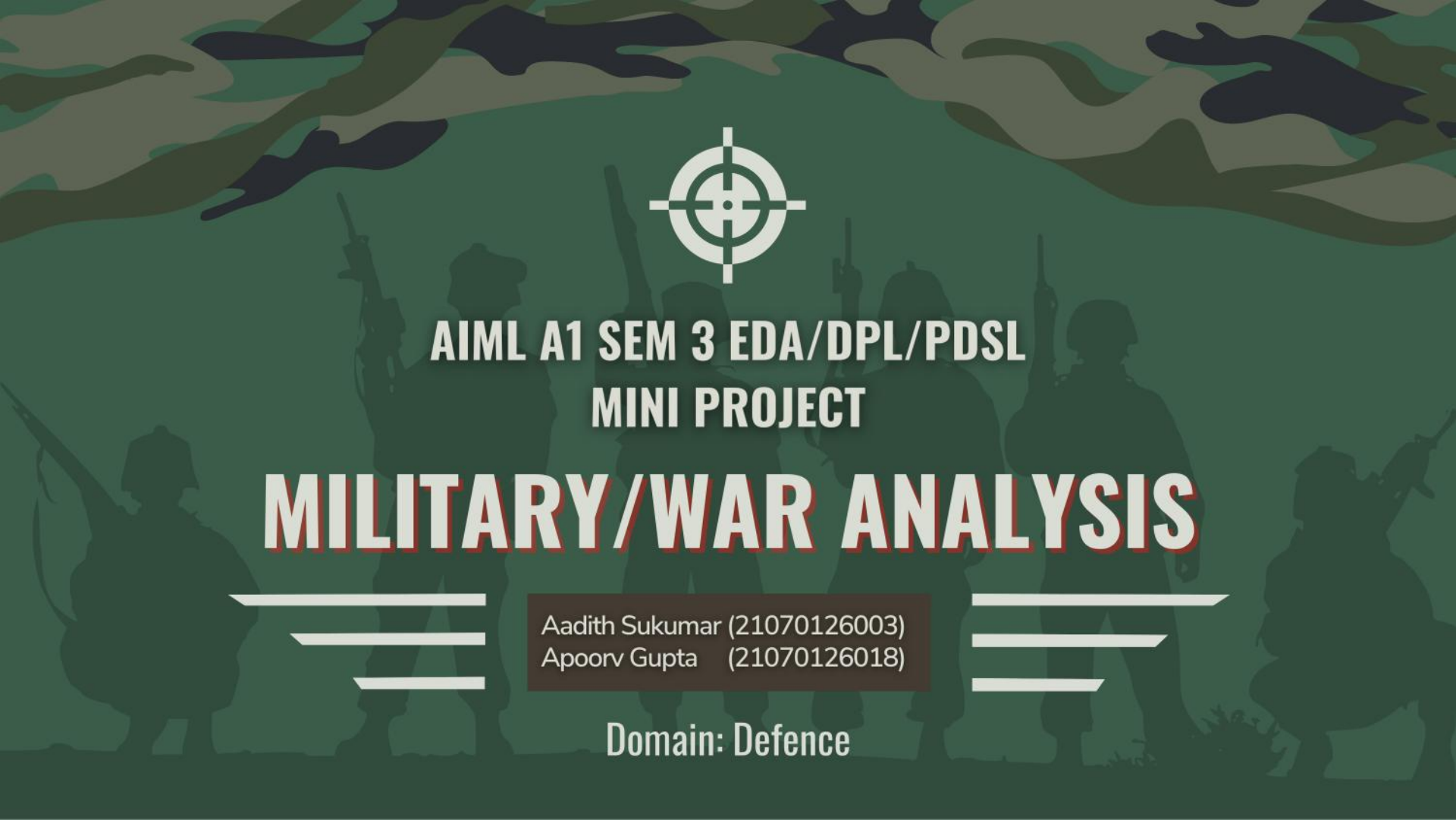


AIML A1 SEM 3 EDA/DPL/PDSL
MINI PROJECT

MILITARY/WAR ANALYSIS

Aadith Sukumar (21070126003)
Apoorv Gupta (21070126018)

Domain: Defence

BACKGROUND

- Military is a field that has existed probably ever since the first civilizations came about to exist in this world. Understanding military and defense warfare gives a significant and strategic advantage to any nation to defend itself from attackers.
- We should study military history primarily so we don't repeat mistakes from time past. Learning about historical military events help us gain insights on how centuries-old conflicts relate to today’s unfolding events and how the economy has been affected or allocated to nations over years to prepare and defend.
- For example, the present Russian conquest of Ukraine is a live example to study and analyze international military spendings, war losses and new methods of warfares.

ABOUT THIS PROJECT

Comprehensive & easy-to-understand visualization to show military spendings across countries across decades. Interactive plots and maps like Plotly, GeoPandas, Flourish and more

Raw .csv data preprocessed, cleaned, imputed to facilitate easier analysis and better visualizations

Creating ML models to forecast and analyze future scope of this project while mapping it to past findings.

Understanding the new era of Cyber Warfare and studying cyber-attacks on governments by state-sponsored threat actors using string processing, EDA, NLP. Specialized analysis on Russo-Ukrainian attacks

DATASETS USED

Military Expenditure By Country

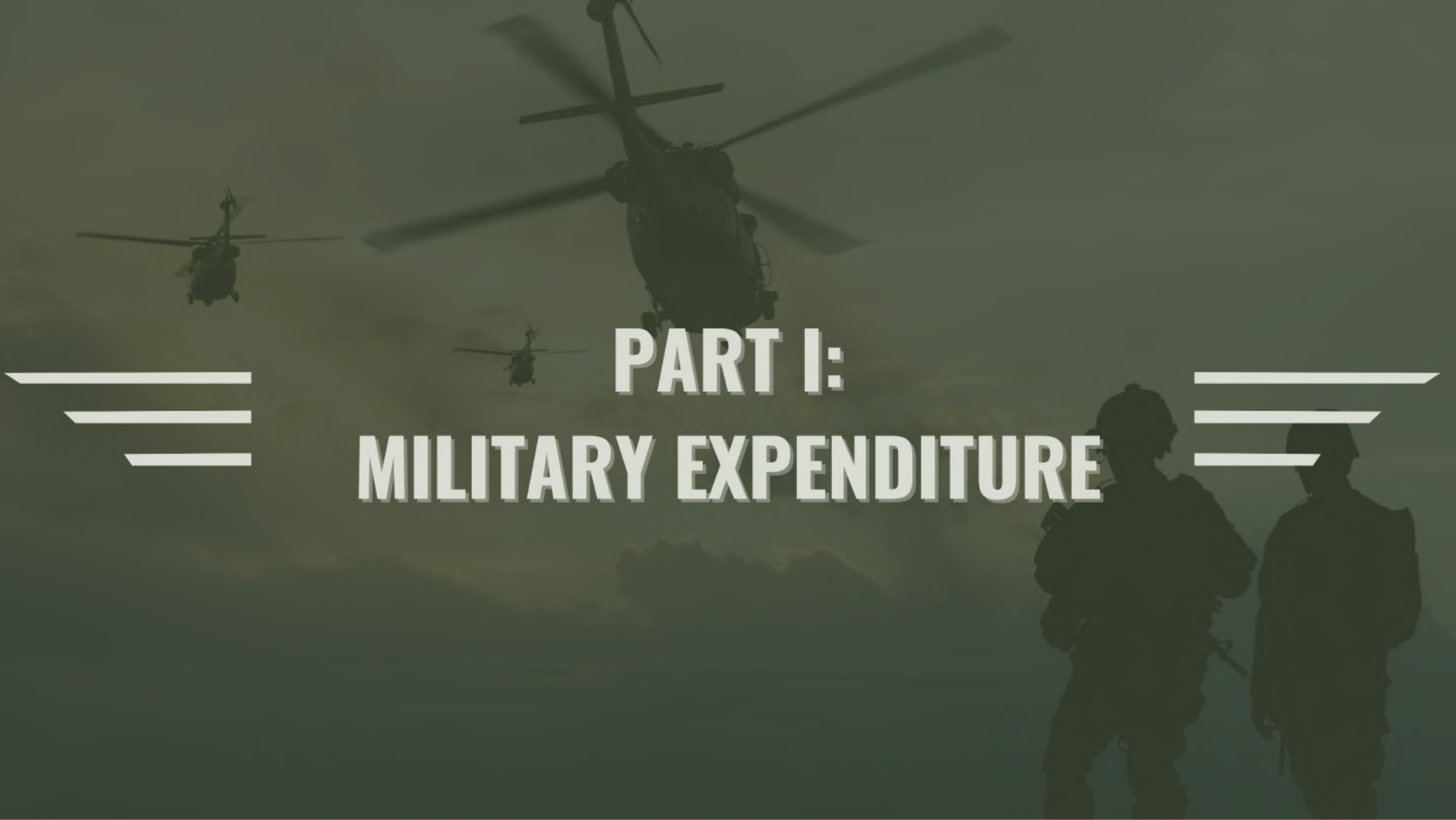
Country and region wise fifty years of data on military expenditure of different territories.

Cyber Incidents 2005 To 2020

Multiple cyberattack incidents from 2005-2020 based on country-wise victim, type and sponsor

2022 Ukraine Russia War Dataset

Dataset describing equipment losses & personnel death of Russians in 2022 Ukraine Russia War.



