DEFENCE STARTUP IDEA

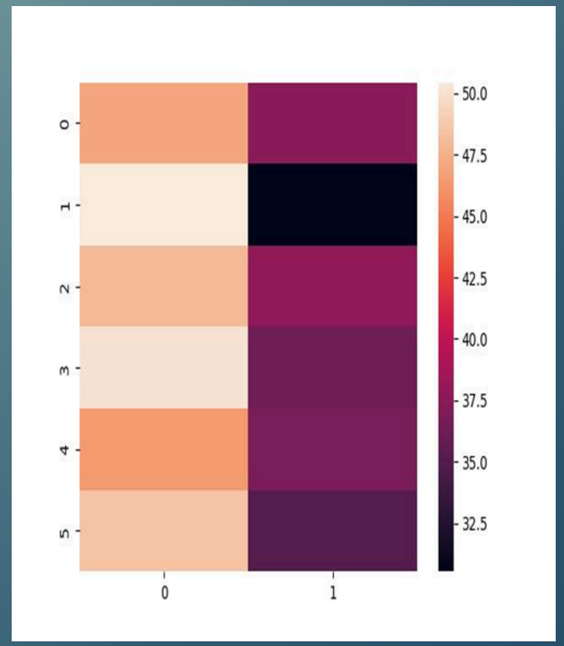
WARFARE TACTICS DECODER

SDG 16-Peace,Justice and Strong Institutions

IDEA: Predicting the risk of attacks and automating the enemy's location in war

Calculating the PROBABILITY OF A FUTURE ATTACK to classify the type of attack whether they involve missiles, drones, artillery or other forms of aggression, on a location that has been attacked in the past and to proivde threat detection systems for the same could be a key to the Ukrainian defence moreover it would be tracking the enemy's movements for timely evacuation of the civilians.

Problem Statement:
To develop a threat-detection system that uses historical data of past attacked locations in Ukraine to classify the region/city as a high-risk or low-risk zone. Calculating the probability of a future attack to classify the type of attack e.g drone,missile etc by machine learning models that require ground data such as crater shape, size and dimensions.
The system also provides a threat-monitoring solution to the approaching enemy in war by automating the workflow of tasks by data pipelining
Solution: To give updates on the enemy's current location To anticipate future attacks by improved decision-making and hyperparameter tuning.To enrich the quality of raw data by preparing it for data analysis and decision-making
Data cleaning,Feature Engineering will be done to preprocess the data.



SELECT * FROM attack_loc;

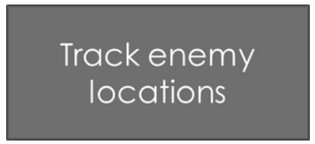
location |latitude | longitude
---------+------------+------------
Mariupol | 47.09710000 | 37.54340000
Kyiv| 50.45040000 | 30.52450000
Donetsk| 48.01590000 | 37.80280000
Kharkiv | 50.00200000 | 36.30740000
Odesa| 46.47020000 | 36.73060000
Dnipro| 48.46470000 | 35.04620000
(6 rows)

Solution

A web-based SaaS platform where the user inputs past attack locations and a predictive model generates the risk of an attack on that region again as high or low.The current enemy locations to be monitored and automated from time-to-time using data pipelining to provide updates on the same.

This solution is currently in the development phase, and we are working to refine the predictive models and automation pipelines for seamless functionality.

Attack Location	Risk level
Mariupol	High risk
Uzhorod	Low risk



DAG Object

```
track_ambulancelocations_task =
PythonVirtualenvOperator(
task_id = 'track_ambulancelocation',
python_callable=track_ambulancelocation,
dag=dag )
```

```
map_center = [50.0, 30.0] # Replace with the actual center of your surveillance region
map_display = folium.Map(location=map_center, zoom_start=12)

for enemy in enemy_locations:
# Convert pixel coordinates (thermal image) to real-world GPS (dummy logic)
latitude = map_center[0] + (enemy[1] - 500) * 0.0001
longitude = map_center[1] + (enemy[0] - 500) * 0.0001

# Add markers to the map
folium.Marker([latitude, longitude], popup="Enemy Detected").add_to(map_display)

# Save map to an HTML file for visualization
map_display.save("enemy_tracking_map.html")
```

Type of attack

Top view

Data

Ground Dimensions

Crater size and depth

Crater shape

Naïve-Bayes(NB) classification model to classify the type of attack

•When a drone attack is made on a location capture the image of the attacked location and use the ML solution to distinguish drone-attacks from other forms of attack.

data models like data pipelines will automate the workflow of task such as tracking enemylocations

Vision

To minimize the destruction caused by War which will allow for the peace and justice of strong institutions.

