TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

EMERGING AND DISRUPTIVE TECHNOLOGIES: AN EXPLORATION OF AI-POWERED WARGAMING AND PREDICTIVE MODELING IN MILITARY DECISION-MAKING

Marin-Marian COMAN, Claudiu-Vasile KIFOR

Abstract: *The unstable contemporary environment, characterized by numerous crises and conflicts demanding effective intelligence gathering and great coordination of military forces and capabilities during military operations across land, sea, air, space, and cyberspace, is a challenge for every commander and leading staff. The implementation of Emerging and Disruptive Technologies (EDTs) particularly Artificial Intelligence (AI), as an enabler during wargaming, could augment and transform the manner in which trainees and decision makers conduct training and prepare strategic decisions. Employing the Weka platform, this article explores the role of AI as a supporting tool during wargaming vignettes and clarifies how machine learning (ML) algorithms anticipate threats and enhance decision-making, enabling more flexible and adaptable military forces and capabilities in today's contested environment.*

Keywords: *wargaming, military decision-making, artificial intelligence, machine learning, predictive modeling, threat assessment*

1. INTRODUCTION

The convergence of cyber and physical threats in modern warfare necessitates advanced training environments that replicate the uncertainty and complexity of contemporary battlefields, where multidomain operations must be conducted. The contemporary security landscape is characterized by increasing volatility, uncertainty, complexity, and ambiguity, driven largely by the advancements and proliferation of EDTs. The rapid employment of new technologies in many activity domains is aligned with the new and actual framework: today's security environment is brittle (fragile systems that fail unpredictably), anxious (heightened human and institutional stress), nonlinear (small changes produce disproportionate effects in time), and incomprehensible (complex dynamics that resist clear understanding) – a condition amplified by the rapid spread and implementation of EDTs.

The employment of particular EDTs as tools for training, such as AI used in scenarios specific to multidomain operations and contested environments, is a new facet of AI implementation in military education and training processes. Through wargaming and the implementation of AI and other types of EDTs, the armed forces can achieve a significant strategic advantage, thereby enabling them to reach their training objectives. This study aims to explore and provide a framework for transforming military training and strategic decision-making through the implementation of AI-powered wargaming vignettes.

Wargaming has long been a foundational tool for military education and strategic planning. Military leaders and planners use wargaming to test and evaluate concepts and technologies in a controlled environment. Peter Perla defines wargames as warfare models and simulations whose operation does not involve the activities of actual military forces and whose sequence of events is impacted by the decisions made by other players on the other

side of the table. There are two teams in every wargame, with each side seeking to defeat the other with the capabilities at their disposal [1].

The importance of training through specific, tailored wargaming vignettes in NATO and allied nations has been proven by numerous publications and training events. A series of professional wargaming handbooks have been published, including the US Navy's Wargaming Handbook, the US Army War College Strategic Wargaming Series Handbook, the UK's Ministry of Defence Wargaming Handbook, the German Army Handbook, and the Polish Wargaming Handbook [2].

Machine learning (ML), a subset of AI, enables computers to analyze data and decide what information is most relevant, facilitating fast and accurate decision making [3]. Military organizations worldwide are actively seeking to integrate these technologies into their training and operations to enhance situational awareness and predictive capabilities [4].

With the capability to analyze extensive volumes of data and predict future outcomes, AI is increasingly being used as an indispensable tool for predictive modeling and resource optimization. AI-powered wargaming for the military decision-making process represents a significant advancement in strategic planning and tactical analysis. This training framework leverages AI to process vast amounts of data, simulate complex scenarios, and provide insights that may not be immediately apparent to human analysts. By incorporating ML algorithms and real-time data analysis, AI-powered wargaming platforms can adapt to dynamic battlefield conditions and offer commanders a broad range of strategic options.

In the context of defense, AI applications range from autonomous logistics and maintenance prediction to autonomous weapons systems and intelligence analyses [5]. ML algorithms are particularly valuable because of their ability to process vast amounts of sensor data and identify correlations that indicate enemy intent or capability [6]. Awan A. explains in "What is Online Machine Learning?" that a ML algorithm is a specific type of AI that is fed by a stream of data from which the model incrementally learns and adapts over time in an iterative and dynamic process [7].

The Military Decision-Making Process (MDMP) – the US Army's standard analytical framework for operational planning – has been identified as a natural integration point for AI-enabled tools. As argued in the "Artificial Intelligence-Enabled Military Decision-Making Process" by Gallitelli V., the AI techniques, including supervised classifiers, can enhance each phase of the MDMP, from mission analysis and intelligence preparation of the battlefield to course of action (COA) development and decision briefing [8]. Adler J. demonstrated in an analysis published by the Army University Press how predictive algorithms trained on operational data can forecast enemy movements, identify high-payoff targets, and accelerate the COA comparison process [9].

