasting**:
   For each ASN_i in Unique ASNs:
   - Filter D for ASN_i: $D_i = D[D(\text{'GeoIP ASN'}) = \text{ASN}_i]$
   - Prepare data for Prophet: $D_{i,\text{Prophet}} = \{(d, c, b) \mid (d, c, b) \in D_i(\text{'Date'}, \text{'Count'}, \text{'Behavior Score'})\}$
   - Prophet Model Forecast for 45 days: $F_i = \text{ProphetForecast}(D_{i,\text{Prophet}}, 45)$
3. **Combining Forecasts**:
   $F_{\text{combined}} = \bigcup_{i=1}^{n} F_i$
4. **Pivoting and Ranking**:
   - Pivot F_{combined} to get P with dates as rows and ASNs as columns.
   - Calculate combined scores (multiplication of 'yhat' and 'Behavior Score'): $C = P \times B$ where B is the matrix of Behavior Scores.
   - Rank ASNs based on C: $R = \text{Rank}(C)$
5. **Top 20 ASNs Selection**:
   For each date d in R:
   $\text{Top 20 ASNs}_d = \{\text{ASN} \mid R(d, \text{ASN}) \leq 20\}$
6. **Output**:
   $\text{Output} = \bigcup_{d \in R} \{(d, \text{Top 20 ASNs}_d)\}$

Figure 4. ASN behavior score forecasting and ranking model workflow.

The dependent variables throughout the process are the behavior score and the final C (combined scores), which are used to rank and select the top ASNs. The independent variables are the date, count, and ASN, which generate the forecasts and rankings. The methodology's strength lies in its systematic approach to extracting, forecasting, and ranking ASNs based on behavior scores, a sequence of dependent and independent variable transformations.

2.7. Evaluation Metrics for ASN Predictions

The methodology focuses on evaluating ASN predictions, adapting traditional binary classification metrics for the multi-class nature of ASNs [8,36]. It emphasizes True Positives (TP), False Positives (FP), and False Negatives (FN), redefining "True Negatives" and "False Negatives' in the context of ASN predictions [31].

For each Target, precision, recall, and the F1 score are calculated using these outcomes [37]. The study uses a macro-averaging technique to compute metrics per class and then average them. This technique ensures the fair consideration of all classes, addressing label imbalance [38]. This evaluation approach aligns with the unique characteristics of multi-class classification, demonstrating a comprehensive methodology for ASN prediction assessment.

2.8. Accuracy Assessment for ASN Predictions

Accuracy in the multi-class classification system, with a focus on ASNs, is evaluated using precision, recall, and the F1 score:

1. Precision—Measures the accuracy of correct ASN predictions against all predicted positives (TP and FP) [8];
2. Recall—Assesses the model's ability to identify all relevant ASNs, calculated as the ratio of true positives to actual positives (TP plus FN) [37];
3. F1 Score—The harmonic mean of precision and recall, balancing identifying correct ASNs and minimizing incorrect ones, with a higher score indicating better performance [38].

These metrics offer a specialized approach to multi-class classification in cybersecurity, aiming for a comprehensive evaluation of model accuracy in relation to identifying and categorizing cyber threats [36].

2.9. Summary

In summary, this research methodology [4,5,18,20,28] 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, and 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 [20].

As cyber threats evolve in complexity, this methodology represents 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.

3. Results

This section outlines the main empirical results when using the CFBA model, highlighting its role in enhancing the precision and accuracy of cyber threat predictions, particularly in relation to specific ASNs. It discusses how combining CBDFA with predictive tools like the Prophet model improves cyber threat forecasting, demonstrating the importance of an interdisciplinary approach in advancing cybersecurity's predictive effectiveness and confirming the study's research questions and hypotheses.

3.1. Introduction to Results

This section details the empirical results of CFBA, focusing on improving the accuracy and precision of predicting cyber threats using specific ASNs. The key findings include the following:

- The study's central question investigated the impact of integrating CBDFA with predictive modeling (using the Prophet model and CFBA) on cyber threat prediction from ASNs;
- H1—The effectiveness of the adapted Prophet model in accurately forecasting ASN threats is confirmed;
- H2—Integrating the CBAM and CBS into the model significantly boosts threat prediction accuracy;
- H3—The combined use of the IPM and CFBA leads to substantial improvements in predicting ASN-related threats.

In conclusion, the research demonstrates a significant leap in cybersecurity through the effective integration of CFBA modeling, with an interdisciplinary approach crucial for enhancing the precision and reliability of cyber threat predictions. Comparative analyses validate the Prophet model's accuracy in predicting ASN behaviors, support the study's research question and hypotheses, and highlight the importance of a multidisciplinary approach in cybersecurity for more targeted and effective threat prediction and mitigation strategies.

3.2. Data Collection and Processing Results

This section expands on the foundational data handling and analysis procedures detailed in Sections 2.3–2.8, focusing on the outcomes and insights gained from data collection and processing. It acts as a bridge from the general methodologies to specific findings related to cyber threat demographics, setting the stage for a deeper understanding of the cyber threat landscape.

3.2.1. Definition of Targets and Relationship with ISPs

Three targets represent distinct and separate real-world business sectors, each with 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 engaged 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 independent entities, operating without any business affiliations among them. Consequently, Target1's internet connectivity is provisioned by ISP1, and Target2 and Target3 are independently serviced by ISP2 and ISP3, respectively.

3.2.2. Demographics (Preprocessing)

This section emphasizes the significance of demographics in understanding the cyber threat landscape. It presents data collected from three Targets over 638 days, highlighting the diverse nature of cyber threats, especially with Target3. The temporal and demographic data analysis, illustrated in Figure 5 and Table 4, provides a solid base for grasping cyber threat activities' distinct characteristics and trends across different targets. This in-depth

analysis of threat patterns supports the study's goal of enhancing cyber threat prediction, which is crucial for the effectiveness of the predictive models discussed in Sections 2.3–2.8, improving their forecasting relevance and accuracy.

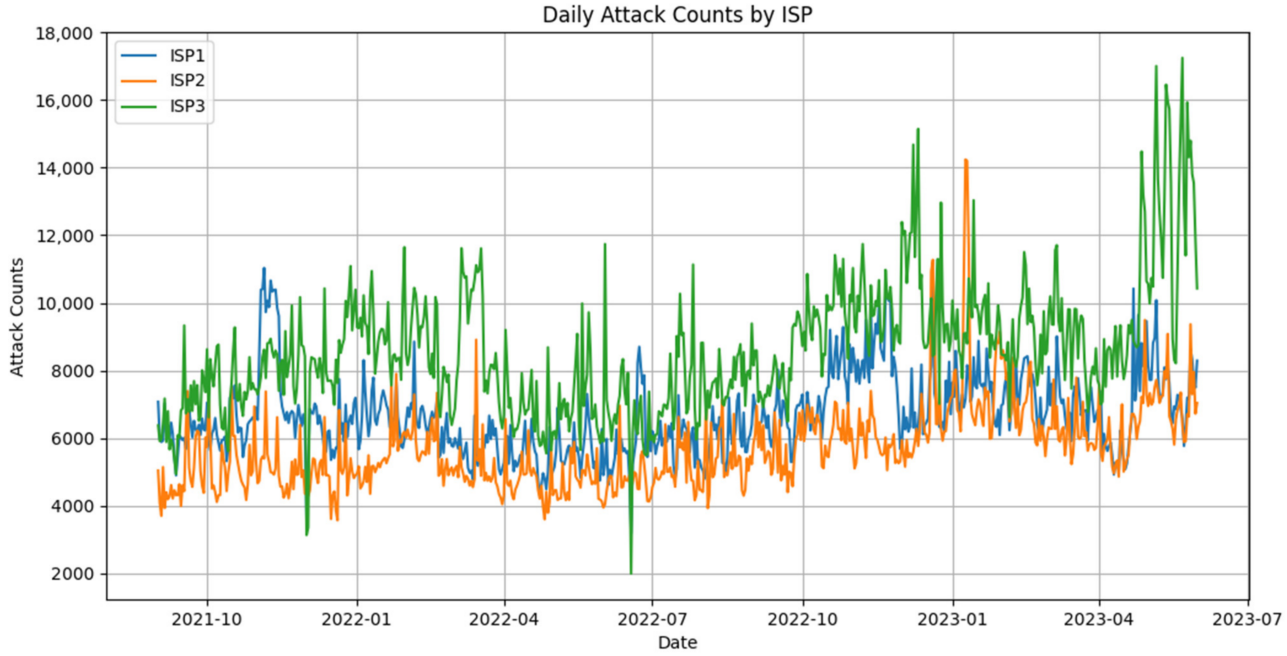

Figure 5. Temporal daily patterns.

Table 4. Summarized demographic data for each ISP-Target.

Parameter	ISP-Target1	ISP-Target2	ISP-Target3
Start date	1 September 2021	1 September 2021	1 September 2021
End date	31 May 2023	31 May 2023	31 May 2023
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	5 November 2021	9 January 2023	22 May 2023
Date with the lowest number of attacks	18 June 2022	20 December 2021	18 June 2022
Mean	6659	5694	8598
Standard deviation (std)	1190	1237	1928
Minimum (min) number of attacks per day	3180	3571	1994
25th Percentile (25%)	5888	4865.25	7279
Median (50%)	6480	5460	8427
75th Percentile (75%)	7204	6289	9588
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	8596	8577	7618
Number of unique Source-AS-Org-Names	8063	8055	7141
Number of unique destination IP ports	65,532	65,536	65,531
Number of unique destination IP services	263	265	261

3.2.3. Key Insights from the Datasets

- Internet traffic volume—Target3 experienced the highest, Target2 the lowest.
- Unique source IPs—Most at Target3, least at Target2.
- IP and AS organizational name—ASN "202425", linked to "IP Volume Inc.", was prominent across all ISPs, suggesting notable internet activity from this source and meriting further exploration.

- Geographical origin—Europe and North America were significant sources, with the United States as the top contributing country.
- Data variations—Differences in unique countries, continents, contacted ports, services, source ASNs, and organizations were noted.

Target3 showed a significantly higher attack volume and variability, highlighting the need for the in-depth analysis of specific vulnerabilities or threats responsible for increased malicious activity.

Target3 will be the primary focus for the remainder of the study.

3.3. H1—PM Results (Technical Approach)

Sections 2.6–2.8 and Figure 4 describe a 45-day prediction process for three targets using the Prophet model. This analysis, focused on daily security events, is categorized into accuracy, agreement, analysis, and visualization for the structured interpretation and comparison of results. Table 5 presents the means, standard deviations of correct predictions, and accuracy percentages for each target, enabling a quantitative evaluation of the Prophet model's performance.

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 45-day evaluation offers key insights into the forecasting model's behavior and consistency across different targets, laying the foundation for deeper discussions in later sections. Table 6 compares the Prophet model's accuracy and moving averages across targets, notably emphasizing Target3's high 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—IPM and ATPT CBAM Effectiveness (Behavioral Approach)

The CBAM process assigns a final CBS to each ASN, quantifying behaviors to enhance threat prediction accuracy [25,26], which supports H2, indicating a link between behavioral patterns and threat levels. By integrating these methods, the study bolsters the effectiveness of the IPM and ATPT processes, marking a significant advancement in predicting and comprehending cyber threats from ASNs.

