

# AI-Driven Cybersecurity Threats: A Survey of Emerging Risks and Defensive Strategies

Sai Teja Erukude<sup>1</sup>, Viswa Chaitanya Marella<sup>2</sup>, and Suhasnadh Reddy Veluru<sup>2</sup>

<sup>1</sup> Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India  
[erukude.saiteja@gmail.com](mailto:erukude.saiteja@gmail.com)

<sup>2</sup> Vellore Institute of Technology, Vellore, Tamil Nadu, India  
[viswachaitanyamarella@gmail.com](mailto:viswachaitanyamarella@gmail.com)  
[suhasnadhreddyveluru@gmail.com](mailto:suhasnadhreddyveluru@gmail.com)

**Abstract.** Artificial Intelligence's dual-use nature is revolutionizing the cybersecurity landscape, introducing new threats across four main categories: deepfakes and synthetic media, adversarial AI attacks, automated malware, and AI-powered social engineering. This paper aims to analyze emerging risks, attack mechanisms, and defense shortcomings related to AI in cybersecurity. We introduce a comparative taxonomy connecting AI capabilities with threat modalities and defenses, review over 70 academic and industry references, and identify impactful opportunities for research, such as hybrid detection pipelines and benchmarking frameworks. The paper is structured thematically by threat type, with each section addressing technical context, real-world incidents, legal frameworks, and countermeasures. Our findings emphasize the urgency for explainable, interdisciplinary, and regulatory-compliant AI defense systems to maintain trust and security in digital ecosystems.

**Keywords:** AI-Driven Cybersecurity, Cybersecurity Threats, AI-Enhanced Scams, Legislative Responses

## 1 Introduction

AI allows new vulnerabilities in cybersecurity. Criminals, adversaries, and malicious actors use AI and other technologies to circumvent detection systems and automate attacks with minimal human intervention. The dual-use nature of AI raises major risks in the areas of cybersecurity, privacy, and public trust from those who exploit AI as a technological advancement for malicious use.

This study will discuss the growing cybersecurity risks that AI is creating, including deepfakes, adversarial attacks on machine learning models, and automating malware generation. We will demonstrate the increasing emergence of AI-facilitated social engineering attacks, including phishing and fraud, as well as a risk we call data poisoning, where an adversary can manipulate training data to compromise AI systems. Through case studies and discussion about defensive strategies and regulations, we hope to illustrate the lack of guarantees on a future response and the necessity of enforcement in the legal and technological response they need to defend against future vulnerabilities and risks.

### 1.1 Survey Methodology

The survey evaluated over 70 academic, industrial, and regulatory publications from 2017 to 2025, including peer-reviewed journals, preprint repositories, cybersecurity advisories, and whitepapers, and validated media outlets. The main selection criteria included: relevance to the threats of AI systems, such as deepfakes, adversarial attacks, automated malware, and AI-enabled scams; real-world solutions include case studies, toolkits, and frameworks (2019-2025); authority and credibility of sources, including governmental agencies.

### 1.2 Comparative Taxonomy of Threats and Solutions

Table 1 summarizes primary AI-driven threats mapped to attack modalities and defense strategies and forms the backbone of the subsequent sections.

**Table 1.** Taxonomy of AI-Driven Cybersecurity Threats and Corresponding Defensive Strategies

Threat Category	Attack Vectors / Tools	Real-World Incidents	Defensive Strategies
Deepfakes & Synthetic Media	GANs, Voice Cloning, Face Swaps, Text-to-Video	Political deepfakes in Canada, AI-generated scams with celebrity voices [1], [2], [3]	XAI frameworks (n-gram analysis), wavelet-based detection, human-in-the-loop review, regulation (Digital India Act)
Adversarial AI Attacks	FGSM, PGD, C&W, CleverHans, ART Toolkit, Poisoning	Adversarial image classification errors, model evasion in CAVs [8], [14], [15]	Adversarial training, Defensive distillation, Gradient masking, Certified robustness
Automated Malware Generation	FraudGPT, WorgmGPT, Polymorphic Engines, Obfuscators	AIIMS Ransomware (2022), WannaCry, BlackMamba AI malware [20], [22], [21]	EDR/XDR systems, AI-based behavior monitoring, automated incident response, UEBA
AI-Powered Phishing & Scams	LLM-generated phishing, Deepfake voices, Chatbots	Pig Butchering scams, CEO voice fraud via AI [27], [28], [29]	Weighted linguistic pattern detection, biometric authentication, scam detection models
Social Engineering Automation	AI Chatbots, Synthetic Identities, Face + Voice Deepfakes	\$25M Hong Kong executive fraud via Zoom deepfake, AI-driven dating scams [27]	User education, deception detection software, image/audio verification, digital literacy

