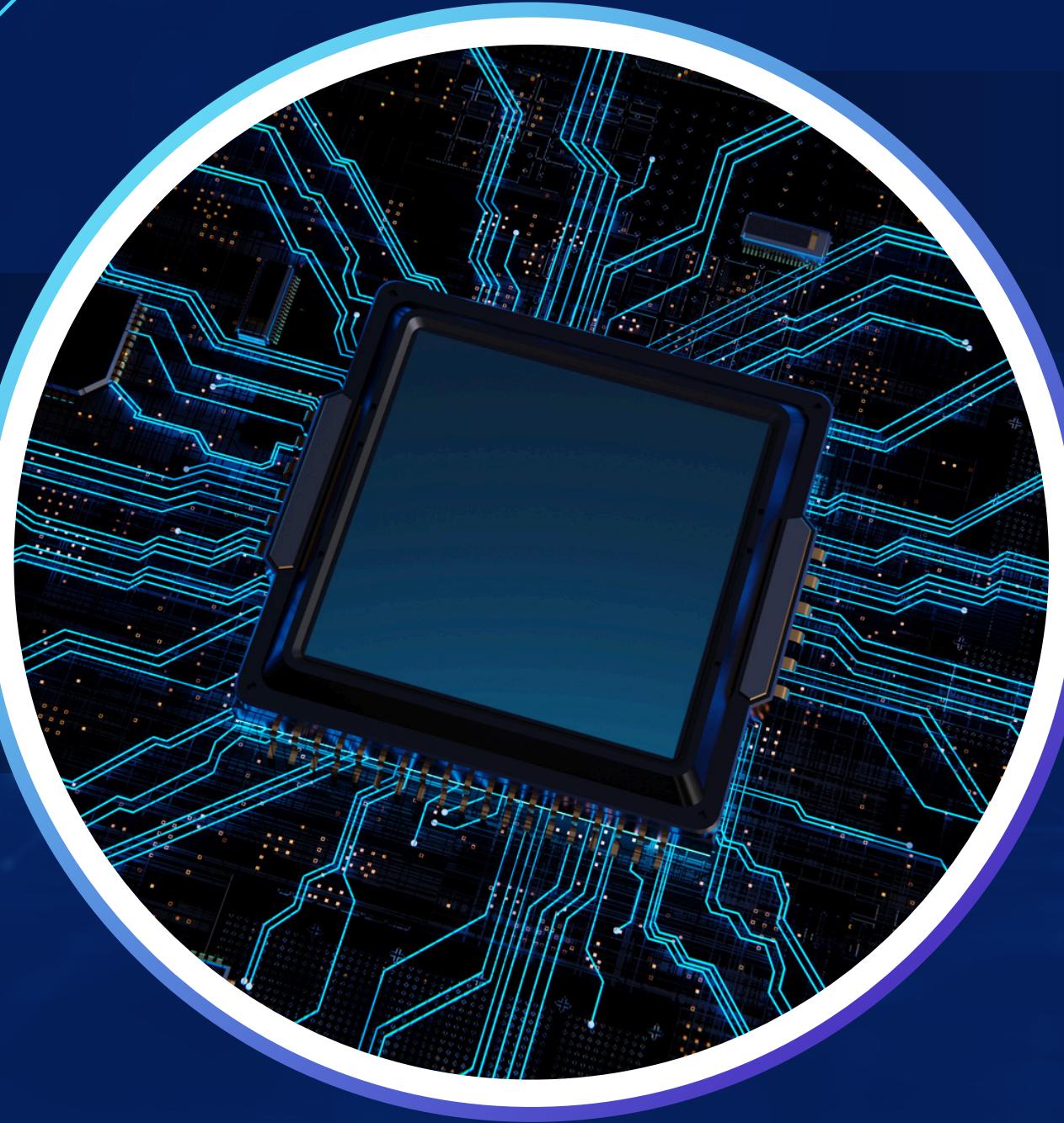




-By Bhavya Balyan



GLOBAL CYBER SECURITY



INTRODUCTION

Global Cybersecurity: A Worldwide Priority Cybersecurity has become a pressing issue in today's interconnected digital world. From data breaches to ransomware attacks, malicious actors increasingly target individuals, organizations, and governments, causing significant financial losses and disruptions.

