ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

Fortifying the Global Data Fortress: A Multidimensional Examination of Cyber Security Indexes and Data Protection Measures across 193 Nations

Yijie Weng[1,a], Jianhao Wu[2,b,*]

[1]*University of Maryland, MD, USA*
[2]*Cornell University, NY, USA*
[a]*jaweng333@gmail.com*, [b]*johnwu2417@gmail.com*
[*]*Corresponding author*

Abstract: *This study conducts a comprehensive examination of the global cyber security landscape by analysing four prominent indexes: the Cybersecurity Exposure Index (CEI), Global Cyber Security Index (GCI), National Cyber Security Index (NCSI), and Digital Development Level (DDL). Leveraging an extensive dataset spanning 193 countries and territories across five geographic regions, the research employs advanced statistical techniques and data visualization methodologies to unravel the multidimensional challenges and opportunities in fortifying international data protection. By uncovering potential correlations, regional disparities, and emerging trends shaping the cyber security paradigm, the study aims to provide actionable insights to inform policymakers, security professionals, and stakeholders. The overarching objective is to enhance data protection measures, foster cross-border collaboration, and cultivate a resilient global digital ecosystem, while contributing a comprehensive, data-driven perspective to ongoing dialogues on mitigating evolving cyber threats and safeguarding the world's digital fortress.*

Keywords: *Cyber Security, Data Security, Security AI, Digital Technologies, Cybersecurity Exposure Index, Global Cyber Security Index, National Cyber Security Index, Digital Development Level*

1. Introduction

In the digital age, data has emerged as a pivotal asset, fueling innovation, economic growth, and societal advancement. However, the rapid proliferation of digital technologies and the exponential growth of data have amplified the risks associated with cyber threats, data breaches, and malicious cyber activities. The consequences of such incidents can be far-reaching, ranging from financial losses and reputational damage to compromised national security and erosion of public trust. The global community has witnessed a surge in sophisticated cyber attacks targeting critical infrastructure, government agencies, and private enterprises, underscoring the urgency of fortifying data security measures on an international scale. [1] Recognizing the transnational nature of cyber threats, numerous initiatives have been undertaken to assess and enhance the cyber security posture of nations worldwide. Among these initiatives are four prominent cyber security indexes: the Cybersecurity Exposure Index (CEI) [2], Global Cyber Security Index (GCI) [3], The National Cyber Security Index (NCSI) [4], and The Digital Development Level (DDL) [5].

This study aims to conduct a comprehensive examination of these four cyber security indexes across 193 countries and territories, spanning five geographical regions: Africa, North America, South America, Europe, and Asia-Pacific. Leveraging advanced statistical techniques and data visualization methodologies, the research endeavors to unravel the intricate patterns, regional disparities, and emerging trends that shape the global cyber security landscape. The overarching objective is to provide actionable insights and recommendations that can inform policymakers, security professionals, and stakeholders in their efforts to enhance data protection measures, foster international collaboration, and cultivate a resilient digital ecosystem. By rigorously examining these indices, the study aspires to contribute to the ongoing discourse on cyber security, offering a comprehensive and data-driven perspective on safeguarding the global data fortress against evolving threats. These research findings hold the potential to guide strategic decision-making processes, facilitate the development of robust cyber security

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

frameworks, and foster international cooperation in mitigating the risks posed by cyber threats, ultimately strengthening the global digital infrastructure and protecting the invaluable data.

2. Literature Review

The evolution of cyber threats and data breaches has been well-documented in various studies. The latest 2023 IBM Cost of a Data Breach Report [6] revealed that the average total cost of a data breach increased by 15% over the past 3 years, reaching $4.45 million. Organizations that extensively leverage security AI and automation can achieve significant cost savings, with an average of USD 1.76 million compared to those that don't utilize such technologies. Similarly, the recent 2023 Verizon Data Breach Investigations Report [7] highlighted that cyber-attacks have become more frequent, complex, and costly, with ransomware and phishing attacks being among the most prevalent threats. Most data breaches, a staggering 83%, involve external actors driven primarily by financial motivations. Moreover, the human element plays a crucial role in a significant portion of breaches, accounting for 74% of incidents, which include social engineering attacks, errors, or misuse. Notably, a substantial 50% of all social engineering attacks are attributed to pretexting incidents, nearly doubling the previous year's figures. This highlights the persistent threat posed by deceptive tactics exploiting human vulnerabilities within organizations.

In response to these challenges, various frameworks and models have been developed to assess and improve cyber security postures. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 [8], for instance, provides a comprehensive set of guidelines and best practices for organizations to manage and reduce cyber risk. Additionally, the International Organization for Standardization (ISO) has introduced the ISO/IEC 27000 series [9], which outlines information security management systems and practices.

Regional and national initiatives have also been undertaken to address data protection concerns. The European Union's General Data Protection Regulation (GDPR) [10] has set a global standard for data privacy and security. Similarly, the United States has implemented various cybersecurity measures, such as the Cybersecurity and Infrastructure Security Agency (CISA) and the National Strategy for Trusted Identities in Cyberspace (NSTIC) [11]. Despite these efforts, the challenges and limitations of current approaches persist. The dynamic nature of cyber threats and the rapid evolution of technology often outpace the ability of organizations and nations to adapt their security measures [12]. Furthermore, the lack of standardized metrics and assessment methodologies hinders the effective evaluation and comparison of cyber security postures across different regions and nations [13].

3. Methodology

3.1 Statistical Analysis Techniques

In this study, we leveraged the power of several Python libraries to perform statistical analysis and data visualization. The primary library utilized was Pandas, which facilitated efficient data manipulation and analysis. Numpy, a fundamental library for scientific computing, was employed to perform numerical operations on arrays and matrices. For visualizing the data, we relied on the robust capabilities of Matplotlib, Seaborn and Plotly. Matplotlib (and Seaborn), widely used plotting libraries, enabled us to create static, high-quality 2D and 3D visualizations. Plotly generated interactive, web-based visualizations, enhancing the exploratory data analysis process.

```
import pandas as pd
import matplotlib.pyplot as plt
import plotly.express as px
import seaborn as sns
import plotly.graph_objects as go
from plotly.subplots import make_subplots
```

3.2 Data Sources and Description

This study draws upon a comprehensive dataset (Figure 1 shows *the dataset* Cyber_security.csv *pandas data frame Information*) titled "Cyber Security Indexes," [14] (Figure 2 shows the *dataset Cyber_security.csv top 10 rows data preview*) encompassing four distinct indicators (Figure 3 shows each index's *statistics description*) that collectively illustrate the current global cyber security landscape

