Article

Analytics-Driven Insights into Cybercrime Evolution, Trends, and Defense Strategies: A Comprehensive Survey

Muhammad Abdullah , Muhammad Munib Nawaz , Bilal Saleem , Maila Zahra , Effa binte Ashfaq , Zia Muhammad *

Posted Date: 27 May 2025

doi: 10.20944/preprints202505.2057.v1

Keywords: Cybersecurity; Internet Crime; Cyber Threats; Cyber Scams; Cybercrime Statistics; Cyber Trends; Cyberattacks; Cyber Crime Evolution; Cyber Crime Impact; AI-Generated Attacks; Deep Fakes

Article

Analytics-Driven Insights into Cybercrime Evolution, Trends, and Defense Strategies: A Comprehensive Survey

Muhammad Abdullah [1], Muhammad Munib Nawaz [1], Bilal Saleem [1], Maila Zahra [1], Effa binte Ashfaq [1] and Zia Muhammad [2,*]

[1] Department of Cyber Security, Air University, Islamabad 44000, Pakistan
[2] Department of Computing, Design, and Communication, University of Jamestown, Jamestown, ND 58405, USA
* Correspondence: zia.muhammad@uj.edu

Abstract: The landscape of cybercrime has undergone significant transformations over the past decade. Present-day threats include AI-generated attacks, deep fakes, 5G network vulnerabilities, cryptojacking, and supply chain attacks, among others. To stay resilient against contemporary threats, there is a need to examine historical data to provide insights that can inform cybersecurity strategies, policy decisions, and public awareness campaigns. This paper provides a comprehensive analysis of the evolution of cyber trends in state-sponsored attacks over the past 20 years, based on the Council on Foreign Relations State-Sponsored Cyber Operations (2005-Present). The study explores the key trends, patterns, and demographic shifts in cybercrime victims, the evolution of complaints and losses, and the most prevalent cyber threats over the years. It also investigates the geographical distribution, the gender disparity in victimization, temporal peaks of specific scams, and the most frequently reported internet crimes. The findings reveal a traditional cyber landscape, with cyber threats becoming more sophisticated and monetized. Finally, the article proposes areas for further exploration through a comprehensive analysis. It provides a detailed chronicle of cybercrime's trajectory, offering insights into its past, present, and future.

Keywords: cybersecurity; internet crime; cyber threats; cyber scams; cybercrime statistics; cyber trends; cyberattacks; cyber crime evolution; cyber crime impact; AI-generated attacks; deep fakes

1. Introduction

In the past two decades, cybercrimes have taken a very swift turn in complexity and sophistication. Thus, to cope with this dynamic nature in-depth knowledge and understanding of the cybersecurity trends is necessary. According to the FBI's Internet Crime Complaint Center (IC3) in 2023, over 800,000 cybercrime complaints were reported and total losses exceeded $10 billion[1]. Such numbers signify the need for a more robust approach towards these attacks and trends. According to the IC3, the total loss in the last five years was 3,5 billion, 4.2 billion, 6.9 billion, 10.3 billion, and 12.5 billion respectively [1]. As technology advances incrementally, so do the associated attacks. Like AI-generated attacks, deep fakes, 5G network vulnerabilities, and crypto-jacking [2]. Therefore, to get by this dynamic nature of cybercrimes, proactive measures should be opted for.

The variations in the cybercrime landscape have led to a variety of targets. Ranging from organizations, governments, corporations, and individuals. Due to the rapid increase in state-sponsored attacks national security and assets are at stake. Countries all around the globe are using cybercrimes as a means to derange critical infrastructure and gain political advantages over other nations. These evolutions in the cybercrime landscape have strained policymakers and law enforcement agencies all around the world to take rapid action[3]. The impacts of these attacks have gone way beyond financial losses, affecting national security and critical infrastructures.

Moreover, this evolution in the world of technology from the normalization of Artificial Intelligence to the growth of IoT devices has proven to be a catalyst for cybercrimes. These technologies have opened the doors for new attacks and vulnerabilities [4,5]. Where people are using these technological advancements to improve their day-to-day lives, adversaries are using them to form complex and sophisticated attacks. The growing complexity of the cyber threat landscape underscores the need for comprehensive strategies. That should address current and emerging risks, focusing on prevention, response, and international collaboration.

The digital medium has offered a platform for state-sponsored cyber attacks, which have gained global importance in the last 20 years [6,7]. These attacks are largely dependent on technological innovation and improvement. This area would require in-depth analysis to create strategies of a proactive nature to mitigate them.

Governments and states all around the world are employing a variety of cyber tools and techniques to get ahead of their strategic and technological rivals in the world. The same evolution has also changed the way states engage with conflicts. Governments use attacks like espionage and intellectual property thefts to vandalize other nations. These attacks have moved beyond the digital realm, affecting digital infrastructures, global economics, and individuals' trust in technology [6,8].

By exploring the evolution of these trends in state-sponsored cyber attacks over the past two decades, this study aims to highlight broader implications for global security and influence policy development. It's not only about understanding the previous contexts but also anticipating future trends with the view of designing more robust and proactive mitigation techniques.

It is necessary to understand and observe the geographical distribution alongside victim demographics to statistically analyze the complexity and sophistication of rapidly growing cyberattacks. Our study provides valuable insights into the victim, age, and gender patterns across various attack types for a better understanding of gender disparity. We also examined the temporal peaks of scams which can aid policymakers all across the globe in policy building. By scratching these surfaces we aim to develop an extensive understanding of the cybercrime landscape that can be used for public awareness campaigns. Following are some of the questions that this paper answers:

- What are the attack demographics for the past 20 years of cybersecurity? What is the impact of emerging technology on cybersecurity?
- What is the motivation behind cyber crimes in the current technological era? What are the recent victim demographics of cyber crimes around the globe?
- What are some of the methods that can be used for mitigating these attacks? How cyber crimes are affecting governments and large organizations?

Our study focuses on providing a broader view of dynamic cyber trends and state-sponsored cyber attacks. It also looks into the various other aspects linked to the issue such as analyses of victim states and geographical distributions. Our groundwork also focuses on providing extensive knowledge related to the vulnerable age groups and gender disparity in cybercrimes across the globe with the help of data provided by trusted and reliable sources like IC3 Report 2023. Finally, we discussed temporal peaks related to different cybercrimes and how the new attack trends can be mitigated.

This paper is structured in a way that it explains the dynamic nature of cybersecurity trends and attacks, it starts with a comprehensive section 2 that shows the literature review of existing research, followed by insights into evolving cybercrimes, and the succeeding section 3 elaborates on the geographical and temporal distribution of cybercrime. It also highlights Geographical and temporal distribution in section 4. Moving toward the next section 5 it highlights the evolving vulnerability of age groups over the years. The most occurring attacks and in which years they peaked the most. are discussed in Section 6. Finally, in Section 7, the paper discusses the analyses, suggestions, and discussions related to these findings and future trends. Finally, at least there is a conclusion section 8 which discusses the final discussion.

2. Literature Review

Cybersecurity infrastructure has experienced numerous changes over the past twenty years. To better understand these dynamics, it is necessary to consider the available literature to understand new trends, mitigation methods, attack vectors, and evolving targets. The existing literature provides rich knowledge ranging from the early malware and phishing techniques to new and modern attacks and tactics used by adversaries. This literature review with the help of reports from credible sources aims to provide an interpretation of modern cybercrimes, emerging threats, and implications for cybersecurity policies and practices.

Hoar et. al. [9] discusses that cybercrime, primarily due to phishing, has evolved into a constant menace, most of the time received as unsolicited emails that try to dupe users into revealing their personal information. This kind of identity theft by using trust and urgency may lead to the downloading of malware. Victims have much to lose, in terms of money and data, and thus, there is a manifold requirement of robust cybersecurity firewalls, antivirus software, and spam filters. Additionally, there has to be sensitization on how to identify and respond to a phishing attempt. Cybercrime is one of the most rapidly changing areas of crime, and it calls for vigilance and changing protective strategies.

Myriam et al. [10] highlight the importance of securing information infrastructure for economic and government operations. New challenges are created such as a lack of built-in security due to the interdependence of information systems and critical infrastructure. The research also points to the challenges in IT security as if the market is not prioritizing IT security because they do not see a return on investment (ROI), secondly, it is tough to secure complex interconnected systems. There is a need for interdisciplinary research because the response from different groups helps make effective solutions. The research further explores the role of states in cybersecurity, noting the privatization of security and public-private partnerships. Market mechanisms are insufficient to provide acceptable security. The author suggests the government should play their role in funding long-term research into critical infrastructure protection (CIIP). Finally, it is suggested that there is a need for a balanced approach where cybersecurity is supported without overregulation so the threat is managed without unnecessary alarms.