2. METHODOLOGY AND MATERIALS USED IN THE PROPOSED ANALYSIS FRAMEWORK

To investigate the usefulness of AI in military wargaming, this study employed a quantitative experimental design using the Weka (Waikato Environment for Knowledge Analysis) machine-learning platform. To explore the use of AI as an enabler during wargaming vignettes, we established a suitable training framework linked to a contested environment in which the analysis of information from the INTEL gathering process is paramount to detecting future threats. A short fictional wargaming scenario called "Operation CyberShield200" was created as a narrative framework that demands a hybrid approach by having specific actors act as Blue Forces (good guys) and Red Forces (bad guys), employing new technologies. In addition, a dataset was created to replicate events or actors and describe the real effects in the actual contested environment. The dataset was then uploaded to Weka version 3.8, to be tested and analyzed using RandomForest as the main ML algorithm. Finally, the results were interpreted after running the ML algorithm.

Weka is a widely used, open-source, Java-based ML software developed by the

University of Waikato that provides a suite of tools for data preprocessing, classification, regression, clustering, association rule mining, and visualization [10]. It is designed for data mining tasks and is often used in academia and industry. The RandomForest ML algorithm is an ensemble learning method that operates by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes (classification) of the individual trees [11]. RandomForest is a supervised-learning ML algorithm. The "forest" it builds is an ensemble of decision trees, usually trained using the bagging method. The general idea of the bagging method is that a combination of learning models increases the overall result [12]. This ML algorithm could help analysts understand which indicators are most predictive of an attack, being particularly suitable for military datasets (INTEL feed) because it reduces the risk of overfitting associated with individual decision trees and provides a measure of feature importance.

The core of the research methodology involved a predictive modeling framework through the generation of a representative dataset and the training of the RandomForest ML classifier to predict future risks and threat levels during wargaming vignette. Predictive modeling involves the use of statistical techniques and machine learning to predict future outcomes based on historical data [13]. Gartner defines predictive modeling as a commonly used statistical technique for predicting future behavior. Predictive modeling solutions are a form of data mining technology that work by analyzing historical and current data and generating a model to help predict future outcomes [14]. By leveraging predictive analytics, military planners can foresee emerging threats and evaluate the consequences of various courses of action with higher precision.

This study focused on the research objectives at the intersection of AI, wargaming, and decision support within a fictional scenario to answer the following research questions:

RQ1: Can AI-powered wargaming vignettes provide a realistic training contested environment for military decision-making?

RQ2: Can predictive modeling support and enhance military decision-making in an unstable contemporary environment?

2.1 Wargaming Fictional Scenario Setup

The proposed fictional scenario involves all relevant actors suitable for wargaming vignettes and pertains to a contested environment characterized by competition, scarce resources, geopolitical tensions, and rapidly evolving technological advancements [15]. Generally, a contested environment is a geographical, cyber, or electromagnetic space (even outer space) in which adversaries actively compete to disrupt, deny, or degrade access and communication within civilian and military operations or the continuous functioning of critical infrastructure. It features intense competition, requiring robust strategies, such as AI, decentralized logistics, and hardened communications, to maintain functionality against near-peer adversaries. This makes contested environments dynamic and unpredictable, requiring adaptability and resilience [16]. The fictional scenario was developed to provide a rich, contextual background for the data analysis, simulating the complexities of a modern hybrid conflict. This scenario serves as the narrative framework within which the AI model operates.

Wargaming Fictional Scenario Name: *Operation CyberShield200*

Historical Background: The world is on the brink of a new type of warfare in which cyber and physical threats converge. The scenario is set in the fictional region of Faurichia, a strategic corridor bridging major economic zones. The primary protagonist is Veloria, a democratic nation with approximately 15 million people. Veloria has established itself as a regional economic hub because of its advanced technological sector, particularly in semiconductor manufacturing and digital services. Its strategic location makes it a vital transit point for energy and commerce in the region. Opposing Veloria is its larger neighbor, Zanthos, an authoritarian state with a population of approximately 33 million people. Although resource-rich, Zanthos lags technologically and harbors deep-seated historical grievances against Veloria. Tensions

stem from an unresolved border conflict 18 years prior, involving the disputed Khorkus Highlands, a territory rich in rare-earth minerals essential for modern electronics.

Currently Operational Background: Veloria faces an imminent threat from the hostile neighboring nation of Zanthos. Zanthos aims to destabilize Veloria by launching coordinated cyber and physical attacks on its critical infrastructure. Additionally, a group of cyber mercenaries called "CyberWolves66", supported by Zanthos, acts as a notorious cybercrime syndicate based in a neutral third country, adding to the threat. Comprising 50-75 highly skilled hackers, this group is highly motivated by financial gains and ideological anarchism. Their expertise lies in zero-day exploits, ransomware deployment, and dark-web operations.

Insider Threat Network: Zanthos Intelligence has fostered a network of insiders within Veloria's government and critical infrastructure sectors. Recruited through financial incentives, ideological alignment, or coercion, these individuals provide critical access to credentials and physical intelligence, thereby bypassing perimeter defenses.

