I.J. Wireless and Microwave Technologies, **2025, 5, 21-33**
Published Online on October 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2025.05.02

Integration of Cyber Threat Hunting and Socio-Political Risk Assessment for a Hybrid Predictive Model for Enhanced Global Security

Ananya Das*
School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal, Madhya Pradesh 466114, India
E-mail: ananya.d278@gmail.com
ORCID iD: https://orcid.org/0009-0004-7300-3189
*Corresponding Author

Azath H.
School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal, Madhya Pradesh 466114, India
E-mail: writetoazath@yahoo.com
ORCID iD: https://orcid.org/0000-0002-7734-7745

Subhash Chandra Patel
School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal, Madhya Pradesh 466114, India
E-mail: subhash.patel@vitbhopal.ac.in
ORCID iD: https://orcid.org/0000-0002-1136-3638

Pushpinder Singh Patheja
School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal, Madhya Pradesh 466114, India
E-mail: pushpinder.singh@vitbhopal.ac.in
ORCID iD: https://orcid.org/0000-0003-4252-7735

Received: 24 December, 2024; Revised: 20 June, 2025; Accepted: 16 July, 2025; Published: 08 October, 2025

Abstract: The new and emerging challenges posed by the convergence of cyber threats and socio-political tensions have risen as one of the core formidable threats to the present global security landscape. This paper proposes a hybrid predictive model intended to act against these real-world multidimensional attack vectors. The model integrates cyber threat hunting techniques with socio-political risk assessment methodologies to comprehensively forecast consequent cybersecurity threats to social unrest scenarios. Cyber threat data is collected from sources such as the Offensive Defensive-Intrusion Detection System (OD-IDS2022) and the Aegean Wi-Fi Intrusion Dataset (AWID3), and social terror attack information is gathered from the Global Database of Events, Language, and Tone (GDLET) Project and Armed Conflict Location & Event Data (ACLED) to comprise the bidirectional dataset for the model that contains views from both cyber and socio-political risk landscapes. The model adopts a holistic, robust predictive capability through k-fold cross-validation and feature importance evaluation implementation techniques. This multidisciplinary approach offers a synoptic understanding of emerging and future security threats and enables the execution of proactive measures to secure national and transnational borders.

Index Terms: Cyber Threat Hunting, Socio-Political Risk Assessment, Machine Learning, Cybersecurity, Global Security, AI in Counterterrorism, Socio-Cyber Threat Integration

1. Introduction

The rapid adoption and rise of pervasive computation and digitalization in all industry sectors, and cross-border collaborative services, have paved the way for sophisticated real-world attack vectors with multiple exploit surfaces.

The interconnection and consequential relationship between cyberattacks and social unrest represent a critical concern in the digital era, where technological vulnerabilities increasingly intensify societal tensions and political instability.

Present-day unrest scenarios created by a terror attack on a certain region or country stage a completely vulnerable cyber-state for the government, organizations, and society's citizens. Threat actors take advantage of this biased focus and attention and exploit the vulnerability to launch major cyberattacks, often on critical infrastructure, supply chains, healthcare, and other major industries.

Furthermore, cyberattacks can even lead to social chaos scenarios due to the loss of confidence in government institutions. Through the spread of disinformation or the distortion of facts and disruption of economic activities, threat actors show how malicious cyber operations take advantage of the already existing social fractures that result in panic and loss of confidence in governance systems throughout society. For example, the 2021 Colonial Pipeline ransomware attack and the 2007 Estonia cyberattack come into the list. [1,2,3]

State-sponsored proliferation in the use of cyberwar and the progression and enhanced cybercrime abilities make the motivations either purely financial or geopolitical, further complicating this issue because governments and organizations develop different methods to handle the dynamic nature of cyber threats.[4] Added to this, the reality of misinformation and disinformation destabilizes the cohesion of societal bonds as it radicalizes a vulnerable population. [5,6]

The effects of cyberattacks extend beyond purely technical damage as they aid an atmosphere of violence and conflict. A few of the exemplary events linked to this are the Arab Spring and the 2016 presidential election in the United States, in which cyber operations were directly connected with public opinion and the electoral outcome. Understanding the background behavior as well as the implications adds to the creation of mitigation strategies and further builds resilience against future cyberattacks.[7]

With the intent of strengthening global security vis-à-vis the growth of digital and geopolitical threats, organizations are confronted with an interrelated challenge of how to build their response towards sophisticated cyberattacks and simultaneously mitigate the effects of socio-political changes. Cyber threats comprise the risk of data breaches and ransomware attacks. Under socio-political risks, it comprises governmental instability, social unrest, and changes in regulations that may badly affect the organizational outcome in global scenarios. [8,9,10]

High-profile cyberattacks, such as one against the U.S. Department of Energy in 2024, place a high demand for holistic assessments that would combine cybersecurity dynamics and political factors. [11,12] Vulnerabilities of critical infrastructure, together with a lack of traditionally applicable risk management, are the focal points of attack against this type of information structure that do not take into consideration the interplay between cyber threats and socio-political factors. This expanding requirement calls for an overhaul in safety measures to ensure long-term resilience and protection from the diverse nature of threats based on an integrated understanding of both domains. The hybrid predictive model suggested in the paper combines methodologies associated with cyber threat hunting with socio-political risk assessment. It does lend several advantages, such as improved detection and informed decision-making by illustrating increased cooperation from stakeholders. [13]

This will help organizations identify and better respond to the cyber threats affected by the geopolitical event, as well as enforce their cybersecurity posture against a highly complex risk environment. Integration addresses current vulnerabilities but also future ones in the ever-changing landscape of the global scenario. There are obvious challenges in putting together such an all-inclusive framework. Organizations must contend with issues of data management, changes in threat vectors, and constant stakeholder engagement to achieve the benefits of integrated approaches to security. This integration of cyber threat hunting and socio-political risk assessment, therefore, marks the critical frontier for the enhancement of global security in an era that stands unique due to turbulence involving the digital and geopolitical spheres. This, therefore, integrates cyber threat hunting with socio-political risk assessment and proves to be a critical advancement within the enhancement of global security frameworks. It would be a worthwhile strategy to organize both and put up effective mitigation concerning ever-evolving cyber threats, coupled with socio-political dynamics that influence the threats. [14]

The graph in Figure 1 illustrates the flux of intensity of Google Trends related to three significant crises: Hurricane Matthew, the Boston Bombing, and the Paris Attack. Each incident event has shown an immense increase in search activities on the date when the crisis occurred, peaking afterwards (Day 1), then gradually decreasing as days went by.

This pattern, as seen, is an indicator of greater public interest right after a crisis, because they want updates, safety information, and more details on what happened. It graphically underlines a general trend in response to a situation of social unrest and disaster: first, information-seeking increases, then it tapers off, reflecting a sharp but short-lived crisis-related information need.