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

across 193 countries and territories, grouped into five geographical regions: Africa, North America, South America, Europe, and Asia-Pacific (Figure 4 shows country count by region). The Cybersecurity Exposure Index (CEI) by PasswordManagers.co measures a country's exposure to cybercrime on a scale from 0 to 1, with higher scores indicating greater exposure. The Global Cyber Security Index (GCI) by the International Telecommunication Union (ITU) assesses the commitment of countries to cybersecurity and their legal, technical, and organizational capabilities. The National Cyber Security Index (NCSI) by the e-Governance Academy Foundation evaluates the preparedness of nations to prevent cyber threats and manage cyber incidents. Lastly, The Digital Development Level (DDL), also by the e-Governance Academy Foundation, offers a holistic measure of a nation's digital development and potential vulnerability to cyber threats. The dataset, collected from open sources, has been previously utilized in relevant research, ensuring its reliability and validity in the field of cybersecurity analysis.

```
df = pd.read_csv('./Cyber_security.csv')
df.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 192 entries, 0 to 191
Data columns (total 6 columns):
 #   Column   Non-Null Count  Dtype
---  ------   --------------  -----
 0   Country  192 non-null    object
 1   Region   192 non-null    object
 2   CEI      108 non-null    float64
 3   GCI      190 non-null    float64
 4   NCSI     167 non-null    float64
 5   DDL      152 non-null    float64
dtypes: float64(4), object(2)
memory usage: 9.1+ KB
```

Figure 1: Dataset Cyber_security.csv *pandas data frame Information.*

```
df.head(10)
```

	Country	Region	CEI	GCI	NCSI	DDL
0	Afghanistan	Asia-Pasific	1.000	5.20	11.69	19.50
1	Albania	Europe	0.566	64.32	62.34	48.74
2	Algeria	Africa	0.721	33.95	33.77	42.81
3	Andorra	Europe	NaN	26.38	NaN	NaN
4	Angola	Africa	NaN	12.99	9.09	22.69
5	Antigua and Barbuda	North America	NaN	15.62	11.69	57.10
6	Argentina	South America	0.514	50.12	63.64	60.43
7	Armenia	Europe	0.655	50.47	35.06	55.06
8	Australia	Asia-Pasific	0.131	97.47	66.23	77.61
9	Austria	Europe	0.162	93.89	68.83	75.76

Figure 2: Dataset Cyber_security.csv top 10 rows data preview.

```
df.describe()
```

	CEI	GCI	NCSI	DDL
count	108.000000	190.000000	167.000000	152.000000
mean	0.471861	52.769526	43.306587	51.707829
std	0.217246	34.884013	26.820907	18.283847
min	0.110000	1.350000	1.300000	11.300000
25%	0.279500	18.257500	19.480000	36.532500
50%	0.483000	53.145000	40.260000	51.790000
75%	0.624250	89.187500	64.940000	65.237500
max	1.000000	100.000000	96.100000	82.930000

Figure 3: Column statistics description.

```
dfr.columns = ['Region', 'Country Count']
dfr['text'] = dfr['Country Count'].astype(str)
fig = px.bar(dfr, title='Country Count by Region', x='Country Count', y=['Region',
color_discrete_sequence=px.colors.qualitative.Vivid, text='text', orientation='h')
fig.update_traces(textposition='outside')
fig.show()
```

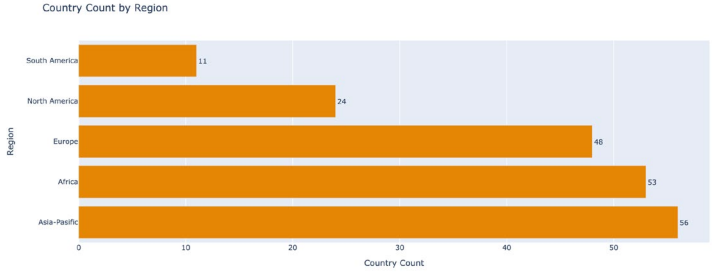

Figure 4: Country count by region.

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

3.3 Missing Data Distribution and Implications

The analysis of data completeness across the four cybersecurity indexes – the Cybersecurity Exposure Index (CEI), Global Cyber Security Index (GCI), National Cyber Security Index (NCSI), and Digital Development Level (DDL) – reveals significant variations in missing data proportions (*Figure 5 shows percentage of null values in each index column*). The CEI exhibits the highest percentage of null values at 43.75%, while the GCI emerges as the most complete with only 1.04% missing data. The NCSI and DDL exhibit moderate levels of missing data, at 13.02% and 20.83%, respectively (*Figure 5 shows the percentage of null values in each index column*). These disparities in data availability highlight the complexities of comprehensive global cybersecurity data collection and reporting, underscoring the need for enhanced international collaboration, knowledge sharing, and capacity-building initiatives to strengthen cybersecurity data infrastructure and foster a resilient global data fortress.

```
null_percentage = df[['CEI', 'GCI', 'NCSI', 'DDL']].isnull().mean() * 100
plt.figure(figsize=(10, 6))
bars = null_percentage.plot(kind='bar', color='orange')
for bar in bars.patches:
    plt.annotate(format(bar.get_height(), '.2f') + '%', (bar.get_x() + bar.get_width() / 2,
    bar.get_height()), ha='center', va='center', xytext=(0, 5), textcoords='offset points')
plt.title('Percentage of Null Values in CEI, GCI, NCSI, DDL Columns')
plt.xlabel('Columns')
plt.ylabel('Percentage of Null Values')
plt.xticks(rotation=0)
plt.grid(axis='y')
plt.tight_layout()
plt.show()
```

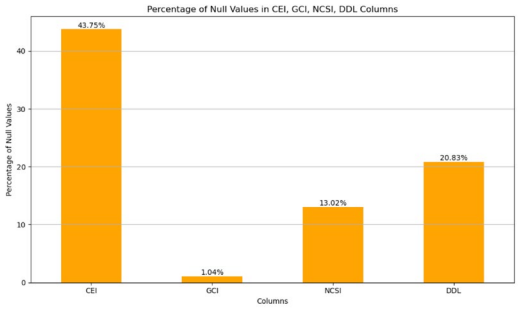

Figure 5: Percentage of null values in each index column.

4. Results and Analysis

4.1 Global Overview of Cyber Security Indexes [15]

```
fig = make_subplots(rows=2, cols=2, subplot_titles=('CEI Distribution', 'GCI Distribution', 'NCSI
Distribution', 'DDL Distribution'))
fig.add_trace(go.Histogram(x=df['CEI']), row=1, col=1)
fig.add_trace(go.Histogram(x=df['GCI']), row=1, col=2)
fig.add_trace(go.Histogram(x=df['NCSI']), row=2, col=1)
fig.add_trace(go.Histogram(x=df['DDL']), row=2, col=2)
fig.update_layout(showlegend=False)
fig.show()
```

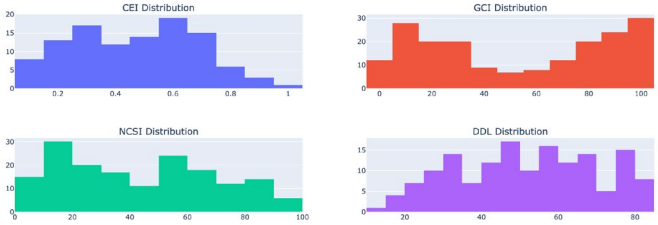

Figure 6: Cyber security index distributions.

