Predicting The Success of Terrorist Attacks Using Logistic Regression Analysis

Jaden Goodwin

STA3180: Statistical Modelling

Dr. Winner

April 23, 2025

Abstract

The study investigates the patterns and outcomes of global terrorist attacks from the years 2000 to 2020 using the Global Terrorism Database (GTD). The aim is to understand how certain predictors of terrorist attacks can predict the likelihood of a terrorist attack's success. Data analysis was conducted in R, where a logistic regression model was used to predict the binary outcome of attack success or failure. This analysis focuses on five predictor variables: attacktype1, region, weaptype1, targtype1, and suicide. Based on the GTD, these variables were selected due to their relevance in identifying strategic and contextual factors that assess the effectiveness of terrorist attacks and can work to predict future outcomes. Moreover, stepwise selection was used for model reduction and choosing the most parsimonious combination of predictors. The data was split into train and test data to evaluate the model's performance in predicting attack success, visualized by a confusion matrix. A cross-validated set was then used to increase the robustness of the model, and finally, an optimal threshold was chosen using Youden's J statistic. This study contributes to the understanding of global terrorism dynamics, offering insights into which tactical and regional patterns most influence the success of terrorist events. The findings aim to support future efforts in risk mitigation, policy development, and global security strategy.

Predicting Terrorist Attack Success Using Logistic Regression Analysis

Terrorism poses a significant threat to global security, political stability, and civilian life. Its impact extends beyond casualties and destruction. The effects of terrorism instill fear, disrupt social cohesion, and influence broader international relations (Petmezas, 2022). As such, a statistical analysis of the factors that contribute to the success of terrorist attacks is both timely and essential.

Empirical investigation of terrorism data contributes to the broader understanding of the phenomenon by quantitatively evaluating the relationship between tactical variables, such as weapon or attack type, and the probability of attack outcomes. The results can inform future counterterrorism strategies by identifying high-risk patterns and scenarios. In this paper, it is hypothesized that certain contextual variables can predict the likelihood of a terrorist attack's success. This analysis aims to provide statistics-backed insights that can help policymakers mitigate the risks posed by future acts of terrorism through understanding the situations where terrorists succeed the most.

Literature Review

Existing literature has discovered that one of the most prominent forms of lethality success is suicide attacks due to the attacker's commitment and ability to breach security measures (Pape, 2003). Despite these insights, there remains a gap in the literature when it comes to integrated, predictive modeling using updated global data. To dispute this, Qu (2024) used confirmatory factor analysis methods to evaluate and score the harm of terrorist attacks using an indicator system with levels of different predictor variables (Qu et al., 2024, p.3). The harm indicator evaluation model was deemed accurate as it scored major terrorist events such as 9/11 with the highest harm score, which can be corroborated by subjective news reports (Qu et al., 2024, p.4). Qu created a model to assess harm, a subjective idea, with an objective index.

In line with this paper, the aim is to use logistic regression to predict the likelihood of an attack. Tarakji (2021) similarly employed logistic regression to classify attack probability, while also incorporating random forests and neural networks to enhance predictive accuracy. The regression results suggest that factors such as political instability, economic downturns, and geographic location significantly influence attack frequency, with coefficients indicating a 10–15% increase in the likelihood of attacks in regions experiencing ongoing conflict (Tarakji, 2021, p.31). Machine learning models, particularly random forests, achieve an accuracy of approximately 85%, outperforming traditional regression models in out-of-sample predictions. To visualize the data, Xu (2024) identified four major "turbulent cores" of global terrorism risk: Middle and North Africa, South Asia, Central Asia, and Central America and the Caribbean. By integrating Xu's findings with our data processing, we utilized region as a predictor in the model.

In summary, past studies have used models to assess the risk and likelihood of a terrorist attack. This leaves the question unanswered: Is there a way to predict the success of an incident of terrorism?

Aim

The intelligent prediction and prevention of terrorism has been an ongoing struggle since the midst of the information age. In performing this research, the aim is to contribute to an ongoing discussion on the methods, trends, and results that arise out of the thousands of non-outlying terrorist attacks that have occurred within the last 25 years. The ability to predict situations that may lead to a cost of civilian life before they occur and project the likely damage of an ongoing event can inform counterintelligence agencies of the caliber of response they should invoke in any given situation.

