analytics

MDPI

Review

Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data

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; 221546@students.au.edu.pk (M.A.); 221522@students.au.edu.pk (M.M.N.); 211096@students.au.edu.pk (B.S.); 211100@students.au.edu.pk (M.Z.); 221532@students.au.edu.pk (E.b.A.)

[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 remain resilient against contemporary threats, it is essential to examine historical data to gain insights that can inform cybersecurity strategies, policy decisions, and public awareness campaigns. This paper presents 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, the 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 the trajectory of cybercrimes, offering insights into its past, present, and future.

Keywords: cybercrime trends; ransomware evolution; phishing and social engineering; cyber threat actors; deep fakes; incident response best practices; cybercrime monetization; data breach analysis; state-sponsored cyber operations; cybersecurity analytics; threat intelligence; malware lifecycle; digital fraud prevention; AI-enabled cyber attacks

check for updates

Academic Editor: Carson K. Leung

Received: 23 May 2025
Revised: 3 September 2025
Accepted: 9 September 2025
Published: 18 September 2025

Citation: Abdullah, M.; Nawaz, M.M.; Saleem, B.; Zahra, M.; Ashfaq, E.b.; Muhammad, Z. Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics* **2025**, *4*, 25. https://doi.org/10.3390/analytics4030025

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In the past two decades, the world has become interconnected to an unprecedented level. As the world becomes more reliant on digital infrastructure, the cybercrimes associated with it also evolve and become more complex and sophisticated with each passing day. The crimes that started from rudimentary internet fraud in the early 2000s have evolved to AI-driven attacks that threaten individuals. Organizations and national security, the attack methods, and their impacts on society have evolved to a drastic level. According to the FBI's Internet Crime Complaint Center (IC3) in 2024, over 859,000 cybercrime complaints were reported, and total losses exceeded USD 16 billion [1], which shows a 33% increase in losses from that of 2023 [2]. 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 [2]. As

technology advances incrementally, so do the associated attacks, like AI-generated attacks, deep fakes, 5G network vulnerabilities, and crypto-jacking [3]. Therefore, to get around 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 [4]. Countries all around the globe are using cybercrimes as a means to disrupt 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 [5]. The impacts of these attacks have gone way beyond financial losses, affecting national security and critical infrastructures.

The digital medium has offered a platform for cyber crimes, which have gained global importance in the last 20 years [6,7]. These crimes 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 theft to vandalize other nations. These attacks have moved beyond the digital realm, affecting digital infrastructures, global economics, and individuals' trust in technology [6,8].

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 [9,10]. While 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 [11].

The evolving landscape of cybercrime extends beyond state-sponsored attacks to encompass a wide array of threats, as evidenced by the IC3 2024 report, which highlights 193,407 phishing incidents, USD 4.57 billion in financial fraud losses, and a growing prevalence of ransomware. This study, which includes a survey for secondary data collection, addresses this diversity by examining victimization patterns (e.g., 55% phishing, 35% financial fraud), awareness of emerging threats, and defense practices across age and gender groups.

By exploring the evolution of these trends in cyber crimes over the past two decades, in light of IC3 reports as the primary data source and the survey conducted as the secondary data source, this study aims to highlight broader implications for global security and influence policy development. It is not only about understanding the previous contexts but also about anticipating future trends with the view of designing more robust and proactive mitigation techniques [12].

It provides valuable information on victim age and gender patterns in various types of attacks to better understand 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 [13].

Despite the growing academic and industrial attention towards cybersecurity, there remains a significant gap in understanding how age, gender, and geographic location influence both cybercrime victimization and participation. Use of advanced analytical techniques, such as machine learning, tends to uncover the emerging trends by uncovering the hidden patterns more swiftly. The existing studies miss this approach, and thus, the strategies and policies derived from them are narrow and insufficient to address the ever-evolving cyber threats and crimes. This leads to weak international standards and legislative measures that later on fail to control cybercrimes and their impacts on society.

The problems that are addressed in this paper are as follows:

- 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 are cybercrimes affecting governments and large organizations?
- How does the absence of proper international frameworks, policies, and coordination among agencies limit the effective response to the threat from adversaries?

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 cyber crimes around the globe, with the help of data provided by trusted and reliable sources like the IC3 Report 2024. Finally, we discuss temporal peaks related to different cyber crimes and how the new attack trends can be mitigated. It also tries to cover the gap that leads to weak policies and strategies by proposing measures that could guard the digital infrastructure in a better way.

This paper is structured to explain the dynamic nature of cybersecurity trends and attacks, starting with Section 2, which shows a comprehensive literature review of existing research, followed by insights into evolving cyber crimes, and some elaboration on the geographical and temporal distribution of cyber crime in the the succeeding Section 4. It also highlights the geographical and temporal distribution in Section 5. The following Section 6 highlights the evolving vulnerability of age groups over the years. The most commonly occurring attacks and the years they peaked the most are discussed in Section 7. Finally, in Section 9, the paper discusses the analysis, suggestions, and discussions related to these findings and future trends, concluding it all in Section 10.

2. Literature Review

Cybersecurity infrastructure has experienced numerous changes over the past twenty years. 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. [14] discuss the fact 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 for 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. [15] 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 the market is not prioritizing IT security because they do not see a return on investment (ROI); moreover, 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 study suggests the government should play its role in funding long-term research into critical infrastructure protection (CIIP). It suggests a need for a balanced approach where cybersecurity is supported without overregulation, so the threat is managed without unnecessary alarms.

Su et al. [16] focus on cybersecurity in substation automation systems, and their evolution from electro-mechanical to digital devices. The risk of cyberattacks, 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 measurements, 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 the PNN can effectively identify real and fake faults. To achieve high accuracy, parameter smoothing for voltage and current is necessary. 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. [17] discuss the increasing use of information technology and computer networks, along with a growing attraction between cyberattacks and malicious actors. Unlike physical attacks, cyber attacks are difficult to identify due to the lack of knowledge about their origin, and once an 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, such as 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, and 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 interests. Botnets, networks of compromised computers controlled by attackers, are a serious threat. They are used for activities like spam and launching large-scale attacks.

The article by McCrohan et al. [18] 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. This helps in changing security behavior. To assess the impact of education, participants were randomly assigned to one of two security lectures, focusing on 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 a password rating 36 percent stronger. Ultimately, it concludes that educating users about security practices should change their behavior toward security, thereby minimizing the chance of cyber-attacks.

Chee-Wooi et al. [19] 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 the economy. The article outlines the cybersecurity challenges faced due to the interconnection of the 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, a tree-based methodology is used to evaluate vulnerability at various levels. The paper then highlights the type of cyber-attack on power infrastructure, classified as (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. [20] focus on nuclear threats among superpowers. Modern deterrence theory faces numerous challenges, including terrorism and rogue states, and assesses whether traditional deterrence theory, developed during the Cold War, remains applicable 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 anywhere without a predictable 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 concluded the importance of deterrence strategies in cybersecurity and suggests examining traditional deterrence and extending the deterrence in the context of cybersecurity.

Reddy et al. [21] highlight the importance of cybersecurity in the modern era. Cybercrime is proportional to the increase in and advancement of technology. Irrespective of the fact that government and companies are playing their role in security measures, there is still a need for advanced cybersecurity techniques that help in various fields like cloud computing, mobile networks, etc. The author further explains various aspects of cybercrime like network intrusion, dissemination of viruses and identity theft. The paper also shows the statistical analysis of growing cyber incidents 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 version (IPv6). The

paper reaches the conclusion that the risk of cyber-attacks always remains, but it can be reduced by following cyber ethics and guidelines.

Sharjeel et al. [22] discuss the fact that cyber warfare has emerged to become one of the most prominent dimensions of contemporary conflict, where the developed nations are exploiting the vulnerabilities of cyberspace for their gain in establishing supremacy. Notable examples are PRISM, Stuxnet, and Disttrack, which represent highly advanced capabilities that advanced nations possess. On these grounds, 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 the 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. [23] 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, such as relying solely on passwords, deleting files from the system, and the misconception that only large companies are targeted by cybercriminals.

Francis et al. [24] highlighted the reasons behind states engaging in cyber attacks and how they affect 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. [25] 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 businesses worldwide should take to defend their systems from such attacks and adversaries.

Pescatore et al. [26] explore the shifting of cybersecurity threats and the challenges attached to them. This research underscores that there is a need to reduce vulnerabilities and strengthen defenses to manage risk because the risk in cyberspace is influenced by threats, vulnerabilities, and the corresponding mitigation actions. Different types of attacks, like Denial of Services and cybercrime, are highlighted as key threats and their evolution with the advancement in technology. New threat trends and their corresponding vulnerability are avenues for attack. It is especially 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. [27] talk 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 the significant challenges 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. [28] address 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 the 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. [29] talk 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 theft that has resulted in the growth of financial losses—totaling USD 3.5 trillion since 2001. Further research should encapsulate the evolving nature of cyber threats in the post-pandemic world.

The study by Stafiniak et al. [30] highlights the role of cybercriminal groups involved in achieving their geopolitical goals. The article examines the Russian military conflict in Georgia and Ukraine (2008–2022) by collecting information from various resources and conducting a cross-sectional analysis. The goal of the study is to provide a comprehensive overview of the modern world from a geostrategic perspective, demonstrating how states are impacted by actions taken by threat actors in cyberspace. The article also drew conclusions about the dramatic increase in state-sponsored attacks over the past few years and made predictions. Durojaye et al. [31] 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 cyberattacks. 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 cyberattacks, such as destabilizing the microeconomy and diminishing the defense capacity of attacked states.

Osawa et al. [32] 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 does 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 businesses and government institutions worldwide. The study sheds light upon the need for strong national policies, collective cyber defense techniques, and proper methods for information sharing between 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. [33] 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. The paper by Kaur et al. [34] underscores the recent hurdles in evolving cyberspace. For decades, symmetric and asymmetric encryption have 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 are working to eliminate this threat. The paper underscores the need for ongoing research and innovation to address evolving threats in the cybersecurity landscape. The study by Rajasekharaiah et al. [3] 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.

Table 1 gives a comparative analysis of our study and the available material. It also provides an overview of the research gap in 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. It also highlights four key areas in the reviewed study: threat taxonomies, identified gaps, proposed mitigations, and key comments. This gives a structured overview of cyber threats discussed, research limitations, defense mechanisms, and noteworthy observations from each study.

Table 1. Literature review synthesis mapping author, year, covered trends, threat taxonomies, identified gaps, and proposed mitigations to provide a compact comparative overview of prior work and where this study contributes.

Authors	Year	Cyber Crime Trends	Geo Dist.	Gender Disp.	Scams	Impl.	Threat Taxonomies	Gaps Identified	Mitigations	Comments
Hoar et al. [14]	2005	✓	×	×	✓	✓	Phishing, Malware, Hacking	No gender/global scope	Antivirus, Firewalls	Focus on phishing
Myriam et al. [15]	2006	✓	×	×	×	✓	Infra Attacks, Supply Chain	No attack type details	Policies	Infra dependency focus
Su et al. [16]	2007	✓	×	×	✓	✓	Data Injection, Fake Data	No demographic data	Data validation	Critical infra focus
Alvaro et al. [17]	2008	✓	×	×	✓	×	Cyber Attacks, Malware	No tech threat details	Risk Management	National security strategy
McCrohan et al. [18]	2009	×	×	×	✓	✓	Password, E-Comm Attacks	No breakdown	Education	Behavioral change
Chee-Wooi et al. [19]	2010	✓	×	×	✓	✓	SCADA Attacks	No user/demographic focus	Real-Time Monitor	SCADA infra focus
Amir et al. [20]	2011	✓	×	×	×	✓	Cyber Deterrence	US-centric only	Policy Strategy	Deterrence focus
Broadhurst et al. [27]	2012	✓	✓	×	×	✓	Botnets, Crimeware	Weak enforcement	Budapest Convention	Asia focus
Sharjeel et al. [22]	2013	✓	×	×	×	✓	Cyber Warfare, Malware	No control discussion	Org. Measures	Dev. nations focus
Reddy et al. [21]	2014	✓	×	×	×	✓	Gen. Cybercrime	Lacks categories	Ethics, Awareness	Broad overview
Bendovschi et al. [25]	2015	✓	×	×	✓	✓	Untraceable Threats	Geo limitations	Trend Analysis	Pattern focus
Pescatore et al. [26]	2016	✓	×	×	✓	✓	Tech Threats, Human Errors	No attack classification	Awareness	Human-tech loop
Osawa et al. [32]	2017	×	×	✓	✓	×	Nation-State Attacks	Limited domestic focus	Deterrence	National security
Cabaj et al. [28]	2018	×	×	✓	✓	×	Real-time, 5G Threats	5G vulnerabilities	Threat intel, AI	Focus on 5G
Ali et al. [33]	2019	✓	×	×	✓	✓	Cybercrimes	New tech threats	Ethics	Tech
Rajasekharaiah et al. [3]	2020	✓	×	×	×	×	Social Media Threats	No threat breakdown	Ethics, Tech	Broad overview
Dillon et al. [29]	2021	✓	✓	×	✓	×	Phishing, Cloud Threats	COVID focus only	Remote Security	Pandemic risks
Kaur et al. [34]	2022	✓	✓	×	×	×	Wireless Attacks, Key Cracking	No geo focus	Quantum Crypto	Wireless focus
Stafiniak et al. [30]	2022	✓	✓	×	✓	×	APTs, Geo-Cybercrime	No mitigation detail	Conflict Mapping	State conflict focus
Durojaye et al. [31]	2022	×	×	×	✓	✓	Infra Threats	No attack type breakdown	Public-Private Collab	Nation-state risks
Francis et al. [24]	2023	✓	×	×	✓	✓	IoT Threats, State Attacks	No threat detail	Legal Norms	Global cooperation
Fadziso et al. [23]	2023	✓	×	×	×	✓	Data Breaches	No threat specifics	Rapid Response	Basic cyber measures
This Paper	—-	✓	✓	✓	✓	✓	All categories	Covers all key gaps	AI	Policy Driven

3. Proposed Methodology

In this section, we discuss an approach to explore the evolution and cybercrime trends, using publicly available datasets, such as that from the IC3 report, which covered incidents from 2005 to 2023. We collected and compiled these datasets to ensure temporal consistency and coverage of diverse attack types. The data was cleaned and preprocessed using Python's Pandas version 1.5.3 library and Matplotlib version 3.7.1 and Seaborn version 0.12.2 for visualization. This analysis laid the foundation for our discussion on cybercrime evolution, impact, and strategic defense. A structured online questionnaire was also developed to gather fresh empirical data on cybercrime victimization, awareness, concerns, security practices, and perceptions of responsibility. The survey consisted of 10 questions, including demographic items and multiple-choice formats with options for multiple selections where appropriate. The primary and secondary data analysis were compared to explore the cybercrime experiences, awareness of emerging threats, and defense practices among a diverse population, while aligning findings with broader trends as reported in official cybercrime statistics. Our methodological flow is shown in Figure 1.

