Meta-Analysis of Cyber Dominance in Modern Warfare: Attacks and Mitigation Strategies

Dr. Rashid A. Khan

Assistant Professor, Computer & Information Science & Cybersecurity, Gannon University, USA & Md Rasheduzzaman Labu (2023), MSc-Information Assurance and Cybersecurity, Gannon University, USA

ABSTRACT

This meta-analysis study focused on cyber dominance in modern warfare, particularly, exploring cyber-attacks and mitigation strategies. The study ascertained that the escalating growth of internet connectivity and the rising reliance on networked digital technologies have opened new avenues for cyber-attacks in the contemporary era. Various actors, comprising state and non-state entities, parties in offensive hacking operations and information campaigns to achieve strategic goals. The study conducts a comprehensive meta-analysis of existing research to explore key strategies for establishing and maintaining cyber-attacks and mitigation strategies. This study analyzed peer-reviewed papers that investigate both cyber-attack tactics employed by state actors and defensive policy frameworks and measures adopted by nations. The significant volume of studies indicated that the execution of robust authentication strategies, such as multi-factor authentication (MFA) could mitigate cyber-attacks. The meta-analysis studies equally ascertained that consistently employing security patches and software updates is instrumental to addressing these vulnerabilities promptly. Besides, configuring firewalls to limit unnecessary inbound and outbound traffic helps create a strong defense perimeter and prevents unauthorized communication.

Keywords: Cyber dominance, Cyber-attack, Modern warfare, Data breaching, Mitigation Strategies.

1.INTRODUCTION

Cyberspace has emanated as a fundamental domain of warfare in the contemporary era. The exponential growth and development of internet connectivity across the world combined with the escalating dependence of militaries and governments on networked digital technologies has launched new fronts for conflict and espionage. Countries now actively adopt offensive hacking operations and information campaigns to accomplish strategic goals during peacetime and periods of open hostilities. As cyber competencies proceed to proliferate, controlling this online battlefield has become an essential national security priority for many nations. Nonetheless, achieving cyber dominance is an enormously complicated challenge due to the interconnected nature of networks and the difficulty of attributing attacks.

1.1. BACKGROUND

According to Algarni et al., (2021), cyber warfare revolves around the use of digital technology to disrupt, infiltrate, or destroy the information systems of an adversary. It has become a prevalent common method used by non-state actors, state actors, and terrorist organizations in contemporary warfare. The escalating significance of cyber dominance is an essential aspect to be investigated. In the recent past, the reliance on information systems and technology has escalated exponentially, leading to the prevalence and emergence of cyber warfare. The increase in cyber warfare has greatly impacted modern warfare strategies and tactics.

This research undertakes a meta-analysis of current research to explore key strategies for maintaining and asserting cyber dominance in contemporary warfare. The study aims to analyze peer-reviewed papers examining both cyber-attack tactics deployed by state actors and defensive policy frameworks and measures employed by nations. The prime objective is to synthesize the present understanding of how government intelligence, military, and political dimensions cooperate in cyber conflicts. Insights generated can assist in terms of enhancing strategies for reinforcing cyber capabilities, defending critical infrastructure, and executing effective deterrence policies.

1.2 PROBLEM STATEMENT

The challenge of cyber dominance in contemporary warfare presents significant threats to national security, organizations, and international stability. With the interconnectedness of worldwide systems, cyber-attacks can cause tremendous damage, ranging from economic interruptions to compromising instrumental infrastructure. The sophistication and frequency of cyber threats in warfare have accelerated substantially in recent years (Bamrara, 2023). Cyber-attacks have been employed to obtain a tactical or strategic advantage and to disrupt the enemy's command and control systems. As such, Mitigation strategies are instrumental in terms of countering these threats effectively.

1.3 RESEARCH OBJECTIVES

The prime objectives of this meta-analysis are to explore current research on cyber dominance in modern warfare and pinpoint key attack techniques and mitigation strategies. These objectives facilitate an extensive comprehension of the subject matter and present valuable insights for military and policy decision-making.

- To undertake a meta-analysis of research published studies in the last 8 years regarding cyber-attacks, operations, and strategies deployed by nation-states and organizations in modern warfare.
- To assess and synthesize data extracted from various literature to pinpoint common cyber-attack techniques, defense methods, and policy frameworks discussed.
- To assess trends over time in technologies, cyber-attacks, and governance techniques proposed by researchers to provide insight regarding how the threat landscape and responses are evolving.

1.4 RESEARCH QUESTION

- What are the key trends in the cyber dominance landscape and how are they influencing modern warfare?
- What are the key cyber-attack strategies employed by organizations and nation-states in modern warfare?
- What are the most effective defense methods against cyber-attacks in modern warfare?

1.5 SIGNIFICANCE OF THE STUDY

Enhancing our comprehension of cyber warfare is pivotal for governments, organizations, policymakers, and military professionals. This research paper contributes to an in-depth comprehension of the evolving nature of warfare and the strategic effects of cyber dominance. By pinpointing attack techniques and mitigation strategies, this study presents valuable insights that can inform governments, companies, policing agencies, military strategies, and policy decisions. It provides a foundation for establishing robust cybersecurity measures and international norms to safeguard national security interests.

1.6 KEY TERMS

- **Cyber Attack:** A malicious activity aimed at collecting, denying, disrupting, deteriorating, or obliterating information system resources or the information they contain.
- **Cyber Attack Incident**: A security event that endangers the confidentiality, integrity or accessibility of an information asset.
- **Breach**: A security compromise culminating in the unlawful or unintended destruction, loss, alteration, unauthorized disclosure, or access to safeguarded data, whether transmitted, stored, or otherwise handled.
- **Mitigation Strategies:** Refers to mechanisms of countering cyber-attacks and threats.