Methods

Data Collection

The Global Terrorism Database (GTD) is an open-source database maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland. The GTD contains over 200,000 records of terrorist attacks from 1970-2020 from several phases of data collection efforts relying on unclassified source materials, mainly media articles and electronic news archives (START, 2021, p.2). Incidents from 1970 through 1997 were collected by the private security agency called Pinkerton Global Intelligence Service (PGIS), incidents from 1998 through March 2008 were recorded in collaboration with the Center for Terrorism and Intelligence Studies (CETIS), incidents from April 2008 through October 2011 were collected primarily from the Institute for the Study of Violent Groups and lastly START leads current GTD data collection as of November 2011 (START, 2021, p.3). START uses automated and manual data collection strategies to compile the GTD and promotes accuracy in its data collection by following a time lag to avoid inaccurate reports, prioritizing recent sources, using highly valid sources, specifically documenting the geo-location of the incident, using specific language about assailants, and including names of victims. (START, 2021, p.4). For the purposes of the GTD, a terrorist attack is defined as “the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation” (START, 2021, p.11).

Before running statistical tests, data cleaning methods were utilized to ensure reliability and accuracy of results. First, the dataset was cleaned to include only events that occurred between 2000 and 2020. This time frame was chosen to avoid inconsistencies in older records and limit the scope to modern attacks. Doubtful cases—those flagged by the GTD as questionable in their classification as terrorist incidents—were excluded to maintain data accuracy and clarity. Observations containing missing or unknown values for any of the five

predictor variables were also removed. Additionally, any anomalous or outlier entries, such as those with undefined or misclassified categories, were identified and removed.

Variables

We selected initially six predictor variables based on their relevance to understand the outcomes of terrorist attacks: “attacktype1”, “region”, “weaptype1”, “targtype1”, “nperps”, and “suicide”. Attack type is a categorical predictor with 8 levels and describes the method or tactic used in the incident (1=Assassination, 2=Armed Assault, 3=Bombing, 4=Hijacking, 5= Barricade Incident, 6=Kidnapping, 7=Infrastructure, or 8=Unarmed Assault)(START, 2021, p.25). Understanding attack types is essential in assessing which tactics are more likely to yield successful outcomes, and it can also help display the most common methods used in terrorist attacks from 2000-2020. The region variable is categorical with 12 levels, and specifies the location of the attack by world region (1=North America, 2=Central American and Caribbean, 3=South America, 4=East Asia, 5=Southeast Asia, 6= South Asia, 7=Central Asia, 8=Western Europe, 9=Eastern Europe, 10=Middle East and North Africa, 11=Sub-Saharan Africa, and 12=Australasia and Oceania)(START, 2021, p. 21-22). Regional patterns may reveal structural or contextual factors influencing success and show the prevalence of terrorism. The categorical variable weapon type classifies the primary weapon used in the attack and consists of 12 responses (1= Biological, 2=Chemical, 3=Radiological, 4=Nuclear, 5=Firearms, 6=Explosives, 7 = Fake Weapons, 8= Incendiary, 9= Melee, 10= Vehicle, 11=Sabotage Equipment, and 12 = Other)(START, 2021, p. 28-29). Analyzing weapon types provides insight into the lethality and strategic utility of different tools of violence. This will help display that various weapon types have different scales of harm and casualties. The categorical variable targtype1 indicates the general category of the target, such as government officials, military, civilians, businesses, etc. and consists of 22 levels. This helps in identifying whether certain targets are more vulnerable to effective attacks than others. The quantitative variable nperps is the number of terrorists directly involved in committing the attack, possibly indicating the difference between small and large operations. And lastly, suicide is a binary predictor with a 1 indicating a suicide attack and 0 if not.

The binary response variable used in the model is “success” which indicates whether the attack had tangible effects that align with the type of attack (1=successful, 0=unsuccessful). It does not take into account the larger goals of the perpetrators.

Analytic Methods

Since the analysis has a binary response variable, a logistic regression model was chosen because it is suitable for predicting binary outcomes based on categorical or quantitative predictors. After fitting the full model, Akaike Information Criterion (AIC) stepwise selection was performed to determine the best combination of variables to use for model fitness and complexity. The data will then be split into test and training data to assess the predictive capabilities of the model. To improve the robustness of the model and reduce variance, k-fold

cross-validation (k=10) was performed, and a confusion matrix was created to evaluate the performance of the prediction model.