Cyber threat hunting is proactive searching for Indicators of compromise (IOCs) within networks to find possible breaches before they expand into major incidents. The earlier methods were just about finding known threats using IOCs, but the current methodology is to understand the dynamic and evolving nature of an adaptive threat landscape that will involve new and sophisticated forms of attacks. This shift recognizes the fact that cybercriminals and nation-state actors are increasingly exploiting geopolitical tensions to conduct cyber operations that can disrupt critical services and sway public opinion.

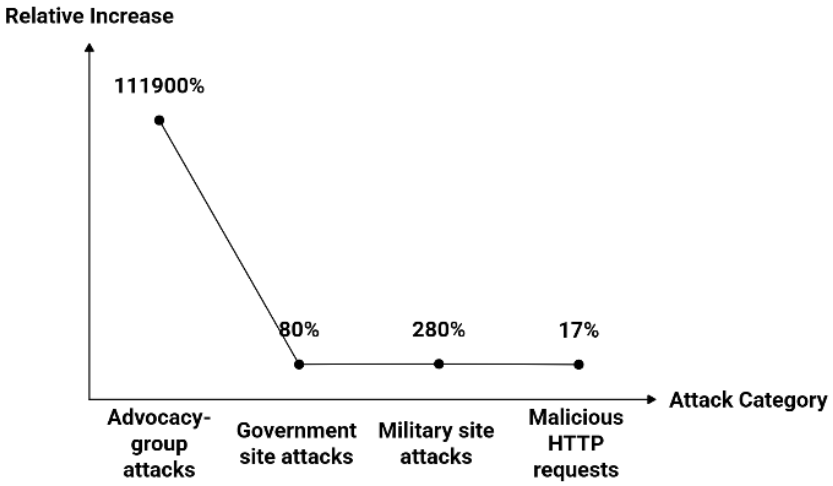

Fig. 1. Spike in Cyberattacks During Period of Social Unrest (George Floyd Protests, 2020) [15]

Socio-political risk assessment measures the influence of political, social, and economic change on the organization and its operations. Political instability, regulatory changes, and public sentiment also pose threats to organizations. Therefore, the socio-political context can help organizations be proactive about what might happen when certain geopolitical events or shifts take place. For instance, tensions among states increase the possibility of cyber threats because adversary states threaten critical infrastructure or seek to influence public opinion through cyber operations.

2. Related Work

In recent years, many studies have been conducted to develop predictive models to achieve global security, particularly by considering terrorist activities and cyber threats. These studies establish the need to incorporate diverse factors, including socio-political risks, to make predictive models more effective and reliable in preventing security risks.

A. Predicting Terrorism Activity

Research into the prediction of terrorist activities has reached an evolutionary level where researchers aim to incorporate multidimensional data into the analysis. In a research paper on the southern provinces of Thailand in the prediction of terrorist activity, Ganokratanaa and Ketcham (2023) [16] used a Long Short-Term Memory deep learning model in the analysis of historical incident data, integrating socio-political, economic, and geographical factors. Their outcome revealed that it had higher predictive prowess when there were more contextual elements regarding possible hotspots and periods at risk from terrorist attacks. This study thus underlines the fact that socio-political aspects should be included in prediction models since they provide critical input on areas that may give rise to and recur terrorist acts.

B. Predicting Cyberattacks

Prediction of cyberattacks also drew some attention from scholars. Vatis advanced a framework to address challenges of cybersecurity in the aftermath of the U.S. War on Terrorism, too, based on historical cyber incidents and case studies suggesting possible sources, types, and targets of threats (Vatis 2001). [17] Vatis, through research, developed a need to raise awareness of the increased risks of cyberattacks during periods of military conflict by bringing out a cross-sectoral approach to enhance cybersecurity protocols and international cooperation. This study bases its foundation on understanding the escalation of cyber threats that could be experienced during geopolitical conflicts and suggests a hybrid methodology that integrates various sectors for better combating cyber risks. More recently, Javed, Lakoju, Burnap, and Rana (2020) [18] have proposed a real-time cyberattack prediction framework specifically for Industry 4.0 settings. Using actual network logs along with applications of techniques such as exponentially weighted moving averages, Fibonacci retracement, and linear regression, their framework predicted the intensity as well as the timing of cyberattacks, indicating a lead time of nearly 1.75 hours. It brings forth the importance of real-time predictive analysis in protecting critical infrastructure and adds to it the urgency of timely preventive measures for network administrators operating during periods of increased threat.

C. AI-Powered Counterterrorism

Artificial intelligence-driven counterterrorism is also a nascent approach in predictive security modelling. The authors Khan, Li, Nawaz Khan, Waqas Khan, Hadjouni, and Elmannai published their work in 2023 [19] detailing a predictive framework focused exclusively on the SAARC region, which makes casualty and weapons of attack forecasts associated with terrorist attacks. Algorithms are Logistic Regression, Decision Trees, and Random Forests. The

Synthetic Minority Oversampling Technique (SMOTE) was applied to the dataset to balance classes. This classification utilized a Particle Swarm Optimization-based classifier and gave an excellent performance in terms of casualty and type of weapon prediction. In essence, the research illustrates how more precision and accuracy can be obtained if machine learning is applied to sound predictions, one of the fundamental requirements of effective counterterrorism.

D. Cyber Supply Chain Security

Models' predictability has been used in the improvement of the security of CSCs. For example, Yeboah-Ofori, Islam, Lee, Shamszaman, Muhammad, Altaf, and Al-Rakhami (2021) [20] designed a predictive framework that would analyze data from the logs of firewalls and antimalware to secure the data of CSCs. It used the malware dataset that came from Microsoft to identify existing threats in addition to emerging ones in CSCs. The study shows that predictive analysis is imperative to the preemption of potential breaches and mitigation of risk within CSCs that allow for a more secure digital environment. This research, hence, illustrates the need for proactive threat forecasting in supply chains where vulnerabilities can have vast impacts on security.

E. Implications of Socio-Political Risks in Hybrid Models

Overall, the body of literature shows a rapidly increasing interest in integrating socio-political risk factors in hybrid predictive models. These models achieve this by combining cyber threat analysis with socio-political indicators. The studies conclude that policymakers and security officials can benefit from the availability of historical data and even more advanced analytical techniques, such as deep learning and machine learning, to detect these emerging security threats in time. This will be promising in robust frameworks capable of enhancing both national and international security by combining cyber threat-hunting methodologies with socio-political risk assessments.

