AI Raises Stakes Across Cybersecurity And Disputes Landscape

Published on Alvarez & Marsal | Management Consulting | Professional Services
(https://www.alvarezandmarsal.com)

April 10, 2024

As Artificial Intelligence (AI) systems become more advanced, public institutions and companies face growing risks from increasingly sophisticated cyber threats.

New And Emerging Threats Posed By AI

There are several new and emerging threats created by AI which are noteworthy from both a corporate and national security perspective. Modern cyber security is best categorised as an arms race between defenders and attackers, with the latter having the advantage of picking when, where and how to attack. In many cases this leaves defenders catching up, patching holes and shutting down systems in order to protect or repair them.

While attacks are inevitable and increasing both in volume and sophistication, defenders should never view themselves as defenceless. Various tactics and tools are available to help organisations build defences, improve resilience and update systems, processes and culture. Defenders are able to deploy security tools, share threat intelligence and employ dedicated teams to quickly mount an effective defence in the event of an attack or hostile reconnaissance.

However, the landscape continues to evolve as technology continues to advance. AI is increasing the speed and efficiency of pre-existing cyber-attack techniques, while accelerating the development of new tactics and making them increasingly difficult to detect, monitor and remediate.

AI dramatically speeds up the intensity and scale of hostile activity and, when used by malicious actors, allows attackers to quickly adapt to defeat defences and find new vulnerabilities to exploit. AI also allows attackers to adapt their software tools to make them harder to detect in order to carry out more stealthy attacks.

One of the primary sources of threats to systems comes from malware. There are many different families and strains of malware which utilise system vulnerabilities, and traditionally these threats have been met by identifying and blocking malicious links and outbound traffic and looking for the “footprint” these hostile programs leave in systems.

AI allows attackers to quickly produce “hybrid” malware which can easily conceal itself from security tools as benign software, and allows those carrying out hostile activity to combine different malware families, producing programs which will have a new signature. This is a common evasion technique currently used by attackers, but the speed of this process has now dramatically increased due to new AI tools.

To highlight the issues posed by AI, a significant increase in targeting of mobile devices facilitated by AI has been seen, with a 59% increase reported by global cyber intelligence company Recorded Future in the last year. This increase is brought about by a shift in capability, allowing attackers to generate more targeted “designer” malware to leverage vulnerabilities more quickly – and before they are patched.

The increasing levels of public usage of AI for wider applications has led to the creation of a very data rich environment, effectively making it easier for attackers to hide themselves and their traffic within increasingly large and sophisticated data flows and storage facilities throughout companies and the public sector. This increased ability to change malware signatures in minutes has left defenders in many cases struggling to keep up.

The large scale targeting and use of advanced AI algorithms, combined with the increasing deployment of software platforms using large language models has prompted information technology departments to install business systems which are increasingly autonomous. New AI generated malicious capabilities can be automated by attackers to target multiple victims near simultaneously, can be stealthier in their implementation and also use persistency around cracking passwords or temporal vulnerabilities to wear defences down through their volumes and polymorphic nature.

Attackers are also leveraging AI to identify vulnerable gaps in the defences of organisations’ expanding public attack surfaces. The fragmented nature of the modern workforce and workplace, with their increased dependence on communications systems, also allows AI systems to quickly scan the increased “attack surface” and potentially find gaps.

As AI systems and platforms become more publicly available, attackers can easily access more sophisticated tools which allow technically unskilled malicious actors to conduct increasingly sophisticated attacks. The ability to stage anonymised attacks through infrastructure procured via the underground economy or Dark Web forums, through compromised IT environments and even through legitimate cloud accounts has also made it more difficult to conduct identification and attribution exercises and allows attackers to conceal their identities more effectively.

The Regulatory Environment And Potential For Dispute

This increasing sophistication and pervasion of cyber activity throughout all corners of business and life is likely to give rise to a tsunami of litigation and disputes.

A 2023 report found that 75% of cybersecurity professionals had witnessed an increase in the number of cyberattacks, with 85% of those polled believing this increase was due to ‘bad actors using generative AI’.[1]

In response, there will be growing expectations for organisations to bolster defences and resilience coupled with increased scrutiny on appropriate measures being taken to ensure cyber security. Those found lacking could open themselves up to swarms of claims or criticism.

Individuals and organisations affected by cyber-attacks may not only be entitled to seek recourse under the relevant data protection law but also potentially under other legislative frameworks such as consumer protection laws, IP infringement law, product safety and equality law, contract law etc.