2. LITERATURE SEARCH STRATEGY

The literature review is a fundamental phase of any research study as it offers an extensive and comprehensive comprehension of the present knowledge and research gaps in a specific field. This section focuses on the research process, which comprises the literature review for the meta-analysis on cyber dominance in modern warfare. This section entails the identification of relevant research papers, the establishment of exclusion and inclusion criteria, and the collection, organization, and documentation of selected papers. The objective was to collect an extensive range of scholarly sources that provide theoretical frameworks, empirical studies, case studies, and expert opinions on the subject matter. The search process was performed systematically to ensure that no relevant papers were missed.

A systematic literature review was conducted to pinpoint peer-reviewed journal articles and relevant to the research topic published between 2018-2023. Five electronic databases and search engines were queried – *Google Scholar, Academia, Science Direct, Research Gates, and Web of Science*. Search phrases combined keywords such as 'cyber-attacks', 'network warfare', 'offensive operations', 'policy frameworks', 'cyber deterrence' etc. Additional criteria were applied to refine the results. Only English-language papers with a minimum of 50% focus on the cyber strategies of nation-state organizations were considered. Papers focusing only on techniques like DDoS or ransomware with no linkage to modern warfare were excluded.

2.1 LITERATURE REVIEW

Over the years, a multitude of studies have emerged, investigating the causes, dynamics, and implications of cyber threats. This proliferation of studies acts as a noteworthy indicator of the escalating significance of cyberattack preparedness for organizations, whether private or public and citizens globally. Moreover, these cyberattacks are increasingly captivating the media's attention. These joint efforts lead to enhancing awareness and understanding of cyber threats, eventually paving the way for enhanced mitigation, prevention, and resilience strategies. This

research is devoted to assisting in this endeavor by assessing the current knowledge of cybersecurity threats, drawing insights from a comprehensive review of 13 studies published by companies, public authorities, International Journal articles, and research institutions across different nations in recent years. It aims to address key questions: What do we understand regarding the frequency, origins, and effects of cyberattacks? What are the emerging and prevailing trends in cybersecurity? And how well-equipped are organizations equipped to mitigate cyber-attacks?

2.2 CYBER ATTACK ASSESSMENT

As per Boscoianu (2021), cyber-attacks have been considered the 5th top-rated threat in 2022 and have become the new norm across private and public sectors. This risky sector proceeds to escalate in 2023 as the Internet of Things cyber-attacks alone are anticipated to double by 2025. In that regard, the *World Economic Forum's* 2020 Global Risk Report indicates that the rate of detection is as low as 0.05% in America.

According to Hasan (2022), there was a noticeable upward pattern regarding the reported scenarios of cyber-attacks, propelled substantially by escalating cyber activity and enhanced reporting mechanisms. Approximations concerning the growth of the number of cyber-attacks vary significantly, ranging from a moderate few percent rise to a staggering tenfold surge. Most of these attacks are primarily inspired by criminal objectives, specifically those associated to financial gain. Moreover, there seems to be a noticeable escalation in scenarios associated to surveillance.

The backdrop of cyber threats also adjusts by the form of attack. For example, Symantec reported that in 2022, over 27% of all cyber-attack activities were traced back to computers in America. Meanwhile, as per the assessment by Verizon, approximately half of all cyber spying activities originated from East Asia (Gandal et al, 2023). Despite these observations, the precise attribution of these cyber-attacks to specific entities or individuals remains elusive.

Hasan (2022) contended that the majority of cyberattacks originated from external entities, but it is worth mentioning that several reports highlighted a significant portion of these attacks comprised former or current employees, accounting for anywhere from 6% to 28% of all cyber-attack incidents. Governments, alongside the financial industries and various sectors, emerge as primary targets.

The literature review exposed that there was a consensus concerning the substantial costs related to cyberattacks, with a majority of analyses concentrating on big companies (normally those with above 500 employees). Current approximations indicated a substantial expense that elevates in correlation with the organization's size on an individual per-organization basis. On a national scale, these costs translated into significant economic losses. As per McAfee, the average yearly loss attributable to cyberattacks exceeded 0.8% of a nation's GDP, with the Germany and Netherlands ranking at the top with losses exceeding 1.5% (Kolesnikov, 2023). However, it is fundamental to note that the range of estimates for these losses is quite extensive.

2.3 CYBER CRIME TRENDS

Hassan (2022), indicates that the new cyber-crime economy is on the rise. Cyber-attacks on all organizations, but specifically small to medium-sized enterprises, are becoming more prevalent, complex, and targeted. As per, the *World Economy Forum,* 43% of cyber-attacks are targeted at small businesses, but only 14% are prepared to defend and safeguard themselves. Not only does a cyber-attack interfere with normal operations, but it also causes damage to vital IT assets and infrastructure that can be challenging to recover from without the budget or resources to do so.

As regards the prospective targets, escalating interdependencies, partially driven by the increasing of the Internet of Things (IoT), are giving rise to interconnected threats. Cyber-attacks are rapidly directed towards Big Data hosting organizations and digital certificate providers, which have become principal targets. Furthermore, there is an evident shift in focus towards personal identities in cyberattacks, with perpetrators asserting more emphasis on "who you are" rather than "what you possess." Furthermore, the vulnerability of critical systems is intensified by weaknesses in GPS navigation, positioning, and timing, making it a noticeable concern in terms of affirming the security of vital infrastructure (Hasan, 2022).

According to Kelemen (2020), the assignment of mitigating cyber-attacks is becoming increasingly challenging because of the expanding array of options available to malicious actors. The exponential growth of anonymization tools and the abuse of of Big Data analytics have advanced a robust cybercrime industry, providing data and software for virtually any type of cyber-attack on a commercial basis.