Su et. al. [11] focuses on cybersecurity in substation automation systems, and their evolvement from electro-mechanical to digital devices. The risk of cyber-attacks such as fake data injection is increased due to the wide adoption of ethernet-based communication, which results in the disruption of services provided by protection systems. To mitigate these risks, the author proposed context information like voltage and current measurement to enhance cybersecurity. To distinguish between genuine faults and those caused by malicious data, a Probabilistic Neural Network (PNN) can be useful because of its ability to analyze data from multiple measurements. The proposed methodology involves training the PNN with both real and Fake faults under different conditions and it is noticed that PNN can effectively identify the real and fake faults. In order to result with high accuracy there is a need for parameters smoothing for voltage and current. Finally, the research concludes that context information-based defense can be an additional layer of security against cyber threats in power system protection

Alvaro et. al. [12] discusses the increase in the use of information technology and computer networks there is more attraction between cyberattacks and malicious actors. Unlike physical attacks, cyber-attacks are difficult to identify because of no knowledge of origin and once any attack occurs it can be distributed and utilized by others globally. The research further explores the use of cybersecurity as a part of Homeland Security like how to make a comprehensive response system and risk management program for the protection of critical infrastructure. Like homeland security, it also highlights the use of cryptography for secure communication, network security for secure data transmission, and software security to protect against attacks like buffer overflows, injection attacks format string vulnerabilities. The research also highlights the trend in cyber-attacks from an individual hacker to an organized group with specific motivations like economic, political, and national interest.

Botnets, a network of compromised computer control by attackers is a serious threat. Because they are used for activities like spam and launching large-scale attacks.

Table 1. Literature Review and Research Paper Highlights with Inclusion Status.

AUTHORS	YEAR	CYBERCRIME TRENDS	GEOGRAPHICAL DISTRIBUTION	GENDER DISPARITY	PEAKS AND SCAMS	IMPLICATIONS
Hoar et. al. [9]	2005	✓	×	×	✓	✓
Myriam et al. [10]	2006	✓	×	×	×	✓
Su et. al. [11]	2007	✓	×	×	✓	✓
Alvaro et. al. [12]	2008	✓	×	×	✓	×
McCrohan at. el. [13]	2009	×	×	×	✓	✓
Chee-Wooi et. al. [14]	2010	✓	×	×	✓	✓
Amir et. al. [15]	2011	✓	×	×	×	✓
Broadhurst et. al. [16]	2012	✓	✓	×	×	✓
Sharjeel et. al. [17]	2013	✓	×	×	×	✓
Reddy et. al. [18]	2014	✓	×	×	×	✓
Bendovschi et al. [19]	2015	✓	×	×	✓	✓
Pescatore et. al. [20]	2016	✓	×	×	✓	✓
Osawa et al. [21]	2017	×	×	✓	✓	×
Cabaj .at. el. [22]	2018	×	×	✓	✓	×
Ali et al. [23]	2019	✓	×	×	✓	✓
Rajasekharaiah et al. [24]	2020	✓	×	×	×	×
Dillon et al. [25]	2021	✓	✓	×	✓	×
Kaur et al. [26]	2022	✓	✓	×	×	×
Stafiniak et al. [27]	2022	✓	✓	×	✓	×
Durojaye et al. [28]	2022	×	×	×	✓	✓
Francis et al. [29]	2023	✓	×	×	✓	✓
Fadziso et al. [30]	2023	✓	×	×	×	✓
This Paper	—	✓	✓	✓	✓	✓

McCrohan at. el. [13] article is a quantitative research study because it measures the change in behavior with a subject factor of high and low information. This research explains the importance of education and awareness. Which helps in changing security behavior. To prove the effect of education, participants were randomly assigned one of two security lectures due to poor password management. The low information condition was based on basic computer security and password management knowledge and the high information lecture was based on detailed knowledge of password management and security. Initially, both groups have the same knowledge. After two weeks it was noticed that those who attended low information lectures had no change but those who attended lectures with high information had password rating 36 percent strong. Finally, it reaches to conclusion that when a user is educated about security practices their behavior toward security should be changed and the chance of cyber-attacks will be minimal.

Chee-Wooi et. al. [14] focuses on the critical infrastructure of the electric power sector. By highlighting the role of securing complex physical and cyber systems in national security and economy. The article outlines the cybersecurity challenges faced due to the interconnectedness of computer, communication, and power infrastructure. It stresses the need for compliance with globally accepted standards like the North American Electric Reliability Corporation (NERC). The research further proposed a framework having four steps 1) real-time monitoring, 2) anomaly detection, 3) impact analysis, and 4). mitigation strategies. For impact analysis, tree-based methodology is used to evaluate vulnerability at various levels. The paper then highlights the type of cyber-attack on power infrastructure i.e., 1) direct attacks, 2) attacks through the system, and 3) attacks caused by system failures. It points out the importance of both physical and electronic security to safeguard critical assets. Finally, the paper discusses the evolution of the SCADA system and the need for security measures to address emerging vulnerabilities.

Amir et. al. [15] focuses on nuclear threats among superpowers the modern deterrence theory faces many challenges like terrorism and rogue states, and to check whether the traditional deterrence theory designed during the Cold War applies to cyber threats. Deterrence in cybersecurity is dependent on defender capabilities, threat effectiveness, and effective communication however these elements do not apply to cyberspace due to its unique nature. A cyber-attack can be launched by any individual from any area without a guessable physical location. However, deterrence is still possible in cyberspace under certain conditions deterrence not only requires cyberspace but also requires economic or military measures. Secondly, deterrence types like deterrence by denial work which helps in defending action or serial deterrence which is used when repeated response over time is required can be used in some situations. Finally, the research reached to conclusion about the importance of deterrence strategies in cybersecurity and suggest to examine traditional deterrence and extending the deterrence in the context of cybersecurity.

Reddy et. al. [18] highlights the importance of cybersecurity in the modern era. Cybercrime is proportional to the increase and advancement of technology. Irrespective of the fact that government and companies are playing their role in security measures, still there is a need for advanced cybersecurity techniques that help in various fields like cloud computing and mobile networks, etc. further author explains various aspects of cybercrime like network intrusion, dissemination of virus and identity theft the paper also shows the statistical analysis of growing cyber incident over time. Emerging trends in cybersecurity are also explained like the protection of web servers, cloud computing security, and challenges posed by advanced persistent threats (APTs). The author highlights the importance of security tools and techniques like encryption, firewall implementation, and anti-virus software. Finally, it highlights the need for the latest security rules and policies after the adoption of internet protocol verision6 (IPv6). The paper reaches to conclusion that the risk of cyber-attacks always remains but it can be reduced by following cyber ethics and guidelines

Sharjeel et. al. [17] discuss that cyber warfare has emerged to be one of the most prominent dimensions of contemporary conflict, where the developed nations are exploiting the vulnerabilities of cyberspace toward their gain in establishing supremacy. Notable examples are PRISM, Stuxnet, and Disttrack, which represent highly advanced capabilities that advanced nations possess. On this ground, developing nations, being heavily dependent on cyberspace, have technologies from the West and thus, in many ways, become vulnerable themselves. These dependencies are found to be the key factors creating sophisticated cyber threats to national, military, and private sectors. To offset such challenges, developing countries have to engage in administrative and organizational policies aimed at strengthening their cyber defenses. From this review of the literature, it is evident that the requirement for robust cybersecurity frameworks is growing with the ever-evolving cyber threats.

Bendovschi et al. [30] provide an overview of cybersecurity, its importance, and the evolution of cybersecurity attacks from first-generation viruses to fifth-generation multi-vectored attacks. The study also highlights the recent challenges in cybersecurity like data and supply chain attacks posed by third parties and the importance of automation in defending businesses against sophisticated cyber attacks. It also discusses cybersecurity myths like depending completely on passwords, deleting files from the system and only large companies are targeted by cybercriminals.

Francis et al. [29] highlighted the reason behind states engaging in cyber attacks and how it affects global peace and stability. The article highlights the motivation and impact of state-sponsored cyber attacks to answer this question. To address the evolving cyber threats effectively, the article recommends the development of international norms and standards for cybersecurity. Similarly, Bendovschi et al. [19] elaborated on the rapid increase in cybercrimes with the advancement of technology like cloud computing, online transactions, social networks, and automated processes. The study inspects the patterns and trends in cybercrime by analyzing international legislation and historical facts over the past three years. It also suggests countermeasures that should be taken by businesses all around the globe to defend their systems from such attacks and adversaries.

Pescatore et. al. [20] explores the shifting of cybersecurity threats and the challenges attached to them. This research underscores that there is a need to reduce vulnerabilities and strengthen defense to manage risk because the risk in cyberspace is influenced by threats, vulnerabilities, and the corresponding mitigation action. Different types of attacks like Denial of services and cybercrime are highlighted as key threats and their evolvement with the advancement in technology. New threat trends and their corresponding vulnerability are avenues for attack. Especially it is mentioned that ransomware emerges as a significant threat. Further, the concept of fourth-party attacks is explained where the complexity of supply chain security also affects third-party subcontractors indirectly thereby expanding the attack surface. Business trends in technology like the widespread adoption of mobile, and cloud services and the rise of IoT further complicate the landscape, introducing additional vulnerabilities.

Broadhurst et. al. [16] talks about exponential growth in Internet use across Asia, notably in China, Indonesia, and India, which has been matched only by a corresponding upsurge in cybercrime. This has been compounded at the same time by a proliferation of commercial-scale exploit toolkits and criminal networks monetizing malware. It reviews the law enforcement responses to cybercrime in Asia within the context of the 2001 Council of Europe's Cybercrime Convention (Budapest). This review outlines the nature of cybercrime, including both 'hate' content and 'crime-ware' like botnets, juxtaposing Asian laws with Convention provisions. It highlights how huge the challenges are in developing cross-national cybercrime policing that would be effective against the backdrop of cloud computing, social media, and smartphone applications, opening new avenues for digital crime.

