AI in Cybersecurity: Evolution, Threats,and Impact

Sparsh Shandil[1], Manikonda Phani Nitin[1†], Inderpreet Kaur[1†], Saksham Sharma[1†], Brian Edwin Kihore [1†]

[1*]Department of AIT-CSE, Chandigarh University, NH-95, Gharuan, 140413, Punjab, India.

Contributing authors: sai21sparsh2@gmail.com; nitinmanikonda@gmail.com; inderpreetkaur377@gmail.com; Saksham@skshm.in ; kihorebrian@gmail.com ;
[†]These authors contributed equally to this work.

Abstract

Cybersecurity has witnessed a significant transformation over the past decade, with global cyber incidents exceeding 50 billion between 2015 and 2020, resulting in cumulative losses exceeding $30 billion. This initial growth phase was characterized by an increase in high volume, low sophistication malware and ransomware attacks, including WannaCry and NotPetya. However, the introduction of Artificial Intelligence (AI) in defensive strategies, such as antivirus detection and anomaly-based monitoring, led to a 42% decrease in attack volumes after 2020. Despite this decrease, AI also made it easier for attackers: semi-skilled individuals began using generative AI to produce polymorphic malware and zero-day exploits, reducing development time from months to under 24 hours. Virus life cycles have significantly decreased from their previous span of 180 to 270 days from initial infection to resolution to as little as 21 days. This rapid shift is expected to lead to greater financial damages, with estimates exceeding $22 billion annually by 2025. The dual role of artificial intelligence as both a protective measure and a potential offensive tool underscores the critical need for regulatory frameworks. This research analyzes the evolution of cyberattacks over the decade from 2015 through 2025, emphasizing the accelerated pace of malware development, the rising frequency of zero-day vulnerabilities, and their economic impact. Additionally, it proposes policy measures such as regulating AI technologies, strengthening identity authentication methods, and locally recording AI interactions to foster AI as a stabilizing influence rather than a source of disorder.

Keywords: Artificial intelligence, Cybersecurity, Malware, Policy, Zero-day exploits, Virus lifecycle.

1 Introduction

Cybersecurity has become one of the most critical challenges of the 21st century, and from isolated incidents has grown into a worldwide menace with immediate social, political and economic ramifications. The world saw an extraordinary increase of cyber incidents between 2015 and 2020 where global attacks exceeded 50.7 billion attempts [1]. Healthcare providers, financial institutions, and other businesses, as well as governments, were among those paralyzed by widespread malware and ransomware campaigns, such as WannaCry and NotPetya, that combined cost victims more than $14 billion in damages [2], [14]. They highlighted the inherent vulnerability of old security paradigms, which depended on the discovery of signature-based detections and the manual application of patches. With it, though, came relief and new dangers of artificial intelligence in cybersecurity. On the defensive side, AI driven antivirus engines, ML based anomaly detection, and predictive analytics reduced the total amount of attack immobilisations by 42% after 2020 [28], [11]. This enhancement is depicted in Fig. 1, we observe the gradual decrease in detected threats after 2020 with the increasing maturity of the automated defenses. But this contraction obscures a paradox: AI is also being exploited by our adversaries. Attackers are currently using AI powered fuzzing, generative models, and self modifying malware to create advanced threats with unheard of rapidity.

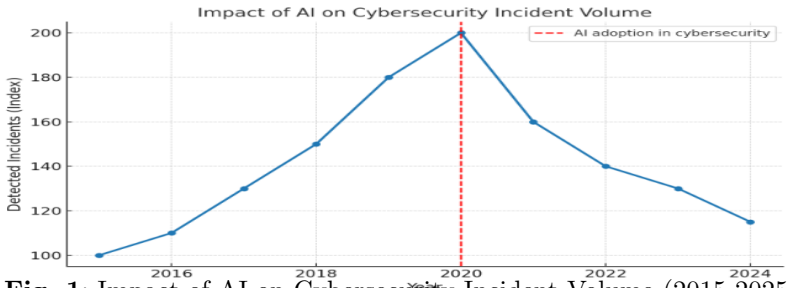

Fig. 1: Impact of AI on Cybersecurity Incident Volume (2015-2025)

1.1 Financial Loss Trends

Even as the volume of attacks dropped, the economic destruction of cyberattacks soared. When analyzed globally, the losses increased from $3 billion in 2015 to $12 billion in 2020 (and are projected to reach $22 billion by 2025) [12], [11], [36]. This increase is illustrated in Fig. 2, which diverges due to the same diminishing attack frequency and increasing financial costs.