PART I:
MILITARY EXPENDITURE

PART I:
MILITARY EXPENDITURE

A Data set containing all data about military expenditure for over **200 territories.**

PART I:
MILITARY EXPENDITURE

Military Spending of Countries (1960-2019)

Annual expenditure of over 200 countries in terms of current USD

Data Code (27) Discussion (2)

About Dataset

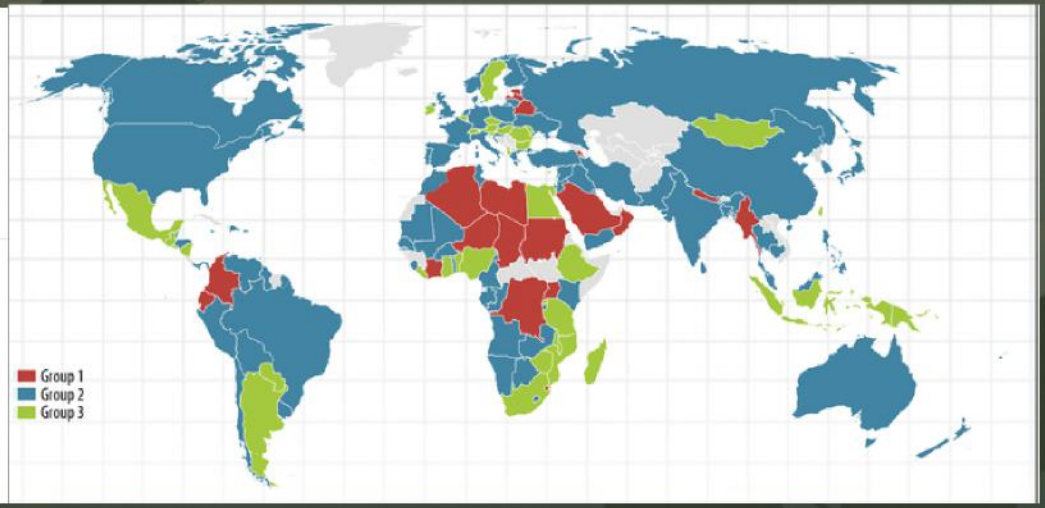
Acknowledgements

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE (SIPRI)

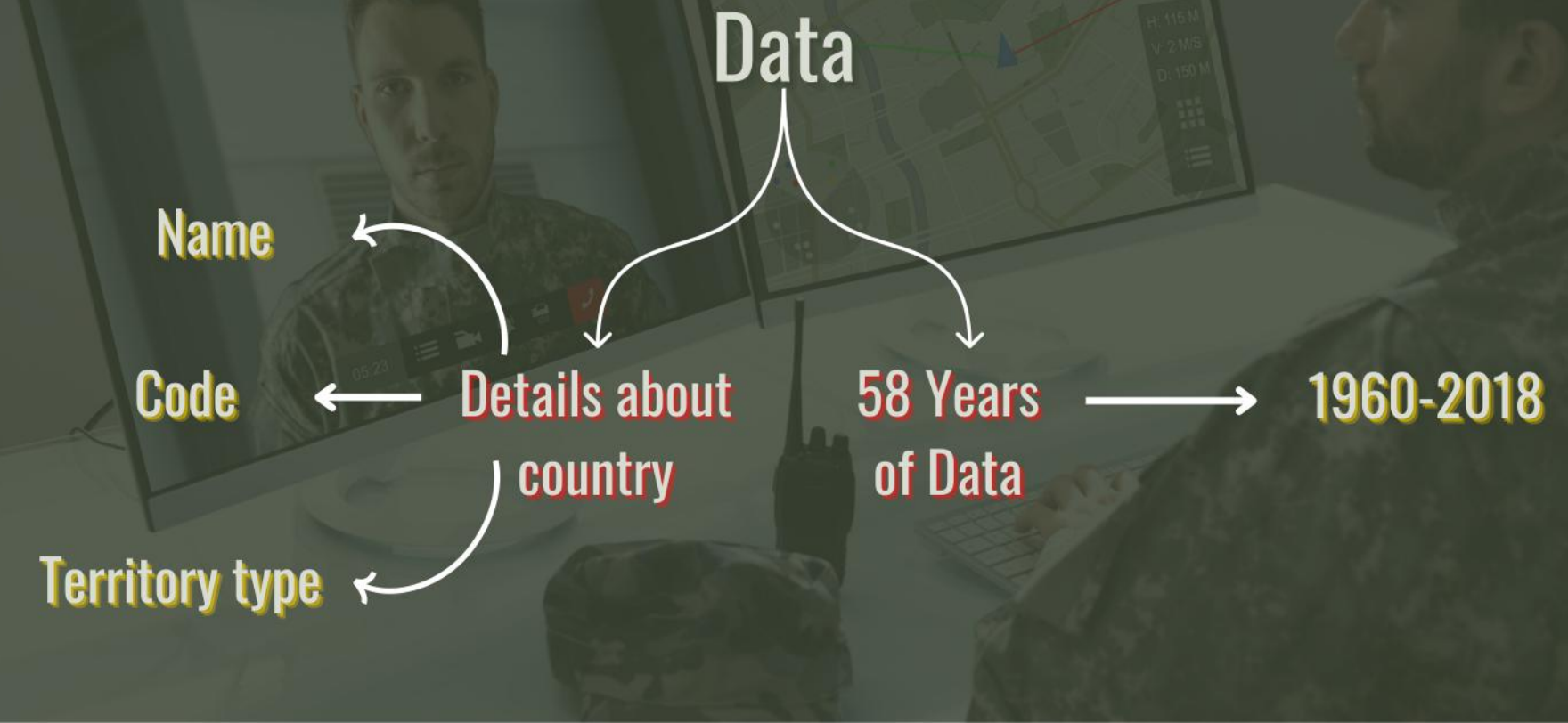
The World Bank Database

More Relevant Data

https://data.worldbank.org/indicator/MS.MIL.XPND.CD



UNDERSTANDING DATASET



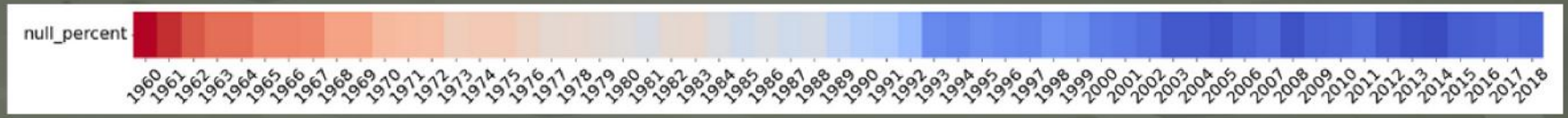
DIVISION OF ANALYSIS

We saw potential in this dataset for two major analysis

INTERNATIONAL

National

DEALING WITH EMPTINESS

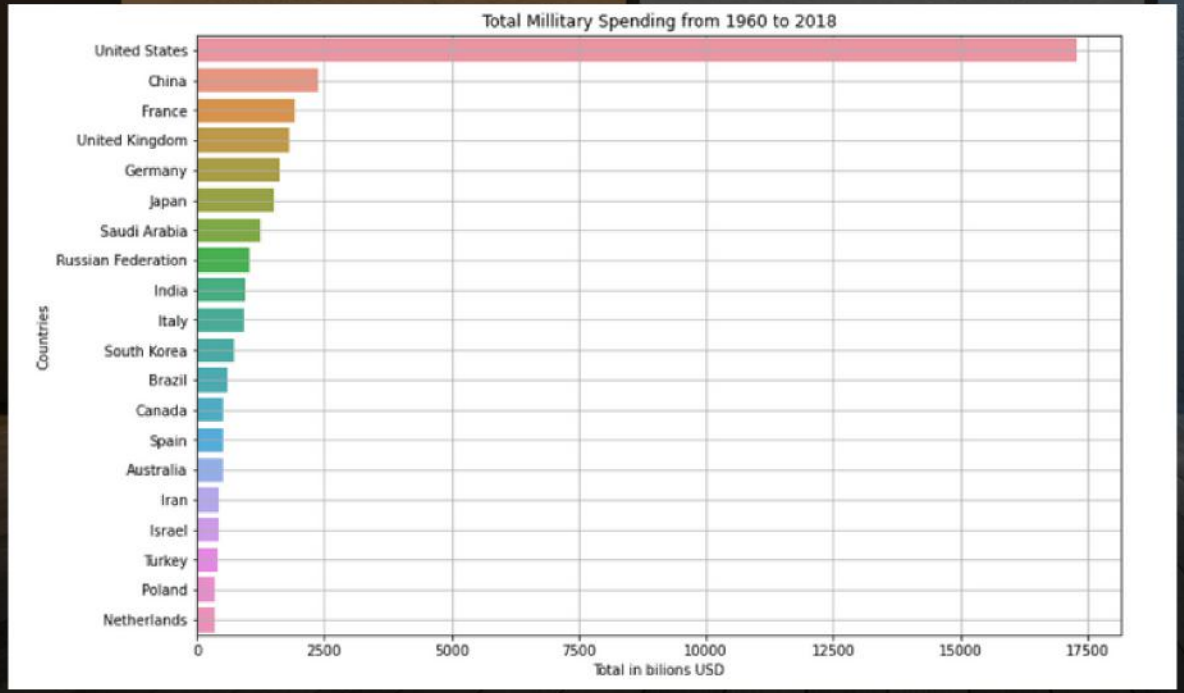


Result:

NULL Values are far greater in earlier years. This might be due to lack of technological advancements.

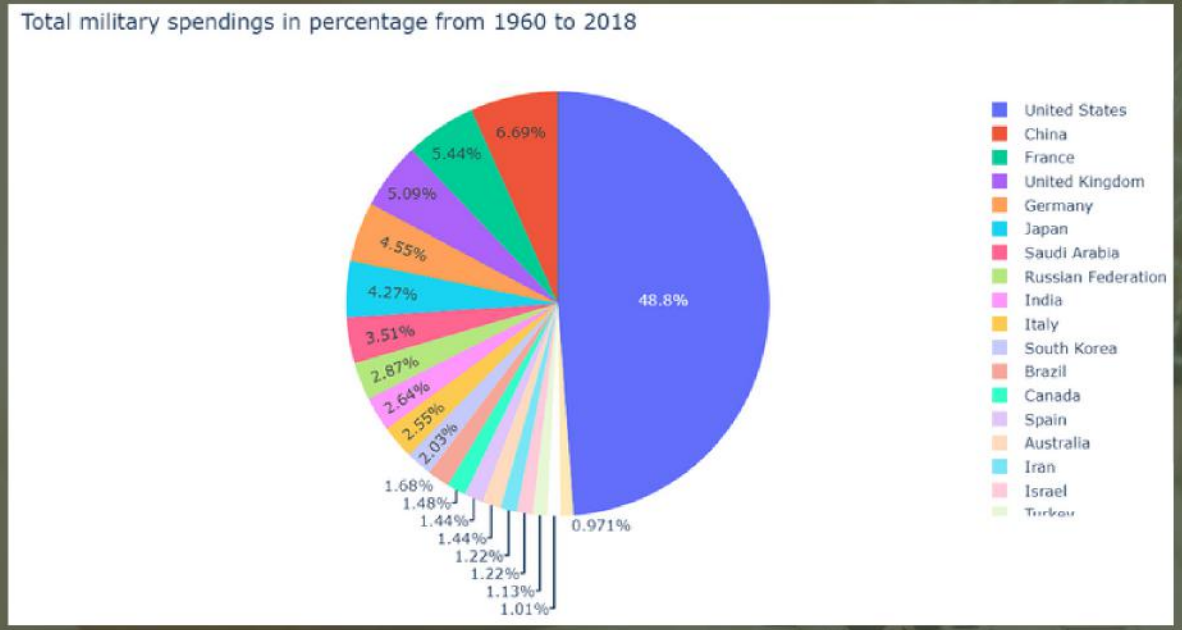
The Rampant availability of data has improved the density of the Data.