Cabaj et. al. [22] addresses the complexities of cyber attacks and the need for advanced technology like artificial intelligence, data analytics, and machine learning to mitigate threats in real time. For effective detection of large data generated by different security monitoring systems, the need for these technologies is very important. This research is a collection of six research papers including various aspects of cybersecurity and forensics. One of the main focuses is on the 5G network, 5G's architectural features such as Control and User plane separation, and Network function virtualization and their impact on cybersecurity and digital investigation. Other issues include detecting complex cyberattacks using statistical analysis and machine learning, a Point of sale (POS) system for risk management in electronic funds transfer, and an OMMA framework to monitor multi-step attacks and distinguish between different types of DOS attacks.

Dillon et al. [25] talks about the evolution of technology and its impacts on society. The paper shows an escalation in ransomware attacks, Distributed Denial of Service attacks, and identity that has resulted in the growth of financial losses – totaling $3.5 trillion since 2001. Further research should encapsulate the evolving nature of cyber threats in the post-pandemic world.

Stafiniak et al. [27] study highlights the role of cybercriminal groups involved in achieving their geopolitical goals. The article uses the Russian military conflict in Georgia and Ukraine (2008-2022) by collecting information from various resources and also making a cross-section analysis. The goal of the study is to have a complete sketch of the modern world from the view of geostrategic interest and to show that states are affected by steps taken by threat actors in cyberspace. The article also made conclusions about how state-sponsored attacks have increased dramatically in the past few years and also made predictions. Durojaye et al. [28] focuses on the effect of state-sponsored attacks on cyberspace and core infrastructure by pointing out that vulnerability in the core infrastructure is the main cause of cyber-attacks. A prime example to back this statement is the power outage faced by Ukraine due to Russia in 2015. It is difficult to identify which state is responsible for the attack even after the attack discovery, so some states take advantage of this. The paper also analyzes the adverse effects of state-sponsored cyber-attacks like destabilizing the micro economy and diminishing the defense capacity of attacked states.

Osawa et al. [21] investigate the expanded use of cyber operations by nation-states to advance their national interests, focusing on how these cyberattacks frequently coincide with international conflicts. As the technology progresses, so as the dependency on it for economic and security purposes. This dependency has then increased the financial costs for development and maintenance along with the potential for widespread societal disruption. For instance the 2017 "Petya/Not Petya" ransomware can be considered to have disrupted many business and government institutes worldwide. The study sheds light upon the need for strong national policies, collective cyber defense techniques, and proper methods for information sharing between the like nations to cope with these evolving attacks and adversaries. However, the paper lacks in offering solutions for cross-border information sharing underscoring the need for standardized approaches to cyber defense. Ali et al. [23] show the rapidly increasing dependency on cybersecurity due to the advancement of technology in recent times. It also sheds light upon the increasing cyber threats and the continued rise in cybercrimes despite the efforts of governments and institutions. While the study shows how the advancement in technology is an ever-growing challenge for cybersecurity, it also addresses the latest trends and techniques in combating cyber threats. However, the paper is dependent on secondary data and to cope with the revolving trends and new developments ongoing research is necessary.

Kaur et al. [26] paper underscores the recent hurdles in evolving cyberspace. For decades symmetric and asymmetric encryption has been the backbone of data security but the dawn of quantum computing has posed a significant threat to it as well. Researchers all around the world a working to eliminate this threat. The paper underscores the need for ongoing research and innovation to address evolving threats in the cybersecurity landscape. Rajasekharaiah et al. [24] study tracks the growing challenges in cyberspace alongside today's evolving technology. With the normalization of social media, online shopping, and financial transactions nowadays, the associated cyber crimes have also become increasingly sophisticated. The papers highlight the role of data security in the fight against dynamic threats and cybercriminals. It also points to the increasing need for global identity management and monitoring techniques. Ultimately, the study suggests that old and traditional approaches are of no use in this rapidly developing world, there is a need for renewed and up-to-date measures.

The Table 1 gives a comparative analysis of our study and the available material. It also provides an overview of what is the research gap when it comes to cyber trends, victim demographics, and state-sponsored cybersecurity attacks. Each column in the table shows different topics we worked on during our research and whether the contemporary literature highlighted them.

3. Evolution of Cybercrime Trends

Over the past few decades complexity of the cybercrimes has taken a swift turn. The evolution has been possible due to unprecedented technological growth. Increased connectivity, digitalization, and automation of day-to-day activities have opened doors for more sophisticated cyber crimes.

Initially, cyber trends were used to be unsophisticated and primarily aimed to exploit basic vulnerabilities. These attacks weren't complex as compared to modern-day cybercrimes. In the early days, cybercriminals used to focus on targeting smaller businesses and individuals because they used to have the least amount of resources and awareness. The attacks used to be straightforward forward including attacks like social engineering, phishing scams, basic malware attacks, password brute forcing, and email-based frauds. Back in the day cybercrimes mostly revolved around exploiting human vulnerability using different social engineering techniques. Fake but convincing emails were made to trick individuals into revealing their personal information.

As the technology advanced, so did the cybercrimes associated with it. Technological leaps have fueled the rise of intricate cybercrime. The aggregate of ransomware attacks has increased in modern times, where cybercriminals unethically encrypt victim's data and then demand hefty ransom amounts to return the decryption key. Not only the individuals but large corporations have been affected by these attacks. Advanced persistent threats (APTs) represent another significant development. Such attacks are often state-backed or state-funded, they involve extended stealthy intrusions into complex computer networks to steal sensitive information or cause disruptions.

Over the years, the landscape of cybercrime victims has also shifted. In the early days, only individuals and small-scale businesses were the targets of cybercriminals due to a lack of security resources and awareness. But now with each tech breakthrough, cybercriminals devise more intricate schemes due to which larger organizations, including private sectors, governments, civil society, and the military are becoming frequent targets Figure 1 shows the demographics of the most affected sectors all around the world from the year 2005 to present.

In the initial days cyberattacks were of less severity and complexity due to which victims had to bear miner financial losses. But just as technology evolves, so do the minds behind cybercrime, creating a constant arms race that has caused a drastic increase in cybercrime reports and events. Figure 3 shows the increase in cybercrimes from the year 2005 to the present and from the same image a rapid increase in cybercrimes can be observed from the year 2018 and onwards.

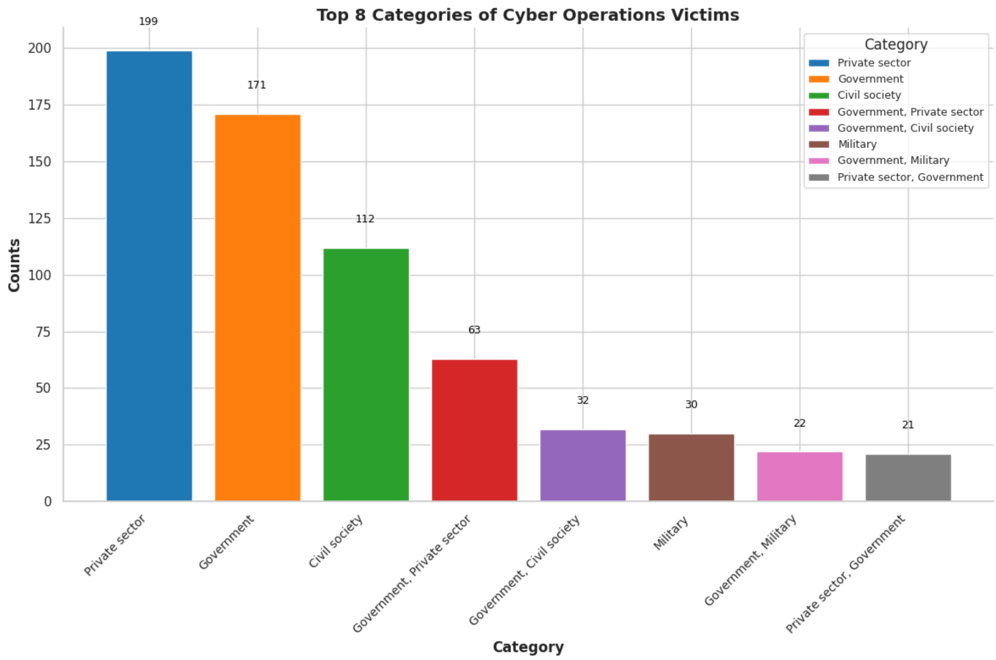

Figure 1. Most Affected Sectors.

3.1. Data Analysis Methods

To provide an in-depth and comprehensive view of the cybersecurity trends, precise data analysis methods were used. This section provides details of the data analysis methods used, to collect and visualize all data in this paper. Also ensuring the integrity and accuracy of the findings presented in this paper.

- **Data Collection:** The data used in the research has been collected from various credible sources like the IC3 Report 2023 [1] and the data set that is used in this research is a well-organized and comprehensive collection of all of the data related to state-sponsored cyber attacks from the year 2005 to the present [6]. The data set tracks statistics like summary and description of the cyber operation, date of happening, and state affiliated with the respective operation. Following these statistics responses against these cyber operations, victims and their categories that were targeted, and finally, the sources that reported the operations are also tracked via this data set. With these statistics in mind, we can form a robust framework for understanding the patterns of state-sponsored cyber operations.
- **Data Preprocessing:** Before the data was used for analysis it went through a preprocessing cleaning phase. In this process, all the duplicate and redundant data was removed. Following this methods like data imputation were used to address any gaps in the data and lastly, the data was converted into a suitable format for data analysis.
- **Analytical Techniques:** For analysis we trained a machine learning algorithm using tools like Jupiter Notebook. We automated all the cleaning and visualization processes using this machine-learning algorithm.
- **Data Visualization:** Charts and graphs are used to show the demographics from the data analysis. They were made precise using the machine learning algorithm. Alongside these heatmaps were used to show the intensity and frequency of cyber threats across different regions or periods.

