IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 January 2024, accepted 15 February 2024, date of publication 19 February 2024, date of current version 23 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3367240

RESEARCH ARTICLE

2019–2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques

OLUFUNSHO I. FALOWO, (Student Member, IEEE), AND JACQUES BOU ABDO
School of Information Technology, University of Cincinnati, Cincinnati, OH 45221, USA
Corresponding author: Olufunsho I. Falowo (falowooi@mail.uc.edu)

ABSTRACT This comprehensive study investigates the trends, impacts, and global distribution of major Distributed Denial of Service (DDoS) attacks from 2019 to 2023, aiming to understand their evolution and predict future trends. Over the past five years, we have observed a significant escalation in both the frequency and severity of major cybersecurity incidents associated with DDoS attacks, underscoring their evolution from sporadic disruptions to more persistent and globally distributed threats. This study meticulously analyzes data from major incidents reported by reputable institutions, providing a focused insight into impactful cyberattacks. This approach highlights the increasing sophistication of threat actors and the expanding scope of targets, including critical national infrastructures and key economic sectors. The impact analysis reveals that these attacks not only cause immediate operational disruptions but also lead to substantial economic and reputational damages, reflecting the growing dependency of modern societies on digital infrastructure. Additionally, this study explores the correlation between these cyberattacks and geopolitical tensions, suggesting their use as strategic tools in broader political and economic conflicts. To predict future trends, the study employs ARIMA and Exponential Smoothing State Space (ETS) models, offering a quantitative forecast for 2024-2026. These models provide valuable insights, although they also exhibit limitations due to the dynamic nature of cyber threats and technological advancements. The study, contributed by authors with over 40 years of combined experience in cybersecurity, underscores the need for adaptive and resilient cybersecurity strategies. It highlights the importance of continuous monitoring and evolving defense mechanisms to counter the unpredictable nature of DDoS attacks in an increasingly interconnected world.

INDEX TERMS DoS attacks, DDoS attacks, major cybersecurity incidents, incident response strategies, geo-politics.

I. INTRODUCTION

The 2023 Data Breach Incident Report (DBIR) provides crucial insights into the evolving landscape of Distributed Denial of Service (DDoS) attacks, particularly focusing on the period between November 1, 2021, and October 31, 2022 [1]. A standout finding from the report is the significant growth in the intensity of DDoS attacks. The median attack size surged by an astonishing 57%, rising from 1.4 gigabytes per second (Gbps) in the previous year to 2.2 Gbps [1]. This notable increase in the median attack size is indicative of a worrying trend in the cyber threat arena, suggesting that attackers are gaining access to more powerful resources to amplify their attacks [1]. Furthermore, the report notes an increase in the upper percentiles of attack sizes, with the 97.5 percentile witnessing a 25% growth from 99 Gbps to 124 Gbps. These statistics not only underscore the escalating severity of DDoS attacks but also highlight the growing challenge faced by organizations in mitigating such high-volume cyber assaults.

The insights from the 2023 Data Breach Incident Report (DBIR) about the marked increase in the intensity and scale of Distributed Denial of Service (DDoS) attacks align closely with the trends observed in our study of another independent report [2] spanning from 2013 to 2023. The DBIR's finding of a significant jump in the median DDoS attack size - from

The associate editor coordinating the review of this manuscript and approving it for publication was Francesco Tedesco.

1.4 gigabytes per second (Gbps) to 2.2 Gbps, and the upper percentile growth from 99 Gbps to 124 Gbps - resonates with the spike we observed in 2022 in Figure 1 which is drawn from major incidents caused by DDoS according to the Major Cyber Incidents reported by the Center for Strategic & International Studies [2]. This parallel not only validates the need to investigate but also highlights a crucial evolving aspect of DDoS attacks: their growing capability to inflict more severe damage. The escalation in attack magnitude over the years, culminating in the substantial surge in 2022, suggests an alarming trend in the cyber threat landscape, where attackers are increasingly leveraging more powerful resources, making DDoS attacks more formidable and challenging to mitigate.

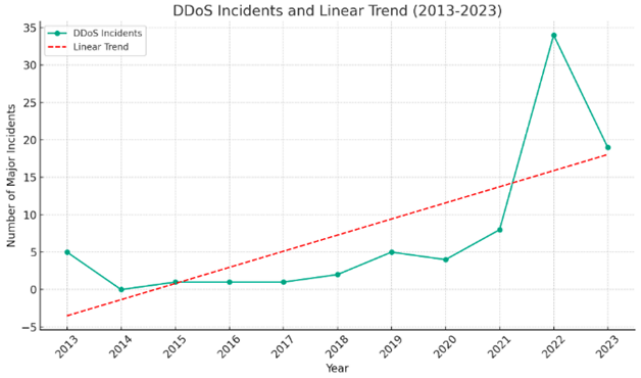

FIGURE 1. Reported major incidents: 2013 - 2023 [2], [3].

The significant surge in Distributed Denial of Service (DDoS) attacks witnessed in 2022 [2], set against the broader context of the five-year period from 2019 to 2023, necessitates a detailed and targeted inquiry into the underlying causes of this escalation. This investigation is crucial for gaining a deeper understanding of the dynamics and factors driving such spikes in DDoS incidents. By thoroughly examining these aspects, one of the aims of this study is to enhance our capability to foresee and effectively predict future occurrences of this type of cyber threat. This enhanced predictive ability is not just vital for preparedness but also for developing more robust and resilient cyber defense mechanisms to mitigate the impact of such attacks in the years ahead. The DBIR points to the increased accessibility and affordability of bandwidth and CPU processing power as key enablers of this trend [1]. However, understanding the nuances of the surge of this threat in very recent years requires a deeper dive. It's imperative to explore whether this increase was driven by advancements in attack technologies, the emergence of new threat actor groups, geo-political dynamics or the exploitation of specific vulnerabilities that became more pronounced in recent years. Investigation like this will provide valuable insights into the dynamics of DDoS threats and inform the development of more effective defense strategies. This research is not only important for advancing our understanding of DDoS attacks but also for guiding policymakers, cybersecurity professionals, and organizations in reinforcing their defenses against these increasingly sophisticated cyber threats.

A. RESEARCH QUESTION

The research question that this study aim to address is "How have the trends, impacts, and global distribution of major DDoS attacks evolved from 2019 to 2023, and to what extent can threat like this be predicted?"

II. BACKGROUND LITERATURE

A. ATTACK VECTOR DIVERSITY

Many security experts and academic studies have highlighted how DDoS attacks can be executed through various vectors [4], such as volumetric attacks [5], protocol attacks, and application layer attacks [6], [7]. Examining the diversity of these vectors is crucial for understanding the full range of tactics used by threat actors to the extent where they cause disruption. Volumetric attacks, for instance, has capability to flood an enterprise network with traffic, while application layer attacks on the other hand target specific aspects of a website or application [5], [6], [7]. By understanding the range and nature of these vectors, organizations can better anticipate and enhance their preparedness for different types of DDoS attacks, ensuring a more robust and comprehensive defense strategy.

B. BOTNET UTILIZATION AND EVOLUTION

The malicious use of botnets is becoming very prominent in this digital age to the extent that these networks of infected devices can be used to amplify DDoS attacks [8], [9]. Investigating how these constantly evolving botnets are assembled, controlled, and utilized can provide critical insights into the scale and capability of DDoS attacks. The evolution of botnets, especially with the increasing use of IoT devices, have been described to represents a significant threat as it allows attackers to seamlessly launch larger and more disruptive DDoS attacks [8], [9]. Hence, the understanding the dynamics of botnet utilization can aid in developing specific strategies to disrupt or mitigate these networks.

C. SOURCE AND TARGET ANALYSIS

Leveraging advance technology in analyzing the sources and targets of DDoS attacks can reveal patterns and motives behind these incidents and may even help with attribution is other cases [10]. Identifying common characteristics of target systems, such as industry type, system vulnerabilities, or geographic location, may significantly helps in understanding why certain systems are targeted and how to effectively protect them. Similarly, tracing the source of attacks, though may be challenging, can provide very useful insights into the threat actors' profiles, their techniques, and possibly their motivations, enabling more targeted countermeasures and policy responses.

D. MITIGATION AND RESPONSE STRATEGIES

With reference to an enterprise or an entity's network or cloud infrastructure, examining existing mitigation and response strategies against DDoS attacks is essential in order to evaluate their effectiveness and identify areas for improvement. This includes analyzing the deployment of defensive measures like firewalls, intrusion detection systems, intrusion prevention systems, DDoS protection services and other administrative controls as well [11], [12]. It's important to frequently assess how these strategies stand up to the evolving nature of DDoS attacks and whether or not they are adaptable to the constantly increasing complexity and scale of these threats [13], [14]. Periodic evaluation of incident response strategies which often involves looking at how organizations prepare for, respond to, and recover from DDoS attacks, tend to be very crucial for reducing downtime and mitigating damage [13], [14], [15]. Each of these aspects plays a pivotal and a fundamental role in the appraisal of DDoS attacks. By examining them, cybersecurity professionals, organizations, and policymakers can gain a holistic view of the nature and dynamics of these threats, leading to the development of more effective defense and mitigation strategies.

