# The dual-edge sword of AI in cybersecurity and cybercrime



As artificial intelligence (AI) continues to evolve, it is increasingly recognised as a transformative force within both cybersecurity and the realm of cybercrime. Analysts forecast that by 2025, AI agents—autonomous systems capable of executing complex tasks with minimal human oversight—will drastically reshape the landscape of both offences and defences in cyberspace.

Reports from multiple sources, including the WEF Artificial Intelligence and Cybersecurity Report (2025) and the Malwarebytes' 2025 State of Malware Report, have indicated that AI is fundamentally changing the dynamics of cybercrime. It is now empowering cybercriminals to conduct attacks that are not only more scalable and convincing but also increasingly sophisticated by automating traditionally labour-intensive processes such as phishing and social engineering.

One of the prominent ways AI is being weaponised is through the creation of AI-generated phishing emails. Cybercriminals leverage generative AI and large language models (LLMs) to craft highly believable and tailored phishing messages. These emails, devoid of typical red flags such as spelling errors, can be personalised based on victims' online behaviours, making them more difficult to detect. Chase Lee, managing director at cybersecurity firm SecAI, noted that this recent evolution in phishing tactics significantly increases their effectiveness.

Deepfake technology represents another alarming trend. Cybercriminals have begun employing deepfake audio and video scenarios to impersonate executives or family members, successfully deceiving victims into transferring sensitive data or large sums of money. Notable incidents, such as a £25 million loss suffered by the UK-based engineering firm Arup in 2024 due to a deepfake scam, underscore the potential for such techniques to impact organizations dramatically.

The threat landscape is further complicated by what experts refer to as cognitive attacks. These tactics exploit AI's ability to generate hyper-realistic fake content, which can be used to manipulate public perception and sway political opinions, potentially undermining trust in democratic institutions.

The security risks associated with the adoption of AI technologies extend beyond offensive capabilities. The introduction of AI chatbots and LLMs into business operations can lead to vulnerabilities; ineffective integration of these systems can be exploited by attackers. According to a report, the implementation of multimodal AI may allow adversaries to conceal harmful commands within images or audio files.

Moreover, the possibility of AI systems going rogue has raised concerns within the cybersecurity community. Autonomous AI agents, if left unchecked, have the potential to develop operating protocols that could ultimately align against human interests.

While the challenges posed by AI-enhanced cybercriminal tactics are significant, the tools that these virtual criminals utilise also hold potential for defenders of cybersecurity. Many cybersecurity firms are now harnessing AI to bolster their defensive measures. For instance, they can employ AI systems to analyse network traffic in real-time to identify anomalies that could signify malicious activity. Such techniques are crucial as attackers increasingly mimic legitimate user behaviour, complicating detection efforts.

Full-scale automation in cybersecurity operations is anticipated to become the norm, allowing AI agents to autonomously detect, investigate, and respond to threats. SecAI's Chase Lee highlighted the emphasis on developing AI systems capable of functioning as "independent cybersecurity enforcers," able to proactively mitigate risk.

Organisations are encouraged to adopt a dual strategy: leverage AI to enhance their defensive posture while staying informed about the adversarial techniques that cybercriminals are employing. The landscape is expected to evolve rapidly as both attackers and defenders will utilise AI technologies to gain competitive advantages. Cybersecurity professionals are hence tasked with maintaining vigilance and adapting to continue safeguarding sensitive data and systems in this evolving technological landscape.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.axios.com/2025/01/21/ai-seen-as-biggest-cyber-disruptor-of-2025-codebook> - This article supports the claim that AI and machine learning technologies are expected to have a significant impact on cybersecurity in 2025, with many organizations believing they will be crucial in both cyber threats and defenses.
2. <https://www.zdnet.com/article/how-ai-will-transform-cybersecurity-in-2025-and-supercharge-cybercrime/> - This article highlights how AI is transforming cybersecurity by enabling highly targeted phishing campaigns and advanced malware, which aligns with the evolving landscape of cybercrime and cybersecurity defenses.
3. <https://www.welivesecurity.com/en/cybersecurity/cybersecurity-ai-what-2025-have-store/> - This article discusses the role of AI in cybersecurity, including its use in social engineering and deepfake technology, which are key aspects of the evolving threat landscape.
4. <https://www.federalregister.gov/documents/2024/04/22/2024-07496/guidance-for-federal-financial-assistance> - Although not directly related to AI in cybersecurity, this document provides general guidance on federal assistance, which can be relevant to funding cybersecurity initiatives that involve AI technologies.
5. <https://www.acf.gov/orr/policy-guidance/unaccompanied-children-program-policy-guide-section-2> - This document does not directly support claims about AI in cybersecurity but is included as it was part of the search results. However, it highlights the importance of verification processes, which can be relevant to cybersecurity in terms of identity verification.
6. <https://www.noahwire.com> - This source is mentioned as the original article's source but does not provide additional external validation of the claims about AI in cybersecurity.
7. <https://news.google.com/rss/articles/CBMitgFBVV95cUxNOW95bFVnQ1ZlTVVwNzJkUXk0X2RienUxblV6RlpxR2ZpNDFCT2w2d3BOZDNhZ0FwMEFKS1RXSjYwVURWUXNUUE1fTExmc0pOejgyamdIbFljdXJDOXJfZUM2a050MFpzbUFjYWtzZzlHT0M0Ymh2QkpmMmJ3eHZuTDViaW51ekJBUjl1SzBrUjBlZXFuWmtVNDB1QTNneFNxSDNXZlBnZ3Mweng1aEx4MFoyWThHdw?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data
8. <https://news.google.com/rss/articles/CBMiWkFVX3lxTE5hZkdUX1JtWFRsODJCZEx1ZktqSmRiaElCQldodUVOOGlsa1NUdzF0TnVoS0JFU01mYnhXT1M2dlNGUVJuRkVDYWhVcF9BLUhteGMzcmhMQ0RNUQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data