CyberShield200 Task Force Mission: The mission of the special unit CyberShield200 TF is to analyze multiple data streams to thwart attacks and risks in order to ensure national security by fusing real-time intelligence across cyber, physical, and financial domains to provide actionable warnings to national civilian and military leadership.

The CyberShield200 TF, Veloria's elite Intelligence agency, is tasked with analyzing an overflow of data to anticipate and neutralize Zanthos's impending attacks by operating from a state-of-the-art command center and employing advanced AI and machine learning tools.

Table 1 presents the main elements related to the wargaming fictional scenario *Operation CyberShield200*, such as scenario features and their descriptions, data type, features of attributes, and scenario key elements.

Table 1

Attributes of the wargaming fictional scenario

Scenario Features (Attributes)	Descriptions	Data Type	Attributes Features	Scenario Key Elements
Cyber_Attack_Signatures	Number of known malware signatures and cyber attack indicators observed. A higher number of detected signatures indicates increased cyber activity, suggesting an imminent or ongoing attack.	NUMERIC	Monitor and identify patterns of cyber attacks originating from Zanthos and CyberWolves66	**Cyber Attacks:** Zanthos and CyberWolves66 are launching sophisticated cyber attacks targeting Veloria's financial institutions, power grids, and communication networks.
Drone_Activity_Frequency	Frequency of drone activity observed in the area. Increased drone activity can signal reconnaissance, surveillance, or preparation for a physical attack.	NUMERIC	Track drone activity over key infrastructure and potential targets.	**Drone Activity:** Zanthos is deploying drones for surveillance, reconnaissance, and potential targeted strikes against critical infrastructure.
Social_Media_Threat_Level	Level of threat indicated by social media activity, including disinformation and propaganda. High levels of social media manipulation, disinformation, and propaganda can create chaos and destabilize the target, paving the way for attacks.	{Low, Medium, High}	Analyze social media for indications of planned attacks or civil unrest instigated by Zanthos propaganda.	**Social Media Manipulation:** Zanthos is spreading disinformation and propaganda through social media to incite panic and unrest among Velorian citizens.
Financial_Transaction_Volume	Volume of financial transactions observed, potentially indicating unusual activity. Unusual spikes or drops in financial transactions can indicate attempts to disrupt the economy or fund hostile activities.	NUMERIC	Detect abnormal financial transactions that could indicate funding or coordination of attacks.	**Financial Warfare:** Zanthos is attempting to disrupt Veloria's financial markets through cyber attacks and manipulation of transaction volumes.
Insider_Threat_Alerts	Number of alerts indicating potential insider threats. A higher number of insider threat alerts suggests potential sabotage or intelligence leaks.	NUMERIC	Monitor internal communications and activities to identify any potential insider threats collaborating with Zanthos.	**Insider Threats:** CyberWolves66 has infiltrated key organizations within Veloria, providing them with inside information and access to sensitive systems.
Weapon_Acquisition	Level of confidence in weapon acquisition by hostile forces. Confirmed weapon acquisition by hostile forces strongly indicates an imminent physical attack.	{No, Possible, Confirmed}	Track and report on unusual patterns of weapon purchases or thefts within Veloria.	**Weapon Acquisition:** There are reports of Zanthos and CyberWolves66 acquiring advanced weaponry, raising concerns about potential physical attacks.
Communication_Traffic_Volume	Volume of communication traffic observed, potentially indicating increased activity. Increased communication traffic can indicate coordination and planning among hostile forces.	NUMERIC	Analyze communication traffic for suspicious activities and potential coordination of attacks.	**Communication Interception:** Veloria's intelligence agencies are monitoring communication traffic to identify potential threats and intercept enemy communications.
Attack_Likely	Indicates the likelihood of an attack (0 for No, 1 for Yes).	{0, 1}	Predict the likelihood of an attack based on the analysis of the above attributes.	**Attack Likely:** It is the central objective of the intelligence analysis and decision-making trigger. It serves as the primary indicator for decision-makers. A "1" (Yes) signals the need for immediate action, while a "0" (No) indicates a lower level of urgency.

Operational Planning: AI models trained on the *Operation CyberShield200* dataset provide predictive assessments of the likelihood of imminent attacks, enabling the Task Force to prioritize resources and deploy suitable countermeasures. "Attack_Likely" informs operational planning staff to:

- direct intelligence-gathering efforts;
- guide the deployment of defensive measures;
- trigger contingency plans as necessary.

Wargaming Objective: In the wargaming fictional scenario, "Attack_Likely" is the central objective of intelligence analysis. Players or decision-makers strive to accurately predict and respond to the likelihood of attacks. By employing AI tools, predictive modeling supports the main purpose of wargaming: the anticipation and mitigation of future threats.

INTEL Feed for Wargaming Vignette:

1. *Cyber_Attack_Signatures:*
- Detected increase in phishing emails targeting key government officials;
- Multiple attempts to breach Veloria's power grid infrastructure using custom malware.