III. METHODOLOGY

In this study, we adopted an integrative approach, incorporating a variety of scientific research methodologies to ensure a robust and nuanced analysis. Key to our approach was the application of sampling theory [16], [17], which ensured the representativeness and comprehensiveness of the data we collected, a fundamental aspect for the credibility and relevance of our findings. Alongside this, we employed principles of reliability and validity theory [18], which were critical in affirming the accuracy and dependability of our results, thus bolstering the integrity of our research.

Moreover, our study extended to include a thematic analysis [19], which allowed us to identify and analyze patterns or themes within other studies related to DDoS attacks. This qualitative approach complemented our quantitative methods, offering deeper insights into the underlying narratives and contextual factors surrounding major incidents typically connected to DDoS. In parallel, we examined the geographical distribution of major DDoS attacks, seeking possible causation or correlations [20], [21] with geopolitical tensions, which provided a broader understanding of the external factors influencing these cyber threats. For forecasting future trends in major cybersecurity incidents that are likely as a result of DDoS attack, we utilized the Exponential Smoothing State Space Model (ETS) [22], [23] and ARIMA models [24], [25]. These statistical tools were pivotal in predicting future DDoS attack patterns, equipping us with a predictive framework to anticipate and prepare for future cyber challenges effectively.

A. SAMPLING THEORY

In this study, we meticulously analyzed all 612 major incidents that were associated with various types of attack techniques which includes, phishing, malware, exploit of vulnerabilities, DDoS and other attack techniques based on what is publicly reported over the last five years, spanning from 2019 to 2023. To ensure the statistical robustness of our findings and to accurately generalize them to the larger set of major cybersecurity incidents, we employed a sample size calculation formula. This calculation was anchored on a set of specific parameters: a 90% confidence level, a 5% margin of error, and an assumed population proportion of 5%. These parameters were carefully chosen to balance the need for a precise and reliable representation of the wider population of major cybersecurity incidents, while also considering the practical limitations of data availability and analysis.

The theory of sampling as one of few cornerstone of statistical analysis was fundamental to our calculation. It provides us with the framework for estimating characteristics of a large population based on a smaller, representative subset, or sample. In this study, this theory guided us in selecting a sample size that was not only statistically significant but also feasible to study. It ensured that our sample was sufficiently large to reflect the broader population trends and behaviors accurately, thereby minimizing the potential for sampling bias. By adhering to the principles of sampling theory, we were able to draw reliable and generalizable conclusions from our analysis, offering valuable insights into the nature and dynamics of major cybersecurity incidents over the specified period. This methodology underscores the importance of rigorous statistical planning in conducting research that aims to reflect broader patterns and trends accurately.

B. STATISTICAL SIGNIFICANCE

With reference to the calculated sample size [26], [27] of 66 from the formular below, derived from the parameters defined in our study—90% confidence level, 5% margin of error, and a population proportion of 5%—is pivotal for ensuring the statistical significance and reliability of our investigation into major cybersecurity incidents. This figure represents the minimum number of major cybersecurity incidents that need to be analyzed to confidently generalize our findings to the broader population of major incidents. A sample size of 66 or more provides a robust basis for drawing inferences, as it adequately captures the variability and trends within the larger dataset of 612 major incidents. This ensures that the conclusions drawn are not just reflective of a small, potentially unrepresentative subset of data, but are in fact indicative of the wider patterns and characteristics of major incidents over the last five years. The ability to generalize from this sample size is fundamental to the credibility and applicability of our study's insights, making it a crucial element in the field of cybersecurity research and analysis.

The sample size (n) is calculated according to the formula:

$$n = \frac{\left(\frac{(z^2 \times p) \times (1-p)}{e^2}\right)}{1 + \left(\frac{(z^2 \times p) \times (1-p)}{(e^2 \times N)}\right)}$$

where: z = 1.96 for a confidence level (α) of 95%, p = proportion (expressed as a decimal), N = population size, e = margin of error.

$$z = 1.96, \quad p = 0.05, \; N = 612, \; e = 0.05$$

$$n = \frac{\left(\frac{(1.96^2 \times 0.05) \times (1-0.05)}{0.05^2}\right)}{1 + \left(\frac{(1.96^2 \times 0.05) \times (1-0.05)}{(0.05^2 \times 612)}\right)}$$

$$n = \frac{72.99}{1.12}$$

$$n \approx 66$$

C. RELIABILITY AND VALIDITY THEORY

Utilizing the Exponential Smoothing State Space Model (ETS) and ARIMA models for forecasting future trends in major cybersecurity incidents attributable to DDoS attacks aligns with the principles of reliability and validity [28], [29], key tenets in our study. These statistical models are well known for their accuracy in time-series forecasting, offering an important framework for predicting future major incidents based on historical data patterns. By employing these models to project the trajectory of major DDoS incidents for the next three years (2024 to 2026), we ensure that our forecasts are not only consistent (reliability) but also accurately reflect the true nature of the cybersecurity landscape (validity). This methodological rigor bolsters the credibility of our study, ensuring that the insights and forecasts provided are both trustworthy and relevant in the context of evolving cybersecurity threats.

D. UNRAVELLING CORRELATION WITH GEO-POLITICS

The analysis of the geographical distribution of these major DDoS attacks plays an important role in our study, as it aims to investigate the potential correlation or causation between these major DDoS attack incidents and regional geopolitical tensions. By mapping the target countries of these major DDoS attacks and examining their frequency in various regions, we intend identify patterns and trends that may be associated with geopolitical dynamics. This approach involves a detailed examination of the temporal and spatial aspects of the attacks, looking for possible indicators that aligns with political events, international conflicts, or regional disputes. The goal is to discern whether these cyber incidents are random occurrences or if they are possibly influenced by, or even instrumental in, the broader context of global or regional political unrest. This method not only aids in understanding the motivations behind some of these major DDoS attacks but also in anticipating future cybersecurity threats in relation to evolving geopolitical scenarios.

E. THEMATIC ANALYSIS

In our effort to incorporate a thematic analysis of recent studies associated with major DDoS incidents, we harnessed the power of cross-querying electronic databases by utilizing Google Scholar, a comprehensive academic search engine. We specifically tailored our search to focus on studies published between 2019 and 2023, applying a filter to hone in on relevant research. In the first week of January 2024, we conducted a targeted search for ''Major DDoS Incidents,'' from which we carefully selected the top 10 most pertinent studies. Our analysis involved a thorough review of the abstracts, introductions, discussions, and conclusions of these selected studies to identify and extract common themes. This approach allowed us to synthesize a broad range of academic insights and perspectives on the subject, providing a well-rounded understanding of the trends and dynamics in major DDoS incidents during the specified period. This methodological strategy of incorporation of thematic analysis ensured both depth and breadth in our analysis, leveraging existing academic knowledge to augment our study.

IV. RESULTS

A. TAKEAWAY SUMMARY FROM THEMATIC ANALYSIS

Through our methodical search in Google Scholar, adhering to the set of criteria outlined in our methodology section, we identified 50 relevant mostly studies and few books within the first five pages of our search results. From this pool, we meticulously selected 10 journal and proceeding publications, as enumerated below. This selection was based on their direct relevance to our focus on major DDoS incidents. Our thematic analysis of these carefully chosen sources revealed several compelling common themes that underpin the current understanding of DDoS attacks within the academic community.

A prominent theme emerging from all these studies is the unanimous recognition of the significance of disruptive nature of major incidents caused as a result of DDoS attacks. This disruption is often not merely confined to only temporary technical inconveniences but often extends to economic and societal impacts. Furthermore, these studies collectively highlight the evolution of DDoS threats, emphasizing their increasing complexity and sophistication. They echoed how threat actors have continuously refined their methods, making DDoS attacks more complex and challenging to mitigate. This sophistication is often characterized by the use of advanced techniques, making DDoS a preferred tool for attackers due to its effectiveness and impact. These common findings underscore the pertinence of our study, as they align with and reinforce our research objectives, providing a robust academic foundation to our investigation into the nature, trends, and implications of DDoS attacks. Below is brief description of each of these final selected studies:

1) Brooks et al., [30] provides an overview of the technologies and tools used in Distributed Denial of Service (DDoS) attacks, traces their historical timeline, discusses their evolution from hacker culture to commercial and political exploitation, and examines how the Internet's structure enables these attacks.
2) Merlino et al., [31] discusses the development of a situational awareness tool designed to detect and

understand amplification DDoS attacks on the smart grid, highlighting the tool's effectiveness against real attack instances and the need for defensive capabilities in cyber-attack identification.