Moreover, even encryption, a prevalent security measure, seems to struggle to keep pace with the substantially enhanced computing power, particularly, when combined with the presence of software backdoors. Furthermore, cyber-attacks are advancing to happen in plain sight but remain hidden within legitimate activities. Legitimate actions are increasingly being abused as a means to obtain an unfair advantage via cyber-attacks (Kelemen, 2020).

2.4 MITIGATION STRATEGIES

1) Strong Authentication and Access Controls:

Aslan & Samet (2018), indicated that execution of robust authentication strategies, such as multi-factor authentication (MFA), substantially enhanced security. Multi-factor authentication adds an extra layer of safeguarding by mandating users to provide multiple factors (e.g., fingerprint, password, or token) to access sensitive data or systems. Moreover, access controls ought to be executed to affirm that users only have the permissions required to perform their specific tasks, restricting the possible damage that can be caused by compromised accounts.

2) Regular Software Updates and Patch Management:

Hasan (2022) equally ascertained that consistently employing security patches and software updates is instrumental in addressing these vulnerabilities promptly. Companies ought to implement a robust patch management process that comprises monitoring testing patches, and vendor releases and executing them promptly in a manner across all systems and devices. Automated patch administration tools can streamline this process and guarantee that critical updates are not overlooked.

3) Network Segmentation and Firewall Configuration:

Some studies exposed that segmenting networks into smaller, insulated subnetworks can restrict the lateral movement of cyber attackers and diminish the effect of a possible breach. By segmenting the network into compartments, companies can isolate sensitive data, making it more challenging for cyber attackers to obtain unauthorized access (Aslan & Samet, 2018). Moreover, configuring firewalls to limit unnecessary inbound and outbound traffic helps create a strong defense perimeter and prevents unauthorized communication.

4) Anomaly Detection

Anomaly detection is a cyber-attack mitigation strategy for detecting network traffic that deviates from the normal expected behavior. This is deployed by establishing a baseline for normal traffic and then flagging any traffic that falls outside of that baseline. Anomaly detection can be used to detect a wide variety of attacks, including denial-of-service attacks, malware infections, and data breaches (Aslan & Samet, 2018).

5) Whitelisting

Whitelisting denotes to proactive cyber-attack mitigation strategy that only permits trusted and known applications, domains, network traffic, and processes to access the system. This is undertaken by developing a whitelist of trusted and known entities and then blocking everything else. Whitelisting is a very efficient way to combat cyber-attacks, as it makes it very hard for cyber attackers to gain access to the system (Khalel & Khudher, 2022).

6) Blacklisting

As per Khalel & Khudher, (2022), blacklisting refers to a reactive cyber-attack mitigation strategy that blocks known malicious processes and applications. This is undertaken by developing a blacklist of known malicious entities and subsequently blocking all traffic from those entities. Blacklisting is simpler to deploy and manage than whitelisting, but it is less secure. This is because blacklisting cannot prevent new or unknown attacks.

3. RESEARCH METHODOLOGY

The researcher applied quantitative meta-analysis to examine cyber dominance, cyber-attacks, and mitigation strategies. This method was selected since it facilitated for the synthesis of findings from different studies into one source with quantified data represented by an overall effect size. The employment of the meta-analytic method holds significance in the domain of research, as the vital evaluation of evidence from a myriad of studies on a provided subject is a paramount and valuable skill within the discipline. The systematic review and meta-analysis on "Cyber Dominance in Modern Warfare: Attacks and Mitigation Strategies" played an instrumental role for professionals in the Information Technology sector, underscoring a comprehensive perspective beyond isolated pivotal studies.

3.1 INCLUSION CRITERIA

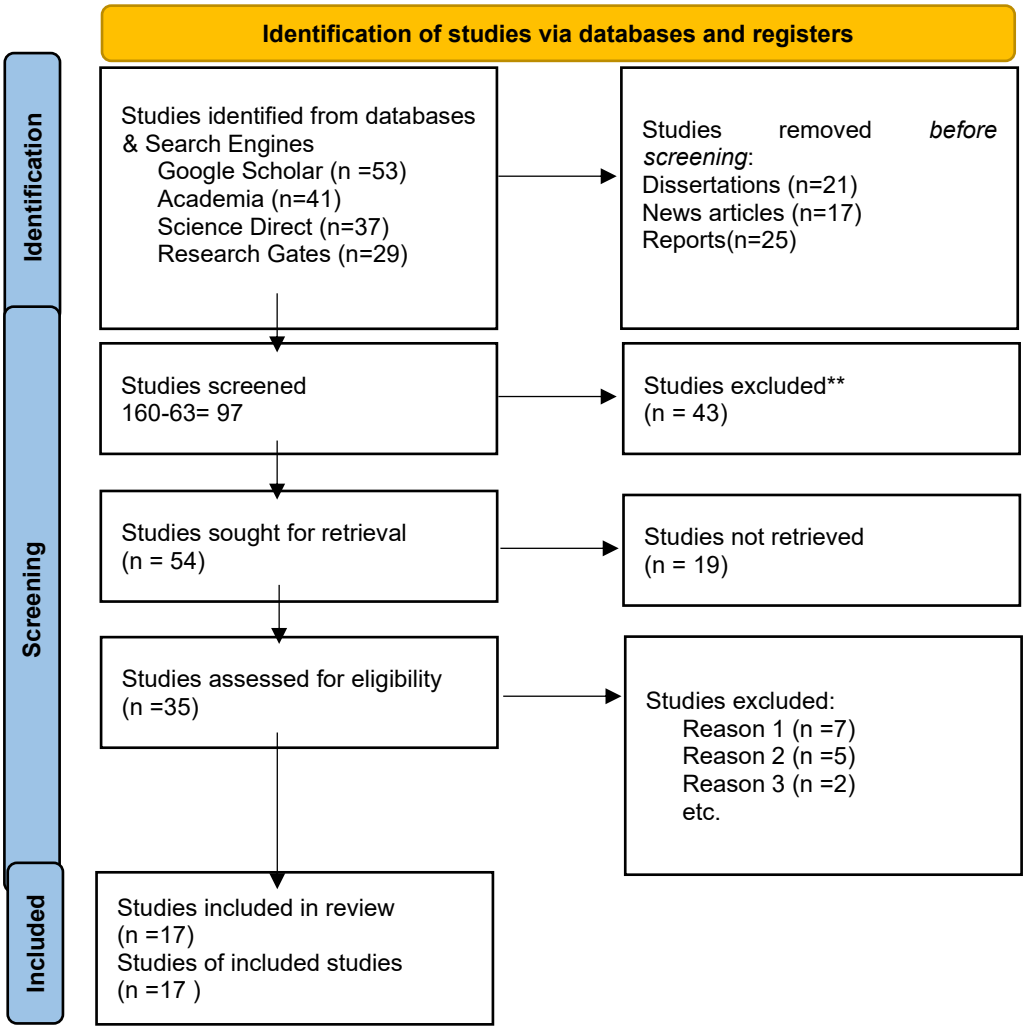
The prime objective of the literature review was to identify all scientific research studies associated with cyber security. The process of pinpointing and choosing studies for integrating into the meta-analysis observed a set of preset steps, which comprised upholding meticulous records of the procedure employed to include or exclude studies in the ultimate sample targeted for meta-analysis. This research followed the study selection process described in the PRISMA guidelines flowchart, as showcased in Figure 1. The flowchart describes the progression of the study selection process, proceeding from identification to screening, then to eligibility, and eventually to the studies included in the meta-analysis.

