(Online) ISSN 2744-1741
Original Research

Defense and Security Studies
Vol. 7, No. 1, 2026, pp.22-42
https://doi.org/10.37868/dss.v7.id303

Threat assessment model in air defense systems using Artificial Neural Networks

Salih Taşdemir[1*], Murat Atan[2]

[1] Department of Econometrics, Hacı Bayram Veli University, Türkiye
[2] Department of Econometrics, Hacı Bayram Veli University, Türkiye

*Corresponding author E-mail: salihtasdemir35@hotmail.com

Received: Dec. 25, 2025
Revised: Jan. 11, 2026
Accepted: Jan. 13, 2026
Online: Jan. 13, 2026

Abstract

This study aims to automate threat assessment and target assignment processes in air defense systems using a dynamic, learning artificial intelligence-based model. Unlike threat assessment studies in the literature that use different criteria and methods, this study integrates missing data completion, multi-criteria analysis, and artificial neural networks to dynamically update the threat score. Furthermore, unlike studies in the literature, the number of criteria used has been increased to enable the model to provide a broader perspective. Most studies are static and use a small number of criteria; this study presents a dynamic, multi-criteria model that can handle incomplete data. The developed Geometric Threat Score proposes an average perspective for threat assessment, which varies depending on individuals and geographical conditions. The model generates threat scores using criterion data obtained from radars and sensors and can respond adaptively to changing conditions. The results achieved demonstrated high performance with mean square errors (MSE) of 0.0005–0.0072 and a correlation coefficient (R) above 95%. This approach accelerates decision support processes in air defense systems, reducing human influence and increasing system effectiveness.

Keywords: Threat assessment; Artificial neural networks; Air defense systems; Multi-criteria decision making; Missing data completion.

1. Introduction

Threat assessment and weapon assignment in air defense systems are among the most critical processes for decision-makers in a combat environment [1]. These decisions are often made within limited time frames and re-quire considering multiple variables simultaneously. Therefore, artificial intelligence-based approaches are gaining importance to reduce human-related errors and create faster decision-making mechanisms. Traditional methods often struggle to dynamically adapt to evolving battlefield conditions and new threats [2]. This paper proposes a novel and dynamic threat assessment model that uses an Artificial Neural Network (ANN) to prioritize air targets. The model was trained on a comprehensive dataset synthesized from literature and expert opinions, covering 26 different threat criteria. A key innovation is the development of the "Combined Geometric Threat Score," which aligns threat values obtained from the literature with a weighted score based on the im-portance of the criteria, forming a solid foundation for ANN training. The experimental results demonstrate the

model's high performance with an R-value around 0.95 for regression across various data splits and a low mean square error (MSE), highlighting its accuracy in predicting threat levels. It has been concluded that the AI-focused approach can significantly increase decision-making speed and accuracy, reduce human error, and provide a scalable framework for automatic threat prioritization in network-centric air defense systems. This study takes into account more criteria in order to fill the gap in the literature. A comprehensive data set consisting of 26 criteria has been used. It provides an average perspective on threat assessments that may vary depending on geographical conditions or individuals, identifies the relationship between the criteria for the first time, performs missing data completion, and offers a more verifiable training set in a dynamic structure.

2. Literature Review

It has been stated that the threat assessment concept and the weapon assignment model should be implemented, and that this should be evaluated using sensor information from systems on an interconnected network [3].

A review of the literature reveals that different numbers of different criteria are used and different threat assessment methods are employed. Studies in the literature have grouped threat assessment methods under four main headings, as listed below. It has been stated that the combined use of these methods and the provision of visualization will improve performance [4].

Rule-Based Fuzzy Logic: Also defined as gray relational analysis (GRA). It analyzes the relationship be-tween threats using gray system theory. As the number of criteria increases, so does the number of rules. Since too many rules are required, evaluation can be performed with smaller-scale criteria. Expert opinions are re-quired for accuracy. The results obtained here are important in terms of their use in the testing and training model of artificial neural networks.

Bayesian Networks and Stochastic Methods: They evaluate threats using probabilistic inference. They are useful for uncertain data, but require a large data set for training. It is very difficult to clearly determine the strike effectiveness of systems. A sufficient number of strikes and successful outcomes must be obtained. Generating such data is very difficult due to confidentiality concerns and the lack of sufficient samples.

Multi-Criteria Decision-Making Methods: When applying multi-criteria decision-making methods, in cases where weights are unknown in the literature, ranking superiority methods such as the Borda Method, Condorcet Method, and Basic Lexicographic Method are available. Methods for determining the criterion weights necessary for calculation also play an important role. The most preferred methods for determining criterion weights are the Simple Cardinal Method, the Analytic Hierarchy Process (AHP), the Critic Method, and the Entropy Method are among the most preferred methods. Once the weights have been determined, it is also important to compare the weights obtained. Kullback-Leibler Divergence and Mean Absolute Error Methods are used to compare the obtained weights. When weights are determined, TOPSIS, ELECTRE, PROMETHE, Permutation, DEMATEL, and MAUT methods are frequently preferred for ranking or selection processes. Most of these methods require the accuracy of expert opinions. The results deter-mined by multi-criteria decision-making methods can be used as training data for artificial neural networks.

Artificial Neural Networks: The model architecture section, consisting of input, output, and hidden layers, the training section comprising the dataset, preprocessing, optimization, and validation stages, and the mathematical formulation. Criteria are used as input parameters. The number of layers is determined by the activation function in the hidden layer. The desired result is specified in the output layer. It is necessary to know a sufficient number of output results for the start. It is important that the data set consists of calculated, validated results. Normalization and missing data completion are performed in the preprocessing section. In the optimization section, the training, validation, and testing ratios are determined. The learning rate, number of hidden layers, and number of hidden layer neurons are optimized. The number of iterations or the stopping success rate is determined with the learning function. After finding good ratios and numbers for MAPE and R-squared values, the artificial intelligence model is created.

Studies in the literature according to the number of criteria and the method used are shown in the Table 1.

Table 1. Studies in the literature according to the number of criteria and method used

Number of criteria	Rule-based fuzzy logic	Bayesian networks and stochastic methods:	Multi-criteria decision-making methods	Artificial Neural Networks
1			Reference [5]	
2				Reference [6]
3	Reference [7]	Reference [8]	Reference [9]	Reference [10]
	Reference [10]			Reference [11]
	Reference [12]			
	Reference [13]			
4	Reference [14]	Reference [15]	Reference [16]	Reference [17]
	Reference [18]		Reference [19]	Reference [20]
				Reference [21]
5	Reference [22]		Reference [23]	Reference [24]
			Reference [25]	
6	Reference [26]	Reference [27]	Reference [28]	
	Reference [28]		Reference [29]	
	Reference [30]		Reference [32]	
	Reference [31]			
	Reference [33]			
	Reference [34]			
	Reference [35]			
7	Reference [36]	Reference [37]	Reference [38]	Reference [39]
				Reference [40]
				Reference [38]
8	Reference [41]	Reference [42]	Reference [43]	Reference [44]
	Reference [43]			
9		Reference [45]	Reference [46]	
10	Reference [47]		Reference [48]	
11	Reference [49]	Reference [50]		
12	Reference [51]			
13	Reference [52]			
	Reference [53]			
16			Reference [54]	Reference [55]
			Reference [56]	
17		Reference [57]		
18	Reference [58]		Reference [59]	
	Reference [60]			
22			Reference [61]	
55				Reference [62]

Threat perception and reaction time may vary from person to person [1]. It has been noted that threat prioritization may differ depending on the individual or geographical conditions, and that reaction time may vary [63]. This is due to factors such as the capacity, experience, knowledge base, length of hierarchical approval time, and delegation of authority of the individuals performing this task. It has been stated that a decision support system is needed to reduce the initial uncertainty in threat assessment and that priorities must be correctly identified for this purpose [64]. It has been stated that threat priority zones and threat priorities must be determined [65]. It has been stated that communication on the command and control network, the collection of air pictures and sensor information, weapon assignment compatibility, training, and simulation must be coordinated to provide weapon engagement control support [66]. It has been stated that in a combat environment where situational awareness is very difficult, threats can be quickly neutralized using artificial neural networks, fuzzy logic, and genetic algorithms [67]. It has been stated that the information necessary for threat assessment must be generated and collected on a network basis [68]. Threat assessment requires the identification of proximity, capability, and intent [69]. It has been stated that the rapid development of technology has led to new threats entering the war environment, that traditional methods attempted with hu-man capacity will be

insufficient, and that it is important to establish a network-centric artificial intelligence-supported decision support system [70]. In addition, there are studies in different fields conducted with image-based artificial neural networks [71]. It is also possible to establish a diagnostic model through the automatic evaluation of radar image traces in threat assessment.