3) Patil et al., [32] provides a comprehensive review of existing distributed frameworks for DDoS attack detection, evaluates their effectiveness, and discusses open issues, datasets, and future directions in enhancing web-based application defenses against growing DDoS threats.
4) Falowo et al., [3] conducts an exploratory analysis of hundreds of major cybersecurity incidents, finding that malware, phishing, DDoS among others are the predominant attack techniques, and emphasizes the importance of organizational readiness and adherence to frameworks like NIST for effective incident response.
5) Bhardwaj et al., [33] in a survey examines the gaps in existing DDoS defense solutions for cloud environments, highlights future attack potentials, explores machine learning detection methods, and aims to guide the research community in developing effective strategies against escalating DDoS threats in cloud computing.
6) Vishwakarma et al., [34] delves into the issue of DDoS attacks in IoT networks, discussing the role of malware and botnets, comparing various defense techniques, and identifying open research challenges for developing more effective and smarter DDoS defenses in the IoT landscape.
7) Nehinbe et al., [35] in this research work addresses the challenges of DDoS attacks and datasets, proposing the merger of different datasets using C++ programming for enhanced analysis and investigation, aiding in legal enforcement against cyber intruders.
8) Hekmati et al., [36] introduces a dataset from an urban IoT deployment and a synthetic DDoS attack generator, demonstrating their use in training and evaluating a neural network to detect and defend against DDoS attacks in large-scale IoT networks.
9) Falowo et al., [37] in this study, focuses on how machine learning techniques can be leveraged for the detection and mitigation of DDoS attacks, analyzing hundreds of major incidents that were publicly reported from 2015 to 2022 and advocating for the use of AI and frameworks like NIST's "AI Risk Management Framework" for comprehensive DDoS defense.
10) Jayasekara et al., [38] in this investigation, conducted by an independent digital intrusion consultancy, focuses on a DDoS attack involving Mirai malware at Dash LLC's London branch, aiming to analyze the breach, identify the perpetrator and their motives, and offer strategic cybersecurity recommendations to mitigate future threats.

B. SAMPLE SIZE ANALYSIS

The observation of 70 major incidents associated with DDoS attacks out of the 612 major incidents publicly reported from 2019 to 2023 holds significant statistical importance, particularly in the context of sampling theory. This 70 major incidents not only surpasses the threshold of required sample size of 66, as determined by our sample size calculation, but exceeds it and also constitutes 11.4% of the total major incidents that we analyzed. Just to reiterate, this 70 major incidents exceeds the minimum sample size required for our study, affirming the statistical robustness and representativeness of our findings. From a sampling theory perspective, having a sample size that exceeds the calculated minimum is advantageous. It enhances the reliability and validity of the conclusions drawn from the data, as it reduces the margin of error and increases confidence in the generalizability of the results. Thus, these 70 incidents provide a substantial and statistically significant sample to analyze the patterns and implications of DDoS attacks during the studied period.

With reference to Figure 2, the year-on-year percentage increase in major incidents associated with DDoS attacks from 2019 to 2023 shows a worrying escalation. Starting with only five incidents in 2019, then four in 2020, followed by a doubling to eight in 2021. However, the most striking jump occurred in 2022 with thirty-four incidents, an increase of over 325% from the previous year. The trend continued in 2023 with nineteen incidents, though this represents a decrease from the 2022 peak. This trend highlights a growing prevalence and possibly an increasing sophistication of DDoS attacks over the years, underscoring the need for heightened vigilance and advanced countermeasures in the cybersecurity landscape.

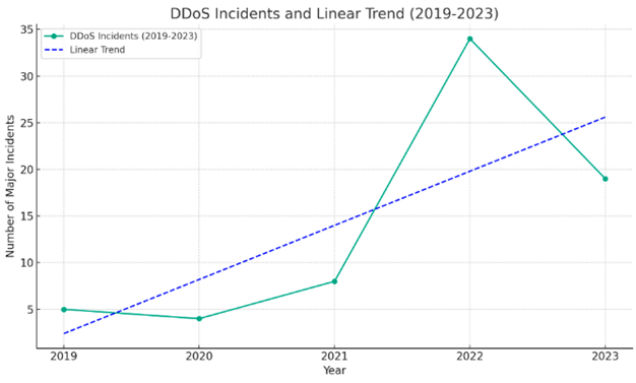

FIGURE 2. Reported major incidents: 2019 - 2023 [2], [3].

1) 2021 IN REVIEW

As visualized in Figure 3, the trend of major DDoS attacks in 2021, as observed from a month-on-month analysis, presents a highly uneven distribution throughout the year. The year began and mostly continued with a minimal occurrence of attacks, as evidenced by zero incidents in January, March,

April, and from August to December. A slight uptick was observed in February, May, and June, each recording a single DDoS attack. However, a significant and anomalous spike is evident in July, with eight attacks, a number that starkly contrasts with the otherwise low frequency in other months. This outlier suggests either a unique set of circumstances or an escalation in threat activity during that period. Overall, the 2021 trend of DDoS attacks demonstrates a generally low but erratic pattern, punctuated by a sudden and notable surge in July, highlighting the unpredictable nature of these cyber threats.

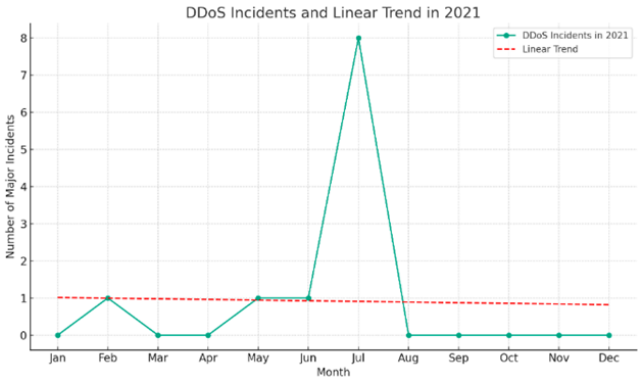

FIGURE 3. Reported major incidents in 2021 [2], [3].

2) 2022 IN REVIEW

In reference to Figure 4, the 2022 trend in major DDoS attacks, as delineated from a month-on-month perspective, shows a consistent and relatively elevated level of activity throughout the year compared to 2021. The year commenced with a steady occurrence of two incidents each in January, February, and March, followed by a slight increase to three incidents in April, May, September, and October. June and November also saw a continuation of this moderate frequency with two incidents each. Notably, July and August marked the peak of DDoS activities, with three and six incidents respectively, indicating a significant rise during these months. The consistency in the number of attacks per month, along with the heightened activity in the mid-year, suggests an overall increase in the frequency and possibly the sophistication of DDoS attacks in 2022. This trend underscores a persistent and growing threat landscape, necessitating vigilant and adaptive cybersecurity measures.

3) 2023 IN REVIEW

Per Figure 5, in 2023, the trend of major DDoS attacks, as revealed by a month-on-month analysis, exhibited a somewhat fluctuating pattern. The year began with a single attack in January, followed by an increase to three in February, then a slight decrease to two incidents each in March and April. A notable aspect of 2023 was the complete absence of attacks in May, October, November,

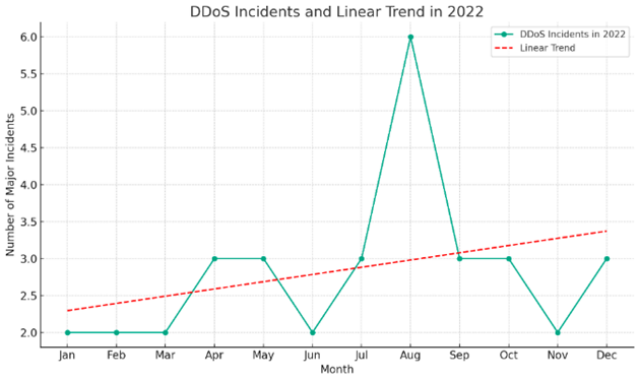

FIGURE 4. Reported major incidents in 2022.

and December, indicating periods of relative calm. However, the middle of the year witnessed an escalation, with June recording two attacks, July three, and August experiencing the peak with four incidents. September then saw a reduction to two attacks. This pattern suggests a concentration of DDoS activity particularly in the summer months, with a significant drop-off towards the end of the year. The fluctuating nature of these incidents throughout 2023 highlights the dynamic and unpredictable character of DDoS attack trends, necessitating continuous monitoring and adaptive cybersecurity strategies.

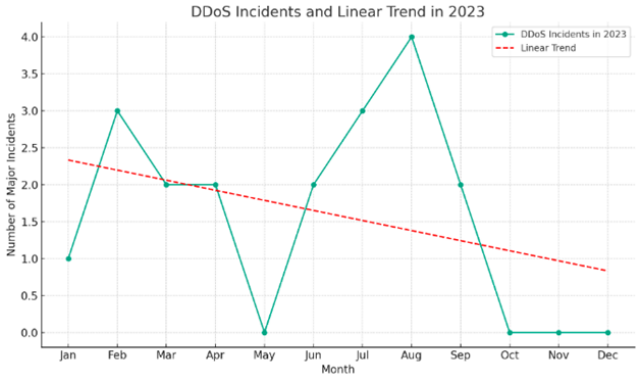

FIGURE 5. Reported major incidents in 2023.

