AI Attacks: Who Bears Responsibility?

Tara Martin

I. Introduction

Artificial Intelligence (AI) has vastly transformed the world of cybersecurity, and the impact has just begun.[1] The number of threat actors using AI to carry out their cyberattacks has grown exponentially in recent years.[2] Cyberattacks are no longer carried out through a series of trial and error, but rather AI-driven, high-precision attacks.[3] AI-powered algorithms can identify vulnerabilities in systems, adapt to avoid detection, and target individuals or specific software.[4] Generative AI in particular enables threat actors to impersonate their potential victims by drafting sophisticated and convincing phishing communications and emulating real voices.[5] Not only are individual threat actors carrying out attacks on private companies, but there are reports that nations such as Russia, China, Iran, and North Korea are using AI to mount cyberattacks against the United States.[6] To protect themselves against the growing threats, AI cyberattacks must be taken seriously by companies, government organizations, and individuals.[7] These attacks must also be taken seriously by lawmakers and judges, who must set rules and standards to regulate the use of AI and prevent its continued use in cyberattacks.[8]

II. AI Attacks on Companies: A Growing Threat

Almost half of all companies have been victimized by AI attacks in some capacity.[9] This is in no small part due to how easy AI has made it for attacks to be carried out.[10] Anyone with a desire to carry out a cyberattack can do so as long as they have access to an AI tool.[11] It has also

---

[1] Edward McNicholas, Shannon Capone Kirk, & Kevin Angle, AI's Impacts on Cybersecurity & Legal Requirements, Incident & Breach Management, Professional Perspective - AI's Impacts on Cybersecurity & Legal Requirements, Practical Guidance, BLOOMBERG LAW: PRACTICAL GUIDANCE. https://www,bloomberglaw.com/external/document/XFFFPLEG000000/incident-breach-management-professional-perspective-ai-s-impacts [https://perma.cc/MC7B-4FYE].

[2] *Id.*

[3] *AI-Driven Cyberattacks: The New Frontier of Legal Liability*, INSIDE OUT LEGAL, https://inoutlaw.com/ai-driven-cyberattacks-the-new-frontier-of-legal-liability/ [https://perma.cc/2ZAQ-WAU5].

[4] Lucia Stanham, *AI-Powered Cyberattacks*, CROWDSTRIKE, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/ [https://perma.cc/A5JA-GU5E].

[5] *Id.*

[6] David Klepper, *Microsoft: Russia, China increasingly using AI to escalate cyberattacks on the US*, ASSOCIATED PRESS, https://apnews.com/article/ai-cybersecurity-russia-china-deepfakes-microsoft-ad678e5192dd747834edf4de03ac84ee [https://perma.cc/8S5R-677W].

[7] *Id.*

[8] *See* Kevin Frazier, *We're Not Ready for AI Liability*, AI FRONTIERS, https://ai-frontiers.org/articles/options-for-ai-liability [https://perma.cc/977U-JGWA].

[9] Eric Geller, *Businesses fear AI exposes them to more attacks*, Cybersecurity Dive, https://www.cybersecuritydive.com/news/it-leaders-concern-ai-cyberattacks-survey/802151/ [https://perma.cc/848X-GKPH].

[10] Lizzie Short, *AI and the Future of Cybersecurity*, Harvard Extension School, https://extension.harvard.edu/blog/ai-and-the-future-of-cybersecurity/#How-AI-Enables-the-Next-Generation-of-Cyber-Attacks- [https://perma.cc/M3G6-M6BN].

[11] *Id.*

become much easier to launch attacks at a faster pace than ever before.[12] Not only does AI allow for more precise attacks on companies' software, but it also provides the opportunity for many more attacks to be launched, increasing the chances of success.[13]

Threat actors are using AI to exploit traditional methods of cyberattacks through more advanced processes.[14] These methods include stolen credentials (accounting for 30% of initial access points to company software) and social engineering.[15] Social engineering is a type of cyberattack that aims to manipulate human behavior to produce a result such as sharing data, transferring money, or granting access to a private database.[16] Such attacks can use AI algorithms to assist from the beginning to the end of the attack, from researching targets and identifying vulnerabilities all the way through execution.[17] Phishing attacks, conducted with the same goals as social engineering attacks, can also use Generative AI to create highly personalized and realistic communications.[18] The use of AI only expands the ability of threat actors to carry out their attacks through more sophisticated means. However, the growing threat of cyberattacks is not only coming from the advancement of third-party attackers, but businesses using their own AI models are also increasingly vulnerable to attacks from their own software.[19] As a result, companies must focus on developing internal governance even with very little outside regulation.[20] However, there are not only questions of regulation when it comes to internal matters, but also when it comes to holding attackers accountable.