GLOBAL COMPARISION



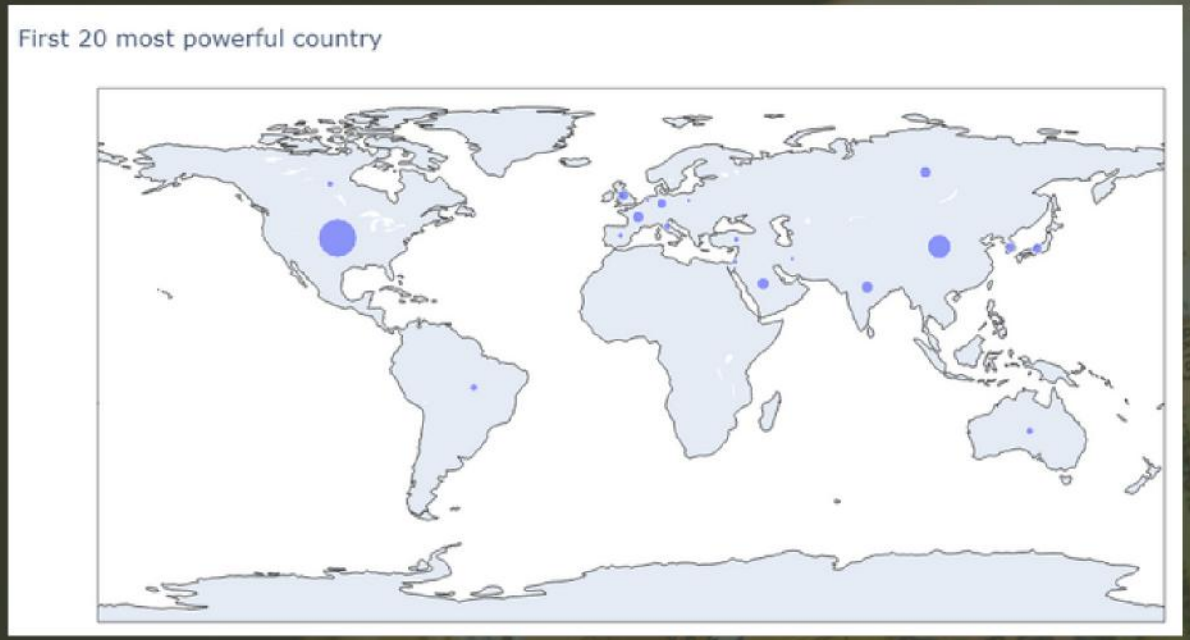
- This Dataset contain a lot information from around the world.
- It is a general curiosity of who is acing the stats.

SHARES



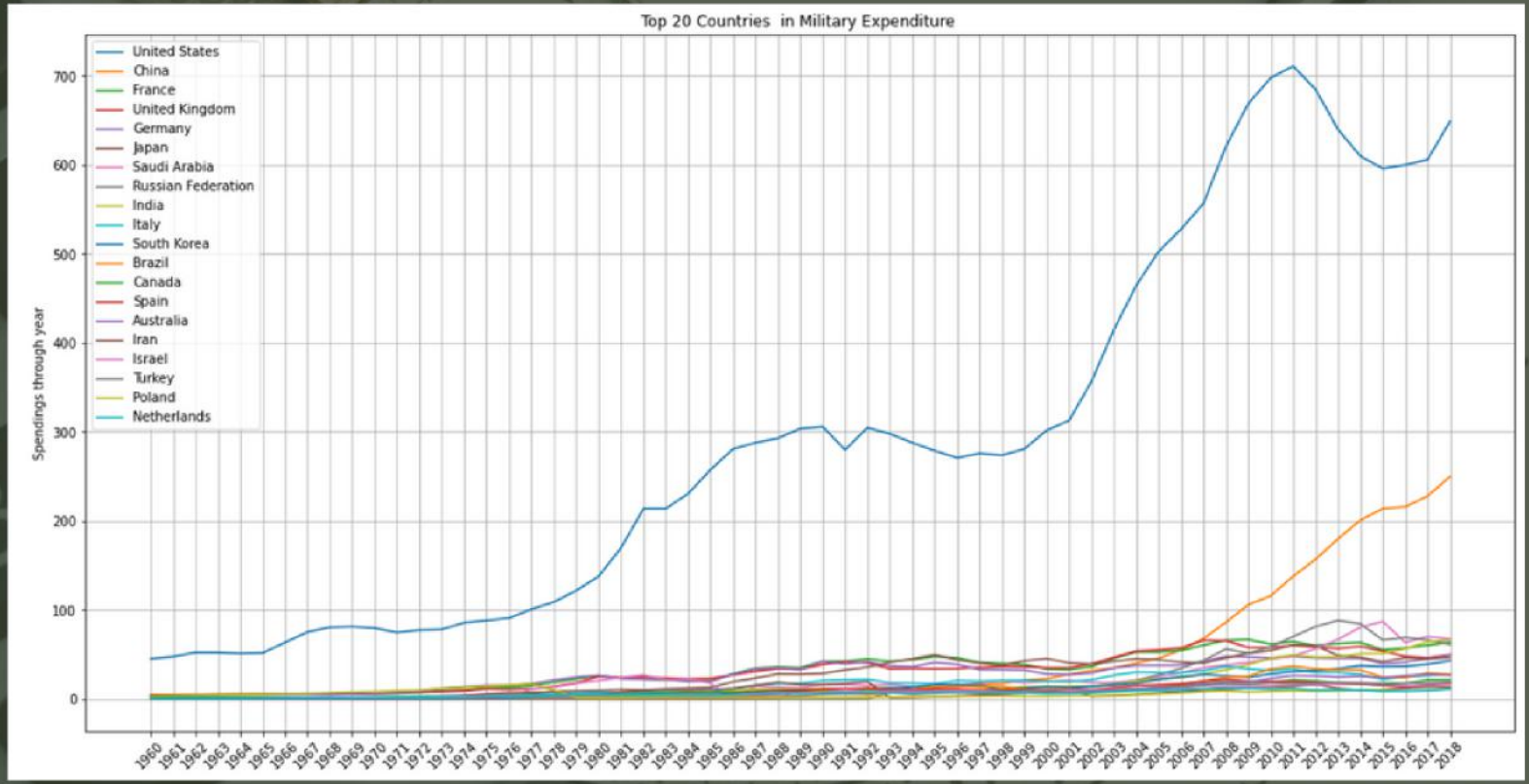
- The chart here shows how much shares a country/territory take out of the total spends

GEO PLOT

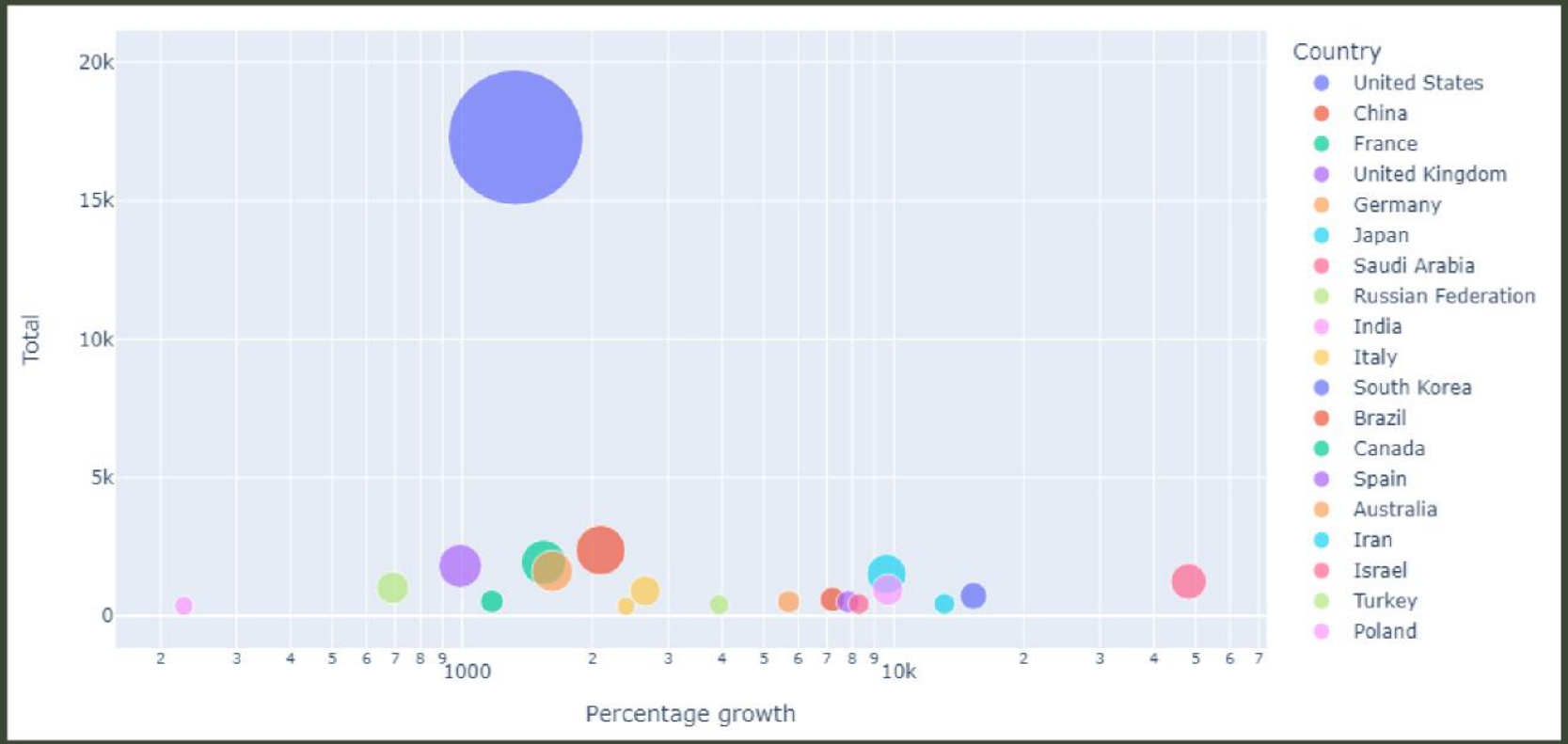


- GeoPlot used to locate and annotate the spending's of 20 major countries in 2018 (latest in the dataset)