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

The skewed distribution patterns (*Figure 6 shows cyber security index distributions*) and presence of outliers exhibited in the Cybersecurity Exposure Index (CEI), Global Cyber Security Index (GCI), National Cyber Security Index (NCSI), and Digital Development Level (DDL) unveil stark disparities in cybersecurity preparedness, threat response capabilities, and digital development across nations. This heterogeneity challenges the notion of a uniform, globally cohesive approach to combating cyber threats, underscoring the urgency of bridging gaps through capacity-building initiatives, knowledge transfer, and strategic interventions. The non-normal distributions suggest a significant portion of the global community may be lagging in cybersecurity efforts and digital infrastructure development, necessitating nuanced, tailored approaches to address unique regional and national needs. By revealing these disproportions, this study serves as a catalyst for policymakers and stakeholders to re-evaluate existing strategies, forge collaborative pathways, and implement effective measures to cultivate a more resilient and equitable global digital ecosystem, safeguarding the collective data fortress from evolving cyber threats.

4.2 Cyber Security Index by Regions Analysis

4.2.1 Cybersecurity Exposure Index (CEI)

The Cybersecurity Exposure Index (CEI) provides a crucial lens into the varying degrees of vulnerability to cybercrime across nations and regions. This index quantifies the level of exposure on a scale from 0 to 1, with higher scores indicating heightened susceptibility to cyber threats.

```
cei_df = df[['Country', 'Region', 'CEI']].dropna(subset=['CEI'])
plt.figure(figsize=(10, 6))
sns.violinplot(data=cei_df, x='Region', y='CEI')
plt.title('CEI by Regions')
plt.xlabel('Region')
plt.ylabel('CEI')
plt.show()
```

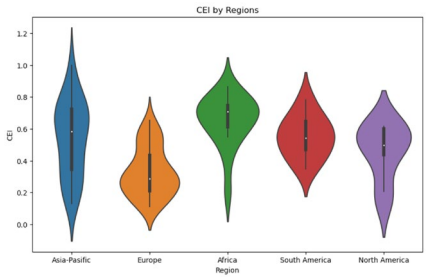

Figure 7: Cybersecurity Exposure Index (CEI) violin plots by regions.

The regional analysis of the Cybersecurity Exposure Index (CEI) data unveils a stark contrast (*Figure 7 shows Cybersecurity Exposure Index (CEI) violin plots by regions.*), with Europe emerging as the least vulnerable region, exhibiting the lowest average CEI score of 0.3285 per country, attributable to robust cybersecurity measures. Conversely, Africa grapples with the highest level of exposure, averaging 0.6431 per country, necessitating targeted interventions and capacity-building initiatives. South America closely trails with an average of 0.5766, highlighting the need for a focused approach to address regional challenges. The Asia-Pacific region occupies a moderate position with an average of 0.5399, demanding tailored strategies to fortify resilience across its diverse landscape. Notably, North America emerges as the second-least vulnerable region, averaging 0.4621 per country, underscoring its proactive stance and investment in robust cybersecurity measures. These disparities underscore the urgency for international collaboration, knowledge transfer, and strategic resource allocation to cultivate a resilient global digital ecosystem, addressing the unique cybersecurity needs of nations and regions.

```
cei_bins = [0, 0.2, 0.4, 0.6, 0.8, 1]
cei_labels = ["5 - Very low", "4 - Low", "3 - Moderate", "2 - High", "1 - Very high"]
cei_df['cybercrime_exposure'] = pd.cut(cei_df['CEI'], bins=cei_bins, labels=cei_labels)
dfg = cei_df.groupby(['Region', 'cybercrime_exposure']).size().reset_index(name='Country Count')
cei_labels.reverse()
fig = px.bar(dfg, x='Region', y='Country Count', color='cybercrime_exposure',
    color_discrete_sequence=px.colors.sequential.Reds, title="Cybercrime Exposure by Regions")
fig.update_layout(legend=dict(traceorder='reversed'))
fig.show()
```

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

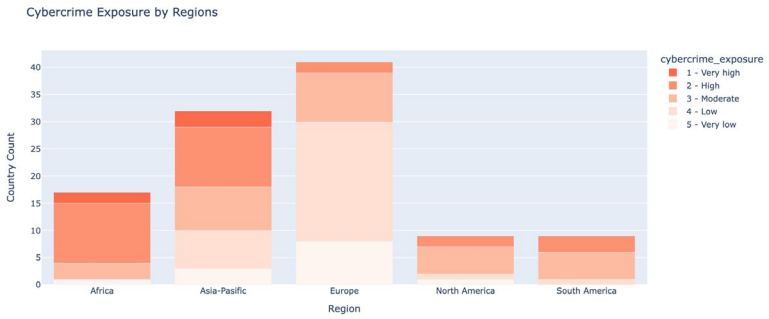

Figure 8: Cybercrime exposure by regions.

The regional analysis of the Cybersecurity Exposure Index (CEI) unveils stark disparities (Figure 8 shows cybercrime exposure by regions), with Europe emerging as a bastion of resilience, boasting 71% of its nations in the low and very low exposure categories, while only 4.88% fall into the high exposure group. In contrast, the Asia-Pacific region accounts for a concerning 60% of countries with very high exposure and 36.67% with high exposure levels globally. South America mirrors these vulnerabilities, with 40% of its nations facing high or very high exposure. Alarmingly, Africa grapples with the direst situation, as 75% of its countries exhibit high or very high exposure to cyber threats, jointly accounting with the Asia-Pacific for the largest proportion (36.67%) of highly exposed nations worldwide. These findings underscore the pressing need for targeted interventions, strategic resource allocation, knowledge-sharing, and robust international collaboration to address the unique cybersecurity challenges faced by vulnerable regions, fostering a more equitable and resilient global cybersecurity landscape.

```
fig = px.scatter_geo(cei_df, locations='Country', locationmode='country names', color='CEI',
    size='CEI', range_color=[0, 1], title='Cybersecurity Exposure Index (CEI) Across the Globe',
    color_continuous_scale=px.colors.sequential.Reds)
fig.update_layout(margin=dict(t=40, b=0, l=5, r=5))
fig.show()
```

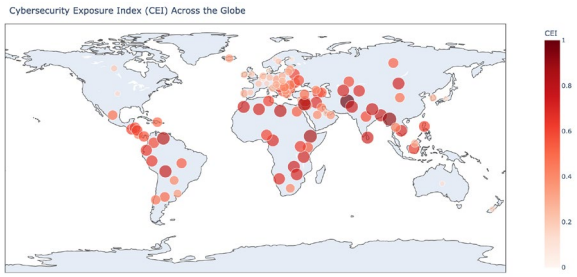

Figure 9: Cybercrime exposure by countries across the globe.

```
cei_df_asc = cei_df.sort_values(by='CEI')
cei_df_asc.reset_index(drop=True, inplace=True)
cei_df_asc.index += 1
cei_df_asc[cei_df_asc['CEI'] < 0.2]]
```

	Country	Region	CEI	cybercrime_exposure
1	Finland	Europe	0.110	5 - Very low
2	Denmark	Europe	0.117	5 - Very low
3	Luxembourg	Europe	0.124	5 - Very low
4	Australia	Asia-Pasific	0.131	5 - Very low
5	Estonia	Europe	0.134	5 - Very low
6	Norway	Europe	0.134	5 - Very low
7	Japan	Asia-Pasific	0.138	5 - Very low
8	United States	North America	0.145	5 - Very low
9	Austria	Europe	0.162	5 - Very low
10	Switzerland	Europe	0.172	5 - Very low
11	New Zealand	Asia-Pasific	0.179	5 - Very low
12	Belgium	Europe	0.190	5 - Very low

Figure 10: Very low cybercrime exposure countries.