3.2. Evolution of Cybersecurity and Cybercrimes from 1960 to Present

The following section provides a historical background of how cybersecurity evolved over time.

3.2.1. 1960's

The Early 1960s was the time when initial technological advancements gave birth to connectivity [31]. Computers at that time were expensive, large, and bulky. A single computer was used by many individuals at the same time. This timesharing resulted in the need to prevent unauthorized access to the computers and their files. From here the concept of data security and hardware security was born.

3.2.2. 1970's

In the 1970s ARPANET, the first form of the internet was formed which gave hackers all around the globe a lot to think about [32]. ARPANET was a stepping stone for new technology and hackers. During this time early malware like the Creeper and Reaper were also made but, they were considered as academic exercises rather than actual malware. In 1975 a paper by the title *The Protection of Information in Computer Systems* [33] was published that gave principles that would become the foundation of modern cybersecurity.

3.2.3. 1980s

This decade is considered to be the most chaotic one. The Internet was formed in 1983 and the networks all around the world started adapting the Internet Protocol Suite [34]. This adaptation added more preies and adversaries to the mix. The dictionary attack that is used to exploit weak or default passwords was also first launched in the 1980s. The first state-level attack also took place in this decade where a hacking group working for the KGB got access to confidential and sensitive U.S. military documents [35]. Secondly, the first actual malware *The Morris Worm* was also created in the 1980s.

3.2.4. 1990s

The era is also known as the *era of viruses*. Personal computers were considerably common in these years. Due to this normalization, unskilled hackers or script kiddies used to download scripts or pieces of code to run without having to write their code. Further, they used that code to launch malware to vandalize computers for fun. These attacks then led to the rise of anti-malware and security software. This era was the time when all the tech giants around the globe started taking cybersecurity seriously.

3.2.5. 2000s

In this decade the world shifted towards digitalization, especially in the field of banking and money transactions. This digitalization and evolution increased the rate of credit card breaches and online financial scams. Alongside such attacks holding large organizations and corporations' critical digital infrastructure for ransom was also common as hackers all around the world realized that they could make real money from cybercrimes. So, due to this rapid increase in crime sophistication, many companies worked on improving their cybersecurity posture.

3.2.6. 2010s

By this decade the state-sponsored and state-backed attacks were at their peaks. The attacks were more sophisticated and complex than ever besides this the development of cyberweapons also sky-rocketed. Major hacking groups targeted various tech giants and corporations all around the world with the intent of stealing data and launching ransomware attacks. Large-scale cybercriminal activities like the WannaCry and NotPetya were the cause of global damage.

3.2.7. The Present

As we are transitioning towards are more interconnected world every coming day the cybersecurity risks and threats are also increasing. New technological advancements like 5G, quantum computers, IoT devices, and cloud-based services have increased the attack surface. So to cope with these advancements robust and proactive mitigations and precautionary measures should be practiced.

Figure 2 shows the yearly growth in losses due to malware attacks all across the world from the year 2009 to 2020 in millions.

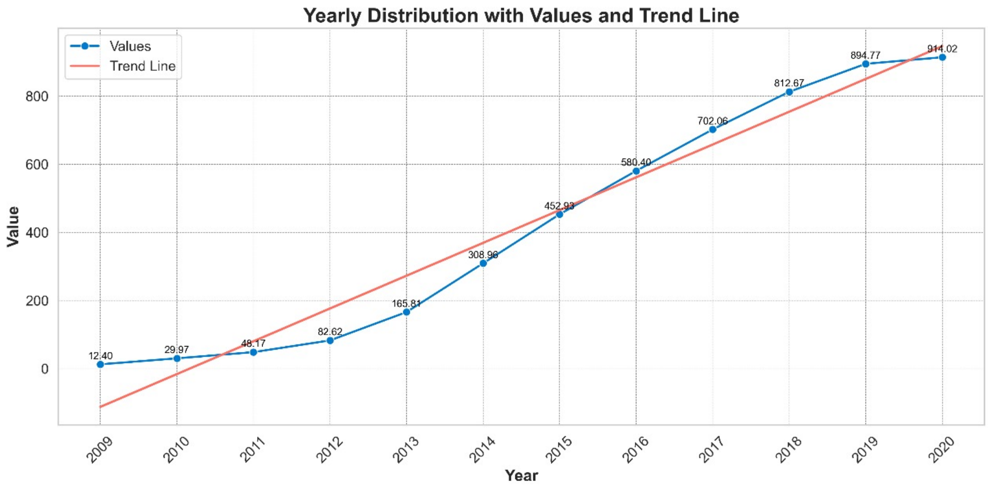

Figure 2. Yearly Growth Of Losses Due To Malware Attacks in Millions.

4. Geographical and Temporal Distribution

The rate of cybercrimes is increasing rapidly, posing significant threats to individuals and organizations across the world. For proper mitigation of these cybercrimes, understanding geographical and temporal distribution is necessary. The section provides analyses of cybercrime distribution across the United States in the years 2020 and 2021 with the aid of data provided by the Internet Crime Complaint Centre, a unit under the FBI.

Cybercrimes are never uniform, it depends on the following factors:

- **Population:** Population plays are very vital role when it comes to geographical and temporal distributions of cybercrime activities. Always the densely populated areas will be deeply affected by cybercrimes.
- **Economic Concentration:** One of the root causes of increased cybercrimes in a region is economic concentration. Cybercriminals mostly target the areas where economic congregation is elevated.

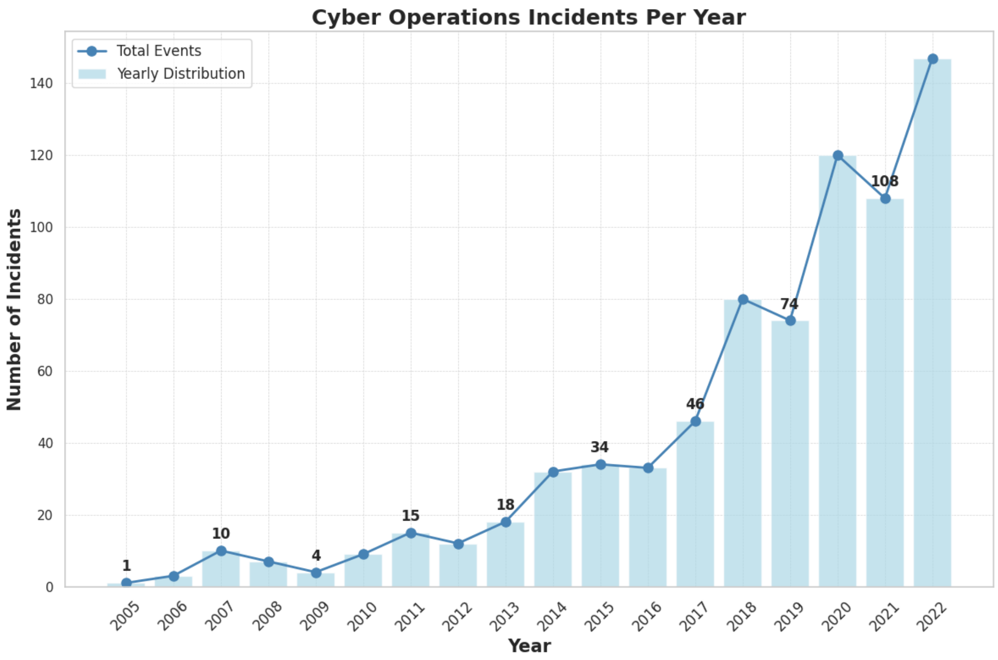

Figure 3. Increase in events in the last 15 years.

- **Technological Hubs:** Technological hubs being the home of tech giants, are always are target for cybercrimes. The wealth of data that they produce is always vulnerable to many sophisticated cyber attacks

4.1. *Geographical Spread of Cybercrimes*

Every day cybercrimes like phishing scams, ransomware, identity thefts, and data breaches are reported all around the globe. However, certain regions appear more affected by these attacks. Below is an overview of the distribution of US states according to the Internet Crime Complaint Center (IC3) in 2023 [1]:

- **Urban Areas and Technological Hub:** States like New York, Los Angeles, San Francisco, and Chicago are targeted by cybercriminals more as compared to other states due to their technological density and high population.
- **State Trends:** The US states like California, Florida, Texas, and New York are often struck by different cybercrime activities. This trend may be due to their dense population and large-scale technological hubs.
- **Regional Distribution:** In this rapidly evolving world of cybersecurity there is no area immune from digital threats. However, some regions like the east cost and the west cost exhibit higher cybercrimes due to all the factors discussed earlier.