III. Liability for these Growing Attacks

There are growing questions about the liability that should be placed on AI developers and the punishment they can face for their role in cyberattacks.[21] While threat actors can be punished under the current legal regime, there is no clear pathway for AI developers to face repercussions.[22] The Securities and Exchange Commission as well as other federal and state regulators have focused attention on cybersecurity risks, a focus that is expanding to include cyberattacks on business.[23] The Federal Communications Commission has issued new reporting rules designed to keep the agency informed on data breaches and attacks on critical telecommunications infrastructure.[24] Further, under the Federal Trade Commission Act "companies can face enforcement actions for failing to implement adequate data-security safeguards."[25]

---

[12] *Id.*; See also *AI-Driven Cyberattacks: The New Frontier of Legal Liability*, *supra*, note 3.
[13] *AI-Driven Cyberattacks: The New Frontier of Legal Liability*, *supra* note 3.
[14] Marco Túlio Moraes, *AI agents: the new frontier of cybercrime business must confront*, WORLD ECONOMIC FORUM, https://www.weforum.org/stories/2025/06/ai-agent-cybercrime-business/ [https://perma.cc/PX73-CK9Q].
[15] *Id.*
[16] Stanham, *supra* note 4.
[17] *Id.*
[18] *Id.*
[19] Short, *supra* note 10.
[20] *Id.*
[21] Frazier, *supra* note 8.
[22] *Id.*
[23] McNicholas, Kirk, & Angle, *supra* note 1.
[24] *Id.*
[25] *AI-Driven Cyberattacks: The New Frontier of Legal Liability*, *supra* note 3.

Tort law is also likely to become an essential component of cybersecurity law as the area continues to develop. The goal of tort law is to compensate those who have been harmed by others, deter excessively risky behavior, and right wrongs.[26] Cyberattacks will likely fit into the categories of negligence and strict liability, frameworks meant to hold responsible parties liable for the harm they've caused.[27] While negligence claims would require a showing that reasonable care was not exercised, strict liability would only require it be shown that the AI systems caused harm, not that there was a failure to exercise reasonable care.[28] In terms of AI cyberattacks, this would mean a negligence claim could be made if AI developers fail to exercise reasonable care in developing the software to prevent against use in AI attacks, whereas a strict liability claim could be made on AI software causing harm alone. To develop a framework of tort law for AI cyberattacks, state legislators must act to define duties of care and to create liability standards.[29] Frameworks such as this are being developed in some east coast states including New York and Rhode Island, where there are bills pending in the legislatures to implement tort liability for cyberattacks.[30] The legal landscape will continue to develop to increase tort law liability for threat actors and AI developers for their roles in AI cyberattacks, increasing legal ramifications and encouraging more stringent measures to prevent such attacks.

IV. Conclusion

The liability for threat actors and AI developers in cyberattacks is continuing to grow and will increase the risks associated with carrying out such attacks. Tort liability seems to be the best path forward to create this accountability, as there are negligence and strict liability frameworks that can be expanded to include AI attacks.[31] Without clear regulations, there will be uncertainty from the time AI systems are developed all the way through the legal liability process for those involved in potential attacks.[32] Government agencies and state legislatures must continue to work to implement policies and procedures to keep up with the growing sophistication of AI software and its ability to help threat actors carry out attacks.[33] Highly sophisticated AI developments are making it far easier for threat actors to breach sensitive systems and cause significant damage.[34] Therefore, to protect companies, individuals, and the United States government from continued attacks, implementation of regulations for AI developers is key to the development of software that cannot be used to carry out such attacks.

---

[26] Fraizer, *supra* note 8.
[27] *Id*.
[28] *See Id.*
[29] *See Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] McNicholas, Kirk, & Angle, *supra* note 1.
[34] *See AI-Driven Cyberattacks: The New Frontier of Legal Liability*, *supra* note 3.