After evaluating the confusion matrix, a Receiver Operating Characteristic curve will be used to visualize and analyze model performance across the different classification thresholds. ROC curves test the sensitivity against 1 minus specificity. The AUC (area under the curve) will also be calculated to help summarize the ROC by measuring the overall performance of the binary classification model. A high AUC value is equated to better model performance. Following the ROC curve, to further improve the model, Youden's J Statistic will be used to determine the optimal classification threshold. The Youden Index is maximized as the sensitivity + specificity – 1 (Berrar, 2019). The J statistic range is from 0 to 1. Utilizing the J cutoff in a classification model attempts to balance the sensitivity and specificity. Such a trade-off is especially meaningful when dealing when analyzing terrorism since focusing just on high accuracy can underestimate the lack of robustness in model performance, where one class is under-identified. An alpha level of 5% will be used for all significance tests.

Results

A full logistic regression model was constructed and includes predictors nperps, suicide, attacktype1, region, weaptype1, and targtype1. Stepwise model selection was used for model reduction. First, attacktype1 was added to the null model, then weaptype1 was added, then targtype1 was added, then region, and finally suicide. The AIC of the full model is 9736.034

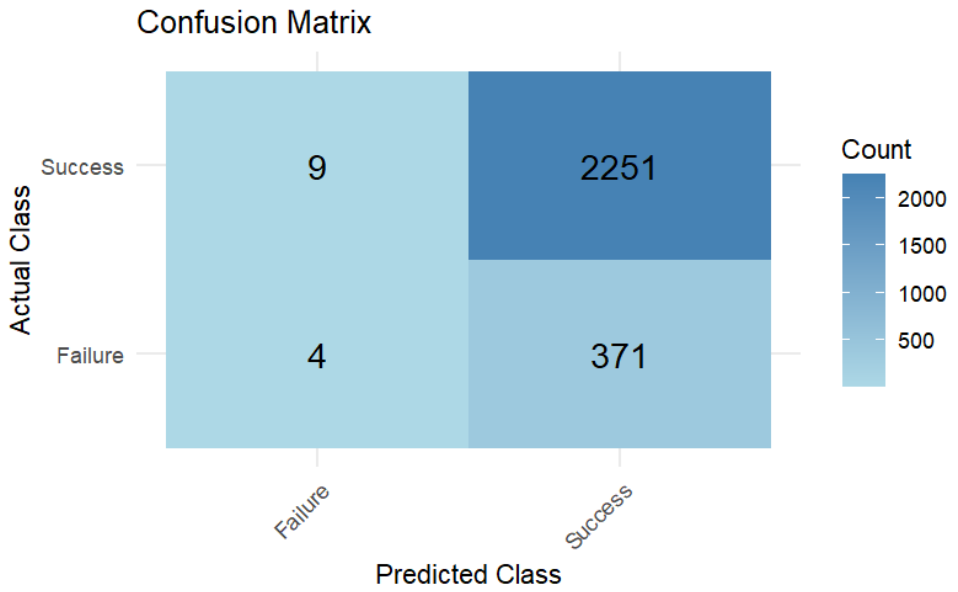
According to stepwise model selection, the logistic regression model with the lowest AIC had 5 predictors: attacktype1, weaptype1, targtype1, region, and suicide. Forward and backward selection methods also had the same results. The AIC of the five-predictor model is 9734.113. A table of the 5-variable logistic regression model standard errors was created (Appendix A). The standard errors for the variable weaptype1 are incredibly large in magnitude as well as the coefficients being very large and not significant. This is an indication of numerical instability or multicollinearity. Removal of the variable is best for the rest of the analysis. Thus, the chosen model is a four-predictor model with attacktype1, region, suicide, and targtype1 (Appendix B).

All the attacktype1 categories were highly significant with positive coefficients, meaning that certain attack types have increasing effects on the probability of attack success. The region categories Central America/Caribbean, South America, Southeast Asia, Eastern Europe, Middle East/North Africa, and Sub-Saharan Africa were all statistically significant and positive, indicating that in these regions there is a higher probability of attack success. The suicide predictor is also highly significant and positive, meaning that suicide attacks increase the probability of attack success. The targtype1 statistically significant categories include Government, Police, Abortion Related, Airports, Diplomatic, Maritime, and Transportation are significant and vary on being positive or negative. Note that the targtype1 category

To test the prediction abilities of the logistic regression model, the data was split into training and test datasets using the 80-20 method. Using a threshold of 0.5, with a probability less than 0.5 classified as a failure and greater than 0.5 classified as a success, the results below show the confusion matrix in Table 1.