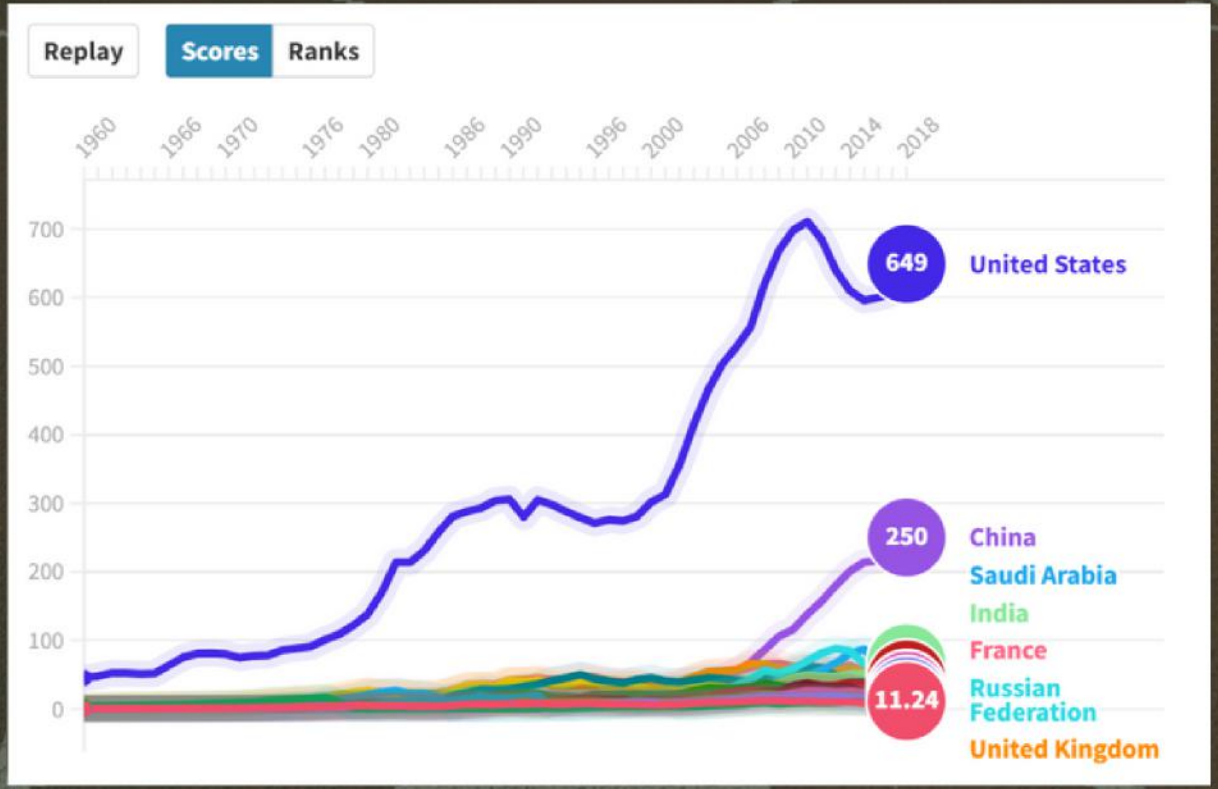
SPENDING OVER THE YEARS



ANALYSING GROWTH



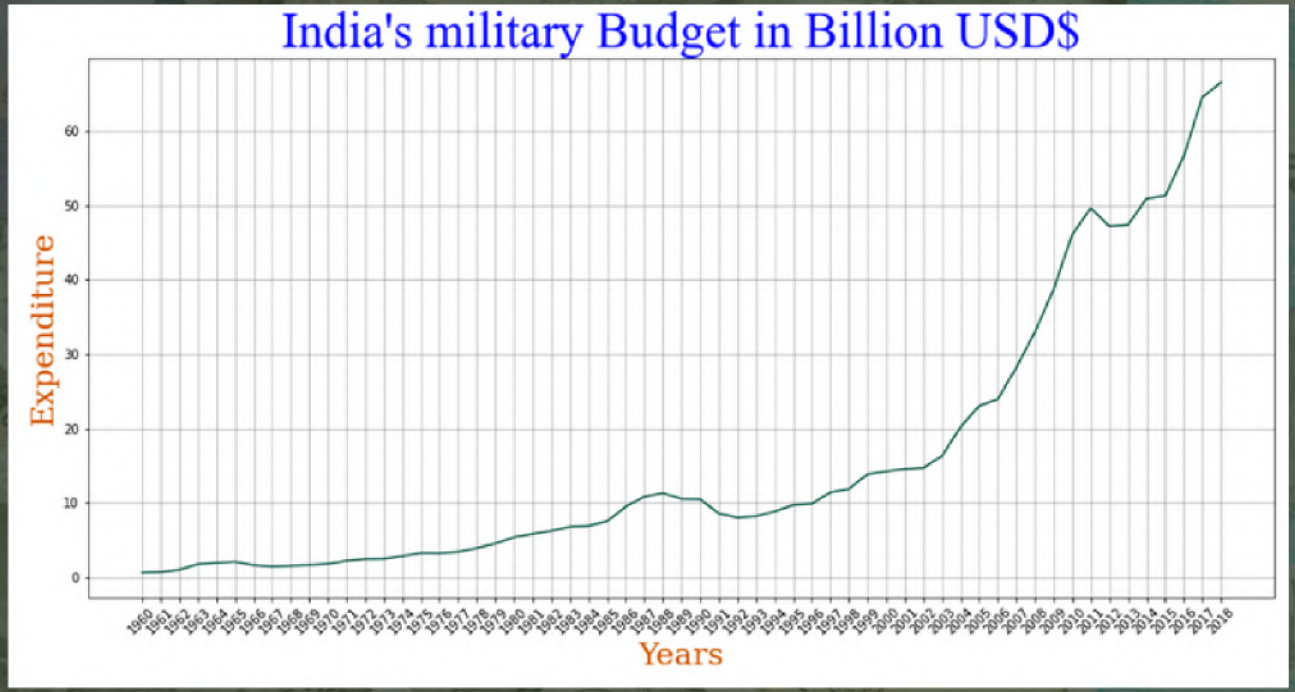
RACE GRAPH


Replay
Scores
Ranks
1960
1966
1970
1976
1980
1986
1990
1996
2000
2006
2010
2014
2018
700
600
500
400
300
200
100
0
649
United States
250
China
Saudi Arabia
India
France
11.24
Russian Federation
United Kingdom

INDIVIDUAL COUNTRY

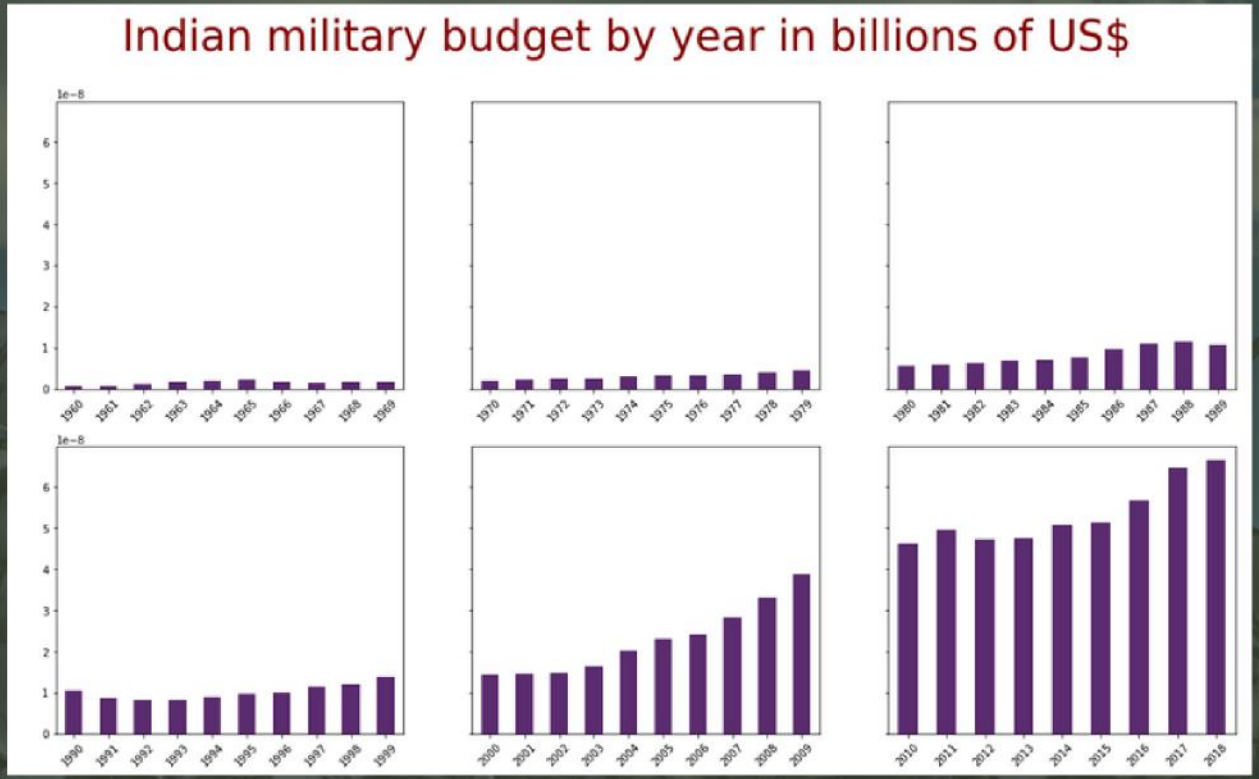
- Out of all countries we sorted out all the data related to India.
- An Analysis was then performed using facts

INDIA'S EXPENSES



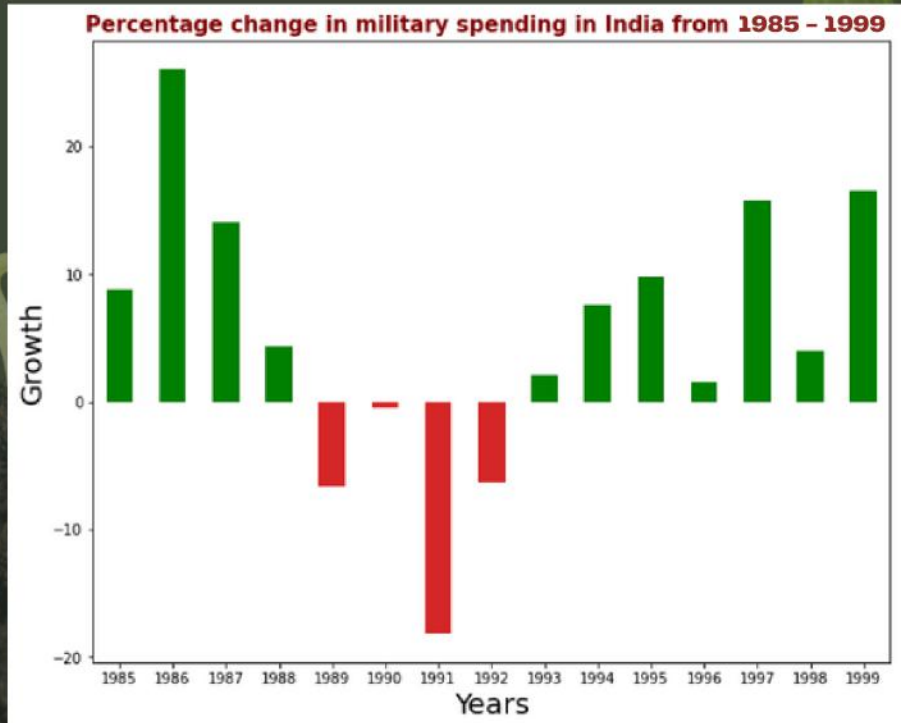
- A basic line graph to see how India's budget span's out