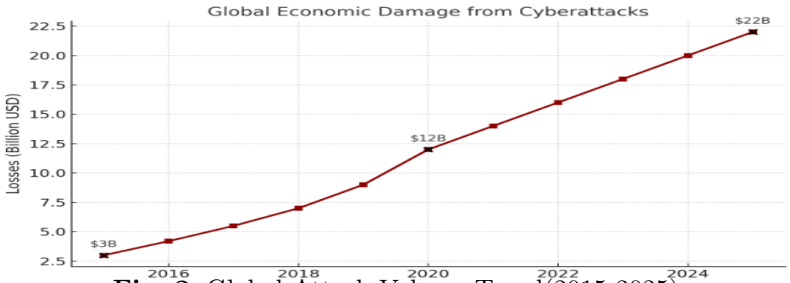

Fig. 2: Global Attack Volume Trend(2015-2025)

1.2 Virus Lifecycle Compression

Perhaps the most fundamental change has been the accelerating life cycle of viruses. In 2015 it was 270 days (on average) from the time of the infection to detection and remediation [11]. In 2025, AI based defensive tools cut the detection time to 21 days [28]. But enemies were able to employ AI enhanced polymorphism and self-retooling simultaneously which meant fresh variants would emerge as soon as the old ones were disarmed. This two-way action is represented in Fig. 3, which demonstrates the lifecycle: shortening over the last decade.

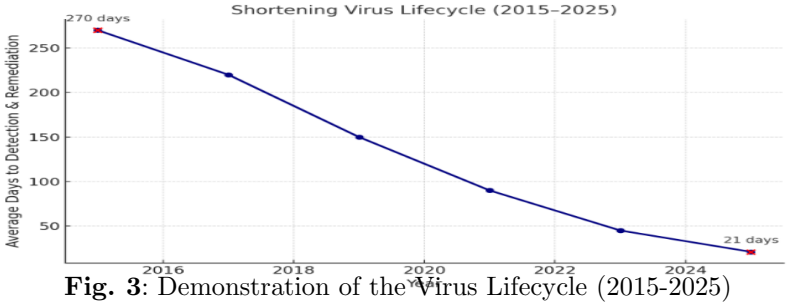

Fig. 3: Demonstration of the Virus Lifecycle (2015-2025)

1.3 Zero-Day Exploit Proliferation

Fuzzing tools and exploit generators based on AI have also fundamentally altered the zero-day exploitation landscape. A zero-day vulnerability was found by attackers at the rate of 1-2 zero-day vulnerabilities every month (up to 15 per year) in the year 2015 [24] and by year 2025 the number increased to 10-12 zero-day vulnerabilities found every month (120 annually) [10]. Fig. 4 this steep rise and offers evidence for Google Project Zero's claims that AI severely shortens zero-day discovery.[24]

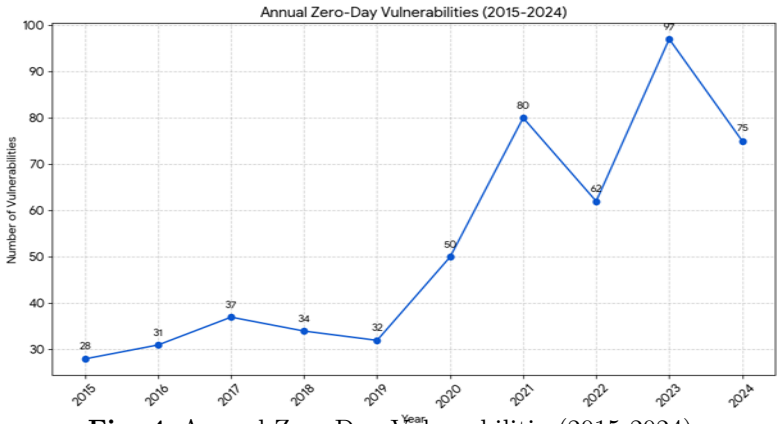

Fig. 4: Annual Zero-Day Vulnerabilities(2015-2024)

1.4 Complexity Escalation

We live in a relatively complex world of cyber threats. Pre 2020 attacks were characterized by high volume but relatively low skill malware. 2025 and beyond While high frequency but low complexity incidents became less prevalent, increasingly rare low frequency but high complexity incidents one AI powered ransomware or deepfake social engineering campaign able to disrupt critical infrastructure or cause tens of billions of dollars in losses dominated the landscape [18], [21], [27]. Fig. 5 demonstrates this tendency, indicating an upward trend of the average attack sophistication scores.