3.4.1. IPM Meta-Analytic Evaluation

Table 7 summarizes the performance metrics for three real-world Targets using the IPM methodology, showing how actual CBS aligns with expected outcomes by categorizing results into matching and non-matching CBS. The study's unique multi-class classification approach resulted in equal precision, recall, and F1 scores for each target. This was attributed to a balanced distribution of predictive errors (FPs and FNs) and their specific counting and averaging methods in this research.

Table 7. Percent of matching behavior scores.

Target Predicted ASN Prophet Behavior Score	Total True Positives	Total False Positives	Total False Negatives	Total Precision	Total Recall	Total F1 Score
Target1	220	230	230	0.4889	0.4889	0.4889
Target2	276	174	174	0.6133	0.6133	0.6133
Target3	317	133	133	0.7044	0.7044	0.7044

The study conducted a meta-analytic evaluation of ASN prediction accuracy using models from three real-world targets. ASN predictions were the independent variables, and the dependent variables were precision, recall, and the F1 score, reflecting predictive accuracy.

Critical aspects of the evaluation include:

- ASNs are treated categorically, focusing on True Positives (TPs), False Positives (FPs), and False Negatives (FNs), which are suitable for multi-class classification;
- Precision, recall, and F1 scores were computed for each ISP, with an unconventional interpretation of "TNs" and "FNs" as "FPs" in this multi-class context;
- A macro-averaging process ensured balanced assessments across all classes.

The analysis found:

- Target1's model had moderate accuracy (F1 score: 0.489), indicating balanced predictive errors;
- Target2's model showed higher accuracy (F1 score: 0.613) with a conservative prediction pattern, having fewer FPs but missing some actual positives;
- Target3's model had the best performance (F1 score: 0.704) and was precise and sensitive to actual positive cases.

The F1 score was critical in this analysis, balancing precision and recall. Target3's model, with the highest F1 score, demonstrated robustness, indicating its efficacy in operational contexts for precise and reliable ASN predictions in network management and cybersecurity. Figure 6 visually illustrates Target3's day-by-day matches (TPs) and non-matches (FPs).

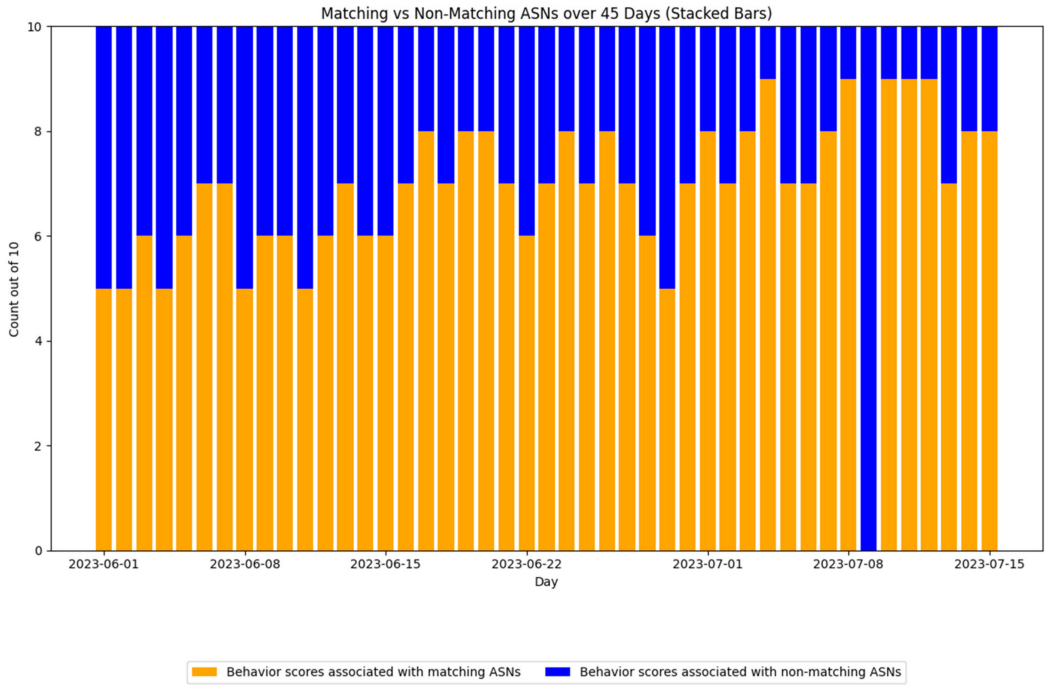

Figure 6. Target3 45-day Prophet cyberbehavioral score accuracy.

3.4.2. IPM Evaluation

A comparative analysis of Target3's CBS over a 45-day predictive period was performed to assess IPM performance. Table 8 provides a sample of this assessment, showcasing insights from two specific days. The complete 45-day data for all three Targets are available in Appendix A. This sample focuses on data observed for Target3 on 1 June 2023 and 15 June 2023, comparing predicted and actual ASN CBS. Notable variations in these scores were observed, suggesting possible discrepancies between expected and actual cyber activities.

Table 8. Comparative evaluation of behavior scores.

Day	Target3 Predicted ASN Prophet	Target3 Predicted Behavior Score	Target3 Actual ASN	Target3 Actual Behavior Score
1 June 2023	202,425	465	14,061	946
1 June 2023	396,982	276	202,425	465
1 June 2023	49,943	171	57,523	351
1 June 2023	50,867	105	50,360	276
1 June 2023	14,618	66	396,982	276
1 June 2023	16,509	55	398,324	190
1 June 2023	400,161	45	50,867	105
1 June 2023	40,244	28	204,428	91
1 June 2023	209,559	28	14,618	66
1 June 2023	19,750	3	16,509	55
15 June 2023	202,425	465	202,425	465
15 June 2023	49,943	171	50,360	276
15 June 2023	14,618	66	396,982	276
15 June 2023	396,982	276	57,523	351
15 June 2023	19,750	3	204,428	91
15 June 2023	16,509	55	14,061	946
15 June 2023	400,161	45	14,618	66
15 June 2023	57,523	351	16,509	55
15 June 2023	209,559	28	209,605	253
15 June 2023	14,061	946	398,324	190

The data from 15 June 2023, in Table 8, show the prediction accuracy of the top 10 most malicious ASNs. A 60% positive match (TP) rate (highlighted in orange) was achieved, with a 40% discrepancy (FP) rate (in blue). Actual CBS thresholds were applied to the missed ASNs, categorizing them into high-risk (in red) and medium-risk (in yellow) threats based on a preset threshold of 250. This analysis revealed the discrepancies between two high-risk and two medium-risk threats, indicating the model's accuracy in predicting potential threats.

3.5. Summary

This section presents key findings from the CFBA model, emphasizing its effectiveness in enhancing the precision and accuracy of predicting cyber threats from ASNs. Integrating CBDFA with tools like the Prophet model significantly refines these predictions. The results confirm the study's hypotheses and highlight the critical role of an interdisciplinary approach in improving cybersecurity's predictive abilities. They also stress the importance of a multidisciplinary approach, suggesting a trend towards more specific and personalized methods for predicting and mitigating cyber threats.

4. Discussion

This section evaluates how the CFBA model enhances cyber threat prediction accuracy. It demonstrates that merging digital forensics with cyberpsychology in a predictive framework improves threat understanding and prediction, particularly from ASNs. The

research shows that integrating technical and behavioral sciences in cybersecurity leads to more effective threat detection methods.

4.1. Overview

This study investigates cyberattack dynamics, blending technical methods and behavioral perspectives within an interdisciplinary framework. It employs predictive modeling, digital forensics, and data analysis to understand cyber threat actors' network behaviors and strategies. Key to this is integrating cyber behavioral sciences insights, which focus on human interactions in digital environments, as detailed previously in Table 3. These insights are essential for understanding cybercriminals' behaviors and motivations.

The research combines these insights with technical methods for improving threat prediction accuracy. By merging technical indicators with insights into the cyber behavioral sciences, the IPM achieves greater accuracy in predicting threats. The approach not only identifies network behaviors but also delves into the deeper behavioral profiles of threat actors, enhancing early detection and efficient resource allocation in cybersecurity.

The study's combination of predictive modeling, digital forensics, and cyber behavioral sciences offers a comprehensive view of cyber threats, emphasizing the value of an interdisciplinary methodology. It highlights the need for further investigations into specific vulnerabilities, particularly in "Target3", which experienced a higher frequency and variability of attacks. This methodological approach aims to enhance proactive threat detection and mitigation, providing a more accurate and in-depth cyberattack analysis.

4.2. Interpretation of Results

The study's in-depth examination of integrating CBDFA with predictive modeling in cyber threat analysis, mainly through the IPM, has yielded transformative insights. Evaluating predictive models for ASNs across three Targets reveals the strengths and limitations of current methods of network management. Shifting the focus from traditional binary classification metrics to TPs, FPs, and FNs, it addresses the categorical nature of ASN predictions. This method underscores the complexity of ASN prediction, which binary models cannot fully capture due to network routing and policies' dynamic and multifaceted aspects.

4.2.1. Research Question

Employing the Prophet model with CFBA enhanced the assessment and prediction accuracy of cyber threats from ASNs. This method is crucial in forensic cyberpsychology, part of cyber behavioral sciences, as it focuses on understanding the behavioral aspects of cybercriminal behavior for the effective prediction and mitigation of cyber threats. These insights are crucial to creating targeted cybersecurity interventions and preventive measures.

4.2.2. H1—Prediction

The IPM stands as a testament to the evolution of threat prediction strategies. By incorporating components like ABS-FaRM and CBS, IPM has created a comprehensive framework for accurate threat forecasting utilizing cyber behavioral sciences [2,3]. This approach, as supported by extensive research, utilizes machine learning algorithms and CBDFA to enhance the precision and accuracy of predictions from ASNs.

Using the Prophet model highlights the IPM's effectiveness in enhancing predictive models. The data in Tables 7 and 8 and Figure 5 demonstrate the model's accuracy in predicting cyber threats over 45 days [8]. Target3 showed higher accuracy than Target1 and Target2, supporting hypothesis H1 [38].

These results emphasize the Prophet model's role in advancing cyber threat prediction, with significant implications for reinforcing network security and understanding cyber behavioral patterns [3,14,15,17,42]. The results underscore the necessity of continued research to improve technological defenses and contribute to the theoretical growth of cyber behavioral sciences [14,15].

4.2.3. H2—Cyber Behavioral Scoring

As detailed in Table 6, the accuracy of the Prophet model, a core component of ABS-FaRM, across various targets is remarkably high. Notably, Target3 underlines the effectiveness of integrating ABS-FaRM's methods within the IPM framework. This integration bolsters the IPM's capability and marks a significant advancement in understanding and predicting cyber threats from ASNs, thus supporting H2 regarding the correlation between behavioral patterns and threat levels [2,26].

The integration of malicious CBS with predictive analytics, demonstrated by Target3's 70.44% match rate with actual behaviors, supports H2. This integration confirms the accuracy of the combined threat assessment approach, as shown in Tables 7 and 8 and Figure 5 [4,11,16,21,39]. The study follows the frameworks of Rich (2023) [26] and Martineau (2023) [2], incorporating insights from Attrill and Fullwood (2016) [52], and balances technological vulnerabilities with CFBA. The predictive versus actual behavior comparison for Target3 indicates opportunities for further model refinement.