By adhering to the PRISMA guidelines for describing eligibility procedures for study inclusion or exclusion, the researcher integrated an extensive range of studies, excluding only those studies that did not meet the specified inclusion criteria. Studies considered unsuitable for data extraction in the setting of the meta-analysis, and those lacking data appropriate for calculating impact sizes, were considered ineligible. While these studies

were not included in the meta-analysis, the researcher thoroughly assessed them to obtain insights into interpreting impact size calculations. Furthermore, the researcher reviewed these studies for guidance on reporting directions for future research.

Once studies were pinpointed as possible candidates for inclusion in the meta-analysis, the researcher evaluated the abstracts of these studies against specific inclusion and exclusion criteria. To be qualified for inclusion in the meta-analysis, studies had to satisfy the following criteria: (a) be published in English, (b) have been published within the last 8 years (if published), (c) be quantitative or qualitative empirical studies focusing exclusively on human subjects (excluding meta-analyses or reviews), Duplicate studies, reviews, meta-analyses, editorials, and articles based opinions were excluded from consideration in this meta-analysis.

After thoroughly reviewing the abstracts, studies that appeared to be in alignment with the inclusion procedure and were accessible in full text went through further scrutiny to verify adherence to the criteria. Studies lacking fundamental data such as standard deviations, mean, correlation coefficients, or t-test information necessary for effect size calculations were excluded. Following this assessment, the remaining studies were earmarked for inclusion in the meta-analysis.



3.2 Data Extraction

Every study satisfying the inclusion criteria was subjected to the organization and manual coding as per the data format, which comprised sample size, standard deviations, means, correlations, and t-tests. For every outcome, impact sizes by employing Cohen's d were manually calculated. The statistical evaluation for the meta-analysis was undertaken by applying Comprehensive Meta-Analysis (CMA) software Version 3, the latest version available in 2019. This software, particularly CMA (2019), was applied to perform the computations, approving

various data formats (means, sample size, standard deviations, t-tests, and correlations) for impact size and confidence interval calculations. Following the coding and organization of every study by outcomes and data format, the data were inserted into the spreadsheet interface of CMA (2019) for the computation of the meta-analysis, which comprised data statistics for every study, such as Hedges' g and confidence intervals at a 95% level.

3.3 DATA ANALYSIS

The analysis of data was undertaken by employing the review manager software, a statistical software available for free from the Brown University website. Review manager software simplifies the statistical analysis necessary for systematic meta-analytic reviews by calculating impact sizes for individual studies and presenting graphical results. Furthermore, the software facilitates the coding of studies as per their characteristics and moderators.

3.4 STATISTICAL PROCEDURE AND EFFECT SIZE CALCULATIONS

For studies presenting means and standard deviations, the impact size was determined by computing the standardized mean difference. normally, when studies comprise the comparison of groups on a continuous dependent variable. The equation for calculating the standardized mean difference is outlined as follows:

$$SMD = \frac{Difference\ in\ mean\ outcome\ between\ groups}{Standard\ Deviation\ of\ outcome\ among\ participants}$$

Upon computing the impact size for every study in the sample, initial transformations were conducted to address the possible small sample bias. Successively, the standard error was calculated to determine the inverse variance weights assigned to every study. Employing Review Manager Software under the assumption of a random-impact framework with weighted impact sizes, a composite result was computed. This calculation integrated a 95% confidence interval.

4. RESULTS

Effect sizes, such as mean differences, were assessed by classifying them into three categories: small, medium, and large. Interpretations of impact sizes in the setting of comparing independent means involved metrics such as Cohen's d, and Hedge's g. Specifically, a small effect indicated by 0.20, medium effects by 0.50, and large effects by 0.80. In the case of the hypothesis regarding cyber-attacks and their implication on organizational performance, the weighted standard mean difference was 0.399 (95% CI: -0.165, 0.963).