2. *Drone_Activity_Frequency:*
- Unidentified drones spotted over Veloria's critical data centers;
- Increase in drone activity near border areas and military installations.

3. *Social_Media_Threat_Level:*
- Hashtag #DownWithVeloria trending on multiple social media platforms;
- Videos released by CyberWolves66 threatening coordinated cyber and physical attacks.

4. *Financial_Transaction_Volume:*
- Sudden surge in cryptocurrency transactions linked to Zanthos-based wallets;
- Large cash withdrawals and transfers in border towns.

5. *Insider_Threat_Alerts:*
- Employees at a key telecommunications company flagged for unusual access patterns;
- Anonymous tips regarding potential insider conspiracies with Zanthos agents.

6. *Weapon_Acquisition:*
- Reports of missing weapons from Veloria's military depots;
- Unusual spike in black-market weapon sales.

7. *Communication_Traffic_Volume:*
- Encrypted communications intercepted between Zanthos operatives and CyberWolves66;
- Increased radio traffic in regions close to critical infrastructure.

8. *Attack_Likely:*
- High likelihood of a coordinated cyber-physical attack within the next 24–72 hours based on current data trends.

Table 2 presents the dataset related to the wargaming fictional scenario *Operation CyberShield200*. Based on the proposed features linked to our fictional scenario, a dataset comprising 200 fictional instances was tailored for use in Weka to train and test the RandomForest ML algorithm. The results can be used to understand and warn civilian and military leadership if any attacks from Zanthos are likely to occur.

Table 2

Sample INTEL Feed dataset for Operation CyberShield200 wargaming fictional scenario

No.	Cyber_Attack _Signatures	Drone_Activity _Frequency	Social_Media _Threat_Level	Financial _Transaction _Volume	Insider _Threat _Alerts	Weapon _Acquisition	Communication _Traffic _Volume	Attack _Likely
1	50	5	Medium	525000	10	Possible	500	0
2	80	9	High	905000	18	Confirmed	800	1
3	20	3	Low	216000	2	No	220	0
4	60	6	Medium	652000	12	Confirmed	480	1
5	10	2	Low	125000	1	No	300	0
6	11	7	Medium	452000	3	Possible	270	0
...	...	...	...	...	...	...	...	...
194	44	7	Medium	790000	6	Confirmed	710	1
195	15	3	Low	194000	4	No	240	0
196	18	4	Low	232000	9	No	270	1
197	62	7	Medium	650000	15	Confirmed	720	1
198	18	5	Medium	142000	6	No	310	0
199	11	6	Medium	496000	3	Possible	320	0
200	84	8	High	724000	17	Possible	753	1

2.2 RandomForest ML Algorithm Running - Reading the Output

For the *Operation CyberShield200* dataset, which likely consists of high-stakes binary outcomes (Attack vs. No Attack) based on sensor data, selecting the right algorithm is the difference between a reliable defense and a series of "false alarms". Many ML algorithms can be employed for wargaming scenario analysis. In our case study, having only 200 instances tailored per dataset (proof-of-concept), it is suitable to use an ML algorithm that avoids overfitting (the model memorizing the noise) and interpretability (the need to explain why an attack was flagged) that could incur the best results of predictive modeling and analysis (Table 3).

Table 3

Examples of ML algorithms

Algorithm	Strengths	Major weaknesses for CyberShield200 wargaming scenario
Logistic Regression	Simple, fast, and highly interpretable via coefficients	Assumes a linear relationship. It will miss complex "blended" attack patterns where multiple sensors must trip simultaneously.
SVM (Support Vector Machines)	Excellent for high-dimensional data; finds the "best" boundary	Extremely sensitive to hyperparameters. On a 200-instance dataset, it can easily overfit the specific noise of that "day's" data (a specific instance).
Decision Trees	Easy to visualize; follows human-like "if-then" logic	High variance – a single tree is notoriously unstable. A small change in one of the 200 instances could result in a completely different tree.
J48	Builds one single, complex tree	Prone to overfitting. It might be 100% accurate in training but unsatisfactory for new Zanthos attacks (for confirmed data, leading to "Attack Likely").
Naive Bayes	Requires very little training data; extremely fast	Assumes feature independence. In tactical sensors, "Heat" and "Smoke" are usually correlated; Naive Bayes ignores this correlation, resulting in poor accuracy. Because it assumes they are independent, it double-counts the evidence.
K-Nearest Neighbors (KNN)	Simple and makes no assumptions about data distribution	Sensitive to irrelevant features and noise. If one 'sensor' is malfunctioning (noisy), the KNN may misclassify everything near it.