The granular examination of the Cybersecurity Exposure Index (CEI) unveils nuanced insights, highlighting specific areas of concern demanding targeted interventions (Figure 9 shows cybercrime exposure by countries across the globe). While Europe boasts commendable performance overall, with Belarus and Armenia as outliers in the high exposure group, Ukraine has made strides in improving its situation. North America lacks extreme outliers, presenting opportunities for collaborative efforts.

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

Alarmingly, the Asia-Pacific harbors Afghanistan and Myanmar as the world's most vulnerable, necessitating comprehensive strategies and international support. In South America, Venezuela stands out with high exposure, while Africa grapples with Ethiopia as the most sensitive nation to cyber threats, underscoring the need for capacity-building initiatives. Notably, Europe dominates the top 10 least exposed countries, with North America and the Asia-Pacific contributing a few nations, highlighting pockets of excellence (Figure 10 shows the very low cybercrime exposure countries). These findings underscore the importance of tailored approaches, regional partnerships, knowledge-sharing, and resource mobilization to cultivate a resilient and equitable global cybersecurity landscape.

4.2.2. Global Cyber Security Index (GCI)

The Global Cybersecurity Index (GCI), an authoritative reference developed by the International Telecommunication Union (ITU), evaluates the commitment of 193 ITU Member States and the State of Palestine to cybersecurity on a global scale. Launched in 2015 and periodically updated, the GCI assesses national cybersecurity initiatives and preparedness levels across five pillars: legal, technical, organizational, capacity development, and cooperation measures, through a comprehensive set of 82 questions. Serving as a benchmarking tool, the GCI enables countries to identify areas for improvement, incorporate good practices, facilitate self-assessments and coordination efforts, and foster awareness among stakeholders. By promoting regional comparisons and encouraging the adoption of robust cybersecurity strategies aligned with global standards, the GCI remains a trusted and relevant reference, offering valuable insights to policymakers, security professionals, and stakeholders in their pursuit of fortifying national and international cyber defenses.

```
gci_df = df[['Country', 'Region', 'GCI']].dropna(subset=['GCI'])
plt.figure(figsize=(10, 6))
sns.violinplot(data=gci_df, x='Region', y='GCI')
plt.title("GCI by Regions")
plt.xlabel('Region')
plt.ylabel('GCI')
plt.show()
```

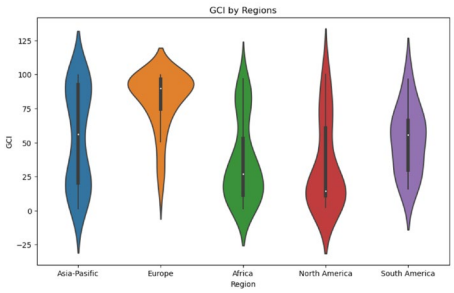

Figure 11: Global Cyber Security Index (GCI) violin plots by regions.

```
gci_bins = [0, 20, 40, 60, 80, 100]
gci_labels = ["5 - Very low", "4 - Low", "3 - Moderate", "2 - High", "1 - Very high"]
gci_df['cybersecurity_level'] = pd.cut(gci_df['GCI'], bins=gci_bins, labels=gci_labels)
dfg = gci_df.groupby(['Region', 'cybersecurity_level']).size().reset_index(name='Country Count')
gci_labels.reverse()
fig = px.bar(dfg, x='Region', y='Country Count', color='cybersecurity_level',
      color_discrete_sequence=px.colors.sequential.Greens, title="Cybersecurity Level by Regions")
fig.update_layout(legend=dict(traceorder='reversed'))
fig.show()
```

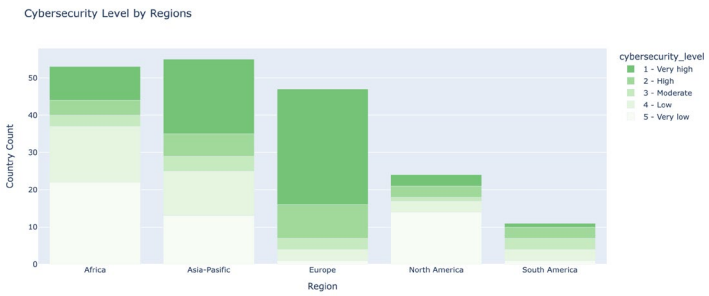

Figure 12: Cybersecurity level by regions.

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

The regional analysis (Figure 11 shows Global Cyber Security Index (GCI) violin plots by regions) of the Global Cybersecurity Index (GCI) unveils Europe leading with the highest average score, reflecting its position at the forefront of cybersecurity readiness, with most nations ranking in the 'Very High' and 'High' categories, showcasing concerted efforts and robust cyber defense strategies. The Asia-Pacific region trails closely, demonstrating notable preparedness and growing recognition of cybersecurity as a strategic priority. South America occupies a moderate stance, reflecting room for further enhancement and regional collaboration to align with global best practices. Notably, Africa and North America exhibit the lowest average GCI rankings, highlighting vulnerability areas necessitating targeted interventions, capacity-building initiatives, knowledge-sharing, and leveraging international partnerships to cultivate robust cybersecurity postures. These disparities underscore the urgency of fostering international cooperation, mobilizing resources, and tailoring strategies to address regional cybersecurity needs, leveraging the strengths of leading nations to build a more resilient and equitable global cybersecurity landscape fortified against evolving cyber threats. (Figure 12 shows cybersecurity level by regions)

```
fig = px.scatter_geo(gci_df, locations='Country', locationmode='country names', color='GCI', size=
'GCI', range_color=[0, 100], title= 'Global Cyber Security Index (GCI) Across the Globe',
color_continuous_scale=px.colors.sequential.Greens)
fig.update_layout(margin=dict(t=40, b=0, l=5, r=5))
fig.show()
```

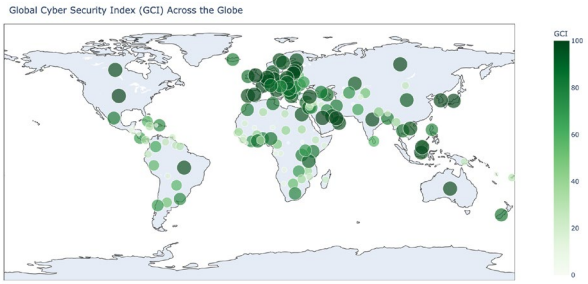

Figure 13: Cybersecurity level by countries across the globe.

```
gci_df_desc = gci_df.sort_values(by='GCI', ascending=False)
gci_df_desc.reset_index(drop=True, inplace=True)
gci_df_desc.index += 1
gci_df_desc[:10]
```

	Country	Region	GCI	cybersecurity_level
1	United States	North America	100.00	1 - Very high
2	United Kingdom	Europe	99.54	1 - Very high
3	Saudi Arabia	Asia-Pasific	99.54	1 - Very high
4	Estonia	Europe	99.48	1 - Very high
5	South Korea	Asia-Pasific	98.52	1 - Very high
6	Spain	Europe	98.52	1 - Very high
7	Singapore	Asia-Pasific	98.52	1 - Very high
8	Russia	Europe	98.06	1 - Very high
9	United Arab Emirates	Asia-Pasific	98.06	1 - Very high
10	Malaysia	Asia-Pasific	98.06	1 - Very high

Figure 14: Top 10 high cybersecurity level countries.