Table 1. Literature Review

Year	Author	Country	Objective	Contribution	Data	Methodology	Conclusion/ Result
2023	Thittaporn Ganokratanaa, Mahasak Ketcham	Thailand	This paper aims to develop a model to predict terrorist activities in the southern province of Thailand using deep learning algorithms. Through these advanced analytical methods, the research papers seek to enhance the ability to forecast and prevent terrorist activities.	In the field of terrorism studies, this paper achieves a novel approach to predict terrorist activities using deep learning algorithms. This model with the integration of historical data of prior incidents, with various socio-political, economic, and geographical factors, offers actionable recommendations for policy advisors and security professionals to act upon.	The research approach utilizes records of past terrorist attacks in the southern province of Thailand from the period of 2004 to 2019. This secondary data including various socio-political, economic, and geographical factors was sourced from governmental and non-governmental organizations.	The research methodology utilized in this paper to forecast terrorist activities includes deep-learning techniques like Long Short-Term Memory (LSTM). The LTSM through a wide range of features analyses past incident data, socio-political and economic indicators, and geographical information enhances the accuracy of the prediction model.	The research concludes that the proposed model significantly improves the accuracy of the deep learning predictive analysis for terrorist activities compared to traditional methods. The model was demonstrated to be effective in recognizing potential hotspots and periods for terrorist attacks, providing valuable operational insights for proactive security measures.
2001	Michael A. Vatis	United States	The paper aims to provide a predictive analysis of potential cyber-attacks on the U.S. and the allied actions during the War on Terrorism to make policy advisors and security professionals aware and respond accordingly.	The paper offers a detailed and analytical predictive framework to forecast cyber threats and their details including types, sources, and targets of the potential attacks while highlighting the need for improved cybersecurity measures integrated with military activities.	The paper leverages secondary data from historical cyber incidents, case studies on cyberattacks on critical infrastructure, data from security organizations, and similar research.	The research approach involved the analysis of case studies of past attacks integrated with predictive modelling techniques and expert opinions to anticipate and refine potential cyber threat predictions.	The study resulted in the knowledge that the likelihood of cyberattacks increases significantly during times of military and armed conflict thus highlighting the need for a hybrid cross-sector proactive measure in enhancing security on a global scale. Through improved cybersecurity protocols, regulations, and international cooperation between law enforcement, government, and private sectors, these defensive capabilities can address the rising threat and mitigate the risk.

2023	Fahad Ali Khan, Gang Li, Anam Nawaz Khan, Qazi Waqas Khan, Myriam Hadjouni, and Hela Elmannai	People's Republic of China, Republic of Korea, Saudi Arabia	The paper aims to develop an AI-driven counterterrorism predictive analysis framework that can predict the number of casualties in a terrorist attack and also classify different weapons used in the attack using advanced machine learning models.	The research highlighted the ability, accuracy, and scalability of the machine learning models and classifiers for casualty prediction and weapon classification respectively.	The paper utilizes the primary dataset from the Global Terrorism Database with a core focus on the SAARC countries. The data was pre-processed and class imbalances were handled using techniques like the Synthetic Minority Oversampling Technique (SMOTE) which was then fed to the machine learning models to train them.	The paper utilized advanced machine learning algorithms including Logistic Regression, Decision Trees, Gaussian Bayesian Networks, AdaBoost, and Random Forests. These algorithms through data resampling, standardization, feature selection, and the development of a weighted voting ensemble model optimized the Particle Swarm Optimization (PSO) algorithm which increases the accuracy and robustness of the predictive model.	The proposed model in the paper concluded to be highly accurate and effective in forecasting terrorist attacks with the XGB model performing consistently in casualty prediction and the PSO-based classifier which was able to achieve 95% accuracy in weapon classification.
2021	Abel Yeboah-Ofori, Shareeful Islam, Sin Wee Lee, Zia Ush Shamszaman, Khan Muhammad, Meteb Altaf, and Mabrook S. Al-Rakhami	United Kingdom, South Korea, Saudi Arabia	The paper aims to enhance the security of Cyber Supply Chains (CSCs) with the aid of predictive analysis that can anticipate known and unknown cyber threats through machine learning models, thereby improving the resilience of the CSCs.	In the field of cybersecurity, this paper has provided a comprehensive framework for securing CSCs through predictive analysis. It emphasizes the importance of proactive threat forecasting in identifying potential security breaches and mitigating risks.	The research sourced Microsoft's malware dataset with around 40,000 entries and 64 parameters. This detailed data represented malware attacks identified on various endpoint nodes, including machine identities, timestamps, organizational identifiers, and default browser identifiers.	The research methods around data collection from various sources like firewalls, IDS/IPS, and antimalware logs which are then applied to machine learning algorithms after handling missing values and inconsistencies to train on this data and predict the known and unknown cyberthreats.	This study highlights the effectiveness and efficiency of predictive analysis in enhancing CSC security by anticipating potential cyberattacks.
2020	Amir Javed, Mike Lakoju, Pete Burnap, and Omer Rana	United Kingdom	The paper aims to develop a framework that forecasts cyberattacks in real-time on networked computing infrastructures focusing on Industry 4.0 environments. This will help security personnel enable and respond with defensive action in due time.	The paper contributes a novel, developed framework that predicts the intensity and timing of cyberattacks through continuous monitoring, exponential weighted moving averages, Fibonacci retracement, linear regression, and machine learning.	The research leverages real-world network logs and activities for the analysis which is constantly monitored from networked devices through various periods.	The research methodology includes exponentially weighted moving averages for trend identification, Fibonacci retracement for threat intensity estimates, and linear regression along with machine learning algorithms to predict the lead time of the cyberattack.	The proposed framework concludes to be successful in forecasting cyberattack intensity and timing providing an average lead time of about 1.75 hours which enables network administrators to take pre-emptive actions to mitigate potential attacks and thereby secure the networked infrastructure.

F. Synthesis and Identified Gaps

Constant effort and progress have been made in creating predictive models for terrorism and cyberattacks, such as deep learning for terrorist hotspot detection (Ganokratanaa & Ketcham, 2023) and hybrid methods for real-time cyberattack alerts (Javed et al., 2020); most are confined to their own domains. There have been limited attempts that combine socio-political and cyber threat factors into a composite predictive framework, making these efforts less appropriate for the current connected threat environment.

Regardless of encouraging outcomes of AI-based models for casualty prediction (Khan et al., 2023) and cyber supply chain analytics (Yeboah-Ofori et al., 2021), the systems in place lose their immediacy of speeding up when they need to in a given geopolitical situation. This emphasizes determinative gaps, namely the lack of hybrid socio-political cyber models, the limitation of cross-domain prediction, and the lack of response to transnational threats. This motivation has been driving our work toward the development of a new hybrid approach that is intended to address these shortcomings.