Considering the behavior of other ML algorithm types, RandomForest is the most suitable ML algorithm for our case study. It is sophisticated enough to handle the complex cyber–physical signatures of the wargame, yet robust enough not to be distracted by the small sample size of 200 instances (the sensors – meaning some data instances – could be "noisy"). It provides reliability (Precision) and safety (Recall), which are superior tactical engines required for military-grade predictive modeling in *Operation Cybershield200*. The following key technical reasons emphasize why the RandomForest algorithm balances predictive power, robustness, and interpretability in ways that align with the dataset size, feature mix (data type), and operational goals:

- ensemble stability – it averages many decision trees, to reduce the variance and make predictions less sensitive to single noisy features or small changes in the training data;
- handles mixed feature types – it natively accepts numeric and categorical inputs without complex encoding; therefore, it can use the wargaming vignette attributes (counts, flags, categorical descriptors, etc.) with minimal preprocessing;
- robust to noise and outliers – individual trees can overfit noisy signals, but the forest dilutes these effects, improving generalization on real-world, messy vignette data;
- good ranking performance – it often produces high Area Under the Curve (AUC) because it learns various decision boundaries across trees (a reliable ranking in the context of AUC refers to a model's high capability to correctly order, or rank, positive instances higher than negative instances – a metric used to measure how well the model can distinguish two classes).

The INTEL Collection Prioritization Advantage of RandomForest Algorithm

An important operationally distinctive advantage of employing the RandomForest algorithm is its ability to produce a native ranked feature importance output (Table 4). In the *Operation CyberShield200* study, the execution of both the AttributeSelected Classifier and InfoGainAttributeEval produced the ranked intelligence collection guide.

Table 4

Ranked attributes of CyberShield200 wargaming scenario features

Weka Attribute Ranking	Scenario No. / Attribute	InfoGain	INTEL Domain
1	7 / Communication_Traffic_Volume	**0.609**	SIGINT (Signal Intelligence)
2	4 / Financial_Transaction_Volume	**0.567**	FININT (Financial Intelligence)
3	5 / Insider_Threat_Alerts	**0.532**	HUMINT (Human Intelligence)
4	1 / Cyber_Attack_Signatures	**0.517**	CYBINT (Cyber Intelligence)
5	6 / Weapon_Acquisition	0.431	IMINT (Imagery Intelligence) – evidence-based
6	3 / Social_Media_Threat_Level	0.338	OSINT (Open-Source Intelligence)
7	2 / Drone_Activity_Frequency	0.226	ISR (Intelligence, Surveillance, and Reconnaissance)

This SIGINT – FININT – HUMINT – CYBINT sequence was valuable and directly translated into an actionable INTEL collection prioritization framework for the CyberShield200 Task Force. The other three attributes were used for "fine-tuning" in the final prediction (No Attack vs. Attack).

Figure 1 displays the manner in which Weka visualizes all attributes in the first preprocessing stage (cleaning missing values, converting nominal attributes to numeric, normalizing/scaling, and optionally selecting or generating features) before the classification process is performed by the RandomForest ML algorithm. In the Weka Preprocess tab, the colors represent the target class, *Attack*_Likely: blue represents No Attack (0), and red represents an Attack (1). The "blended" or stacked appearance occurs when both classes share the same range of values for a specific attribute. The numbers at the top of each bar indicate the total count of instances (reports) in that specific bin.

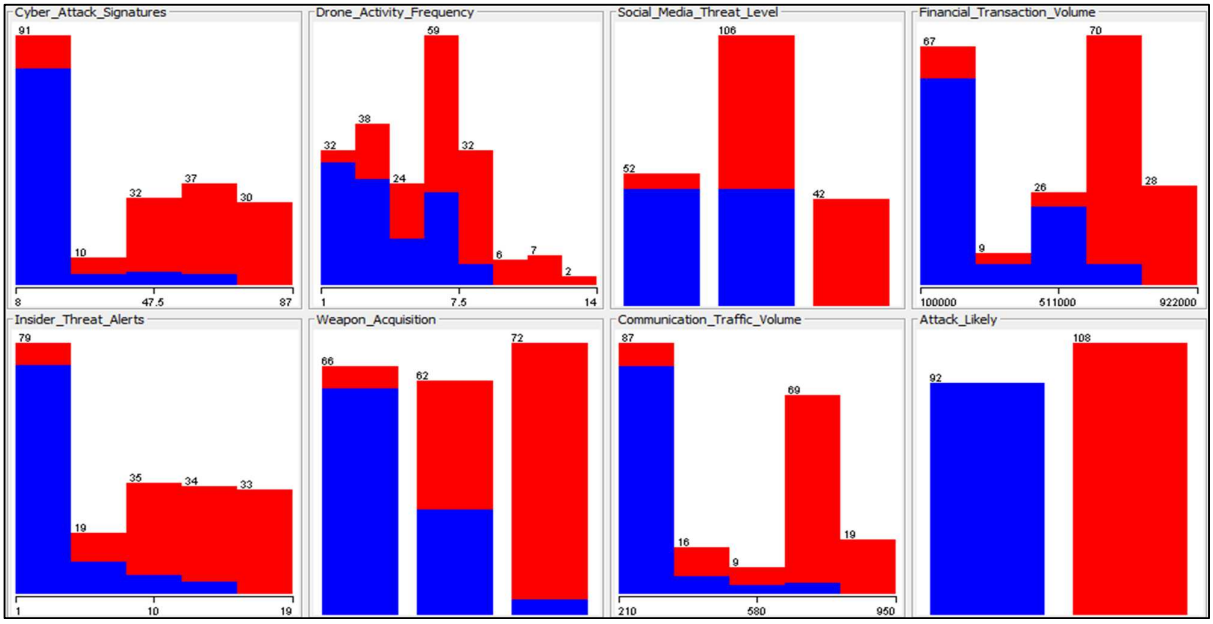
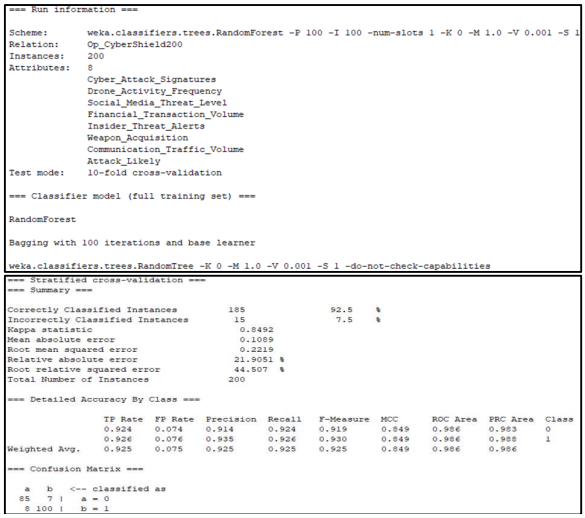