That said, the current regulatory environment as it relates specifically to AI is complex. Governments and regulatory bodies are struggling to legislate or place effective controls on the new technology, which is developing at a faster pace than policies can be implemented or approved. Although an increased emphasis has been placed on regulators to ensure controls are in place, the borderless nature of the internet and accessibility of new tools is making this a nearly impossible task.

There has been some movement in the global race to regulate the technology, however. In March 2024, Members of the European Parliament (MEPs) voted in favour of the European Union (EU) AI Act.

The Act, first published in December 2023, is the world’s first comprehensive piece of legislation regulating the use of AI. The Act raises a number of considerations and challenges for cybersecurity professionals and leaders at organisations operating within the EU.

The Act takes a risk-based approach and classifies a certain number of ‘high-risk’ AI systems which will require particular attention. ‘High-risk’ AI systems are defined as those concerning: biometrics; critical infrastructure; education and vocational training; employment; worker management and access to self-employment; access to and enjoyment of essential private services and essential public services and benefits, law enforcement; migration, asylum and border control management; and administration of justice and democratic processes.[2]

These high-risk systems will be required to comply with a determined level of cybersecurity throughout their lifetime – in accordance with Article 15 of the Act. These systems must be resilient to attempts by third parties to exploit system vulnerabilities to alter use, outputs or performance. They must also make use of – as appropriate – a number of technical solutions to mitigate cybersecurity risk, including measures to 'prevent, detect, respond to, resolve and control' any attempts to manipulate data / components used to train AI systems as well as the system inputs.

The Act also introduces new obligations concerning cybersecurity of general-purpose AI models (GPAIs), which now must be subject to an 'adequate level of cybersecurity protection' and introduces a requirement to report serious incidents to the AI office and relevant national authorities. Cybersecurity measures should consider 'accidental model leakage, unsanctioned releases, circumvention of safety measures, and defence against cyberattacks, unauthorised access or model theft'. The Act also lists a number of ways in which AI models may be protected from compromise such as through 'operational security measures for information security, specific cybersecurity policies, adequate technical and established solutions, and cyber and physical access controls'.[3]

Similar legislation is in development by several other jurisdictions globally. In the US, the White House has released their blueprint for an AI Bill of Rights, whilst the UK government has set out its proposals for regulating the use of AI in its 2023 AI White Paper.[4][5]

The effectiveness of AI legislation is yet to be seen, however, particularly given the long timeframes for implementation and the speed at which the technology is advancing.

Harnessing AI For Good

Although this paints a bleak future for cyber security defenders, there is hope on the horizon. AI also gives defenders the ability to identify complex patterns in the increasingly large amounts of data. New security tools are being developed which allow defenders to leverage the power of AI to help them mitigate threats at 'machine speed', to increase the speed of the analytical cycle and quickly predict shifts in an attacker's patterns of activity.

When discussing AI, it is also important to include the potential future issue of quantum computing. To cope with the increasing levels of data, devices, and bandwidth, it is likely that an exponential increase and availability of quantum-based systems will be seen over the next few years. The raw computing speed and power produced by these systems combined with AI will lead to a further arms race between defenders and attackers.

National security will also have to adapt to the cyber risks posed by AI. Unless public sector systems develop their defences at a comparable rate to systems utilised by malicious threat actors to carry out wide ranging attacks against Critical National Infrastructure (CNI), there may develop an imbalance in capabilities of those with hostile intent and public sector bodies to defend themselves. Sectors such as healthcare, power generation and water supplies are considered a particular focus of disruptive or destructive attacks by hostile nation states or criminals in ransomware attacks.

In summary, AI offers many opportunities to enhance information systems for the better, but it also leads to a significant increase in the threat landscape. The key thing to mitigate this threat is for defenders to enhance their defences using AI at the same rate as the attackers, but that will present a significant challenge. The genie is very much out of the bottle and organisations and law enforcement must now prioritise investment in this rapidly evolving area, otherwise they will be left behind in the race to adopt and leverage AI.

Endnotes

1. https://www.deepinstinct.com/pdf/voice-of-secops4th-edition?hsCtaTracking=982e81ff-d1a0-47a4-9adf-6e279398d361%7C1d16a471-1022-4dff8d07-dd79dac66a52

2. Annex III: https://data.consilium.europa.eu/doc/ document/ST-5662-2024-INIT/en/pdf

3. 60r: https://data.consilium.europa.eu/doc/ document/ST-5662-2024-INIT/en/pdf

4. https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

5. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/

**This article was originally published in Mealey's Data Privacy Law Report*

Source URL:https://www.alvarezandmarsal.com/insights/ai-raises-stakes-across-cybersecurity-and-disputes-landscape

Authors:
Lorenzo Grillo