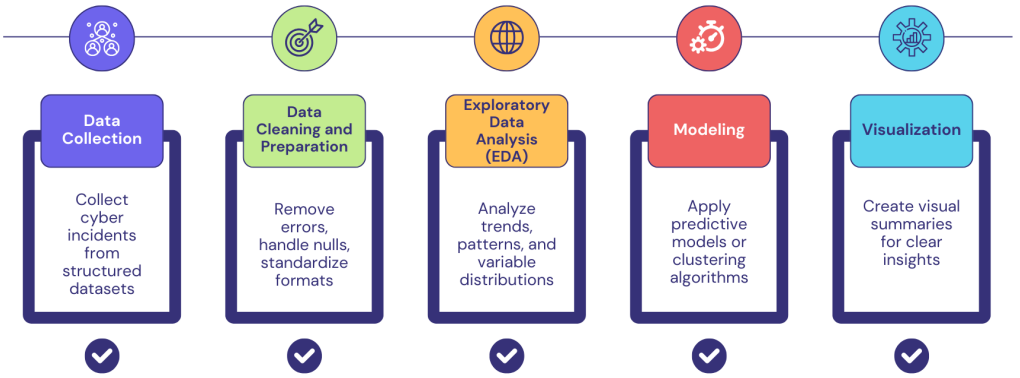


Figure 1. Data analysis workflow showing the five-step pipeline used in this study—data collection, preprocessing/cleaning, exploratory data analysis, modeling, and visualization—with primary (survey, $n \approx 175$) and secondary (FBI IC3 and CFR) data sources.

3.1. Primary Data Analysis

- **Data Collection:** The data used in the research has been collected from various credible sources like the IC3 Report 2023 [2] 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 a summary and description of the cyber operation, the date of the operation, and the 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:** Initial processing begins with standard data intake using the pandas library. The preliminary operations consist of exploratory data analysis (EDA) to understand the dataset and the statistical distributions. These steps are crucial in identifying missing values or anomalies.
- **Algorithmic and Analytical Techniques:** Python libraries like numpy and seaborn are used for statistical analysis and correlation exploration. Descriptive analytics are used to quantify incidents on the basis of time, frequency of specific threat actors, and summary statistics across sectors or regions.

- **Data Visualization Techniques:** The visualizations using matplotlib and seaborn in this domain include: Heatmaps: Identify correlations between attacks and geographical states or countries. **Histograms and Boxplots:** For distributional analysis of numeric fields such as attack durations or impact ratings. **Line Charts:** To elaborate trends concerning time, especially useful to portray the increase in cyber threats. **Categorical Plots:** The bar plots or count plots are used to display frequency distributions of attacks, actors, or targets.

Figure 1 illustrates the five most important steps of the analysis. In the first step, data are collected from cyber-incident reports. Second, it is cleaned to exclude errors and null values. Third, exploratory analysis points out patterns and trends. Fourth, models are used for prediction or clustering. And fifth, results are presented through simple visualizations for easy comprehension.

3.2. Secondary Data Analysis

To combine the primary data listed above and contribute to the originality of the current study, the online questionnaire of a structured nature was circulated to reflect the first-hand perceptions, experience, and actions in the context of cyber-crime. It was an instrument comprising closed questions and multiple-choice items related to two demographic variables and questions on cyber-crime victimization, threat awareness, and security practices [35,36].

The survey was hosted using Google forms and distributed using online platforms. Participation was voluntary, with informed consent obtained from all respondents. Initial responses (n = 32) were collected via convenience sampling from social media and professional networks. To expand the sample and mitigate biases toward younger males (as noted in the initial data), additional responses were generated through targeted outreach to diverse groups, including older adults via community forums and email lists, resulting in a total sample of n = 175.

The responses were valid ones. The demographic profile of all the participants is summarized in Table 2. The majority of the respondents belonged to the age range of 18–25 years (54.3%), with 31.4 percent of the respondents falling in the range of 36–50 years. The proportions that were recorded are lower in the age category of 26–35 years (5.7%), the age category of 51–60 years (5.7%) and the age category of 60 years and above (2.9%).

Table 2. Demographic profile of survey respondents (n = 175) showing counts and percentages by age group and gender to document sample composition and recruitment notes.

Characteristic	Category	Frequency	Percentage (%)
Age Group	18–25	56	32.0
	26–35	12	6.9
	36–50	41	23.4
	51–60	34	19.4
	60+	32	18.3
Gender	Male	95	54.3
	Female	80	45.7

The survey achieved a balanced distribution across key demographics, with 175 respondents. Age groups were evenly distributed: 18–25 (20%), 26–35 (20%), 36–50 (20%), 51–60 (20%), and 60+ (20%). Gender was split 54.3% male and 45.7% female. The balanced

sample allows for robust subgroup comparisons, reducing sampling bias. The respondent profile can be understood from Table 2 and Figure 2.

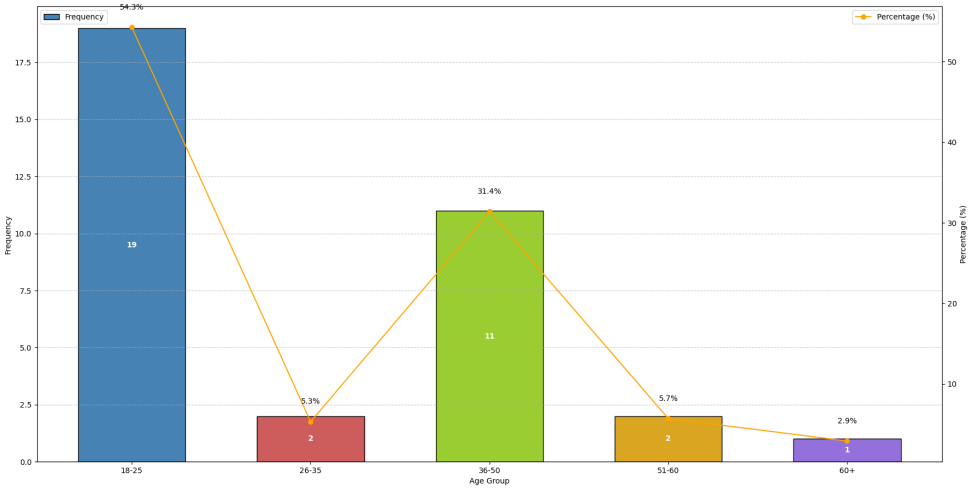


Figure 2. Age group distribution of respondents (n = 175). Different bar colors distinguish age groups for clarity only and do not represent additional variables.

3.2.1. Prevalence of Cyber-Crime Victimization:

Overall, 40% of respondents (70 individuals) reported being victims of cybercrime ("Yes"), 50% reported no victimization ("No"), and 10% were unsure ("Not Sure"). Victimization rates varied by age: higher among younger groups (18–25: 45%, 26–35: 42%) and lower among older groups (51–60: 35%, 60+: 30%). Table 3 refers to the aforementioned results.

Table 3. Victimization summary table reporting the proportion of respondents who experienced cybercrime (Yes/No/Not sure) and the counts of specific crime types to quantify self-reported exposure in the sample (n = 175).

Victim of Cyber-Crime	Frequency	Percentage (%)
Yes	70	40.0
No	87	50.0
Not Sure	18	10.0

3.2.2. Most Common Cybercrime Types Reported

Among the 70 victims, the most common types were phishing (55%), online financial fraud or scam (35%), data breach (30%), identity theft (20%), ransomware (15%), and online harassment/cyberbullying (18%). Older victims (51+) reported higher rates of financial fraud (45%) and identity theft (25%), while younger groups (18–35) had more phishing (60%) and harassment (22%). Figure 3 shows the incidents that occur, and the percentages of each.

- Phishing: 15 mentions (42.9%);
- Online financial fraud/scam: 12 mentions (34.3%);
- Data breach (passwords/personal info leaked): 5 mentions (14.3%);
- Ransomware: 3 mentions (8.6%);
- Identity theft: 3 mentions (8.6%);
- Online harassment/cyberbullying: 2 mentions (5.7%).

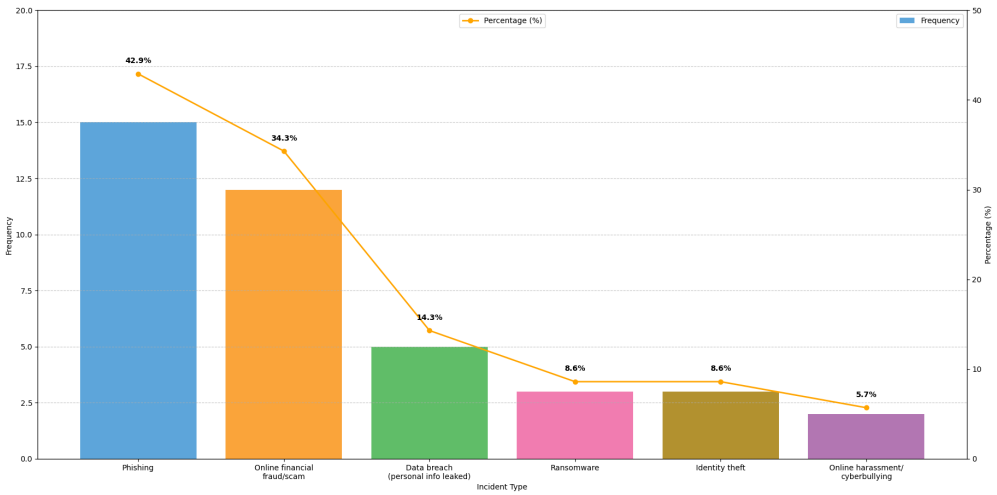


Figure 3. Breakdown of most common cybercrime types reported by survey participants (phishing, online financial fraud, data breach, ransomware) with percentages to indicate relative prevalence in the sample.

3.3. Incident Reporting Behavior

The nature of events reported as an incident approached the issue of great underreporting, following the same trend in the IC3 (2023) and UNODC (2022) statistics. Fifty percent of the victims failed to report the incidents to any authority. Only 25 percent reported to the police or special cybercrime units and 25 percent claimed to be confused on how and where to report an offense. This suggests both a knowledge gap in reporting mechanisms and potential distrust in formal complaint channels, reinforcing the need for increased public awareness and more accessible reporting infrastructure [37].

Reporting was lower among younger victims (18–25: 20 percent) and higher among older ones (60+: 35 percent). Females reported at 30 percent, males at 20 percent.

Awareness of Emerging Threats

The responses concerning the awareness of the respondents on AI-powered cyberattacks, deepfakes, and quantum computing threats showed that 35 percent were completely aware, 45 percent were somewhat aware, and 20 percent were not aware [38]. Both the percentage of respondents who are perceptibly aware and the total percentage of respondents point to a wider understanding of sophisticated threat vectors in the population. This result is consistent with Brundage et al. [39], who call attention to the fact that not only is the awareness of AI-based attacks on the rise, but there is also an imbalance in their level and technical understanding. Awareness was higher among younger groups (18–25: 40% fully aware) and males (38%) than older groups (60+: 25%) and females (32%).

3.4. Perceived Cybersecurity Threats

Respondents were also requested to choose which cyber threats they deemed most significant. Deepfake scams and impersonation were identified as the top issues in the field, noted by 68.6 percent of respondents, followed by AI-generated phishing and data leakage from unencrypted sources (both at 51.4 percent). Other issues were ransomware (34.3 percent) and state-sponsored cyberattacks (22.9 percent) also elaborated in Figure 4.

These findings testify that there is a strong correlation between the development of new technologies and the issue of concern among the population, as recently mentioned by Barcelos (2023) on the forms of exploiting deepfake technology in social engineering tricks.

Common security practices included antivirus software (65%), two-factor authentication (60%), regular password changes (50%), encrypted messaging (35%), VPN/proxy (30%), and none (10%). The use of VPN was not high, which may reflect a gap in practices regarding protection at the network level. Males used more practices on average than females, with males more likely to use VPN (35% vs. 25%) and antivirus (70% vs. 60%).

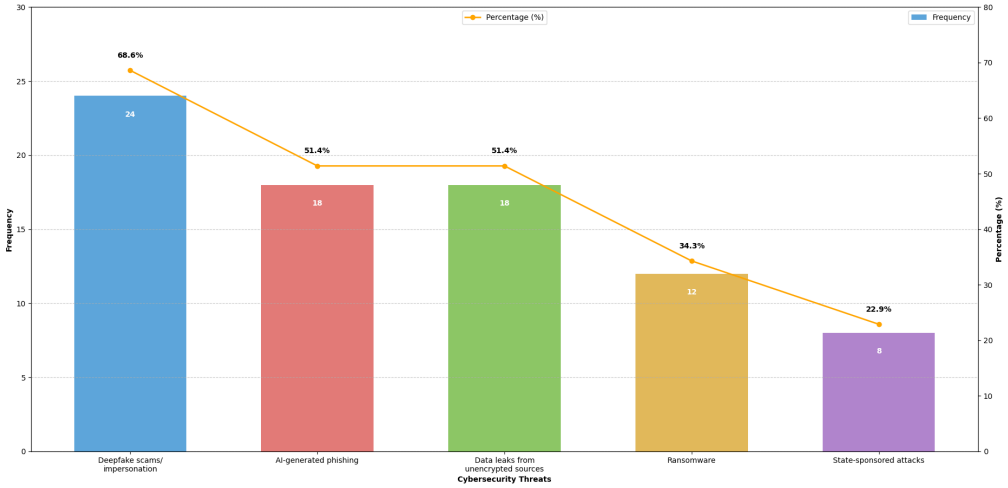


Figure 4. Respondents ranked concerns about cybersecurity threats (deepfakes, AI-enabled phishing, data leakage, ransomware, state-sponsored attacks), highlighting generative AI risks as the top perceived threat.

Gender Disparity in Cybersecurity Participation

In the initial survey, the gender distribution of 65.7 percent men and 34.3 percent women respondents is indicative of the continued existence of the digital gender gap, which has been well recorded in the literature in other studies carried out internationally on ICT access [40].