Our Mission

- predictive modelling of FUTURE ATTACK LOCATIONS
- automated tracking of ENEMY LOCATIONS

- MINISTRY OF DEFENCE OF UKRAINE
- NORTH ATLANTIC TREATY ORGANIZATION(NATO)

BUSINESS MODEL

THE FINANCIAL STRUCTURE OF THE COMPANY

VALUE PROPOSITION

“In today’s rapidly evolving threat landscape, defense agencies need solutions that are agile, intelligent, and secure. Our SaaS website delivers machine learning powered, real-time threat detection systems to provide alerts and help in decision-making. Our platform leverages historical data to classify regions as high risk or low risk for future threats.
The proposed system leverages thermal imaging, automated workflows using Apache Airflow, and real-time reporting to create a robust threat monitoring solution.
Our mission is to empower institutions with secure, scalable, and inclusive technology that safeguards peace and justice.
The SaaS platform ensures how defense agencies will be able to anticipate future war attacks and also monitor enemy movements in the war. Key features such as
Front-end -Number of successful predictions,
Heatmaps for live-visualization of enemy locations

- Risk level
- Apache Airflow Web-UI to monitor the DAG for pipelines
- Secure Scalable Databases like PostgreSQL offering locking protocols and Role-base access controls
- We are committed to advancing national security through innovation. We will try to improve the ukraine’s defence agencies threat analysis and risk detection systems. Let’s discuss how we can collaborate to strengthen your defense capabilities.”

WHO WE SERVE

The customers play a very important role in the successful business operations of a firm and so fulfilling the requirements of the target customer segment is very important.

THE TARGET CUSTOMER SEGMENTS FOR OUR WEBSITE IS IDENTIFIED AS FOLLOWS:-

- NATIONAL DEFENCE FORCES,
  SUCH AS THE UKRAINIAN ARMY, AIRFORCE,
  & NAVY, MINISTRY OF DEFENCE OF UKRAINE
- NATO AND OTHER ALLIED FORCES
  SUPPORTING UKRAINE

CHANNELS

Reaching target customer segments is crucial for an organization and requires effective channel distribution to ensure accessibility and engagement.

The channels for our defence startup are stated as follows :-

- LINKEDIN
- CI/CD pipelines are an integral part of modern software development and deployment workflows. They serve as a channel to efficiently build, test, and deploy projects to production.
- Defence trade shows and expos
- Government procurement portals (eg. SAM.gov (U.S.), GeM (India))
- Industry organizations (e.g., AIA, NDIA, FICCI Defence and Aerospace)
- Collaborate with overseas defense firms or governments looking to acquire advanced technologies.

REVENUE STREAMS

- Subscription Plans for Clients
- LOOKING FORWARD TO ISSUE AN IPO AFTER ATTAINING A STEADY USER BASE
- Publish specialized products, training programs, career opportunities, and industry insights tailored to the defense and security sectors.
- OUTSOURCING TO THIRD PARTIES SUCH AS FREELANCERS, DIFFERENT ORGANIZATIONS, ETC.
- CONDUCTING WORKSHOPS FOR OPERATING OUR PRODUCT

KEY PARTNERSHIPS

- LOCK HEED MARTIN
- NORTHROP GRUMMAN

KEY ACTIVITIES

- Develop a threat detection system to anticipate enemy attacks using real-time data from IoT sensors, drones.
- Monitor enemy movements with ML-powered tools to identify patterns and forecast threats.
- Process and integrate multi-source data for accurate threat classification and real-time alerts.
- Continuously upgrade systems to adapt to evolving enemy strategies.

Warfare Tactics Decoder

THANK YOU