Countries' perspectives on threats vary due to their geographical locations. While the US and China have global defense strategies based on big data and artificial intelligence, Türkiye and South Africa focus on operational speed and human-centered solutions, converting uncertain threat data into mathematical models using mobile systems and fuzzy logic. Germany and Sweden prepare for crisis situations with scenario-based training. Sweden prepares for the worst-case scenario by analyzing the maneuverability of the threat, Germany focuses on modular systems to minimize potential damage from threats, and South Africa focuses on data visualization to facilitate decision-making under stress. China aims to control the distributed structure with cloud-based systems and develops countermeasures against cyberattacks [2].

Some countries' perspectives on threats are summarized in Table 2.

Table 2. Perspectives on threats

Country	Mail approach	Priority capabilities	Technological focus
USA	Multi-layered defense and proactive deterrence.	Speed, range, stealth technology, cyber integration.	THAAD, Patriot systems, artificial intelligence.
Rusia	Hybrid warfare strategies and hypersonic missiles.	Hypersonic speed, electronic warfare, psychological impact.	S-400, S-500, Kinzhal hypersonic missile.
İsrael	Rapid response and high-accuracy defense.	Missile defense (Iron Dome), friend-or-foe identification, real-time data processing.	Iron Dome, Arrow missile system, artificial neural networks.
China	Asymmetric capabilities and space-based surveillance.	Long-range, anti-satellite weapons, unmanned aerial vehicles.	HQ-9, DF-21D, quantum radar.
Türkiye	Domestic defense industry and multi-purpose defense networks.	Air defense missile systems (HİSAR-SİPER), UAV-drone technology, logistical flexibility.	HİSAR-SİPER missile system, TB2, Anka3, Akıncı, Aksungur, Kızılelma.
France	NATO integration and nuclear deterrence.	Nuclear-tipped missiles, air superiority aircraft.	Rafale aircraft, Aster missile system.
North Korea	Weapons of mass destruction and psychological pressure.	Nuclear capacity, long-range missiles, low-cost unmanned vehicles.	Hwasong missile series, drone swarms.

When evaluating studies conducted in different countries within the scope of threat assessment, it has been noted that these studies require high costs, it is difficult to ensure consistency, sufficient data is not available, sufficient parameters cannot be selected, they may not be valid for a long period of time, the level of uncertainty is high, assumptions may not be applicable, there is a need for retraining, and the level of expert knowledge is limited. requiring a sufficient amount of simulation or test data beforehand, the possibility of some parameters being overlooked, and the system's potential sensitivity to interference [2].

Thirty-eight different criteria used in threat assessment have been identified in fifty-six different studies. The most frequently used criteria include distance from air defense systems, speed, altitude, direction, and target type. National perspectives also influence assessment priorities. While the US and China focus on big data and artificial intelligence, countries such as Türkiye and Israel emphasize operational speed and precision defense.

In studies conducted with artificial neural networks, very few criteria are taken into account, training rates between 60% and 95% yield good results, the learning rate between 10^{-2} and 10^{-4}, the mean squared error method is generally used, the number of hidden layers used as parameters varies between 1 and 50, different functions are used, and the number of iterations ranges from 20 to 5000.

In single-layer artificial neural networks, it has been stated that the number of layers in the layer must be one more than twice the number of inputs [72].

The lack of a universally adaptable model that can seamlessly integrate different methods and quickly adapt to the dynamic nature of air threats remains an ongoing challenge.

3. Methodology

3.1. Data collection and criteria selection

Twenty-six different criteria were identified that are most accessible, most frequently used in the literature, and allow for data imputation. The 223 target data points were compiled from the results tables of 56 studies shared in the literature. The frequency of use of the criteria used in the 56 different studies, their level of importance, the number of data points obtained from the literature, and the numbers of the criteria associated with the criteria obtained from expert opinions are shown in Table 3.

Table 3. Perspectives on threats (continued on next page)

Order	Criteria	Usage count	Importance level	Number of data points obtained	Related criteria
1	Distance to Air Defense System	49	0,133152	198	10-15-21
2	Speed	48	0,130435	218	5-6-13-18-21
3	Altitude	38	0,103261	208	5-6-18
4	Direction / dive angle	29	0,078804	116	10-18-21
5	Target type	27	0,073370	160	2-3-6-7-8-9-11-17-18-26
6	Flutter maneuver rate / number - climb rate / altitude change	19	0,051630	80	2-3-5
7	Damage capacity / mission type / combat capability / strike effectiveness	19	0,051630	20	5-11
8	Jamming capability	17	0,046196	126	5
9	Iff status	17	0,046196	71	5-13
10	Defended Element/Distance to Closest Approach Point to Air Defense System/Confrontation Status	13	0,035326	57	1-4
11	Type/Weight of Munitions carried by target	10	0,027174	25	5-7-17-21-26
12	Flight plan information - route status	8	0,021739	20	13
13	Intent	8	0,021739	26	2-9-12-19-20-22-24
14	Friendly Element Support / Engagement Status with Threat / Distance to Friendly Element / Within Range Status	8	0,021739	10	-
15	Engagement rule - political climate / within weapons envelope / within restricted area	8	0,021739	10	1
16	Threat uncertainty level/importance	8	0,021739	15	All
17	Target's weapon engagement distance	6	0,016304	28	5-11
18	Radar cross section	6	0,016304	49	2-3-4-5

19	Multiple Target Status/Target Protection Status/Number of Targets/Strike Size	6	0,016304	10	13
20	Target's fire control radar status	5	0,013587	20	13-24
21	Time Required to Hit Target / Target Arrival Time	5	0,013587	20	1-2-4-11
22	Probable Direction of Attack by Country / Approach Direction Status	4	0,010870	20	13
23	Weather conditions - visibility status	4	0,010870	10	-
24	Missile launch status	3	0,008152	10	13-20
25	Target airborne time	2	0,005435	5	-
26	Target maximum range	1	0,002717	20	5-11

When selecting the criteria to be used in the model, data determining the threat scores obtained based on the criteria calculated in the studies in the literature were taken into account. The data shared in the studies were compiled and used for training, testing, and validation data.

Criteria with no data were not considered. A total of 5,798 data points were compiled for 26 criteria for 223 different target situations. 1,552 data points were readily available, and the remaining 4,246 data points were created through data completion processes. A total of 223 output data points were also collected. Data and results from studies on threat assessment in the literature were compiled and used as training and test data. This aimed to show an average truth based on results obtained from different countries' perspectives.

3.2. Data preprocessing

When collecting data, numerical values were standardized by converting them to the same type (e.g., km/h was converted to m/s). “Unknown” was added to categorical data.

Twenty different target types were identified to standardize target type data, and thirty-eight experts were asked to prioritize engagement with twenty different targets simultaneously. The results revealed differing perspectives due to significant standard deviations in target prioritization. The average and median of the experts' target rankings were determined, along with the weight rankings of the targets. Mode values were not considered as they were not meaningful.

After all criterion data were collected and standardized, the criterion risk direction and the maximum and minimum value ranges of the criteria were determined. The number of criteria obtained for each target was determined.

Data completion has been performed according to priority and the relationship between criteria. While considering similar situations, the completion process was performed by looking at the most important and most da-ta-rich criteria in order. In the completion process, the average, median, or mode value was taken according to the status of the criterion for those with similar threat scores. A completion process specific to each criterion was performed in the completion of missing values.

For each missing criterion data point, data was obtained using the nearest cluster-based estimation method based on clusters created using the related criteria in the relationship network.

The algorithm steps are outlined below.

Step 1: Identify the criterion with the highest number of available data points.

Step 2: Sort the criteria linked to this criterion by order of importance.

Step 3: Filter out targets with missing data in the relevant criterion.

Step 4: Filter the linked criteria with the highest importance level. If there is no data, move on to the next criterion in order of importance. If there is no data in any of the linked criteria, return to Step 1 and move on to the next criterion.

Step 5: Filter the linked criterion value and surrounding data for all targets.