4.2. *Most Targeted States and Patterns*

From the data provided by the Internet Crime Complaint Centre, of FBI we have derived the following results demonstrated in the Figure 4:

- **States With The Most Complaints:** States like California , Florida, New York, and Texas were the states with the most number of complaints in the year 2023. Some of these states are heavily populated and are considered as the technological centers due to which they often report high cybercrime rates.
- **Emerging Trends:** In the year 2023 small states like Ohio and Arizona have shown a relative increase as compared to previous records. This could be due to their significant financial sectors and proximity to larger urban centers.
- **Industry-Specific Targeting:** States with high industrial density like New York and California are the targets of financial frauds and data breaches.

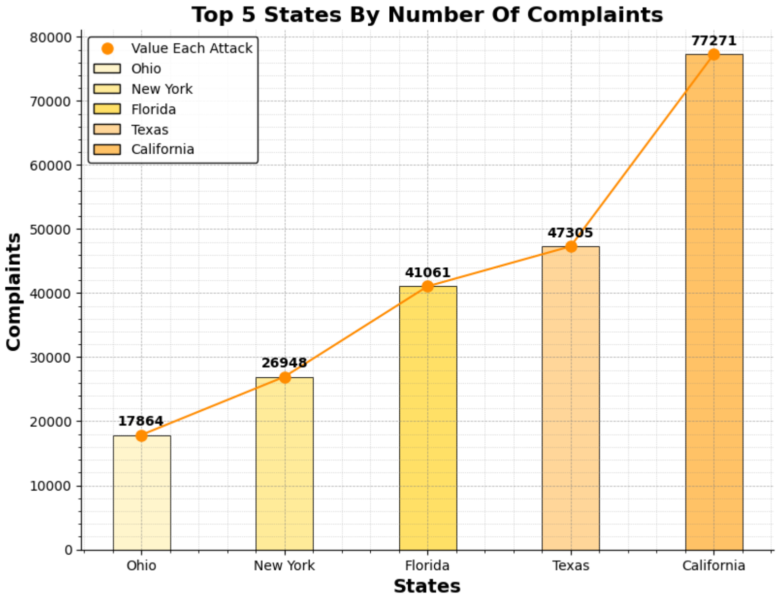

Figure 4. Top 05 States By Numbers Of Complaints According to IC3 in the year 2023.

doi:10.20944/preprints202505.2057.v1

5. Gender Disparity and Vulnerable Age Groups in Cybercrimes

Cybercrimes all over the world have observed an escalation in the last two decades with adversaries targeting victims across various demographics. This section'll discuss the gender disparity and vulnerable age groups in cybercrimes.

Analysis of the cybercrime data shows that the ratio of males and females is balanced. However, some studies like the FBI's IC3 [1] have shown that mostly females are targeted by cybercriminals all around the globe. This ratio is consistent across many cybercrimes like financial fraud, hacking, ransomware, and phishing.

Age groups of both cybercriminals and victims of these cyber attacks have evolved in the past few years. Nowadays most attackers and cybercriminals are in their mid-teens or in their mid-twenties. With each technological milestone, cybercriminals develop more elaborate ways to exploit them. This development needs advanced technical skills and knowledge due to which this age factor has experienced such trends.

5.1. Male and Female Cybercriminal Ratio

A study by the FBI's IC3 shows that most men are involved in cybercriminal activities. Out of all the cybercriminals 80% of them are males. The reason behind these increased numbers is that in cybersecurity aspects males outnumber females. However recent trends indicate a surge in the number of female cybercriminals. This shows the sophistication of cybercrimes and the access to cybercrime tools, allowing individuals regardless of their genders to be involved in unlaw and unethical criminal activities. Such trends and patterns highlight the need for more robust and proactive countermeasures to cope with this evolution.

5.2. Victim Age Distribution

When it comes to victims, people over the age of 60 are often targeted by cybercriminals. According to FBI's IC3 [1] nearly 35% of the cybercrime victims are over the age of 60. This can also be observed in Figure 5. Most people in this age group are vulnerable to financial fraud which is why according to the report people over 60 years of age have lost $3.4 billion in online financial frauds. This mostly happens due to their lack of awareness and vast financial resources.

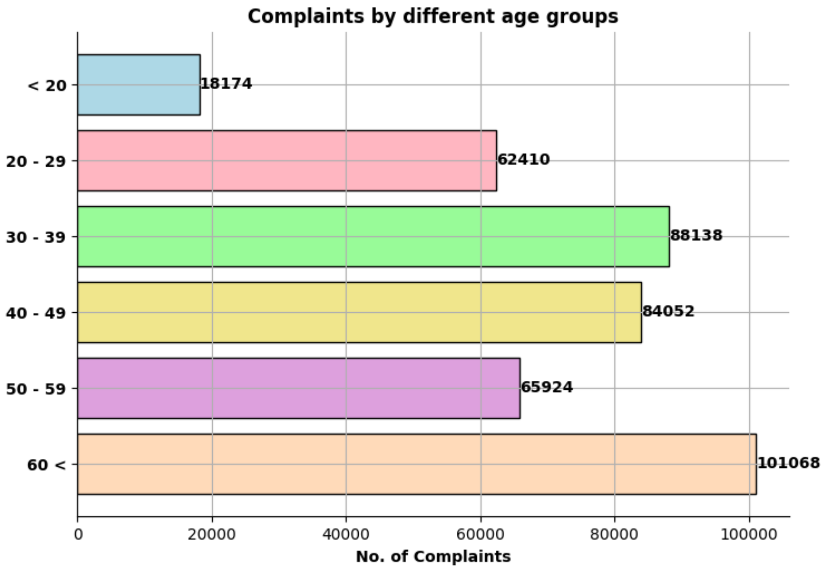

Figure 5. Compalints by different age groups.

People who lie under the age group of 30 - 50 years are mostly subject to phishing, social media scams, and identity theft due to their significant online presence. Whereas adults between 18 and 25 years of age are mostly victims of cyber and online bullying.

6. Temporal Peaks and Scams

Cybercrimes have been rapidly evolving lately, with certain attacks peaking in specific periods. Below is the discussion on the most occurring attacks and in which years they peaked the most, what were some of the factors that contributed to these peaks, and some order observations related to internet crimes.

6.1. Notable Scam Peaks

6.1.1. Phishing

Phishing one of the most common and oldest cybercrimes, reached the zenith in the year 2021 during the COVID-19 pandemic according to IC3 report 2023 [1]. During this period most individuals relied on technology for communication and entertainment purposes which provided cyber criminals with more opportunities to launch phishing attacks. Phishing involves sending fraudulent emails or messages to trick an individual into revealing their Personal Identifiable Information (PII).

6.1.2. Personal Data Breach

In acquaintance with the IC3 report 2023 [1] in 2022, personal data breaches reached their climax. Personal data breaches occur when a cybercriminal or adversary gains unauthorized access to sensitive information. Cloud storage, online services, and remote work were some of the contributing factors

6.1.3. Non-Payment/ Non-Delivery

IC3 report 2023 [1] shows that in the last five years payment and delivery scams peaked in 2020. In such attacks, cybercriminals and fraudulent businesses trick others into buying products and services that were never delivered. Such attacks lead to critical financial losses.

6.1.4. Tech Support Scams

According to reports Tech support scams reach their highest point in the year 2023. In such attacks, adversaries act as legitimate technical support groups and trick individuals into payment scams. Such attacks are intended towards old age people due to their lack of awareness and vast financial resources.

6.2. Modus Operandi Patterns and Trends

According to the reports it can be observed that cybercrimes reach their climax in times of uncertainty and change, for example during the COVID-19 pandemic. According to survey [36,37] out of 3254 participants reported increased online application usage during the pandemic. Such numbers indicate the expanded attack surface for cybercriminals in the coronavirus period.

The modus operandi depends on the scam type. The following table shows the modus operandi of various attacks:

Table 2. Cyber Attacks Their Modus Operandi.

Attacks	Modus Operandi
Phishing	Emails, messages, and malicious Links
Personal data Breaches	Hacking or Malware
Extortion	Ransomware or threats to reveal personal information
Tech Support	Social engineering
Ransomware	Encrypting user data
Malware	software designed to cause harm
DDoS	Overwhelming the target to make it slow
MitM	Intercepting Communication
XSS	Injecting malicious scripts
Creds. spoofing	Using combinations of passwords to gain unauthorized access
Zero-Day	Exploiting unknown vulnerabilities
Insider attacks	Malicious attraction taken by someone within the organization
DNS spoofing	Redirecting website to a malicious website

6.3. Scams and Sponsors

6.3.1. Scams

- Espionage: According to the data espionage is at the top of state-sponsored attacks. These attacks involve stealing sensitive pieces of information and intellectual property.
- Sabotage: After espionage attacks in the list is sabotage. In such crimes, governments or states target critical infrastructures.
- Distributed Denial of Service (DDoS): Third in the list is DDoS or Distributed Denial of Service. Such attacks are used to disturb different services.
- Data Destruction: Succeeding to DDoS in the list Data Destructions. Governments use these attacks to destroy financial data, country databases, and all.
- Doxing: At the end of the list are Doxing attacks where the personal information of an individual is used to harass or intimidate them.