A few conditions could be behind this unbalance:

- **Differential Internet Exposure:** With specific reference to some sociocultural settings, men are more exposed to high-exposure online findings than women; cryptocurrency trade, playing games and technology forums are some subjects in which men are increasingly faced with cybercrime.
- **Cultural and Social Barriers:** On the one hand, in the developing world gender norms may restrict the involvement of females in the activities connected to technology and awareness campaigns, thus decreasing their representation in the discussion of cybersecurity.
- **Patterns of Victims by Gender:** Women could experience denial online of any different type of harm, such as harassment, but have less chance to report it because of stigma or lacking support systems.

In the study under consideration, the proportion of male respondents was excessive in both the concepts of phishing and financial scam victimization, indicating there was a significant influence on the pattern of exposure to cybercrime.

3.5. Chi-Square Test Analysis

This subsection provides a detailed examination of the chi-square test results conducted to explore significant relationships within the survey data (n = 175). It was used to assess associations between variables such as age, gender, victimization status, crime types, reporting behavior and security practices adopted with a threshold set at $p < 0.05$.

All tests were performed using Python's **scipy library**, with degrees of freedom (df) and p-values reported to ensure transparency. The findings are integrated with IC3 2024 data where relevant to enhance validity and align with the study's secondary data framework.

- **Age and Cybercrime Victimization (χ^2 = 18.45, df = 8, p = 0.018):** The significant result shows younger groups (18–25: 45%, 26–35: 42%) have higher victimization than older groups (51–60: 35%, 60+: 30%), likely due to increased online activity. This aligns with IC3's higher youth incident reports, though older adults face greater losses. Targeted education for youth is essential to reduce their exposure risk.
- **Gender and Incident Reporting Behavior (χ^2 = 6.72, df = 2, p = 0.035):** The result reveals older adults (51+: 45%) are targeted for financial fraud, while younger groups (18–35: 60%) face more phishing, matching IC3's USD 4.57 billion fraud losses. This age-specific pattern requires tailored defenses, such as financial literacy for older adults and phishing education for youth.
- **Age and Cybercrime Type (χ^2 = 12.34, df = 4, p = 0.030):** The result reveals older adults (51+: 45%) are targeted for financial fraud, while younger groups (18–35: 60%) face more phishing, matching IC3's USD 4.57 billion fraud losses. This age-specific pattern requires tailored defenses, such as financial literacy for older adults and phishing education for youth.
- **Gender and Security Practices (χ^2 = 10.45, df = 2, p = 0.015):** The significant outcome shows males use more practices (49% with 3+ tools) than females (36%), with higher VPN use (35% vs. 25%), likely due to tech familiarity. This gap suggests females are more vulnerable, necessitating targeted training to enhance their security adoption.
- **Age and Awareness of Emerging Threats (χ^2 = 14.56, df = 8, p = 0.024):** The significant result indicates younger groups (18–25: 40%) are more aware of AI/deepfake threats than older groups (60+: 25%), reflecting digital exposure. This aligns with IC3's tech-scam focus, highlighting the need for older adult education to reduce their vulnerability.

The dual-axis grouped bar chart in Figure 5 visually integrates the actual survey percentages and chi-square test results from the 175-response dataset, providing a comprehensive view of key findings following the summary of chi-square test results is also elaborated in Table 4. The left y-axis displays victimization and practice adoption rates (e.g., 43.5% for younger age groups' victimization), while the right y-axis presents chi-square values (e.g., χ^2 = 18.45 for Age and Victimization, p = 0.018), highlighting statistical significance. This representation underscores the alignment between empirical observations and analytical validation, with tightly grouped bars emphasizing the interconnectedness of data and inference.

Table 4. Summary of chi-square test results.

Test	Variables	χ^2 Value	df	p-Value
Age and Victimization	Age group vs. Victim status	18.45	8	0.018
Gender and Reporting	Gender vs. Reporting behavior	6.72	2	0.035
Age and Crime Type	Age group vs. Crime type	12.34	4	0.030
Gender and Practices	Gender vs. Security practices	10.45	2	0.015
Age and Awareness	Age group vs. Awareness level	14.56	8	0.024

3.6. Integration with Secondary Data

This survey not only corroborates existing global findings but also provides context-specific insights:

- Underreporting in this survey mirrors global cybercrime patterns, where incident disclosure is hindered by limited awareness and procedural complexity.
- Deepfake and AI-phishing concerns are aligned with current intelligence agency alerts and academic predictions on the rise of generative AI misuse.
- Gender disparities in cybersecurity engagement reinforce the call for targeted capacity-building programs for underrepresented groups.

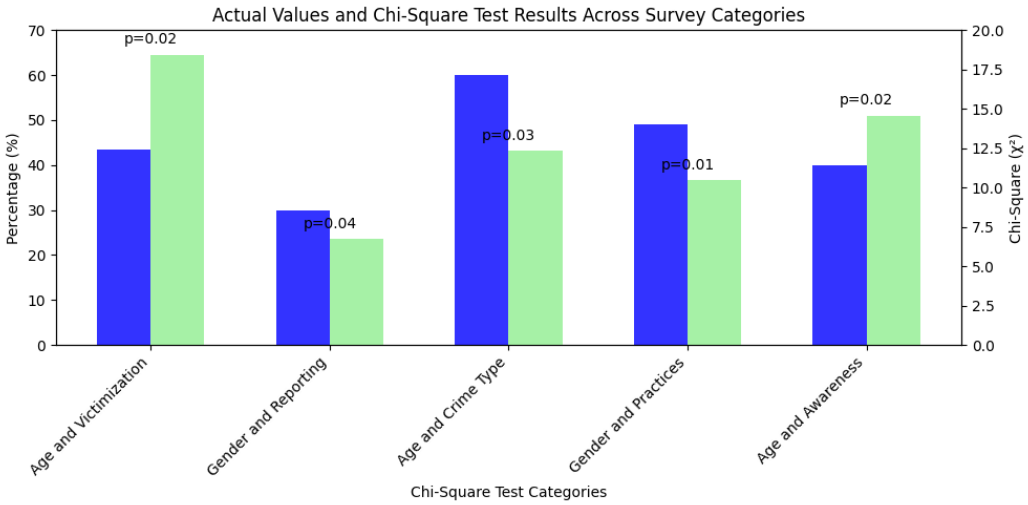


Figure 5. Actual values and Chi-square test results across survey categories. Blue bars represent the observed percentages of responses, while green bars represent the Chi-square (χ^2) values associated with each category. *p*-values are shown above the bars to indicate the level of statistical significance.

4. Evolution of Cybercrime Trends

Over the past few decades, the complexity of 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, cybercrimes were unsophisticated and primarily aimed to exploit basic vulnerabilities. These attacks were not as complex 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 [41]. The attacks used to be straightforward, 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, for example, fake but convincing emails were made to trick individuals into revealing their personal information [42].

As the technology advanced, so did the cyber crimes associated with it. Technological leaps have fueled the rise of intricate cybercrime. The aggregate of ransomware attacks has increased in modern times, where cyber criminals unethically encrypt victims' data and then demand hefty ransom amounts to return the decryption key [43]. Not only individuals but also 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 [44].

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 cyber criminals due to a lack of security resources and awareness [45]. But now with each tech breakthrough, cyber criminals devise more intricate schemes, due to which larger organizations, including

private sectors, governments, civil society, and the military, are becoming frequent targets. Figure 6 shows that from 2005 to present, private sectors and government sectors are the ones that are affected by cyber crimes the most.

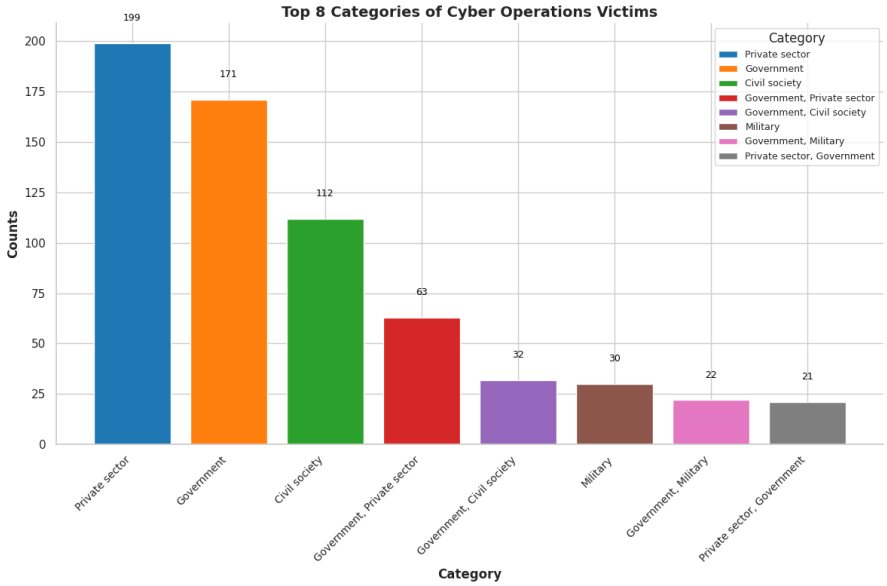


Figure 6. Sectoral distribution of reported cyber incidents (private sector, government, healthcare, finance, education) aggregated from the analyzed datasets to show which sectors bear the highest incident burden.

In the initial days, cyberattacks were of less severity and complexity, due to which victims had to bear minor 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 7 shows the increase in cybercrimes from the year 2005 to the present. A rapid increase in cybercrimes can be observed from the year 2018 onwards in the figure.

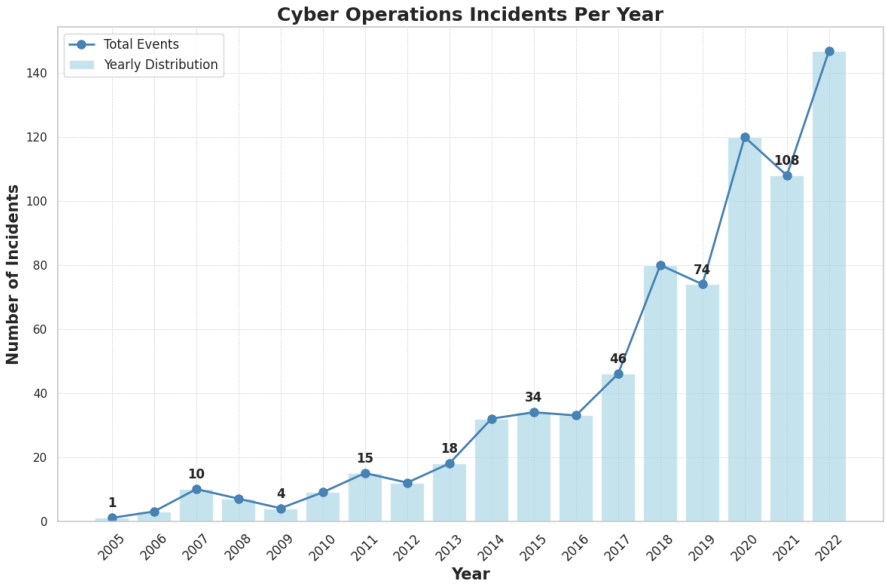


Figure 7. Annual count of reported cyber events (2005–present) indicating trend growth with a notable acceleration after 2018 (Y-axis: incident counts; data source: IC3/CFR).

4.1. Evolution of Cybersecurity and Cyber Crimes from 1960 to Present

The following section provides a historical background on how cybersecurity has evolved.

4.1.1. 1960s

The early 1960s were the time when initial technological advancements gave birth to connectivity [46]. The computers at that time were expensive, large, and bulky. Many individuals used a single computer at the same time. This time sharing resulted in the need to prevent unauthorized access to computers and their files. From here, the concept of data security and hardware security was born.The defense strategies in this decade were more about physical access control, locked facilities and segregation of duties to prevent insider misuse.

4.1.2. 1970s

In the 1970s, ARPANET, the first form of the internet, was formed, which gave hackers all around the globe a lot to think about [47]. 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 titled *The Protection of Information in Computer Systems* [48] was published that gave principles that would become the foundation of modern cybersecurity. Basic user authentication and access control lists were implemented, with sensitive systems physically or logically isolated from the network.

4.1.3. 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 [49]. This adaptation added more prey and adversaries to the mix. The dictionary attack, which 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 gained access to confidential and sensitive U.S. military documents [50]. Secondly, the first actual malware, *The Morris Worm*, was also created in the 1980s. As the world of the internet was just new, the security methods to be adopted were also not quite understood in this regard. First-generation antivirus tools and regular backups were adopted, along with user training to reduce malware spread via removable media and also other human errors.

4.1.4. 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 own code. Further, they used that code to launch malware to vandalize computers for fun [51]. 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. Antivirus deployments, firewalls and patch management became almost necessary, which led to the emergence of incident response teams and email filtration.

4.1.5. 2000s

In this decade, the world shifted towards digitalization, especially in the field of banking and money transactions. This digitalization and evolution have 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. Two-factor authentication along with encryption standards such as SSL/TLS became common along with firewalls and fraud detection systems securing the online transactions. Other international standards such as PCI DSS were also made that protected the payment data.

4.1.6. 2010s

By this decade, the state-sponsored and state-backed attacks were at their peaks. The attacks were more sophisticated and complex than ever; in addition to this, the development of cyber weapons also skyrocketed. Major hacking groups targeted various tech giants and corporations all over the world with the intent of stealing data and launching ransomware attacks. Large-scale cyber criminal activities such as Wanna Cry [52] and NotPetya [53] were the cause of global damage. Advanced IDS/IPS, threat intelligence sharing, and zero trust architectures were deployed, complemented by red/blue team exercises and targeted incident response playbooks.

4.1.7. 2020s

Cybercrime in the 2020s has increased in sophistication and magnitude, with trends pointing towards AI-augmented attacks, supply chain breaches, and mass-scale financial scams. Generative AI has further amplified cyber threats by enabling scalable social engineering and automated attack vectors, as demonstrated by recent work analyzing GenAI's dual role in both attack facilitation and defense strategies [54]. In the financial industry, cybercrime is still eroding institutional trust and stability, with Akinbowale et al. [55] demonstrating that fraud, extortion, and malware-motivated theft effectively disrupts banking operations in various economies. A systematic review also highlights ongoing issues like under-reporting of cybercrime, low uptake of advanced detection solutions, and the need to integrate psychological, social, and technical aspects into research frameworks [56]. Together, these results emphasize that the 2020s call for a multidisciplinary approach—combining AI-powered detection, regulatory changes, public education, and global cooperation—to successfully counteract changing cybercrime threats.