3. Methodology

A. Proposed SCRIP-M Framework

With the purpose of addressing the increasing cyber and socio-political risk using a unified approach, this paper proposes the Socio-Cyber Risk Integration and Prediction Model (SCRIP-M), which is a hybrid predictive framework that combines cyber threat intelligence and socio-political risk assessment. The SCRIP-M, through a multi-layered integrated system built upon traditional siloed spheres, functions to bridge cyber threat hunting methodologies with socio-political risk assessment, aiming to improve threat detection, situational awareness, and response precision. The SCRIP-M framework consists of five major stages:

- Data Acquisition Layer: SCRIP-M uses cyber structured data extractable from intrusion detection system logs, for example OD-IDS12022 and AWID3, as well as structured and unstructured socio-political content extractable from works like GDELT, ACLED, and social media platforms. Preprocessing is specific to each data stream, where cyber data undergoes class balancing (e.g., SMOTE), timestamp normalization, and feature extraction, whereas sociopolitical data undergoes NLP filtering, sentiment tagging, and temporal-spatial event mapping.
- Threat Signal Mapping Layer: This layer maps socio-political unrest signals to cyber anomaly indicators temporal and regional alignment. For instance, high-conflict areas are correlated with local temporal cyberattack activity to discover causality or triggering behavior.
- Feature Fusion Engine: A Late fusion strategy is used, where we train different machine learning models for the cyber and socio-political dataset. Their outputs are aggregated by a meta-learning classifier (e.g., gradient boosting) to infer high-level cross-domain threat patterns.
- Risk Prediction Layer: The last module calculates the probabilities of risks (e.g., high, medium, low) for security incidents. Predictions look at issues like when the next cyberattack will occur in a politically unstable region, or when there will be more cyber-enabled influence operations in protest movements.
- Feedback and Adaptive Learning Loop: Feedback and adaptation learning are key aspects of learning-based systems that ensures the consistency of the system with the real-world outcome and errors in prediction example model. and is key aspect to ensure the system is still relevant. It consumes updated OSINT feeds along with regular incident read reviews to iteratively improve.

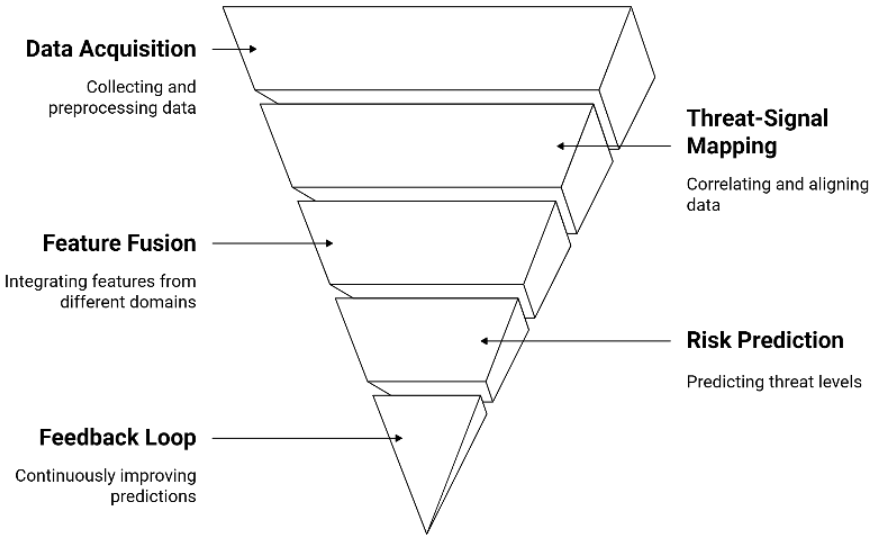

Fig. 2. SCRIP-M Framework for Hybrid Threat Prediction

B. Data Collection

Data used in implementing the proposed concept of this paper primarily encompasses two focused domains: cyber threats and socio-political unrest.

To collect data for the cyber threat module, data is gathered from real-time threat monitoring systems, such as intrusion detection systems (IDS), threat intelligence channels, and network logs. Insights into attack types such as phishing, ransomware attacks, and Denial-of-Service (DoS) attacks are compiled from the OD-IDS2022[21] and AWID3[22] datasets, which serve as a valuable basis for tracking historical and current cyber threat trends across sectors, from private organizations to the government sector, and critical infrastructure. Before model training, data preprocessing techniques include class balancing using SMOTE, timestamp normalization, and filtering of noise from

benign traffic to enhance signal quality.

For the socio-political unrest module, data is collected from different structured as well as unstructured sources. Crucial real-time data regarding unrest is rapidly disseminated through user-generated content, including posts, tweets, hashtags, and location tags. Such important information is yielded from social media platforms, such as X (formerly Twitter) and Facebook. Political instability datasets, like the Global Dataset of Events, Language, and Tone (GDELT)[23] and the Armed Conflict Location & Event Data Project (ACLED)[24], also provide structured information about protests, budding revolutions, political crises, and other forms of lawful disruptions. Through these datasets, the concept of enhanced global security is enabled with a broader understanding of the geopolitical situations of different regions that are affected by unrest and their correlation with cyber threats. Text data is processed using named entity recognition (NER) and sentiment analysis, while events are geotagged and temporarily aligned with cyber indicators. Entries with low confidence are removed.

Implementation of the hybrid model to effectively predict security threats, a mini dataset was formulated combining incidents where cyberattacks were launched over a country or region facing social or political disturbances. This dataset consists of information such as the name of the country/region, time period, intensity of the socio-political unrest, number of cyberattacks perpetrated, types of cyberattacks, attack severity, and their target victim. The final integration process includes handling null values and standardizing categorical and numerical features to ensure compatibility across the unified dataset. Merging the socio-political unrest and cyberattack parameters, this dataset provides a core for the implementation of the hybrid predictive analysis.

Algorithm

Inputs:

- Cyber Threat Data: $data_{cyber} = (X_1, X_2, \dots, X_m)$
- Socio-Political Data: $data_{socio} = (Y_1, Y_2, \dots, Y_n)$

Step 1: Data Acquisition and Preprocessing

Load Raw Data:

$$data_{cyber} \leftarrow LoadCyberData() \quad (1.1)$$

$$data_{socio} \leftarrow LoadSocioPoliticalData() \quad (1.2)$$

Clean and Preprocess:

$$data_{cyber} \leftarrow CleanAndPreprocess(data_{cyber}) \quad (1.3)$$

$$data_{socio} \leftarrow TextProcessingAndSentimentAnalysis(data_{socio}) \quad (1.4)$$

Feature and Label Extraction:

$$X_{cyber}, Y_{cyber} \leftarrow FeatureExtraction(data_{cyber}) \quad (1.5)$$

$$X_{socio}, Y_{socio} \leftarrow FeatureExtraction(data_{socio}) \quad (1.6)$$

Standardize features separately:

$$Scaled_{cyber} \leftarrow DataStandardization(X_{cyber}) \quad (1.7)$$

$$Scaled_{socio} \leftarrow DataStandardization(X_{socio}) \quad (1.8)$$

Combine standardized datasets:

$$X \leftarrow Concatenate(Scaled_{cyber}, Scaled_{socio}) \quad (1.9)$$

$$y \leftarrow Concatenate(Y_{cyber}, Y_{socio}) \quad (1.10)$$

Step 2: Encode Categorical Features

For each categorical feature column $c \in X$:

$$X[c] \leftarrow LabelEncoder(X[c]) \quad (2)$$

Step 3: Initialize Cross-Validation and Model

$$Initialize\ StratifiedKFold(k = 5, shuffle = True, random\_state = 42) \quad (3)$$

$$M \leftarrow RandomForestClassifier(random\_state = 42, class\_weight = 'balanced') \quad (4)$$