Step 6: If the criterion information is quantitative, take the average; if it is qualitative, take the median value. (Since the repetition of the same values is not very likely in such problems, the mode value is not meaningful.)

Step 7: Complete the missing data with this value.

Step 8: Return to Step 1 and move on to the other criterion. Continue until all table data is complete.

The normalization process was performed using the following formula. The x criterion value denotes the minimum value for the relevant criterion column, while max (x) denotes the maximum value for the relevant criterion value.

Minimum-Maximum Method; when the increase in risk and direction are linear;

$$z = \frac{x - min(x)}{max(x) - min(x)} \quad (1)$$

When the increase in risk and direction are not linear;

$$z = \frac{min(x) - x}{min(x) - max(x)} \quad (2)$$

One of the criteria, the threat uncertainty level, is calculated separately for each target after normalization based on the number of criteria for which information is available. Criteria for which information is unavailable increase the uncertainty level, and the uncertainty level increases the risk. The closer it is to 1, the greater the uncertainty and risk. This criterion is included in the threat assessment so that targets with low visibility and very little information obtained are not overlooked.

The normalization values were converted to a 1-10 scale using the x*9+1 transformation so that formula (3) below could be applied. The threat clarity level was calculated using this equation based on these values. It was calculated using the following formula based on how many data points were obtained without imputing missing data from twenty-five criteria (s of 25). $C_{ij} \epsilon [1,10]$ represents the j. criterion value of the i. target [73].

$$\text{Threat Clarity Level} = C_i = \frac{ln\left(\prod_{j=1}^{s} [\![C_{ij}) + 1]\!]\right)}{ln(10^s) + 1} = \frac{\sum_{j=1}^{s} ln(C_{ij}) + 1}{ln(10^s) + 1} \quad (3)$$

$$\text{Threat Uncertainty Level} = 1 - C_i \quad (4)$$

The Threat Uncertainty Level causing the increase in risk was determined by the conversion.

3.3. Threat score calculation

After all criteria values were determined, the weighted total threat score ($\mathbf{v}^{\wedge}$) was calculated based on the importance levels of the criteria. Since the average absolute error value (AAE) between the weighted total threat score and the threat scores compiled from the literature (**vj**) is close to zero, there is similarity.

$$AAE = \frac{\Sigma(Vj - V^{\wedge})}{n} = 0{,}03977141 \quad (5)$$

The relationship between the difference between the threat scores compiled from the literature at the outset and the weighted threat score obtained according to the importance levels of the criteria and the number of data obtained for each threat group is shown in Figure 1. As the number of data obtained increases, the difference tends to increase positively. However, since this difference is not a significant difference, the missing data completion process has yielded effective results.

Figure 1 shows that even after the missing data imputation process, the difference between the original threat scores in the literature and our calculated weighted scores is quite low (Mean Absolute Error = 0.039). This indicates that our imputation method produces reliable results without compromising data integrity.

The slight upward trend suggests that our model offers a slightly different (and possibly more accurate) perspective than the literature for targets with more comprehensive data.

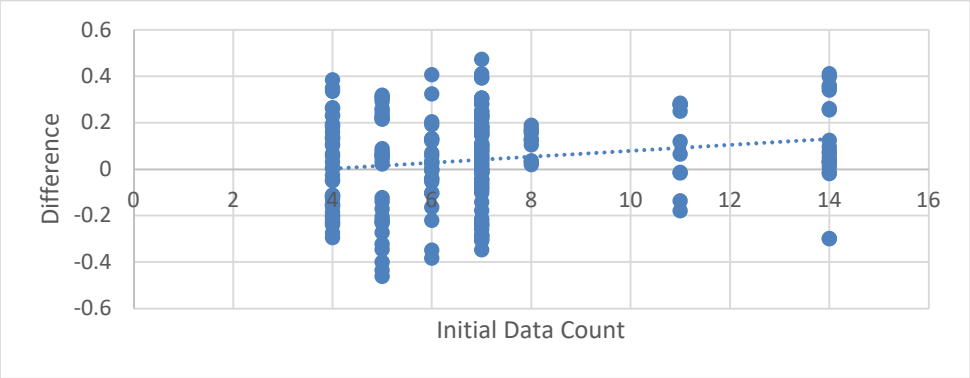

Figure 1. Difference between literature threat score and weighted threat score

To standardize the consistency between threat scores obtained from the literature and eliminate the positive effect of the new data table obtained through missing data imputation, the following process was performed to obtain a combined geometric threat score. The aim here is to reduce the tendency for change resulting from the missing data imputation process by bringing the threat score closer to the smaller value where the difference is large.

$$\text{Combined Geometric Threat Score (CGTS)} = \sqrt{\text{vj} * \text{v}^\wedge} \tag{6}$$

A Combined Geometric Threat Score has been proposed for use as training data in artificial neural networks. This reduces the impact of biased assessments that may arise from different sources.

3.4. Artificial neural network model

3.4.1. Layer structure

The basic architecture of the model consists of three layers;

Input layer: Normalized values of twenty-six criteria
Output layer: CGTS values
Hidden layer: The number of neurons is kept variable as a parameter.

The neuron outputs in the hidden layer are defined as follows. In equation (7), W_1 is the weight matrix, b_1 is the bias vector (which shifts the activation threshold of the neuron), and x is the input vector. The ReLU activation function introduces nonlinearity into the model. $h^{(1)}$ denotes the output of the first hidden layer.

$$h^{(1)} = ReLU(W_1 * x + b_1) \tag{7}$$

In equation (7), W_1 is the weight matrix and b_1 is the bias vector. The output layer is calculated as a linear combination. In equation (8), $h^{(2)}$ is the output of the second hidden layer. W_3 is the weight matrix of the output layer, b_3 is the bias vector of the output layer, and $y_{predict}$ is the result produced by the model. For the output layer;

$$y_{predict} = W_3 * h^{(2)} + b_3 \tag{8}$$

3.4.2. Activation function and learning algorithm

The Levenberg-Marquardt backpropagation algorithm was used to train the model. It is a hybrid algorithm that minimizes the error function using a combination of least squares, gradient descent, and Gauss-Newton methods. In equation (9), e is the error vector.

In equation (10), w_k is the weight vector at the k'th iteration, J is the Jacobian matrix (the derivative of the error terms with respect to the weights), I is the identity matrix, and μ is the damping coefficient.

$$e = y_i - f(x_i, w) \tag{9}$$

$$w_{k+1} = w_k - [J^T J + \mu I]^{-1} J^T * e \tag{10}$$

How the algorithm works:

• Initially, μ starts with a small value (e.g., 0.001).

• If the error decreases in the new iteration, μ is reduced, the algorithm behaves like Gauss–Newton (fast convergence).

• If the error increases, μ is increased, the algorithm behaves like gradient descent (more stable steps).

• In this way, μ is dynamically adjusted to reach the optimum point.

3.4.3. Performance function

Mean Square Error (MSE) was used for model performance. N is the total sample size. MSE is minimized throughout the training process. The $y_{real}^{(i)}$ value is the obtained CGTS value. The $f(x_i, w)$ value indicates the predicted value.

$$E(w) = \frac{1}{N}\sum_{i=1}^{N}[y_{real}^{(i)} - f(x_i, w)]^2 \quad (11)$$

N is the total sample size. MSE is minimized throughout the training process.

3.4.4. Training and testing processes

Data Split: Training, validation, and test data ratios were tested in different combinations. The training ratio was set to 70 % as recommended in the literature. Data was split randomly according to the specified ratios.

Batch Processing: Data was included in the training process in batches.

Number of Epochs: Early stopping was applied when training began to show overfitting to prevent overfitting.

Regularization Techniques:

Dropout: Specific neurons in the layers were randomly disabled.

L2 Regularization: L_{total} is the total loss value, the main error function. It includes both the model's error amount (L) and the regularization penalty shown in Equation (12). Mean squared error (MSE) is preferred for regression, while Cross Entropy Loss is preferred for classification. It measures the difference between the model's prediction and the actual value. λ is the regularization coefficient. It determines how much the weights are penalized. If λ is large, it reduces overfitting more, but the model becomes simpler.

If λ is small, the regularization effect decreases. $\sum\|W\|^2$ is the sum of the squares of all weights. The goal here is to make the model simpler and more generalizable by penalizing large weights.

$$L_{total} = L + \lambda\sum\|W\|^2 \quad (12)$$

Model performance was measured using test data not used in training, and CGTS values were compared with predicted values.