A granular examination of the top performers in the Global Cybersecurity Index (GCI) unveils valuable insights (Figure 13 shows the cybersecurity level by countries across the globe), with the United States leading the rankings, exemplifying its unwavering commitment to fortifying cyber defenses and fostering a robust cybersecurity ecosystem. Europe reinforces its exceptional performance with several nations, including the United Kingdom, Estonia, Spain, and Russia, securing top positions through comprehensive legal frameworks, robust measures, capacity development, and international cooperation. Notably, the Asia-Pacific region contributes top performers like Saudi Arabia, Singapore, South Korea, and the United Arab Emirates, reflecting growing cybersecurity prioritization and alignment with global best practices. This diverse representation highlights the multifaceted nature of cybersecurity challenges and the tailored approaches adopted, underscoring the importance of international collaboration, knowledge-sharing, and leveraging the policies, practices, and initiatives of leading nations to enhance global cyber resilience and address evolving threats (Figure 14 shows the top 10 high cybersecurity level countries).

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

4.2.3. National Cyber Security Index (NCSI)

The National Cyber Security Index (NCSI) is a comprehensive multidimensional metric that evaluates a country's preparedness to address cyber threats and manage cyber incidents effectively. Comprising distinct categories, capacities, and individual indicators with assigned relative weights, the NCSI score represents the percentage a country has achieved relative to the maximum attainable value across all indicators, providing a standardized and comparable measure of cyber readiness on a scale of 0 to 100%. This index serves as a valuable tool for nations to gauge their cyber resilience, identify areas for improvement, prioritize strategic investments in cyber defenses, facilitate cross-country comparisons, and promote knowledge-sharing and collaboration within the global cybersecurity community by enabling the identification of best practices.

```
ncsi_df = df[['Country', 'Region', 'NCSI']].dropna(subset=['NCSI'])
plt.figure(figsize=(10, 6))
sns.violinplot(data=ncsi_df, x='Region', y='NCSI')
plt.title("NCSI by Regions")
plt.xlabel('Region')
plt.ylabel('NCSI')
plt.show()
```

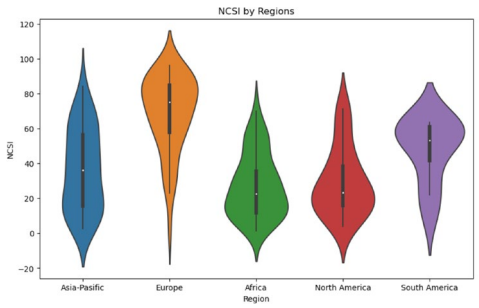

Figure 15: National Cyber Security Index (NCSI) violin plots by regions.

```
ncsi_bins = [0, 20, 40, 60, 80, 100]
ncsi_labels = ["5 - Very low", "4 - Low", "3 - Moderate", "2 - High", "1 - Very high"]
ncsi_df['national_cybersecurity_level'] = pd.cut(ncsi_df['NCSI'], bins=ncsi_bins, labels=ncsi_labels)
dfg = ncsi_df.groupby(['Region', 'national_cybersecurity_level']).size().reset_index(name=Country
Count')
ncsi_labels.reverse()
fig = px.bar(dfg, x='Region', y='Country Count', color='national_cybersecurity_level',
color_discrete_sequence=px.colors.sequential.Greens, title="National Cybersecurity Level by
Regions")
fig.update_layout(legend=dict(traceorder='reversed'))
fig.show()
```

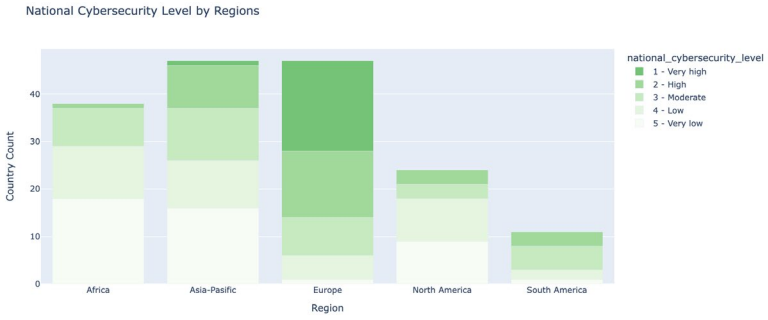

Figure 16: National cybersecurity level by regions.

The regional analysis (Figure 15 shows National Cyber Security Index (NCSI) violin plots by regions) of the National Cyber Security Index (NCSI) unveils Europe leading with the highest average score of 71.88%, showcasing commendable preparedness in managing cyber incidents through concerted efforts and strategic investments in cyber resilience and incident response alignment. South America secures the second position with an average of 47.23%, surpassing the global average and highlighting strides in enhancing cyber defense capabilities. The Asia-Pacific region follows with an average of 36.50%, indicating progress yet substantial room for improvement and capacity-building initiatives. Notably,

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

North America and Africa exhibit nearly parallel average scores of 27.49% and 29.01% respectively, falling below the global average and underscoring the urgent need for targeted interventions, resource allocation, and knowledge sharing to elevate cyber resilience in these regions. These disparities underscore the importance of fostering international cooperation, mobilizing resources, tailoring strategies to address regional cyber preparedness needs, leveraging strengths of leading nations, and promoting knowledge transfer to build a more resilient and equitable global cybersecurity landscape (Figure 16 shows national cybersecurity level by regions).

```
fig = px.scatter_geo(ncsi_df, locations='Country', locationmode='country names', color='NCSI',
size='NCSI', range_color=[0, 100], title= 'National Cyber Security Index (NCSI) Across the Globe',
color_continuous_scale=px.colors.sequential.Greens)
fig.update_layout(margin=dict(t=40, b=0, l=5, r=5))
fig.show()
```

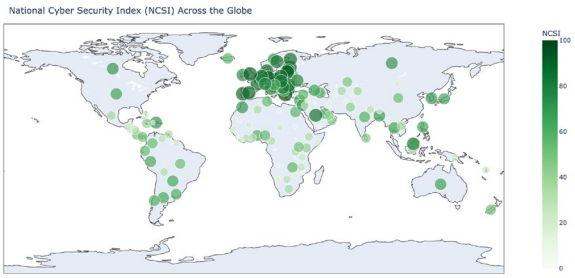

Figure 17: National cybersecurity level by countries across the globe.

```
ncsi_df_desc = ncsi_df.sort_values(by='NCSI', ascending=False)
ncsi_df_desc.reset_index(drop=True, inplace=True)
ncsi_df_desc.index += 1
ncsi_df_desc[ncsi_df_desc[:10]
```

	Country	Region	NCSI	national_cybersecurity_level
1	Greece	Europe	96.10	1 - Very high
2	Belgium	Europe	94.81	1 - Very high
3	Estonia	Europe	93.51	1 - Very high
4	Lithuania	Europe	93.51	1 - Very high
5	Czech Republic	Europe	92.21	1 - Very high
6	Germany	Europe	90.91	1 - Very high
7	Romania	Europe	89.61	1 - Very high
8	Portugal	Europe	89.61	1 - Very high
9	United Kingdom	Europe	89.61	1 - Very high
10	Spain	Europe	88.31	1 - Very high

Figure 18: Very high national cybersecurity level countries.