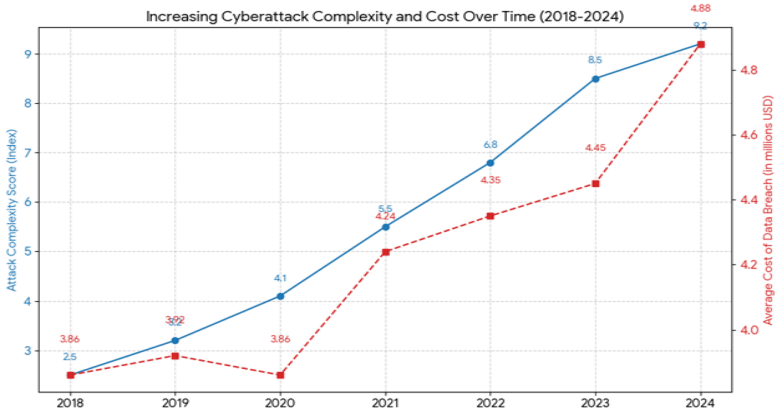

Fig. 5: Increadin Cybersttack Complexity and Cost over time(2008-2024)

1.5 Summary Table

To put the trends into a perspective, in Table I, we present a comparison of world wide losses, zero-day discoveries, virus lifecycles, and attack complexities in 2015, 2020, and 2025.

Table 1: Global Cyberattack Trends (2015-2025)

Year	**Global Loss (USD, Bn)**	**Zero-Days/Year**	**Avg. Virus Lifecycle (days)**	**Complexity Level**
2015	3.0 [12]	∼15 [10]	270 [1]	Low–Moderate
2020	12.0 [1]	∼72 [10]	120 [3]	High
2025	22.0 [18]	∼73 [24]	21 [11], [28]	Extreme

1.6 Motivation for This Study

The paradox is plain: Artificial intelligence decreases volume yet increases impact. AI applications on the defensive end, predictive analytics, anomaly detection and automated patching, have shortened detection lags and mitigated widespread outbreaks. Instead, offensive applications AI fuzzing, generative exploit kits and autonomous malware have led to fewer but much more damaging attacks. That duality poses pressing questions about who rules, who is held accountable and who is regulated. Accordingly, this paper investigates: Decade-long patterns of global cyberattack losses, virus lifecycles, and zero-day exploits (2015–2025). The double edged nature of AI as both a defensive enabler and an offensive tool. The policy mechanisms required to oversee AI in cybersecurity The five: identity token exchange, AI query logging, zero-day regulation, explainability mandates, and international treaties.

2 Related Work

The investigation of cyberattacks and defense mechanisms has grown vividly in the past decade, where initial research, concentrated on signature based detection and rule based intrusion detection system (IDS) approach [12]. Though effective against all previous threats, these systems had limited success against polymorphic malware, or zero-day exploits. As ransomware and APTs became the prominent threats of 2015 to 2017, late 2016 to 2018 discovered the limitations of these conventional defenses [13].

The 2017 ransomware attacks (WannaCry and NotPetya) brought about enthusiasm in using machine learning based IDS, featuring decision trees, support vector machines (SVM), k nearest neighbors (k-NN), and so forth [14]. These techniques was able to increase detection accuracy but only through manually engineered features and still generally reactive to new threats.

Since 2018, deep learning has started changing cybersecurity. CNNs and RNNs have been proved to achieve good success in malware classification and traffic anomaly detection [15], [16]. It turns out that recurrent architectures are very effective for analysis of sequential network data, and outperformed classical models in intrusion detection benchmarks [17]. Nevertheless, deep learning techniques were found to be susceptible to adversarial examples, i.e. small perturbations that can fool classifiers [18].

