OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

Former NYT Reporter Warns of AI Cyber Threats at Black Hat USA

August 9, 2025
— Categories: Defence & Security

Download IPFS

At Black Hat USA 2025, cybersecurity expert and former New York Times reporter Nicole Perlroth delivered a stark warning about the growing threat of artificial intelligence-driven cyberattacks. Perlroth highlighted that these evolving digital dangers now challenge not only networks but also democracy and public discourse.

Speaking Thursday, Perlroth, who is a founding partner of Silver Buckshot Ventures, explained that traditional cybersecurity defenses are struggling to keep pace with new forms of cyber threats. Malware has become quieter and more autonomous, while ransomware now operates like a subscription service. She pointed out that artificial intelligence is being used to distort reality and scale attacks in unprecedented ways.

“The question is not whether we can stop these threats,” Perlroth said, “but whether we dare to try.”

Perlroth’s remarks came from years of frontline experience covering cyber conflicts for The New York Times. During her decade as a cybersecurity reporter, she witnessed major incidents ranging from newsroom hacks to nation-state attacks on critical infrastructure.

Shortly after joining The Times, Perlroth’s newsroom was targeted by hackers linked to foreign governments. Since then, cyberattacks have escalated, including malware hidden in everyday items such as takeout menus, destructive attacks on nations like Iran and Saudi Arabia, the breach of Sony Pictures, and the Democratic National Committee hack that influenced public opinion.

She described these acts as direct assaults on free speech and democratic processes. “What it was,” Perlroth said, “was an assault on the First Amendment.”

Over time, the scope of cyber threats has widened significantly. Hospitals have been crippled by ransomware, journalists intimidated through spyware, and corporations pressured by the leak of sensitive data. These attacks have grown more sophisticated, and the consequences more severe.

“I had a front-row seat to the human cost of these attacks,” she said. “And every time it got worse.”

Despite the growing severity of threats, Perlroth criticized the cybersecurity industry and the public for often moving on too quickly after high-profile incidents. She emphasized that these events were not isolated but served as stress tests revealing systemic weaknesses.

Looking ahead, Perlroth warned that artificial intelligence is changing the rules of cyber engagement. Hackers are already using AI tools to identify valuable targets, create convincing phishing campaigns, and automate psychological pressure during ransomware negotiations.

Defenders face significant challenges. AI-powered workflows and models, such as Claude, have already demonstrated superiority in hacking contests. Still, Perlroth expressed cautious optimism.

“We can still steer AI,” she said, “but the window is narrow, and it’s closing fast.”

Encouragingly, new technologies are emerging to counter these threats. Real-time deepfake detection, scalable risk scanning, and security tools accessible to smaller organizations are helping improve defenses. More importantly, Perlroth stressed that cybersecurity remains a human-driven field with many dedicated professionals committed to protection.

“Despite the challenges, there are people who step up every day to defend rather than destroy,” she said.