C. CORRELATION OF EVENTS FROM 2021, 2022 & 2023

The frequencies of major incidents associated with DDoS attacks over the years 2021, 2022, and 2023 as highlighted in Figure 6, present intriguing trends with some notable differences and similarities, offering insights into the evolving nature of these cyber threats. In 2021, the trend was characterized by a generally low frequency of major incident associated with DDoS attacks throughout the year, with most months recording zero or one incident. The exception was a significant spike in July, where eight major incidents were reported, standing out as an anomalous peak in an otherwise calm year. This pattern suggests that DDoS attacks were sporadic and less frequent in 2021, with a sudden surge in

mid-year that could indicate a targeted wave of attacks or a temporary escalation in threat activity.

In contrast, 2022 displayed a more consistent and heightened level of DDoS incidents throughout the year. Each month recorded at least two major attacks, with a steady rise to three major incidents in several months and reaching a peak of six reported major attacks in August. This consistency and increase in frequency imply a more persistent threat landscape in 2022, with DDoS attacks becoming a more regular occurrence. Moving to 2023, the trend shows a fluctuating pattern, with some months like May and the last quarter of the year experiencing no attacks, while other months, particularly in the summer, saw a higher frequency of major incidents. The peak in August 2023, similar to 2022, suggests a possible seasonal trend or a specific time of heightened vulnerability. Comparing these three years, it is evident that while 2021 was marked by sporadic activity with a notable mid-year spike, 2022 and 2023 demonstrated more consistent and sustained DDoS attack frequencies, albeit with some monthly fluctuations. These observations point towards an evolving and increasingly sophisticated DDoS threat landscape, with varying intensities and patterns of attacks over the years.

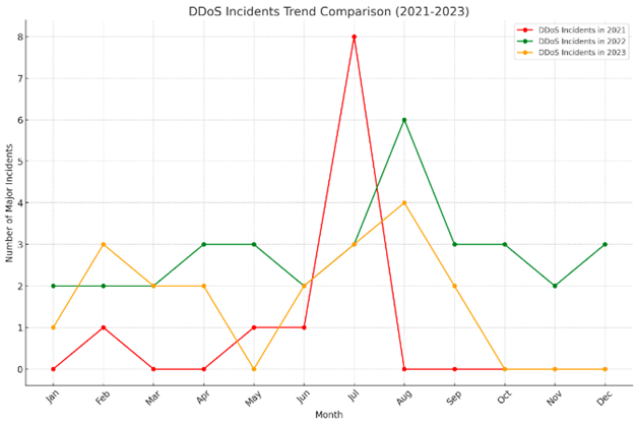

FIGURE 6. Reported major incidents in 2021, 2022 & 2023.

D. UNRAVELLING CORRELATION WITH GEO-POLITICS

With reference to Figure 7, 8 and 9, our observation of major incidents associated with DDoS attacks from 2021 to 2023 shows a clear variation in the impact across different continents. Initially, the focus was heavily on Europe, indicating a higher concentration of such incidents in this region. As time progressed into 2022, this trend not only persisted but also expanded to include North America, signaling an increased breadth in the geographical targeting of these attacks. In 2023, the pattern became even more diverse, with significant incidents reported across various continents, including Africa, Asia, and Oceania. This progression illustrates a shift from a region-centric to a more global focus in the cyber threat landscape. Throughout the three-year period, Europe consistently emerged as the most impacted continent, experiencing a higher frequency of DDoS attacks compared to other regions.

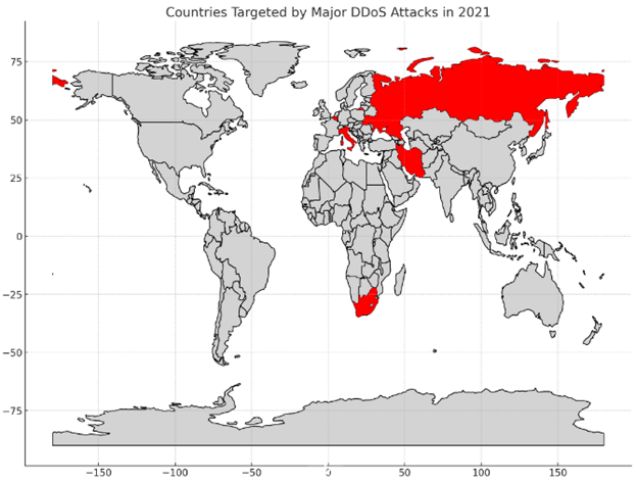

FIGURE 7. Regions targeted by notable DDoS attacks in 2021.

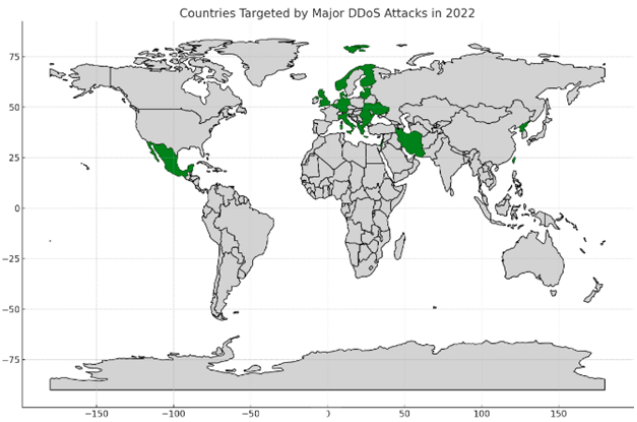

FIGURE 8. Regions targeted by notable DDoS attacks in 2022.

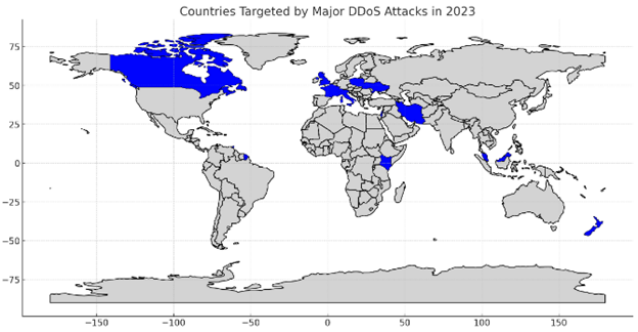

FIGURE 9. Regions targeted by notable DDoS attacks in 2023.

The observation of spatial distribution of major DDoS attacks on critical national infrastructure, institutions, or human populations could suggest a possible correlation with geopolitical tensions. This observation suggest that cyberattacks were often leveraged in geopolitical contexts, aiming to disrupt or influence nations by targeting key

infrastructures. The concentration of attacks in certain regions might reflect the underlying political and economic complexities of those areas, often characterized by their significant roles in global affairs. As the scope of these attacks broadens, encompassing a more varied range of regions, it might indicate changing geopolitical landscapes and alliances. This expansion underscores the growing role of cyber warfare as a tool in international relations and conflict, where its impact is increasingly felt across diverse global locations.

E. FORECAST: 2024 TO 2026

The ARIMA model forecast for DDoS incidents from 2024 to 2026, along with an 80% confidence interval, is visually represented in the plot in Figure 10. This forecast provides a quantitative projection of the expected number of major DDoS incidents in the coming years. Based on the forecast, the following numbers have been predicted:

- For 2024, the forecasted number of major incidents is approximately 16.07. The 80% confidence interval suggests that the actual number could range between −1.26 (which isn't practically plausible and indicates model limitations) and 33.40.
- In 2025, the forecasted incidents are around 14.69, with a confidence interval ranging from −5.38 to 34.77.
- For 2026, it is forecasted to have about 14.05 incidents, with the lower and upper bounds of the confidence interval at −6.99 and 35.09, respectively.

These forecasts, particularly with their wide confidence intervals, highlight a significant degree of uncertainty, reflecting the complex and unpredictable nature of major DDoS attack trends. Given the parameter defined for these forecast, the negative lower bounds is indicative of a limitation in the model's ability to capture the true nature of future major incidents accurately, especially considering the practical impossibility of negative incidents.

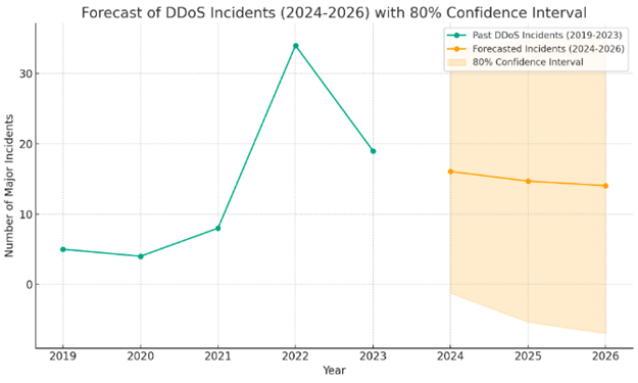

FIGURE 10. Forecast: ARIMA model, 80% confidence interval.