Table 1

Confusion Matrix on Test Dataset



The overall accuracy of the model is 0.8558 with a 95% confidence interval of [0.8418,0.869] on the test dataset. There is an evident numerical imbalance in the success variable, with significantly more successes than failures indicated by shading in the confusion matrix. The model performance metrics are displayed in Table 2 below. The p-value is very large, meaning that there is not enough evidence to say that the model accuracy is significantly better than the accuracy from guessing the most frequent class, success. The results show a very high sensitivity but an extremely low specificity. High sensitivity means that the model is good at classifying cases of success. Low specificity indicates that the model is not good at classifying failures. The model has high detection prevalence indicating bias toward predicting the positive class.

Table 2

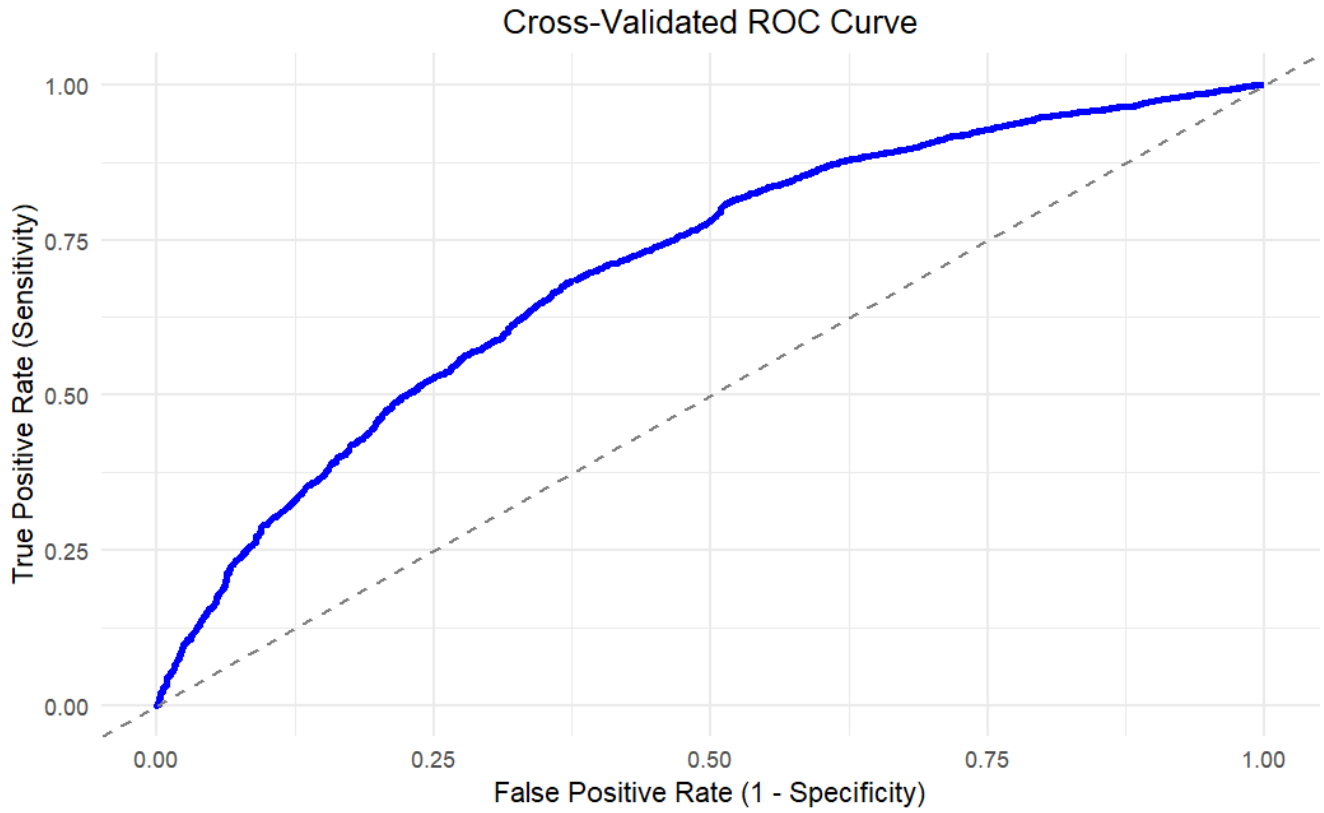
Model Performance Metrics for Test Data

Performance by Class	
Metric	Results
No Information Rate	0.858
P-Value [Acc>NIR]	0.6227
Sensitivity	0.996
Specificity	0.011
PPV	0.859
NPV	0.308
F1	0.922
Prevalence	0.858
Detection Rate	0.854
Detection Prevalence	0.995
Balanced Accuracy	0.503

Next, for a cross-validated model using 10 k-folds, the confusion matrix was created, and performance metrics were calculated (Appendix C). The overall accuracy of the cross-validated model is 0.854 with a 95% confidence interval of [0.8483,0.0.8605], very similar to the previous model. The sensitivity, specificity, PPV, NPV, and other statistics are very similar to the previous estimates without cross-validation, which was the anticipated outcome. The model is, however, slightly better at classifying failures due to a slight increase in specificity, NPV, and balanced accuracy. The p-value did decrease