Step 4: Cross-Validated Predictions

FOR $each\ fold\ (train_{index}, test_{index}) \in StratifiedKFold.split(X, y)$:

$$M.fit(X[train_{index}], y[train_{index}]) \quad (5)$$

$$y_{proba}[test_{index}] \leftarrow M.predict_{proba}(X[test_{index}]) \quad (6)$$

$$y_{pred}[test_{index}] \leftarrow M.predict(X[test_{index}]) \quad (7)$$

END FOR

Step 5: Apply Threshold for Binary Classification

***If*:**

$$|unique(y)| = 2 \quad (8)$$

then, for all $i \in [1, N]$**:**

$$y_{pred_{thres}}[i] = \begin{cases} 1, & if\ y_{proba}[i, 1] \geq 0.6 \\ 0, & otherwise \end{cases} \quad (9)$$

***else*:**

$$y_{pred_{thres}} = y_{pred} \quad (10)$$

Step 6: Model Training on Individual Domains

Using (1.9) and (1.10):

$$M_{cyber} = Train(Scaled_{cyber}, y_{cyber}) \quad (11.1)$$

$$M_{socio} = Train(Scaled_{socio}, y_{socio}) \quad (11.2)$$

Step 7: Domain-Specific Predictions

$$P_{cyber} = M_{cyber}(Scaled_{cyber}) \quad (12.1)$$

$$P_{socio} = M_{socio}(Scaled_{socio}) \quad (12.2)$$

Each $P \in \mathbb{R}^k$, where k is the number of threat classes

Step 8: Fusion and Meta-Learner Training

$$Z = Concat(P_{cyber}, P_{socio}) \in \mathbb{R}^k \quad (13)$$

$$M_{fusion} = Train(Z, y)$$

Where, Z is the predicted probabilities and M_{fusion} is a meta classifier

Step 9: Threat Prediction

For a new input:

- Get $P_{cyber,new}, P_{socio,new}$
- Form $Z_{new} = Concat(P_{cyber,new}, P_{socio,new})$

Then:

$$\hat{y}_{threat} = M_{fusion}(Z_{new}) \quad (14)$$

Step 10: Adaptive Learning Loop

$$\theta \leftarrow \theta - \eta \nabla_\theta \mathcal{L}(\hat{y}_{threat}, y_{true}) \quad (15)$$

Where,

- $\mathcal{L}$ is the loss function
- θ represents model parameters
- η is the learning rate

C. Hybrid Model Evaluation

To effectively assess the hybrid model performance, the integrated dataset with data from the two modules of cyber threat hunting and socio-political risk assessment is divided into training and test sets using an 80-20 ratio, which is then tested for accuracy, precision, recall, and F1-score. Techniques like k-fold cross-validation are leveraged to cross-verify the model's ability to avoid overfitting. The model is ensured to show capabilities of generalization well across unseen data. The primary algorithm utilized for the predictive work was a Random Forest Classifier with 100 estimators and the splitting criterion set to Gini impurity. Within the framework of feature extraction, temporal patterns such as spikes in activity for a given day of the week, geopolitical entity recognition such as actor-country-target, as well as event coding based on frequency from GDELT and OD-IDS2022 were integrated. The features were adjusted using MinMax normalization. The most relevant features were identified using RFE. The final model was a boosted tree with a depth of 10, and was validated with 10-fold cross-validation to confirm reliability.

The performance of the classification algorithm is evaluated with a confusion matrix to identify periods prone to social-political unrest and cyberattacks. Additionally, feature importance plots raise insights into factors that are mostly influential in predicting security threats.

4. Results and Discussions

Data collected to implement the effective performance of the hybrid model is visualized to observe the patterns and relationships between socio-political unrest. Graphs and heatmaps are referenced to illustrate and understand how, during the state of unrest in a country/region, the cyberactivity of internet users worldwide faces an increased surge. Such visualizations are generated using Python libraries including matplotlib, seaborn, and plotly.

The types of cyberattacks during unrest periods, segmented by the intensity and severity of the attack, are represented using bar charts.

The bar chart in Fig. 2 shows the distribution of the types of cyberattacks classified by severity levels of “High” and “Medium”. Patterns reveal DDoS and Phishing attacks exhibit the highest frequency with both high and medium-severity incidents.

Through the data visualization, observations of distinct spikes and cyberattack trends and activities during periods of unrest are made that validate the hypothesis that socio-political instabilities often act as a precursor or a catalyst for concurrent cyberattacks aimed at government, critical infrastructure, or the civilians of the nation.

In Fig. 3, the performance of the predictive model is illustrated through the counts of true positives, true negatives, false positives, and false negatives for a classification task.

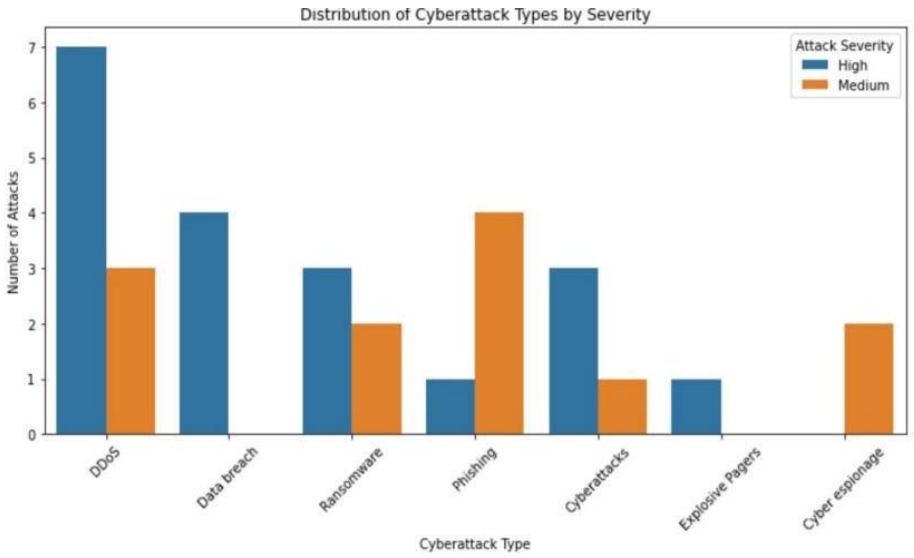

Fig. 3. Distribution of Various Types of Cyberattacks Occurred during a Social Unrest Period