## 2 Deepfakes and Synthetic Media

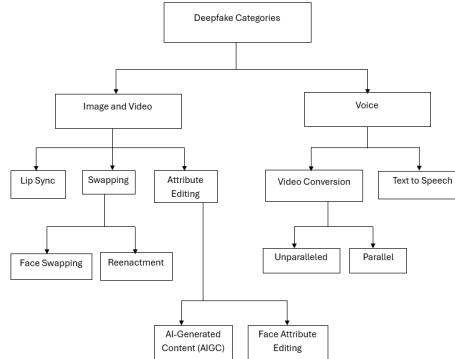
### 2.1 The Rise in Deepfake Proliferation

The rapid growth in AI-generated content has caused obstacles in industries, with the number of deepfake incidents rising tenfold worldwide from the year before [1]. North America, followed by the Asia-Pacific and Europe, experienced increases of 1740%, 1530%, and 780%, respectively, with identity fraud, mostly

about ID cards, being involved in almost 75% of cases. 20% of Americans have fallen for scams utilizing AI-generated celebrity endorsements, rising to 33% for 18-34 year-olds [2]. 1 in 4 Canadians encountered fake political content in the lead-up to the April 2025 election, including deepfake videos that erroneously show Prime Minister Mark Carney endorsing scams [3]. The estimated rate of such attacks has been pegged at happening every five minutes.

## 2.2 Detection Challenges and Observations

Despite advancements in detecting deepfakes, current systems have serious limitations related to robustness and generalization. Benchmarks such as the “Deepfake-Eval-2024” exhibit significant drops in the AUC score for video (50%), audio (48%), and image (45%) in uncontrolled, real-world conditions [4]. Many deep learning models rely on surface artifacts or background cues and thus are rendered ineffective when faced with sophisticated fakes. Wavelet-transformed feature extraction [5], [6], shows promise to improve explainability and accuracy, but is still vulnerable to context, lighting, or language changes. Most deepfake detection systems are black box models and are subject to adversarial spoofing. Human-in-the-loop approaches have improved current detection capabilities, but the lack of a multi-modal approach and systematic enforcement of laws allows detection systems to be subject to zero-day manipulations and societal harm. As shown in Figure 1, deepfakes encompass various forms, from manipulated video and audio to text and image-based fakes, highlighting the scope of challenges faced by detection frameworks



**Fig. 1.** Different categories of deepfakes

## 2.3 Legal and Ethical Dimensions

In the United States, only 14 states have passed anti-non-consensual sexual deepfake content laws, and only 10 have some restrictions on deepfakes relating

to political campaigns. A bipartisan bill introduced in January 2024 aims to allow victims to sue the creators or distributors behind non-consensual sexual deepfake content, but with jurisdictional nuance that prevents legislated enforcement, due to ambiguity. India does not have specific deepfake laws, but some action can be taken under the Indian Penal Code and the Information Technology Act, and according to the Minister of State, AI-related regulations are coming under the new Digital India Act. South Korea has criminalized the distribution of so-called harmful deepfakes to the public interest under the premise of Article 245 of the Criminal Act, punishable by up to five years and/or a fine of 50 million won ( $\approx \$43,000$ ). With evolving regulatory regimes and proposed laws, it is vital to accelerate public understanding of deepfake AI tools and to pursue change to combat the threat of deepfake fraud and manipulation.

### 3 Adversarial AI Attacks

#### 3.1 Understanding Adversarial AI attacks

Adversarial AI attacks refer to the perturbation of input data and methods that target weaknesses in AI models to produce incorrect or unwanted output. In this study, we argue that adversarial machine learning is the study of how adversarial examples (intentionally crafted input data) can successfully manipulate machine learning classifiers. When an adversary applies some perturbations to data at inference time to trick a trained model, the attack is called an evasion attack. In contrast, data poisoning is an adversarial attack where malicious samples are introduced into the training data to “poison” the model and degrade its performance. This mechanism can be applied to any AI system and raises doubts regarding AI systems’ reliability in safety-critical applications [8].