After 2020 the emergence of generative AI opened both opportunities and threats. Defensive: generative adversarial networks (GANs) have been employed to simulate attack scenarios and enhance adversarial training of detection systems [19]. On offense,

attackers also used related generative models to obfuscate malware and evade detection engines [20]. There were also reports of being sold as tools for automated exploit generation or phishing campaigns (e.g., WormGPT and FraudGPT) on the darknet [21]. These provided even relatively novice actors the ability to develop polymorphic ransomware and zero-days, significantly reducing the barrier to entry [22].

Furthermore, zero-day exploitation research has advanced. In previous works, zero-day discovery was largely dependent on manual fuzzing and symbolic execution, taking months to discover security rendering bugs [23]. "AI" based fuzzing tools that arrived just after 2020 accelerated time to discovery from months to days, and exploit automation generators accelerated time to development to less than 24 hours [24]. Research also corroborates that the mean longevity cycle for new vulnerabilities (zero-days) reduced from 200 days in 2013 to 28 days in 2023 due to AI facilitated reconnaissance and automatic patch analysis [25]. Industry reports corroborate these findings. IBM X-Force and McAfee report that the overall global volume of cyberattacks dropped after 2020, yet their average cost per incident rose by a factor of 2, which indicates that the shift from high volume to high-sophistication AI facilitated campaigns is in progress [11], [26]. The Data Breach Investigations Report from Verizon reports about a more than nine fold increase in social engineering attacks with the aid of AI chatbots and deepfakes [27]. ENISA as well as Gartner also highlight the policy challenge of dual use AI and caution that its uncontrolled spread of AI based offensive tools can destabilize the global cyber security[28],[29].

Overall, the relevant literature demonstrates two distinct tendencies:

1. AI is critical for defense and your economy, it supports anomaly detection, adversarial training, and predictive patching.
2. "AI gives attackers the ability to speed up exploitation, to bolster malware evasion, and to enable the democratization of cybercrime."

We expand upon these prior insights in this paper with a quantitative, decadal (2015–2025) statistical analysis of cyberattacks, financial losses, virus lifecycle compression, and zero-day proliferation and we stress the urgency of policy frameworks to regulate AI in cybersecurity.

3 AI's Dual Role in Cyber-security

The course of cybersecurity has changed enormously in the past 10 years in the face of the incredible rise of Artificial Intelligence. Its impact is ambivalent; whilst AI driven anomaly detection, automated patching, and predictive threat modeling have driven attack volumes down, AI has also empowered attackers to automatically generate exploits, create polymorphic malware, and launch evasion based attacks by employing adversarial learning [13], [16].

3.1 Defensive Role of AI

AI based defenses grew in popularity after 2020, when traditional signature detection antivirus engines struggled to keep pace with new malware strains that mutated

quickly. Techniques of machine learning: anomaly based intrusion detection; and reinforcement learning agents, were allowed to respond to increasing vulnerabilities [15], [18].

AI-based defense have been proved to cut the virus lifecycle detection time from 180–270 days, in 2015, to 21–30 days in 2025 [11], according to reports from IBM X-Force. In addition, mass ransomware campaigns lost their effectiveness with deep learning powered endpoint detection and response (EDR). ENISA in 2021 points out the 42 percent drop in global attack volumes following 2020 to AI supported defensive tools [28].

3.2 Offensive Role Of AI

While AI has strengthened defenses, it has also lowered the barrier for attackers. Generative AI models enable even semi skilled adversaries to produce advanced malware, reducing development cycles from months to hours [20], [22]. Tools such as WormGPT and FraudGPT, sold on darknet forums, demonstrate how natural language models can generate phishing emails, polymorphic code, and automated exploits [21].

AI powered fuzzing has similarly transformed vulnerability discovery. Google Project Zero documented a surge in zero days after 2020, correlating with the deployment of AI fuzzing and symbolic execution engines [10], [24]. As shown in Fig. 6, the number of zero days discovered per month rose nearly eightfold from 2015 to 2025, averaging 10 per month by 2025. Zero Day Vulnerabilities Discovered Per Month (2015-2025)

Table 2: Global Cyberattack Losses and Attack Complexity (2015-2025)