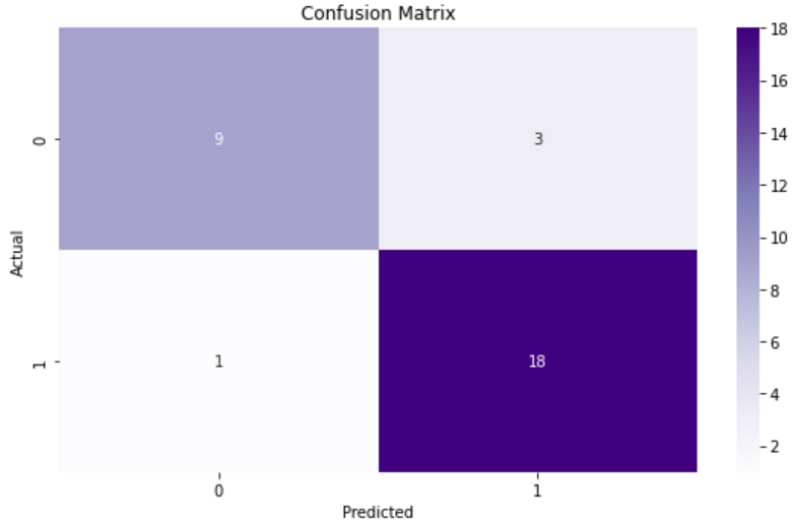

Fig. 4. Confusion Matrix of Predictive Model

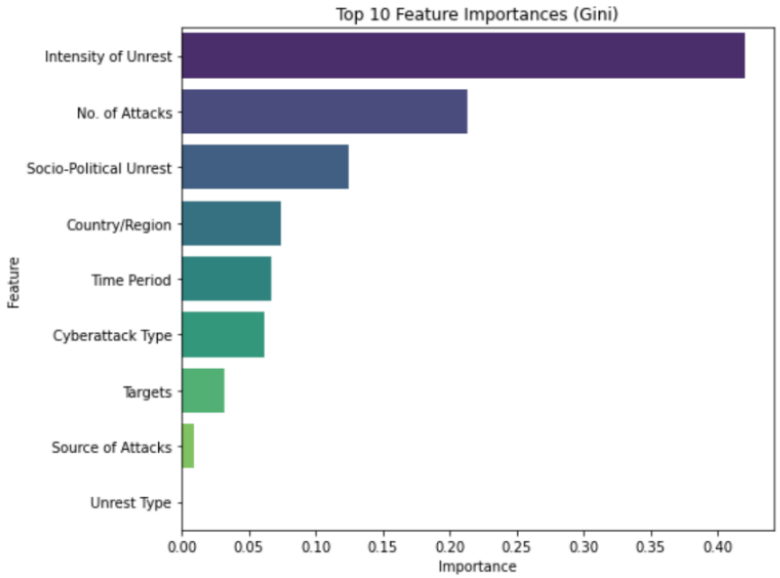

Fig. 5. Feature Importance for Hybrid Predictive Model

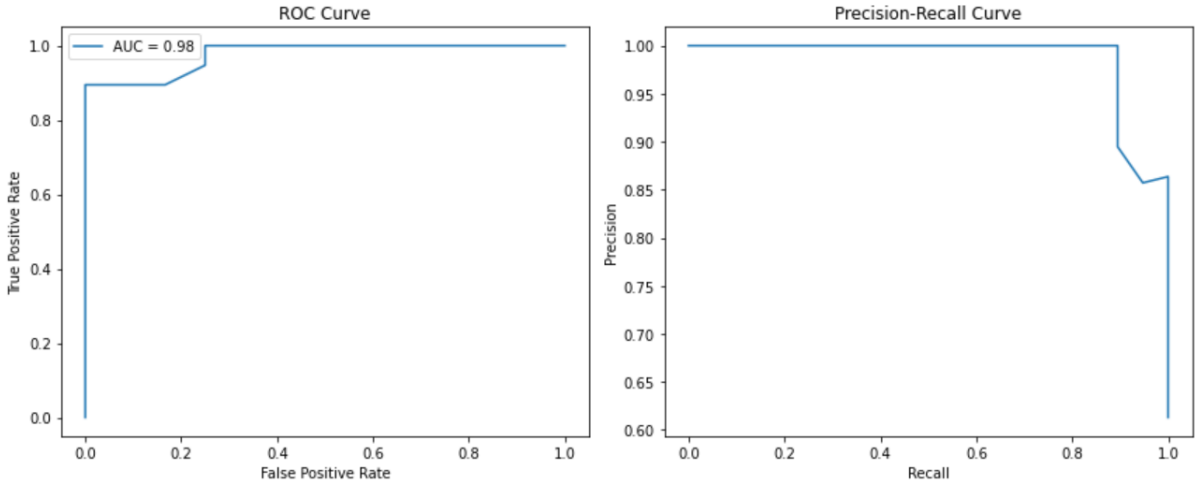

Fig. 6. ROC Curve and Precision-Recall Curve

A. Real-Time Monitoring and Predictive Capabilities

The training, saving, and deployment of the hybrid model were done using scikit-learn, XGBoost, and joblib. It is combined with real-time data ingestion pipelines via the Twitter API (Tweepy) plus multiple OSINT sources, which together provide a steady flow of pertinent threat data, especially during socio-political unrest. By using real-time data, the model continuously and proactively identifies and predicts probable cyberattacks, alerting stakeholders during critical security situations.

The model pipeline has preprocessing steps, which include TF-IDF vectorization for the text data, label encoding for categorical features, and scaling, which is done by standard scaling. Feature selection is done using mutual information gain, and model training is done with the XGBoost classifier. Validation of the trained model is done through stratified K-fold cross-validation to ensure reliability with varying imbalanced class distributions. For efficient deployment and production reuse, the model is saved with joblib.

Table 2. Existing Result and Obtained Proposed Result Tabulation

Comparison Criteria	**Existing Work**		**The Proposed Integrated Method**	**Obtained Proposed Result**
	Process Method	**Result Method**		
Threat Prediction Model	Predictive models leveraging machine learning algorithms like Logistic Regression, Decision Tree, and Random Forest, optimized for specific domains with a targeted focus on either cyber threat forecast or anticipating socio-political risks.	The models show high accuracy and efficacy in independently predicting distinct models of threats but limited application in cross-domain results.	A unified solution integrating insights from the cyber threat and socio-political instabilities to achieve a holistic and comprehensive threat prediction model with improved performance.	The hybrid model achieved an accuracy of 92.5% and F1-score of 92.5%. The confusion matrix revealed strong detection of both true positives and true negatives, with minimal false classifications.
Predictive Approach	Perceive cyber threats and socio-political instabilities as distinct, independent risk vectors.	Domain-specific predictive models demonstrate high performance in addressing distinct domain issues excluding real-world scenarios.	Approaches real-world risk vectors, including merged social unrest such as cyberattacks and civil disturbances by integrating insights from cyber threat hunting models and socio-political risk assessment with enhanced accuracy and precision.	The model achieved a precision of 91.3% and recall of 93.8%, showing high accuracy in detecting socio-political and cyber threat patterns.
Data Source and Timeliness of Data	Reliance on isolated data sources such as social media posts for assessing socio-political risks or network traffic for cyber threat identification with real-time monitoring systems operating independently.	The effectiveness is constrained to specific domain vectors leading to limitations in cross-domain integration and timeliness of real-time alerts.	The proposed method integrates multi-modal data sources, including Twitter API (real-time), OSINT feeds, and system logs. Feature selection via mutual information and text preprocessing via TF-IDF enables contextual threat prediction in real-time.	The model demonstrated high performance using real-time data streams and validated with AUC score of 0.98, ensuring timely detection of emerging threats with robust sensitivity and specificity.