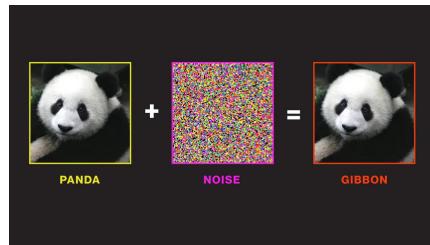
#### 3.2 Attack Methods and Tools

Adversaries have a variety of approaches for creating adversarial instances. For example, two common gradient-based approaches that provide undetectable perturbations to fool neural networks are the Fast Gradient Sign Method (FGSM) [9] and Projected Gradient Descent (PGD) [10]. More advanced approaches like the Carlini & Wagner (C&W) attack can produce subtle and effective inputs that may go undetected [11]. There are also multiple open-source frameworks that researchers and hackers have developed to assist with these attacks. For example, IBM’s Adversarial Robustness Toolbox (ART), CleverHans [12], and Foolbox [13] have dozens of attack algorithms in the image, text, and audio domains. The impact of adversarial manipulations is illustrated in Figure 2, which visualizes how attackers perturb input data to deceive AI models.

#### 3.3 Defense Strategies

Researchers have referred to the defense against adversarial attacks as an “arms race” between the attacker and defender. Some key defense strategies are:

- **Adversarial Training:** Retraining models with adversarial examples seems to be the most developed and most successful defense strategy.
- **Defensive Distillation:** Trains a secondary model on softened outputs to create smoother decision boundaries, increasing resistance to adversarial attacks, though adaptive threats may still bypass it [16].
- **Adversarial Input Detection:** Identify and block adversarial inputs or escalate them for human review [16].



**Fig. 2.** Adversarial attack manipulation

### 3.4 Legal Perspectives: India and International

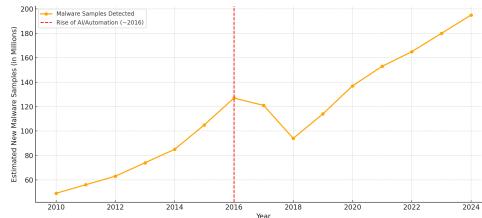
India does not have any specific legislation governing cybersecurity risks from AI systems. The IT Act 2000 does not include emerging threats like data poisoning, and adversarial attacks will be prosecuted as a general cybercrime. The EU is ahead with its likely legislation; the draft AI Act indicates that high-risk AI systems have to prove they can withstand adversarial manipulation. The US continues to issue more guidelines than enforceable legislation, but the National Institute of Standards and Technology (NIST) is expected to release its adversarial threat defense recommendations in 2024. China is expected to propose limitations on the misuse of AI systems such as deepfakes. However, it is important to note that there have been no global laws governing adversarial AI.

### 3.5 Critical Synthesis and Observations

The space lacks a standardized approach to defending against attacks. Adversarial training is expensive and non-scalable. Defensive distillation or gradient masking have been proposed as low-cost, lightweight security measures, but they also have known vulnerabilities in adaptive attacks. The research community has developed a shared understanding that there are no “silver bullets” and requires layered, context-specific security models. Points of divergence remain evident regarding the trade-offs among accuracy, interpretability, and robustness.

## 4 Malware Generation and Automation

Modern malware commonly has polymorphic or metamorphic code, meaning it can change its structure without changing its underlying functionality, allowing the code to elude signature detection. New aspects of malware, such as obfuscation, and services like Malware-as-a-Service have made disseminating malware easier and detection harder. Generative AI extends this further and gives attackers the ability to generate or obfuscate malicious code automatically. Figure 3 illustrates that the difficulty posed by malware has become exponentially more complex since 2016, almost doubling [17].