using the cross-validated model, but it is still much larger than 0.05, indicating that there is not enough evidence to say that the model accuracy is significantly better than the accuracy from guessing the most frequent class. An ROC curve was constructed to visualize the cross-validated model tradeoff between sensitivity and false positive rate in Figure 1.

Figure 1

Receiver Operating Curve of Cross-Validated Data Prediction Results



The AUC= 0.70411, which is considered good model performance in the trade-off between true positive rate and false positive rate. To address the class imbalance in the binary response, Youden's J statistic was calculated to be 0.8534 as the new threshold, maximizing the sum of sensitivity and specificity. A new confusion matrix and model metrics were calculated using Youden's J as the new threshold, shown in Tables 3 and 4, respectively. The overall model accuracy is 0.6721 with a 95% confidence interval of [0.664,0.6801]. This is a decrease in accuracy compared to the previous models. As you can see, there are many more observations on the left side of the confusion matrix now shown by the shading of the matrix. In Table 4 below, the p-value is 1, indicating there is no difference between this model's accuracy and guessing. The sensitivity decreased, and the specificity significantly increased, and this model has the highest balanced accuracy, which gives equal weight to both classes. The balanced accuracy is 0.6550, which is slightly better than simply guessing and an improvement from the previous model iterations.

Table 3

Confusion Matrix on Cross-Validated Model with Optimal Threshold

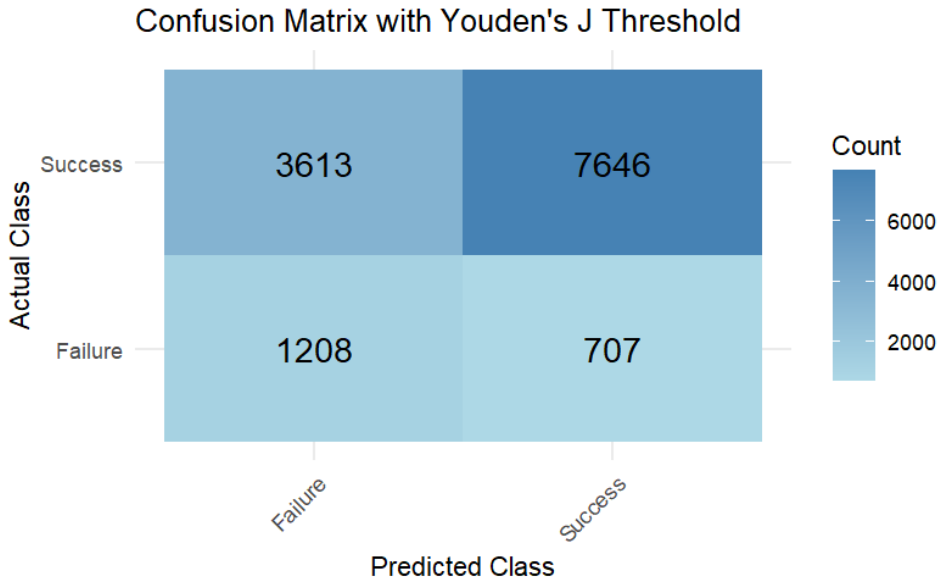


Table 4

Model Performance Metrics for Cross-Validated Dataset with Optimal Threshold

Performance with Youden's J Threshold (By Class)