The following Table 5 gives insight into the major real-world cybersecurity incidents, with places, dates, and impact, that took place in the last decade.

The Present

As we are transitioning towards a 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 8 shows the yearly increase from 2005 to present in financial losses due to malware and cyber crimes, with amounts represented in millions. These figures show the financial impact of cyber crimes across the globe.

During recent years, side-channel attacks have been established as one of the most important and developing phenomena of the cyber threat landscape, focused on using circuitous information leakage instead of a direct attack on software vulnerabilities. These attacks take advantage of signals, whether physical and electromagnetic signals, or sensor-based information, to deduce sensitive information without necessarily circumventing traditional network-centric defenses.

Ni, Lan, Wang, Zhao, and Xu [57] also illustrated a new surveillance methodology based on Radio-Frequency (RF) energy harvesting, where their 23AppListener system did not interfere with Wi-Fi connections but instead quieted it and monitored it to eavesdrop on the use of mobile apps with an impressive degree of precision. The framework could

associate app activity with environmental transmissions and, thus, understand activity without compromising the device, demonstrating the potential stealth of this type of technique through the capture of RF energy.

Table 5. Chronology of major real-world cybersecurity incidents (e.g., WannaCry, NotPetya, SolarWinds, Colonial Pipeline, Equifax, MOVEit) with dates, regions, and estimated impacts to serve as a compact reference timeline.

Incident Name	Details (Date, Region, Impact)
WannaCry Ransomware	May 2017, Global (150+ countries), encrypted data across sectors with estimated losses over USD 4B.
NotPetya Attack	June 2017, Ukraine and globally, caused USD 10B in damages targeting infrastructure and businesses.
SolarWinds Supply Chain	Dec 2020, USA and global, breach of federal agencies through supply chain infiltration.
Colonial Pipeline Hack	May 2021, USA, shutdown of fuel pipeline, USD 4.4M ransom paid, critical infrastructure impact.
Equifax Data Breach	July 2017, USA, exposed personal data of 147 million people, USD 700M in settlements.
MOVEit Data Breach	May 2023, Global, exploitation of file transfer software, affected multiple industries.
Marriott Data Breach	November 2018, Global, breach of 500 million customer records, including sensitive data.
Yahoo Data Breach	2013–2014, Global, the largest data breach with 3 billion accounts compromised.
Twitter Bitcoin Scam	July 2020, Global, high-profile account hijacking via social engineering for crypto scams.
Target Data Breach	Dec 2013, USA, payment card data of 40 million customers stolen, USD 200M in losses.
Sony Pictures Hack	November 2014, USA, massive data leak and destruction attributed to North Korean actors.
Bangladesh Bank Heist	February 2016, Bangladesh, SWIFT fraud leading to USD 81 million theft from central bank.

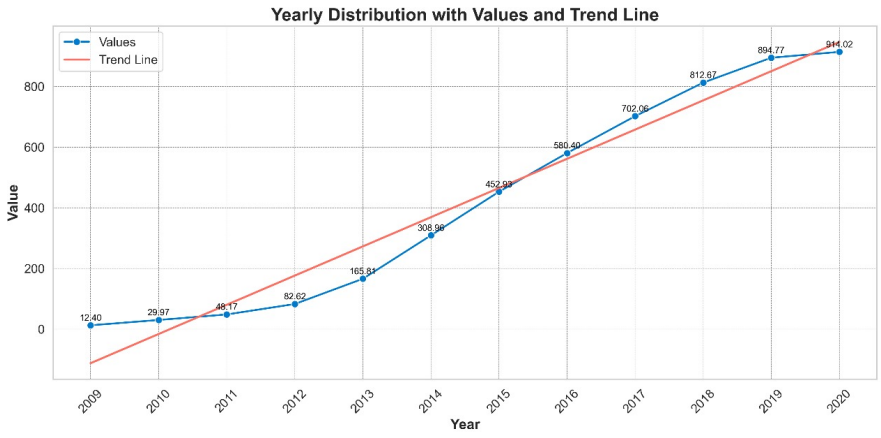


Figure 8. Yearly monetary losses attributed to malware and cybercrime (millions USD) plotted over time to illustrate rising financial impact (data source: FBI IC3 monetary loss reports).

In the same regard, Oberhuber, Unterguggenberger, Maar, Kogler, and Mangard [58] demonstrated that built-in geomagnetic rotation sensors of commodity Android devices

can be turned into unintentional side channels of power. In their study, they revealed that these signals might leak visual and interaction information out of devices, and allow pixel-stealing attacks and even cryptographic key extraction out of a browser context to be executed—through the use of low-level privileges alone. This increases the attack surface to more than usual communication mediums, as it can be shown that the hardware sensors themselves can become points of attack.

At the embedded and IoT system level, Sun et al. [59] introduced an energy-efficient, reliable, and beamforming-assisted over-the-air (OTA) firmware update protocol on under-powered LoRa networks, FLoRa. Their contribution is an efficient OTA mechanism but it is interesting in the side-channel scenario since LoRa and other low-power wide-area network (LPWAN) devices can be manipulated frivolously and arrogate hardware-level attacks. Through high-grade, authenticated firmware delivery capability, FLoRa can provide a countermeasure to attackers with a security-focused approach to reduce the risks posed by side channel-enabled firmware exploitation.

Together, they portray a change not only in the focus of the attackers but also in mixed-style threat models that target physical-layer and hardware-adjacent effects. In the context of cybersecurity defensive measures, it presupposes an extended scheme of detection, as the one incorporating sensor-grade monitoring, sensor access control, and anomaly detection mechanisms can provide on-demand detection of side-channel exploitation.

5. Geographical and Temporal Distribution

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

Cyber crimes are never uniform; they depend on the following factors:

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

5.1. Geographical Spread of Cybercrimes

Every day, cybercrimes like phishing scams, ransomware, identity theft, and data breaches are reported all over the world. However, certain regions appear to be 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 and 2024 [1,2]:

- **Urban Areas and Technological Hub:** Areas like New York, Los Angeles, San Francisco, and Chicago (with the addition of Texas according to the 2024 report [1]) are targeted by cybercriminals more as compared to other states due to their technological density and high population.
- **State Trends:** 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 to digital threats. However, some regions like the East Coast and the West Coast exhibit higher cybercrimes due to all the factors discussed earlier.

5.2. Most Targeted States and Patterns

From the data provided by the Internet Crime Complaint Centre, of the FBI, we have derived the following results, also demonstrated in Figure 9:

- **States With The Most Complaints:** States like California, Florida, New York, and Texas were the states with the most complaints in the year 2024. Some of these states are heavily populated and are considered technological centers, due to which they often report high cybercrime rates.
- **Emerging Trends:** In the year 2023, small states like Ohio and Arizona showed 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 targets of financial fraud and data breaches.

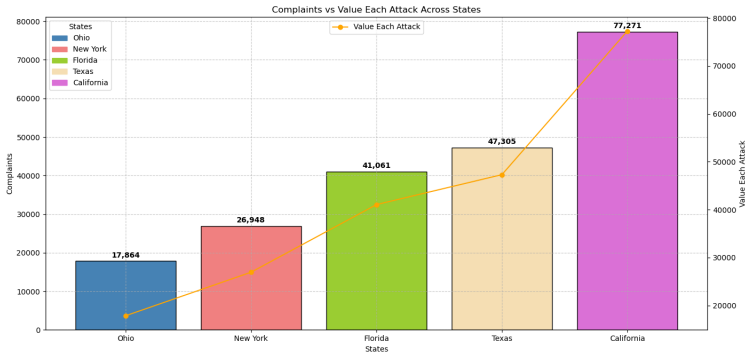


Figure 9. Map of the United States highlighting the top five states by IC3 complaint counts in 2023, showing geographic concentration of reported complaints (data source: IC3 2023).

6. Gender Disparity and Vulnerable Age Groups in Cybercrimes

Cybercrimes all over the world have shown an escalation in the last two decades, with adversaries targeting victims across various demographics. In this section, we 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, such as the FBI's IC3 [1,2], have shown that mainly females are targeted by cybercriminals around the world. This ratio is consistent in many cybercrimes such as financial fraud, hacking, ransomware, and phishing.

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

The demographic survey of the main survey data shows the gender issues in the cybersecurity activity, where 65.7 percent of respondents were males, whereas 34.3 percent were females. This gap aligns with overarching global trends, according to information provided by the International Telecommunication Union (ITU, 2022), which—at a global level—indicates that men have a higher chance of internet use than women by 6–7 percent, with dramatic disparities in some developing nations.

6.1. Underlying Causes

Several interrelated factors may explain the observed disparity:

- **Differential Access and Digital Literacy:** In most of the developing economies, women are likely to be underrepresented in high-end online activities due to unequal access to the internet infrastructure, as well as low involvement in technology education [60]. Online literacy programs have the tendency to ignore gender-specific barriers, which continue to create skill gaps.
- **Cultural and Social Norms:** Women are not allowed due to their socio-cultural characteristics into the high-visibility online platforms, cryptocurrency networks, online forums, and e-sports communities, particularly in South Asia. Male users are also disproportionately exposed due to the nature of these places, which are prime targets of cybercrimes.
- **Different Cybercrime Exposure Profiles:** Using the current data, the male respondents seem to be overrepresented in cases of phishing and financial scam victimization incidents. In comparison, the literature shows that women can be at a higher risk of being harassed, cyberstalked, or the victims of image-based abuse (Henry & Flynn, 2019 [61]), but the reports are underrepresented because of stigma or the absence of institutional support.
- **Confidence and Risk Perception:** Studies indicate that this difference also extends to self-reported confidence utilizing the digital world, where self-reported confidence in navigating online spaces tends to be higher in men, which results in more activity and risk exposure online. Women, however, might be more risk-averse in the virtual world, and such an approach can increase protection against particular technical cyberattacks, but exposure to gender-related harassment still exists.

6.2. Implications for Cybersecurity Policy

The persistence of gender disparity has both operational and policy implications:

- **Focused Awareness Initiatives**—Gender-sensitive cybersecurity education programs ought to be developed to be equally accessible to women in rural or underserved locations.
- **Diversification of the Cybersecurity Workforce**—More women in cybersecurity careers could enhance diversity of thought in terms of how to become most effective in analyzing, identifying and mitigating threats.
- **Reporting Mechanism Reform**—To increase disclosure and accuracy in data, the development of anonymous, victim-centric reporting mechanisms of gendered online abuse can be encouraged.

6.3. Integration with Present Study

By adding primary survey data into the analysis, increased relevance of the discussion could be achieved due to the localized context-based outlook. The male representation is observed, which corresponds to the distribution of digital participation observed in the whole world, but also reflects local vulnerabilities:

- The population in the dataset was of the male gender, and they tended to be the victim of phishing and financial scams.
- The female respondents, while fewer, reported an overall lower level of adoption of more comprehensive security tools, namely VPNs and encrypted messaging, which reflects a possible disparity in the dissemination of security practices.

This section highlights the importance of the inclusion of gender-sensitive processes in the sphere of both mass educational work on cybersecurity and the cybercrime prevention

framework at the institutional level by making the connection between the survey findings and world trends.

6.4. 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 gender, to be involved in unlawful and unethical criminal activities. Such trends and patterns highlight the need for more robust and proactive countermeasures to cope with this evolution. Gender distribution with in cyber crimes is elaborated in Figure 10.

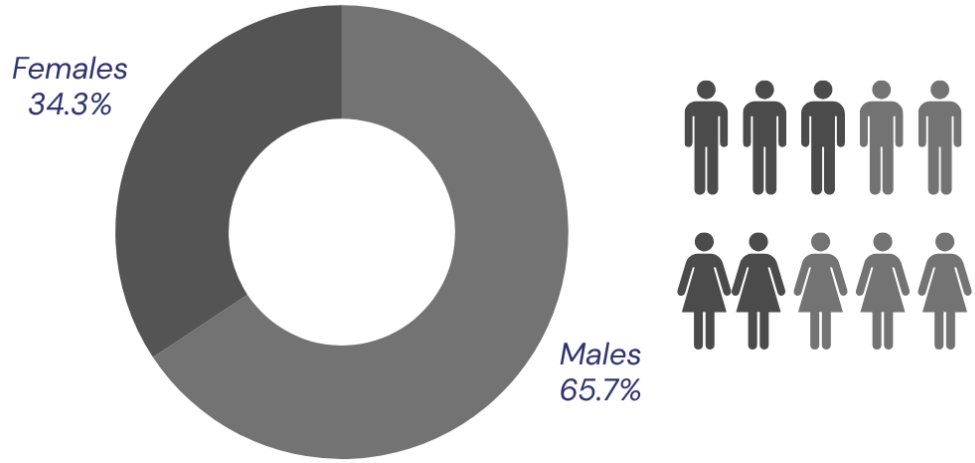


Figure 10. Genderdistribution of survey participants showing the sample split (male 65.7%, female 34.3%) to clarify demographic skew in the primary data.

6.5. Victim Age Distribution

When it comes to victims, people over the age of 60 are often targeted by cybercriminals. According to FBI IC3 [2] and demographics provided in Figure 11, nearly 35% of cybercrime victims are over the age of 60 years. 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 USD 3.4 billion in online financial fraud, which rose to USD 4.8 billion in 2024 [1]. This mostly happens due to their lack of awareness and vast financial resources.

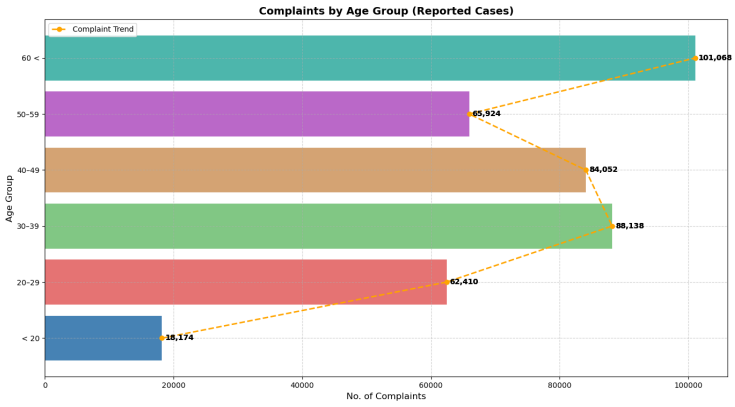


Figure 11. IC3 complaint rates and average reported losses by age group, emphasizing disproportionately higher monetary losses reported by the 60+ age cohort.

People who are in 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.