**Fig. 3.** Global malware sample growth from 2010 to 2024

### 4.1 Tools Available to Criminals for Malware Creation and Delivery

**Crimeware frameworks:** Kits like Blackhole and Nuclear Pack [18] automate the creation and delivery of malware, and both have anti-detection and exploit toolkits [19]. Malware-as-a-Service sites make crime easier by creating a subscription-based model for malicious code and services.

**Botnets and automated delivery:** Botnets allow the delivery of malware and spam at a massive scale by taking advantage of networks of connected devices. The Mirai malware, for instance, infects IoT devices that use default credentials and creates a botnet to spread the malware. Other spam botnets like Emotet and TrickBot infect users by sending phishing emails.

**Obfuscation tools, and polymorphic engines:** Polymorphic malware changes its appearance every 30-60 seconds, producing a unique instance, thereby bypassing signature-based detection [18], [20]. Table 2 provides descriptions and common usages of widely deployed software obfuscation tools, highlighting their dual role in both legitimate software protection and malicious code evasion.

**AI and ML-Driven Tools:** Tools like FraudGPT and WormGPT enable even those lacking technical skills to use AI to launch phishing campaigns and undetectable malware attacks.

### 4.2 Recent Automated or Generated Malware Cases

- **WannaCry Ransomware (2017):** WannaCry is one of the first large-scale malware outbreaks to include automated distribution, and leveraged a

**Table 2.** Descriptions and common usages of various software obfuscation tools

Tool Name	Description	Common Usage
Themida	Commercial Protector combines packing and more.	DRM protection, malware obfuscation
VMProtect	Virtualizes and encrypts code execution flow.	High-end, DRM, software licensing
ConfuserEx	.NET protector with renaming, and resource encryption.	Malware, software IP protection
ProGuard	Java-based, shrinks, optimizes, and obfuscates bytecode	Android and app protection
JavaScript Obfuscator	Encrypts and inserts dummy JavaScript code.	Malicious web scripts, phishing campaigns

worm-based distribution process to propagate without human intervention. It infected more than 300,000 systems across more than 150 countries, with 48,000 in India alone, and has been estimated to have caused damages in the billions of dollars. The rapid, automated propagation of WannaCry used the EternalBlue vulnerability to overwhelm various defenses and make a timely and effective response and containment almost impossible [21].

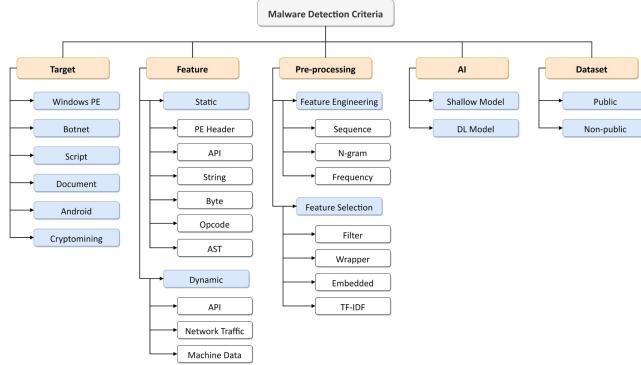
- **AIIMS Hospital Ransomware Attack (2022):** AIIMS Delhi was attacked with ransomware in November 2022 that encrypted 1.3 TB of data and impacted operations for multiple weeks. Due to ineffective network segregation, malware spreads across the network automatically. The October 2022 attack was likely ransomware-as-a-service and highlighted critical vulnerabilities in the cybersecurity posture of healthcare organisations [22].

### 4.3 Defensive Technologies Against Automated Malware

Organizations are increasingly adopting multi-dimensional, AI-enhanced defenses against rapidly evolving threats:

- **Antivirus and Heuristics:** AVs have introduced ML and behavioral heuristics for signature detection and to detect unmapped malware [20].
- **Endpoint Detection and Response (EDR):** EDR tools continuously observe behaviors on systems and identify anomalous behavior [23].
- **Extended Detection and Response (XDR):** XDR examines data across endpoints and networks to identify complicated, multi-staged attacks.
- **AI-Based Threat Detection:** ML can process massive amounts of telemetry and detect anomalies and zero-day threats in real-time.
- **Behavioral Analytics:** UEBA can observe a user's and system's behavior, and identify anomalies that may indicate malware activity, even when there is no prior knowledge of the malware [24].
- **Automated Incident Response:** Playbooks are implemented to isolate compromised endpoints or to disable accounts and quickly contain threats.