Metric	Result
No Information Rate	0.855
P-Value [Acc > NIR]	1
Sensitivity	0.6791
Specificity	0.6308
PPV	0.9154
NPV	0.2506
F1	0.7797
Prevalence	0.8546
Detection Rate	0.5804
Detection Prevalence	0.6341
Balanced Accuracy	0.6550

Discussion

Conclusions

Given the parameters of the AIC-optimized model, results are presented that both affirm the analysis of previous research papers discussed in the Literature Review while providing new insights unique to this study.

Geographic location is a very frequently discussed feature for prediction in attack modeling (Tarakji, 2021; Xu, 2024), yet this study's results not only affirm the significance of geographic location in terms of attack likelihood, but also in terms of the success of that attack. One interpretation of this pattern is that terrorist efforts are more likely to see success in regions with less urban development and militarization. With North America as the reference level for the region features, we see that regions such as East Asia, West Europe, and Oceania have near zero or even negative, while statistically significant, coefficients. This is compared to regions such as SE Asia, the Carribean, and Sub-Saharan Africa, which all have a coefficient greater than 1.5 and statistical significance. Thus, it appears that regions such as SE Asia, the Carribean, and Sub-Saharan Africa have much higher log-odds as compared to more economically developed regions.

Similarly to the interpretation of the significance of the geographic location, target type presents an impactful pattern. Compared to 'Business' being the reference category as the attack type, there are two important traits of note. First, all statistically significant target types (excluding Abortion-Related) are either militarized or state-owned. For example, Government, Telecommunications, and Transportation are all significant features; in most nations, these buildings and pieces of infrastructure are owned or maintained by the state. The second point of note is that all statistically significant categories have negative coefficients (excluding Terrorists), many with a quite large magnitude. It appears that these categories being state maintained may strongly lower the log odds of a successful attack. From the comparison of these features, we see that non-state-owned categories such as Business, Tourists, and NGO result in a positive increase in the log odds. Though these three categories are not statistically significant, this difference may still show a separation between those types of targets that are more likely to have stronger security policy, faster response times, and more trained personnel (state-owned), versus those targets who do not (non-state-owned).

The balanced accuracy of the study's highest-performing model was 0.6550, markedly lower than the No Information Rate of 0.855. However, it is important to consider what the comparison of these two values means in the context of this study. The No Information Rate, derived from predicting the most common class in a dataset for all samples, would implies that a municipal government would respond with the full and highest caliber of force to all possible incidents of potential terrorism. For many nations globally, especially those where terrorism is most prevalent, this strategy may not be economically viable and may wear counterterrorism resources thin. While a recall only above 0.63 does not make this model viable on its own, the

naive solution of interpreting the model only in the context of the dataset loses much of the social implications surrounding terrorism. This proposes a limitation around class-imbalance, which would bring down the No Information Rate and increase the significance of the models against the NIR.

Given these patterns in the categorical differences in types of attacks, it presents that much of what determines whether an attack is "successful" or not comes in the intention and the planning. Given these interpretations, counterterrorism agencies may need intelligence before attacks happen to inform the appropriate response, as features such as whether an attack is a suicide or who it will target are typically not known until an attack commences. Given this study, it appears that successful attacks most commonly present in underdeveloped regions, specifically in those with lacking infrastructure to appropriately or cooperatively respond to militarized threats.

Limitations

About J statistic: there is controversy with this model since it may sacrifice the overall predictive accuracy of the model. The gain in specificity implies a model that is more appropriate to detect true threats. This balance is especially critical in national security applications, where the cost of false negatives (i.e., failing to predict a successful attack) is significantly greater than the cost of false positives. As for the NIR discussed above, a synthetic class upsampling technique such as SMOTE could increase the number of negative samples in the dataset, which would increase the model's robustness with respect to negative cases while lowering the NIR, potentially pushing simple and interpretable models into the realm of statistical significance. However, that is not explored here.

References

Berrar, D. (2019). Performance Measures for Binary Classification. In *Encyclopedia of Bioinformatics and Computational Biology* (Vol. 1, pp. 546–560). Academic Press. https://www.sciencedirect.com/science/article/pii/B978012809633820351.