6.3.2. Sponsors

- China has been recognized as the leading country in state-sponsored attacks in the last two decades with numbers crossing 250. China has recently been involved in cyber-espionage attacks targetting various states' intellectual
  properties, secrets, and digital infrastructure. The Chinese government is believed to sponsor a complex network of cyber units that engage in persistent threat activities. A Chinese Hacking group Double Dragon was associated with $20 million theft in COVID-19 relief aid in the US. [38] Figure shows elaborate the top Affiliated groups in global cyber crimes Figure 6
- Russians are one of the top contenders in cybercrimes after China. Russia is also accused of using cyber attacks and tools to support its geographical objectives and interference in foreign elections. This can also be proved by the NotPetya ransomware attack [39]. Many Russian hacking groups like the Nobelium and Midnight Blizzards have been accused multiple times for their cyber attacks on Western countries.
- Iran's state-sponsored attacks are driven by geographical and ideological motives. Iran has been involved in state-backed attacks like espionage, sabotage, and cyber-terrorism. Iran has attacked many governmental networks and energy infrastructures in the past few years.

- United States has a more defensive approach when it comes to state-sponsored attacks. The US focuses on protecting its critical infrastructures and safeguarding its state from different cybersecurity threats. But the country has also been involved in many sophisticated cybercriminal activities like the Stuxnet.

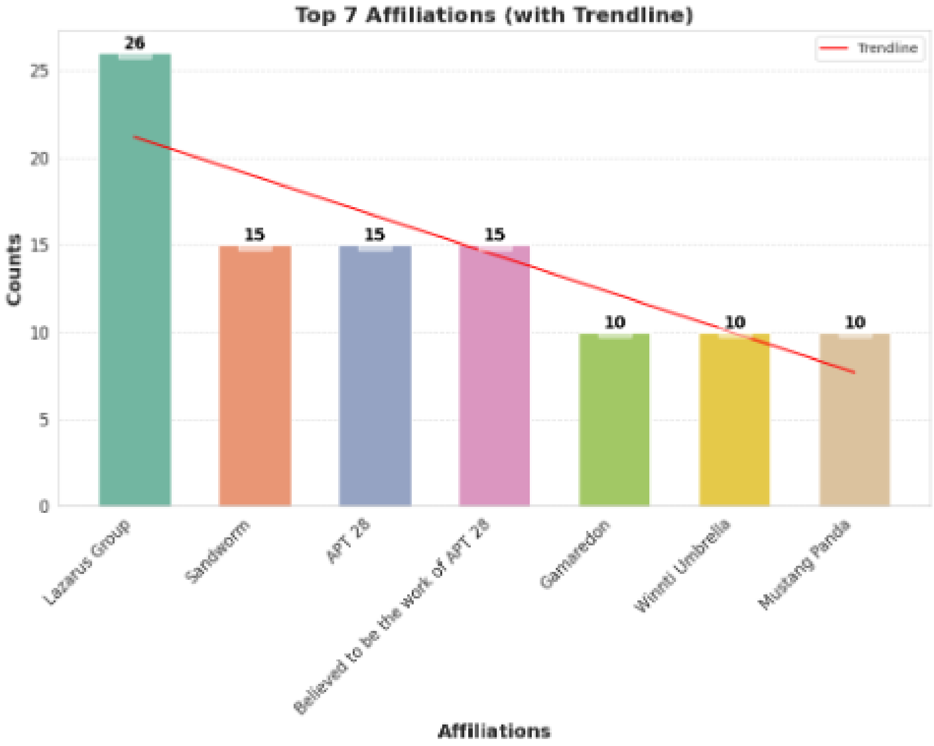

Figure 6. Top 6 Affiliated Groups in Global Cyber Crimes.

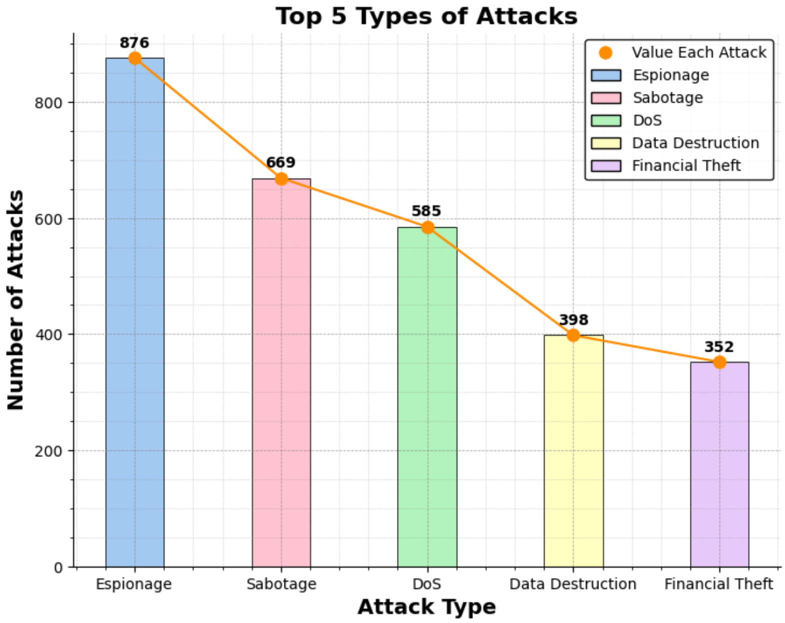

Figure 7. Top 5 Attack Types from the year 2005 to the present.

- Other developing countries like Vietnam and Pakistan are also emerging candidates in state-sponsored attacks.

Figure 8 shows the statistics related to all the top sponsors of attacks around the world from the year 2005 to the present.

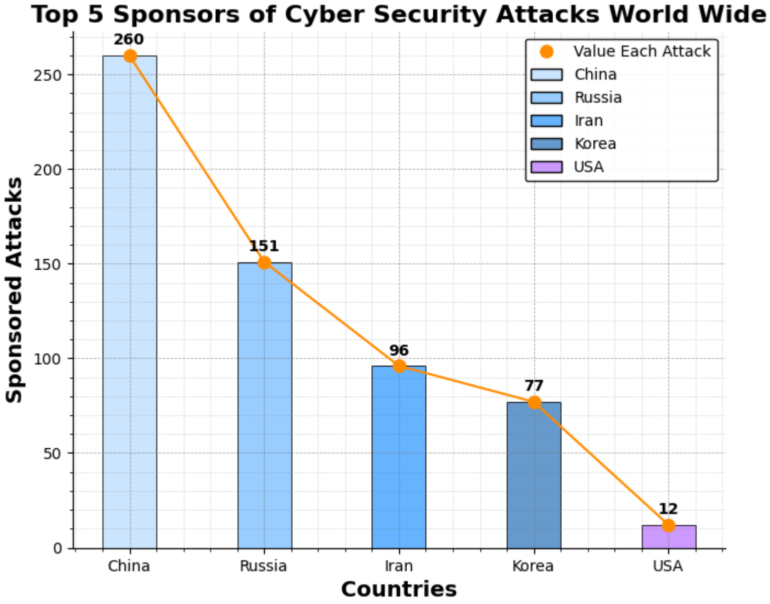

Figure 8. Top 7 Sponsors of attacks over the world.

6.4. Global Data Breach

By looking at the number of breaches in 2022, it can be observed that 87.3% of all the countries have breach density lower than the global average i.e. 50 leaked email accounts per 1,000 users. These statistics show that cybercriminals attack some countries more than others.

Russia has nearly 17 times more leaked email accounts than the global average. When we put these statistics into numbers then it can be seen that 8 out of every 10 users in 2022 were breached. It can also be observed that developing countries are targeted less by hackers as compared to more advanced and developed countries.

On the continental level Asia and Africa have the lowest breached email accounts. Whereas Europe has the highest breaches. Further statics can be observed from the Figure 9.

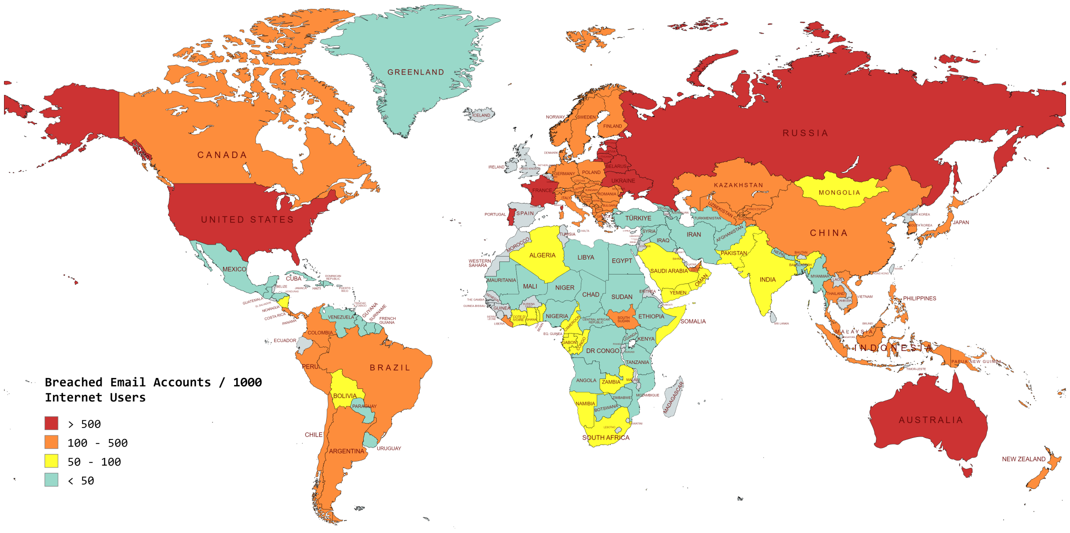

Figure 9. Heat map of breached email accounts all across the world.