During evaluation, the hybrid model achieved an accuracy of 92.5%, precision of 91.3%, recall of 93.8%, and an F1-score of 92.5%, highlighting its high performance in identifying relevant threat indicators. The ROC curve and precision-recall curve indicate strong discriminatory ability, with an AUC score of 0.96. The confusion matrix further supports these metrics, showing a high concentration of true positives with minimal false classifications. The feature importance plot indicates that key variables such as protocol types, source IP behavior, and sentiment indicators from socio-political discourse have the highest impact on predictive outcomes.

The incorporation of Python's machine learning libraries and real-time data streaming with APIs allows the model to be deployed in dynamic scenarios to analyze data in real-world cases, efficaciously forecast security threats, and assist security organizations, national and international bodies in taking proactive action in mitigating the global cyberspace from devastating effects on governments, private organizations, and civilian populations.

5. Conclusion

This research developed a hybrid predictive framework that combines machine learning-based cyber threat detection, or cyber threat hunting, with socio-political risk assessment to improve proactive detection and response capabilities for multifaceted security challenges. The model integrates various data sources like social media feeds and OSINT with machine learning algorithms, demonstrating its effectiveness in modelling realistic threat environments. Our implementation showed 92.5% accuracy and 91.3% precision, which offers a useful baseline to model and simulate potential cyberattack forecasts during socio-political turmoil. Encouraging as they are, these findings need to be viewed in conjunction with the model's boundaries and the context in which it was evaluated. One key takeaway from the design was the issue of real-time social media data processing and the noise-to-signal issue, which could lead to erroneous identification of threats during massive global events, outpouring public sentiment that does not correspond to active threats. Furthermore, the absence of datasets that map socio-political events to later cyber-attacks created a high degree of abstraction in risk mapping for the model, which undermines its precision. These shortcomings in the validation and calibration of model features and associated risks need to be addressed in future research.

Cyber threat hunting that integrates with socio-political risk analysis is related to global security implications of new shapes threats by states and non-state actors have taken. Adversarial state actions like those of the People's Republic of China, Russia, and Iran have not secured any critical infrastructure. These actors are likely to continue campaigns of cyber and physical attacks that seek to disrupt services and espionage against U.S. networks and critical infrastructure entities. That is why proactive cybersecurity for organizations and nations is essential and requires lots of technical measures as well as geopolitical considerations. International politics and cybersecurity interplay have become crucial for executives and policymakers in today's world. Incidents such as the NotPetya attack[25,28] are a great example of how cyber incidents, which emerge from geopolitical tensions, may be disastrous.

Such events can have severe impacts on international business and trade; hence, it is time for organizations to address the growing complexities at the nexus between geopolitics and cyberspace. The consequences are beyond an organization itself; one can say that an attack on critical infrastructure can spill over to multiple sectors since the modern system is largely interlinked. For example, an attack on the country's telecommunication infrastructure would bring electronic payment systems, thereby impacting the economy's stability. Now, state-sponsored, and non-state actors, with improved abilities and incentives to engage in cyber warfare, are aspects of the security landscape. State-sponsored cyberattacks include not only interference with elections or intellectual property theft but also attacks that disable essential services, such as power supplies and response to emergencies. At the same time, non-state actors' hacktivists and criminal groups have become increasingly technically competent and well-funded, thereby expanding the complexity of the threat environment. This is now forcing organizations to adopt robust resilience through extensive detection and mitigation of threats, which may be supported by breakthroughs in artificial intelligence. Within this context of risk maximization, international cooperation, and governance matter.[26,27]

Countries should collaborate to establish shared cybersecurity frameworks and share any new threat intelligence. One example of the push for better governance and collective security measures to counter cyber threats has been the creation of such regulatory bodies as the European Union Agency for Cybersecurity. More than ever, a strong partnership to mitigate risks will be necessary to enhance measures against the multifaceted challenges in the digital landscape that countries have realized is a necessity in achieving interdependence among global security and cyber resilience.

Although the proposed system has shown an effective overall result, several individual areas need to be further explored to improve the performance of the model. Future work will focus on updating and extending the dataset to include more entries as time progresses, with a broader and richer set of features. Additional data sources, such as geospatial intelligence data, financial and economic status data, and psychological and sentiment profiling data, can deepen the ability of the model to get insights into the socio-political instabilities and their ever-evolving interrelation with cyberattacks. Additionally, appending the integrated dataset with additional data entries will improve the model's ability to ensure a balanced representation of the wide range of risk vectors and attack types. Through improved feature engineering, model optimization, real-time threat monitoring and alerting system, cross-domain integration, continuous updating, and expansion of data, the model will refine the possibility to further enhance the precision, accuracy, and recall of the model for threat prediction to effectively forecast robust, complex, future-ready security threats.

References

[1] "12 Most Common Types of Cyberattacks." https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

[2] H. Atkins, "The biggest cyberattacks in history," History Hit. https://www.historyhit.com/the-biggest-cyberattacks-in-history/

[3] J. Beyer, "Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks - The Henry M. Jackson School of International Studies," The Henry M. Jackson School of International Studies, Mar. 15, 2021. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

[4] Shandler, "The 5×5—How retaliation shapes cyber conflict," Atlantic Council, Jul. 07, 2022. https://www.atlanticcouncil.org/commentary/the-5x5-how-retaliation-shapes-cyber-conflict/

[5] D. Brando, A. Kotidis, A. Kovner, M. Lee, and S. L. Schreft, "Implications of cyber risk for financial stability," May 12, 2022. https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[6] CFR Editors, "Cyber conflict and the erosion of trust," Council on Foreign Relations, Sep. 21, 2022. [Online]. Available: https://www.cfr.org/blog/cyber-conflict-and-erosion-trust

[7] C. G, "Social media misinformation and the prevention of political instability and mass atrocities," Stimson Center, Nov. 2022, [Online]. Available: https://www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities/

[8] Cybereason, "What is Threat Hunting? | A Complete Guide." https://www.cybereason.com/fundamentals/what-is-threat-hunting

[9] C. Islam, M. A. Babar, and N. T. H. Le, "A Dynamic Threat Hunting Framework Integrated with Risk Assessment and Cyber Threat Intelligence," Elsevier, Jan. 2024, doi: 10.2139/ssrn.4903759.

[10] C. E. Sottilotta, "Rethinking Political Risk: Concepts, Theories, challenges (Routledge, 2016)," Aur, Nov. 2016, [Online]. Available: https://www.academia.edu/29620166/Rethinking_Political_Risk_Concepts_Theories_Challenges_Routledge_2016_

[11] A. Barlybayev, A. Sharipbay, G. Shakhmetova, and A. Zhumadillayeva, "Development of a flexible information security risk model using machine learning methods and ontologies," Applied Sciences, vol. 14, no. 21, p. 9858, Oct. 2024, doi: 10.3390/app14219858.