The granular analysis (*Figure 17 shows national cybersecurity level by countries across the globe*) of the National Cyber Security Index (NCSI) unveils Europe's dominance, with Greece leading globally at 96.10%, exemplifying unparalleled commitment to cybercrime prevention and cyber incident management. In South America, Argentina and Paraguay emerge as top performers with a shared 63.64% score, highlighting regional strides in enhancing cyber resilience. Saudi Arabia stands out in the Asia-Pacific region with 84.42%, while concerningly over 50% of nations fall below the average, necessitating concerted efforts to bridge gaps. Notably, Canada and Morocco share the highest NCSI of 70.13% in North America and Africa respectively, underscoring commendable efforts and potential for cross-regional collaboration. The presence of these top performers (*Figure 18 shows the very high national cybersecurity level countries*) offers insights into diverse strategies and best practices, enabling knowledge-sharing and adaptation to unique contexts. Simultaneously, the identification of regions with significant proportions below the average NCSI score accentuates the urgent need for targeted capacity-building, resource allocation, and international cooperation to cultivate a more resilient and equitable global cybersecurity landscape.

4.2.4. Digital Development Level (DDL)

The Digital Development Level (DDL) is a comprehensive metric that evaluates a country's overall digital landscape and readiness to leverage information and communication technologies (ICTs). Derived by averaging a nation's performance across the ICT Development Index (IDI) and the Networked Readiness Index (NRI), the DDL offers a holistic perspective on digital development. The IDI measures a country's ICT resources by combining indicators of access, use, and skills, providing insights into the availability, adoption, and proficiency of ICT infrastructure and services. Complementarily, the NRI assesses the degree to which a country is poised to capitalize on ICT opportunities, evaluating factors

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

such as regulatory environments, business and innovation landscapes, and overall economic readiness to leverage digital technologies effectively. By integrating these indices, the DDL serves as a valuable tool for policymakers, researchers, and stakeholders to benchmark national digital readiness, identify areas for improvement, and formulate strategies to foster inclusive and sustainable digital transformation.

```
ddl_df = df[['Country', 'Region', 'DDL']].dropna(subset=['DDL'])
plt.figure(figsize=(10, 6))
sns.violinplot(data=ddl_df, x='Region', y='DDL')
plt.title("DDL by Regions")
plt.xlabel('Region')
plt.ylabel('DDL')
plt.show()
```

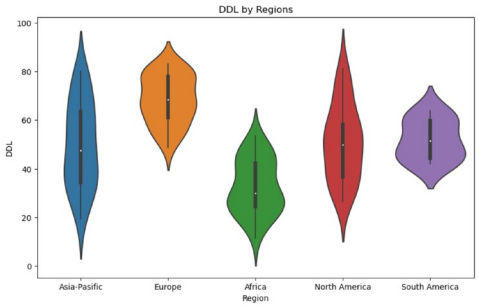

Figure 19: Digital Development Level (DDL) violin plots by regions.

```
ddl_bins = [0, 20, 40, 60, 80, 100]
ddl_labels = ["5 - Very low", "4 - Low", "3 - Moderate", "2 - High", "1 - Very high"]
ddl_df['digital_development_level'] = pd.cut(ddl_df['DDL'], bins=ddl_bins, labels=ddl_labels)
dfg = ddl_df.groupby(['Region', 'digital_development_level']).size().reset_index(name='Country Count')
ddl_labels.reverse()
fig = px.bar(dfg, x='Region', y='Country Count', color='digital_development_level',
color_discrete_sequence=px.colors.sequential.Greens, title="Digital Development Level by Regions")
fig.update_layout(legend=dict(traceorder='reversed'))
fig.show()
```

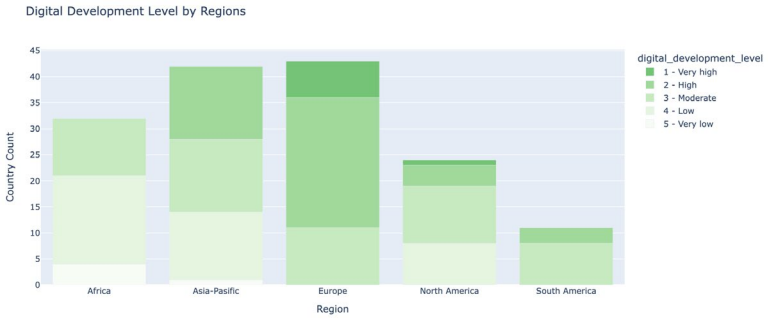

Figure 20: Digital Development level by regions.

The regional analysis (*Figure 19 shows Digital Development Level (DDL) violin plots by regions*) unveils Europe leading in digital development, exemplified by its exceptional Digital Development Level (DDL) performance and the alignment, or surpassing, of cyber security development with its digital trajectory, positioning it as a role model for integrating cyber strategies into digital transformation initiatives. North America, South America, and the Asia-Pacific occupy a middle ground in DDL scores yet exhibit a notable gap between digital advancement and effective cyber preparedness, necessitating targeted investments in cyber resilience and robust cybersecurity integration. Alarmingly, Africa trails behind in DDL, highlighting the pressing need for concerted efforts to bridge the digital divide, promote inclusive ICT access, and cultivate an enabling environment for sustainable digital transformation. These disparities underscore the importance of tailored regional strategies, international cooperation, knowledge-sharing, and resource mobilization to address unique challenges, bridge digital and cybersecurity gaps, and cultivate a more resilient and equitable global digital ecosystem fortified against emerging cyber threats (*Figure 20 shows Digital Development level by regions*).

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

```
fig = px.scatter_geo(ddl_df, locations='Country', locationmode='country names', color='DDL',
size='DDL', range_color=[0, 100], title= 'Digital Development Level (DDL) Across the Globe',
color_continuous_scale=px.colors.sequential.Greens)
fig.update_layout(margin=dict(t=40, b=0, l=5, r=5))
fig.show()
```

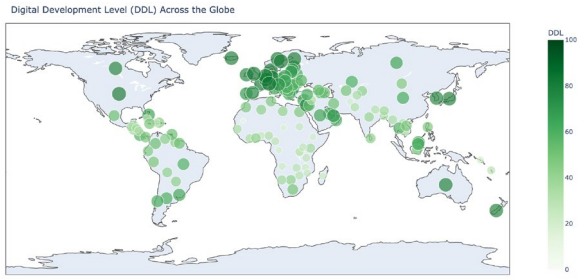

Figure 21: Digital development level by countries across the globe.

```
ddl_df_desc = ddl_df.sort_values(by='DDL', ascending=False)
ddl_df.reset_index(drop=True, inplace=True)
ddl_df.index += 1
ddl_df[:10]
```

	Country	Region	DDL	digital_development_level
1	Switzerland	Europe	82.93	1 - Very high
2	Denmark	Europe	82.68	1 - Very high
3	Netherlands	Europe	81.86	1 - Very high
4	Croatia	Europe	81.51	1 - Very high
5	Sweden	Europe	81.51	1 - Very high
6	United States	North America	81.05	1 - Very high
7	Norway	Europe	80.19	1 - Very high
8	Germany	Europe	80.01	1 - Very high
9	United Kingdom	Europe	79.96	2 - High
10	Singapore	Asia-Pasific	79.93	2 - High

Figure 22: Top 10 high digital development level countries.