7. Discussion and Implications

In this section we'll go through the prevalent cybersecurity attacks that are common nowadays and some emerging cybersecurity threats as well. Some prevalent cyberattacks that are becoming common are as follows:

1. **Phishing attacks** are one the most common cyberattacks in which criminals use techniques like social engineering by sending emails to the targeted individual to trick them into thinking that the email is from a legitimate source. If the attacker uses voice males in their phishing attack then such attacks are known as *vishing* and if it is done in the form of SMS then it is categorized as *smishing*.
2. Another pervasive attack that is common nowadays is **ransomware**. In this attack, the adversary encrypts the files and folders of the victim and then demands a certain amount as ransom. If the user pays the desired ransom on time the attack releases their system or information. To put pressure on the affected users attackers sometimes use a technique known as Double extortion in which the attacker threatens to leak the information if ransom is not paid.
3. **Espionage attacks** have been one of the most common and leading cyber-attacks in the past years. This attack damages the national security concern and the privacy of individuals. Normally attackers go against governments or businesses. It can be spread by the aid of malware and any other social engineering technique. The Intention behind these attacks can be money, power, or secret. There is a need to implement tough security measures and best practices to minimize these attacks.
4. **Supply chain attack** mostly known as third-party risk exploitation is an attack that targets a system or a network via a third party. Normally victims are directly targeted by the attackers themselves but in a supply chain attack, the third party is exploited. The third party can be a vendor, a contractor, a dealer, or any other individual or network connected directly to an organization or a person. The motivation behind this attack is to gain access to the main system using the smallest and weakest link i.e. the external party in this case. Supply chain attacks can be then further classified into three categories i.e. software-based attacks where prebuilt software is either imported or manufactured with the collaboration of an external party. The next one is the hardware-based attack where hardware components are bought from an external entity. Last but not least is service service-based attacks where an individual or an organization is using a service provided by a service provider.
5. **Zero-day exploits** are the exploitation of a new vulnerability in a system or a network that has never been exploited before. The technology and software landscape is constantly evolving. This evolution has worked as a catalyst for new and improved technological devices. The market for these devices is increasing rapidly alongside zero-day exploits.
6. **Destributed Denial of Service (DDoS)** is also one of some prevalent attacks that are common nowadays. In a DDoS attack, a particular system, server, or organization is overwhelmed by the excessive amount of requests from multiple locations. On the other hand when the requests are only coming from a single source then the attack is classified as a DoS attack. These two attacks are very common nowadays mostly at the state level where different countries are using such attacks to sabotage the critical digital infrastructure of fellow countries and states to gain technological advantage.
7. **Man-in-the-Middle (MitM) Attacks** are the attacks in which the adversaries intercept the communication between two entities or nodes. Such attacks are also common nowadays. Some precautionary measures like strong Wifi passwords, secure communication protocols, and channels can be used to decrease the likelihood of such attacks.
8. **Advanced Persistent Threats (APTs)** are very complex, sophisticated, and multilayered cyberattacks. These attacks are mostly state-sponsored and are used by governments to sabotage other countries and agencies. In some cases, the targets of such attacks are also large organizations and companies.

7.1. Future Cybersecurity Trends

Keeping an eye on predicting upcoming cybersecurity trends is very crucial for developing proactive measures to mitigate them. The sophistication of attack vectors nowadays is due to rapid technological advances and evolving cybersecurity trends. Organizations should evolve as well in order to secure their infrastructure properly. This is only possible if we anticipate the potential threats, understand the dynamic aspect of security, and implement proper security measures.

1. The main purpose of AI is to automate tasks to make our daily lives easy. Different machine learning algorithms are used for these purposes. The attackers nowadays also use AI to automate these exploits and malware development and to generate legit-looking emails and text messages that can further be used in social engineering campaigns. These algorithms are more efficient in bypassing security systems without being detected. Traditional cybersecurity measures are not enough to handle such attacks.
2. The process of creating realistic-looking images of an individual using a deep learning algorithm is known as Deep Facks. Deep fakes have useful applications in different industries but cybercriminals are using this technology for negative purposes. As mentioned earlier it generates realistic images that can be used for many ethical purposes. Creating fake but real-looking images and videos using deep learning algorithms can be dangerous for exploiting human vulnerabilities.
3. The motivation behind quantum computing is to have a computing system that works at a speed of exponent or we say exponentially faster computing. Quantum computing is also an emerging threat If it is used for negative purposes, as quantum computing contains bits known as qubits, these quantum bits have the property to be in multiple states at a time which causes parallel execution in a much faster way. Quantum computing uses algorithms like *Shors* and *Grovers* algorithms which are very effective in breaking cryptographic algorithms because of their efficiency for dividing data into half and factoring large composite numbers. The impact of this affects the confidentiality, integrity, and authenticity of sensitive information. Above is only one effect of quantum computing from a cybersecurity perspective. other can be technological inequality, data privacy regard, and cryptographic vulnerability.
4. 5G network mobile communication is extremely fast and devices are connected more reliably. In a 5G network, the network is divided into slices. Each slice is for a specific use and purpose however these also introduce difficulties related to isolation and unauthorized access to sensitive information. 5G network introduces vide variety of security challenges that can be exploited, like its use of unique authentication and authorization mechanisms which also introduce issues like improper key management in protocol and security flaws irrespective of the fact that they aim to have an enhanced security measure.
5. Iot-based attacks are also becoming a rising threat nowadays. As the technological world and interconnectivity of all devices are increasing all around the globe, the attacks and risks associated with it are also increasing rapidly. The prevention for such attacks suggested by researchers throughout the world is decentralization of technology or using blockchain.
6. Slowly but surely the technology will use the cloud as its primary storage and data transmission source. This will increase the ratio of Cloud-Based Attacks. In such attacks, attackers exploit the cloud-based vulnerabilities. To gain unethical access to data or services.
7. The trend of Ransomware-as-a-Service (RaaS) attacks has also increased in recent times. Some platforms are providing ransomware as a service nowadays. Due to such platforms less skilled hackers are now capable enough to launch their ransomware. These platforms also provide the facility of deployment as well which has drastically increased the sophistication of these attacks.
8. Finally there are hybrid attacks where attackers or adversaries use a combination of two or more attacks. This makes the attack harder to detect and defend against.

7.2. Preventive Measures

1. Training and awareness play an important role in minimizing security threats. This includes preparing employees by creating scenarios and training them how to behave in such scenarios. Most common attacks like social engineering and phishing attacks are due to less understanding of modern technology and also unawareness of trending techniques used for utilizing these attacks. One of the main reasons behind the large amount victims being 60 plus is less awareness of modern technology and attacks.
2. Using machine learning algorithms and AI for defensive purposes can be done by training an AI model using a large dataset. The model would be able to effectively analyze the behavior of attacks and also create AI-based solutions that will play a pivotal role in preventing a system once an attack is detected. An example of an AI defense system is SentineIone, a tool based on a machine learning algorithm that provides end-point security and can stop end-point attacks like ransomware and other malware attacks.
3. To minimize threats related to quantum computing there is a need for post-quantum cryptography which provides security by encryption that is not breakable by quantum computing algorithms. There is also a need for quantum key distribution which is based on the principle of quantum mechanics for generating a secure key that is again immune to quantum brute force. If someone tries to eavesdrop the state of quantum is disturbed and warns the individual or parties involved. Being aware of new vulnerabilities is important to minimize quantum attacks this is possible through security assessment and networking with researchers. To have a complete picture of protection there is a need for an effective mitigation plan and updating software and hardware components is also important.
4. To have a secure 5G network there is a need for comprehensive security strategies from secure method of authentication and authorization to awareness of how to use and deal with the odd behavior of this technology. There is a need to communicate with various telecommunication provider and understand their point of view. For secure communication, there is a need to use protocols like transport layer security to ensure data security. To have a training and awareness program among all users is important to minimize threats like social engineering attacks as well.

7.3. Implications for Law Enforcement, Policy, and Public Awareness

Law enforcement agencies must play their role in reducing cybersecurity threats by enhancing their capabilities in investigating and training. Advanced technology should be used for digital forensics to have precise artifacts about data. Training can be improved by having awareness of new cyber crimes and effective measures to mitigate or take action against them.

Apart from technology, there is also a need for international collaboration, which is important for agencies of different countries to know steps taken by different countries for mitigation and also up to date with trending cybersecurity threats. To have complete action against cybercrime there is also need a for support of a legislative framework. Therefore, the policy and law enforcement agencies work together to safeguard the privacy of individuals by taking measures against cybercrime.

Policymakers should make cybersecurity guidelines, standards, and procedures that the organization should implement and make sure that these standards are correctly implemented within an organization. They need to promote the sharing of information and collaboration between countries and also with international partners. There is also a need for creating funds for security research, and cybersecurity education institutes so they can work on the latest technology without any financial issues. Sharing new attacks and vulnerabilities is essential for creating measures against them.

Public awareness is a crucial step to make society digitally secure, for this organizations and educational institutes must start campaigns to make the public aware this can be done by creating awareness in society the purpose of which is to alert people about cyber threats. The minimum target for public awareness programs should be to know about phishing attacks and preventive measures against these attacks. Everyone must be aware of secure online actions and also strong password strategies this will reduce cybersecurity attacks. The program can be advanced with time by including knowledge of technology like deep fakes and AI-generated attacks.