A meta-analysis of the existing studies generated an overall impact size for cyber dominance in modern warfare: Cyber Attacks and Mitigation, a random impact model, which falls within the small-to-medium range. The standardized mean difference was 0.399 (SE = 0.288, p = .166). Therefore, findings suggested that there was no statistically significant difference in effect size.

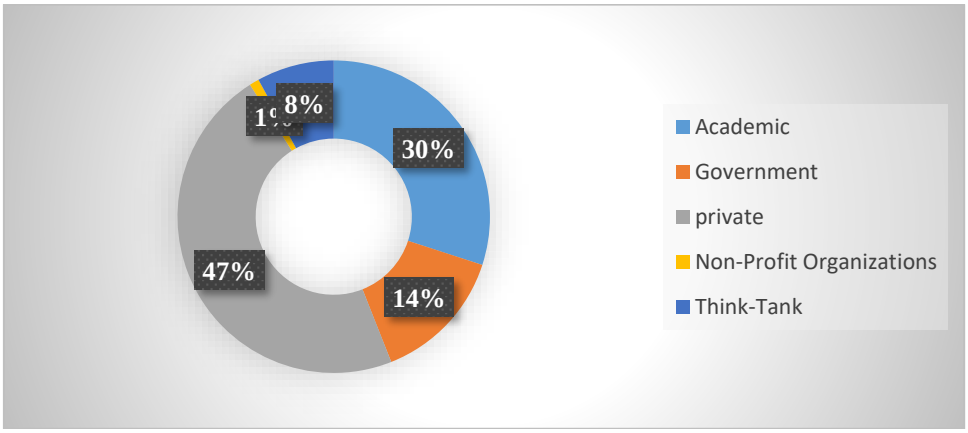


Fig 1: Showcases sources of information for the studies in the Meta-Analysis

The meta-analysis exposed that information for the studies originated from a diverse array of organizations. Particularly, the majority of data (57%) emanated from private software organizations like IBM and security providers such as MacAfee, Symantec, and Kaspersky. Approximately, a quarter of these studies were sourced from academic sources such as Academia, Google Scholar, Science Direct, and Web of Science. The remaining portion, constituting nearly one-fifth, was contributed by governmental institutions, such as *Computer Emergency*

Response Teams (CERTs) and EU-associated bodies, along with non-governmental organizations, such as the World Economic Forum.

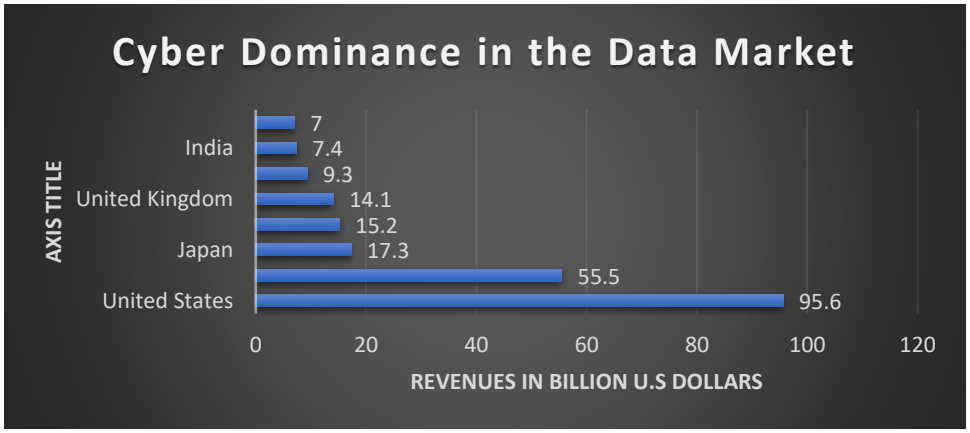


Fig 2: Displays the cyber dominance in the data market.

The figure above showcases the approximated revenue of the data center market in selected nations in 2023, in billion U.S. dollars. From the figure above, America and China are the two biggest markets, with revenues of 95.6 billion and 65.5 billion dollars, respectively. On the other hand, Japan, Germany, the United Kingdom, France, India, and Canada follow, with revenues ranging from 17.3 billion to 7.0 billion dollars. The results demonstrate that America and China are the dominant key players in the data center market, accounting for over two-thirds of global revenue. The other nations on the list are also important markets, but their revenue is significantly lower.