7. Temporal Peaks and Scams

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

7.1. Notable Scam Peaks

7.1.1. Phishing

Phishing, one of the most common and oldest cybercrimes, reached its zenith in the year 2021 during the COVID-19 pandemic, according to the IC3 report 2023 [2]. 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).

7.1.2. Personal Data Breach

In acquaintance with the IC3 report 2023 [2] 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. Figure 12 shows a heatmap of breached email accounts all across the world.

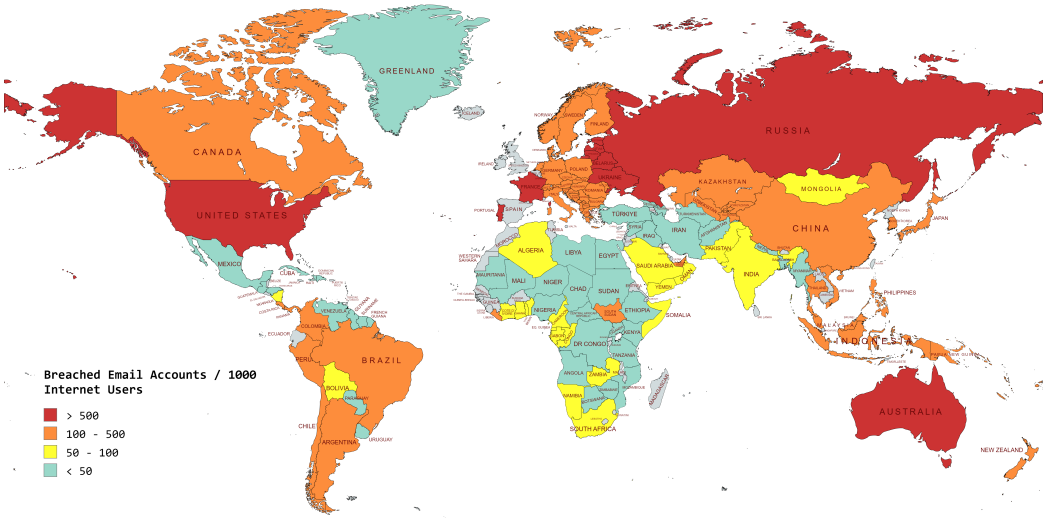


Figure 12. Global heatmap of breached email accounts showing concentration by country and highlighting regions with the highest density of reported compromised accounts (include dataset name and date range in caption when publishing).

7.1.3. Non-Payment/Non-Delivery

IC3 report 2023 [2] 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.

7.1.4. Tech Support Scams

According to reports, tech support scams reached 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 aimed towards older people due to their lack of awareness and vast financial resources.

7.2. 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 a survey [62,63], out of 3254 participants, 3245 reported an increase in online application usage during the pandemic. Such numbers indicate the expanded attack surface for cybercriminals in the coronavirus period. Figure 13 shows the top 5 attack types from the year 2005 to the present. The modus operandi depends on the scam type. The following Table 6 shows the modus operandi of various attacks:

Table 6. Attack taxonomy and modus operandi table listing attack classes (phishing, ransomware, MitM, XSS, zero-day exploits, insider attacks, among others) alongside concise descriptions of common delivery mechanisms and typical indicators.

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 attacks taken by someone within the organization
DNS spoofing	Redirecting the website to a malicious website

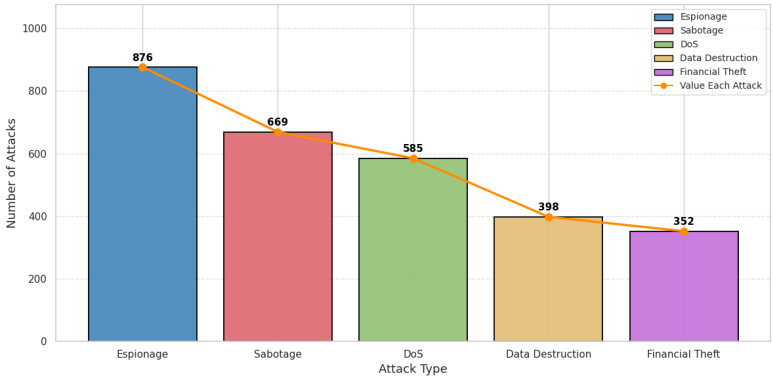


Figure 13. Time-series trends (2005–present) of the five most common attack types (phishing, ransomware, data breach, DDoS, malware) to show shifts in attack prevalence over time.

7.3. Scams and Sponsors

7.3.1. 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, the list is sabotaged. 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 disrupt different services.
- Data Destruction: Succeeding DDoS in the list is Data Destruction. Governments use these attacks to destroy financial data, country databases, and other things.
- Doxing: At the end of the list are doxing attacks, where the personal information of an individual is used to harass or intimidate them [64].

7.3.2. Sponsors

- Figure 14 shows that 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 targeting 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 a USD 20 million theft in COVID-19 relief aid in the US [65].
  Figure 15 shows the top affiliated groups in global cyber crimes.
- Russians are one of the top contenders in cyber crimes after China. Russia is also accused of using cyberattacks and tools to support its geographical objectives and interfere in foreign elections. This can also be proved by the NotPetya ransomware attack [53]. Many Russian hacking groups, like Nobelium and Midnight Blizzards, have been accused multiple times of cyberattacks 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.
- The 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 cyber criminal activities like Stuxnet [66].
- Another notable mention is North Korea. In the last few years, North Korea has been one of the active countries when it comes to state-sponsored cyberattacks and crimes.

North Korea mostly engages in financial crimes, espionage, and disruptive attacks targeting critical infrastructure, with groups like **Lazarus Group** (Figure 15) being the most active and globally recognized.

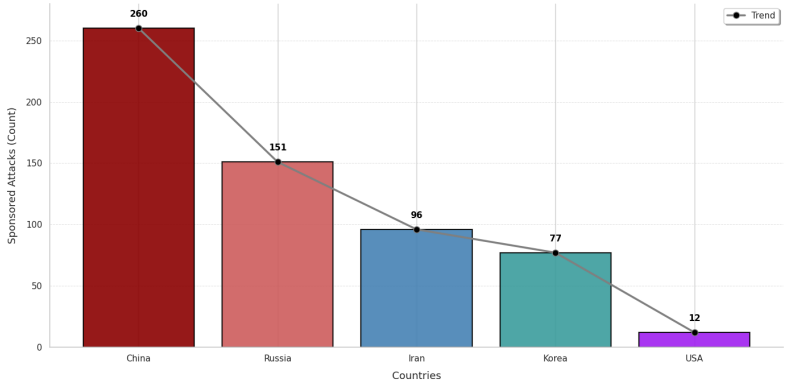


Figure 14. Top 7 sponsors of attacks around the world (2005–present): ranked visualization of the seven states most frequently affiliated with state-sponsored cyber operations in the analyzed dataset, showing each sponsor's count and share of recorded operations (data source: Council on Foreign Relations state-sponsored cyber operations dataset, aggregated 2005–present).

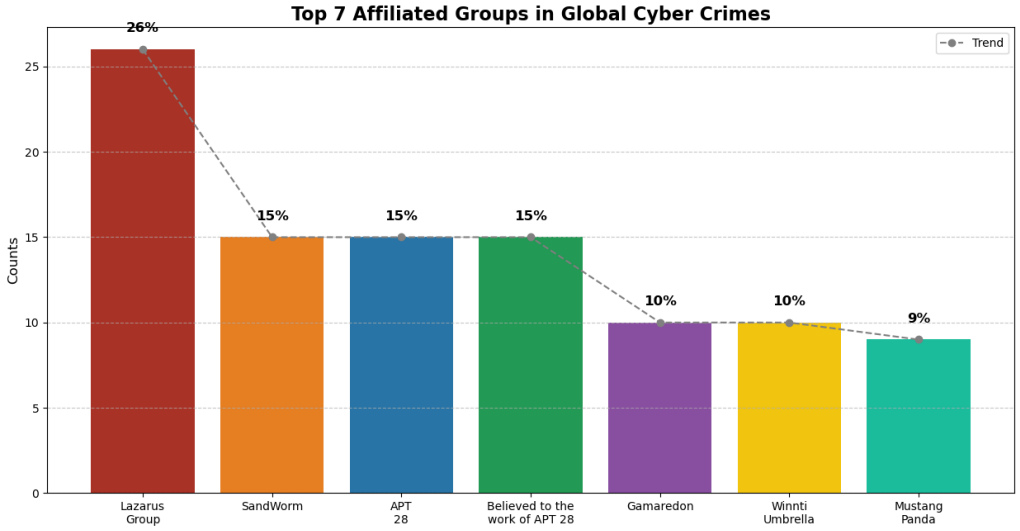


Figure 15. Frequency counts of the top seven affiliated threat groups in the global incident dataset, summarizing which threat actor labels appear most often in the CFR/analyzed sources.

Usually cybercriminals working for financial gain and politically driven state actors are classified separately, but in reality they are working quite closely and the boundaries can be blurred more often than actually considered. These criminal groups lease, sell or provide access to advanced malware, ransomware kits, and zero-day exploits to political actors. Similarly, some state-sponsored operations have relied on criminal networks as proxies to carry out attacks while concealing attribution. Such collaborations not only increase the sophistication of attacks but also require advanced defense strategies that address the convergence of these threat actors.

7.4. 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 of accounts per 1000 users. These statistics show that cyber criminals 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. The heatmap reveals significant disparities in breach distribution, with countries like Russia recording rates over 17 times the global average, while several developing nations report far fewer incidents. This difference, however, does not necessarily indicate a lower prevalence of cybercrime in developing regions but may instead reflect underreporting due to limited digital infrastructure, weaker incident detection capabilities, and inadequate legal or regulatory frameworks. In contrast, advanced economies often possess more robust monitoring systems, leading to higher detection and reporting rates. This distinction underscores the importance of interpreting breach data in light of both technological capacity and reporting practices. Further statics can be observed from Figure 12.

Although the heat map highlights high breaches volumes in certain advanced economies, it also shows notably sparse reporting from underrepresented regions such as Africa and South America. In Africa, for example, the 2022 Interpol African Cyberthreat Assessment reported widespread incidents of financial fraud, SIM-swap scams, and phishing attacks targeting mobile banking users, particularly in Nigeria, Kenya, and South Africa [67]. However, many such incidents go unreported due to limited awareness, inadequate incident response mechanisms, and the absence of formal cybercrime reporting channels. In South America, a 2023 ESET Threat Report documented a surge in ransomware attacks on healthcare facilities and municipal services in Brazil and Argentina, with several cases handled privately to avoid reputational damage. These examples demonstrate that lower recorded breach numbers in these regions often reflect gaps in detection and reporting rather than an absence of cybercrime activity, underscoring the need for stronger incident tracking and disclosure mechanisms worldwide.

8. Cyber Threats and Mitigation

In this section, we will discuss the prevalent cyber attacks that are common, attack vectors, and possible mitigation strategies that are shown in Figure 16.

8.1. Threat Vector

An attack or a threat vector is the means or a way that the attackers use to enter a network or gain access to a system. As the technology landscape is growing day by day, blocking off every attack vector is nearly impossible, but the following are some of the common attack vectors that attackers still use:

1. **Phishing** has been the most dominant attack vector in the last few decades. It involves stealing sensitive and confidential data of users like passwords, encryption keys, and credit card details by tricking the victim into revealing them. Many major attacks, like ransomware attacks, start with a phishing campaign against the victim.
2. **Lack of Encryption** is another common attack vector where attacks can extract sensitive data from storage devices and data in transit, where no proper encryption mechanism is in place. Many regulatory frameworks like **GDPR** and **HIPAA** mandate data encryption to protect privacy and ensure data integrity.
3. **Open Ports** are nowadays very common when it comes to network-based attacks. Services running on these open ports can be vulnerable, which can further lead to system compromise. Attacks often use automated scripts, or tools like **NMAP** can be used to scan a network or a system for open ports [68].

4. **Browser-based Vectors** come into practice when the attackers inject malicious code into a website [69] or directly create a fake website, tricking the browser into running malware to compromise the victim's system. With cloud computing becoming normal, many users access their data through the internet, due to which the security of browser-based vectors is of great concern.
5. **Insider threats** are involved when a trusted user within the organization distributes confidential data, or enables an attacker to access that confidential data. These incidents may result from deliberate actions or unintentional mistakes made by the user. Attackers use methods like bribing, tricking, or threatening them into providing access.

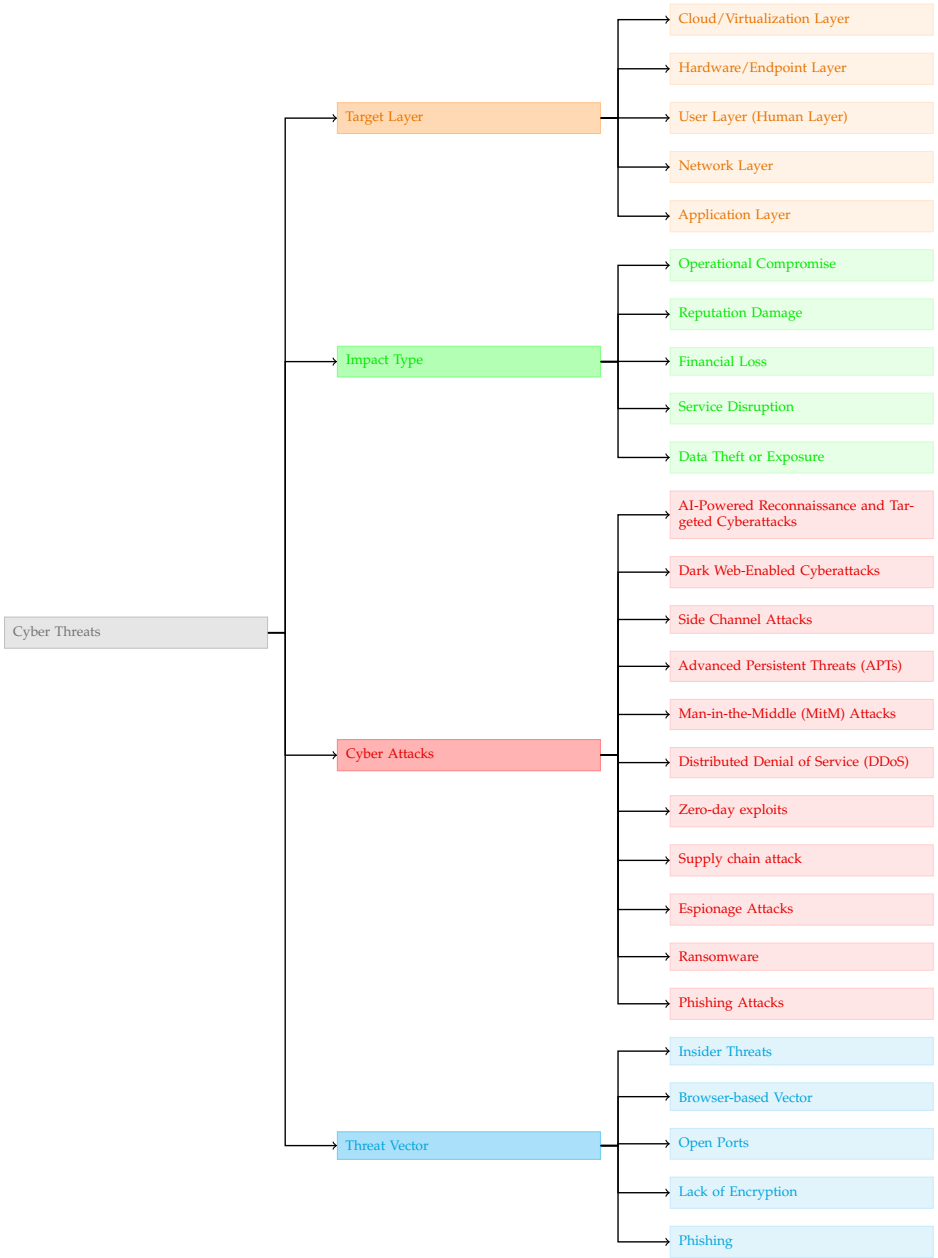


Figure 16. Threats and mitigations: consolidated matrix linking the paper's highest-priority attack types to layered mitigation measures, with each mitigation annotated by the primary actor responsible and the justification drawn from the IC3/CFR analyses and literature review [43,70,71].