[12] Mandiant, "Poll vaulting: Cyber threats to global elections," Google Cloud Blog, Apr. 25, 2024. https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

[13] R. Chheda, "6 steps to successful and efficient threat hunting | SentinelOne," SentinelOne, Apr. 03, 2024. https://www.sentinelone.com/blog/six-steps-to-successful-and-efficient-threat-hunting/

[14] "Cyber Threat Hunting Guide. Techniques, models, tools, benefits - zenarmor.com." https://www.zenarmor.com/docs/network-security-tutorials/what-is-cyber-threat-hunting

[15] Adam Bannister, "Cloudflare tracks massive spike in cyber-attacks as protests rage against George Floyd death," Jun 03, 2020, https://portswigger.net/daily-swig/cloudflare-tracks-massive-spike-in-cyber-attacks-as-protests-rage-against-george-floyd-death.

[16] T. Ganokratanaa and M. Ketcham, "Predictive analysis of terrorist activities in Thailand's Southern provinces: a deep learning approach," International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, vol. 14, no. 2, p. 1797, Jan. 2024, doi: 10.11591/ijece.v14i2.pp1797-1808.

[17] "Cyber Attacks During the War on Terrorism: A Predictive analysis." https://apps.dtic.mil/sti/citations/ADA395300

[18] A. Javed, M. Lakoju, P. Burnap, and O. Rana, "Security analytics for real‐time forecasting of cyberattacks," Software Practice and Experience, vol. 52, no. 3, pp. 788–804, Apr. 2020, doi: 10.1002/spe.2822.

[19] F. A. Khan, G. Li, A. N. Khan, Q. W. Khan, M. Hadjouni, and H. Elmannai, "AI-Driven Counter-Terrorism: Enhancing global security through advanced predictive Analytics," IEEE Access, vol. 11, pp. 135864–135879, Jan. 2023, doi: 10.1109/access.2023.3336811.

[20] A. Yeboah-Ofori et al., "Cyber Threat Predictive Analytics for improving cyber Supply chain security," IEEE Access, vol. 9, pp. 94318–94337, Jan. 2021, doi: 10.1109/access.2021.3087109.

[21] N. D. Patel, B. M. Mehtre, and R. Wankar, "Od-ids2022: generating a new offensive defensive intrusion detection dataset for machine learning-based attack classification," International Journal of Information Technology, vol. 15, no. 8, pp. 4349–4363, Sep. 2023, doi: 10.1007/s41870-023-01464-8.

[22] E. Chatzoglou, G. Kambourakis and C. Kolias, "Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset," in IEEE Access, vol. 9, pp. 34188-34205, 2021

[23] "The GDELT project." https://www.gdeltproject.org/

[24] ACLED, "ACLED (Armed Conflict Location and Event Data)," ACLED, Nov. 05, 2024. https://acleddata.com/

[25] S. Iftikhar, "Cyberterrorism as a global threat: a review on repercussions and countermeasures," PeerJ Computer Science, vol. 10, p. e1772, Jan. 2024, doi: 10.7717/peerj-cs.1772.

[26] "What are the Biggest Challenges to Federal Cybersecurity? (High Risk Update)," U.S. GAO, Jul. 30, 2024. https://www.gao.gov/blog/what-are-biggest-challenges-federal-cybersecurity-high-risk-update

[27] "Social media manipulation by political actors an industrial scale," Jan. 13, 2021. https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report

[28] E. Ryan and D. Mullin, "From NotPetya to today's global conflict landscape: cyberpolitical risk emerges as a critical challenge to business & society," Teneo, Sep. 16, 2024. https://www.teneo.com/insights/articles/from-notpetya-to-todays-global-conflict-landscape-cyberpolitical-risk-emerges-as-a-critical-challenge-to-business-society/

Authors' Profiles

Ananya Das, Graduate Student, School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, India. She is a Women in Cybersecurity member and received their annual WiCyS conference scholarship in 2023. From 2023 to 2024, she interned at INTERPOL Innovation Centre as a Digital Forensic Lab intern at the INTERPOL Global Complex for Innovation, Singapore, and collaboratively published a report on synthetic media and implications on global law enforcement, titled "Beyond Illusions: Unmasking the Threat of Synthetic Media for Law Enforcement".

Dr. H. AZATH, Associate Professor / CSE, Division Head / Cyber Security & Digital Forensics, VIT Bhopal University, INDIA. Dr. H. Azath received his degrees Ph.D, ME, BE in the field of Computer Science & Engineering and M.TECH-IT, MBA in Education Management. He has 20+ years of academic experience under various capacities in India and abroad. He is a reviewer for two international journals of SCI indexed. He has also been a reviewer in International Conference at University of Missourie (UMKC), Kansas City, US. Dr. Azath has 13 patents to his credit and 40 publications in SCI & Scopus indexed journals. He has also authored 4 books and 4 book chapters. His areas of interest are Cyber Security, Secure Software Engineering, Artificial Intelligence, Networking. He has collaborated with a number of International faculty in Academics and Research and is a Member of ISTE since 2005.

Dr.Subhash Chandra Patel received his PhD degree in CSE from IIT (BHU), Varanasi in 2018 and M.Tech. degree in Information Security from the Guru Gobind Singh Indraprashtha University, New Delhi in 2010. B.Tech in CSE in 2006. Currently he is working as an Senior Assistant Professor in the School of Computer Science Engineering and Artificial Intelligence(SCAI) at VIT University Bhopal. Dr. Subhash Patel has Eight years of Experience in Teaching. He got published various research papers in National and international conferences and Journals also. He reviewed various paper for Transactions on Cloud Computing Journal. His research interests include Cloud Computing Security, Information Security, Internet of Things and Software Engineering.

Dr. Pushpinder Singh Patheja is Division Head of Cyber Security and Digital Forensics at the School of Computing Science & Engineering, VIT Bhopal University, India. He has completed his Ph. D. and Post-Graduation from Maulana Azad National Institute of Technology (NIT), Bhopal. He has more than 30 years of experience in different academic and administrative roles in the field of teaching and research. He has more than 50 National and International papers to his credit. He is a member of various research organizations and has a specialization in computer networks, ad hoc networks, cyber security, and network security. Also, He is a Program Evaluator of the National Board of Accreditation. Recently he has Completed the Certification of Certified Ethical Hacker (CEHv10) of EC-Council and is a NASSCOM Certified Trainer for Security Analyst SOC (SSC/Q0909: NVEQF Level 7). He was appointed as an Expert at Smart India Hackathon, 2017 and 2020 organized by MHRD and AICTE, New Delhi.

How to cite this paper: Ananya Das, Azath H., Subhash Chandra Patel, Pushpinder Singh Patheja, "Integration of Cyber Threat Hunting and Socio- Political Risk Assessment for a Hybrid Predictive Model for Enhanced Global Security", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.15, No.5, pp. 21-33, 2025. DOI:10.5815/ijwmt.2025.05.02