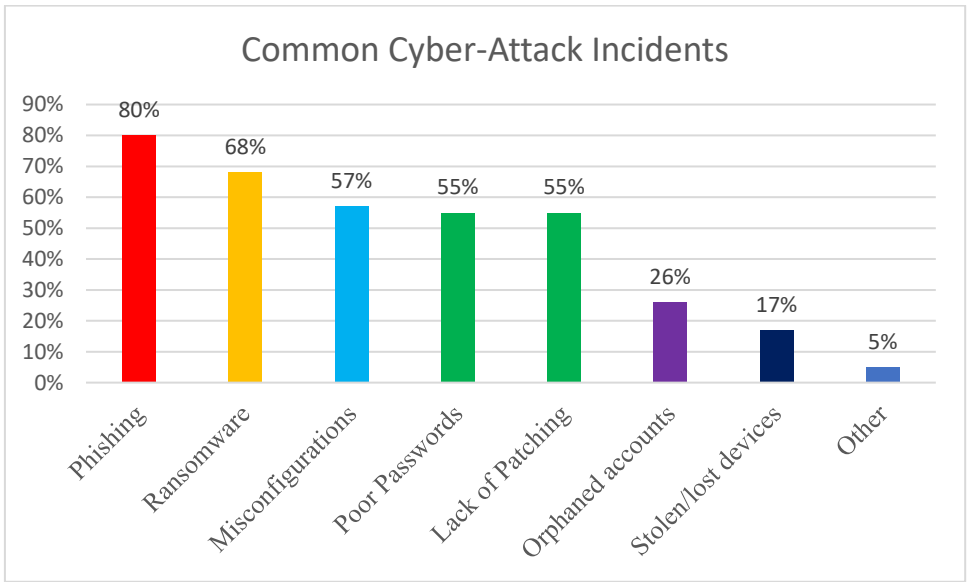


Figure 3: Showcases the Common Cyber-Attack Incidents

From the chart above, it was evident that the top three most common cyber-attacks are: 1) Phishing (68%), 2) Ransomware (68%), and 3) Misconfigurations (57%). According to *Terranova Security* (2023), phishing refers to a type of cyber-attack where the criminal perpetrator sends a fraudulent text message or email that seems to be from a legitimate source, such as a government agency or bank. The text message or email will frequently comprise a link to a malicious website or request the recipient to enter their personal information. On the other hand, ransomware refers to a type of cyber-attack where the cybercriminals encrypt the victim's files and consequently demand a ransom payment in exchange for the decryption key. Ransomware cyber-attacks are very costly and disruptive to businesses and organizations. By contrast, misconfigurations are errors in the configuration of hardware or software that can leave a system vulnerable to attack.

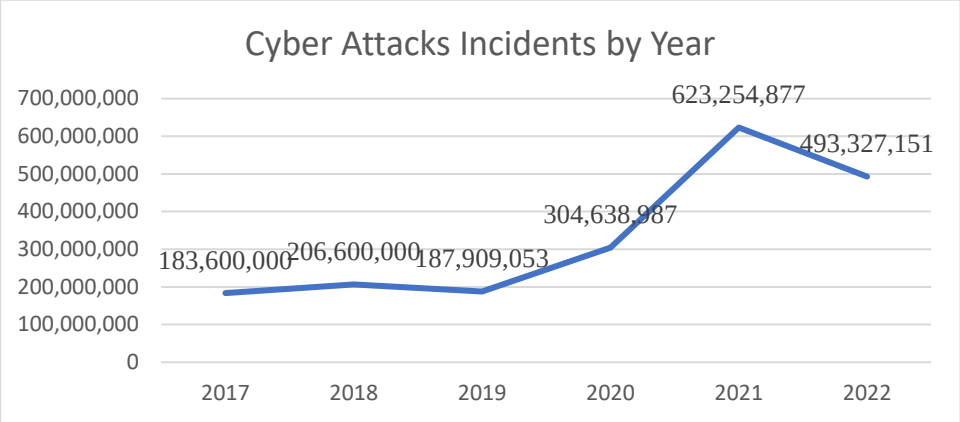


Fig 4: Exhibits Cyber Attacks Incident by Year

The graph shows the number of cyber incidents showcased per year from 2017 (183,600,000) to 2022 (623,254,877). The number of cyber incidents showcased per year is increasing, with a significant increase in 2022. From the analysis, it was evident that there was a widespread consensus across various reports regarding the steady increase in the frequency of cyberattacks globally. As per IBM's findings, in 2022, a typical organization encountered 109 security scenarios that were significant enough to raise genuine concerns. This indicated a notable uptick of 19 scenarios compared to the previous year. Furthermore, it was estimated that approximately 17,000 attacks, coordinated by malicious actors with intentions to disrupt, gather, degrade, deny, or obliterate information system resources or the information itself, occurred.

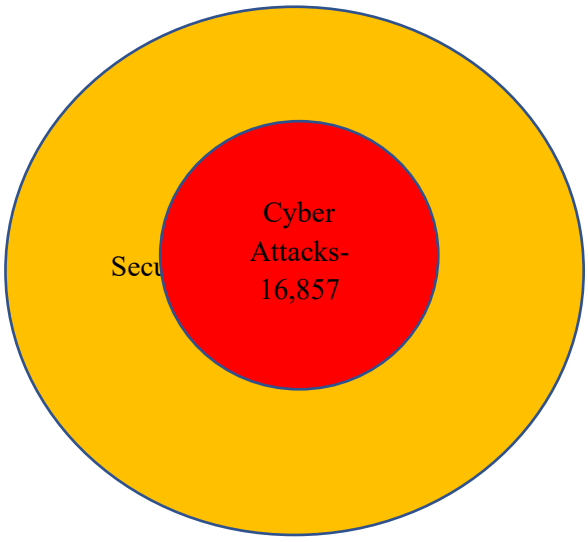


Fig 5: Showcases Cyber Security Events and Cyber Attacks

National Computer Emergency Response Teams have substantiated a consistent noteworthy upward trend in the number of reported scenarios. In the scenario of India, the overall reported scenarios surged from approximately 10,000 in 2021 to well over 70,000 in 2022, marking a remarkable sevenfold increase. Similarly, in Belgium, the reported incidents saw a comparable rise, escalating from 1,389 in 2021 to a total of 9,866 incidents reported in 2022. Meanwhile, data from US-CERT, which solely accounts for incidents reported by federal agencies, indicates a more modest increase, climbing from around 40,000 in 2021 to over 67,000 in 2022. Additionally, CERTs in China and Denmark recorded increases of 50% and over 200%, respectively, underscoring the global nature of this trend.