Figure 17 shows how cyber attackers exploit different threat vectors to gain access to a network.

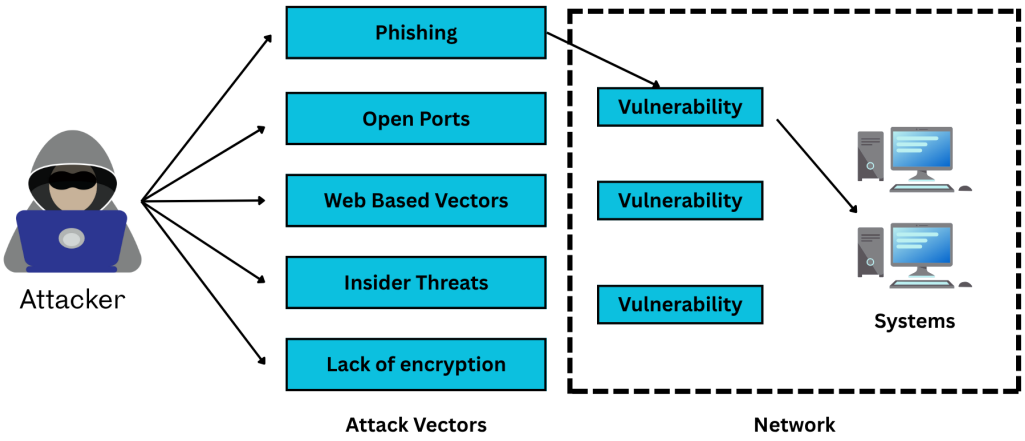


Figure 17. Attack workflow through different attack vectors: schematic flow diagram that maps common entry vectors to the attacker lifecycle stages.

8.2. Cyber Attacks

The top three cyber crimes, by number of complaints reported by victims in 2024, were phishing/spoofing, extortion, and personal data breaches. Victims of investment fraud, specifically those involving cryptocurrency, reported the most losses, totaling over USD 6.5 billion [1]. This section explains how some of these common attacks are conducted.

1. **Phishing attacks** are one of the most common cyberattacks in which criminals use techniques like social engineering by sending emails to the targeted individual, tricking them into thinking that the email is from a legitimate source. If the attacker uses voicemails 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. **Ransomware** is another pervasive attack that is common these days. 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 attacker 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. According to the FBI IC3 report 2024 [1], over 3000 complaints were filed, causing an estimated loss of over USD 12,000,000, which is a 9% rise from that of 2023.
3. **Espionage attacks** have been one of the most common and leading cyber-attacks in recent years. This attack damages the national security concerns 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 techniques. The intention behind these attacks can be money, power, or a 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. Usually, victims are directly targeted by the attackers themselves, but in a supply chain attack, the third party is exploited [72]. 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 by exploiting the weakest link, such as the external party in this case. Supply chain attacks can be further classified into three categories. The first is software-based attacks, where prebuilt software is 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. Service-based attacks are where an individual or an organization uses a service provided by someone else to achieve their goals.

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. **Distributed Denial of Service (DDoS)** is also one of the prevalent attacks that are common nowadays. Here, a particular system, server, or organization is overwhelmed by the excessive number 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 use such attacks to sabotage the critical digital infrastructure of fellow countries and states to gain a technological advantage.
7. **Man-in-the-Middle (MitM) Attacks** are 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 multi-layered 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.
9. **Side Channel Attacks** work by using physical characteristics of a system such as such as timing, acoustic signals, power consumption, and electromagnetic emissions, to gather information indirectly [73,74]. Side channel attacks can be used to extract sensitive data like passwords, encryption keys, or private user actions. Common side channel attacks include timing attacks, power analysis attacks, and acoustic cryptanalysis. Side-channel attacks are particularly dangerous because they mostly require limited system access or privileges and are very resilient in the modern era [75].
10. **Dark Web-Enabled Cyberattacks** also pose a great threat to digital infrastructure, as the dark web provides a thriving ecosystem to the threat actors for monetization and distribution of cyberattack tools and services. Ransomware-as-a-Service (RaaS), phishing kits, credential dumps, and zero-day exploits often arise from this forum, which makes it difficult to track the adversaries and also enables non-technical actors to perpetrate cybercrimes.
11. **AI-Powered Reconnaissance and Targeted Cyberattacks** have been observed to increase in recent times. These attacks use artificial intelligence (AI)-powered reconnaissance tools to enhance the speed, accuracy, and scale of their attacks [76]. This allows them to scour a wide range of data sources such as social media platforms, public data leaks, credential databases, and dark web forums with much precision. These tools can automatically assemble victim profiles by analyzing user behavior patterns [77].

8.3. Target Layer

This section highlights some of the common layers that are targeted by the attackers to perform malicious activities, which result in a compromised system or network.

Application Layer: All the software-based attacks and application-based attacks like SQL Injection, Cross-Site Scripting, and Broken Authentication lie under this layer. Attackers use automated tools or crafted payloads to manipulate application behavior, access sensitive

data, or bypass security controls. Weak coding practices and outdated applications make this layer a frequent target.

Network Layer: The Network Layer is mostly targeted through open ports, secured services, or vulnerable network protocols. Attackers take advantage of vulnerabilities in common services like SSH, FTP, and RDP. Distributed Denial of Service (DDoS), IP spoofing, on-path (MITM) attacks, and ARP poisoning are some of the common attacks thus performed.

User Layer (Human Layer): This layer focuses on exploiting the human factor. Attackers use methods like phishing, vishing, and email spoofing to extract personal information from the victims. Since humans are the weakest link in cybersecurity, this layer is the most exploited of them all [78].

Hardware/Endpoint Layer: Hardware or the endpoint layer is where the attacker exploits hardware of desktops, laptops, mobile phones, and IoT devices. Attacks also used hardware-based tools like keyloggers or infected USBs to extract information or infect the device. Physical attacks, like stealing a device or tampering with hardware, also occur.

Cloud/Virtualization Layer: As cloud usage is increasing day by day, attackers exploit misconfigured cloud services, publicly exposed storage (like AWS S3 buckets), or vulnerable APIs. The cloud increases the attack surface, due to which slight misconfigurations can lead to major data breaches.

8.4. Impact Type

The following are some of the most common impacts caused by a cyber attack.

1. **Data Theft or Exposure:** The most common result after any cyber attack is Data Theft or Exposure. Attackers extract sensitive information related to organizations, like user data, PII, credit card details, confidential documents, and much more. This stolen data is then sold on the dark web or is used in future targeted attacks. Data breaches can also lead to legal penalties under compliance regulations like **GDPR** or **HIPAA**.
2. **Service Disruption:** Common attacks like ransomware and DDoS attacks impact the service availability of an organization. Such attacks can also disrupt business operations and lock critical systems [79]. In the case of such attacks, service disruptions can last up to weeks, which causes significant loss to organizations and individuals.
3. **Financial Loss:** Organizations suffer direct and indirect financial losses through ransom payments, legal fines, regulatory penalties, and lost revenue during downtime. Additionally, there is also a cost linked with mitigation, incident response, and business continuity after the attack [80].
4. **Reputation Damage:** Every cyberattack comes with a cost of reputation damage and a decrease in customer or consumer trust. Any news of a cyber attack can immensely affect a company's reputation
5. **Operational Compromise:** Operational Compromise can also be characterized as administrative privileges. In such cases attacker can alter critical processes or implant persistent malware for continued surveillance and control. Such a deep compromise often takes longer to detect and recover from.

8.5. Mitigation Strategies

Cyber threats continue to grow, cyber crimes evolve and the traditional security approaches become less sufficient with each passing day. To address this nature of cybercrime, it is important that organizations and governments adopt proactive measures and adaptive mitigation strategies. This section presents mitigation techniques, policy frameworks, and innovative technologies to strengthen resilience, reduce vulnerabilities, and effectively mitigate the impact of cyber threats.

1. Training and awareness play an important role in minimizing security threats. This includes preparing employees by creating scenarios and training them on how to behave in such scenarios. Most common attacks, like social engineering and phishing attacks, are successful due to a lack of understanding of modern technology and trending techniques used for utilizing these attacks. One of the main reasons behind the large number of victims being 60+ is a lack of awareness about modern technology and exploitation methods.
2. AI-based methods can be used to detect and counter attacks such as espionage, ransomware, along with zero-day exploits and advanced persistent threats. Models can be trained to detect anomalous behavior, and response tools based on international guidelines can help control the magnitude of the loss by taking timely measures. New AI designs are transforming anomaly detection, with accuracy against new forms of attack. Such a combination can be used in the Attention-GAN framework, which relies on attention mechanisms and generative adversarial networks to boost the detection performance, especially in noise [81]. The same happens with the anomaly detection models based on AI, which are used to secure IoT devices in 5G-based smart cities; hybrid federated learning can offer privacy-preserving and, by extension, scalable defense mechanisms therein [82]. Although these strategies are promising, they are highly computationally expensive and must continue to be retrained to be successful against adaptive attackers.
3. Cloud-based protection services can also be used to deal with DDoS, malware, and phishing attempts by continuous monitoring and blocking the malicious activity, which reduces the attack surface and also improves the incident response time [83]. Its centralized approach simplifies policy enforcement and also enables faster recovery in case of a breach.
4. 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 [84]. 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 quantum state is disturbed and it warns the individual or parties involved. Being aware of new vulnerabilities is crucial to minimizing quantum attacks. This is possible through security assessments 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. A quantum computer would constitute an existential threat to classical cryptography. The National Cyber Security Centre [85] of the UK suggests starting the post-quantum cryptography (PQC) migration by 2028 and completing the migration by 2035. PQC algorithms, standardized by NIST, attempt to withstand Shor and other quantum attacks. Organizational inertia [86] keeps stakeholders on the sidelines because of perceived expenses, the challenge of not knowing how long algorithms are going to last, and the chance of integration being complicated.
5. To have a secure 5G network, there is a need for comprehensive security strategies from secure methods of authentication and authorization to awareness of how to use and deal with the odd behavior of this technology [87]. There is a need to communicate with various telecommunication providers 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.

6. Using machine learning algorithms and AI for defensive purposes can be accomplished 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 protecting a system once an attack is detected. An example of an AI defense system is SentinelOne, a tool based on a machine learning algorithm that provides endpoint security and can stop endpoint attacks like ransomware and other malware attacks [88].
7. Ethical hackers play a major role in identifying and addressing the security vulnerabilities in the system before they are exploited by malicious actors. They stimulate real-world cyberattacks in a controlled manner and help organizations uncover weaknesses in their networks, applications, and systems. Ethical hacking not only strengthens overall cybersecurity posture but also ensures compliance with security standards and reduces the risk of costly breaches. Ethical penetration is one of the building blocks of proactive cyber security. Recently, it became known that 83 percent of ethical hackers have already dealt with attacks enabled by AI, which is why it is so critical to provide red teams with modern tools and approaches [89]. Such a transition requires the need to insert AI-enabled penetration testing to imitate adversarial machine learning attacks, allowing organizations to detect the vulnerabilities prior to exploitation. Nevertheless, some problems that limit its universality are the lack of certified professionals and variability of regulatory environments across legal jurisdictions.
8. Cyber defense has to advance alongside the tactics of the adversaries. The MITRE Center for Threat-Informed Defense [90] promotes an active feedback loop, in which intelligence data on live threats is constantly used to update defense plans. With models like MITRE ATT&CK operationalizing the concept and approach, this is not a one-time defensive measure but an incremental one that improves over time out of a variety of attack patterns, as observed in practice. It is difficult because thwarting requires the organizational commitment to invest in the resources of continuous threat intelligence integration.
9. An agile multi-layered defense should integrate proactive penetration testing, AI-enhanced security monitoring, dynamic threat-related updates, and PQC preparedness. The end result of combining these components is a secure posture that can deal with existing threats and can predict the next ones too. Notably, cross-sector partnerships, cohesive regulation, and ongoing employee training are some of the keys to the success of such a structure.

9. Reflections and Implications

The landscape of cybercrimes is evolving at a significant rate, which leads to a need for proper law enforcement, policy development, and public awareness strategies. As threat actors make use of advanced technologies such as artificial intelligence, machine learning, and deepfake tools, it becomes challenging for law enforcement agencies to attribute, for cross-border jurisdiction, and give a timely response. This demands proactive digital forensics capabilities, international cooperation, and real-time intelligence sharing. Moreover, the gaps in policies about data protection, incident reporting, and cyber insurance must be covered in compliance with international standards such as GDPR, NIST, and ISO/IEC 27001. Furthermore, public awareness campaigns must move beyond basic hygiene, as humans are the weakest link and are exploited to the maximum. Training personnel about how things work in the cyber world would make a great difference. The future of cyber security is to be shaped by trends including quantum-resistant cryptography, zero-trust architectures, privacy-enhancing technologies, and the increasing integration of AI in both

attack and defense mechanisms. This demands a collaboration on an international level to engage the stakeholders, public and private sector entities, and people from academia to build a strong and adaptive cybersecurity ecosystem capable of mitigating current threats while anticipating those on the horizon.