The analytical pipeline of modern malware detection, including feature extraction, AI models, and dataset utilization, is summarized in Figure 4.



**Fig. 4.** Malware Detection based on Target, Features, Pre-processing, AI, and Dataset.

#### 4.4 Legal and Law Enforcement Responses

Cybersecurity law in India is a function of the IT Act, 2000, the Indian Penal Code (IPC), and the Digital Personal Data Protection Act (DPDPA), 2023 [25]. The DPDPA mandates data protection and penalties for breaches. The CERT-In Guidelines, 2022, require incident reporting within 6 hours for critical sectors [26]. However, these frameworks do not address AI-generated malware (WormGPT, FraudGPT) or the ethical challenges of dual-use AI systems. Addressing these gaps may include expanding the definitions of the IT Act to include AI misuse, holding developers accountable. India could also benefit from cybercrime-specialized courts, digital forensics training for law enforcement, and mandatory AI risk assessments for critical systems.

#### 4.5 Critical Synthesis and Observations

Overall, research is advancing toward AI being an effective option for anomaly detection; however, there is still some division regarding explainable AI and trust. Also, an asymptotic dance has begun between obfuscation (adversarial) methods and disengagement (heuristic) systems. Meanwhile, regulatory frameworks like India's DPDPA regarding managing the risk of models of renaissance AI, and CERT-In, mention avoiding risk referred to earlier, but do not offer an answer on how to deal with autonomous, and or self-modifying malware.

### 5 Automation of AI-powered Scams

#### 5.1 Phishing attacks

With advancements in text-to-speech diffusion models, an attacker can clone a target voice in less than 30 seconds of source audio. The synthesized voice is then conveyed over VoIP or conferencing services, exploiting “authority bias” while also bypassing traditional email-centric phishing filters. Recent high-profile

incidents involving AI-driven voice cloning are outlined in Table 3, illustrating the significant financial and operational impacts across sectors.

**Table 3.** Representative voice-cloning-enabled social-engineering incidents (2019–2025)

Year	Loss	Victim	Exploit Vector	Short Take-away
2019	US\$243 k	UK energy subsidiary	Deepfake audio of German CEO pressured CFO to expedite supplier payment	First widely reported AI-voice BEC; payment reached Mexico via Hungary shell account [30]
2020	US\$35 m	UAE bank (HK branch manager)	Cloned director's voice plus forged e-mails convinced manager to authorise 17 wire transfers	Multi-modal spoofing (audio + e-mail) scaled to eight-figure fraud [31]
2024	US\$25 m	Multinational (Hong Kong)	Full-body video deepfakes of CFO and colleagues in Zoom meeting	Liveness cues can be faked; triggered regional regulatory review [32]
2025	≤US\$20 m	Retail crypto investors	YouTube “live” streams of deep-fake Elon Musk promising double-your-money giveaways	Convergence of celebrity deepfakes and mass-phishing; >15 verified channels detected [33]

Explainable AI frameworks, such as the weighted n-gram analysis [7], can be adapted to detect linguistic patterns. By analyzing the similarities between known phishing attempts and unseen ones, this framework provides insights to identify and mitigate phishing campaigns.

## 5.2 Personalized Social Engineering Attacks

AI is changing social engineering by allowing bad actors to deploy personalized fraud attacks with frightening specificity. In a case more recent to Hong Kong, criminals deployed AI to commit fraud, involving deepfake video calls to impersonate executives and even romantic partners [27]. Victims described attending Zoom-style meetings where the entity on the other side appeared and blinked and smiled and spoke in familiar voices; all of this was fake to gain trust, encourage them to invest in the fake business opportunity, or provide sensitive data. One poor victim lost more than \$25 million when they thought they were attending a virtual meeting with the CFO of their own company.

## 5.3 Pig Butchering Scams

Pig butchering scams are long-term frauds where scammers develop levels of trust, often while pretending to be a romantic partner or financial advisor, before persuading them to deposit money, usually into cryptocurrency exchanges.