4.2.4. H3—Synergistic Effect of the IPM

The synergistic effect of the IPM is evident in the research, particularly when examining the combination of CBDFA's insights into cybercriminal behavior and IPM's advanced technical predictive methods, which led to a notable improvement in forecasting accuracy for ASN-related cyber threats [2,26]. The study's findings, especially the enhanced predictive performance observed in Target3 when utilizing advanced tools like the Prophet model alongside CBDFA, showed a higher frequency and variability of attacks, serving as a critical test case to validate H3 [8,38].

In summary, the study confirms H3 by showing that the synergistic use of CBDFA within the IPM significantly boosts the model's ability to predict ASN-related cyber threats, highlighting the effectiveness of merging technical and behavioral approaches in cybersecurity [3,27]. The findings underscore the critical role of advanced tools like the Prophet model, used in ABS-FaRM, in refining the predictive capabilities of the IPM [26,36].

4.2.5. RQ—Integration of CBDFA in Predictive Modeling

The findings emphasize the importance of integrating CBDFA into predictive modeling in cybersecurity, mainly through developing the IPM and the ATPT. This integration, central to the study's RQ, significantly enhances the accuracy and precision of cyber threat predictions, particularly from ASNs [2,26].

Including CBDFA brings a vital understanding of cybercriminal behavior to the technical aspects of threat prediction [3]. The improved prediction accuracy across the studied targets, especially Target3, validates the study's hypothesis and underscores the effectiveness of this interdisciplinary approach [27,38].

The findings contribute theoretically and practically, offering a framework combining technical prediction with behavioral insights. This approach aids in developing more sophisticated and effective cyber threat management strategies, demonstrating the necessity of an integrated approach in cybersecurity. The study's outcomes thus mark a notable advancement in understanding and predicting cyber threats, highlighting the value of combining technical and behavioral perspectives [4,9].

4.3. Practical Implications and Recommendations

The study's findings offer substantial implications for cybersecurity professionals and researchers in cyber behavioral sciences. Integrating CBDFA with predictive modeling, as demonstrated by the IPM and the Prophet model, significantly enhances the capacity to forecast and mitigate cyber threats [2,26].

The findings underscore the necessity of adopting multi-class classification metrics, such as macro-averaged precision, recall, and F1 scores, in evaluating ASN predictive models [36,38]. This methodology provides a more subtle and comprehensive assessment of model performance, particularly in scenarios involving multiple classes and where the

balance of label distribution is a concern [8,37]. The results from Target3, which showed the highest precision and F1 scores, demonstrate the potential of advanced predictive models to accurately anticipate ASN allocations, offering significant benefits for network optimization and cybersecurity [21,27].

4.3.1. The Practical Implications of the CFBA Model in Cybersecurity Are Significant

1. Enhanced cybersecurity through predictive modeling: By integrating CBDFA with advanced predictive modeling, the CFBA model offers a more accurate prediction of cyber threats, aiding in preemptive security measures [3,5,9,16,21,27,35,38,49].
2. Contribution: The interdisciplinary approach of CFBA enriches traditional cybersecurity strategies, enabling a more comprehensive understanding of cyber threats' technical and behavioral aspects [1,6,8,10,16,18,50]. The model's focus on individual and collective cybercriminal behaviors allows for developing more personalized and effective cybersecurity solutions.
3. Forensic and legal advancements: The integration of cyberpsychology and digital forensics within CFBA enhances the capabilities of forensic investigators and law enforcement in understanding and prosecuting cybercrimes.
4. Educational and training benefits: The CFBA model's comprehensive approach can inform educational programs and training modules, equipping cybersecurity professionals with a deeper understanding of the intersection between human behavior and cyber threats.

4.3.2. Based on These Insights, the Following Key Recommendations Are Proposed

1. Implementation of holistic predictive tools: Investing in advanced predictive tools and technologies, such as machine learning algorithms, is crucial for preventing cyber threats [2,12,14,31,46].
2. Ongoing training in cyberattack psychology: Organizations should prioritize training programs focusing on the intersection of cyber behavior and technical vulnerabilities to enhance threat detection and response capabilities [10,17,20,24].
3. 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 [5,27,29,53].
4. 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 [1,26,27].

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 [3,9,11,14,29,46].

4.4. Limitations of the Research

This study, while establishing the effectiveness of the Prophet model and IPM in predicting cyber threats, acknowledges a number of limitations that need to be addressed in future studies:

1. Varying performance metrics across targets—The study reveals that performance metrics differ across various targets, indicating that there is not a universal model suitable for all ASN predictions. Future studies could work towards the development of a universal model. Future research endeavors could focus on developing adaptable models that account for the unique characteristics of various targets. Lundie et al.'s (2024) [22] research supports the idea that cyberattacks are complex and evolving, further emphasizing the need for flexible predictive models;

2. Dependency on specific factors—A multitude of contextual factors may influence the effectiveness of each predictive model. These factors encompass the nature of network traffic, the infrastructure of ISPs and targets, and the dynamics of global internet routing policies. Lundie et al.'s (2024) [22] insights emphasize the need for models to adapt to the specific context in which they are applied. Future studies can explore how predictive models can be tailored to these contextual factors to enhance their accuracy and reliability;
3. Psychological factors—While this study successfully develops the CBAM and the CBS, it is important to acknowledge the exclusion of psychological factors in their development. However, Lundie et al.'s (2024) [22] research highlights the significance of understanding cybercriminal behavior from a psychological perspective. Future studies can build upon this foundation by incorporating and empirically testing specific psychological variables, as Lundie et al. (2024) [22] demonstrated. This enhancement would contribute to a more holistic understanding of cyber threats;
4. Need for broader interdisciplinary integration—The study recognizes the potential value of integrating various disciplines, especially those within criminal justice and broader social sciences, into the CFBA model. While such integration is acknowledged as valuable, it falls outside the scope of this study. Nevertheless, the article by Lundie et al. (2024) [22] reinforces the importance of interdisciplinary approaches in understanding the dynamics of cybercriminal behavior. Future research can explore in-depth discussions and collaborations that involve a broader range of disciplines to enrich our comprehension of cyber threats.

5. Conclusions

This section provides a comprehensive overview of the empirical results of applying the CFBA model. It emphasizes the model's success in predicting cyber threats with greater accuracy and precision. This part of the study analyzes data gathered from various Targets and cyber incidents, highlighting the model's effectiveness in real-world scenarios. It discusses the validation of the research hypotheses and the relevance of the findings in enhancing cybersecurity measures. This section is pivotal in showcasing the practical implications of the integrated approach and its contribution to advancing the field of cyber threat prediction.

5.1. Summary of Main Findings

This interdisciplinary study successfully predicted cyber threats by combining technical accuracy with behavioral insights [11,46]. It verified the Prophet model's capability to predict threats from specific ASNs using varied data sets [6,11,41,46]. CBSs were crucial, linking technical forecasts with CFBA, aligned with a cyber behavioral science approach, thus improving the understanding of threats [2,7,14,16,25,26].

The study underscored the importance of precise predictive tools that integrate technical defenses with insights into human behaviors in cyber threats [9,54]. Acknowledging the human element's dual role as both a potential threat and a defense mechanism is vital in contemporary cybersecurity [9,29,42,50].

5.2. Contributions to the Field

The CFBA framework, an outcome of this study, is a multi-faceted system designed to predict and mitigate cybersecurity threats. The CFBA encapsulated a series of interlinked models and methodologies that collectively analyzed cybercriminal behavior, employed digital forensics, and utilized advanced data analytics.

The framework serves as a blueprint for constructing a robust predictive model that integrates behavioral insights with technical analysis to enhance threat identification, forecasting, and the development of targeted cybersecurity solutions.

This research integrated 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 [8,11,41,46].

The critical aspects of the study include the following:

- Addressing the pivotal role of CBS, which 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 attackers' motivations, informing the development of future predictive models [7,9,50];
- Establishing a crucial synergy of the CBDFA, utilizing ABS-FaRM, with predictive modeling. This integration underscores the importance of interdisciplinary methods in cybersecurity, combining technical precision with behavioral understanding [7,14,16].

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 [9,29,50].

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 [8,11,41,45];
- Integration of behavioral insights—CBS is instrumental in understanding attackers' motivations. This understanding aids in developing proactive defense strategies and targeted training programs [7,14,50];
- Interdisciplinary approach—The effectiveness of cybersecurity is heightened by merging it with CBDFA, offering a more comprehensive strategy for addressing cyber threats [14,16].

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.	[2,3,53]
Analyze Psychological Triggers	Examines psychological triggers and motivations behind cybercriminal behavior.	Provides insights into the "why" behind cyber threats.	[4,12,19]
Utilize Digital Footprints	Analyzes digital footprints left by cyber adversaries, understanding their tactics and techniques.	Enables deeper understanding of cyber adversaries' activities.	[8,49,54]
Detect Patterns	Uses temporal analysis to detect patterns in cyber activities, facilitating proactive threat prediction.	Enhances the ability to identify emerging threats.	[25,36,52,55,56]
Prioritize Threats	Develops risk assessments based on historical data and vulnerabilities, aiding in threat prioritization.	Assists in focusing resources on the most critical threats.	[15,32]
Overall Approach			
Interdisciplinary Lens	Synergizes technical and behavioral dimensions to enhance cyber threat prediction.	Fortifies cybersecurity strategies in an interconnected world.	[6,24,27,32,54]

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.

5.4. Future Research Directions

Based on the limitations identified, future research should explore the following aspects to enhance the understanding and prediction of cyber threats:

1. Development of adaptable models—Future research should aim to develop more adaptable models that cater to varying factors such as network traffic, ISP infrastructure, and internet routing policies;
2. Incorporation of psychological factors—There is a need to examine psychological factors in the behavior score metric to gain a more holistic view of cybercriminal behavior;
3. Interdisciplinary collaboration—Encouraging interdisciplinary collaboration among experts in cybersecurity, behavioral sciences, cyberpsychology, criminal justice, and broader social sciences is essential. Such collaboration would lead to comprehensive solutions combining technical robustness with behavioral insights;
4. Enhancing predictive accuracy—Exploring the incorporation of real-time data analytics and advanced machine learning algorithms may offer new pathways for enhancing the accuracy and reliability of ASN predictions.

These future research directions are crucial for developing more effective strategies for managing cyber threats and ensuring a more secure digital environment.

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

5.5. Final Thoughts

This study presents the CFBA model, offering an approach to the intersection of cyber behavioral sciences and digital forensics. The findings support that combining the behavioral sciences with digital forensic methodologies enhances the prediction and understanding of cyber threats, particularly from ASNs [11,14,30,42,46,50,55]. Using live data from ISP customers signifies a practical and significant advancement in understanding cyber threats.

This interdisciplinary approach marks a significant departure from traditional cybersecurity strategies, which often focus solely on technical aspects instead of focusing on proactive behavior-based predictive capabilities [12,44]. However, it is acknowledged that there are limitations in the current model, including some potential biases in data and methodologies. These limitations, however, offer opportunities for future research to refine and improve the CFBA model.