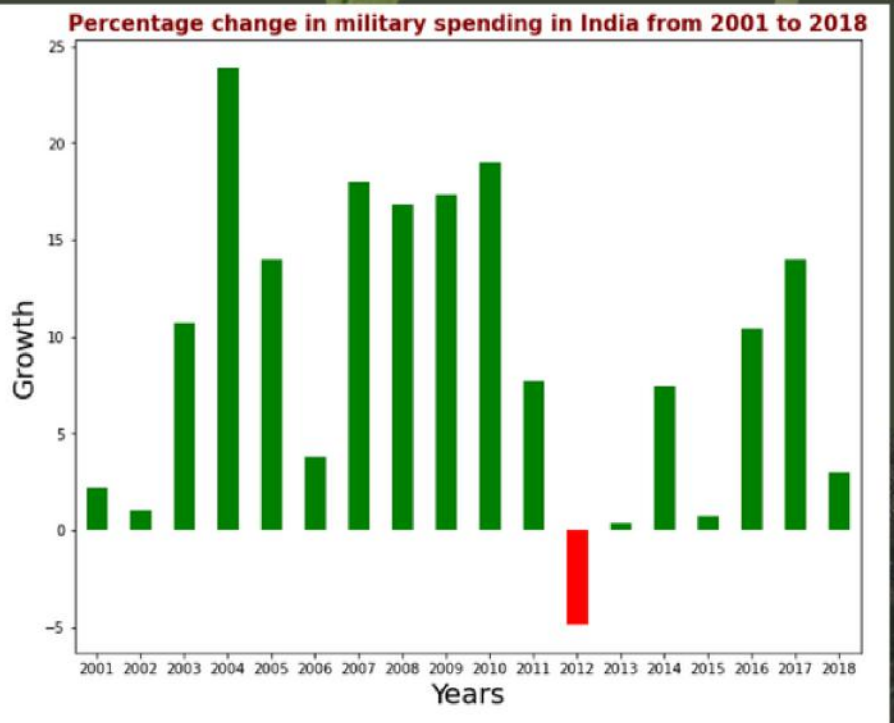
DATASET DIVISION



- Divide and conquer strategy used on Dataset for insights

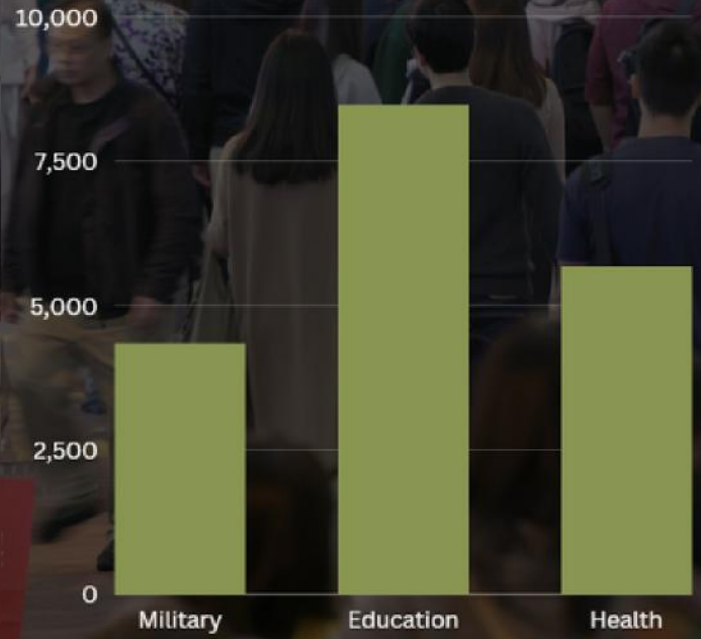
ANALYSING GROWTH

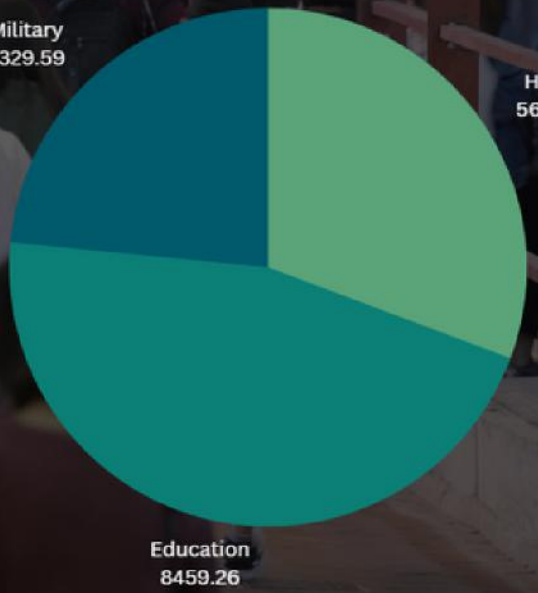




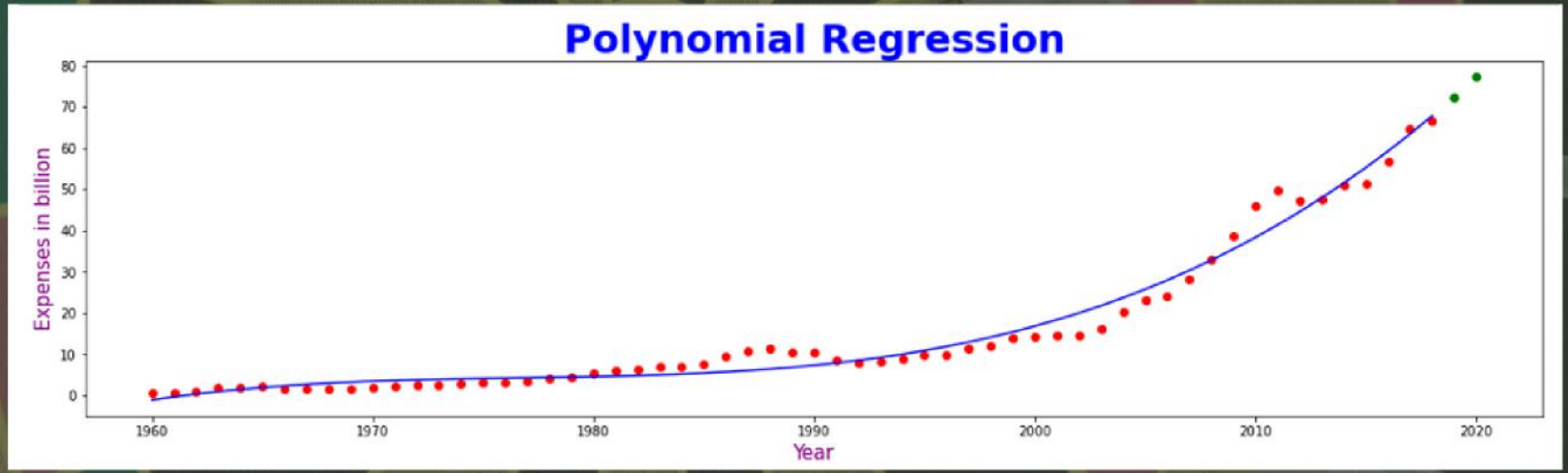
COMPARING ECONOMIC ASPECTS OF COUNTRY

Indian Military x Education x Health





PREDICTING POSSIBLE FUTURE BUDGET



Accuracy: 80.72 %

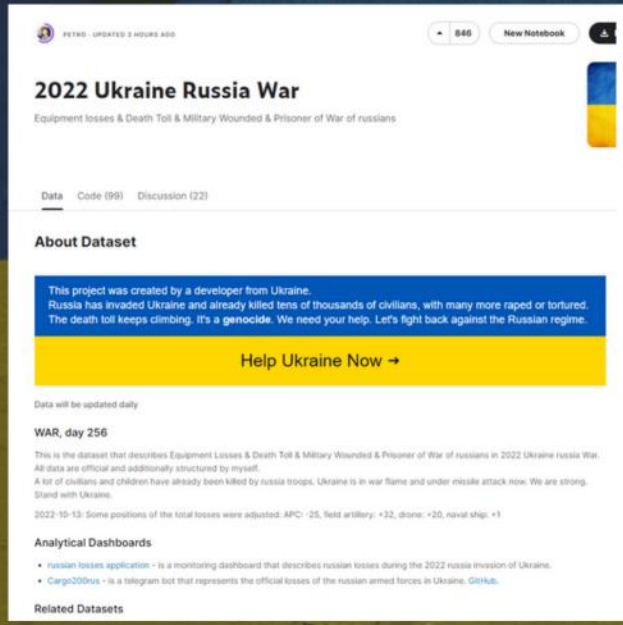
Method: Polynomial Regression

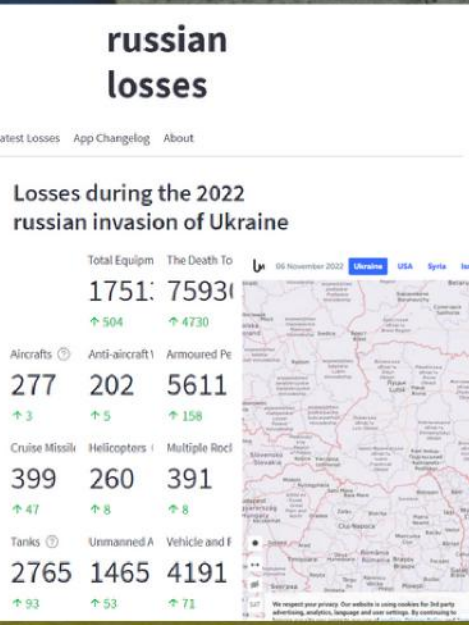
PART II:
ANALYZING WAR

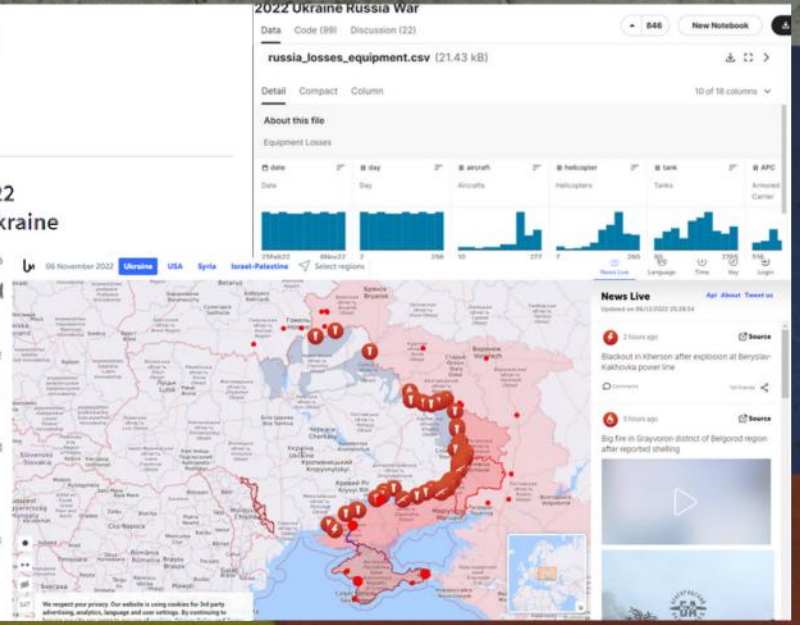
PART II: UKRAINE-RUSSIA CONFLICT

An ongoing horror show in northern Europe that has full potential to turn into the **next World War**.