Fig. 1. Visualization of classification for all fictional scenario attributes

For the CyberShield200 case study, all 200 instances in the tailored dataset were used to train and test the RandomForest ML algorithm. To determine the best RandomForest run, a cross-validation strategy comparison was conducted for six iterations by changing the cross-validation (CV) runs: 10-folds (run A), 20-folds (run B), 50-folds (run C), 100-folds (run D), 150-folds (run E), and 200-folds cross-validation (run F). Run A was the overall best performance with the following results: best ROC (Receiver Operating Characteristic), best PRC (Precision-Recall Curve), and high accuracy. The RandomForest demonstrated exceptional robustness and stability across all six CV strategies (92-92.5% accuracy). Figure 2 presents the run of RandomForest 10-fold cross-validation information (usually, a conventional standard for the ML domain) for the wargaming fictional scenario.



```
=== Run information ===

Scheme:       weka.classifiers.trees.RandomForest -P 100 -I 100 -num-slots 1 -K 0 -M 1.0 -V 0.001 -S 1
Relation:     Op_CyberShield200
Instances:    200
Attributes:   8
              Cyber_Attack_Signatures
              Drone_Activity_Frequency
              Social_Media_Threat_Level
              Financial_Transaction_Volume
              Insider_Threat_Alerts
              Weapon_Acquisition
              Communication_Traffic_Volume
              Attack_Likely
Test mode:    10-fold cross-validation

=== Classifier model (full training set) ===

RandomForest

Bagging with 100 iterations and base learner

weka.classifiers.trees.RandomTree -K 0 -M 1.0 -V 0.001 -S 1 -do-not-check-capabilities

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances         185               92.5    %
Incorrectly Classified Instances        15                7.5    %
Kappa statistic                          0.8492
Mean absolute error                      0.1089
Root mean squared error                  0.2219
Relative absolute error                 21.9051 %
Root relative squared error             44.507  %
Total Number of Instances              200

=== Detailed Accuracy By Class ===

               TP Rate   FP Rate   Precision   Recall  F-Measure  MCC      ROC Area  PRC Area  Class
               0.924     0.074     0.914      0.924    0.919      0.849    0.986     0.983     0
               0.926     0.076     0.935      0.926    0.930      0.849    0.986     0.988     1
Weighted Avg.  0.925     0.075     0.925      0.925    0.925      0.849    0.986     0.986

=== Confusion Matrix ===

   a   b   <-- classified as
  85   7 |   a = 0
   8 100 |   b = 1
```

Fig. 2. RandomForest ML algorithm running/output

3. DISCUSSION

The model parameters were set to generate 100 trees (iterations) with an unlimited depth, which were trained on nine subsamples and tested on the remaining one, repeating the process 10 times to ensure that every instance was used for both training and testing. The RandomForest model achieved exceptional performance on the *Operation CyberShield200* dataset. Using stratified 10-fold cross-validation, the model correctly classified 185 of the 200 instances, resulting in an overall classification accuracy of 92.5%. Only 15 instances (7.5%) were incorrectly classified.

This high level of accuracy indicates a strong capability to distinguish between routine operations and imminent threats based on the provided intelligence attributes. The Kappa statistic, which measures inter-rater agreement for categorical items, was 0.8492 (values between 0.81 and 1.00 are generally interpreted as "almost perfect agreement", suggesting that the model's predictions are statistically significant and not merely due to chance).