The term pig butchering refers to “fattening up” the victim emotionally before “slaughtering” them financially. In 2024, scammers engaged multiple victims at the same time with AI chatbots, ensuring the emotional tone and language fluency stayed the same through consistency [28]. The use of AI-generated images as well as video messages increased the scammers’ credibility. One particular case detailed a U.S. tech executive defrauding him of \$1.2 million by using a realistic, AI-generated crypto platform using fake market data and customer assistance, which was gone when he tried to withdraw money.

#### 5.4 Automation

The real danger of AI in cybercrime is that it’s now possible to automate complex and large-scale scams. With AI, criminals can operate at a level of realism that enhances the social engineering experience for victims. For example, in a U.S.-documented pig butchering scam, an AI chatbot called “Evelyn” had a months-long romantic conversation with a target while sending automated AI-edited selfies of itself and pre-recorded videos, all of which were for a fake crypto exchange [29]. AI has reduced human involvement, enabling scalable fraud.

### 6 Future Work

Several promising directions for future research have emerged from this survey that require collaboration with AI researchers, cybersecurity practitioners, and government officials to create adaptable environments for our digital systems.

- **Multi-Modal Explainable Detection Pipelines:** Develop architectures that can classify video, audio, text, and image data and balance robustness and interpretability.
- **Adaptive Threat Simulation and Benchmarking Platforms:** Create a standardized testing configuration across the public data to evaluate security models across diverse modalities and simulate zero-day threats.
- **Cross-Jurisdictional AI Risk Governance:** Support technical and legal communities in advancing regulatory frameworks across jurisdictions to bridge the disconnect between rapid AI innovation and policy landscapes.

### 7 Conclusion

AI has introduced a new era of cybersecurity challenges by morphing the threats into layered, intelligent, and scalable attack vectors. This paper has examined four types of AI-driven threats: deepfakes, adversarial attacks, automated malware, AI phishing, and AI social engineering. Collectively, we observe the evolving potential of adversarial actors to use generative, personalized, and autonomous capabilities to exploit traditional security-based infrastructure. Table 4 provides a summary of key recommendations for the threats discussed.

**Table 4.** Summary of Threats, Gaps, and Suggested Interventions

Threat Category	Key Gaps	Recommended Responses
Deepfakes	Weak generalization, legal enforcement gaps	Human-in-loop detection, public awareness, AI content watermarking, regulatory acceleration
Adversarial AI	No universal defense, expensive adversarial training	Layered security, XAI, context-aware models, resilient model certification
Malware Automation	Obfuscation bypasses signature detection	Real-time AI anomaly monitoring, developer accountability
Phishing & Scams	Hyper-personalized attacks, low user vigilance	Weighted n-gram filtering, continuous user education, voice biometrics
Social Engineering	Cross-modal deception, emotional manipulation	Real-time verification, scam simulation training, AI reporting portals

## References

1. Sumsup, Sumsup Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023. <https://sumsup.com/newsroom/sumsup-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/>.
2. McAfee Corporation, McAfee's 2024 Global Holiday Shopping Scams Study Highlights Growing Concerns Over AI-Powered Scams, Including Deepfakes, Impacting Holiday Shoppers. <https://www.mcafee.com/en-us/consumer-corporate/newsroom/press-releases/2024/20241121.html>.
3. The Express Tribune, Fake political social media content spikes in Canada ahead of elections. <https://tribune.com.pk/story/2540932/fake-political-social-media-content-spikes-in-canada-ahead-of-elections>.
4. Chandra, N. A., Murtfeldt, R., Qiu, L., Karmakar, A., Lee, H., Tanumihardja, E., ... & Etzioni, O. (2025). Deepfake-eval-2024: A multi-modal in-the-wild benchmark of deepfakes circulated in 2024. arXiv preprint arXiv:2503.02857.
5. Erukude, S. T., Joshi, A., & Shamir, L. (2024). Identifying Bias in Deep Neural Networks Using Image Transforms. Computers, 13(12), 341.
6. Erukude, S. T. (2024). Identifying Bias in CNN Image Classification Using Image Scrambling and Transforms (Doctoral dissertation, Kansas State University).
7. Joshi, A., Erukude, S. T., & Shamir, L. (2025). Explainable identification of similarities between entities for discovery in large text. Future Internet, 17(4), 135.
8. Viso. Attack methods: What is adversarial machine learning? <https://viso.ai/deep-learning/adversarial-machine-learning>.
9. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.
10. Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2017). Towards deep learning models resistant to adversarial attacks. arXiv preprint arXiv:1706.06083.
11. Carlini, N., & Wagner, D. (2017, May). Towards evaluating the robustness of neural networks. In 2017 ieee symposium on security and privacy (sp) (pp. 39-57). Ieee.
12. Papernot, N., Faghri, F., Carlini, N., Goodfellow, I., Feinman, R., Kurakin, A., ... & McDaniel, P. (2016). Technical report on the cleverhans v2. 1.0 adversarial examples library. arXiv preprint arXiv:1610.00768.
13. Rauber, J., Brendel, W., & Bethge, M. (2017). Foolbox: A python toolbox to benchmark the robustness of machine learning models. arXiv preprint arXiv:1707.04131.