The research highlights the growing significance of 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 [26,27].

This study underscores the critical role of interdisciplinary collaboration in cybersecurity. Teamwork is vital for understanding, predicting, and mitigating cyber threats, contributing to a more secure and cohesive online environment and enhancing trust and confidence among digital users [7,53].

Applying the CFBA model in real-world scenarios significantly enhances cybersecurity strategies. Organizations can predict and prevent cyber threats more effectively by incorporating behavioral insights into technical approaches [52]. For instance:

- Organizations can use CFBA to identify threats from observed behavior patterns, proactively mitigating risks;

- Integrating this model in corporate settings may lead to more robust security protocols, tailoring defenses based on technical vulnerabilities and user behavioral patterns;
- In law enforcement, CFBA could aid in preemptively identifying cybercriminal activities, leading to quicker response times and more effective prevention strategies.

This approach represents a significant advancement in bridging the gap between human behavior and technological aspects of cybersecurity [52].

In conclusion, integrating CBDFA with predictive modeling in developing an adapted IPM and ATPT model is a significant step forward in joint endeavors to confront and mitigate cyber threats. This approach is seen as steering towards a more secure and resilient digital era [52]. Facing the challenges of the digital era requires an innovative combination of technical expertise and behavioral insights. This study contributes essential knowledge to cybersecurity and undoubtedly sets the groundwork for future exploration and innovation.

Author Contributions: M.S.R. contributed to all aspects of the article. M.P.A. contributed substantially to the 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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Access to the study data and associated codes 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 Derex O. Griffin and 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 authors declare no conflicts of interest.

Acronyms

ATPT	Advanced Tailored Predictive Tool
ASNs	Autonomous System Numbers
ABS-FaRM	ASN Behavior Score Forecasting and Ranking Model
CBA	Cyber Behavioral Analysis
CBAM	Cyber Behavioral Analysis Metric
CBDFA	Cyber Behavioral Digital Forensic Analysis
CBS	Cyber Behavioral Score
CFBA	Cyber Forensics Behavioral Analysis
DF	Digital Forensics
FCyberPsy	Forensic Cyberpsychology
IDS	Intrusion Detection System
IPM	Interdisciplinary Predictive Model
ISP	Internet Service Provider
ML	Machine Learning
PM	Predictive Modeling

Appendix A

Table A1. 45-Day Prediction Dataset.

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
1 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	40,244	28	202,425	465
1 June 2023	202,425	465	396,982	276	6142	0	396,982	276	202,425	465	396,982	276
1 June 2023	57,043	78	50,360	276	400,161	45	50,360	276	49,943	171	50,867	105
1 June 2023	396,982	276	57,523	351	396,982	276	57,043	78	14,618	66	50,360	276
1 June 2023	400,161	45	14,061	946	50,867	105	135,921	3	396,982	276	57,523	351
1 June 2023	50,867	105	398,324	190	34,088	6	14,061	946	19,750	3	14,618	66
1 June 2023	57,523	351	44,446	78	22,612	55	57,523	351	16,509	55	14,061	946
1 June 2023	14,061	946	20,115	136	14,061	946	204,428	91	400,161	45	204,428	91
1 June 2023	16,509	55	8075	190	50,360	276	398,324	190	50,867	105	16,509	55
1 June 2023	50,360	276	6939	300	204,428	91	207,812	55	209,559	28	398,324	190
2 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
2 June 2023	202,425	465	396,982	276	6142	0	396,982	276	49,943	171	396,982	276
2 June 2023	396,982	276	50,360	276	396,982	276	50,360	276	40,244	28	50,360	276
2 June 2023	400,161	45	57,523	351	50,867	105	57,043	78	14,618	66	57,523	351
2 June 2023	50,867	105	14,061	946	400,161	45	14,061	946	16,509	55	14,618	66
2 June 2023	209,559	28	398,324	190	22,612	55	57,523	351	396,982	276	14,061	946
2 June 2023	57,043	78	44,446	78	14,061	946	398,324	190	57,523	351	16,509	55
2 June 2023	57,523	351	7018	120	50,360	276	207,812	55	400,161	45	204,428	91
2 June 2023	14,061	946	6939	300	204,428	91	204,428	91	50,867	105	398,324	190
2 June 2023	50,360	276	8075	190	34,088	6	44,446	78	209,559	28	44,446	78
3 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
3 June 2023	202,425	465	396,982	276	6142	0	396,982	276	49,943	171	396,982	276
3 June 2023	34,088	6	57,523	351	50,867	105	50,360	276	40,244	28	50,360	276
3 June 2023	396,982	276	50,360	276	396,982	276	209,605	253	14,618	66	57,523	351
3 June 2023	57,043	78	209,605	253	400,161	45	14,061	946	396,982	276	14,618	66
3 June 2023	50,867	105	14,061	946	50,360	276	57,523	351	16,509	55	14,061	946
3 June 2023	209,559	28	398,324	190	14,061	946	204,428	91	50,867	105	16,509	55
3 June 2023	400,161	45	7018	120	22,612	55	207,812	55	400,161	45	204,428	91
3 June 2023	57,523	351	50,867	105	204,428	91	398,324	190	57,523	351	398,324	190
3 June 2023	50,360	276	398,722	171	398,324	190	398,705	91	50,360	276	714	3
4 June 2023	34,088	6	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
4 June 2023	202,425	465	50,867	105	6142	0	396,982	276	49,943	171	396,982	276
4 June 2023	396,982	276	396,982	276	34,088	6	50,360	276	40,244	28	50,360	276
4 June 2023	400,161	45	50,360	276	396,982	276	14,061	946	14,618	66	57,523	351
4 June 2023	57,043	78	57,523	351	50,867	105	209,605	253	396,982	276	14,618	66
4 June 2023	50,867	105	209,605	253	400,161	45	204,428	91	19,750	3	16,509	55
4 June 2023	14,061	946	14,061	946	14,061	946	57,523	351	400,161	45	14,061	946
4 June 2023	57,523	351	398,324	190	50,360	276	207,812	55	16,509	55	204,428	91
4 June 2023	50,360	276	204,428	91	22,612	55	398,324	190	50,867	105	398,324	190
4 June 2023	22,612	55	7018	120	204,428	91	44,446	78	57,523	351	714	3
5 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
5 June 2023	202,425	465	50,360	276	6142	0	50,360	276	49,943	171	50,360	276

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
5 June 2023	57,043	78	57,523	351	34,088	6	14,061	946	40,244	28	57,523	351
5 June 2023	396,982	276	14,061	946	50,867	105	204,428	91	14,618	66	14,618	66
5 June 2023	14,061	946	209,605	253	400,161	45	209,605	253	50,867	105	16,509	55
5 June 2023	50,867	105	396,982	276	396,982	276	396,982	276	16,509	55	204,428	91
5 June 2023	57,523	351	204,428	91	14,061	946	19,318	210	50,360	276	14,061	946
5 June 2023	50,360	276	398,324	190	50,360	276	57,523	351	57,523	351	396,982	276
5 June 2023	400,161	45	7018	120	22,612	55	207,812	55	400,161	45	398,324	190
5 June 2023	16,509	55	6939	300	204,428	91	398,324	190	14,061	946	206,728	78
6 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	40,244	28
6 June 2023	20,115	136	50,360	276	6142	0	50,360	276	49,943	171	202,425	465
6 June 2023	50,867	105	400,161	45	396,982	276	14,061	946	40,244	28	14,618	66
6 June 2023	396,982	276	209,605	253	50,867	105	204,428	91	14,618	66	50,360	276
6 June 2023	57,043	78	57,523	351	400,161	45	209,605	253	400,161	45	16,509	55
6 June 2023	14,061	946	14,061	946	14,061	946	19,318	210	16,509	55	57,523	351
6 June 2023	16,509	55	396,982	276	50,360	276	396,982	276	57,523	351	204,428	91
6 June 2023	57,523	351	204,428	91	22,612	55	398,324	190	50,867	105	14,061	946
6 June 2023	50,360	276	398,324	190	34,088	6	207,812	55	50,360	276	396,982	276
6 June 2023	400,161	45	7018	120	204,428	91	57,523	351	14,061	946	398,324	190
7 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
7 June 2023	202,425	465	50,360	276	6142	0	14,061	946	40,244	28	50,360	276
7 June 2023	396,982	276	396,982	276	50,867	105	396,982	276	14,618	66	400,161	45
7 June 2023	50,867	105	57,523	351	400,161	45	209,605	253	49,943	171	57,523	351
7 June 2023	400,161	45	14,061	946	396,982	276	50,360	276	50,867	105	396,982	276
7 June 2023	16,509	55	209,605	253	50,360	276	204,428	91	400,161	45	14,618	66
7 June 2023	57,043	78	204,428	91	14,061	946	19,318	210	16,509	55	16,509	55
7 June 2023	57,523	351	400,161	45	34,088	6	57,523	351	396,982	276	14,061	946
7 June 2023	14,061	946	398,324	190	22,612	55	398,324	190	57,523	351	204,428	91
7 June 2023	50,360	276	212,283	66	204,428	91	207,812	55	50,360	276	398,324	190
8 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	40,244	28	202,425	465
8 June 2023	202,425	465	50,360	276	6142	0	396,982	276	202,425	465	396,982	276
8 June 2023	57,043	78	396,982	276	400,161	45	14,061	946	49,943	171	50,360	276
8 June 2023	396,982	276	57,523	351	396,982	276	209,605	253	14,618	66	14,618	66
8 June 2023	400,161	45	14,061	946	50,867	105	57,523	351	396,982	276	57,523	351
8 June 2023	50,867	105	209,605	253	34,088	6	50,360	276	19,750	3	14,061	946
8 June 2023	57,523	351	212,283	66	22,612	55	204,428	91	16,509	55	16,509	55
8 June 2023	14,061	946	398,324	190	14,061	946	398,324	190	400,161	45	204,428	91
8 June 2023	16,509	55	44,446	78	50,360	276	19,318	210	50,867	105	398,324	190
8 June 2023	50,360	276	7018	120	204,428	91	207,812	55	57,523	351	15,169	105
9 June 2023	20,115	136	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
9 June 2023	202,425	465	396,982	276	6142	0	396,982	276	49,943	171	396,982	276
9 June 2023	396,982	276	50,360	276	396,982	276	400,161	45	40,244	28	50,360	276
9 June 2023	400,161	45	14,061	946	50,867	105	14,061	946	14,618	66	14,618	66
9 June 2023	50,867	105	44,446	78	400,161	45	209,605	253	16,509	55	57,523	351
9 June 2023	209,559	28	209,605	253	22,612	55	50,360	276	396,982	276	16,509	55
9 June 2023	57,043	78	57,523	351	14,061	946	57,523	351	57,523	351	14,061	946
9 June 2023	57,523	351	212,283	66	50,360	276	207,812	55	400,161	45	204,428	91