Additional error metrics further validate the model's performance: Mean Absolute Error (MAE): 0.1089; Root Mean Squared Error (RMSE): 0.2219; Relative Absolute Error: 21.90%; Root Relative Squared Error: 44.50%. These low error rates confirm the model's precision in fitting the training data.

The model (Table 5) demonstrated balanced performance across both classes ("No Attack" and "Attack Likely"), which is crucial for a military system where both false alarms and missed threats entail high costs.

Table 5

Performance Metrics Comparison by Classes

Class	TP Rate (Recall)	FP Rate	Precision	F-Measure	ROC Area
No Attack (0)	0.924	0.074	0.914	0.919	0.986
Attack (1)	0.926	0.076	0.935	0.930	0.986
Weighted Avg.	**0.925**	**0.075**	**0.925**	**0.925**	**0.986**

Attack Detection (Class 1): The model achieved a True Positive (TP) rate of 93.5%, indicating successfully identified of over 93% of the actual attack 'scenarios'. The precision indicates that when the model predicted an attack, it was correct 93.5% of the time.

Safety Assurance (Class 0): For non-attack 'scenarios', the model achieved a TP rate of 92.4%, with a False Positive (FP) rate of only 7.4%. This low false alarm rate is operationally significant, as it minimizes the risk of 'scenarios' that can lead to alert fatigue among CyberShield200 TF and military leaders.

ROC Curve Analysis: Receiver Operating Characteristic (ROC) Area was 0.986. The ROC curve illustrates the diagnostic ability of a binary classifier system as its discrimination threshold is varied. An area of 1.0 represents a perfect test; an area of 0.5 or under this value represents a worthless test.

The confusion matrix (Table 6) provides a granular view of the classification decisions of the model.

Table 6

Confusion Matrix_CyberShield200 Predictions

Actual Class	Predicted: No Attack (0)	Predicted: Attack (1)	Total
No Attack (0)	85 (True Negatives)	7 (False Alarms)	92
Attack (1)	8 (Missed Attacks)	100 (True Positives)	108
Total	**93**	**107**	**200**

The confusion matrix reveals 85 True Negatives (TN), where the model correctly identified non-attack 'scenarios'. This capability helps prevent resource wastage and alert fatigue. There were 7 FP, where a benign 'scenario' was flagged as a threat. In a military context, a FP is generally preferable to a False Negative (FN), as the cost of vigilance is lower than the cost of surprise. There were 8 FN, where an actual attack was missed. Although concerning, this 6.5% miss rate is low, and the

model's 100 TP demonstrate a strong ability to detect genuine threats.

4. CONCLUSIONS

In a world of rapid and continuous geopolitical and technological change, conventional MDMP is increasingly strained by the velocity, volume, and complexity of modern multidomain warfare. The employment of AI during the MDMP process, specifically using ML algorithms, can lead to a significant enhancement of the traditional way of its development. However, it is relevant and important to maintain expert-in-the-loop oversight to ensure that AI-generated recommendations augment rather than replace human judgement – a principle directly embedded in the *Operation CyberShield200* framework design, where the RandomForest model output threat probability scores for human commanders to act upon.

Even if the tailored dataset comprises only 200 instances, the analysis of CyberShield200 fictional scenario demonstrates that AI-powered wargaming is no longer a theoretical exercise but a practical requirement for modern military decision-making. By leveraging the ML algorithm, we have moved beyond simple "if-then" logic to a nuanced predictive model capable of navigating the "fog of war".

The application of the RandomForest algorithm to the *Operation CyberShield200* fictional scenario dataset yielded significant insights into the potential of AI for threat prediction. The results were analyzed in terms of overall model performance, class-specific metrics, confusion matrix analysis, ROC curve evaluation, and feature importance. The high level of accuracy (92.5%) demonstrates the model's robust capability to discern threat patterns within multidomain intelligence data. The integration of AI in military-decision support systems enhances situational awareness, optimizes resource allocation, and improves response times. These platforms can simultaneously consider multiple scenarios, evaluate potential outcomes, and provide data-driven recommendations. This capability allows military leaders to explore various strategies and their potential consequences before committing to a course of action in real-world situations. The findings indicate that AI-driven models can reliably identify attack likelihood patterns and offer decision-makers actionable insights to improve situational awareness.

While this AI exploration provides a robust baseline for military decision-making support, several avenues for future research remain:

- Adversarial AI defense – further research is needed to determine how the model reacts to "poisoned data". For instance, if the adversary learns that *Communication_Traffic_Volume* tracking is a priority of Veloria, they may flood that sensor with "noise" to trigger intentional False Positives and cause operational fatigue;

- Multi-agent simulations – expanding the dataset to include multiple simultaneous "Attack" types would allow for the use of Multi-Class Classification, moving beyond a simple "0 or 1" binary to real-world threats existing on a spectrum (Low/ Medium/ High/ Critical), and identifying whether an attack is Cyber, Kinetic, or Hybrid;

- Expert-in-the-loop optimization – studying the "Trust Gap" by measuring how quickly human commanders act on, for instance, AI's 10:1 Cost-Sensitive versus Standard alerts.