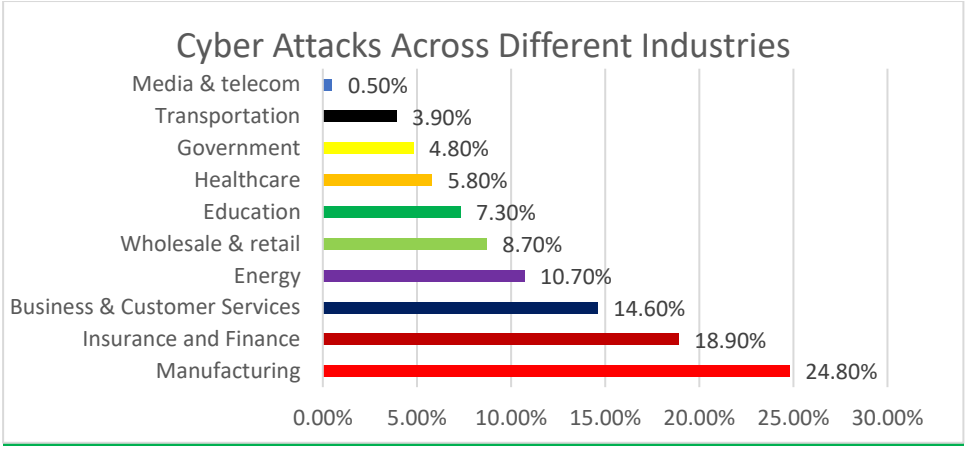


Fig 6: Exhibits Cyber Attacks Across Different Sectors

Referring to the above chart, it was categorical that the manufacturing industry was among the most targeted sectors by cyberattacks in 2022, accounting for approximately 25% of all attacks. The manufacturing sector is considered a major target for cyber attackers since it holds valuable intellectual property and trade secrets. Besides, manufacturing organizations frequently have complex supply chains, which can be exploited by attackers to gain access to sensitive data. Subsequently, finance and insurance was the second most targeted sector (18.9%). The finance and insurance sector is another major target for cybercriminals since it holds sensitive financial data and customer information. Moreover, the business, and consumer services industry (14.6%), is equally targeted by cyber attackers. Businesses activities in this sector frequently depend on third-party vendors, which can introduce security risks.

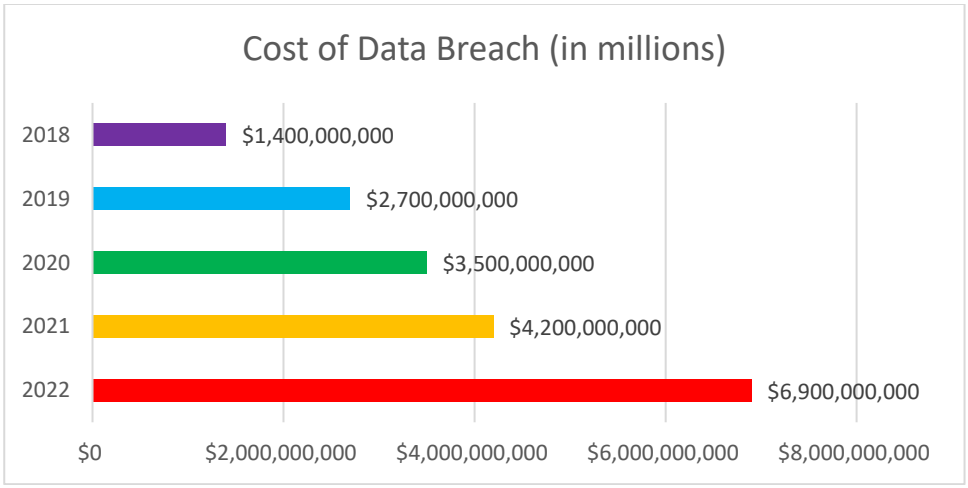


Fig7: Showcases the Cost of Data Breaching

The chart above showcases the cost of data breaches from 2018 to 2022. As displayed in the chart above, it was apparent that the cost of data breaches increased steadily over the past five years. In particular, as of 2018, the average cost of a data breach was $1.4 billion. By 2022, the average cost had escalated to $6.9 billion. Arguably, this is a significant increase, and it demonstrates that data breaches are becoming costlier for businesses and organizations. There is a myriad of factors that can be attributed to the rising cost of data breaches. One factor is the escalating sophistication of cyberattacks. Cybercriminals are consistently developing new and innovative ways to attack organizations and businesses. This makes it more difficult for businesses to safeguard their data, and it also makes it more difficult to recover from a data breach.

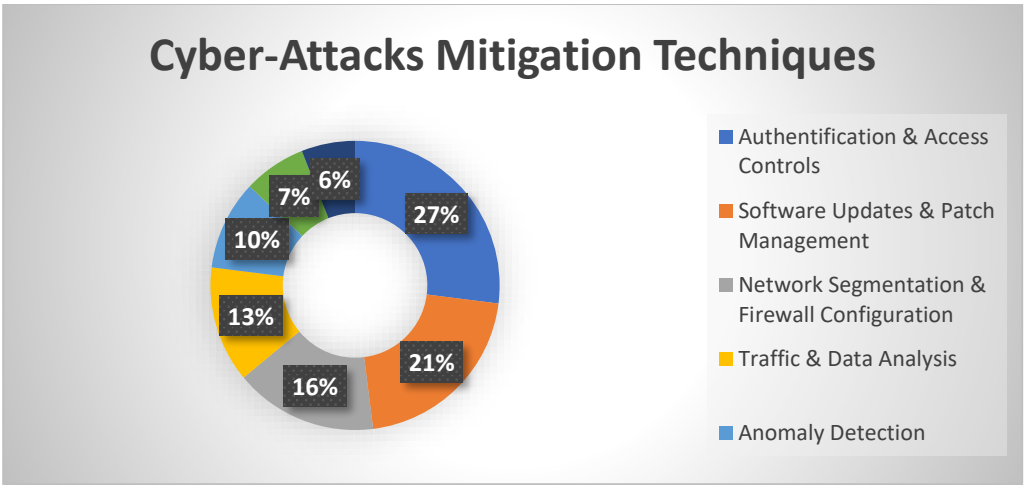


Fig 8: Displays Cyber Attacks Mitigation Strategies

The figure above showcases the utilization of 7 mitigation strategies by different researchers from the analyzed studies, the chart displays the utilization of more than one strategy. From the figure above, the most popular strategy employed was strong authentication and access controls (27%), software updates and patch management (21%), Network segmentation, and firewall configuration (16%). Based on the meta-analysis one technique is inadequate in terms of effectively mitigating Cyber-attacks. A significant volume of studies proposed the implementation of traffic data analysis (13%), with no other method for mitigating the cyber-attacks such as anomaly detection (10%), whitelists (7%), and blacklists. The implementation of these methods was done differently and at different layers and phases. These studies differ in the data presented for analysis, which ranges from logs to web graphs and data from packets.