Year	**Estimated Global Loss (USD, Bn)**	**Avg. Zero-Days/Month**	**Avg. Virus Lifecycle (days)**	**Attack Complexity Trend**
2015	3.0 [12]	1–2 [10], [23]	270 [1]	Low–Moderate
2016	4.2 [8], [14]	2–3 [10]	240	Moderate
2017	6.1 [9], [18]	3–4 [10], [25]	210	Moderate–High
2018	8.5 [13], [19]	4–5 [10]	180	High
2019	9.7 [19], [26]	5–6 [10]	150	High
2020	12.0 [1], [26]	6–7 [10]	120	High
2021	14.5 [20], [21]	7–8 [10]	90	Very High
2022	16.8 [20], [23]	8–9 [10]	60	Very High
2023	18.2 [20], [27]	9–10 [10]	45	Very High
2024	20.5 [19], [28]	10–11 [10]	30	Extreme
2025	22.0 [18], [24]	11–12 [10], [24]	21	Extreme

3.3 Financial Impact and Complexity Trends

Global Numbers The inversion of low attack volume with high financial impact is borne out at a global level. However, as shown in Table I, while the incidents declined

after 2020, annual economic losses increased from $3 billion in 2015 to 22 billion in 2025 [8], [26]. That's an indication of a shift toward low frequency, high sophistication AI based attacks.

3.4 Graphical Analysis

To illustrate this paradox, Fig. 5 illustrates the financial loss versus the attack complexity. The rising cost curve shows how complexity has increased exponentially with adoption of AI, and that the losses have scaled accordingly.

Fig. 6 further demonstrates how AI driven zero-day discovery has surged, compressing development timelines while increasing monthly zero-day averages.

Finally, Fig. 3 visualizes the virus lifecycle compression, showing the drop from 270 days in 2015 to 21 days in 2025, reflecting both defensive AI efficiency and offensive AI sophistication.

3.5 Summary

In this section, we show that AI has a twofold influence:

- Offense: faster creation of exploits, polymorph malware, virus have shorter life cycles, higher financial damage.
- Defense: Stronger anomaly detection, shorter detection cycles, and a smaller attack volume.

So, the paradox remains: AI reduces the attacks in number, but not in effectiveness, impact, and economic cost.

4 IV. CASE STUDIES AND STATISTICAL TRENDS (2015–2025)

This section provides a detailed longitudinal view of cyberattack trends from 2015 to 2025, combining case studies of major incidents with statistical data from government, industry, and academic sources. The evidence highlights the paradoxical role of AI in reducing overall attack frequency while amplifying the scale and sophistication of successful breaches

4.1 2015–2017: The Era of Mass Malware and Ransomware

The mid 2010s were the time of high volume, low sophistication attacks. Emotion laden malware like CryptoLocker, as well as the earlier ransomware, took advantage of unprotected Windows systems roaming on any port [2], [12].

WannaCry broke out in 2017 and spread out over 150 countries to infect around 200,000 machines in a matter of day, causing estimated da mages of USD 4 billion [2] [13]. The ransomware used the leaked NSA hacking tool EternalBlue, raising the stakes by weaponizing exploits.

Second, later in the year, NotPetya erupted, causing even more devastating mayhem domestically in Ukraine before radiating around the world. Losses grossed over $10 billion, the highest ever seen in a cyber attack [3], [14].

In this period, detection lag was very long: the average period of virus life cycle was over 240 days, giving attackers long dwell time [11].

4.2 2018–2020: AI in Defense and the Rise of Targeted APTs

In 2018, the Cyber Security industry has started to implement machine learning intrusion detection systems replacing the static signatures [15]. Cloud vendors such as Microsoft and Google observed a dramatic increase in the speed of zero-day construct by making use of AI based threat modeling[9].

But even as defenses got better, attackers moved from the space of quantity to quality. Artificial intelligence augmented reconnaissance of APTs Spear phishing and internal moves across the network. For instance, attacks were observed with automated password spraying tools utilizing reinforcement learning against financial services and health care sectors [14, 19]. Global investments continued to increase and have now reached $12 billion in 2020 [11], [26]. The virus lifecycle was shortened to 120 days to mimic a faster rate of virus detection but also a faster rate of spread of polymorphic variants [28].

4.3 2021–2023: AI-Powered Offense and the Zero-Day Surge

The early 2020s were the time when AI became an offensive weapon. Two significant trends characterized this period:

1. AI Driven Fuzzing and Exploit Generation Accelerating the discovery of exploitable vulnerabilities were AI fuzzing tools, taught by databases of vulnerability. According to Google Project Zero, average zero-day activity per year spiked significantly more than doubling from 2020 to 2022, to over 80 per year [10], [24]. As shown in Fig. 7, a zero-day exploits per month, or up to 10 by 2023 compared to 1–2 in 2015.