As this new technology continues to evolve, it will be essential to strike a balance between leveraging the advantages of AI-powered wargaming and maintaining the critical role of human decision-makers in military strategy. The future development of these systems may lead to more sophisticated simulations, improved predictive capabilities, and enhanced integration with other military technologies, potentially reshaping the landscape of modern warfare and strategic planning.

5. REFERENCES

[1] Calian Defence, *Wargaming – Testing Assumptions and Assessing Plans,* https://www.calian.com/defence/blogs/wargaming-testing-assumptions-and-assessing-plans/, 2023

[2] Curry J., *Title Professional Wargaming: A Flawed but Useful Tool,* Simulation &

Gaming Journal 51(5), DOI: 10.1177/1046878120901852, 2020
[3] *Machine Learning at Waikato,* https://ml.cms.waikato.ac.nz/index.html
[4] Defense Science Board, *Report of the Defense Science Board task force on counter autonomy*. U.S. Department of Defense, 2020
[5] Congressional Research Service, *Artificial intelligence and national security* (Report No. R45178), Washington, DC: CRS, 2020
[6] NATO Science & Technology Organization, *Science & technology trends 2020-2040: Exploring the S&T edge*, https://www.sto.nato.int/document/science-technology-trends-2020-2040-exploring-the-st-edge/, 2021
[7] Abid Ali Awan, *What is Online Machine Learning?* AI (blog), DataCamp, https://www.datacamp.com/blog/what-is-online-machine-learning, 16 August 2023
[8] MGallitelli V., *AI-Enabled Military Decision-Making Process - The Forgotten Lessons on the Nature of War*, Marine Corps University Press, Journal of Advanced Military Studies, (Vol. 16, No. 2), https://doi.org/10.21140/mcuj.20251602005, 2024
[9] Col. Adler J.N., *Modernizing military decision-making: Integrating AI into Army Planning,* Army University Press, Military Review Online Exclusive, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2025-OLE/Modernizing-Military-Decision-Making, 2025
[10] *Waikato Environment for Knowledge Analysis (WEKA)*, https://www.waikato.ac.nz/research/institutes-centres-entities/institutes/artificial-intelligence-institute/research/software/
[11] Breiman, L., *Random forests*, Machine Learning, 45(1), 5-32. https://doi.org/10.1023/A:1010933404324, 2001
[12] Donges N., Whitfield B., *Random Forest: A Complete Guide for Machine Learning,* https://builtin.com/data-science/random-forest-algorithm, 2024
[13] Kelleher, J. D., Mac Namee, B., & D'Arcy, A., *Fundamentals of machine learning for predictive data analytics: Algorithms, worked examples, and case studies* (2nd ed.). MIT Press, 2020
[14] Gartner, *Predictive Modeling*, https://www.gartner.com/en/information-technology/glossary/predictive-modeling
[15] Roke, *What is a Contested Environment?* https://www.roke.co.uk/capabilities/contested-environment/
[16] Lt. Col. Michelle P. Santayana and Capt. Stephen Gowen, *Strategic Enabler's Lens: Supporting LSCO in a Contested Environment*, https://www.army.mil/article/272921/strategic_enablers_lens_supporting_lsco_in_a_contested_environment, February 1st, 2024

Tehnologii emergente și disruptive: o explorare a jocurilor de război bazate pe AI și a modelelor predictive în procesul de luare a deciziilor militare

Rezumat: Mediul contemporan instabil, caracterizat de numeroase crize și conflicte care necesită o colectare eficientă a informațiilor și o coordonare excelentă a capabilităților și forțelor militare în timpul operațiilor militare terestre, maritime, aeriene, spațiale și cibernetice, reprezintă o provocare pentru fiecare comandant și personal de conducere. Implementarea Tehnologiilor Emergente și Disruptive (EDTs), în special a Inteligenței Artificiale (AI), ca factor catalizator pe timpul desfășurării jocurilor de război (wargaming), ar putea îmbunătăți și transforma instruirea celor care se pregătesc cât și modul de luare a deciziilor strategice de către factorii de decizie. Folosind platforma Weka, acest articol explorează rolul AI ca instrument de sprijin în cadrul vinietelor de wargaming și clarifică modul în care algoritmii de învățare automată (ML) anticipează amenințările și îmbunătățesc procesul decizional, pentru a crea forțe și capabilități militare mai flexibile și adaptabile în mediul actual contestat.

Marin-Marian COMAN, PhD student, "Lucian Blaga" University of Sibiu, "Nicolae Bălcescu" Land Forces Academy, coman.marian@gmail.com, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.
Claudiu-Vasile KIFOR, Prof. Eng. PhD, "Lucian Blaga" University of Sibiu, Faculty of Engineering, claudiu.kifor@ulbsibiu.ro, +40 269 217 779, 10 Victoriei Blvd., Sibiu, Romania.