5. CONCLUSIONS

The prime objectives of this meta-analysis were to explore current research on cyber dominance in modern warfare and pinpoint key attack techniques and mitigation strategies. A systematic literature review was conducted to pinpoint peer-reviewed journal articles and relevant to the research topic published between 2018-2023. From the studies, it was evident that cyber-attacks have been considered the 5th top-rated threat in 2022 and have become the new norm across private and public sectors. Literature review exposed that there was a consensus concerning the substantial costs related to cyberattacks, with a majority of analyses concentrating on big companies the assignment of mitigating cyber-attacks is becoming increasingly challenging because of the expanding array of options available to malicious actors. The significant volume of studies indicated that the execution of robust authentication strategies, such as multi-factor authentication (MFA) could mitigate cyber-attacks. The meta-analysis studies equally ascertained that consistently employing security patches and software updates is instrumental to addressing these vulnerabilities on time. Besides, configuring firewalls to limit unnecessary inbound and outbound traffic helps create a strong defense perimeter and prevents unauthorized communication.

6. REFERENCES

[1]. Aslan, O., and Samet, R., (2018)."Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," *2017 International Conference on Cyberworlds (CW)*, Chester, UK, 2017, pp. 222-225, doi: 10.1109/CW.2017.22.

[2]. Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. Retrieved from https://www.mdpi.com/2076-3417/11/8/3678

[3]. Bamrara, A. (2023). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. Retrieved from https://www.academia.edu/100835187/Cyber_Attacks_and_Defense_Strategies_in_India_An_Empirical_Assessment_of_Banking_Sector

[4]. Boscoianu, M. (2021). Refined Concepts of Massive and Flexible Cyber Attacks with Information Warfare Strategies. Retrieved from

https://www.academia.edu/57722212/Refined_Concepts_of_Massive_and_Flexible_Cyber_Attacks_with_Information_Warfare_Strategies
[5]. Duan, N., Yee, N., Otis, A., Joo, J. C., Stewart, E., Bayles, A., Spiers, N., & Cortez, E. (2021). Mitigation Strategies Against Cyberattacks on Distributed Energy Resources. *IEEE*. https://doi.org/10.1109/isgt49243.2021.9372173
[6]. Gandal, N., Moore, T., Riordan, M., & Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incidents. *Computers & Security*, *133*, 103380. https://doi.org/10.1016/j.cose.2023.103380
[7]. Hasan, M. R. (2022). Cybercrime Techniques in Online Banking. Int. J. of Aquatic Science, 13(1), 524-541. Retrieved from: https://www.journal-aquaticscience.com/article_158883.html (January 2022)
[8]. Khalel, S., & Khudher, S., (2022)."Cyber-Attacks Risk Mitigation on Power System via Artificial Intelligence Technique," *2022 9th International Conference on Electrical and Electronics Engineering (ICEEE)*, Alanya, Turkey, 2022, pp. 117-122, doi: 10.1109/ICEEE55327.2022.9772559.
[9]. Kolesnikov, N. (2023). 50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted. Retrieved from https://www.techopedia.com/cybersecurity-statistics
[10]. Kelemen, R. (2020). Cyber Attacks and Cyber Intelligence in the System of Cyber Warfare. Retrieved from https://www.academia.edu/44681867/Cyber_Attacks_and_Cyber_Intelligence_in_the_System_of_Cyber_Warfare
[11]. Liu, X., Zhang, J., Zhu, P., Tan, Q., & Yin, W. (2021). Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Computers & Security*, *102*, 102138. https://doi.org/10.1016/j.cose.2020.102138
[12]. Hasan, M. R. (2022). Cybercrime Techniques in Online Banking. Int. J. of Aquatic Science, 13(1), 524-
[13]. 541. Retrieved from https://www.journal-aquaticscience.com/article_158883.html
[14]. Pran, R. H. (2022). Business Impact Analysis of Cyber-attacks in Bank by Social Network Analysis and Machine Learning. Retrieved from https://www.academia.edu/92999479/Business_Impact_Analysis_of_Cyber_attacks_in_Bank_by_Social_Network_Analysis_and_Machine_Learning
[15]. Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., … Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Retrieved from https://www.mdpi.com/1424-8220/23/8/4060
[16]. Saad, M., Bukhari, S., and Kim, C., (2019). "A review of various modern strategies for mitigation of cyber-attacks in smart grids," *2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific)*, Seogwipo, Korea (South), 2019, pp. 1-7, doi: 10.1109/ITEC-AP.2019.8903798.
[17]. Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, *24*(12), 1619–1638. doi:10.1080/13669877.2021.1900337 Statista. (2023). *Cyber-attacks: most-targeted industries 2021-2022*. https://www.statista.com/statistics/221293/cyber-crime-target-industries/
[18]. Suzen, A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. Retrieved from https://www.academia.edu/42883345/A_Risk_Assessment_of_Cyber_Attacks_and_Defense_Strategies_in_Industry_4_0_Ecosystem
[19]. Will. (2023). Cyber Risk Evaluation and Mitigation - A Quantitative Research Analysis -. Retrieved from https://researchpod.org/informatics-technology/cyber-risk-evaluation-mitigation