Pape, R. A. (2003). The strategic logic of suicide terrorism. *American Political Science Review, 97*(3), 343–361. https://doi.org/10.1017/S000305540300073X

Petmezas, D. (2022, September 12). *The economic impact of terrorism*. The economic impact of terrorism - durham university business school. https://www.durham.ac.uk/business/impact/world-economy/the-economic-impact-of-terrorism/

Qu, Y., Chen, Y., Tan, Z., & Han, B. (2024). The statistical analysis based on GTD Terrorist Incident Record Data. *Heliyon*, *10*(13). https://doi.org/10.1016/j.heliyon.2024.e33804

START (National Consortium for the Study of Terrorism and Responses to Terrorism). (2022). *Global Terrorism Database 1970 - 2020 [data file]*. https://www.start.umd.edu/gtd

START (National Consortium for the Study of Terrorism and Responses to Terrorism). (2021, August). Global Terrorism Database codebook: Methodology, inclusion criteria, and variables. University of Maryland. https://www.start.umd.edu/gtd/downloads/Codebook.pdf

Tarakji, Mohamed. (2021) *Examining the factors that predict the likelihood of the success of a terrorist attack, and severity from a machine learning and regression lens* (thesis). https://doi.org/doi:10.7282/t3-b2j5-v026

Xu, Z., Lin, Y., Cai, H., Zhang, W., Shi, J., & Situ, L. (2024, August 28). *Risk assessment and categorization of terrorist attacks based on the Global Terrorism Database from 1970 to 2020*. Nature News. https://www.nature.com/articles/s41599-024-03597-y

Appendices

Appendix A

Table A

Table of Standard Errors of the Five-Predictor Logistic Regression Model Coefficients

Standard Errors of Model Coefficients Generalized Linear Model (Binomial Family)	
Variable	Standard Error
(Intercept)	439.747
attacktype1Armed Assault	0.087
attacktype1Bombing	0.113
attacktype1Hijacking	0.405
attacktype1Hostage Barricade	0.610
attacktype1Hostage Kidnapping	0.169
attacktype1Infrastructure Attack	0.227
attacktype1Unarmed Assault	0.387
weaptype1Chemical	439.747
weaptype1Radiological	520.865
weaptype1Firearms	439.746
weaptype1Explosives	439.747
weaptype1Fake Weapons	439.748
weaptype1Incendiary	439.747
weaptype1Melee	439.746
weaptype1Vehicle	439.746
weaptype1Sabotage Equipt	510.354
weaptype1Other	439.747
regionCent.Amer/Carib	1.059
regionS.America	0.219
regionE.Asia	0.316
regionSE. Asia	0.163
regionS.Asia	0.153
regionCent.Asia	0.370
regionWest.Europe	0.183
regionEast.Europe	0.205
regionMidEast N.Afr	0.155
regionSub-Saharan Afr	0.170
regionAustr/Oceania	0.673
suicide1	0.079
targtype1Government	0.121
targtype1Police	0.119
targtype1Military	0.160
targtype1Abortion Related	0.605
targtype1Airports	0.332
targtype1Diplomatic	0.197
targtype1Educational	0.204
targtype1Food/Water Supply	348.192
targtype1Journalists	0.191
targtype1Maritime	0.510
targtype1NGO	0.402
targtype1Private Citizens	0.118
targtype1Religious	0.152
targtype1Telecommunication	1.015
targtype1Terrorists	0.271
targtype1Tourists	1.029
targtype1Transportation	0.158
targtype1Utilities	0.313
targtype1Political	0.225