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
9 June 2023	14,061	946	398,324	190	34,088	6	204,428	91	50,867	105	398,324	190
9 June 2023	50,360	276	7018	120	204,428	91	398,324	190	50,360	276	44,446	78
10 June 2023	202,425	465	202,425	465	202,425	465	6142	0	202,425	465	202,425	465
10 June 2023	396,982	276	396,982	276	6142	0	202,425	465	49,943	171	396,982	276
10 June 2023	57,043	78	16,276	325	50,867	105	396,982	276	40,244	28	57,523	351
10 June 2023	50,867	105	57,523	351	396,982	276	14,061	946	14,618	66	14,618	66
10 June 2023	209,559	28	50,360	276	400,161	45	50,360	276	396,982	276	14,061	946
10 June 2023	400,161	45	44,446	78	50,360	276	57,523	351	16,509	55	204,428	91
10 June 2023	57,523	351	14,061	946	14,061	946	209,605	253	50,867	105	50,360	276
10 June 2023	50,360	276	209,605	253	22,612	55	398,324	190	400,161	45	16,509	55
10 June 2023	14,061	946	212,283	66	204,428	91	204,428	91	50,360	276	398,324	190
10 June 2023	16,509	55	398,324	190	398,324	190	207,812	55	57,523	351	44,446	78
11 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
11 June 2023	396,982	276	50,360	276	6142	0	50,360	276	49,943	171	50,360	276
11 June 2023	57,043	78	396,982	276	34,088	6	396,982	276	40,244	28	396,982	276
11 June 2023	400,161	45	57,523	351	396,982	276	14,061	946	14,618	66	57,523	351
11 June 2023	50,867	105	16,276	325	50,867	105	209,605	253	396,982	276	14,618	66
11 June 2023	14,061	946	209,605	253	400,161	45	57,523	351	19,750	3	14,061	946
11 June 2023	57,523	351	14,061	946	14,061	946	204,428	91	400,161	45	204,428	91
11 June 2023	50,360	276	44,446	78	50,360	276	207,812	55	16,509	55	16,509	55
11 June 2023	8075	190	212,283	66	22,612	55	398,324	190	50,867	105	398,324	190
11 June 2023	16,509	55	398,324	190	204,428	91	44,446	78	50,360	276	44,446	78
12 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
12 June 2023	57,043	78	50,360	276	6142	0	50,360	276	49,943	171	50,360	276
12 June 2023	396,982	276	57,523	351	34,088	6	14,061	946	40,244	28	57,523	351
12 June 2023	14,061	946	14,061	946	50,867	105	209,605	253	14,618	66	14,618	66
12 June 2023	50,867	105	209,605	253	396,982	276	396,982	276	50,867	105	14,061	946
12 June 2023	57,523	351	44,446	78	400,161	45	57,523	351	16,509	55	396,982	276
12 June 2023	50,360	276	396,982	276	14,061	946	204,428	91	50,360	276	204,428	91
12 June 2023	400,161	45	398,324	190	50,360	276	207,812	55	57,523	351	16,509	55
12 June 2023	16,509	55	212,283	66	22,612	55	398,324	190	400,161	45	398,324	190
12 June 2023	398,324	190	49,453	78	204,428	91	44,446	78	14,061	946	15,169	105
13 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
13 June 2023	50,867	105	50,360	276	6142	0	50,360	276	49,943	171	16,509	55
13 June 2023	396,982	276	57,523	351	396,982	276	14,061	946	14,618	66	50,360	276
13 June 2023	57,043	78	14,061	946	50,867	105	209,605	253	400,161	45	57,523	351
13 June 2023	14,061	946	209,605	253	400,161	45	57,523	351	16,509	55	14,618	66
13 June 2023	16,509	55	44,446	78	14,061	946	207,812	55	57,523	351	14,061	946
13 June 2023	57,523	351	396,982	276	50,360	276	396,982	276	50,360	276	204,428	91
13 June 2023	50,360	276	212,283	66	22,612	55	398,324	190	50,867	105	396,982	276
13 June 2023	400,161	45	398,324	190	34,088	6	204,428	91	14,061	946	398,324	190
13 June 2023	44,446	78	7018	120	204,428	91	206,728	78	396,982	276	15,169	105
14 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
14 June 2023	396,982	276	50,360	276	6142	0	50,360	276	14,618	66	50,360	276
14 June 2023	50,867	105	48,090	91	50,867	105	48,090	91	49,943	171	204,428	91
14 June 2023	400,161	45	57,523	351	400,161	45	14,061	946	400,161	45	57,523	351

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
14 June 2023	16,509	55	14,061	946	396,982	276	57,523	351	16,509	55	14,618	66
14 June 2023	57,043	78	44,446	78	50,360	276	204,428	91	396,982	276	14,061	946
14 June 2023	57,523	351	396,982	276	14,061	946	396,982	276	57,523	351	16,509	55
14 June 2023	14,061	946	209,605	253	34,088	6	207,812	55	50,360	276	209,605	253
14 June 2023	50,360	276	212,283	66	22,612	55	398,324	190	19,750	3	396,982	276
14 June 2023	44,446	78	398,324	190	204,428	91	44,446	78	209,559	28	398,324	190
15 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
15 June 2023	57,043	78	50,360	276	6142	0	50,360	276	49,943	171	50,360	276
15 June 2023	396,982	276	396,982	276	400,161	45	396,982	276	14,618	66	396,982	276
15 June 2023	400,161	45	57,523	351	396,982	276	14,061	946	396,982	276	57,523	351
15 June 2023	50,867	105	14,061	946	50,867	105	22,612	55	19,750	3	204,428	91
15 June 2023	57,523	351	44,446	78	34,088	6	57,523	351	16,509	55	14,061	946
15 June 2023	14,061	946	209,605	253	22,612	55	207,812	55	400,161	45	14,618	66
15 June 2023	16,509	55	212,283	66	14,061	946	204,428	91	57,523	351	16,509	55
15 June 2023	50,360	276	398,324	190	50,360	276	398,324	190	209,559	28	209,605	253
15 June 2023	209,559	28	7018	120	204,428	91	206,728	78	14,061	946	398,324	190
16 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
16 June 2023	396,982	276	50,360	276	6142	0	50,360	276	49,943	171	396,982	276
16 June 2023	400,161	45	396,982	276	396,982	276	396,982	276	14,618	66	50,360	276
16 June 2023	50,867	105	14,061	946	50,867	105	22,612	55	16,509	55	14,618	66
16 June 2023	209,559	28	57,523	351	400,161	45	14,061	946	396,982	276	57,523	351
16 June 2023	57,043	78	44,446	78	22,612	55	57,523	351	57,523	351	14,061	946
16 June 2023	57,523	351	209,605	253	14,061	946	207,812	55	400,161	45	209,605	253
16 June 2023	14,061	946	398,324	190	50,360	276	398,324	190	50,360	276	204,428	91
16 June 2023	50,360	276	212,283	66	34,088	6	204,428	91	209,559	28	16,509	55
16 June 2023	16,509	55	49,453	78	204,428	91	206,728	78	14,061	946	398,324	190
17 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
17 June 2023	396,982	276	396,982	276	6142	0	396,982	276	49,943	171	396,982	276
17 June 2023	57,043	78	50,360	276	50,867	105	50,360	276	14,618	66	14,618	66
17 June 2023	50,867	105	14,061	946	396,982	276	47,890	325	396,982	276	50,360	276
17 June 2023	209,559	28	44,446	78	400,161	45	57,523	351	16,509	55	57,523	351
17 June 2023	400,161	45	57,523	351	50,360	276	22,612	55	400,161	45	14,061	946
17 June 2023	57,523	351	209,605	253	14,061	946	14,061	946	50,360	276	209,605	253
17 June 2023	50,360	276	212,283	66	22,612	55	398,324	190	57,523	351	204,428	91
17 June 2023	14,061	946	398,324	190	204,428	91	207,812	55	14,061	946	398,324	190
17 June 2023	16,509	55	7018	120	34,088	6	204,428	91	204,428	91	16,509	55
18 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
18 June 2023	396,982	276	396,982	276	6142	0	396,982	276	49,943	171	396,982	276
18 June 2023	57,043	78	50,360	276	34,088	6	50,360	276	14,618	66	57,523	351
18 June 2023	400,161	45	14,061	946	396,982	276	57,523	351	396,982	276	14,618	66
18 June 2023	50,867	105	57,523	351	50,867	105	14,061	946	19,750	3	14,061	946
18 June 2023	14,061	946	44,446	78	400,161	45	22,612	55	400,161	45	50,360	276
18 June 2023	57,523	351	209,605	253	14,061	946	47,890	325	16,509	55	16,509	55
18 June 2023	50,360	276	398,324	190	50,360	276	207,812	55	50,360	276	209,605	253

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
18 June 2023	8075	190	212,283	66	22,612	55	204,428	91	57,523	351	204,428	91
18 June 2023	16,509	55	57,678	55	204,428	91	398,324	190	14,061	946	398,324	190
19 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
19 June 2023	57,043	78	57,523	351	6142	0	57,523	351	49,943	171	57,523	351
19 June 2023	396,982	276	50,360	276	34,088	6	47,890	325	14,618	66	14,618	66
19 June 2023	14,061	946	396,982	276	396,982	276	50,360	276	16,509	55	396,982	276
19 June 2023	50,867	105	14,061	946	50,867	105	396,982	276	50,360	276	14,061	946
19 June 2023	57,523	351	44,446	78	400,161	45	14,061	946	57,523	351	50,360	276
19 June 2023	50,360	276	209,605	253	14,061	946	207,812	55	400,161	45	204,428	91
19 June 2023	400,161	45	212,283	66	50,360	276	204,428	91	14,061	946	16,509	55
19 June 2023	16,509	55	398,324	190	22,612	55	398,324	190	396,982	276	209,605	253
19 June 2023	398,324	190	49,453	78	204,428	91	44,446	78	204,428	91	398,324	190
20 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
20 June 2023	396,982	276	396,982	276	6142	0	50,360	276	49,943	171	14,618	66
20 June 2023	50,867	105	57,523	351	396,982	276	14,061	946	14,618	66	57,523	351
20 June 2023	57,043	78	50,360	276	50,867	105	396,982	276	400,161	45	14,061	946
20 June 2023	14,061	946	14,061	946	400,161	45	57,523	351	16,509	55	396,982	276
20 June 2023	16,509	55	44,446	78	14,061	946	207,812	55	57,523	351	50,360	276
20 June 2023	57,523	351	209,605	253	50,360	276	204,428	91	50,360	276	204,428	91
20 June 2023	50,360	276	212,283	66	22,612	55	47,890	325	14,061	946	16,509	55
20 June 2023	400,161	45	398,324	190	34,088	6	398,324	190	396,982	276	209,605	253
20 June 2023	209,559	28	7018	120	204,428	91	206,728	78	204,428	91	398,324	190
21 June 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
21 June 2023	396,982	276	202,425	465	6142	0	57,678	55	14,618	66	50,360	276
21 June 2023	50,867	105	396,982	276	50,867	105	47,890	325	49,943	171	50,867	105
21 June 2023	400,161	45	57,523	351	396,982	276	50,360	276	16,509	55	57,523	351
21 June 2023	16,509	55	14,061	946	400,161	45	396,982	276	400,161	45	14,618	66
21 June 2023	57,043	78	44,446	78	50,360	276	14,061	946	396,982	276	396,982	276
21 June 2023	57,523	351	209,605	253	34,088	6	57,523	351	57,523	351	14,061	946
21 June 2023	14,061	946	212,283	66	14,061	946	204,428	91	50,360	276	204,428	91
21 June 2023	50,360	276	8075	190	22,612	55	398,324	190	19,750	3	16,509	55
21 June 2023	44,446	78	398,324	190	204,428	91	207,812	55	14,061	946	209,605	253
22 June 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
22 June 2023	57,043	78	202,425	465	6142	0	57,678	55	49,943	171	50,360	276
22 June 2023	396,982	276	396,982	276	400,161	45	396,982	276	14,618	66	396,982	276
22 June 2023	400,161	45	57,523	351	396,982	276	50,360	276	396,982	276	57,523	351
22 June 2023	50,867	105	14,061	946	50,867	105	14,061	946	19,750	3	14,618	66
22 June 2023	57,523	351	44,446	78	34,088	6	47,890	325	16,509	55	16,509	55
22 June 2023	14,061	946	212,283	66	22,612	55	57,523	351	400,161	45	14,061	946
22 June 2023	16,509	55	49,453	78	14,061	946	22,612	55	57,523	351	204,428	91
22 June 2023	50,360	276	398,324	190	50,360	276	398,324	190	209,559	28	398,324	190
22 June 2023	209,559	28	7018	120	204,428	91	207,812	55	14,061	946	209,605	253
23 June 2023	202,425	465	50,360	276	202,425	465	57,678	55	202,425	465	202,425	465
23 June 2023	396,982	276	396,982	276	6142	0	202,425	465	49,943	171	50,360	276
23 June 2023	400,161	45	202,425	465	396,982	276	396,982	276	14,618	66	396,982	276