PART II: UKRAINE-RUSSIA CONFLICT







UNDERSTANDING DATASET

Data

18 columns

257 rows*

null values present with varied datatypes like int64, object, float64, str, datetime

equipment_losses.csv

personnel_losses.csv

5 columns

257 rows*

null values present with varied datatypes like int64, object, float64

Equipment losses

```
[7]: equip_losses.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 254 entries, 0 to 253
Data columns (total 18 columns):
 #   Column                      Non-Null Count  Dtype
---  ------                      --------------  -----
 0   date                        254 non-null    object
 1   day                         254 non-null    int64
 2   aircraft                    254 non-null    int64
 3   helicopter                  254 non-null    int64
 4   tank                        254 non-null    int64
 5   APC                         254 non-null    int64
 6   field artillery             254 non-null    int64
 7   MRL                         254 non-null    int64
 8   military auto               65 non-null     float64
 9   fuel tank                   65 non-null     float64
 10  drone                       254 non-null    int64
 11  naval ship                  254 non-null    int64
 12  anti-aircraft warfare       254 non-null    int64
 13  special equipment           235 non-null    float64
 14  mobile SRBM system          36 non-null     float64
 15  greatest losses direction   178 non-null    object
 16  vehicles and fuel tanks     189 non-null    float64
 17  cruise missiles             189 non-null    float64
dtypes: float64(6), int64(10), object(2)
```

Personnel losses

```
[10]: person_losses.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 254 entries, 0 to 253
Data columns (total 5 columns):
 #   Column      Non-Null Count  Dtype
---  ------      --------------  -----
 0   date        254 non-null    object
 1   day         254 non-null    int64
 2   personnel   254 non-null    int64
 3   personnel*  254 non-null    object
 4   POW         62 non-null     float64
dtypes: float64(1), int64(2), object(2)
memory usage: 10.0+ KB
```

*at time of analysis, data is updated daily

DATA EXTRACTION & PREPROCESSING

Extracting Data From Kaggle

Using Kaggle API to directly extract, download, unzip and load data to variables

kaggle

Loading to a Pandas DataFrame

Finding NULL Values in Data

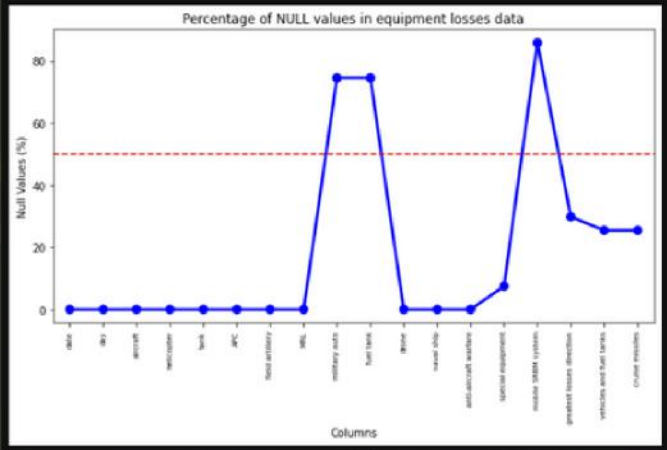
Imputing or Dropping NULL Value

DateTime conversion, object to string categorizing new data column into dataframe

Converting DataTypes as Needed

DEALING WITH NULL VALUES

```
equip_null = pd.DataFrame((equip_losses.isnull().sum())*100/equip_losses.shape[0]).reset_index()
equip_null.columns = ['Column Name', 'Null Values Percentage']
fig = plt.figure(figsize=(10,5))
ax = sns.pointplot(x="Column Name",y="Null Values Percentage",data=equip_null,color='blue')
plt.xticks(rotation =90,fontsize =7)
ax.axhline(50, ls='--',color='red')
plt.title("Percentage of NULL values in equipment losses data")
plt.ylabel("Null Values (%)")
plt.xlabel("Columns", )
plt.show()
```



COLUMNS

NULL Values Existing

07

85

SRBM

% Of NULL values in SRBM column

> MEDIAN

Columns with NULL Values more than 50%

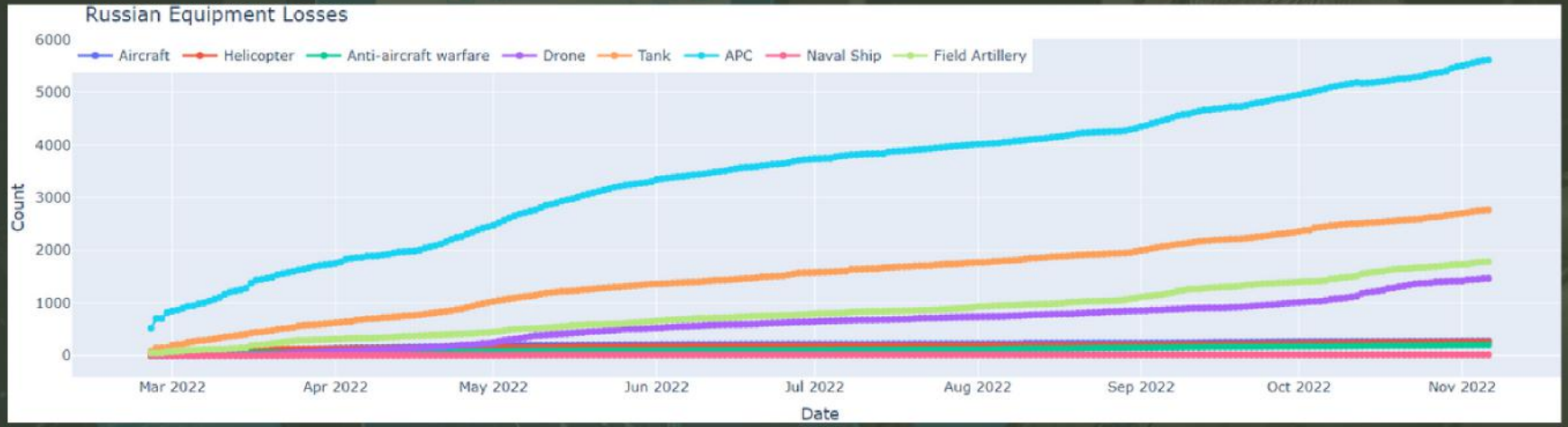
03

DATA VISUALIZATION / ANALYSIS

Russia has been steadily losing its own militants in this conflict. In 8 months of this war, Russia has lost close to 80000 of their military personnel

*made using Plotly

DATA VISUALIZATION / ANALYSIS

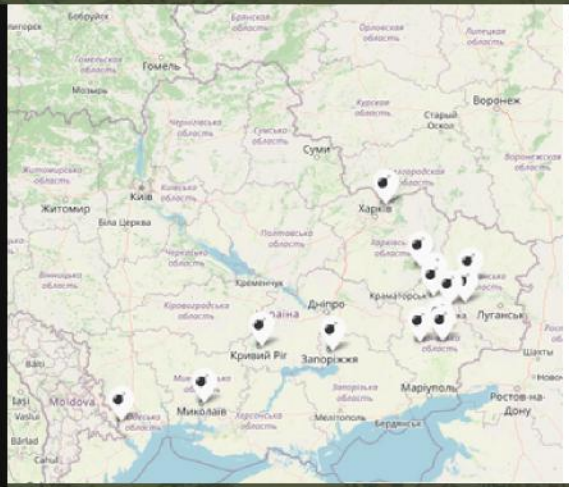


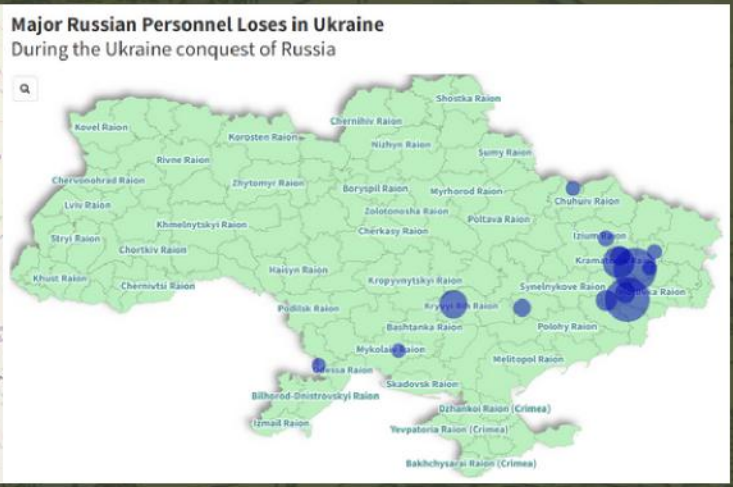
Equipment losses alone have cost Russian treasuries very deeply. They have lost a significant number of Aircrafts, Tanks, APCs, and Artilleries