Appendix B

Table B

Logistic Regression Model Coefficients and Significance

	Dependent variable:
	success
attacktype1Armed Assault	1.776***
	(0.082)
attacktype1Bombing	0.939***
	(0.079)
attacktype1Hijacking	1.730***
	(0.379)
attacktype1Hostage Barricade	2.977***
	(0.595)
attacktype1Hostage Kidnapping	1.684***
	(0.165)
attacktype1Infrastructure Attack	2.089***
	(0.156)
attacktype1Unarmed Assault	1.452***
	(0.199)
regionCent.Amer/Carib	2.119**
	(1.066)
regionS.America	0.957***
	(0.216)
regionE.Asia	-0.284
	(0.271)
regionSE. Asia	1.271***
	(0.158)
regionS.Asia	0.758***
	(0.147)
regionCent.Asia	0.026
	(0.367)
regionWest.Europe	0.157
	(0.177)
regionEast.Europe	0.631***
	(0.199)
regionMidEast N.Afr	0.451***
	(0.151)
regionSub-Saharan Afr	1.134***
	(0.165)
regionAustr/Oceania	0.282
	(0.689)
suicide1	0.236***
	(0.077)
targtype1Government	-0.491***
	(0.119)
targtype1Police	-0.273**
	(0.118)
targtype1Military	0.062
	(0.158)
targtype1Abortion Related	-1.499**
	(0.599)
targtype1Airports	-1.890***
	(0.326)
targtype1Diplomatic	-0.850***
	(0.196)
targtype1Educational	-0.152
	(0.202)
targtype1Food/Water Supply	10.107
	(128.842)
targtype1Journalists	-0.051
	(0.188)
targtype1Maritime	-1.453***
	(0.496)
targtype1NGO	0.227
	(0.393)
targtype1Private Citizens	-0.142
	(0.117)
targtype1Religious	-0.184
	(0.151)
targtype1Telecommunication	1.749*
	(1.016)
targtype1Terrorists	0.681**
	(0.266)
targtype1Tourists	1.115
	(1.028)
targtype1Transportation	-1.127***
	(0.157)
targtype1Utilities	-0.603*
	(0.310)
targtype1Political	-0.076
	(0.220)
Constant	0.171
	(0.184)
Observations	13,174
Log Likelihood	-4,973.741
Akaike Inf. Crit.	10,025.480
Note:	*p<0.1; **p<0.05; ***p<0.01

Appendix C

Table C

Confusion Matrix on Cross-Validated Model

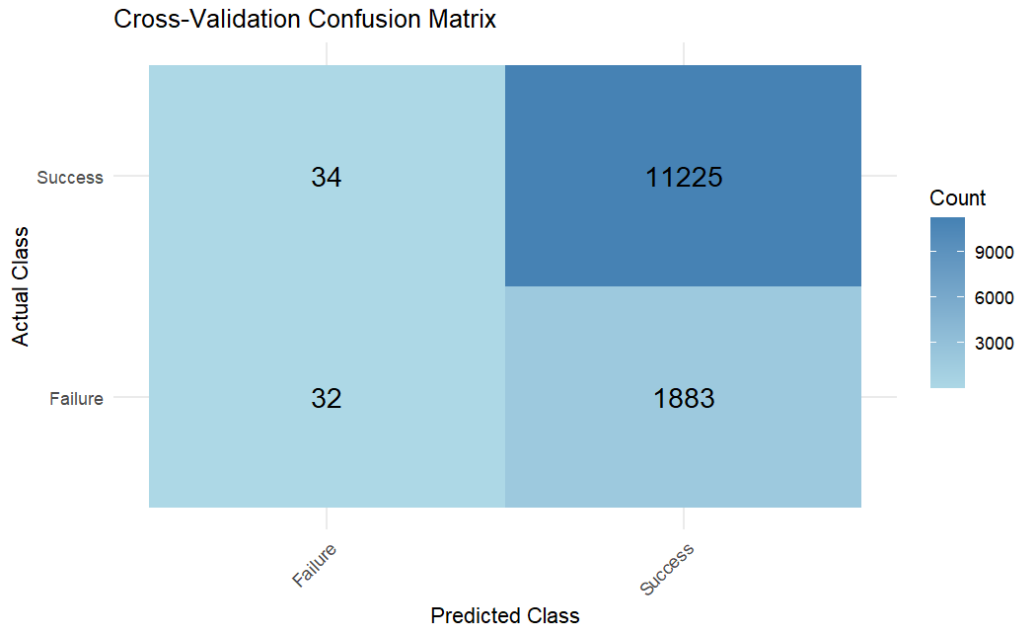


Table D

Model Performance Metrics for Cross-Validated Dataset

Cross-Validation Performance by Class	
Metric	Result
No Information Rate	0.8545
P-Value [Acc > NIR]	0.5258
Sensitivity	0.997
Specificity	0.017
PPV	0.856
NPV	0.485
F1	0.921
Prevalence	0.855
Detection Rate	0.852
Detection Prevalence	0.995
Balanced Accuracy	0.507