3.4.5. Threat assessment model flowchart

Step 1: Collecting sensor data in a standardized format

Step 2: Completing missing data and verifying information from different sensors, considering the criterion relationship network, starting with the criterion that yields the most data

Step 3: Performing normalization for twenty-five criteria

Step 4: Calculating the threat uncertainty level, which is the twenty-sixth criterion

Step 5: Obtaining results using the trained ANN model

4. Simulation and empirical results

The best results were obtained when the training rate was 70%, the validation rate was 10%, and the test rate was 20%. The mean square error ranged from 0.0005 to 0.0072, and the correlation coefficient (R) was 0.9617. These results show that the model predicts threat scores with high accuracy.

4.1. Training and test results

The dataset consists of two hundred twenty-three target sets. Each is a vector with twenty-six inputs. Figure 2 shows the training process of the proposed ANN architecture. In the first stage, a set of 223 targets with 26 inputs enters the 10-layer training process. A single result, the threat score, is obtained in the output layer.

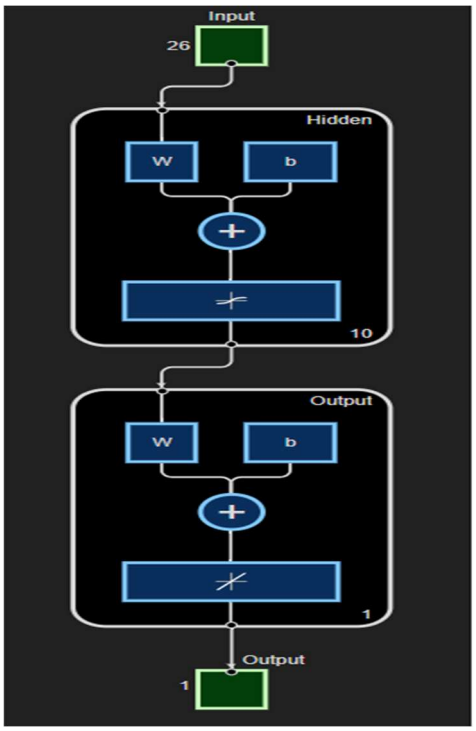

Figure 2. ANN Training Model

As shown in Figure 2, the ANN model we propose consists of an input layer with 26 neurons (representing normalized criteria), a hidden layer (with an optimal number of neurons set to 10), and an output layer that produces a single CGTS value. This architecture effectively processes multidimensional input data to learn complex, nonlinear relationships for threat assessment.

The results of the hidden layer number variation in the most successful cases within the training, validation, and testing results are shown in Table 4.

Table 4. Training and test results

Data distribution (Training / Validation / Test)	Hidden layer	MSE (Test)	R (Test)	Epochs
70 / 10 / 20	10	0.0025	0.9617	9
70 / 10 / 20	10	0.0027	0.9461	9
70 / 10 / 20	5	0.0060	0.8883	12
70 / 10 / 20	15	0.0049	0.9138	9

The results show that the ten-layer hidden model achieved an excellent balance between accuracy and efficiency on the test set with a high regression value ($R > 0.9617$) and low error ($MSE < 0.003$), and effectively generalized the data. Because the 10-layer hidden model provides an optimal balance between complexity and generalization, capturing the nonlinear features in the data while preventing overfitting. Performance results related to training, testing, error, and correlation are shown in Figure 3.