*made using Plotly

MAPPING LOSSES LOCATIONS

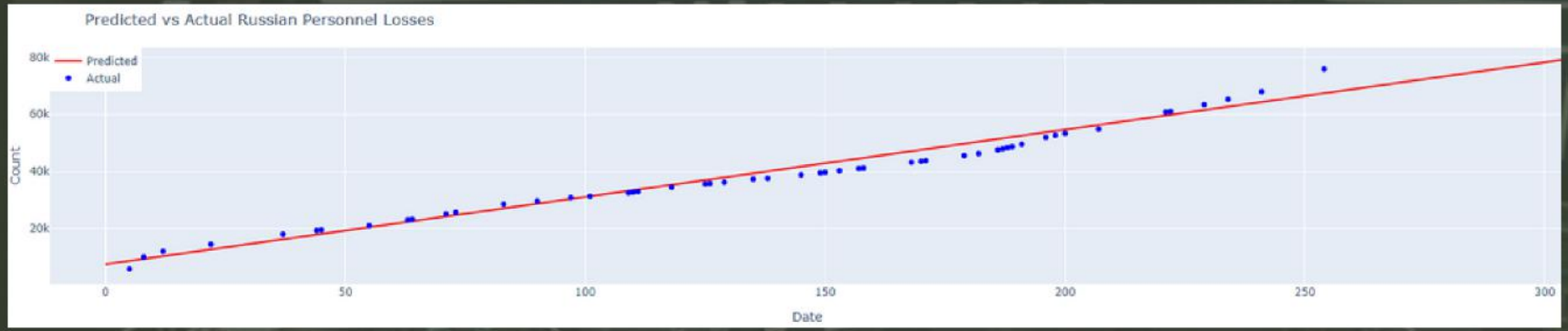
	City	Count	Latitude	Longitude
14	Donetsk	62	48.002777	37.805279
7	Bakhmut	61	48.594410	37.999830
11	Kramatorsk	32	48.738968	37.584351
13	Kryvyi Rih	25	47.910483	33.391783
5	Avdiivka	20	47.983300	37.266700
6	Kurakhove	14	48.136596	37.749133
10	Sloviansk	12	48.866700	37.616700
9	Zaporizhzhia	10	47.837800	35.138300
8	Lyman	9	49.209999	37.260746
1	Izyum	8	48.948319	38.491661
0	Sievierodonetsk	7	46.975033	31.994583
12	Mykolaiv	4	55.533300	28.650000
4	Novopavlivsk	3	46.679443	29.974368
2	Popasna	1	48.628242	38.372715
3	Slobozhanskyi	1	50.189320	36.424140





Plotting maps with folium in Python and using Flourish App

PREDICTING FUTURE LOSSES



Accuracy: 96.987 %

Method: Linear Regression

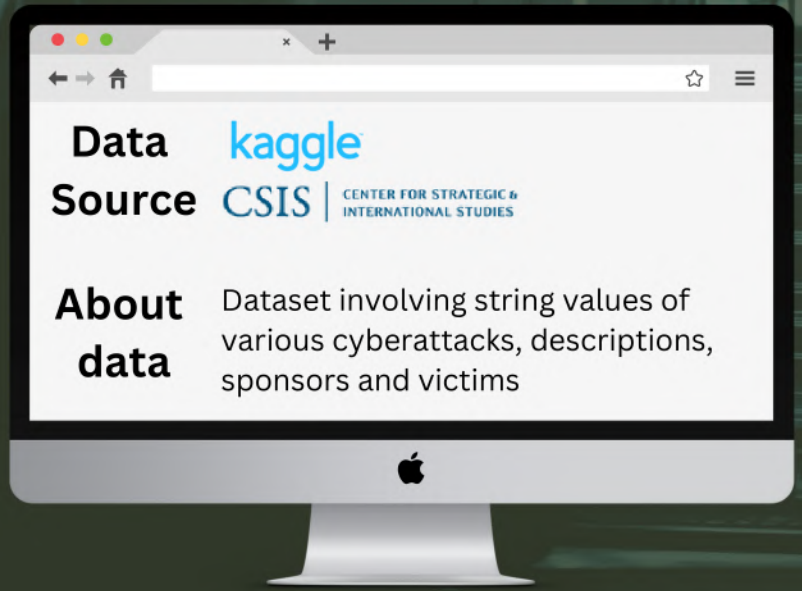
Since the war is presently still ongoing at the time of analysis, the data further might change drastically depending on further attacks from any belligerents. The accuracy and thus produced predictive results might not back a sudden intense warfare where losses might exponentially rise or of a subsiding war in the near future.


Остановите войну!
WAR AHEAD
Stop the War!

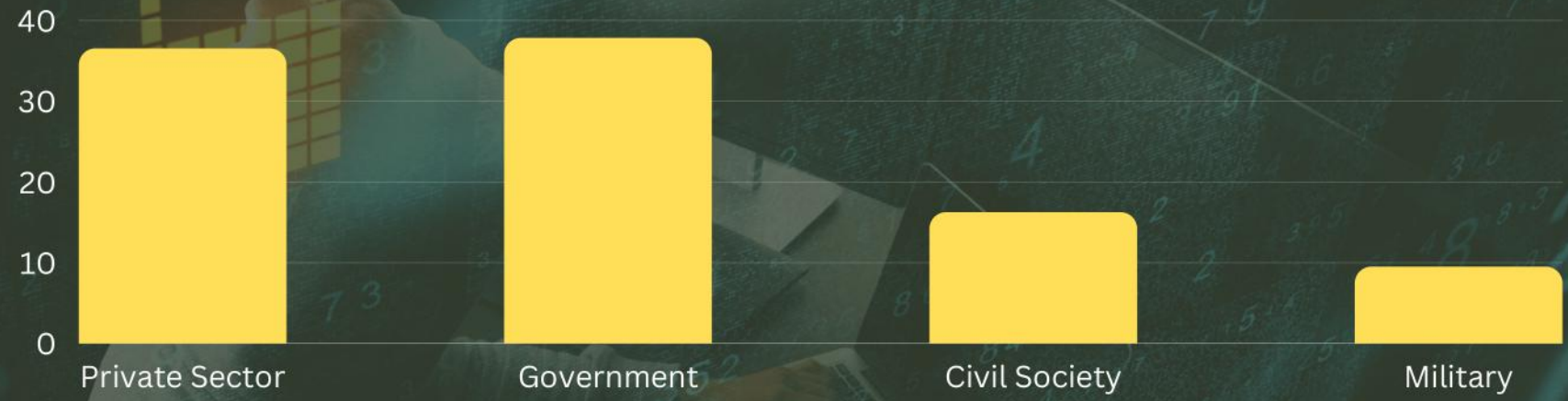
PART III:
CYBER WARFARE

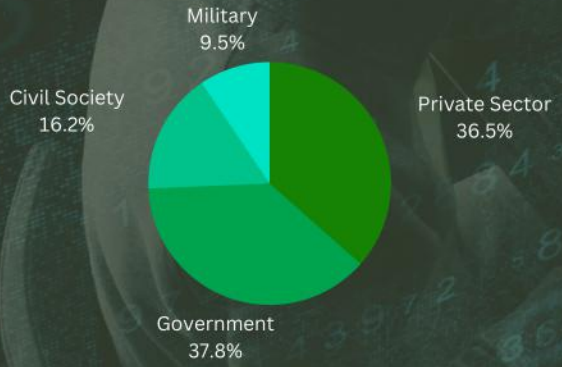
The next global offensive world is heavily underprepared for

ANALYZING DATASET



VISUALIZATIONS

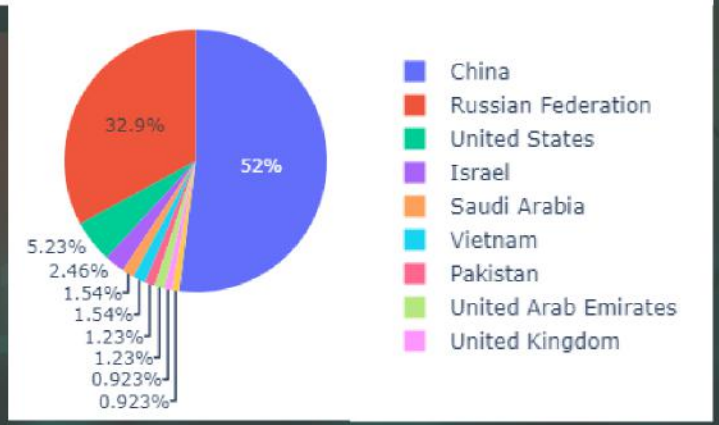




Most of the cyber attacks target governmental organization or private corporations

VISUALIZATIONS

China and Russia are two of the biggest contributors to state-sponsored cyberattacks happening worldwide.



RUSSIAN SPONSORED CYBER ATTACK ON UKRAINE

	Title	Date	Description	Victims	Sponsor	Type	Category
182	Attempt to compromise Ukraine's judicial system	2018-12-04	Ukraine's security agency thwarted an attack a...	Ukraine	Russian Federation	Espionage	Government
231	Compromise of Ukrainian government	2018-11-20	A Russian actor tied to Russia's Federal Secur...	Ukraine	Russian Federation	Espionage	Government
252	Bad Rabbit	2017-10-24	Using a tool called Bad Rabbit, a threat actor...	Ukraine, Japan, Russia, Bulgaria, Turkey	Russian Federation	Sabotage	Government
259	NotPetya	2017-07-01	Threat actors deploy a tool, called NotPetya, ...	Rosneft, WPP Plc., Maersk, Cie de Saint-Gobain...	Russian Federation	Data destruction	Government, Private sector
331	Gamaredon	2015-04-28	A Russian-linked threat group known as Gamared...	Ukraine	Russian Federation	Espionage	Government
349	Targeting of Ukrainian law enforcement and gov...	2015-03-13	A threat actor attempted to compromise Ukraini...	Ukraine	Russian Federation	Espionage	Military, Government
361	Crouching Yeti	2014-07-31	This threat actor targets companies in the edu...	United States, Spain, Japan, Germany, France, ...	Russian Federation	Espionage	Private sector, Government
368	APT 28	2014-10-28	This threat actor is linked to espionage campa...	Georgia, NATO, OSCE, France, Ukraine, United K...	Russian Federation	NaN	Government, Military, Private sector
369	Sandworm	2014-11-03	This threat actor targets industrial control s...	Russia, Ukraine, Poland, Lithuania, Belarus, A...	Russian Federation	Espionage	Private sector, Government
374	Attempted compromise of Ukrainian email accounts	2014-12-09	A threat actor attempted to compromise email a...	Ukraine	Russian Federation	Espionage	Government, Military
399	The Dukes	2013-02-01	This threat actor targets government ministrie...	United States, Georgia, Brazil, China, Japan, ...	Russian Federation	Espionage	Government, Private sector
405	Red October	2013-01-14	This threat actor targets governments, diploma...	Russia, Kazakhstan, Azerbaijan, Belgium, India...	Russian Federation	Espionage	Government, Private sector