The ARIMA model forecast for DDoS incidents from 2024 to 2026 with a 95% confidence interval on the other hand, as presented in Figure 11, provides an even more comprehensive view of the expected trends and their associated uncertainties:

- For 2024, the forecast estimates approximately 16.07 incidents. The 95% confidence interval for this year spans from −10.44 to 42.58, indicating a significantly broader range of possible outcomes. This wider interval reflects a higher level of uncertainty in the prediction.
- In 2025, the forecast is around 14.69 incidents, with the confidence interval extending from −16.01 to 45.40.
- For 2026, the model predicts about 14.05 incidents, with a confidence interval ranging from −18.13 to 46.23.

Utilizing a 95% confidence interval results in the widest range of potential outcomes, encompassing a greater level of uncertainty compared to the 80% and 90% intervals. The negative lower bounds in these intervals are a statistical artifact indicating the model's limitations and the inherent challenges in accurately forecasting the complex dynamics of DDoS attacks. The wide confidence intervals underscore the unpredictability of these cyber threats and the need for flexible and adaptive cybersecurity strategies.

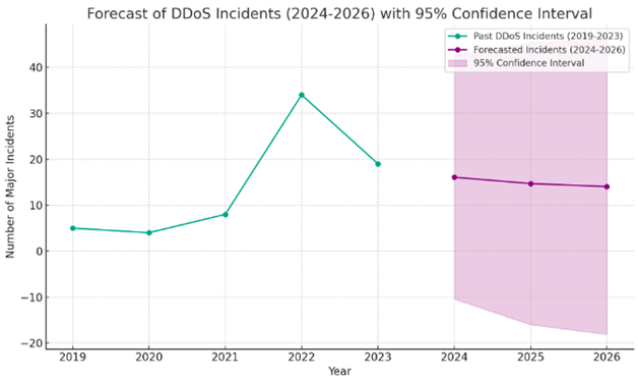

FIGURE 11. Forecast: ARIMA model, 95% confidence interval.

The Exponential Smoothing State Space Model (ETS) forecast for major DDoS incidents from 2024 to 2026 is depicted in Figure 12. This model, using trend components and a damping factor, calculates and projects the estimated number of anticipated major incidents that are attributable to DDoS attacks for the next three years. Based on the ETS model forecast, the predicted numbers of major DDoS incidents for the years 2024 to 2026 are as follows:

- 2024: Approximately 29.93 incidents are forecasted.
- 2025: The forecast predicts around 34.33 incidents.
- 2026: The model estimates about 38.40 incidents.

These forecasts suggest an increasing trend in the number of DDoS incidents over the next three years. The ETS model, by accounting for both historical data and trends, provides a valuable tool for anticipating future cybersecurity challenges, indicating a potential escalation in DDoS attack frequencies in the coming years.

The use of both ARIMA and ETS models in forecasting future trends of DDoS incidents significantly contributes

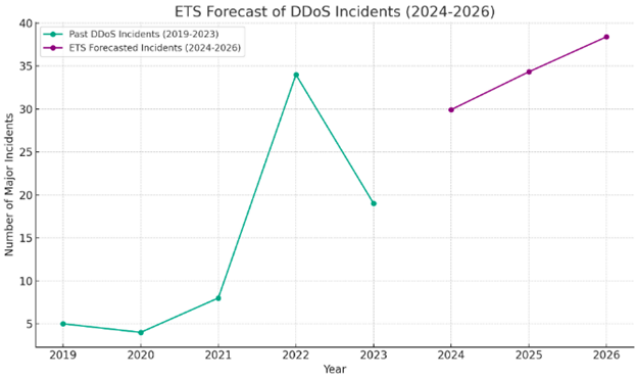

FIGURE 12. Forecast: ETS model.

to the reliability and validity of this study. The ARIMA model, with its emphasis on understanding and leveraging the autocorrelations within the historical data, provides a nuanced view of how past trends in these major DDoS incidents may influence future occurrences. For instance, the ARIMA forecasts for 2024 to 2026, despite their wide confidence intervals, reflect a realistic uncertainty inherent in predicting cyber threats, acknowledging the complexities and variabilities in attack patterns. This acknowledgment of uncertainty is crucial for a balanced and realistic forecast, enhancing the study's reliability. The wide confidence intervals, though suggesting high uncertainty, are more realistic representations of the unpredictable nature of DDoS attacks, thereby lending validity to the study by not overstating the precision of the predictions.

On the other hand, the ETS model, known for its ability to capture trends and seasonality in time series data, offers a complementary perspective. The ETS forecasts for the years 2024 to 2026 show an increasing trend in DDoS incidents, indicating a potential escalation in future threats. This model's strength lies in its capacity to incorporate both the error, trend, and seasonality components of the time series data, providing a comprehensive outlook. The differing approaches of ARIMA and ETS models enrich the study's findings, allowing for a more robust and well-rounded analysis. The combination of these models, each with its unique methodological strengths, ensures that the study's forecasts are grounded in varied analytical perspectives, thus enhancing the overall reliability and validity of this research.

Figure 13 simultaneously plots the forecasts from both the ARIMA model (with a 95% confidence interval) and the ETS model for the years 2024, 2025, and 2026, based on the frequency of major incidents associated with DDoS attacks from 2019 to 2023. Further comparing and contrasting these two forecasting models:

- ARIMA Model: The ARIMA forecast (in orange) with a 95% confidence interval indicates a projection with a significant range of possible outcomes, as shown by the shaded area. This model's forecasts for the years 2024 to 2026 suggest a relatively stable or slightly declining trend in DDoS incidents as described in prior section. The wide confidence intervals reflect a considerable degree of uncertainty, acknowledging the unpredictable nature of cyber threats.
- ETS Model: The ETS forecast (in green) shows a different trend, predicting a steady increase in the number of DDoS incidents for each subsequent year. Unlike the ARIMA model, the ETS does not inherently provide a confidence interval in this visualization, but it suggests a clear upward trend in the frequency of major cybersecurity incidents that will be attributable to DDoS attacks.

In summary, while the ARIMA model with its confidence interval indicates a broader range of potential outcomes with a more conservative estimate, the ETS model predicts a consistent increase in DDoS incidents. This divergence highlights the inherent differences in these models' approaches to forecasting, with ARIMA focusing on the historical autocorrelation and ETS emphasizing trend and seasonality. The choice between these models for strategic planning would depend on the level of risk tolerance and the specific requirements of cybersecurity policy and resource allocation.

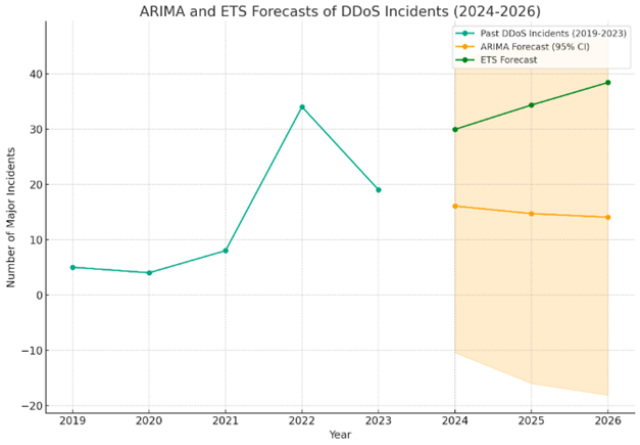

FIGURE 13. Comparing ARIMA & ETS.

F. ATTACK VECTOR DIVERSITY ANALYSIS

In our effort to further deep-dive into very granular nature of these DDoS incidents investigated, we observed indicators of DDoS Attack Vector Diversity in the some of major incidents examined to the extent of confirming the sophistication and complexities of these attacks. It is important to note a significant limitation in the granularity of available data. Despite identifying the occurrence of diverse DDoS attacks, our analysis lacked sufficient evidence to categorically distinguish the specific nature of these incidents, such as whether they were volumetric, protocol, or application layer DDoS attacks. This gap in detailed information restricts our ability to provide a more nuanced understanding of the DDoS attack methodologies employed by these threat actors. The absence of this granular data highlights a critical challenge in

cyber threat analysis: the difficulty in obtaining detailed and specific information about attack vectors, which is essential for a comprehensive understanding of the threat landscape. As a result, while our study sheds light on the variety and frequency of DDoS attacks, the intricacies regarding their exact technical nature remain less defined, indicating an opportunity for further in-depth research and data collection in the future.

V. DISCUSSION

A. FORECASTING IMPLICATIONS

Leveraging data derived from [2] major DDoS incidents reported from the past five years to forecast the next three years is of paramount importance for several reasons. Firstly, it provides us with a historical context, enabling us to understand patterns and trends in major cyberattacks, which are crucial for predicting future incidents. The past five years encompass a variety of major incidents attributed in part or in whole to DDoS attacks and responses, offering a rich dataset to analyze the evolution of attack methods, frequencies, and targets. This historical analysis aids in identifying patterns that might repeat or evolve, thereby enhancing the accuracy of future forecasts. Additionally, such a retrospective examination helps us in understanding the impact of various external factors, such as technological advancements [39], [40] and geopolitical shifts [41], [42], on the nature and scale of DDoS attacks. By incorporating these insights, forecasts for the upcoming years can be more precisely tailored to anticipate not just the frequency but also the potential severity and nature of future DDoS events.