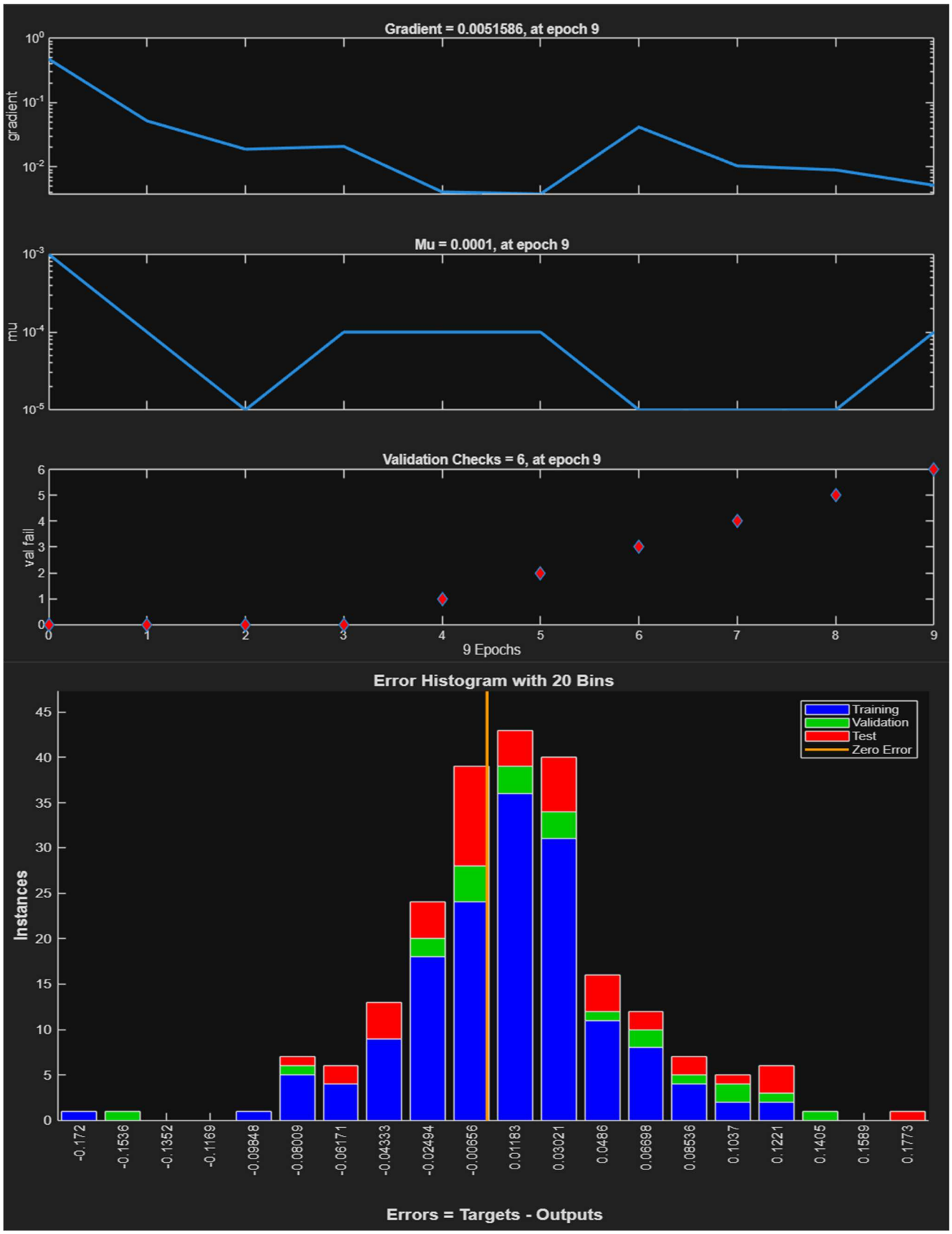

Figure 3. Performance Results

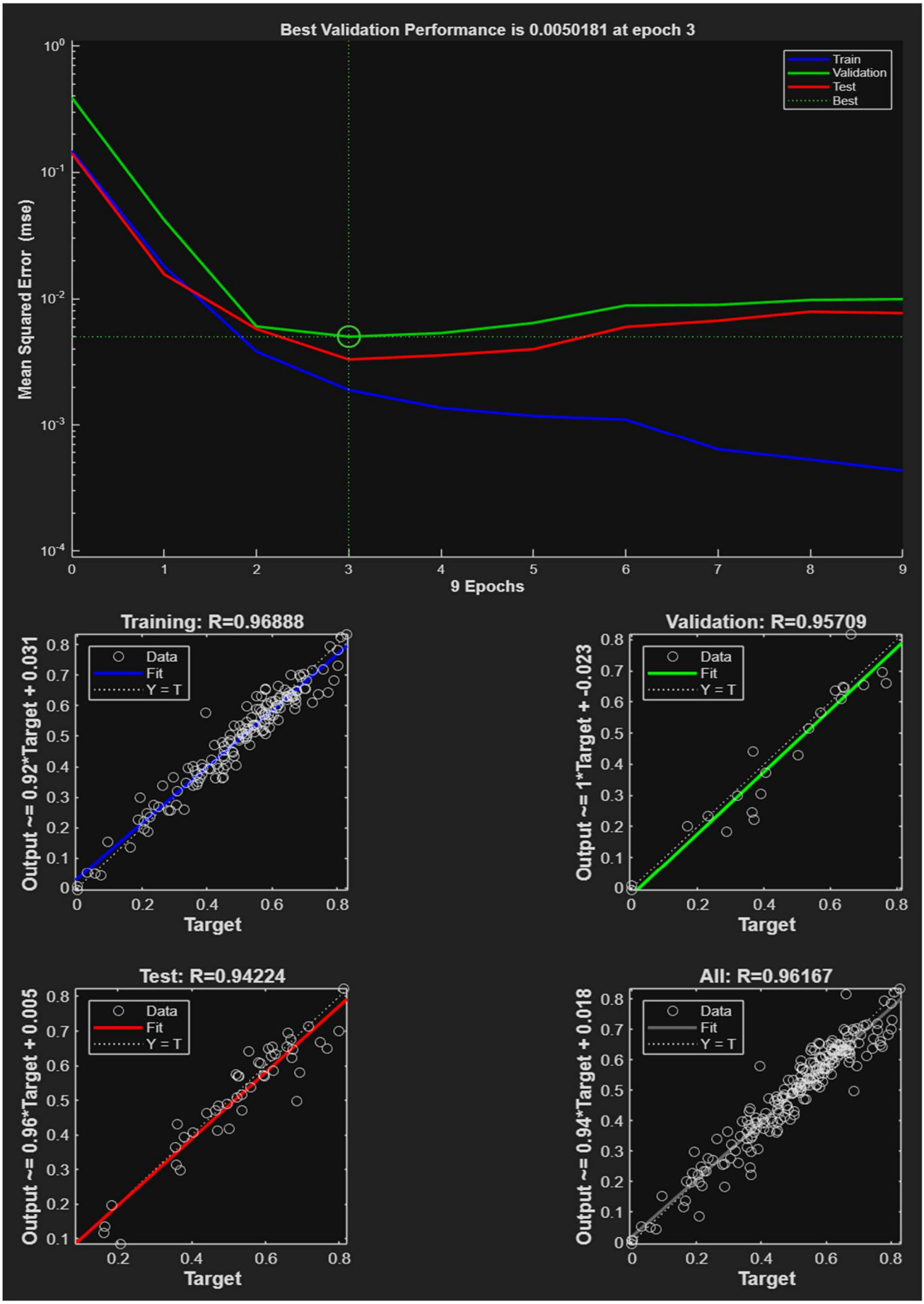

Figure 3. Performance Results (continued)

The performance results demonstrate that the model's training process is sound and successful. The graph in the upper left shows that all training, validation, and test errors have decreased and converged smoothly, indicating no significant overfitting. The error histogram (upper right) confirms the model's high accuracy by showing that most prediction errors cluster around zero. The regression plots for training, testing, and validation (below) show R values very close to 1 (0.96+). This strong linear relationship between the predicted and actual CGTS values across all data subsets confirms the model's generalization ability.

4.2. Comparative analysis

A comparison between this study and studies conducted with artificial neural networks in the literature is shown in Table 5.

Table 5. Comparison with studies in the literature

Studies	Model fitting	Number of data	Epoch number	Number of criteria
Reference [10]	-	-	-	3
Reference [6]	-	-	20	-
Reference [17]	-	1500	100	4
Reference [20]	0,0003	140	2100	4
Reference [55]	-	-	30 - 100 - 500 - 800	-
Reference [44]	0,0100	60	148	8
Reference [39]	-	100	30	7
Reference [24]	0,0010	336	30	5
Reference [21]	0,0100	75	-	4
Reference [38]	-	4000	20	-
Reference [74]	0,0010	100	150	-
Reference [63]	0,0010	600	5000	55
This study	0,0025	223	9	26

Compared to studies in the literature, more criteria were considered than in other studies. The success rate of stopping showed faster results than other studies due to the low number of epochs. Although the cell data was 223*26, which was more than others, it yielded effective results in a shorter time. This allows threat assessment to be performed in shorter periods according to changes in real-time threat data. The model validation yielded similar results. The model's efficiency is directly proportional to the number of data points and criteria and inversely proportional to the number of epochs and the model validation rate. Accordingly, efficiency was calculated using the following equation (13) and results are shown in Table 6.

$$Efficiency = \frac{Number\ of\ Data * Number\ of\ Criteria}{Epoch\ Number * Model\ Fitting} \quad (13)$$

Table 6. Efficiency

Studies	Efficiency
Reference [10]	-
Reference [6]	-
Reference [17]	-
Reference [20]	889
Reference [55]	-
Reference [44]	324
Reference [39]	-
Reference [24]	56000
Reference [21]	-
Reference [38]	-
Reference [74]	-
Reference [62]	6600
This study	26577

This metric is presented as an indicator of how much data complexity the model can process per unit learning cycle (epoch) and demonstrates that our work achieves higher learning efficiency compared to others.

When the same initial data is used to obtain the output with the artificial intelligence training model, the difference between the Combined Geometric Threat Score (CGTS) used in the training model and the Artificial Intelligence Threat Score has become quite close.

The difference trend depending on the number of initial data has been reduced. Thus, the quality of the training and test data has been improved, and the training model output has been ensured to provide very good results. This is shown in Figure 4.

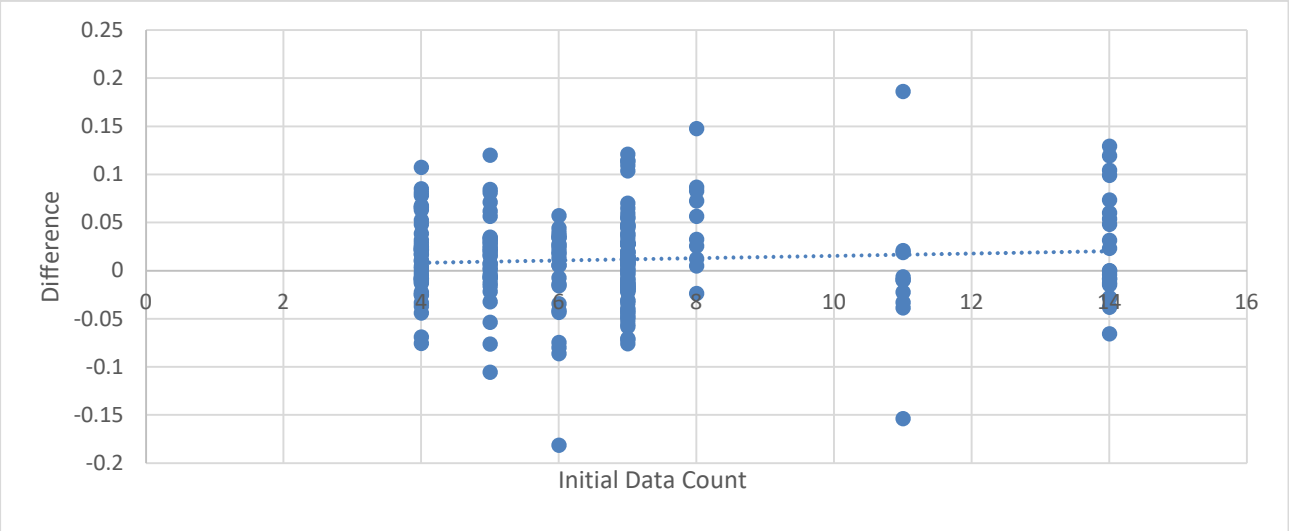

Figure 4: Difference between the Combined Geometric Threat Score and the Artificial Intelligence Threat Score

Figure 4 shows that the difference between the outputs of our trained ANN model (Artificial Intelligence Threat Score) and the target values used in training (Combined Geometric Threat Score - CGTS) is close to zero. This is the clearest evidence that our model has learned and can predict the CGTS with high accuracy. Furthermore, the difference trend observed in Figure 1, which was dependent on the initial number of data points, has been eliminated thanks to the trained model.