This project delves into global cyber threats, analyzing attack patterns, affected industries, and defensive strategies. By exploring key trends and solutions, it aims to contribute to a safer, more secure digital environment for all.



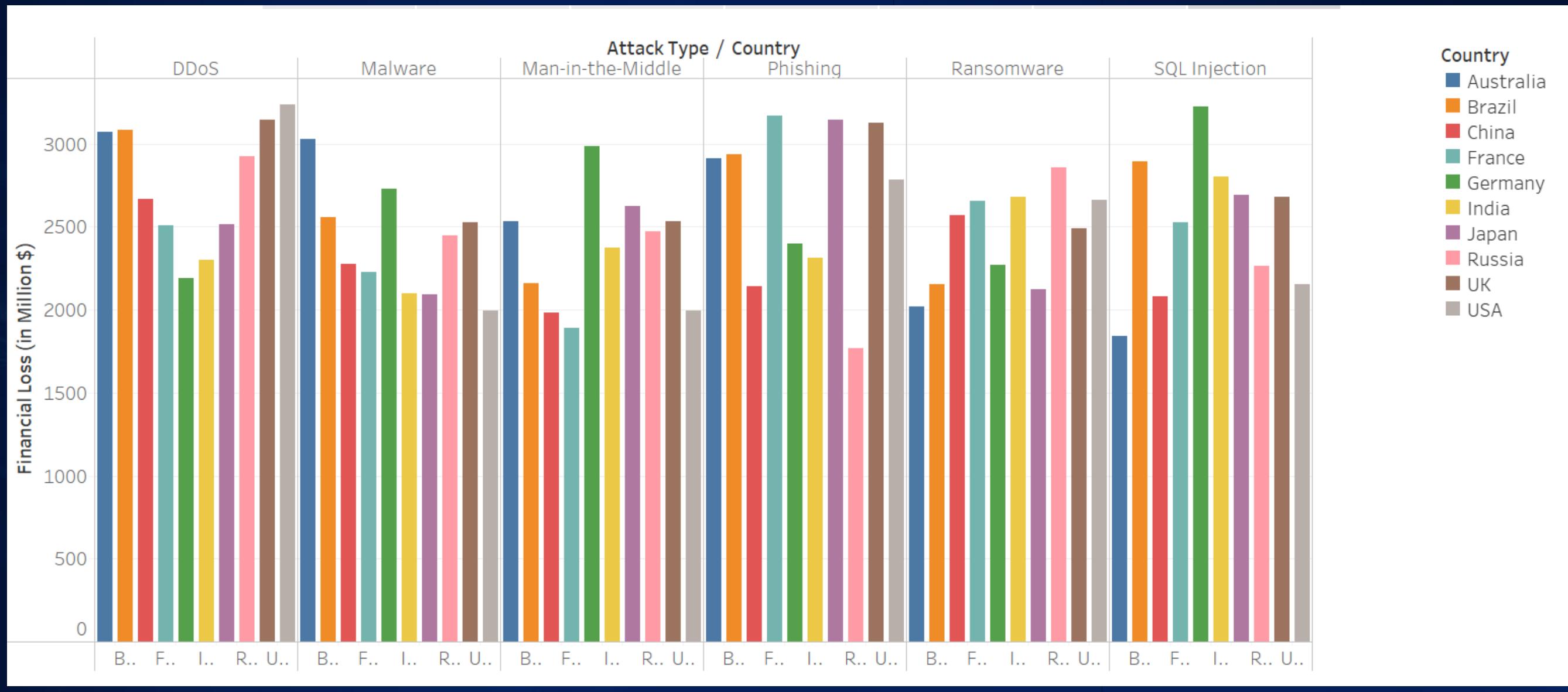
PROBLEM STATEMENT

In today's rapidly evolving digital landscape, cybersecurity threats have become a critical global issue. Industries like healthcare, banking, education, and retail are increasingly targeted, leading to significant financial losses, disrupted operations, and compromised user data. Attackers exploit vulnerabilities such as weak passwords, unpatched software, and social engineering tactics to infiltrate systems. This project aims to analyze cybersecurity patterns, industry-specific vulnerabilities, and effective defense mechanisms, providing actionable insights to mitigate risks and ensure a resilient digital future.