RUSSIAN SPONSORED CYBER ATTACK ON UKRAINE

	Title	Date	Description	Victims	Sponsor	Type	Category
182	Attempt to compromise Ukraine's judicial system	2018-12-04	Ukraine's security agency thwarted an attack a...	Ukraine	Russian Federation	Espionage	Government
231	Compromise of Ukrainian government	2018-11-20	A Russian actor tied to Russia's Federal Sec...	Ukraine	Russian Federation	Espionage	Government
252	Bad Rabbit	2017-10-24	Us... actor...	Ukraine, Japan, Russia, Bulgaria, Turkey	Russian Federation	Sabotage	Government
259	[illegible]	2017-[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible] sector
331	Gamaredon	2015-04-28	A Russian-linked threat group known as Gamared...	Ukraine	Russian Federation	Espionage	Government
349	[illegible]	2015-[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Military, Government
361	Cloud Atlas	2014-07-31	This threat actor targets companies in th...	United States, Spain, Japan, Germany, France, ...	Russian Federation	Espionage	Private sector, Government
368	APT 28	2014-10-28	This threat actor is linked to espionage compa...	Georgia, NATO, OSCE, France, Ukraine, United K...	Russian Federation	NaN	Government, Military, Private sector
369	Sandworm	2014-11-03	This threat actor targets industrial co...	Russia, Ukraine, Poland, Lithuania, Belarus	Russian Federation	Espionage	Private sector, Government
374	Attempted compromise of Ukrainian email accounts	2014-12-09	A threat actor attempted to compromise email a...	Ukraine	Russian Federation	Espionage	Government, Military
399	The Dukes	2013-02-01	This threat actor targets government ministrie...	United States, Georgia, Brazil, China, Japan, ...	Russian Federation	Espionage	Government, Private sector
405	Red October	2013-01-14	This threat actor targets governments, diploma...	Russia, Kazakhstan, Azerbaijan, Belgium, India...	Russian Federation	Espionage	Government, Private sector

RUSSIA HAS BEEN ATTACKING UKRAINE ON THE CYBERFRONT FOR 71 MONTHS

THAT IS CLOSE TO 6 YEARS

January 13
Intensive diplomatic talks between Russia, US, Ukraine, NATO, Europe fail

February 17
Kremlin said it would respond with military-technical measures if the US continued to ignore calls for guarantees that Ukraine will never be admitted to NATO but denied plans to invade Ukraine.

February 21
President Putin recognizes independence of Ukrainian separatist regions, nullifying terms of existing Minsk peace agreements with Ukraine. Starting the Invasion

January 13
DEV-0586 deploys WhisperGate wiper to limited number of Ukrainian government and IT sector systems.

February 15–16
Russian military intelligence (GRU) DDoS attacks against Ukrainian financial institutions

February 23
IRIDIUM deploys FoxBlade wiper to hundreds of systems in Ukrainian government, IT, energy, and financial sectors.

Source: Microsoft, Digital.Security.Unit. An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

UKRAINE INDUSTRIES UNDER ATTACK

WEB SCRAPING LATEST DATA

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Significant Cyber Incidents

This timeline records significant cyber incidents since 2006. We focus on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million

csis.org

August 2022. Hackers targeted the website of Ukraine's state energy agency responsible for the oversight of Ukraine's nuclear power plants. The agency stated Russian hackers carried out the attack.

May 2022. Russian hackers hit Italian websites with a DDoS attack, including the Senate, the Ministry of Defence and the National Health Institute. The group states its goal was to target NATO countries and Ukraine.

April 2022. The Romanian National Directorate of Cyber Security said that multiple public and private sector websites were hit with DDoS attacks. The victims included the ministry of defense, border police, national railway company, and the OTP Bank. A group claiming credit for the attack said on Telegram that it hacked the websites because Romania supported Ukraine since the Russian invasion of the country.

April 2022 . Hackers targeted a Ukrainian energy facility, but CERT-UA and private sector assistance largely thwarted attempts to shutdown electrical substations in Ukraine. Researchers believe the attack came from the same group with ties to the Russian GRU that targeted Ukraine's power grid in 2016, using an updated form of the same malware.

February 2022. The websites of the Ukrainian Cabinet of Ministers and Ministries of Foreign Affairs, Infrastructure, and Education were disrupted in the days before Russian troops invaded Ukraine. Wiper malware was also used to penetrate the networks of one Ukrainian financial institution and two government contractors.

USING NLP FOR DEEP ANALYSIS

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

	Date	Description	Key Words
0	August 2022	Hackers targeted the website of Ukraine's stat...	[Hackers, targeted, website, Ukraine, state, e...
1	May 2022	Russian hackers hit Italian websites with a DD...	[Russian, hackers, hit, Italian, websites, DDo...
2	April 2022	The Romanian National Directorate of Cyber Se...	[The, Romanian, National, Directorate, Cyber, ...
3	April 2022	. Hackers targeted a Ukrainian energy facility...	[Hackers, targeted, Ukrainian, energy, facilit...
4	February 2022	The websites of the Ukrainian Cabinet of Minis...	[The, websites, Ukrainian, Cabinet, Ministers,...

CONCLUSION

From the Analysis, Cyber Warfare is the new method of war rather than swords and guns and cannons. With the rise of digitalization, threat actors are finding more and more methods to exploit others. When this crosses national boundaries and onto bigger governmental/military target, it blows up into a cyberwar. There is urgent need to have top-tier cyber security across all levels -
from the civillians to the highest power of the nation.

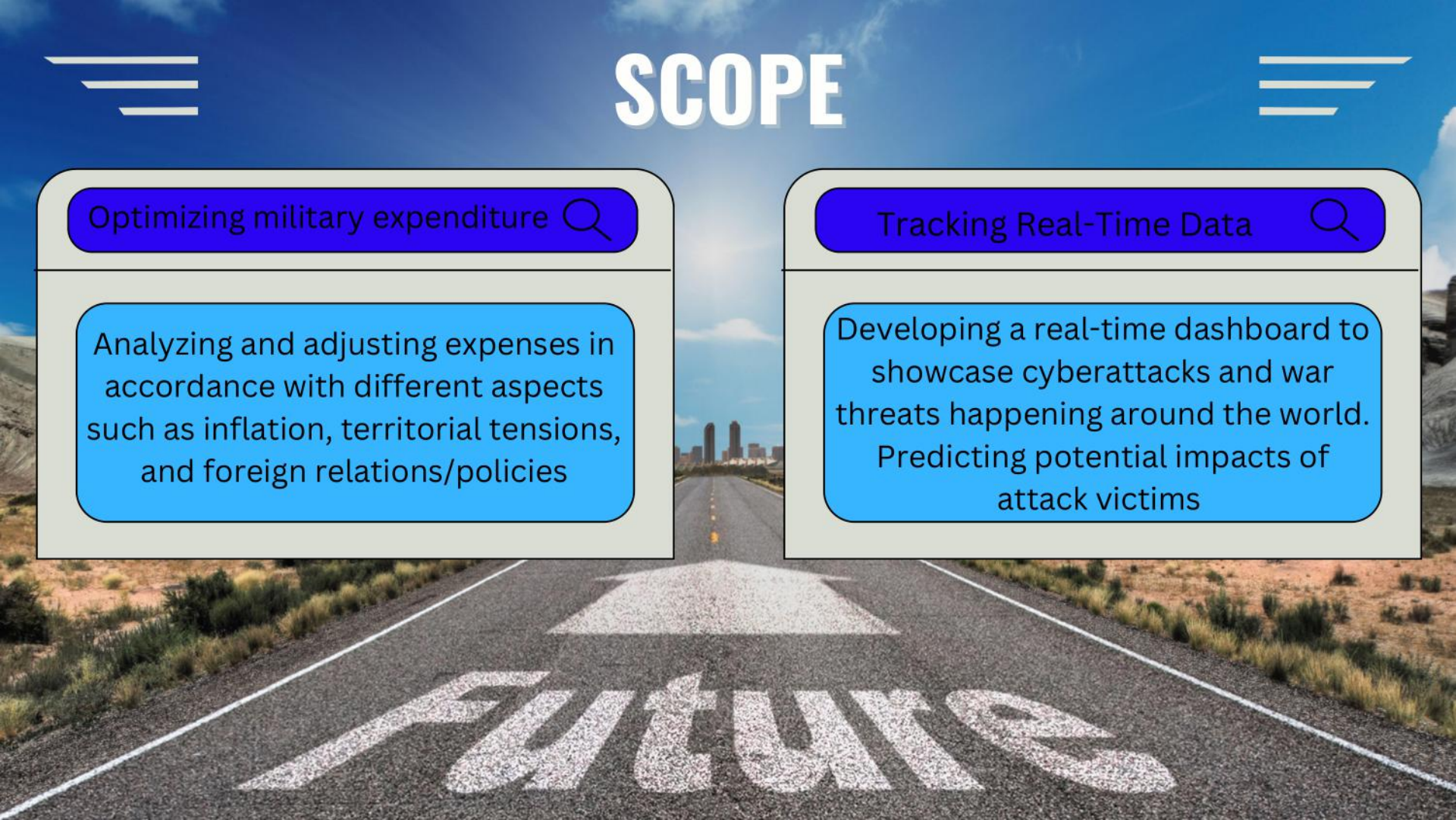
SCOPE

Optimizing military expenditure

Analyzing and adjusting expenses in accordance with different aspects such as inflation, territorial tensions, and foreign relations/policies

Tracking Real-Time Data

Developing a real-time dashboard to showcase cyberattacks and war threats happening around the world. Predicting potential impacts of attack victims



REFERENCES

- Microsoft, Digital Security Unit. An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
- Elgin, C., et al. "Military Spending and Sustainable Development." Review of Development Economics, vol. 26, no. 3, 2022, pp. 1466-1490. SCOPUS, www.scopus.com, doi:10.1111/rode.12893
- Sarwar, S., & Idrees, A. S. (2021). Impact of Military Expenditures on the Globalization Process: A Spatial Econometric Analysis for African Region. Journal of Asian and African Studies. https://doi.org/10.1177/00219096211010324
- Amirkhanov, Eltaj. (2022). Analysis of the Russia-Ukraine War (2014) from the Perspectives of Three Theories of International Relations.
- Eichensehr, K. (2022). Ukraine, Cyberattacks, and the Lessons for International Law. AJIL Unbound, 116, 145-149. doi:10.1017/aju.2022.20
- Russia's Use of Cyberattacks: Lessons from the Second Ukraine War - Foreign Policy Research Institute (fpri.org)

THANK YOU

PROJECT BY

APOORV GUPTA

apoorv.gupta.btech2021@sitpune.edu.in
+91 98213 80213

/in/er-apoorv-gupta/

/erApoorvGupta

AADITH SUKUMAR

aadith.sukumar.btech2021@sitpune.edu.in
+91 98330 27155

/in/aadith-sukumar/

/aadi1011