The artificial neural network training model has yielded results with a high accuracy rate. By providing an average view of threats, the impact varying by geography has been reduced. The criterion relationship network has ensured that the missing data completion process is performed correctly.
In future studies, threat-based assignment can enable air defense systems to engage automatically. The contribution of this study to the literature is the dynamic updating of the threat score using an artificial neural network and its integration with the missing data completion algorithm.

4.3. Simulation scenario

The training model was tested for five different targets, and sample simulation results are shown in Table 7. Missing values were completed using data imputation methods to obtain the threat score.

Table 7 presents an example of our model's performance for five different targets. For example, Target 3 (Bomber Aircraft) has been assessed as having the highest threat score (0,7303) due to its high ammunition capacity (8460) and low engagement distance (10).

In contrast, Target 4 (SEAD Aircraft), despite its high electronic warfare capability, received a relatively lower threat score (0,5904) due to its higher engagement distance (28). These results demonstrate that our model can perform realistic and interpretable threat prioritization by balancing different criteria.

The threat scores obtained can be used to prioritize automatic engagement by air defense systems.

Table 7. Simulation results

Order	Criteria	Target 1	Target 2	Target 3	Target 4	Target 5
1	Distance to Air Defense System					
2	Speed	315,9	275,4	267,3	305,1	280,8
3	Altitude	12500	11000	9500	10000	9500
4	Direction / dive angle	3,7912	24,024	0	24,8864	17,1136
5	Target type	Air Defence Fighter Aircraft	Air Defence Fighter Aircraft	Bomber Aircraft	SEAD Aircraft	SEAD Aircraft
6	Flutter maneuver rate / number - climb rate / altitude change	1,09	1,15	0,68	1,09	1,09
7	Damage capacity / mission type / combat capability / strike effectiveness					
8	Jamming capability	Negative	Negative	Positive (Low)	Positive (High)	Positive (High)
9	Iff status	Foe	Foe	Foe	Foe	Foe
10	Defended Element/Distance to Closest Approach Point to Air Defense System/Confrontation Status					
11	Type/Weight of Munitions Carried by Target	900	1816	8460	900	900
12	Flight plan information - route status	None	None	None	None	None
13	Intent					
14	Friendly Element Support / Engagement Status with Threat / Distance to Friendly Element / Within Range Status					
15	Engagement rule - political climate / within weapons envelope / within restricted area					
16	Threat uncertainty level/importance	0,6109	0,6037	0,5741	0,6098	0,5711
17	Target's weapon engagement distance	15	15	10	28	28
18	Radar cross section					
19	Multiple Target Status/Target Protection Status/Number of Targets/Strike Size					
20	Target's fire control radar status	Active	Active	Active	Inactive	Active
21	Time Required to Hit Target / Target Arrival Time	1	15	1	5	1
22	Probable Direction of Attack by Country / Approach Direction Status	1 (%30)	2 (%50)	1 (%30)	3 (%80)	3 (%80)
23	Weather conditions - visibility status					
24	Missile launch status					
25	Target airborne time					
26	Target maximum range	3000	2900	1100	3000	3000
	Threat Score	**0,6380**	**0,6318**	**0,7303**	**0,5904**	**0,6279**

5. Conclusions

The results obtained show similar error rates when compared to those reported in studies in the literature. Furthermore, results can be achieved with fewer iterations based on the amount of data. This proves that the model's missing data completion and dynamic learning features are effective. Furthermore, recalculating the threat score using the geometric mean method has increased the model's generalization ability. Thus, a high-quality training set has been created. This approach has successfully reduced the “human factor” variability mentioned in studies such as [1] and [62] and provided a consistent and automatic basis for evaluation.

The model has been trained using simulated and literature-derived data; its response to noisy and incomplete data in a real-time combat environment has not yet been fully tested.

From a practical perspective, real-time analysis, error reduction, and scalability are the model's strengths. However, due to the black-box nature of artificial neural networks, data dependency that changes with new technologies and vulnerability to cyberattacks should be addressed as weaknesses in operational applications.

Most existing studies are static in nature and cannot adapt to changing threat conditions. Therefore, the integration of artificial neural networks with dynamic learning capabilities into the threat assessment process fills an important gap in the literature. There is a significant gap in the development of both dynamic and adaptive models. Many systems rely on static rules or require extensive datasets that are often confidential for training, which limits their practical applications and adaptability to new threat profiles.

This study addresses this gap by proposing a hybrid methodology that synthesizes historical information in the literature with the adaptive learning capabilities of ANNs. The main contributions of this article are as follows:

The criteria used in fifty-six different studies in the literature were compiled and standardized, taking into account frequency of use, and data standardization was achieved.

Depending on the connection between the criteria examined for threats, the relationship network was revealed for the first time, and missing data completion processes related to the relationship network were performed. Thus, a comprehensive threat assessment data set consisting of 26 criteria was created. The missing data completion algorithm solves the problem of combining and making usable the limited and scattered data sets in the literature.

An innovative approach to calculating the Combined Geometric Threat Score has been proposed to generate reliable training, testing, and validation data. CGTS neutralizes biased threat scores from different studies, creating a more reliable target variable.

An ANN model that accurately predicts threat scores and demonstrates high performance and generalizability in different validation scenarios has been designed and validated (R=0,96). The proposed model aims to provide fundamental validation for next-generation, network-centric air defense systems capable of real-time, intelligent threat assessment.

This study has developed a dynamic and learning artificial neural network model for the threat assessment process in air defense systems. The model successfully predicts threat scores by integrating data from different sources. The contribution of this study to the literature is the dynamic updating of the threat score using an artificial neural network, its integration with an incomplete data completion algorithm, the proposal of the CGTS formulation offering a generalizable perspective, and the provision of an effective training dataset.

The proposed dataset, application strategy, and CGTS formulation will be made publicly available after acceptance to support reproducibility and further research.

In future studies, testing the model with real-time radar data, comparing it with deep learning architectures, integrating it with automatic weapon assignment modules, applying and testing the model in a high-accuracy simulation environment, and evaluating its performance under realistic, dynamic combat conditions will be possible.

The problem areas will be protecting data privacy, sending real-time sensor information without exposure to interference, excessive compliance risk, and cybersecurity risk.

Within the scope of operational implementation, software integration into command and control systems will be required. There is a possibility of delays in the radar and air defense systems loop cycle. All sensor transmission systems must be interoperable.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] C. C. Jorgensen and M. H. Strub, *Analysis of Manual Threat Evaluation and Weapon Assignment (TEWA) in the AN/TSQ-73 Air Defense System*, U.S. Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, USA, Tech. Rep. 1246, 1979.

[2] A. Naseem, S. T. H. Shah, S. A. Khan, and A. W. Malik, "Decision support system for optimum decision-making process in threat evaluation and weapon assignment: Current status, challenges and future directions," *Annual Reviews in Control*, vol. 43, pp. 203–220, 2017. https://doi.org/10.1016/j.arcontrol.2017.03.003

[3] S. Paradis, A. Benaskeur, M. Oxenham, and P. Cutler, "Threat evaluation and weapons allocation in network-centric warfare," in *Proc. 7th Int. Conf. Information Fusion (FUSION)*, Philadelphia, PA, USA, 2005. https://doi.org/10.1109/ICIF.2005.1591942

[4] A. Dahlbom and T. Helldin, "Supporting threat evaluation through visual analytics," in *Proc. IEEE Int. Multi-Disciplinary Conf. Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, San Diego, CA, USA, pp. 155–162, 2013. https://doi.org/10.1109/CogSIMA.2013.6523924

[5] H. Naeem, A. Masood, M. Hussain, and S. A. Khan, "A novel two-staged decision support based threat evaluation and weapon assignment algorithm," *Int. J. Computer Science and Information Security*, vol. 2, no. 1, 2009.

[6] M. K. Allouche, "Real-time use of Kohonen's self-organizing maps for threat stabilization," *Information Fusion*, vol. 6, no. 2, pp. 153–163, 2005. https://doi.org/10.1016/j.inffus.2004.06.004

[7] R. L. Carling, "A knowledge-base system for the threat evaluation and weapon assignment process," *Naval Engineers Journal*, vol. 105, no. 3, pp. 91–101, 1993. https://doi.org/10.1111/j.1559-3584.1993.tb02732.x

[8] N. Okello and G. Thoms, "Threat assessment using Bayesian networks," in *Proc. 6th Int. Conf. Information Fusion (FUSION)*, Cairns, QLD, Australia, pp. 1102–1109, 2003.

