LLOYD'S

Generative AI: Transforming the cyber landscape

Major leaps in the effectiveness of Generative AI (GenAI) and Large Language Models (LLMs) have dominated the discussion around artificial intelligence over the past 18 months. Given its growing availability and sophistication, the technology will inevitably reshape the cyber risk landscape.

Generative AI: Transforming the cyber landscape, explores how GenAI could be used by threat actors and cyber security professionals and highlights its potential impacts on the cyber risk landscape. Each of the four headings below is explored in detail in the full report.

Lloyds.com/genAI

1. The LLM landscape

Generative AI and LLMs (Large Language Models) are a very new set of technologies, with pivotal enabling advancements happening only about 6 years ago.

Major leaps in model effectiveness across a variety of tasks relevant to cyber security have occurred in the last 18 months and are likely to continue into the near future.

Applications of LLMs to cybercrime have been minimal to date due to effectiveness of AI model governance, cost and hardware barriers, and content safeguards.

The release of unrestricted frontier models plus recent algorithmic efficiency discoveries represent a pivotal breakdown in AI governance. There are now many publicly available models which can create explicitly harmful content, and they can now be run on commodity hardware cheaply.

2. Transformation of cyber risk

Vulnerability discovery: Automated vulnerability discovery, especially in domains which elude human experts, is likely to significantly increase the pool of options for threat actors. Threat actor tooling is likely to outpace defensive tools created by the security industry due to asymmetric incentives.

Campaign planning and execution: Cyber-campaign targeting and scoping is likely to become cheaper, more fine-tuned, and broader due to automation of target discovery. This would mean threat actors could generate bespoke attack materials for many potential targets.

Risk-reward analysis: Threat actors' ability to evade attribution and achieve their desired outcomes (exfiltration of funds, etc) is likely to be enhanced. This could shift risk-reward calculations in their favour and embolden them.

Single points of failure: The rise of a new class of service provider linked to the provision of LLMs, could generate a new type of single points of failure. Losses arising from interruption or compromise of these single points of failure are likely to be different from what we expect today.

3. Considerations for business and insurance

A new threat landscape: AI is likely to augment threat actor capability, enhancing the effectiveness of skilled actors, improving the attractiveness of the unit cost economics, and lowering the barrier to entry.

Cyber catastrophes: There may be a modest increase in the risk of manageable cyber catastrophes. In contrast, smaller scale events are likely to increase at a greater pace as AI-enhancements allow threat actors to more effectively design targeted and lower profile campaigns.

State-backed, hostile cyber activity: AI has the potential to improve the effectiveness of state-sponsored hostile activity, both in terms of espionage and sabotage. However, it is unclear to what extent the proliferation of advanced capabilities will increase the risk of a major catastrophe happening, due to the human factor.

4. Taking action

At Lloyd's, we will continue to work with our stakeholders to support the development of this important technology, and evaluate and address the potential threats.

Educating our community: Build awareness and education through Lloyd's Futureset as the growth of AI technology transforms the risk landscape.

Partnering with industry: Encourage greater collaboration with governments, regulators and technology companies to better manage AI risks.

Engaging policymakers: Work with insurers, governments and others to inform the development of intelligent policy guiderails that can support this important technology.

Supporting sustainable innovation: Enable new product development through the Lloyd's Lab that will serve as a springboard to develop new solutions responding to the changing cyber threat landscape.

Lloyd's Futureset