14. HiddenLayer, Unpacking the AI Adversarial Toolkit. <https://hiddenlayer.com/innovation-hub/whats-in-the-box>.
15. Hao, K. (2019). How we might protect ourselves from malicious AI.
16. Oleszak, M., Neptune AI: Adversarial Machine Learning: Defense Strategies. <https://neptune.ai/blog/adversarial-machine-learning-defense-strategies>.
17. Av-test Institute: Malware Statistics. <https://www.av-test.org/en/statistics/malware/>.
18. Chickowski, E.: Malware: The Next Generation. <https://www.darkreading.com/vulnerabilities-threats/malware-the-next-generation>.
19. HP Inc. (2023, October 31). Malware ‘Meal Kits’ Are Helping Attackers Steal Businesses’ Lunch, HP Finds. <https://www.hp.com/us-en/newsroom/press-releases/2023/hp-wolf-security-q3-2023-threat-insights-report.html>.
20. Chennette, S.: The Future of Automated Malware Generation. <https://ioactive.com/the-future-of-automated-malware-generation>.
21. Mail Today Bureau. (2017). WannaCry did hit India and even central govt portal. So why did Centre downplay the ransomware attack? India Today. <https://www.indiatoday.in/mail-today/story/ransomware-wannacry-cyberattack-global-ransomware-attack-india-983427-2017-06-19>.
22. Parasnis, S. (2024). China backed hacker group behind 2022 AI-IMS attack: Report. MediaNama. <https://www.medianama.com/2024/06/223-china-backed-hacker-group-behind-aiims-attack-report/>.
23. Burgin, J. (2025). EDR vs. XDR: Choosing the right endpoint security solution. Upwind. <https://www.upwind.io/glossary/edr-vs-xdr>.
24. Stanham, L.: Behavioral Analytics. <https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/behavioral-analytics>.
25. Kalra, L. (2023). Decoding the Digital Personal Data Protection Act, 2023. EY India. [https://www.ey.com/en\\_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023](https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023).
26. George, A. A. (2023). National Cyber Security Policy 2013 – In a nutshell. ClearIAS. <https://www.clearias.com/national-cyber-security-policy-2013/>
27. Wired. (n.d.). Pig butchering scams are going high tech. <https://www.wired.com/story/pig-butchering-scams-go-high-tech/>
28. United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking, and technological innovation: A shifting threat landscape. [https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC\\_Convergence\\_Report\\_2024.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf)
29. Burgers, M. (2024). Microsoft’s AI can be turned into an automated phishing machine. <https://www.wired.com/story/microsoft-copilot-phishing-data-extraction/>
30. Trend Micro. (2019). Unusual CEO fraud via deepfake audio steals US \$243,000 from UK company. <https://www.trendmicro.com/vinfo/br/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company>.
31. AI Incident Database. (2020). AI-cloned voice used to deceive Hong Kong bank manager in US \$35 million fraud, Incident 147. <https://incidentdatabase.ai/cite/147/>.
32. Incode. (2024, February). \$25 million stolen using deepfakes in Hong Kong. <https://incode.com/blog/25-million-deepfake-fraud-hong-kong/>.
33. CloudSEK. (2025, April). Elon Musk deepfakes are fueling crypto scams: A dangerous trend. <https://www.cloudsek.com/knowledge-base/elon-musk-deepfakes-are-fueling-crypto-scams-a-dangerous-trend>.