[9] L. Wang, Z. G. Liu, and W. Wang, "Aerial target threat evaluation method," *Advances in Engineering Research*, vol. 117, pp. 1014–1017, 2016. https://doi.org/10.2991/mme-16.2016.168

[10] A. X. Dong and L. G. Qing, "Application of neural network in the field of target threat evaluation," in *Proc. IEEE Int. Conf. Intelligent Processing Systems*, pp. 586–589, 1999. https://doi.org/10.1109/ICIPS.1999.814343

[11] J. Zhu *et al*., "Mastering air combat game with deep reinforcement learning," *Defence Technology*, vol. 34, pp. 295–312, 2024. https://doi.org/10.1016/j.dt.2023.08.019

[12] H. Rizwan, S. Tayyaba, M. W. Ashraf, H. Rasheed, and Z. Ahmed, "Threat evaluation of suspicious target for cognitive radar," in *Proc. IEEE 17th Int. Multi-Topic Conf. (INMIC)*, pp. 176–181, 2014. https://doi.org/10.1109/INMIC.2014.7072461

[13] Z. Genyuan, L. Zhiwei, Z. Zhipeng, and B. Zhipeng, "Research on time compensation of cooperative tracking for UAVs swarm," in *Proc. 7th World Conf. Computer Communication Technology*, 2024.

[14] F. Beser, D. Adıgüzel, Ö. Yıldırım, and T. Yıldırım, "Bulanık mantık kullanarak hava savunma karar destek sistemi tasarımı," *Akıllı Sistemler ve Uygulamaları Dergisi*, vol. 1, no. 2, pp. 135–139, 2018.

[15] J. N. Roux and J. H. van Vuuren, "Real-time threat evaluation in a ground based air defence environment," *ORiON*, vol. 24, no. 1, pp. 75–101, 2008. https://doi.org/10.5784/24-1-61

[16] L. G. Chen, Y. Zhang, and X. L. Liu, "Analysis of multi aerial targets threaten degree on terminal defense system," in *Proc. Int. Conf. Computer Information Systems and Industrial Applications (CISIA)*, 2015. https://doi.org/10.2991/cisia-15.2015.191

[17] M. Azak and A. E. Bayrak, "A new approach for threat evaluation and weapon assignment problem, hybrid learning with multi-agent coordination," in *Proc. 23rd Int. Symp. Computer and Information Sciences (ISCIS)*, pp. 1–6, 2008. https://doi.org/10.1109/ISCIS.2008.4717937

[18] T. Ö. Ülten, "Hava hedefleri için bulanık mantık ile tehdit algılama ve silah atama algoritması geliştirilmesi," M.S. thesis, Gazi Univ., Ankara, Turkey, 2022.

[19] W. Xingyu *et al*., "Integrated threat assessment method of beyond-visual-range air combat," *Journal of Systems Engineering and Electronics*, vol. 36, no. 1, pp. 176–193, 2025. https://doi.org/10.23919/JSEE.2025.000017

[20] H. Lee *et al*., "Threat evaluation of enemy air fighters via neural network-based Markov chain modeling," *Knowledge-Based Systems*, vol. 116, pp. 49–57, 2017. https://doi.org/10.1016/j.knosys.2016.10.026

[21] L. Sheng *et al*., "Target threat assessment in air combat with BP neural network for UAV," *Journal of Physics: Conference Series*, vol. 2506, no. 1, p. 012010, 2022. https://doi.org/10.1088/1742-6596/2506/1/012010

[22] T. Helldin *et al*., "Transparency of military threat evaluation through visualizing uncertainty and system rationale," in *Proc. 4th Int. Conf. Advanced Cognitive Systems*, 2013. https://doi.org/10.1007/978-3-642-39056-2_30

[23] Q. Changwen and H. You, "A method of threat assessment using multiple attribute decision making," in *Proc. 6th Int. Conf. Signal Processing*, vol. 2, pp. 1091–1095, 2002. https://doi.org/10.1109/ICOSP.2002.1180017

[24] X. Ximeng *et al*., "Threat assessment in air combat based on ELM neural network," in *Proc. IEEE Int. Conf. Artificial Intelligence and Computer Applications (ICAICA)*, pp. 491–494, 2019. https://doi.org/10.1109/ICAICA.2019.8873966

[25] S. Haiwen and X. Xiaofang, "Threat evaluation method of warships formation air defense based on AR(p)-DITOPSIS," *Journal of Systems Engineering and Electronics*, vol. 30, no. 2, pp. 297–307, 2019. https://doi.org/10.21629/JSEE.2019.02.08

[26] H. Naeem and A. Masood, "An optimal dynamic threat evaluation and weapon scheduling technique," *Knowledge-Based Systems*, vol. 23, no. 4, pp. 337–342, 2010. https://doi.org/10.1016/j.knosys.2010.01.002

[27] K. Kalcı, "Gemi savunma sistemlerinde tehdit değerlendirme ve silah atama uygulamaları," M.S. thesis, Ankara Univ., Ankara, Turkey, 2008.

[28] L. Feng, Q. Xue, and M. Liu, "Threat evaluation model of targets based on information entropy and fuzzy optimization theory," in *Proc. IEEE Int. Conf. Industrial Engineering and Engineering Management (IEEM)*, pp. 1789–1793, 2011. https://doi.org/10.1109/IEEM.2011.6118224

[29] H. Li, R. Song, and B. Liu, "Air attack target threat assessment based on combination weighting," *Int. J. Advanced Network Monitoring and Controls*, vol. 7, no. 2, pp. 60–68, 2022. https://doi.org/10.2478/ijanmc-2022-0017

[30] C. Dongfeng, F. Yu, and L. Yongxue, "Threat assessment for air defense operations based on intuitionistic fuzzy logic," *Procedia Engineering*, vol. 29, pp. 3302–3306, 2012. https://doi.org/10.1016/j.proeng.2012.01.484

[31] M. Coşkun, "Hava savunma sistemlerinde bulanık mantık tabanlı tehdit değerlendirmesi ve derecelendirmesi," M.S. thesis, Selçuk Univ., Konya, Turkey, 2021.

[32] M. Coşkun, "Hava savunma sistemlerinde bulanık mantık tabanlı tehdit değerlendirmesi ve derecelendirmesi," M.S. thesis, Selçuk Univ., Konya, Turkey, 2021.

[33] M. Öztürk, "Hava savunma sistemlerinde çok kriterli karar verme yöntemleri kullanılarak tehdit değerlendirme," M.S. thesis, Selçuk Univ., Konya, Turkey, 2024.

[34] Ö. Tuncer and H. A. Çırpan, "Target priority based optimisation of radar resources for networked air defence systems," *IET Radar, Sonar & Navigation*, vol. 16, no. 7, pp. 1212–1224, 2022. https://doi.org/10.1049/rsn2.12255

[35] M. Coşkun and S. Taşdemir, "Fuzzy logic based threat assessment application in air defense systems," *IEEE Trans. Aerospace and Electronic Systems*, 2022. https://doi.org/10.1109/TAES.2022.3168853

[36] X. T. Nguyen *et al*., "A target threat assessment method for application in air defense command and control systems," *J. Russian Universities Radioelectronics*, vol. 26, no. 3, pp. 90–98, 2023. https://doi.org/10.32603/1993-8985-2023-26-3-90-98

[37] R. Zhao *et al*., "Dynamic air target threat assessment based on interval-valued intuitionistic fuzzy sets, game theory, and evidential reasoning methodology," *Mathematical Problems in Engineering*, vol. 2021, Art. no. 6652706, 2021. https://doi.org/10.1155/2021/6652706

[38] X. T. Nguyen, "Threat assessment in tactical airborne environments," in *Proc. 5th Int. Conf. Information Fusion (FUSION)*, 2002. https://doi.org/10.1109/ICIF.2002.1020935

[39] R. Song *et al*., "Air target threat assessment: A kernel extreme learning machine based on a multistrategy improved sparrow search algorithm," *Mathematical Problems in Engineering*, vol. 2023, Art. no. 1315506, 2023. https://doi.org/10.1155/2023/1315506

[40] L. Yue *et al*., "Air target threat assessment based on improved moth flame optimization-gray neural network model," *Mathematical Problems in Engineering*, vol. 2019, Art. no. 4203538, 2019. https://doi.org/10.1155/2019/4203538

[41] Ö. Tuncer, *Hava Savunma Sistemleri için Makine Öğrenme Yöntemleri Kullanılarak Hedef Sınıflandırma Uygulaması*, Savunma Sistem Teknolojileri Sektör Başkanlığı, Ankara, Turkey, Tech. Rep., 2018.