Forecasting DDoS attack trends for a three-year period, we argue strikes a balance between relevance and accuracy. Short-term forecasts [43], [44], like a three-year window, tend to be more accurate because they are less likely to be affected by unforeseen future technological advancements, new cybersecurity measures, or unpredictable geopolitical changes that can significantly alter the cyber threat landscape. Additionally, a three-year forecast is likely to align well with typical strategic planning cycles [45], [46] in organizations, making it particularly useful for cybersecurity strategy development and resource allocation. It provides a practical horizon for organizations to prepare and implement effective defense mechanisms. In the rapidly evolving field of cybersecurity, a longer forecast period might lead to less accurate predictions [47] due to the dynamic nature of technology and cyber threats. Therefore, a three-year forecast offers a pragmatic and strategic approach to anticipating and preparing for future major DDoS challenges.

While the forecasted numbers of major incidents attributable to DDoS attacks provide valuable insights, we argue that relying solely on these predictions warrants caution. The primary intent of presenting these forecasts is not to offer precise future event counts, but rather to underscore the critical importance of cybersecurity incident response and preparedness. These calculated projections serve as a reminder of the ever-present and evolving threat of major cyber attacks, emphasizing the need for organizations and nations to bolster their cybersecurity defenses, develop robust response strategies, and maintain a state of readiness. The focus on forecasted trends aims to drive home the point that in the dynamic and unpredictable realm of cyber threats, proactive measures and readiness are key to mitigating potential risks and minimizing the impact of such incidents.

B. GEOPOLITICAL IMPLICATIONS

In highlighting our observation of the correlation between major DDoS incidents targeting national critical infrastructure and institutions, and the indication of geopolitical tensions, the following two theoretical frameworks were adopted and referenced as our guiding principle to reflect on the geopolitical aspect of the findings in this study. The combination of both frameworks offers a lens to explore the strategic dimensions of cyber warfare and aided this study by providing us with a deeper understanding of how DDoS attacks fit into the broader narrative of geopolitical tensions and state behavior in the digital age. Below is how these frameworks were juxtaposed with the correlation of these major attacks to geopolitical tension:

1) Realist Theory in International Relations: This theory argues that states are the primary actors in international relations to the extent that they act in pursuit of their own national interests, often in terms of security, economic and political power [48], [49], [50]. In the context of cyber warfare, Realist Theory was applied in this study to understand how states might engage in leveraging major DDoS attacks as a form of power projection [51] or to safeguard their own national interests. Under this framework, DDoS attacks we argue could be interpreted as strategic moves in the broader game of international power politics, where nations use cyber capabilities to assert dominance, retaliate, or influence other states. Further testing of the correlation between DDoS attacks and geopolitical tensions through the lens of Realist Theory would involve examining whether these attacks align with the national interests or strategic objectives of the states involved - this aspect would be great area for future collaboration with political scientists.
2) Cyber Deterrence Theory: Building on the principles of traditional deterrence theory [52], [53], Cyber Deterrence Theory explores how the threat of retaliation or punitive action can be used to prevent adversaries from launching cyberattacks [54], [55], [56], [57]. Reflecting through the lens of this framework, there are indicators in the sample size of major incidents that we examined, that suggest that major DDoS attacks against a nation's critical infrastructure for example can be seen as acts that test the resilience and response capabilities of the target state. This theory when further reflected upon, can help in deeper understanding whether the patterns

of DDoS attacks correlate with the perceived strengths or vulnerabilities of nations and their ability to respond to cyber threats. Further testing of this correlation would involve very granular assessment of whether the frequency and intensity of DDoS attacks are influenced by the target nation's cyber defense posture and its reputation for retaliatory capabilities in cyberspace. Further studies are encoureaged here as well.

Examining the countries and regions impacted by major DDoS attacks over recent years has significantly shaped our understanding of the interplay between cyber threats and geopolitics. The geographical distribution of these attacks often mirrors the global political landscape, reflecting how cyber warfare [58], [59] is increasingly used as a tool to exert influence, cause disruption, or signal discontent in international relations. For instance, attacks concentrated in politically sensitive or strategically important regions may suggest that state actors or politically motivated groups are using DDoS attacks as an extension of geopolitical strife. Such patterns is capable of revealing the strategic use of cyber capabilities by state and non-state actors to achieve potentially political, economic, or ideological objectives. This understanding highlights the need for cybersecurity strategies that not only address technical vulnerabilities but also consider the broader political context in which these major cybersecurity incidents occur.

To the extent of information that is available in the public domain, the correlation between major DDoS attacks and geopolitical tensions might be relatively understood through the lens of cyber warfare and international security. In an era where digital infrastructure [60] is integral to national security [61], [62] and economic stability [63], [64], major incidents that are caused by DDoS attacks represent a potent tool for major disruption. The timing, targets, and intensity of these notable attacks often correlate with escalating tensions between nations, political events, or international disputes. For example, a surge in DDoS attacks during an election period or amid diplomatic tensions may (or not) indicate attempts to influence political processes or to potentially destabilize a region. Such correlations, we argue underscore the evolving nature of conflict and security in the digital age, where cyber attacks are not just isolated incidents of technical disruption but are arguably increasingly used as strategic components in broader geopolitical conflicts. Understanding these dynamics is crucial for developing comprehensive security policies that address the complexities of modern warfare and international relations in the digital realm.

C. DISCLOSURE

In this study, the authors, while being seasoned cybersecurity experts, acknowledge their general expertise in geopolitics rather than a specialized focus. As such, this study intentionally steered away from in-depth interpretations of the geopolitical implications observed in conjunction with major DDoS incidents. This decision stems from a recognition of the complex interplay between cyber threats and international political dynamics, an area that often demands very specialized knowledge in political science. This study merely suggests a correlation between significant DDoS attacks and geopolitical conflicts, particularly noting that these attacks frequently target a country's critical infrastructure, government agencies, or public-private entities integral to national interests - only to the extent of our understanding of the findings that were observed during our analysis. Also, the authors opted not to delve deeply into the geopolitical analysis, paving the way for future research by political scientists who can more thoroughly investigate this geopolitical aspect. This approach ensures that the study remains within the bounds of the authors' expertise while highlighting a crucial area for further interdisciplinary exploration.

D. STUDY'S BROADER OBJECTIVE

The broader goal of this study, therefore, is to provide a comprehensive analysis of the trends, nature, and geographical distribution of major DDoS attacks, laying a foundation for further investigation into their geopolitical dimensions. By mapping the occurrences of these attacks against the backdrop of global political events, the study opens a window to a potential linkage that could be pivotal in understanding the strategic use of cyber threats in international relations. The authors' intention is not to present a definitive account of the geopolitical context but rather to signal its significance and the need for its exploration by experts in that field. This approach underscores the interdisciplinary nature of cybersecurity, inviting collaboration and further study from experts in related domains to build a more holistic understanding of the threats in the digital age.

VI. STUDY LIMITATIONS

Investigating only major cybersecurity incidents attributed to DDoS attacks that have been reported or announced by reputable institutions or the targets themselves presents both strengths and limitations. On one hand, focusing on major incidents ensures that the study is dealing with impactful and significant events, which can provide deep insights into the most critical threats and their consequences. This approach allows for a concentrated examination of sophisticated attacks, which are likely to have substantial implications for national security, economic stability, or public safety. It helps in understanding the tactics of high-profile attackers and in formulating effective responses to significant threats. However, this focus also poses limitations, as it potentially overlooks the broader landscape of DDoS activities, including smaller-scale but still disruptive attacks. Such a selective approach might lead to a skewed understanding of the overall threat landscape, missing out on patterns and trends evident in less significant but more frequent attacks. This limitation could impact the comprehensiveness of cybersecurity strategies and the ability to anticipate a wider range of cyber threats.

The utilization of ARIMA and ETS models in forecasting major DDoS attack trends in this study offers both strengths and limitations. On the positive side, these sophisticated statistical tools are adept at analyzing time series data, providing very valuable insights into future trends based on historical patterns. ARIMA for instance excels in capturing underlying trends and seasonality in data, while ETS is described to be particularly effective in modeling data with trends and cyclic changes. This combination can yield reliable predictions for short to medium-term forecasts, that are very crucial for strategic cybersecurity planning. However, these models also have limitations as they heavily rely on historical data and assume that past patterns will continue into the future, which may not always hold true in the rapidly evolving domain of cyber threats. Technological advancements, changes in attacker tactics, and unforeseen global events can significantly alter the threat landscape, rendering model predictions less accurate. Additionally, these models might not fully capture the complexity of factors influencing cyber threats, such as geopolitical dynamics or technological innovation, potentially oversimplifying the multifaceted nature of cybersecurity threats.