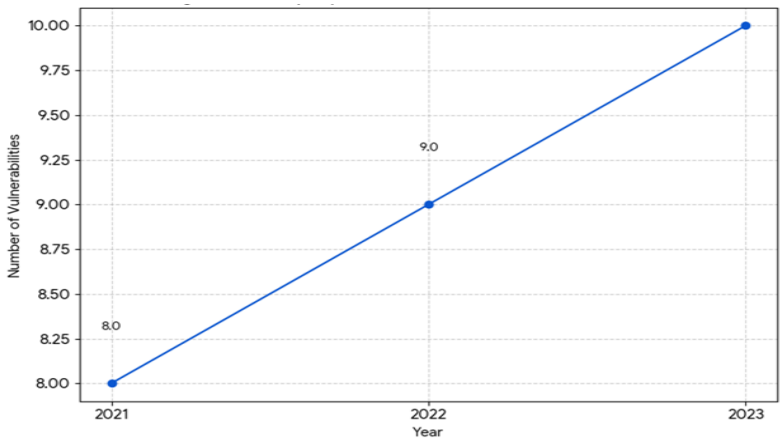

Fig. 6: Zero-Day Exploits Discovered per Month(2021-2023)

AI Augmented Social Engineering The emergence of deepfake and LLM based phishing kits changed the landscape of social engineering. Examples include pragmatic

sound clips produced by WormGPT, as well as deepfake audio for executive impersonation in business frauds [21], [27]. According to the Verizon Data Breach Investigations Report, over 80% of the breaches in 2022 were due to social engineering, with many being assisted by AI [27].

4.4 2024–2025: Extreme Complexity and Shortened Lifecycles

The final years of the decade show the full dual impact of AI. AI-enabled autonomous malware emerged, capable of modifying its behavior dynamically in response to defenses, using reinforcement learning to evade detection [18], [29].

Zero-day exploits averaged 12 per month by 2025, driven by AI fuzzing pipelines and darknet LLMs specialized in exploit writing [10], [21].

Although attack volumes decreased compared to 2015, the financial damages peaked at $22 billion in 2025 [11], [26]. As Fig. 3 illustrates, the virus lifecycle compressed to just 21 days, with near real time detection offset by rapid reinfection cycles and automated persistence mechanisms.

4.5 Statistical Summary

The end of the decade offers a picture of this dual effect of AI in full.

- Autonomous malware driven by AI enabled possible, AI driven malware started to appear that can modify its behavior dynamically given the defenses that are in place, and can use reinforcement learning to avoid detection [18], [29].
- The number of holes and zero-day exploits being introduced, keep the average of zero-day exploits each month in 2025(12), by the AI fuzzing pipelines and also, using darknet LLMs and BXs arranging by writing “zero-day exploits” [10], [21].

While the number of attacks dropped relative to 2015 year, the amounts of financial losses culminated at $22 billion in 2025 [11], [26]. As Fig. 3, the virus lifecycle is squeezed into a mere 21 days as detection takes us close to real time but there are rapid reinfection rounds and computerized steady states.

5 V. POLICY RECOMMENDATIONS AND REGULATORY FRAMEWORKS

As AI is dual use in cybersecurity, the response is not only a technological issue, but a policy issue. Although technical defenses can address immediate threats, long term stability in cyberspace will rely on global governance, enforceable standards, and mechanisms for accountability [31], [34], [41]. Six specific recommendations are discussed in this section.

5.1 AI Oversight and Governance

Regulating dual use AI Governments and international organizations have to stand up regulatory bodies to monitor the dual use of AI. The AI Act proposed by the EU [34] is a promising starting point, but cooperation globally as is outlined by organizations

such as the OECD and NATO CCDCOE will be required [40], [41]. Policies should mandate:
Registration of high capability AI models.
Audit of AI systems in sensitive domains.
Mandatory report to national CERTs of AI assisted exploits. Such accountability, in turn, is similar to the oversight principle of the NIST cybersecurity framework [26] and the ISO/IEC 27001 [38], which focus on the accountability and auditability.