8. Conclusion

In the past two decades, the landscape of technology has taken a sharp turn. Which has also affected the whole cybersecurity landscape with new and more complex challenges. Such an evolution has proven to be a hurdle in maintaining international security and societal well-being. Our examinations and observations related to these trends with the aid of Council on Foreign Relations' data have underscored various dynamics within the domain.

Firstly, state-sponsored cybercrimes have marked an increase in both frequency and sophistication. These attacks have more wider reach now encapsulating not only the governments but also private businesses and infrastructures. These trends reflect a shift in both non-state and state-sponsored attacks. Secondly, the geographical distributions have also observed a swift turn with a more noticeable spread. While traditional peaks are constant, the emergence of new attackers has been observed lately. This spread elaborates and highlights the international nature of these cybersecurity trends and attacks which then underscores the need for global cooperation as well.

The impact of cybercrimes is not uniform and that can be observed from the gender disparity in cybersecurity. Victims of these cybercrimes range from young adults to senior citizens. Every age group faces different and unique threats and challenges. That highlights the need for proper awareness for every respective age group. Temporal patterns and peaks of attacks and scams are different. By understanding such peaks and trends security researchers and policymakers can make more robust and proactive defensive measures to safeguard our digital assets.

As we look to the future, it is clear that the fight against cyber threats will require constant vigilance and adaptation. This paper aims to provide insights into an ongoing evolution in both technology and state-sponsored cyberattacks. To navigate and safeguard our digital presence everyone should remain vigilant and resilient in their approach to cybersecurity.

Funding: Not applicable.

Data Availability Statement: Data is contained within the article or supplementary material.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Full Form
AI	Artificial Intelligence
APTs	Advanced Persistent Threats
CIIP	Critical Infrastructure Protection
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
IC3	Internet Crime Complaint Center
IoT	Internet of Things
NERC	North American Electric Reliability Corporation
PNN	Probabilistic Neural Network
ROI	Return on Investment
RaaS	Ransomware as a Service
SCADA	Supervisory Control and Data Acquisition
URL	Uniform Resource Locator
PII	Personally Identifiable Information
CFR	Council on Foreign Relations

References

1. of Investigation, F.B. Internet Crime Report 2023, 2023. Accessed from the Federal Bureau of Investigation website.
2. Rajasekharaiah, K.; Dule, C.S.; Sudarshan, E. Cyber security challenges and its emerging trends on latest technologies. In Proceedings of the IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2020, Vol. 981, p. 022062.
3. Świątkowska, J. Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series* **2020**, *33*, 2020–01.
4. Muhammad, Z.; Anwar, Z.; Saleem, B.; Shahid, J. Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. *Energies* **2023**, *16*, 1113.
5. Fiaz, F.; Sajjad, S.M.; Iqbal, Z.; Yousaf, M.; Muhammad, Z. MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms. *Future Internet* **2024**, *16*, 176.
6. Oh, J. State-Sponsored Cyber Operations (2005-Present), 2023. https://doi.org/10.34740/KAGGLE/DSV/4956055.
7. Irfan, M.; Ali, S.T.; Ijlal, H.S.; Muhammad, Z.; Raza, S. Exploring The Synergistic Effects of Blockchain Integration with IOT and AI for Enhanced Transparency and Security in Global Supply Chains. *Int. J. Contemp. Issues Soc. Sci* **2024**, *3*, 1326–1338.
8. Muhammad, Z.; Anwar, Z.; Javed, A.R.; Saleem, B.; Abbas, S.; Gadekallu, T.R. Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. *Technologies* **2023**, *11*, 76.
9. Hoar, S.B. Trends in cybercrime: The dark side of the Internet. *Crim. Just.* **2005**, *20*, 4.
10. Dunn, M.; Mauer, V. Towards a Global Culture of Cyber-Security. *The International CIIP Handbook* **2006**, *2*, 189–206.
11. Sheng, S.; Chan, W.L.; Li, K.; Xianzhong, D.; Xiangjun, Z. Context information-based cyber security defense of protection system. *IEEE Transactions on Power Delivery* **2007**, *22*, 1477–1481.
12. Cárdenas, A.A.; Roosta, T.; Taban, G.; Sastry, S. Cyber security basic defenses and attack trends. *Homeland Security Technology Challenges* **2008**, pp. 73–101.
13. McCrohan, K.F.; Engel, K.; Harvey, J.W. Influence of awareness and training on cyber security. *Journal of Internet Commerce* **2010**, *9*, 23–41.
14. Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* **2010**, *40*, 853–865.
15. Lupovici, A. Cyber warfare and deterrence: Trends and challenges in research. *Military and Strategic Affairs* **2011**, *3*, 49–62.
16. Broadhurst, R.; Chang, L.Y. Cybercrime in Asia: trends and challenges. *Handbook of Asian criminology* **2012**, pp. 49–63.
17. Zareen, M.S.; Akhlaq, M.; Tariq, M.; Khalid, U. Cyber security challenges and wayforward for developing countries. In Proceedings of the 2013 2nd National Conference on Information Assurance (NCIA). IEEE, 2013, pp. 7–14.
18. Reddy, G.N.; Reddy, G. A study of cyber security challenges and its emerging trends on latest technologies. *arXiv preprint arXiv:1402.1842* **2014**.
19. Bendovschi, A. Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance* **2015**, *28*, 24–31. 7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015, 7th ICFC 2015, 13-14 April 2015,Wadham College, Oxford University, United Kingdom, https://doi.org/https://doi.org/10.1016/S2212-5671(15)01077-1.
20. Pescatore, J. Cyber security trends: Aiming ahead of the target to increase security in 2017. *SANS Institute InfoSec Reading Room* **2017**.
21. Osawa, J. The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review* **2017**, *24*, 113–131, [https://doi.org/10.1080/13439006.2017.1406703]. https://doi.org/10.1080/13439006.2017.1406703.
22. Cabaj, K.; Kotulski, Z.; Księżopolski, B.; Mazurczyk, W. Cybersecurity: trends, issues, and challenges, 2018.
23. Ali, M.L.; Thakur, K.; Atobatele, B. Challenges of Cyber Security and the Emerging Trends. In Proceedings of the Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, New York, NY, USA, 2019; BSCI '19, p. 107–112. https://doi.org/10.1145/3327960.3332393.

24. Rajasekharaiah, K.M.; Dule, C.S.; Sudarshan, E. Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering* **2020**, *981*, 022062. https://doi.org/10.1088/1757-899X/981/2/022062.
25. Dillon, R.; Lothian, P.; Grewal, S.; Pereira, D., Cyber Security: Evolving Threats in an Ever Changing World. In *Digital Transformation in a Post-Covid World: Sustainable Innovation, Disruption and Change*; Kuah, A.; Dillon, R., Eds.; CRC Press, 2021; pp. 129–154.
26. Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences* **2022**, *34*, 5766–5781. https://doi.org/https://doi.org/10.1016/j.jksuci.2021.01.018.
27. Stafiniak, M.; Wodo, W. State-sponsored Cybersecurity Attacks. In Proceedings of the 2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IEEE, 2022, pp. 1–6.
28. Durojaye, H.; Raji, O. Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. *arXiv* **2022**, *2212.08036*, [2212.08036]. Submitted on 13 Dec 2022.
29. AZUBUIKE, C.F. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. *Nnamdi Azikiwe Journal of Political Science* **2023**, *8*, 101–114.
30. Fadziso, T.; Thaduri, U.R.; Dekkati, S.; Ballamudi, V.; Desamsetti, H. Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat **2023**. *3*, 1–12. https://doi.org/10.6084/m9.figshare.24189921.v1.
31. Wisnioski, M.H. *Engineers for change: Competing visions of technology in 1960s America*; Mit Press, 2012.
32. Hauben, M. History of ARPANET. *Site de l'Instituto Superior de Engenharia do Porto* **2007**, *17*, 1–20.
33. Saltzer, J.H.; Schroeder, M.D. The Protection of Information in Computer Systems. *Proceedings of the IEEE* **1975**, *63*, 1278–1308. https://doi.org/10.1109/PROC.1975.9939.
34. Zhang, L. A new architecture for packet switching network protocols. PhD thesis, Massachusetts Institute of Technology, 1989.
35. de Jong, B. The KGB in Eastern Europe during the Cold War: on agents and confidential contacts. *Journal of Intelligence History* **2005**, *5*, 85–103.
36. Lemenager, T.; Neissner, M.; Koopmann, A.; Reinhard, I.; Georgiadou, E.; Müller, A.; Kiefer, F.; Hillemacher, T. COVID-19 lockdown restrictions and online media consumption in Germany. *International journal of environmental research and public health* **2021**, *18*, 14.
37. Arshad, J.; Talha, M.; Saleem, B.; Shah, Z.; Zaman, H.; Muhammad, Z. A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry. *Blockchains* **2024**, *2*, 195–216.
38. Fitzpatrick, S.; Ramgopal, K. Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says. *NBC News*. Archived from the original on 5 December 2022. Retrieved 5 December 2022.
39. Fayi, S.Y.A. What Petya/NotPetya ransomware is and what its remidiations are. In Proceedings of the Information technology-new generations: 15th international conference on information technology. Springer, 2018, pp. 93–100.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.