The authors' combined 40 years of working experience as cybersecurity experts with international exposure significantly strengthens this study, primarily through their deep understanding of the field and ability to interpret complex data accurately. Their extensive experience ensures a nuanced and informed analysis, drawing on a wealth of practical knowledge and understanding of global cybersecurity trends. However, this can also be a limitation, as the interpretation of the [1] and [2] reports is subject to the authors' perspectives and potential biases. While their experience provides valuable insights, it might also influence the analysis in specific ways, potentially overlooking alternative interpretations or emerging perspectives in the rapidly evolving field of cybersecurity. Their long-standing experience, though invaluable, may also inadvertently align with traditional approaches, possibly underemphasizing novel threats or innovative solutions. This duality highlights the importance of balancing experienced insights with diverse viewpoints and emerging research in the field.

VII. CONCLUSION

This study comprehensively addressed the research question, ''How have the trends, impacts, and global distribution of major DDoS attacks evolved from 2019 to 2023, and to what extent can threats like this be predicted?'' by meticulously analyzing derived data from major DDoS incidents over the five-year period. The investigation revealed an evolving pattern in DDoS attacks, both in terms of frequency and geographical distribution. Early years like 2019 and 2020 witnessed sporadic and less major cybersecurity incidents attributed to intense DDoS activities, predominantly concentrated in specific regions. As the study progressed to 2021 and beyond, there was a notable increase in both the frequency and severity of these major attacks, spreading to a more diverse set of global targets. This shift illustrates an escalation in the threat landscape, with DDoS attacks becoming more common and impactful, affecting a broader spectrum of nations and industries.

In terms of impact, this study echoed the significant disruptions caused by these major DDoS attacks, ranging from crippling essential services to causing arguably substantial economic and potential reputational damages. These incidents underscored the increasing reliance of societies on digital infrastructure and the consequent vulnerabilities. The analysis in this study provided valuable insights into the potential consequences of such attacks, emphasizing the need for robust cybersecurity measures and awareness. This study also drew attention to the correlation between major DDoS attacks and geopolitical tensions, suggesting that these cyber threats are often used as instruments in larger political and economic conflicts.

Finally, regarding the predictability of such threats, the study leveraged ARIMA and ETS forecasting models to project future trends in major DDoS attacks for the subsequent three years. These models, based on historical data, provided a quantitative foundation for anticipating future occurrences from 2024 to 2026, reflecting both the expected number of incidents and the associated uncertainties. However, it is noteworthy to reiterate that this study also acknowledged the inherent limitations of these predictive models, given the dynamic and rapidly evolving nature of cyber threats and technology. While the forecasts offered valuable foresight, this study highlighted the need for continual adaptation and vigilance in cybersecurity strategies, considering the unpredictable and sophisticated nature of future DDoS attacks.

Focusing solely on major incidents associated with DDoS attacks, while crucial, also presents a dual aspect of strength and limitation in this study. On one hand, this specialized study focus allows us for an in-depth analysis of DDoS attacks, a prevalent and disruptive form of cyber threat in this digital age. While we argue that this study enables a thorough understanding of the trends, methods, and impacts specific to these attacks, offering valuable insights for developing targeted strategies to mitigate such incidents - we also understand that this specialized focus also presents a limitation, as it excludes other significant attack techniques like exploitation of vulnerabilities [65], credential stuffing [66], malware [67], [68], and phishing [69], which are equally important in the broader landscape of cybersecurity threats. Moreover, recognizing that DDoS attacks are arguably sometimes used as a distraction tactic for more sinister activities, such as data breaches or malware deployment, further highlights the limitation of the narrowed scope of this study. It underscores the need for a comprehensive approach to cybersecurity that considers the multifaceted and interrelated nature of cyber threats. This comprehensive approach is essential for building robust and resilient cyber defenses, capable of addressing the full spectrum of potential cyber risks.

ACKNOWLEDGMENT

The primary dataset used or referenced in this study is derived from the Significant Cyber Incidents Report, that is consolidated by the Center for Strategic and International Studies (CSIS), but cross-referenced and validated with insights derived from Data Breach Investigation Reports (DBIR). Any perspective, findings, observation, interpretations, recommendation, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of either the CSIS or the DBIR. The authors would like to thank the School of Information Technology, University of Cincinnati, OH, USA, for providing them with the tools, environment, and guidance to conduct this study.

REFERENCES

[1] Verizon Business. (2023). *Verizon Data Breach Investigations Report (DBIR)*. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[2] Center for Strategic & International Studies. (2023). *Significant Cyber Incidents Since 2006*. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[3] O. I. Falowo, S. Popoola, J. Riep, V. A. Adewopo, and J. Koch, "Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents," *IEEE Access*, vol. 10, pp. 134038–134051, 2022.

[4] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–8.

[5] J. Li, M. Liu, Z. Xue, X. Fan, and X. He, "RTVD: A real-time volumetric detection scheme for DDoS in the Internet of Things," *IEEE Access*, vol. 8, pp. 36191–36201, 2020.

[6] Y. Xie and S.-Z. Yu, "Monitoring the application-layer DDoS attacks for popular websites," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 15–25, Feb. 2009.

[7] A. Praseed and P. S. Thilagam, "DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 661–685, 1st Quart., 2019.

[8] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art," 2012, *arXiv:1208.0403*.

[9] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, "Performance evaluation of Botnet DDoS attack detection using machine learning," *Evol. Intell.*, vol. 13, no. 2, pp. 283–294, Jun. 2020.

[10] D. A. Wheeler and G. N. Larsen, "Techniques for cyber attack attribution," Inst Defense Anal., Tech. Rep., Feb. 2003.

[11] M. E. Ahmed and H. Kim, "DDoS attack mitigation in Internet of Things using software defined networking," in *Proc. IEEE 3rd Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Apr. 2017, pp. 271–276.

[12] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS attack detection using deep learning and IDS," *Int. Arab J. Inf. Technol.*, vol. 17, no. 4A, pp. 655–661, Jul. 2020.

[13] M. Bartsch and S. Frey, *Cybersecurity Best Practices*. Springer, 2018.

[14] O. Szumski, "Cybersecurity best practices among Polish students," *Proc. Comput. Sci.*, vol. 126, pp. 1271–1280, Jan. 2018.

[15] D. Death, *Information Security Handbook: Develop a Threat Model and Incident Response Strategy to Build a Strong Information Security Framework*. Packt Publishing, 2017.

[16] M. N. Murthy, *Sampling Theory and Methods*, 1967.

[17] P. Minkkinen, "Practical applications of sampling theory," *Chemometric Intell. Lab. Syst.*, vol. 74, no. 1, pp. 85–94, Nov. 2004.

[18] D. A. Cook and T. J. Beckman, "Current concepts in validity and reliability for psychometric instruments: Theory and application," *Amer. J. Med.*, vol. 119, no. 2, pp. 166.e7–166.e16, Feb. 2006.

[19] V. Braun and V. Clarke, "Thematic analysis," in *APA Handbook of Research Methods in Psychology*. American Psychological Association, 2012.

[20] M. Schield, *Correlation, Determination and Causality in Introductory Statistics* (Section on Statistical Education). American Statistical Association, 1995.

[21] J. J. Lee, "Correlation and causation in the study of personality," *Eur. J. Personality*, vol. 26, no. 4, pp. 372–390, Jul. 2012.

[22] Y. Shi, "Forecasting mortality rates with the penalized exponential smoothing state space model," *J. Oper. Res. Soc.*, vol. 73, no. 5, pp. 955–968, May 2022.

[23] R. Hyndman, A. B. Koehler, J. K. Ord, and R. D. Snyder, *Forecasting With Exponential Smoothing: State Space Approach*. Springer, 2008.

[24] N. R. Pokhrel, H. Rodrigo, and C. P. Tsokos, "Cybersecurity: Time series predictive modeling of vulnerabilities of desktop operating system using linear and non-linear approach," *J. Inf. Secur.*, vol. 8, no. 4, pp. 362–382, 2017.

[25] B. Biswas and S. Patra, "Forecasting problems in cybersecurity: Applying econometric techniques to measure it risk," in *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. Boca Raton, FL, USA: CRC Press, 2018, pp. 45–93.

[26] S. Das, K. Mitra, and M. Mandal, "Sample size calculation: Basic principles," *Indian J. Anaesthesia*, vol. 60, no. 9, p. 652, 2016.

[27] F. Y. Hsieh, D. A. Bloch, and M. D. Larsen, "A simple method of sample size calculation for linear and logistic regression," *Statist. Med.*, vol. 17, no. 14, pp. 1623–1634, Jul. 1998.

[28] W. J. Potter and D. Levine-Donnerstein, "Rethinking validity and reliability in content analysis," *J. Appl. Commun. Res.*, vol. 27, no. 3, pp. 258–284, Aug. 1999.

[29] P. A. Moss, "Themes and variations in validity theory," *Educ. Meas., Issues Pract.*, vol. 14, no. 2, pp. 5–13, Jun. 1995.