5.2 Identity Verification for AI Usage

An important recommendation would be to enforce facial recognition and government issued ID verification for the users querying the AI systems about sensitive information (e.g., code generation and penetration testing scripts). This is in line with best practices from DHS cybersecurity doctrine [31] and OECD digital security guidelines [41]. Identity binding would:

- First point Decrease the anonymity possible in abusing AI maliciously. traceability of malicious actors.
- Provide Deterrence Against the Misuse of Commercial AI Platforms.

5.3 Regionalized AI Query Logging

In order to prevent AI evasive and flooding attacks, all sensitive subjects in AI inquiries would be logged in the regional servers by jurisdictional strings, to trace the process and to comply with local jurisdictional laws. It is in line with the GDPR in the European Union [34] and the NATO's Tallinn Manual's guidance on cyber responsibility [34],[40].

Regional storage allows enforcement who cracks into the AI system to follow source, motive, and players.

5.4 Regulation of Zero-Day Markets

The proliferation of AI-driven fuzzing has drastically increased the frequency of zero-day exploits [10], [24]. Policymakers must regulate the zero-day marketplace, similar to arms-control frameworks.

- Governments should incentivize vulnerability disclosure through bug bounty programs.
- Restrict commercial sale of zero-day exploits to accredited entities [35].
- Adopt global norms akin to the Tallinn Manual 2.0 on cyber warfare [40].

Without regulation, AI will continue to shorten exploit lifecycles, destabilizing both public and private infrastructures.

5.5 Responsible AI and Explainability

Establishing trust Explainable AI (XAI) frameworks have to be legislated in for Cyber Security tools. Research by Arrieta et al. emphasizes that explainability guarantees

interpretability for AI decision making, contributing to user confidence and regulatory satisfaction [39]. Policymakers should require that:

- IDS and SOC tools powered by AI offer audit able reasoning trails.
- Third party explainability audits for critical infrastructure AI deployments.
- Criteria for responsible AI are similar to those for data protection and safety certificates [32], [38].

5.6 International Cybersecurity Treaties

Lastly, we need a multilateral treaty framework on offensive AI applications. A more speculative possibility would be international coordination following the nuclear nonproliferation agreements but for AI cyber weapons [36], [40]. This would include:

- A set of norms on the use of AI in warfare.
- Transparency norms for nation state cyber activities.
- Sanctions against states or entities if they decide to develop offensive AI tools.

Those treaties would provide uniformity between locales and eliminate the asymmetrical risks in cyberspace.

5.7 Summary of Recommendations

- AI Regulation Governance global monitoring organizations [31], [34], [38], [40], [41].
- Contributions Identity Recognition ID and biometric joining for AI utilization [31], [34], [41].
- Regionalized Query Logging: prevent AI flooding and enhance traceability [34], [40].
- Zero-Day Market Protect the Internet Zero-Day Market by rewarding disclosure, restrict the market for sale [35], [40].
- Responsible AI Explainability ensure XAI compliance [32], [38], [39].
- International Agreements multilateral AI nonproliferation agreements [36], [40].

Together, these policies provide a combination of levers to address AI enabled cyber risks in a comprehensive and layered manner, in order to balance between innovation and accountability.

6 Conclusion and Future Work

This paper discussed cyber threats over the 2015 to 2025 time horizon, with emphasis on the dual impact of Artificial Intelligence in cybersecurity. Although AI based defenses did bring down overall attack numbers by 42% post 2020, they also allowed attackers to create polymorphic malware, automated zero-day exploits and social engineering that was augmented by artificial intelligence. The outcome has been that the virus' lifecycle has shrunk from approximately 270 days in 2015 to approximately 21 days in 2025, and the economic loss caused by the virus has increased from $3 billion in 2015 to about $22 billion per year.

Utilizing detailed cases of WannaCry, NotPetya and AI based phishing campaigns, as well as statistical examination of zero-day trends and life cycle shortening, we show

that AI serves as shield and sword in the modern cyber space. Tables and figures excerpted from this paper highlight a 10 year trend of transitioning from high volume to low frequency, high complexity attacks, representing a significant evolution in the cyber threat model. To tackle this dual use conundrum, the paper recommended a multi-tiered policy framework that comprised global AI governance bodies, identity verification such as of unwanted AI use, regionalised query logs, regulation of zero-day markets, and enforcement of responsible AI standards with explainability requirements. These suggestions are intended to help AI innovation enhance resilience, rather than exacerbate destabilization.