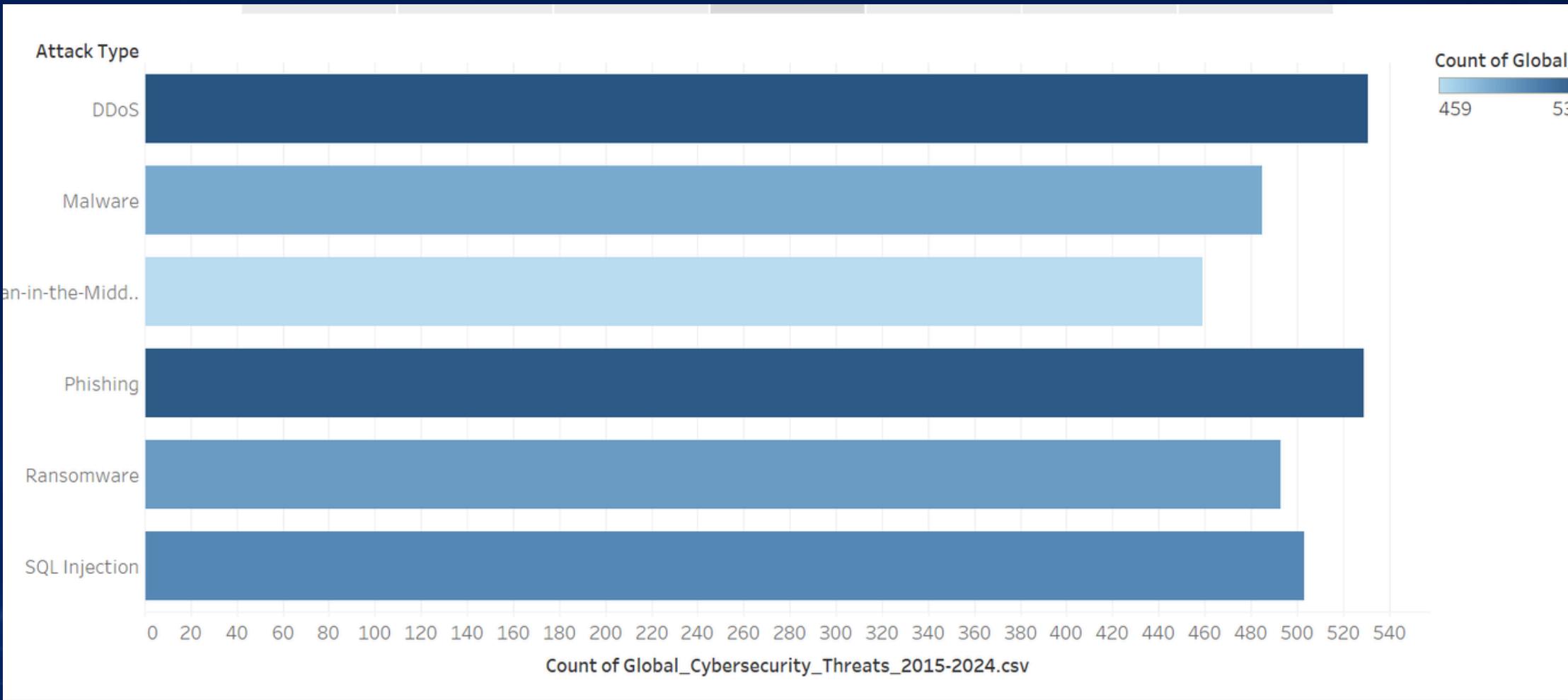




FINANCIAL IMPACT



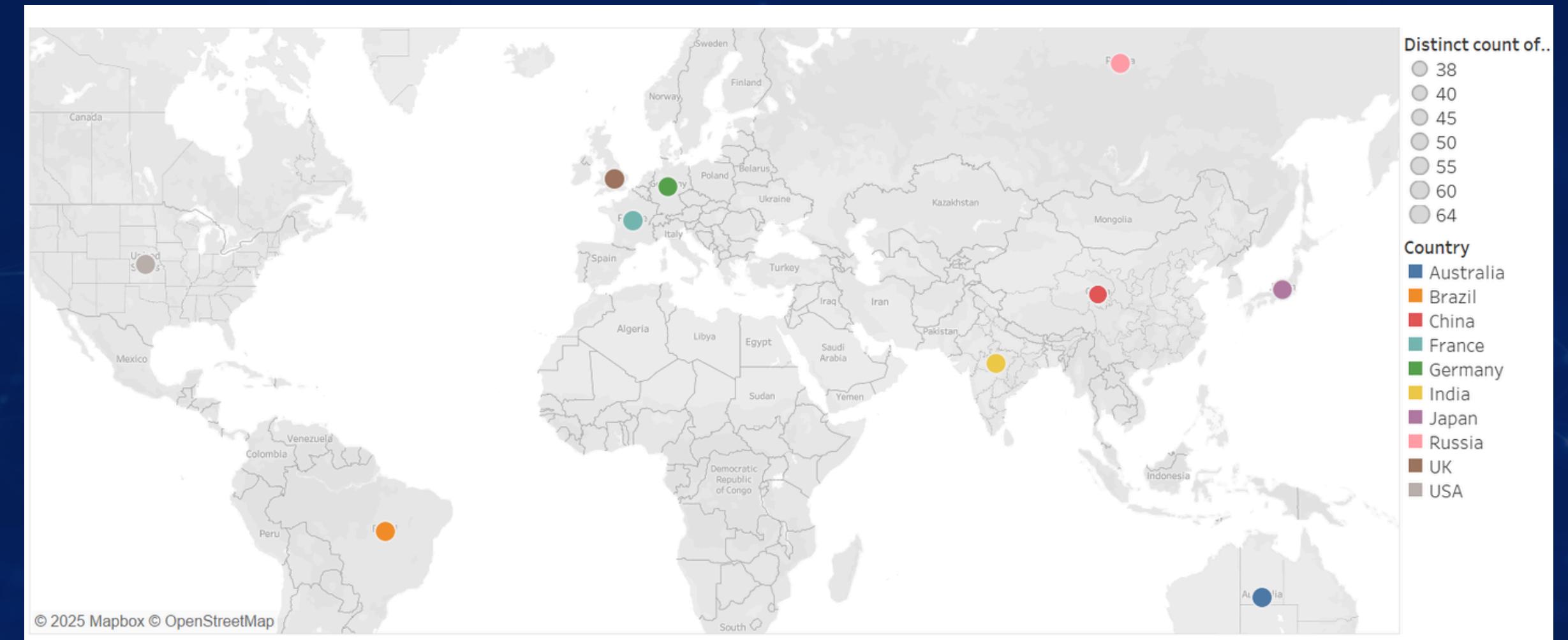




CYBER THREAT TRENDS

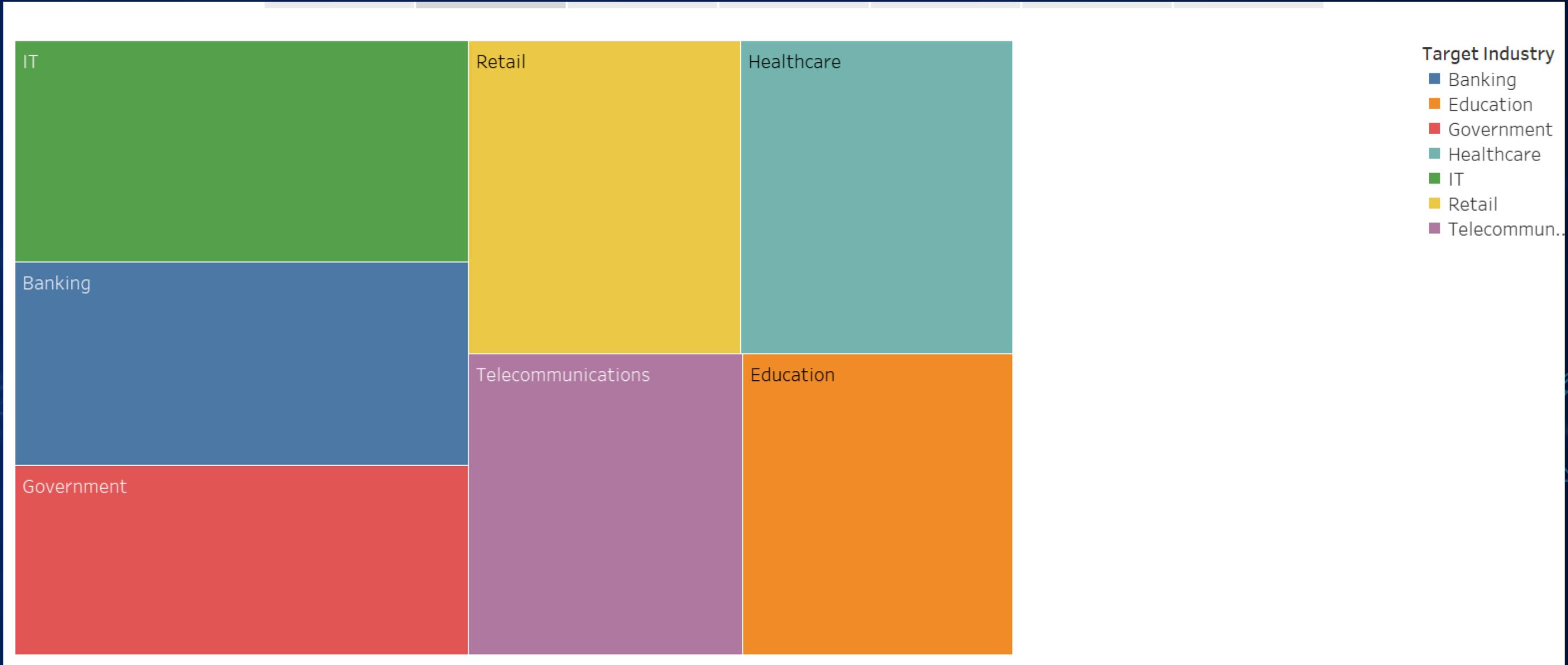


GEOGRAPHICAL ANALYSIS





INDUSTRY INSIGHTS





Source and Defense Mechanisms

Attack Sour..	Defense Mechan..	Security Vulnerability Type			
		Social Eng..	Unpatched ..	Weak Passw..	Zero-day
Hacker Group	AI-based Detection	■	■	■	■
	Antivirus	■	■	■	■
	Encryption	■	■	■	■
	Firewall	■	■	■	■
	VPN	■	■	■	■
Insider	AI-based Detection	■	■	■	■
	Antivirus	■	■	■	■
	Encryption	■	■	■	■
	Firewall	■	■	■	■
	VPN	■	■	■	■
Nation-state	AI-based Detection	■	■	■	■
	Antivirus	■	■	■	■
	Encryption	■	■	■	■
	Firewall	■	■	■	■
	VPN	■	■	■	■
Unknown	AI-based Detection	■	■	■	■