[30] R. R. Brooks, L. Yu, I. Ozcelik, J. Oakley, and N. Tusing, "Distributed denial of service (DDoS): A history," *IEEE Ann. Hist. Comput.*, vol. 44, no. 2, pp. 44–54, Apr. 2022.

[31] J. C. Merlino, M. Asiri, and N. Saxena, "DDoS cyber-incident detection in smart grids," *Sustainability*, vol. 14, no. 5, p. 2730, 2022.

[32] N. V. Patil, C. R. Krishna, and K. Kumar, "Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 10, p. e6197, May 2021.

[33] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100332.

[34] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020.

[35] U. S. Onyeabor and J. O. Nehinbe, "An exhaustive study of DDOS attacks and DDOS datasets," *Int. J. Internet Technol. Secured Trans.*, vol. 10, no. 3, pp. 268–285, 2020.

[36] A. Hekmati, E. Grippo, and B. Krishnamachari, "Large-scale urban IoT activity data for DDoS attack emulation," in *Proc. 19th ACM Conf. Embedded Netw. Sensor Syst.*, 2021, pp. 560–564.

[37] O. I. Falowo, I. Okpala, E. Kojo, S. Azumah, and C. Li, "Exploration of various machine learning techniques for identifying and mitigating DDoS attacks," in *Proc. 20th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2023, pp. 1–7.

[38] G. Jayasekara, "Security operations & incident management: Case study analysis," *SSRN J.*, Aug. 2022.

[39] N. Renu, "Technological advancement in the era of COVID-19," *SAGE Open Med.*, vol. 9, Jan. 2021, Art. no. 205031212110009.

[40] A. Mounia, R. Ajhoun, and L. Ensias, "Impact of technological advancement on pedagogy," *Turkish Online J. Distance Educ.*, vol. 13, no. 1, pp. 224–237, 2012.

[41] C. Ruhl, D. Hollis, W. Hoffman, and T. Maurer, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Carnegie Endowment for International Peace, 2020.

[42] J. B. Sheldon, "Geopolitics and cyber power: Why geography still matters," *Amer. Foreign Policy Interests*, vol. 36, no. 5, pp. 286–293, Sep. 2014.

[43] P. J. Harrison and C. F. Stevens, "A Bayesian approach to short-term forecasting," *Oper. Res. Quart.*, vol. 22, no. 4, p. 341, Dec. 1971.

[44] E. I. Vlahogianni, J. C. Golias, and M. G. Karlaftis, "Short-term traffic forecasting: Overview of objectives and methods," *Transp. Rev.*, vol. 24, no. 5, pp. 533–557, 2004.

[45] J. M. Bryson, "Strategic planning and the strategy change cycle," in *The Jossey–Bass Handbook of Nonprofit Leadership and Management*, 2016, pp. 240–273.

[46] R. Dye and O. Sibony, "How to improve strategic planning," *McKinsey Quart.*, vol. 3, p. 40, Aug. 2007.

[47] S. K. Smith and T. Sincich, "Evaluating the forecast accuracy and bias of alternative population projections for states," *Int. J. Forecasting*, vol. 8, no. 3, pp. 495–508, Nov. 1992.
[48] W. J. Korab-Karpowicz, "Political realism in international relations," Tech. Rep., 2010.
[49] C. G. Thies, "Progress, history and identity in international relations theory: The case of the idealist-realist debate," *Eur. J. Int. Relations*, vol. 8, no. 2, pp. 147–185, Jun. 2002.
[50] S. Guzzini, "The enduring dilemmas of realism in international relations," *Eur. J. Int. Relations*, vol. 10, no. 4, pp. 533–568, Dec. 2004.
[51] P. Harris and P. Trubowitz, "The politics of power projection: The pivot to Asia, its failure, and the future of American primacy," *Chin. J. Int. Politics*, vol. 14, no. 2, pp. 187–217, Jun. 2021.
[52] R. Jervis, "Deterrence theory revisited," *World Politics*, vol. 31, no. 2, pp. 289–324, Jan. 1979.
[53] T. C. Pratt, F. T. Cullen, K. R. Blevins, L. E. Daigle, and T. D. Madensen, "The empirical status of deterrence theory: A meta-analysis," in *Taking Stock*. Evanston, IL, USA: Routledge, 2017, pp. 367–395.
[54] A. S. Wilner, "U.S. cyber deterrence: Practice guiding theory," *J. Strategic Stud.*, vol. 43, no. 2, pp. 245–280, Feb. 2020.
[55] W. Goodman, "Cyber deterrence: Tougher in theory than in practice?" *Strategic Stud. Quart.*, vol. 4, no. 3, pp. 102–135, 2010.
[56] A. F. Brantly, "The cyber deterrence problem," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, May 2018, pp. 31–54.
[57] S. Soesanto and M. Smeets, "Cyber deterrence: The past, present, and future," in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence 21st Century-Insights From Theory Practice*, 2020, pp. 385–400.
[58] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, vol. 49, pp. 70–94, Mar. 2015.
[59] G. R. Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. London, U.K.: Oxford Univ. Press, 2017.
[60] M. Dawson, R. Bacius, L. B. Gouveia, and A. Vassilakos, "Understanding the challenge of cybersecurity in critical infrastructure sectors," *Land Forces Acad. Rev.*, vol. 26, no. 1, pp. 69–75, Mar. 2021.
[61] M. P. Leffler, "National security," *J. Amer. Hist.*, vol. 77, no. 1, pp. 143–152, 1990.
[62] M. A. Levy, "Is the environment a national security issue?" *Int. Secur.*, vol. 20, no. 2, pp. 35–62, 1995.
[63] O. V. Pavlov, M. Radzicki, and K. Saeed, "Stability in a superpower-dominated global economic system," *J. Econ. Issues*, vol. 39, no. 2, pp. 491–500, Jun. 2005.
[64] M. Kahler, "Economic crisis and global governance: The stability of a globalized world," *Proc. Social Behav. Sci.*, vol. 77, pp. 55–64, Apr. 2013.
[65] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, K. S. Ehlert, and D. Sisalem, "Survey of security vulnerabilities in session initiation protocol," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 3, pp. 68–81, 3rd Quart., 2006.
[66] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh, and E. Bursztein, "Protecting accounts from credential stuffing with password breach alerting," in *Proc. 28th USENIX Secur. Symp.*, Aug. 2019, pp. 1556–1571.
[67] A. Ali, "Ransomware: A research and a personal case study of dealing with this nasty malware," *Issues Informing Sci. Inf. Technol.*, vol. 14, pp. 87–99, Apr. 2017.
[68] R. Brewer, "Ransomware attacks: Detection, prevention and cure," *Netw. Secur.*, vol. 2016, no. 9, pp. 5–9, 2016.
[69] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers Comput. Sci.*, vol. 3, Mar. 2021, Art. no. 563060.

OLUFUNSHO I. FALOWO (Student Member, IEEE) received the B.A. degree in philosophy from the University of Lagos, Nigeria, in 2004, and the M.B.A. degree from the Isenberg School of Management, University of Massachusetts, in 2021. He is currently pursuing the Ph.D. degree in information technology with the School of Information Technology, University of Cincinnati, OH, USA. He has been a Certified Information Systems Security Professional, since 2017; a Certified Information Security Manager, since 2020; a Certified Computer Hacking Forensic Investigator, since 2011; and a Certified Security Analyst, since 2010. In 2021, he completed an executive education in design thinking: a toolkit for breakthrough innovation from the Kellogg School of Management, Northwestern University. In 2022, he also completed an executive education in cybersecurity: managing risks in the information age from Harvard University. He also completed an executive education in behavioral economics from the University of Chicago Booth School of Business, in 2022. He also completed an executive education in negotiation strategies from the Yale School of Management, in 2022. He also completed an executive education in building resilience and agility from London Business School, in 2022. He is a certified ISO/IEC 27001:2005 Lead Implementer. His research interests include cloud security, security information and event management, security incident detection and response, ethical computer hacking, and digital forensic investigation among others. He is a member of the International Information System Security Certification Consortium and the Information Systems Audit and Control Association.

JACQUES BOU ABDO received the Diplôme d'Ingènieur degree in electrical and electronics engineering from Lebanese University, Roumieh, Lebanon, in 2009, the B.B.A. degree in management from Lebanese University, Beirut, Lebanon, in 2010, the M.E. degree in telecommunication networks from the Saint Joseph University of Beirut, Lebanon, in 2011, the first Ph.D. degree in computer science (cybersecurity) from Sorbonne University, Paris, France, in 2014, and the second Ph.D. degree in management sciences (network economics, competition, and complexity economics) from Paris-Saclay University, Paris, in 2021. He is currently an Assistant Professor with the School of Information Technology, University of Cincinnati. He is an interdisciplinary researcher with expertise in complex systems, cybersecurity, cyber warfare, computational economics, and network economics. He is interested in the universality of laws governing networks and systems. His research has multiple applications, such as cyber and strategic deterrence, flow of information and disinformation in irregular warfare, flow of cyberattacks and network resiliency in cyber warfare, flow of infectious diseases in biological warfare, and resilience of supply chains.