[42] M. Riveiro *et al*., "Towards future threat evaluation systems: User study, proposal and precepts for design," in *Proc. 16th Int. Conf. Information Fusion (FUSION)*, Istanbul, Turkey, pp. 1863–1870, 2013.

[43] S. Kumar and B. K. Tripathi, "Modelling of threat evaluation for dynamic targets using Bayesian network approach," *Procedia Technology*, vol. 24, pp. 1268–1275, 2016. https://doi.org/10.1016/j.protcy.2016.05.109

[44] W. Bi *et al*., "Threat assessment method for air defense of warship based on variable weight intuitionistic fuzzy technique for order preference by similarity to ideal solution," *The Aeronautical Journal*, 2024. https://doi.org/10.1017/aer.2024.12

[45] H. Yang, C. Han, and C. Tu, "Air targets threat assessment based on BP-BN," *Journal of Communications*, vol. 13, no. 1, pp. 38–43, 2018. https://doi.org/10.12720/jcm.13.1.38-43

[46] F. Johansson and G. Falkman, "A Bayesian network approach to threat evaluation with application to an air defense scenario," in *Proc. 11th Int. Conf. Information Fusion (FUSION)*, Cologne, Germany, 2008. https://doi.org/10.1109/ICIF.2008.4632313

[47] D. Yu *et al*., "PROMETHEE-based multi-AUV threat assessment method using combinational weights," *Journal of Marine Science and Engineering*, vol. 11, no. 7, p. 1422, 2023. https://doi.org/10.3390/jmse11071422

[48] X. Liu *et al*., "Threat evaluation of air targets based on the generalized Shapley Choquet integral of GIFSS," *Aerospace*, vol. 8, no. 5, p. 144, 2021. https://doi.org/10.3390/aerospace8050144

[49] A. Naseem, A. Ahsan, and M. Mahmood, "A logistic provider threat evaluation and weapon selection using analytical hierarchy process," in *Proc. IEEE Int. Conf. Technology Management and Operational Decisions (ICTMOD)*, 2025.

[50] E. Azmirad and J. Haddadnia, "Target threat assessment using fuzzy sets theory," *Advances in Intelligent Information*, vol. 1, no. 2, pp. 57–74, 2015.

[51] J. F. B. Brancalion and K. H. Kienitz, "Threat evaluation of aerial targets in an air defense system using Bayesian networks," in *Proc. IEEE 15th Int. Conf. Dependable, Autonomic and Secure Computing*, pp. 490–497, 2017. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.92

[52] J. Yun, S. S. Hong, and M. M. Han, "Dynamic neuro fuzzy knowledge based system in threat evaluation," in *Proc. Joint 6th Int. Conf. Soft Computing and Intelligent Systems (SCIS)*, pp. 1762–1765, 2012. https://doi.org/10.1109/SCIS-ISIS.2012.6424578

[53] A. Benavoli *et al*., "An approach to threat assessment based on evidential networks," in *Proc. 10th Int. Conf. Information Fusion (FUSION)*, 2007. https://doi.org/10.1109/ICIF.2007.4408157

[54] A. Benavoli *et al*., "An application of evidential networks to threat assessment," *IEEE Trans. Aerospace and Electronic Systems*, vol. 45, no. 2, pp. 620–639, 2009. https://doi.org/10.1109/TAES.2009.5089064

[55] S. Ünver, "Threat evaluation in air defense systems using analytic network process," M.S. thesis, Galatasaray Univ., Istanbul, Turkey, 2015.

[56] R. Di *et al*., "A threat assessment method for unmanned aerial vehicle based on Bayesian networks under the condition of small data sets," *Mathematical Problems in Engineering*, vol. 2018, Art. no. 8484358, 2017. https://doi.org/10.1155/2018/8484358

[57] S. Ünver and T. Gürbüz, "Threat evaluation in air defense systems using analytic network process," *Journal of Military and Strategic Studies*, vol. 19, no. 4, 2019.

[58] A. Naseem, S. A. Khan, and A. W. Malik, "Real-time decision support system for resource optimization and management of threat evaluation and weapon assignment in air defense," in *Proc. IEEE Int. Conf. Industrial Engineering and Engineering Management (IEEM)*, pp. 565–569, 2014. https://doi.org/10.1109/IEEM.2014.7058694

[59] M. Liebhaber and B. Feher, *Air Threat Assessment: Research, Model, and Display Guidelines, and Human Systems*, SPAWAR Systems Center, San Diego, CA, USA, Tech. Rep. 1877, 2002.

[60] A. Naseem and Y. Ahmad, "Critical success factors for neutralization of airborne threats," *SAGE Open*, vol. 10, no. 3, 2020. https://doi.org/10.1177/2158244020963066

[61] Y. Liang, "An approximate reasoning model for situation and threat assessment," in *Proc. 4th Int. Conf. Fuzzy Systems and Knowledge Discovery (FSKD)*, pp. 317–321, 2007. https://doi.org/10.1109/FSKD.2007.350

[62] M. Liebhaber and C. A. P. Smith, "Naval air defense threat assessment: Cognitive factors and model," in *Proc. 5th Int. Command and Control Research and Technology Symp. (ICCRTS)*, Canberra, Australia, 2000.

[63] P. Zhang *et al*., "A systematic effectiveness evaluation method for air defense operations based on deep confidence networks," *Applied Sciences*, vol. 14, no. 4, 2024. https://doi.org/10.3390/app14041452

[64] M. Riveiro *et al*., "Effects of visualizing uncertainty on decision-making in a target identification scenario," *Computers & Graphics*, vol. 45, pp. 84–98, 2014. https://doi.org/10.1016/j.cag.2014.08.005

[65] J. Holt, “Assessing the need for decision support systems,” *European Journal of Operational Research*, vol. 37, no. 1, pp. 73–82, 1988. https://doi.org/10.1016/0377-2217(88)90280-3

[66] J. D. Pantaleon, “A way to control medium and low range weapons systems in an air defense artillery command and control system,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2000.

[67] T. F. Iversen, “Mobile and netted air defense systems,” in *Proc. RTO SCI Symp. Integrated Air Defense for Multinational Mobile Crisis Reaction Forces*, Valencia, Spain, pp. 1–11, 2000.

[68] U. Krogmann, “Distribution of intelligence in airborne air-defense mission systems,” in *Proc. RTO SCI Symp. Integrated Air Defense for Multinational Mobile Crisis Reaction Forces*, Valencia, Spain, pp. 2–12, 2000.

[69] A. Claire and B. Brisset, “Ontological engineering for threat evaluation and weapon assignment: A goal-driven approach,” in *Proc. 9th Int. Conf. Information Fusion (FUSION)*, Florence, Italy, 2006. https://doi.org/10.1109/ICIF.2006.301569

[70] M. L. Truter and J. H. van Vuuren, “Prerequisites for the design of a threat evaluation and weapon assignment system evaluator,” in *Proc. ORSSA Annual Conf.*, pp. 54–61, 2014.

[71] K. Goztepe, V. Dizdaroglu, and S. Sagiroglu, “New directions in military and security studies: Artificial intelligence and military decision making process,” *Int. J. Information Security Science*, vol. 4, no. 2, pp. 48–56, 2015.

[72] J. Zhou *et al*., “Graph neural networks: A review of methods and applications,” *AI Open*, vol. 1, pp. 57–81, 2020. https://doi.org/10.1016/j.aiopen.2021.01.001

[73] A. N. Kolmogorov, “On the representation of continuous functions of several variables by superposition of continuous functions of one variable and addition,” *Doklady Akademii Nauk SSSR*, vol. 114, no. 5, pp. 953–956, 1957.

[74] J. P. Yang, J. Wang, and W. T. Liang, “Research on method of the threaten queuing based on anti-missile,” *Journal of China Academy of Electronics and Information Technology*, vol. 7, no. 4, pp. 432–436, 2012.

[75] S. Li *et al*., “Weapon-target assignment strategy in joint combat decision-making based on multi-head deep reinforcement learning,” *IEEE Access*, vol. 11, pp. 109281–109295, 2023. https://doi.org/10.1109/ACCESS.2023.3324193