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
23 June 2023	50,867	105	57,523	351	50,867	105	50,360	276	16,509	55	57,523	351
23 June 2023	209,559	28	14,061	946	400,161	45	22,612	55	396,982	276	14,061	946
23 June 2023	57,043	78	44,446	78	22,612	55	14,061	946	57,523	351	14,618	66
23 June 2023	57,523	351	212,283	66	14,061	946	204,428	91	400,161	45	204,428	91
23 June 2023	14,061	946	398,324	190	50,360	276	57,523	351	50,360	276	16,509	55
23 June 2023	50,360	276	49,453	78	34,088	6	207,812	55	209,559	28	398,324	190
23 June 2023	16,509	55	7018	120	204,428	91	398,324	190	14,061	946	22,822	0
24 June 2023	202,425	465	202,425	465	202,425	465	27,385	1	202,425	465	202,425	465
24 June 2023	396,982	276	50,360	276	6142	0	202,425	465	49,943	171	50,360	276
24 June 2023	57,043	78	396,982	276	50,867	105	396,982	276	14,618	66	396,982	276
24 June 2023	50,867	105	57,523	351	396,982	276	400,161	45	396,982	276	57,523	351
24 June 2023	209,559	28	14,061	946	400,161	45	50,360	276	16,509	55	14,061	946
24 June 2023	400,161	45	44,446	78	50,360	276	14,061	946	50,360	276	204,428	91
24 June 2023	57,523	351	209,605	253	14,061	946	47,890	325	400,161	45	14,618	66
24 June 2023	50,360	276	212,283	66	22,612	55	22,612	55	57,523	351	209,605	253
24 June 2023	14,061	946	398,324	190	34,088	6	57,523	351	14,061	946	398,324	190
24 June 2023	16,509	55	7018	120	204,428	91	204,428	91	204,428	91	16,509	55
25 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
25 June 2023	396,982	276	57,043	78	6142	0	396,982	276	49,943	171	396,982	276
25 June 2023	57,043	78	396,982	276	34,088	6	50,360	276	14,618	66	57,523	351
25 June 2023	400,161	45	50,360	276	396,982	276	22,612	55	396,982	276	50,360	276
25 June 2023	50,867	105	57,523	351	50,867	105	47,890	325	19,750	3	14,061	946
25 June 2023	14,061	946	14,061	946	400,161	45	14,061	946	16,509	55	14,618	66
25 June 2023	57,523	351	44,446	78	14,061	946	57,523	351	400,161	45	204,428	91
25 June 2023	50,360	276	212,283	66	50,360	276	207,812	55	50,360	276	16,509	55
25 June 2023	8075	190	209,605	253	22,612	55	204,428	91	57,523	351	209,605	253
25 June 2023	16,509	55	398,324	190	204,428	91	398,324	190	14,061	946	398,324	190
26 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
26 June 2023	57,043	78	50,360	276	6142	0	50,360	276	49,943	171	57,523	351
26 June 2023	396,982	276	396,982	276	34,088	6	22,612	55	14,618	66	50,360	276
26 June 2023	14,061	946	57,523	351	396,982	276	396,982	276	16,509	55	396,982	276
26 June 2023	50,867	105	14,061	946	50,867	105	14,061	946	50,360	276	14,061	946
26 June 2023	57,523	351	44,446	78	400,161	45	204,428	91	57,523	351	16,509	55
26 June 2023	50,360	276	209,605	253	14,061	946	207,812	55	400,161	45	14,618	66
26 June 2023	400,161	45	212,283	66	50,360	276	57,523	351	14,061	946	204,428	91
26 June 2023	16,509	55	398,324	190	22,612	55	398,324	190	396,982	276	209,605	253
26 June 2023	398,324	190	7018	120	204,428	91	17,858	190	204,428	91	398,324	190
27 June 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
27 June 2023	396,982	276	202,425	465	6142	0	50,360	276	49,943	171	50,360	276
27 June 2023	50,867	105	396,982	276	396,982	276	47,890	325	14,618	66	57,523	351
27 June 2023	57,043	78	57,523	351	50,867	105	22,612	55	16,509	55	14,061	946
27 June 2023	14,061	946	14,061	946	400,161	45	14,061	946	400,161	45	14,618	66
27 June 2023	16,509	55	44,446	78	14,061	946	396,982	276	50,360	276	204,428	91
27 June 2023	57,523	351	209,605	253	50,360	276	57,523	351	57,523	351	396,982	276
27 June 2023	50,360	276	398,324	190	22,612	55	204,428	91	14,061	946	209,605	253

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
27 June 2023	400,161	45	212,283	66	34,088	6	207,812	55	396,982	276	398,324	190
27 June 2023	209,559	28	7018	120	204,428	91	17,858	190	204,428	91	206,728	78
28 June 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
28 June 2023	396,982	276	202,425	465	6142	0	400,161	45	14,618	66	50,360	276
28 June 2023	50,867	105	396,982	276	50,867	105	396,982	276	49,943	171	396,982	276
28 June 2023	400,161	45	14,061	946	396,982	276	50,360	276	16,509	55	57,523	351
28 June 2023	16,509	55	57,523	351	400,161	45	22,612	55	400,161	45	14,061	946
28 June 2023	57,043	78	44,446	78	50,360	276	14,061	946	396,982	276	14,618	66
28 June 2023	57,523	351	209,605	253	14,061	946	57,523	351	50,360	276	204,428	91
28 June 2023	14,061	946	212,283	66	22,612	55	204,428	91	57,523	351	209,605	253
28 June 2023	50,360	276	398,324	190	204,428	91	47,890	325	19,750	3	398,324	190
28 June 2023	44,446	78	7018	120	398,324	190	207,812	55	14,061	946	50,867	105
29 June 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
29 June 2023	57,043	78	202,425	465	6142	0	396,982	276	49,943	171	50,360	276
29 June 2023	396,982	276	396,982	276	400,161	45	50,360	276	14,618	66	396,982	276
29 June 2023	400,161	45	57,523	351	396,982	276	22,612	55	396,982	276	50,867	105
29 June 2023	57,523	351	14,061	946	50,867	105	14,061	946	19,750	3	57,523	351
29 June 2023	16,509	55	44,446	78	22,612	55	204,428	91	16,509	55	14,061	946
29 June 2023	14,061	946	212,283	66	14,061	946	207,812	55	400,161	45	14,618	66
29 June 2023	50,360	276	398,324	190	50,360	276	57,523	351	57,523	351	204,428	91
29 June 2023	209,559	28	47,890	325	204,428	91	398,324	190	209,559	28	47,890	325
29 June 2023	44,446	78	7018	120	398,324	190	44,446	78	50,360	276	398,324	190
30 June 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
30 June 2023	396,982	276	50,360	276	6142	0	396,982	276	49,943	171	50,360	276
30 June 2023	400,161	45	396,982	276	396,982	276	50,360	276	14,618	66	396,982	276
30 June 2023	209,559	28	57,523	351	50,867	105	22,612	55	16,509	55	57,523	351
30 June 2023	57,043	78	14,061	946	400,161	45	14,061	946	396,982	276	14,618	66
30 June 2023	57,523	351	44,446	78	22,612	55	204,428	91	57,523	351	14,061	946
30 June 2023	14,061	946	212,283	66	14,061	946	398,324	190	400,161	45	204,428	91
30 June 2023	50,360	276	398,324	190	50,360	276	57,523	351	50,360	276	398,324	190
30 June 2023	16,509	55	7018	120	204,428	91	44,446	78	209,559	28	16,509	55
30 June 2023	44,446	78	6939	300	398,324	190	6939	300	14,061	946	44,446	78
1 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
1 July 2023	396,982	276	50,360	276	6142	0	396,982	276	49,943	171	50,360	276
1 July 2023	57,043	78	396,982	276	396,982	276	22,612	55	14,618	66	396,982	276
1 July 2023	209,559	28	57,523	351	50,867	105	14,061	946	396,982	276	57,523	351
1 July 2023	400,161	45	44,446	78	400,161	45	50,360	276	16,509	55	14,618	66
1 July 2023	57,523	351	14,061	946	50,360	276	57,523	351	50,360	276	14,061	946
1 July 2023	50,360	276	398,324	190	14,061	946	204,428	91	400,161	45	204,428	91
1 July 2023	14,061	946	212,283	66	22,612	55	398,324	190	57,523	351	16,509	55
1 July 2023	16,509	55	7018	120	204,428	91	206,728	78	14,061	946	398,324	190
1 July 2023	44,446	78	6939	300	398,324	190	44,446	78	204,428	91	206,728	78
2 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
2 July 2023	396,982	276	50,360	276	6142	0	22,612	55	49,943	171	50,360	276
2 July 2023	57,043	78	57,043	78	396,982	276	396,982	276	14,618	66	57,523	351