The analysis (*Figure 21 shows digital development level by countries across the globe*) of the Digital Development Level (DDL) unveils a distinct concentration of top-performing nations within Europe, underscoring the continent's leadership in fostering robust digital landscapes and effective ICT leverage. An overwhelming European majority dominates the top 10 rankings (*Figure 22 shows the top 10 high digital development level countries*), highlighting concerted efforts in cultivating enabling environments, nurturing digital skills, and promoting widespread ICT adoption across sectors. Notably, the United States and Singapore stand out as the sole non-European representatives, exemplifying their unwavering commitment to technological innovation, digital infrastructure development, and conducive ecosystems for digital entrepreneurship. Remarkably, the United States surpasses the 80% threshold, indicating a very high digital development level and ability to harness ICTs' transformative power across domains. This concentration of top performers underscores the multifaceted nature of digital development, emphasizing enabling regulatory environments, digital infrastructure investments, skilled workforce development, and innovation embracement as catalysts for sustainable transformation. As the global digital landscape evolves, these nations' experiences and best practices serve as guideposts for accelerating digital trajectories through international collaboration, knowledge-sharing, and proven strategy adoption.

4.2.5. Cross Indexes Relationship

```
fig = px.scatter_3d(df, x='Region', y='CEI', z='GCI', color='DDL', hover_name='Country', title='CEI-
GCI-DDL Cross Relationship')
fig.show()
```

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

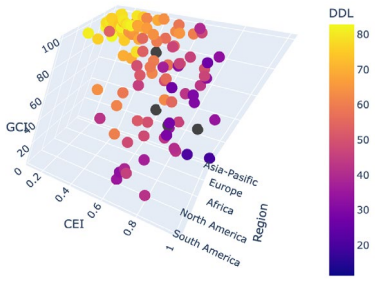

Figure 23: CEI-GCI-DDL cross relationship.

```
fig = px.scatter_3d(df, x='Region', y='CEI', z='NCSI', color='DDL', hover_name='Country', title='CEI-NCSI-DDL Cross Relationship')
fig.show()
```

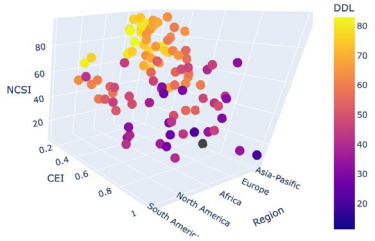

Figure 24: CEI-NCSI-DDL cross relationship.

The analysis (*Figure 23 shows CEI-GCI-DDL cross relationship*) unveils an intriguing group of nations concentrated in the Asia-Pacific region and parts of Europe that are on an accelerated digital development trajectory, yet their cybersecurity readiness lags. Nations like Malaysia, Saudi Arabia, the United Arab Emirates, Qatar, Kazakhstan, Belarus, and Armenia exemplify this phenomenon. While fostering robust digital landscapes, nurturing innovation, and promoting widespread ICT adoption, their cybersecurity posture remains relatively vulnerable, as evidenced by medium-to-high Cybersecurity Exposure Index (CEI) scores and medium National Cyber Security Index (NCSI) levels (*Figure 24 shows CEI-NCSI-DDL cross relationship*). This suggests that while embracing digitalization, their cybersecurity infrastructure, preparedness, and capacity to effectively respond to cyber threats may not have kept pace with digital development.

This disparity poses significant risks, as these nations' integration of digital technologies makes them attractive targets for malicious cyber actors. The consequences of successful cyber-attacks could be severe, compromising national security, economic stability, and trust in digital ecosystems. It is imperative for these countries to prioritize cybersecurity as a strategic imperative, allocating resources to fortify cyber defenses. This includes strengthening legal and regulatory frameworks, investing in cybersecurity talent and capacity-building, fostering public-private partnerships, and actively participating in international cooperation efforts to share best practices and stay ahead of evolving threats. Proactively addressing this cybersecurity gap and aligning strategies with digital development goals can mitigate risks, safeguard digital assets, and realize the full potential of digital transformation initiatives, averting potential undermining of economic aspirations and jeopardizing of national security in an increasingly interconnected world.

5. Discussion

5.1 Interpretation of Key Findings

The comprehensive analysis of the "Cyber Security Indexes" dataset reveals crucial insights that underscore the complexities inherent in the cybersecurity landscape. Notably, better readiness to prevent cybercrimes does not necessarily translate into the lowest exposure to cyber threats, necessitating a multidimensional approach to fortifying digital defenses. Additionally, stark regional disparities are unveiled, with Europe emerging as the least exposed and most prepared region, while Africa grapples with significant vulnerabilities and limited preparedness. North America exhibits a lower exposure level than South America, yet its National Cyber Security Index (NCSI) score is lower, indicating diminished

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

preparedness to manage cyber incidents effectively.

Furthermore, the analysis of the Digital Development Level (DDL) unveils a concerning trend. While the North American, South American, and Asia-Pacific regions occupy a middle ground in digital development, the digital advancement in North America and the Asia-Pacific appears to outpace their readiness to address cybersecurity threats. This discrepancy potentially exacerbates the risks of cybercrime and cyber-attacks in these regions, necessitating proactive measures to align cybersecurity strategies with digital transformation initiatives and mitigate potential vulnerabilities arising from the accelerated integration of digital technologies.

5.2 Implications for Policymakers and Stakeholders

The findings of this study carry profound implications, underscoring the urgent need for concerted efforts and tailored strategies to address the disproportions in cybersecurity exposure, threat response, and digital development levels. Policymakers must prioritize the development and implementation of robust cybersecurity frameworks, foster international cooperation, and allocate resources to bolster cyber resilience, particularly in lagging regions. Stakeholders, including businesses, civil society organizations, and citizens, must recognize their shared responsibility in maintaining a secure digital ecosystem and actively participate in capacity-building initiatives.

Moreover, the identification of countries on a soaring track of digital development yet exhibiting medium-to-high levels of cybersecurity exposure and preparedness demands immediate attention. Policymakers in these nations must proactively align their cybersecurity strategies with digital transformation goals, fortifying cyber defenses to mitigate escalating threat risks. This proactive approach is crucial to safeguard the potential benefits of digital transformation while mitigating associated vulnerabilities arising from the accelerated integration of digital technologies.