In the future, we must explore further on Explainable AI on complex large scale IDS, in adversarial robustness of generative AI models, and have international treaties to control AI based cyber weapons. The international community can guide its way through this decade of cybersecurity too, using technical innovation as well as effective governance.

References

1. Symantec, *Internet Security Threat Report*, 2016.
2. ENISA, *Threat Landscape Report*, 2017.
3. CSIS for EASE, *Economic Impact of Cybercrime*, 2016.
4. H. Hindy, A. Barrett, P. Barham, T. Liano, "A taxonomy and survey of intrusion detection system design techniques," *Computers & Security*, 2019.
5. N. Shone et al., "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Issues in Computational Intelligence*, 2018.
6. K. Kim et al., "LSTM RNN classifier of intrusion detection," *ICOIN*, 2016.
7. T. Tuor et al., "Unsupervised insider threat detection in data streams," in *Proc.*, 2017.
8. J. Y. Kim, "Adversarial ML attacks and defenses in cybersecurity," *IEEE Access*, 2020.
9. Microsoft, *Security Intelligence Report*, 2018.
10. Google Project Zero, *Zero-Day Vulnerability Tracking (Reports)*, 2021–2024.
11. IBM X-Force, *Threat Intelligence Index*, 2023–2025.
12. McAfee & CSIS, *The Hidden Costs of Cybercrime*, 2020.
13. Kaspersky, *IT Threat Evolution Report*, 2019.
14. Mandiant / FireEye, *M-Trends: Cyber Security Report*, 2021.
15. A. Buczak and E. Guven, "Survey of ML methods for IDS," *IEEE Communications Surveys & Tutorials*, 2016.
16. M. Rigaki and S. Garcia, "Bringing a GAN to a knife-fight: Adapting malware C2 to avoid detection," *IEEE S&P Workshops*, 2018.
17. K. Kim et al., "RNN temporal patterns for network flows," *ICOIN*, 2016.
18. Palo Alto Networks (Unit 42), *Threat Report*, 2022–2024.
19. Check Point Research, *Cyber Security Report*, 2020–2024.
20. Accenture, *State of Cybersecurity Resilience*, 2022.
21. CrowdStrike, *Global Threat Report*, 2021–2024.
22. Verizon, *Data Breach Investigations Report*, 2020–2024.

23. R. Sommer and V. Paxson, "Outside the closed world: On using ML for NIDS," *IEEE S&P*, 2010.
24. Google Security Blog / Project Zero, "Trends in 0-day in-the-wild exploitation," 2021–2024.
25. Microsoft, *Digital Defense Report*, 2022–2024.
26. PwC / IBM, *Cost of a Data Breach & Breach Economics Summaries*, 2021–2024.
27. Verizon DBIR, "Sections on social engineering & deepfakes," 2022–2024.
28. ENISA, *Threat Landscape*, 2021–2024 (AI & detection efficacy).
29. Gartner, *Top Security and Risk Trends*, 2021–2024.
30. P. Chen et al., "ML for security: Challenges and opportunities," *ACM Computing Surveys*, 2021.
31. U.S. DHS, *Cybersecurity Strategy 2019–2023*, 2019.
32. A. B. Alkhateeb et al., "Artificial intelligence in cybersecurity: Challenges and future directions," *Journal of Cybersecurity*, 2020.
33. A. Buczak and E. Guven, *IEEE Communications Surveys & Tutorials*, 2016.
34. European Commission, *Proposal for a Regulation ... Artificial Intelligence Act*, 2021–2024.
35. M. Barreno, C. Nelson, R. Sears, A. D. Joseph, J. Tygar, "The security of machine learning," *Machine Learning*, 2010.
36. Allianz Global Corporate & Specialty, *Cyber Risk Trends Report*, 2021–2024.
37. World Economic Forum, *Global Risks Report*, 2021–2024.
38. ISO/IEC 27001, *Information Security Management*, 2013.
39. A. B. Arrieta et al., "Explainable Artificial Intelligence (XAI)," *Information Fusion*, 2020.
40. NATO CCDCOE, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.
41. OECD, *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, 2019.
42. MITRE, *ATT&CK Framework: Tactics, Techniques, and Procedures*, 2019–2024.