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
2 July 2023	14,061	946	396,982	276	50,867	105	14,061	946	396,982	276	396,982	276
2 July 2023	57,523	351	57,523	351	400,161	45	207,812	55	19,750	3	14,618	66
2 July 2023	50,360	276	14,061	946	14,061	946	204,428	91	16,509	55	14,061	946
2 July 2023	16,509	55	44,446	78	50,360	276	57,523	351	400,161	45	204,428	91
2 July 2023	8075	190	212,283	66	22,612	55	50,360	276	50,360	276	16,509	55
2 July 2023	209,559	28	398,324	190	204,428	91	398,324	190	57,523	351	398,324	190
2 July 2023	44,446	78	22,612	55	398,324	190	206,728	78	14,061	946	22,612	55
3 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
3 July 2023	57,043	78	50,360	276	6142	0	22,612	55	14,618	66	50,360	276
3 July 2023	396,982	276	14,061	946	396,982	276	14,061	946	16,509	55	57,523	351
3 July 2023	14,061	946	44,446	78	50,867	105	204,428	91	50,360	276	14,618	66
3 July 2023	57,523	351	57,523	351	400,161	45	396,982	276	57,523	351	14,061	946
3 July 2023	50,360	276	396,982	276	14,061	946	57,523	351	400,161	45	204,428	91
3 July 2023	16,509	55	212,283	66	50,360	276	50,360	276	14,061	946	16,509	55
3 July 2023	398,324	190	398,324	190	22,612	55	398,324	190	396,982	276	396,982	276
3 July 2023	209,559	28	22,612	55	204,428	91	207,812	55	204,428	91	398,324	190
3 July 2023	8075	190	6939	300	398,324	190	44,446	78	19,750	3	22,612	55
4 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
4 July 2023	396,982	276	14,061	946	6142	0	22,612	55	14,618	66	14,618	66
4 July 2023	57,043	78	57,523	351	396,982	276	14,061	946	16,509	55	57,523	351
4 July 2023	14,061	946	44,446	78	50,867	105	204,428	91	400,161	45	14,061	946
4 July 2023	16,509	55	396,982	276	400,161	45	396,982	276	50,360	276	204,428	91
4 July 2023	57,523	351	212,283	66	50,360	276	50,360	276	57,523	351	50,360	276
4 July 2023	50,360	276	50,360	276	14,061	946	57,523	351	14,061	946	396,982	276
4 July 2023	209,559	28	398,324	190	22,612	55	398,324	190	396,982	276	16,509	55
4 July 2023	398,324	190	50,321	3	204,428	91	44,446	78	204,428	91	398,324	190
4 July 2023	44,446	78	132,203	190	398,324	190	6939	300	398,324	190	44,446	78
5 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
5 July 2023	396,982	276	50,867	105	6142	0	396,982	276	14,618	66	57,523	351
5 July 2023	16,509	55	57,523	351	50,867	105	22,612	55	16,509	55	14,618	66
5 July 2023	57,043	78	396,982	276	396,982	276	14,061	946	400,161	45	396,982	276
5 July 2023	57,523	351	14,061	946	400,161	45	57,523	351	396,982	276	14,061	946
5 July 2023	14,061	946	44,446	78	50,360	276	50,360	276	50,360	276	204,428	91
5 July 2023	50,360	276	50,360	276	14,061	946	204,428	91	57,523	351	50,360	276
5 July 2023	209,559	28	212,283	66	22,612	55	398,324	190	19,750	3	16,509	55
5 July 2023	44,446	78	398,324	190	204,428	91	206,728	78	14,061	946	398,324	190
5 July 2023	398,324	190	34,665	91	398,324	190	132,203	190	209,559	28	206,728	78
6 July 2023	202,425	465	396,982	276	202,425	465	202,425	465	202,425	465	202,425	465
6 July 2023	57,043	78	202,425	465	6142	0	400,161	45	14,618	66	396,982	276
6 July 2023	396,982	276	57,523	351	396,982	276	396,982	276	396,982	276	57,523	351
6 July 2023	57,523	351	50,867	105	50,867	105	22,612	55	19,750	3	14,618	66
6 July 2023	16,509	55	14,061	946	22,612	55	14,061	946	16,509	55	14,061	946
6 July 2023	14,061	946	44,446	78	50,360	276	50,360	276	400,161	45	16,509	55
6 July 2023	50,360	276	50,360	276	14,061	946	57,523	351	57,523	351	204,428	91
6 July 2023	209,559	28	398,324	190	204,428	91	204,428	91	209,559	28	50,360	276

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
6 July 2023	398,324	190	212,283	66	398,324	190	398,324	190	50,360	276	398,324	190
6 July 2023	44,446	78	34,665	91	207,812	55	206,728	78	14,061	946	701	78
7 July 2023	202,425	465	396,982	276	202,425	465	202,425	465	202,425	465	202,425	465
7 July 2023	396,982	276	202,425	465	6142	0	396,982	276	14,618	66	396,982	276
7 July 2023	209,559	28	50,360	276	396,982	276	50,360	276	16,509	55	50,360	276
7 July 2023	57,043	78	14,061	946	50,867	105	6142	0	396,982	276	14,618	66
7 July 2023	57,523	351	44,446	78	22,612	55	22,612	55	57,523	351	14,061	946
7 July 2023	14,061	946	212,283	66	50,360	276	14,061	946	400,161	45	57,523	351
7 July 2023	50,360	276	57,523	351	14,061	946	57,523	351	50,360	276	16,509	55
7 July 2023	16,509	55	398,324	190	204,428	91	398,324	190	14,061	946	398,324	190
7 July 2023	398,324	190	34,665	91	398,324	190	204,428	91	209,559	28	204,428	91
7 July 2023	44,446	78	6939	300	207,812	55	44,446	78	204,428	91	206,728	78
8 July 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
8 July 2023	396,982	276	202,425	465	6142	0	50,360	276	14,618	66	50,360	276
8 July 2023	57,043	78	396,982	276	396,982	276	6142	0	396,982	276	396,982	276
8 July 2023	209,559	28	44,446	78	50,867	105	396,982	276	16,509	55	57,523	351
8 July 2023	57,523	351	14,061	946	50,360	276	14,061	946	50,360	276	14,618	66
8 July 2023	50,360	276	57,523	351	14,061	946	57,523	351	400,161	45	14,061	946
8 July 2023	14,061	946	212,283	66	22,612	55	398,324	190	57,523	351	16,509	55
8 July 2023	16,509	55	398,324	190	204,428	91	22,612	55	14,061	946	398,324	190
8 July 2023	44,446	78	4134	630	398,324	190	204,428	91	204,428	91	204,428	91
8 July 2023	398,324	190	398,722	171	207,812	55	44,446	78	398,324	190	44,446	78
9 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
9 July 2023	396,982	276	50,360	276	6142	0	50,360	276	14,618	66	50,360	276
9 July 2023	57,043	78	396,982	276	396,982	276	396,982	276	396,982	276	400,161	45
9 July 2023	14,061	946	57,523	351	50,867	105	14,061	946	16,509	55	396,982	276
9 July 2023	57,523	351	14,061	946	14,061	946	57,523	351	400,161	45	57,523	351
9 July 2023	50,360	276	44,446	78	50,360	276	398,324	190	50,360	276	14,618	66
9 July 2023	16,509	55	398,324	190	22,612	55	204,428	91	57,523	351	14,061	946
9 July 2023	8075	190	212,283	66	204,428	91	44,446	78	14,061	946	16,509	55
9 July 2023	209,559	28	398,722	171	398,324	190	206,728	78	204,428	91	398,324	190
9 July 2023	398,324	190	47,890	325	207,812	55	400,161	45	398,324	190	204,428	91
10 July 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
10 July 2023	57,043	78	202,425	465	6142	0	50,360	276	14,618	66	50,360	276
10 July 2023	396,982	276	57,523	351	396,982	276	400,161	45	16,509	55	14,618	66
10 July 2023	14,061	946	396,982	276	50,867	105	14,061	946	50,360	276	57,523	351
10 July 2023	57,523	351	14,061	946	14,061	946	396,982	276	57,523	351	396,982	276
10 July 2023	50,360	276	44,446	78	50,360	276	57,523	351	400,161	45	16,509	55
10 July 2023	16,509	55	398,324	190	22,612	55	398,324	190	14,061	946	14,061	946
10 July 2023	398,324	190	212,283	66	204,428	91	204,428	91	396,982	276	398,324	190
10 July 2023	8075	190	47,890	325	398,324	190	44,446	78	204,428	91	204,428	91
10 July 2023	44,446	78	398,722	171	207,812	55	6939	300	398,324	190	57,678	55
11 July 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	202,425	465
11 July 2023	396,982	276	202,425	465	6142	0	50,360	276	14,618	66	50,360	276
11 July 2023	57,043	78	396,982	276	396,982	276	14,061	946	16,509	55	14,618	66

Table A1. *Cont.*

Day	ISP1 Predicted ASN Prophet	ISP1 Predicted ASN Prophet Behavior Score	ISP1 Actual ASN	ISP1 Actual ASN Behavior Score	ISP2 Predicted ASN Prophet	ISP2 Predicted ASN Prophet Behavior Score	ISP2 Actual ASN	ISP2 Actual ASN Behavior Score	ISP3 Predicted ASN Prophet	ISP3 Predicted ASN Prophet Behavior Score	ISP3 Actual ASN	ISP3 Actual ASN Behavior Score
11 July 2023	14,061	946	14,061	946	50,867	105	396,982	276	50,360	276	57,523	351
11 July 2023	16,509	55	44,446	78	50,360	276	57,523	351	57,523	351	396,982	276
11 July 2023	57,523	351	57,523	351	14,061	946	398,324	190	14,061	946	14,061	946
11 July 2023	50,360	276	398,324	190	22,612	55	204,428	91	396,982	276	16,509	55
11 July 2023	398,324	190	212,283	66	204,428	91	207,812	55	204,428	91	47,890	325
11 July 2023	44,446	78	47,890	325	398,324	190	44,446	78	398,324	190	398,324	190
11 July 2023	8075	190	8075	190	57,523	351	206,728	78	44,446	78	204,428	91
12 July 2023	202,425	465	50,360	276	202,425	465	202,425	465	202,425	465	50,360	276
12 July 2023	396,982	276	202,425	465	396,982	276	50,360	276	14,618	66	202,425	465
12 July 2023	57,043	78	396,982	276	50,867	105	396,982	276	16,509	55	396,982	276
12 July 2023	57,523	351	14,061	946	50,360	276	14,061	946	396,982	276	57,523	351
12 July 2023	14,061	946	57,523	351	14,061	946	57,523	351	50,360	276	14,618	66
12 July 2023	50,360	276	44,446	78	22,612	55	398,324	190	57,523	351	14,061	946
12 July 2023	44,446	78	212,283	66	204,428	91	204,428	91	14,061	946	16,509	55
12 July 2023	398,324	190	398,324	190	398,324	190	701	78	204,428	91	47,890	325
12 July 2023	8075	190	47,890	325	207,812	55	63,949	300	398,324	190	398,324	190
12 July 2023	6939	300	63,949	300	57,523	351	207,812	55	44,446	78	204,428	91
13 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
13 July 2023	396,982	276	396,982	276	396,982	276	50,360	276	14,618	66	50,360	276
13 July 2023	57,523	351	50,360	276	50,867	105	396,982	276	396,982	276	396,982	276
13 July 2023	14,061	946	14,061	946	22,612	55	14,061	946	16,509	55	400,161	45
13 July 2023	50,360	276	57,523	351	50,360	276	42,821	0	57,523	351	57,523	351
13 July 2023	398,324	190	42,821	0	14,061	946	57,523	351	50,360	276	14,618	66
13 July 2023	44,446	78	47,890	325	204,428	91	398,324	190	14,061	946	14,061	946
13 July 2023	8075	190	44,446	78	398,324	190	204,428	91	204,428	91	16,509	55
13 July 2023	6939	300	398,324	190	207,812	55	206,728	78	398,324	190	42,821	0
13 July 2023	132,203	190	212,283	66	206,728	78	63,949	300	44,446	78	47,890	325
14 July 2023	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465	202,425	465
14 July 2023	396,982	276	396,982	276	396,982	276	396,982	276	14,618	66	396,982	276
14 July 2023	57,523	351	14,061	946	22,612	55	14,061	946	16,509	55	57,523	351
14 July 2023	14,061	946	57,523	351	50,360	276	42,821	0	396,982	276	14,061	946
14 July 2023	50,360	276	44,446	78	14,061	946	57,523	351	50,360	276	16,509	55
14 July 2023	398,324	190	42,821	0	204,428	91	50,360	276	57,523	351	14,618	66
14 July 2023	44,446	78	50,360	276	398,324	190	398,324	190	14,061	946	42,821	0
14 July 2023	8075	190	398,324	190	207,812	55	207,812	55	204,428	91	50,360	276
14 July 2023	6939	300	212,283	66	206,728	78	204,428	91	398,324	190	400,161	45
14 July 2023	132,203	190	8075	190	6939	300	44,446	78	44,446	78	398,324	190
15 July 2023	202,425	465	396,982	276	202,425	465	202,425	465	202,425	465	202,425	465
15 July 2023	396,982	276	202,425	465	396,982	276	396,982	276	14,618	66	396,982	276
15 July 2023	57,523	351	14,061	946	50,360	276	14,061	946	396,982	276	14,618	66
15 July 2023	50,360	276	44,446	78	14,061	946	57,523	351	16,509	55	57,523	351
15 July 2023	14,061	946	42,821	0	22,612	55	42,821	0	50,360	276	14,061	946
15 July 2023	44,446	78	57,523	351	204,428	91	398,324	190	57,523	351	42,821	0
15 July 2023	398,324	190	398,324	190	398,324	190	204,428	91	14,061	946	16,509	55
15 July 2023	8075	190	212,283	66	207,812	55	207,812	55	204,428	91	398,324	190
15 July 2023	6939	300	6939	300	6939	300	44,446	78	398,324	190	204,428	91
15 July 2023	132,203	190	47,890	325	206,728	78	6939	300	44,446	78	206,728	78