5.3 Strategies for Enhancing Data Protection Measures

To enhance data protection measures and cultivate a resilient global data fortress, a multifaceted approach encompassing legal and regulatory frameworks, capacity-building initiatives, technological advancements, and international cooperation is imperative. Nations must prioritize the development and enforcement of comprehensive cybersecurity laws and regulations that address emerging threats and promote data privacy and security. Simultaneously, investing in cybersecurity education, training, and public-private partnerships is crucial to nurturing a skilled workforce capable of defending against sophisticated cyber-attacks and leveraging industry expertise.

Embracing cutting-edge technologies, such as artificial intelligence, machine learning, and advanced encryption techniques, can bolster cyber defenses, facilitate proactive threat detection and response mechanisms. Furthermore, promoting international cooperation, knowledge-sharing, and the adoption of best practices from leading nations can accelerate the development of robust cyber resilience strategies across regions. This collaborative approach, integrating legal frameworks, capacity-building, technological innovations, and global partnerships, is essential to safeguarding the invaluable asset of data and fostering a resilient global digital ecosystem.

5.4 Fostering International Cooperation and Knowledge Sharing

The transnational nature of cyber threats necessitates a concerted global effort to fortify the digital fortress. International cooperation and knowledge-sharing initiatives are pivotal in addressing the disparities in cybersecurity preparedness revealed by this study. Platforms for dialogue, such as regional and global forums, can facilitate the exchange of best practices, lessons learned, and collaborative strategies, while capacity-building programs, facilitated by leading nations and international organizations, can empower regions lagging in cybersecurity by transferring expertise and providing technical assistance. The establishment of robust information-sharing mechanisms can enable real-time threat intelligence sharing, facilitating swift responses to emerging cyber threats and mitigating their potential impact. Ultimately, fostering a culture of trust, transparency, and mutual understanding among nations is paramount in cultivating a resilient global cybersecurity ecosystem.

5.5 Limitations of the Study and Future Research Directions

While this study provides a comprehensive analysis of the global cybersecurity landscape, it is

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

essential to acknowledge its limitations and outline potential avenues for future research. The dataset's reliance on web-scraping techniques may introduce inconsistencies or data gaps, necessitating the development of robust data collection and validation methodologies, while the dynamic nature of cyber threats and the rapid evolution of digital technologies demand continuous monitoring and updating of the cybersecurity indices to ensure their relevance and accuracy. Future research endeavors could explore the integration of additional indicators or indices to capture emerging dimensions of cybersecurity, such as the impact of artificial intelligence, the Internet of Things, and quantum computing on cyber resilience, as well as longitudinal studies tracking the progress of nations over time to provide valuable insights into the effectiveness of implemented strategies and policies, enabling data-driven adjustments and course corrections. Additionally, interdisciplinary collaborations between cybersecurity experts, policymakers, economists, and social scientists could yield a holistic understanding of the socioeconomic implications of cyber threats and the cost-benefit analysis of cybersecurity investments.

6. Conclusion

6.1 Summary of Research Objectives and Findings

This study set out to conduct a comprehensive examination of the global cybersecurity landscape by analyzing four prominent indices: the Cybersecurity Exposure Index (CEI), Global Cyber Security Index (GCI), National Cyber Security Index (NCSI), and Digital Development Level (DDL). By leveraging an extensive dataset spanning 193 countries and territories across five geographic regions, the research employed advanced statistical techniques and data visualization methodologies to unravel the multidimensional challenges and opportunities in fortifying international data protection.

The findings unveiled stark regional disparities, with Europe emerging as the least exposed and most prepared region to combat cybercrime, while Africa grappled with significant vulnerabilities and limited preparedness. Notably, the digital advancement in the North American and Asia-Pacific regions appeared to outpace their readiness to address cybersecurity threats, potentially exacerbating the risks of cybercrime and cyber-attacks. Additionally, the study identified a group of nations on a soaring track of digital development yet exhibiting medium-to-high levels of cybersecurity exposure and preparedness, highlighting the urgent need to align their cybersecurity strategies with their digital transformation goals.

6.2 Recommendations for Fortifying the Global Data Fortress

To fortify the global data fortress and cultivate a resilient digital ecosystem, this study recommends a multifaceted approach encompassing robust legal and regulatory frameworks, investments in cybersecurity education and capacity-building initiatives, the adoption of cutting-edge technologies such as artificial intelligence and advanced encryption techniques, as well as fostering international cooperation, knowledge-sharing, and the implementation of best practices from leading nations, which are crucial in bridging the gaps in cybersecurity preparedness and addressing the disparities unveiled by this research.

6.3 Call to Action for a Concerted Effort towards Cyber Resilience

The transnational nature of cyber threats demands a concerted global effort to safeguard the digital fortress, with this study serving as a clarion call for policymakers, security professionals, and stakeholders across the globe to prioritize cybersecurity as a strategic imperative and recognize the shared responsibility in maintaining a secure digital ecosystem. By embracing a collaborative approach, nurturing a culture of trust and transparency, and leveraging the expertise and best practices from leading nations, the global community can work towards cultivating a resilient cybersecurity landscape, fortified against evolving threats, and unlocking the vast potential of digital technologies for economic growth and societal progress. The path towards cyber resilience is arduous, but the collective commitment and unwavering determination of nations, organizations, and individuals will pave the way for a secure and prosperous digital future, where the global data fortress stands as an impregnable bastion, safeguarding the invaluable assets of our interconnected world.

References

[1] Center for Strategic and International Studies. (2024). Significant cyber incidents. https://www.csis.

ISSN 2706-655X Vol.6, Issue 2: 13-28, DOI: 10.25236/IJFET.2024.060203

org/programs/strategic-technologies-program/significant-cyber-incidents
[2] PasswordManagers.co (2020). Cybersecurity Exposure Index. https://passwordmanagers. co/cybersecurity-exposure-index/
[3] International Telecommunication Union. (2021). Global Cybersecurity Index 2020. https://www. itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[4] e-Governance Academy Foundation. (2023). National Cyber Security Index 2023. https://ncsi.ega. ee/ncsi-index/
[5] e-Governance Academy Foundation. (2023). Digital Development Level 2023. https://ncsi.ega.ee/ ncsi-index/
[6] IBM. (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/security/data-breach
[7] Verizon. (2023). 2023 Data Breach Investigations Report. https://www.verizon.com/business/ resources/ reports/dbir/
[8] Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
[9] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2).
[10] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.
[11] National Institute of Standards and Technology. (2011). National Strategy for Trusted Identities in Cyberspace (NSTIC). https://obamawhitehouse.archives. gov/sites/default/files/rss_viewer/ NSTICstrategy _ 041511 .pdf
[12] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
[13] Shey, H., Valente, A., & Carney, E. (2021). The Cyber Insurance Roller Coaster: As Demand Speeds Up, Some Insurers Disembark Effects Across Providers And Their Customers. https://www.forrester. com/blogs/the-cyber-insurance-roller-coaster-as-demand-speeds-up-some-insurers-disembark/
[14] Kateryna Meleshenko. (2023). Cyber Security Indexes [Data set]. Kaggle. https://doi.org/ 10.34740/KAGGLE/DS/3135173
[15] Vyshnia, Georgii (2024, March 1st). Global Cybersecurity: Geospacial EDA and Insights [Notebook]. Kaggle. https://www.kaggle.com/code/gvyshnya/global-cybersecurity-geospacial-eda-and-insights