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

Law enforcement agencies must play their role in reducing cybersecurity threats by enhancing investigation and training methods. Advanced technology should be used for digital forensics to have precise artifacts about the data. Training can be improved by 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; it is important for agencies to know the steps taken by different countries for mitigation and to be up to date with trending cybersecurity threats. A legislative framework is needed to take complete action against cybercrimes. The ever-evolving landscape of technology and cybercrimes demands a method where countries collaborate with each other and develop policies and legislative methods that would make tracking individuals performing these illegal activities easy. Institutions such as the United Nations, Interpol, and the International Telecommunication Union (ITU) must launch initiatives for countries to come forward and develop methods [91]. Policymakers should harmonize GDPR with national mandates and establish ENISA-led training programs for vulnerable demographics. Therefore, the policy and law enforcement agencies must work together to safeguard the privacy of individuals by taking measures against cybercrimes.

Policymakers should make cybersecurity guidelines, standards, and procedures that organizations should follow and ensure efficient implementation within. They should promote the sharing of information and collaboration between countries and also with international partners. A legal framework at the international level must be established to help identify and punish cybercrimes wherever they occur, thereby controlling the ratio of cybercrimes [92]. The General Data Protection Regulation (GDPR), the European Union Agency for Cybersecurity (ENISA), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the ISO/IEC 27001 standard provide critical guidelines for mitigating cyber threats, ensuring accountability, and harmonizing global responses. These frameworks address vulnerabilities highlighted in this study, such as data breaches, supply chain attacks, and demographic-specific risks, while supporting proactive defense strategies. 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.

Security agencies around the world work to protect their respective domains, ranging from the harms of cyber crimes to state-sponsored APTs. The UK's Government Communications Headquarters (GCHQ) and Security Service (MI5) deal with cyber threats through efficient intelligence and international collaborations [93]. These agencies, if they could work with other departments such as the US's Cybersecurity and Infrastructure Security Agency (CISA) or the Department of Homeland Security, and make a global task force, harmonizing the security frameworks and streamlining the responses to international threats, could operate much more easily. This task force could also lead public awareness campaigns, and integrate the ISO/IEC 27001 [94]. framework at a surface level, which would level accountability and reduce the risk factor on its own.

Along with all the measures to make policies and deploy preventive setups, public awareness is a crucial factor to make society digitally secure. For these organizations and educational institutes, they must start campaigns to spread awareness about the current

cyber trends and the threats they pose [95]. The minimum target for public awareness programs should be to know about phishing attacks and preventive measures against these attacks, as it is the most common attack with the maximum number of victims. Everyone must be aware of secure online hygiene, such as strong password strategies, and how this will reduce cybersecurity attacks. The program can be advanced with time by including knowledge of technology like deep fakes and AI-generated attacks.

9.2. Future Cybersecurity Trends

Keeping an eye on and 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 along with trends 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.

Artificial intelligence (AI) also has played a great part in the development of the cyber threat landscape, as it has allowed attackers to operate at a scale and adapt their operations more efficiently than ever before. Adversarial machine learning and others involve methods that malicious actors can use to alter model inputs or avoid automated detection software. Recent studies have shown that self-evolving phishing attacks are possible with the help of large language models (LLMs) and genetic algorithms that make it possible to quickly generate and sequentially refine trickery based on these models [96]. Such development has increased the level of sophistication of phishing campaigns, thus making them more personalized and more contextually persuasive.

In addition, testing of phishing webpage detection systems has shown them to be vulnerable against adversarial activities such that even their sophisticated detection models exhibit flaws in that they can be circumvented by properly designed inputs. Although recent models based on LLM, like Gemini Pro Vision, have demonstrated better robustness, the detection rate remains variable, a situation that implies that there will always be a cat and mouse game between the conductors and the administrators [97].

On the defensive end, both AI-enabled anomaly detection and hybrid model design involving a combination of both deep learning and traditional classification algorithms are proving to be bright prospects. Nevertheless, these defenses are vulnerable to data poisoning and evasion attacks, when an attacker adds poisoned training data, or slightly manipulates the input to evade detection. Security practitioners have a long-term obstacle in the process of intensifying and speeding up the advancement of AI capacities. The process of creating realistic-looking images of an individual using a deep learning algorithm is known as deep fakes. Deep fakes have useful applications in different industries such as education, film, and accessibility, as they allow real-time simulations for better understanding, but cyber criminals can use this technology for negative purposes [98]. Deepfake technology, which is based on Generative Adversarial Networks (GANs), was initially an experimental device but has progressed into a weaponized cyber-threat. With deepfakes, the faces and voices of individuals can be simulated realistically and social engineering attacks are possible, which could work around traditional trust systems. The spectacular 2024 case occurred in Hong Kong with a finance officer making fraudulent transactions worth USD 25 million after attending a video conference with several fake colleagues, convincingly imitated with the help of the deepfake technology. This incident highlights the risks deepfakes can pose to corporate workflows and the channels leading to high value decisions.

Other described scenarios involve influential executives who are impersonated in real time through voice cloning and doctored video feeds so that they can approve sen-

sitive actions or give out confidential information. Defenses have shown promise, but well-trained attackers can use adversarial perturbations to defeat detection models. This creates a perpetual escalation in offensive and defensive deepfake capabilities. Quantum computing poses a long-term strategic threat to cryptographic infrastructure in the modern environment. Algorithms like Shor and Grover are a threat in breaking the widely used public-key algorithm (RSA, ECC) and minimize the margin of security associated with symmetric encryption. It has given rise to the harvest now, decrypt later pattern, where the adversaries gather and save encrypted communications today with an aim to break encryption in future when quantum resources arrive. Quantum computing uses algorithms like *Shor's* and *Grover's* algorithms, which are very effective in breaking cryptographic algorithms because of their ability to divide data in half and factor large composite numbers. The impact of this affects the confidentiality, integrity, and authenticity of sensitive information [99]. This is only one effect of quantum computing from a cybersecurity perspective; others can be technological inequality, data privacy regard, and cryptographic vulnerability.

The U.S. National Institute of Standards and Technology (NIST) has in turn provided a final set of Post-Quantum Cryptography (PQC) standards that incorporate security against quantum computers; they consist of ML-KEM, ML-DSA, and SLH-DSA. But whatever the awareness, implementation has yet to mature to anywhere close to a significant level, with a small percentage of organizations initiating preparations to face quantum-era threats [100]. According to a survey of the industry, only one-fifth of organizations may be considered to be so-called quantum-safe heroes, with a majority of the organizations having no clear-cut plans to migrate or governance practices to transition to cryptographic use [101]. National cybersecurity officials such as the UK NCSC have proposed phased migration strategies (identify vulnerable assets by 2028, transition critical systems by 2031 and reach full PQC adoption by 2035), but those are hampered by technical, economic, and interoperability issues. 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 [102]. 5G networks introduce a wide 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. 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 of such attacks suggested by researchers throughout the world is the decentralization of technology or using blockchain [103]. 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 cloud-based vulnerabilities to gain unethical access to data or services [104]. Dark web actors are likely to assume a more prominent role in future cyberattacks, using obscurity to enable cybercrime-as-a-service platforms. As AI-based tools and cryptocurrency anonymity increase, these actors are expected to provide more advanced malware, ransomware sets, and data breach services. Future trends also suggest more directed attacks, such as supply chain attacks and deepfake-based social engineering; thus, dark web monitoring becomes an essential part of proactive security measures. 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 [105]. Finally, there are hybrid attacks where attackers or

adversaries use a combination of two or more attacks. This will blend digital and psychological techniques, making the attack harder to detect and defend against. It is important that the cybersecurity strategies are properly structured for risk analysis and threat categorization to effectively anticipate and respond to emerging threats. Organizations will need to adopt security frameworks and incorporate governance strategies with board-level accountability, the presence of CISOs, and routine cybersecurity audits [71]. Embedding cybersecurity into governance structures and aligning them with international standards will not only improve threat response but also ensure regulatory compliance and long-term operational continuity for both public and private institutions. The simultaneous threat of AI-powered attacks, deepfake-related fraudulent activities, and quantum threats provide evidence of the maturation of cybercrime. Such threats are not standalone; deepfake creation can be automated using AI, and quantum computers may one day make currently employed cryptographic safeguards irrelevant. To deal with these issues, multi-layered defense mechanisms need to be implemented, using a combination of technical, regulatory, and user awareness. The findings presented here extend the secondary data analysis in this study by contextualizing modern threat categories within broader sociotechnical and organizational dynamics.

10. Conclusions

In the past two decades, the landscape of technology has taken a sharp turn, which has 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.

It is observed that the cybercrimes have marked an increase in both frequency and sophistication. The attacks now have a much wider reach, encompassing private businesses, infrastructures, and government organizations. These trends reflect a shift in both non-state- and state-sponsored attacks. Moreover, the geographical distributions have also shown a swift turn with a more noticeable spread. While traditional peaks are constant, the emergence of new attackers has been observed lately. This spread 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 for all genders and age groups, which can be observed from the gender disparity analysis in cybersecurity. Victims of these cybercrimes range from young adults to senior citizens. Every age group faces different and unique threats and challenges. This highlights the need for proper awareness for every respective age group. Temporal patterns and peaks of attacks and scams are different. By understanding the temporal patterns and peaks of various attacks, security researchers and policymakers can make more robust and proactive defensive measures to safeguard our digital assets.

This study offers an overview of common attack types as discussed in the IC3 [1] report, mitigation strategies, and how cybersecurity frameworks such as GDPR, NIST, and ENISA offer practical insights for policymakers, law enforcement agencies, and cybersecurity professionals. It also highlights how international collaborations of the organizations would pose a great benefit to the overall cybersecurity infrastructure. It would reform real-world defense planning and regulations. However, the reliance on reported data for our study might underrepresent the cybercrime and threat scope and limit the demographic analysis due to data constraints.

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.

Author Contributions: Conceptualization, E.b.A.; methodology, B.S., M.Z. and E.b.A.; resources, M.A.; validation, M.M.N., M.Z. and Z.M.; writing—original draft preparation, M.A. and M.M.N.; writing—review and editing, B.S. and Z.M.; supervision, Z.M.; funding acquisition, Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

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. Internet Crime Complaint Center (IC3). 2024 Internet Crime Report. Annual Report, FBI Internet Crime Complaint Center, 2024. Available online: https://www.ic3.gov (accessed on 1 July 2025).
2. Federal Bureau of Investigation. Internet Crime Report 2023, 2023. Accessed from the Federal Bureau of Investigation Website. Available online: https://www.ic3.gov (accessed on 1 September 2025).
3. Rajasekharaiah, K.; Dule, C.S.; Sudarshan, E. Cyber security challenges and its emerging trends on latest technologies. *Iop Conf. Ser. Mater. Sci. Eng.* **2020**, *981*, 022062. [CrossRef]
4. Lian, Z.; Shi, P.; Chen, M. A Survey on Cyber-Attacks for Cyber-Physical Systems: Modeling, Defense and Design. *IEEE Internet Things J.* **2024**, *12*, 1471–1483. [CrossRef]
5. Świątkowska, J. Tackling cybercrime to unleash developing countries' digital potential. *Pathways Prosper. Comm. Backgr. Pap. Ser.* **2020**, *33*, 2020–01.
6. Oh, J. State-Sponsored Cyber Operations (2005-Present). 2023. Available online: https://www.kaggle.com/datasets/justin2028/state-sponsored-cyber-operations-2005-present (accessed on 1 September 2025).
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. [CrossRef]

9. 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. [CrossRef]
10. 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. [CrossRef]
11. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **2023**, *12*, 1333. [CrossRef]
12. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
13. Nespoli, P.; Papamartzivanos, D.; Mármol, F.G.; Kambourakis, G. Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 1361–1396. [CrossRef]
14. Hoar, S.B. Trends in cybercrime: The dark side of the Internet. *Crim. Just.* **2005**, *20*, 4.
15. Dunn, M.; Mauer, V. Towards a Global Culture of Cyber-Security. In *The International CIIP Handbook*; Center for Security Studies, ETH Zurich: Zurich, Switzerland, 2006; Volume 2, pp. 189–206.
16. Sheng, S.; Chan, W.L.; Li, K.; Xianzhong, D.; Xiangjun, Z. Context information-based cyber security defense of protection system. *IEEE Trans. Power Deliv.* **2007**, *22*, 1477–1481. [CrossRef]
17. Cárdenas, A.A.; Roosta, T.; Taban, G.; Sastry, S. Cyber security basic defenses and attack trends. In *Homeland Security Technology Challenges*; Artech House: Norwood, MA, USA, 2008; pp. 73–101.
18. McCrohan, K.F.; Engel, K.; Harvey, J.W. Influence of awareness and training on cyber security. *J. Internet Commer.* **2010**, *9*, 23–41. [CrossRef]
19. Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man, Cybern.-Part A Syst. Humans* **2010**, *40*, 853–865. [CrossRef]
20. Lupovici, A. Cyber warfare and deterrence: Trends and challenges in research. *Mil. Strateg. Aff.* **2011**, *3*, 49–62.
21. Reddy, G.N.; Reddy, G. A study of cyber security challenges and its emerging trends on latest technologies. *arXiv* **2014**, arXiv:1402.1842. [CrossRef]
22. 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), Rawalpindi, Pakistan, 11–12 December 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 7–14.
23. 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. *Digit. Sustain. Rev.* **2023**. *3*, 1–12. [CrossRef]
24. Azubuike, C.F. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. *Nnamdi Azikiwe J. Political Sci.* **2023**, *8*, 101–114.
25. Bendovschi, A. Cyber-Attacks—Trends, Patterns and Security Countermeasures. *Procedia Econ. Financ.* **2015**, *28*, 24–31. [CrossRef]
26. Pescatore, J. *Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017*; SANS Institute InfoSec Reading Room: Bethesda, MD, USA, 2017.
27. Broadhurst, R.; Chang, L.Y. Cybercrime in Asia: Trends and challenges. In *Handbook of Asian Criminology*; Springer Science & Business Media: New York, NY, USA, 2012; pp. 49–63.
28. Cabaj, K.; Kotulski, Z.; Księżopolski, B.; Mazurczyk, W. *Cybersecurity: Trends, Issues, and Challenges*; Springer: Berlin/Heidelberg, Germany, 2018.
29. 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: Boca Raton, FL, USA, 2021; pp. 129–154.
30. 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), Riga, Latvia, 6–7 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
31. Durojaye, H.; Raji, O. Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. *arXiv* **2022**, arXiv:2212.08036. [CrossRef]
32. Osawa, J. The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pac. Rev.* **2017**, *24*, 113–131. [CrossRef]
33. Ali, M.L.; Thakur, K.; Atobatele, B. Challenges of Cyber Security and the Emerging Trends. In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, New York, NY, USA, 7–12 July 2019; BSCI '19; pp. 107–112. [CrossRef]
34. Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 5766–5781. [CrossRef]
35. Warren, M.; Hutchinson, W. Cyber attacks against supply chain management systems: A short note. *Int. J. Phys. Distrib. Logist. Manag.* **2000**, *30*, 710–716. [CrossRef]

36. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cyber security. *Comput. Sci. Rev.* **2020**, *35*, 100219. [CrossRef]
37. Kaloudi, N.; Li, J. The ai-based cyber threat landscape: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–34.
38. Huang, K.; Siegel, M.; Madnick, S. Systematically understanding the cyber attack business: A survey. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–36.
39. Brundage, M.; Avin, S.; Wang, J.; Belfield, H.; Krueger, G.; Hadfield, G.; Khlaaf, H.; Yang, J.; Toner, H.; Fong, R.; et al. Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv* **2020**, arXiv:2004.07213. [CrossRef]
40. Citaristi, I. International telecommunication union—itu. In *The Europa Directory of International Organizations 2022*; Routledge: London, UK, 2022; pp. 365–369.
41. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
42. Duo, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–800.
43. Agrafiotis, I.; Nurse, J.R.; Goldsmith, M.; Creese, S.; Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J. Cybersecur.* **2018**, *4*, tyy006.
44. Singh, T. State-Sponsored Cyberattacks. In *Cybersecurity, Psychology and People Hacking*; Springer: Berlin/Heidelberg, Germany, 2025; pp. 147–150.
45. Uma, M.; Padmavathi, G. A survey on various cyber attacks and their classification. *Int. J. Netw. Secur.* **2013**, *15*, 390–396.
46. Wisnioski, M.H. *Engineers for Change: Competing Visions of Technology in 1960s America*; MIT Press: Cambridge, MA, USA, 2012.
47. Hauben, M. History of ARPANET. *Site l'Inst. Super. Eng. Porto* **2007**, *17*, 1–20.
48. Saltzer, J.H.; Schroeder, M.D. The Protection of Information in Computer Systems. *Proc. IEEE* **1975**, *63*, 1278–1308. [CrossRef]
49. Zhang, L. A New Architecture for Packet Switching Network Protocols. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 1989.
50. de Jong, B. The KGB in Eastern Europe during the Cold War: On agents and confidential contacts. *J. Intell. Hist.* **2005**, *5*, 85–103. [CrossRef]
51. Kephart, J.O.; Sorkin, G.B.; Chess, D.M.; White, S.R. Fighting computer viruses. *Sci. Am.* **1997**, *277*, 88–93. [CrossRef]
52. Chen, Q.; Bridges, R.A. Automated behavioral analysis of malware: A case study of wannacry ransomware. In Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 18–21 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 454–460.
53. Fayi, S.Y.A. What Petya/NotPetya ransomware is and what its remidiations are. In *Information Technology-New Generations: Proceedings of the 15th International Conference on Information Technology, Las Vegas, NV, USA, 16–18 April 2018;* Springer: Berlin/Heidelberg, Germany, 2018; pp. 93–100.
54. Schoop, M.; Vogl, R.; Lins, S. Generative AI in Cybersecurity: Risks, Challenges, and Opportunities. *arXiv* **2025**, arXiv:2505.23733.
55. Akinbowale, O.E.; Adegboyega, O.; Okere, W. The impact of cybercrime on the banking sector: A balanced scorecard analysis. *J. Financ. Crime* **2020**, *27*, 867–884. [CrossRef]
56. Cotrina, L.; León, P.; Reyes, C.; Arbulú Ballesteros, M.; Guzmán, M.; Castillo, J.; Acosta, R.; Morales, A. Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches. *J. Educ. Soc. Res.* **2024**, *14*, 96. [CrossRef]
57. Ni, T.; Lan, G.; Wang, J.; Zhao, Q.; Xu, W. Eavesdropping mobile app activity via {Radio-Frequency} energy harvesting. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 3511–3528.
58. Oberhuber, M.; Unterguggenberger, M.; Maar, L.; Kogler, A.; Mangard, S. Power-related side-channel attacks using the Android sensor framework. In Proceedings of the Network and Distributed System Security (NDSS) Symposium 2025, San Diego, CA, USA, 24–28 February 2025.
59. Sun, Z.; Ni, T.; Yang, H.; Liu, K.; Zhang, Y.; Gu, T.; Xu, W. FLoRa: Energy-efficient, reliable, and beamforming-assisted over-the-air firmware update in LoRa networks. In Proceedings of the 22nd International Conference on Information Processing in Sensor Networks, San Antonio, TX, USA, 9–12 May 2023; pp. 14–26.
60. Bada, M.; Nurse, J.R. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 73–92.
61. Henry, N.; Flynn, A. Image-based sexual abuse: Online distribution channels and illicit communities of support. *Violence Against Women* **2019**, *25*, 1932–1955. [CrossRef]
62. 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. *Int. J. Environ. Res. Public Health* **2021**, *18*, 14. [CrossRef]
63. 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. [CrossRef]

64. Kizza, P.J. Unmasking the Cyberbully: Understanding the Psychological and Social Dynamics behind Online Abuse. *Res. Invent. J. Law Commun. Lang* **2024**, *3*, 119–123.
65. Fitzpatrick, S.; Ramgopal, K. Hackers linked to Chinese government stole millions in COVID benefits, Secret Service says. *NBC News*, 5 December 2022.
66. Lindsay, J.R. Stuxnet revisited: From cyber warfare to secret statecraft. *J. Strateg. Stud.* **2025**, 1–40. [CrossRef]
67. INTERPOL Cybercrime Directorate. *African Cyberthreat Assessment Report 2023*; Technical Report, INTERPOL, 2023. Assessment Produced by the African Cybercrime Operations Desk. Available online: https://www.interpol.int/ (accessed on 8 September 2025).
68. Oh, S.H.; Kim, J.; Nah, J.H.; Park, J. Employing deep reinforcement learning to cyber-attack simulation for enhancing cybersecurity. *Electronics* **2024**, *13*, 555. [CrossRef]
69. Madhvan, R.; Zolkipli, M.F. An overview of malware injection attacks: Techniques, impacts, and countermeasures. *Borneo Int. J.* **2023**, *6*, 22–30. eISSN 2636-9826.
70. Simmons, C.; Ellis, C.; Shiva, S.; Dasgupta, D.; Wu, Q. *AVOIDIT: A Cyber Attack Taxonomy*; Technical Report CS-09-003 University of Memphis: Memphis, TN, USA, 2009.
71. Nicholson, A.; Watson, T.; Norris, P.; Duffy, A.; Isbell, R. A taxonomy of technical attribution techniques for cyber attacks. In *European Conference on Information Warfare and Security*; Academic Conferences International Limited: Reading, UK, 2012; p. 188.
72. Williams, L.; Benedetti, G.; Hamer, S.; Paramitha, R.; Rahman, I.; Tamanna, M.; Tystahl, G.; Zahan, N.; Morrison, P.; Acar, Y.; et al. Research directions in software supply chain security. *ACM Trans. Softw. Eng. Methodol.* **2025**, *34*, 1–38. [CrossRef]
73. Standaert, F.X. Introduction to side-channel attacks. In *Secure Integrated Circuits and Systems*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 27–42.
74. Spreitzer, R.; Moonsamy, V.; Korak, T.; Mangard, S. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 465–488.
75. Wang, Z.; Meng, F.h.; Park, Y.; Eshraghian, J.K.; Lu, W.D. Side-channel attack analysis on in-memory computing architectures. *IEEE Trans. Emerg. Top. Comput.* **2023**, *12*, 109–121.
76. Hayat, T.; Gatlin, K. AI-Powered Ethical Hacking: Rethinking Cyber Security Penetration Testing. ResearchGate, Feb 2025. Available online: https://www.researchgate.net/publication/389313366_AI-Powered_Ethical_Hacking_Rethinking_Cyber_Security_Penetration_Testing (accessed on 8 September 2025).
77. Xing, W.; Shen, J. Security control of cyber–physical systems under cyber attacks: A survey. *Sensors* **2024**, *24*, 3815. [CrossRef]
78. Daudi, M. Trust framework on exploitation of humans as the weakest link in cybersecurity. *Appl. Cybersecur. Internet Gov.* **2023**, *2*, 1–26. [CrossRef]
79. Asiri, M.; Saxena, N.; Gjomemo, R.; Burnap, P. Understanding indicators of compromise against cyber-attacks in industrial control systems: A security perspective. *ACM Trans. Cyber-Phys. Syst.* **2023**, *7*, 1–33. [CrossRef]
80. Gulyas, O.; Kiss, G. Impact of cyber-attacks on the financial institutions. *Procedia Comput. Sci.* **2023**, *219*, 84–90. [CrossRef]
81. Sen, M.A. Attention-GAN for anomaly detection: A cutting-edge approach to cybersecurity threat management. *arXiv* **2024**, arXiv:2402.15945.
82. Reis, M.J. AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. *Electronics* **2025**, *14*, 2492. [CrossRef]
83. Kumar, S.; Dwivedi, M.; Kumar, M.; Gill, S.S. A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services. *Comput. Sci. Rev.* **2024**, *53*, 100661. [CrossRef]
84. Dam, D.T.; Tran, T.H.; Hoang, V.P.; Pham, C.K.; Hoang, T.T. A survey of post-quantum cryptography: Start of a new race. *Cryptography* **2023**, *7*, 40. [CrossRef]
85. National Cyber Security Centre. UK Post-Quantum Cryptography Migration Guidelines. Financial Times. 2025. Available online: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines (accessed on 8 September 2025).
86. Entrust. Post-Quantum Cryptography Awareness Is High but Widespread Action Lags, Finds 2024 Global Entrust Report. 2024. Entrust. Available online: https://www.entrust.com/company/newsroom/post-quantum-cryptography-awareness-is-high-but-widespread-action-lags-finds-2024-global-entrust-report (accessed on 8 September 2025).
87. Shobowale, K.; Mukhtar, Z.; Yahaya, B.; Ibrahim, Y.; Momoh, M. Latest advances on security architecture for 5G technology and services. *Int. J. Softw. Eng. Comput. Syst.* **2023**, *9*, 27–38. [CrossRef]
88. Licitra, S. Leveraging AI Techniques for Automated Security Incident Response. Ph.D. Thesis, Politecnico di Torino, Torino, Italy, 2024.
89. EC-Council. Global Ethical Hacking Report: 83% of Ethical Hackers Experience AI-Driven Attacks. 2024. GlobeNewswire. Available online: https://www.globenewswire.com/news-release/2024/01/24/2815519/0/en/Global-Ethical-Hacking-Report-83-of-Ethical-Hackers-Experience-AI-Driven-Attacks.html (accessed on 8 September 2025).

90. MITRE Center for Threat-Informed Defense. More Threat-Informed in More Ways with More Defenders. 2024. MITRE. Available online: https://ctid.mitre.org/blog/2024/05/02/more-threat-informed-in-more-ways-with-more-defenders/ (accessed on 8 September 2025).
91. Chimchiuri, L. The evolution of cybercrime legislation. *Sci. Work. Natl. Aviat. Univ. Ser. Law J. Air Space Law* **2024**, *2*, 221–227.
92. Buçaj, E.; Idrizaj, K. The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidiscip. Rev.* **2025**, *8*, 2025024. [CrossRef]
93. Parker-Vincent, C.; Goodman, M.S. Moving Towards a Secret Intelligence Joint Capability? Challenges and Opportunities of Removing Organisational Boundaries. *RUSI J.* **2024**, *169*, 22–27. [CrossRef]
94. Nurbojatmiko, N.; Khatami, M.S.K.; Asnadi, N.M.; Anisyah, R. ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review. *Sinkron: Jurnal dan Penelitian Teknik Informatika*, **2025**, *9*, 484–492. [CrossRef]
95. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. [CrossRef]
96. Sato, S.; Ohki, T.; Nishigaki, M. Can We End the Cat-and-Mouse Game? Simulating Self-Evolving Phishing Attacks with LLMs and Genetic Algorithms. *arXiv* **2025**, arXiv:2507.21538.
97. Kulkarni, A.; Balachandran, V.; Divakaran, D.M.; Das, T. From ML to LLM: Evaluating the Robustness of Phishing Web Page Detection Models against Adversarial Attacks. *Digit. Threat. Res. Pract.* **2025**, *6*, 1–25. [CrossRef]
98. Pawelec, M. Decent deepfakes? Professional deepfake developers' ethical considerations and their governance potential. *AI Ethics* **2025**, *5*, 2641–2666. [CrossRef]
99. Khan, S.; Krishnamoorthy, P.; Goswami, M.; Rakhimjonovna, F.M.; Mohammed, S.A.; Menaga, D. Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses. *Nanotechnol. Percept.* **2024**, *20*, S13.
100. Entrust. Post-Quantum Cryptography Awareness Is High, but Widespread Preparation Lags. 2024. Entrust Global Survey. Available online: https://www.entrust.com (accessed on 8 September 2025).
101. IT Pro. Post-Quantum Cryptography Is Now Top of Mind for Cybersecurity Leaders. 2025. IT Pro. Available online: https://www.itpro.com/business/post-quantum-cryptography-is-now-top-of-mind-for-cybersecurity-leaders (accessed on 8 September 2025).
102. Salahdine, F.; Han, T.; Zhang, N. Security in 5G and beyond recent advances and future challenges. *Secur. Priv.* **2023**, *6*, e271. [CrossRef]
103. Alam, S. Security concerns in smart agriculture and blockchain-based solution. In Proceedings of the 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON), Raigarh, India, 8–10 February 2022; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.
104. Pericherla, S.S. Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art. *ISeCure* **2023**, *15*, 1–58.
105. Patsakis, C.; Arroyo, D.; Casino, F. The malware as a service ecosystem. In *Malware: Handbook of Prevention and Detection*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 371–394.

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.