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 23 September 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. [CrossRef]
3. Aiken, M.P.; Davidson, J.C.; Kirichenko, A.; Markatos, E.P. Human Drivers of Cybercrime: A Forensic Cyberpsychology Approach to Behavioral Profiling. 2023. Available online: https://www.ccdriver-h2020.com/_files/ugd/0ef83d_d7709f405dbb40d2a125dff9e5e4872a.pdf (accessed on 27 February 2024).
4. Kirwan, G. *The Psychology of Cyber Crime: Concepts and Principles*; IGI Global: Hershey, PA, USA, 2011.
5. Ahmad, A.; Hadgkiss, J.; Ruighaver, A. Incident response teams—Challenges in supporting the organisational security function. *Comput. Secur.* **2012**, *31*, 643–652. [CrossRef]
6. Spitaletta, J.A. *Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations*; Johns Hopkins University Applied Physics Laboratory: Baltimore, MD, USA, 2021. Available online: https://nsiteam.com/social/wp-content/uploads/2021/07/Invited-Perspective-Operational-Cyber-Psych_FINAL.pdf (accessed on 23 September 2023).
7. Donalds, C.; Osei-Bryson, K.M. Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach. *Comput. Hum. Behav.* **2019**, *92*, 403–418. [CrossRef]
8. Alrowaily, M. Investigation of Machine Learning Algorithms for Improving Network Intrusion Detection System in Cybersecurity. Ph.D. Thesis, University of South Florida, Tampa, FL, USA, 2020.
9. Connolly, I.; Palmer, M.; Barton, H.; Kirwan, G. *An Introduction to Cyberpsychology*; Routledge: Abingdon, UK, 2016.
10. ReSCIND. Reimagining Security with Cyberpsychology-Informed Network Defenses. Office of the Director of National Intelligence; Intelligence Advanced Research Projects Activity (IARPA). Available online: https://www.iarpa.gov/research-programs/rescind (accessed on 12 October 2023).
11. Back, S.; LaPrade, J. The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *Int. J. Cybersecur. Intell. Cybercrime* **2019**, *2*, 1–4. [CrossRef]
12. 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, 2022; p. ch002. [CrossRef]
13. Kirwan, G.; Power, A. *Cybercrime: The Psychology of Online Offenders*; Cambridge University Press: Cambridge, UK, 2013.
14. Yan, Z. *Encyclopedia of Cyber Behavior*; IGI Global: Hershey, PA, USA, 2012; Volume 1, ISBN-10 1668425475.
15. INTERPOL. Cybercrime. 2022. Available online: https://www.interpol.int/en/Crimes/Cybercrime (accessed on 23 October 2023).
16. Gillam, A.R. Technology Threat Avoidance Factors as Predictors of Risky Cybersecurity Behavior within the Enterprise. Ph.D. Thesis, Indiana State University, Terre Haute, IN, USA, 2019.
17. Greitzer, F.L.; Hohimer, R.E. Modeling human behavior to anticipate insider attacks. *J. Strateg. Secur.* **2011**, *4*, 25–48. [CrossRef]
18. McAlaney, J.; Thackray, H.; Taylor, J. The Social Psychology of Cybersecurity. 2016. Available online: https://www.bps.org.uk/psychologist/social-psychology-cybersecurity (accessed on 12 June 2023).
19. 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. [CrossRef]
20. Bada, M.; Nurse, J.R.C. The social and psychological impact of cyber-attacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*; Academic Press: Cambridge, MA, USA, 2020.
21. Stallings, W. *Network Security Essentials: Applications and Standards*; Pearson: London, UK, 2017; ISBN-13 978-0134527338.
22. Lundie, M.J.; Lindke, K.L.; Aiken, M.P.; Janosek, D.M.; Amos-Binks, A. The Enterprise Strikes Back: Conceptualizing the HackBot—Reversing Social Engineering in the Cyber Defense Context. In Proceedings of the 57th Hawaii International Conference on System Sciences, Honolulu, HI, USA, 3–6 January 2024; pp. 984–993.
23. Aiken, M.P.; Davidson, J.C.; Walrave, M.; Ponnet, K.S.; Phillips, K.; Farr, R.R. Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. *Forensic Sci.* **2024**, *4*, 24–41. [CrossRef]
24. Benson, V.; McAlaney, J. *Cyber Influence and Cognitive Threats*; Academic Press: Cambridge, MA, USA, 2019.
25. Rich, M.S. Enhancing Microsoft 365 Security: Integrating Digital Forensics Analysis to Detect and Mitigate Adversarial Behavior Patterns. *Forensic Sci.* **2023**, *3*, 394–425. [CrossRef]
26. Rich, M.S. Cyberpsychology: A Longitudinal Analysis of Cyber Adversarial Tactics and Techniques. *Analytics* **2023**, *2*, 618–655. [CrossRef]
27. Pollini, A.; Callari, T.C.; Tedeschi, A.; Ruscio, D.; Save, L.; Chiarugi, F.; Guerri, D. Leveraging human factors in cybersecurity: An integrated methodological approach. *Cogn. Technol. Work* **2022**, *24*, 371–390. [CrossRef] [PubMed]
28. 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 23 September 2023).
29. Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [CrossRef]

30. 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: Salisbury, Australia, 2010.
31. Plachkinova, M.; Vo, A. A Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure (TRACI). *Commun. Assoc. Inf. Syst.* **2022**, 52. [CrossRef]
32. Rohan, R.; Funilkul, S.; Pal, D.; Chutimaskul, W. Understanding of Human Factors in Cybersecurity: A Systematic Literature Review. In Proceedings of the International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 1–3 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 133–140. Available online: https://ieeexplore-ieee-org.captechu.idm.oclc.org/document/9752358 (accessed on 23 September 2023).
33. 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 23 October 2023).
34. 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 23 October 2023).
35. 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. Priv.* **2022**, *2*, 527–555. [CrossRef]
36. 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*, 1789. [CrossRef]
37. Kia, A.N.; Murphy, F.; Sheehan, B.; Shannon, D. A cyber risk prediction model using common vulnerabilities and exposures. *Expert Syst. Appl.* **2024**, *237*, 121599. [CrossRef]
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*, 41. [CrossRef]
39. CC-Driver. Human and Technical Drivers of Cybercrime. 2022. Available online: https://www.ccdriver-h2020.com/project (accessed on 26 September 2022).
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 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW), Melbourne, Australia, 15–19 November 2021; pp. 153–158.
41. Weems, C.F.; Ahmed, I.; Golden, G.R., III; 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*, e0207408. [CrossRef] [PubMed]
42. Abdullah, M.M.; Ahmed, H.; Hasan, A.A.; Ali, D.B.; Al-Maeeni, M.K.A.; Gdheeb, S.H.; Salman, S.D. Designing Predictive Models for Cybercrime Investigation in Iraq. *Int. J. Cyber Criminol.* **2022**, *16*, 47–60. [CrossRef]
43. Wu, L.; Peng, Q.; Lembke, M. Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database. *Int. J. Cybersecur. Intell. Cybercrime* **2023**, *6*, 5–28. [CrossRef]
44. Samtani, S.; Kantarcioglu, M.; Chen, H. Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. *ACM Trans. Manag. Inf. Syst.* **2020**, *11*, 1–19. [CrossRef]
45. Pouani Tientcheu, P. Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals. Ph.D. Thesis, Walden University, Minneapolis, MN, USA, 2021.
46. Bhardwaj, A.; Kaushik, K.; Alomari, A.; Alsirhani, A.; Alshahrani, M.M.; Bharany, S. BTH: Behavior-Based Structured Threat Hunting Framework to Analyze and Detect Advanced Adversaries. *Electronics* **2022**, *11*, 2992. [CrossRef]
47. Sites, A.L., Sr. Thinking Like a Cyber Adversary: Exploring the Impact of Language Fluency for Cyber Security. Ph.D. Thesis, Northcentral University, La Jolla, CA, USA, 2019.
48. 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 27 November 2023).
49. Fernandez, G.C. Deep Learning Approaches for Network Intrusion Detection. Master's Thesis, The University of Texas at San Antonio, San Antonio, TX, USA, 2019.
50. Kaye, L.K. *Issues and Debates in Cyberpsychology*; Open University Press: London, UK, 2022.
51. Khader, M.; Neo, L.S.; Chai, W.X.T. *Introduction to Cyber Forensic Psychology: Understanding the Mind of the Cyber Deviant Perpetrators*; World Scientific: Singapore, 2021.
52. Attrill, A.; Fullwood, C. *Applied Cyberpsychology: Practical Applications of Cyberpsychological Theory and Research*; Palgrave Macmillan: New York, NY, USA, 2016.
53. Sutter, O.W. The Cyber Profile: Determining Human Behavior through Cyber-Actions. Ph.D. Thesis, Capitol Technology University, Laurel, MD, USA, 2020.
54. Withers, K.L. A Psychosocial Behavioral Attribution Model: Examining the Relationship between the "Dark Triad" and Cyber-Criminal Behaviors Impacting Social Networking Sites. Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale, FL, USA, 2019.

55. Burgio, D.A. Reduction of False Positives in Intrusion Detection Based on Extreme Learning Machine with Situation Awareness. Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale, FL, USA, 2020.
56. 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.