	Antivirus	■	■	■	■
	Encryption	■	■	■	■
	Firewall	■	■	■	■
	VPN	■	■	■	■



SOURCES AND DEFENSE MECHANISMS





PROPOSED SOLUTIONS

Encryption: Implement strong encryption protocols to secure sensitive data, especially in cases of ransomware or supply chain attacks.

AI-based Detection: Use AI algorithms for real-time monitoring and early detection of ransomware and phishing attempts.

Antivirus: Regularly update antivirus software to protect against malware, including cryptojacking scripts

Firewall: Deploy robust firewalls to guard against unauthorized access and mitigate risks associated with IoT devices and DDoS attacks.

VPN: Use VPNs to secure remote connections, ensuring data integrity when accessing networks, especially in remote work setups.



CONCLUSION

The analysis of global cybersecurity trends highlights the ever-growing complexity and diversity of cyber threats across industries and regions. With financial losses mounting and millions of users affected, it is clear that addressing vulnerabilities such as weak passwords, unpatched software, and sophisticated social engineering tactics is critical. This project underscores the need for innovative defense mechanisms, proactive monitoring, and global collaboration to build a resilient digital ecosystem. Together, we can drive meaningful actions toward a safer and more secure cyberspace



THANK YOU FOR YOUR ATTENTION



bbalyan1996@gmail.com



[Github](#)



[Portfolio](#)