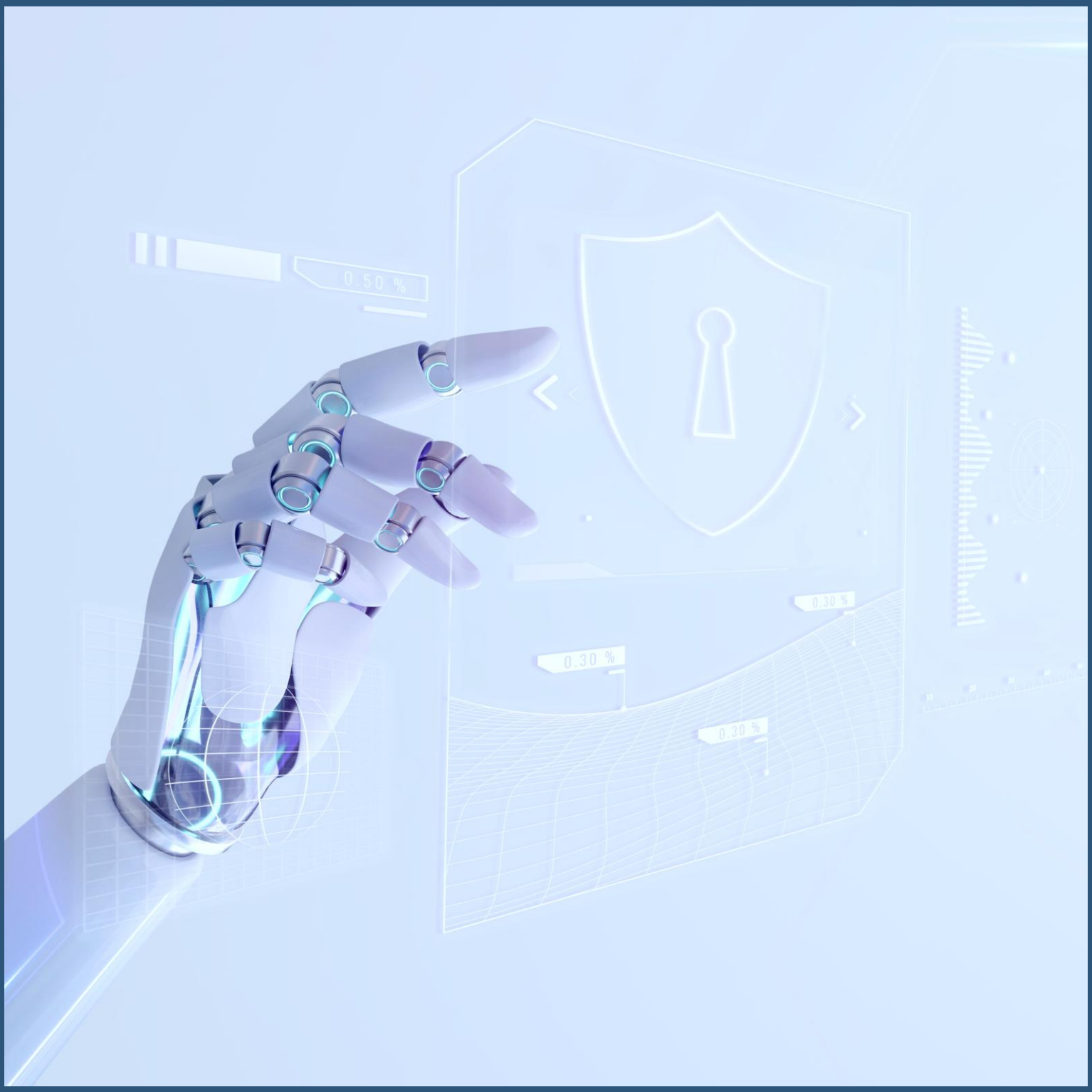


Accelerating AI-enabled cybersecurity

Macro PDF series

mazars

Introduction
PDF series

Artificial Intelligence and Cybersecurity are inherently intertwined, given their shared emphasis on data management. This convergence has the potential to revolutionise information governance significantly.

The development and proliferation of artificial intelligence (AI) in the last ten years has been nothing short of extraordinary. As per a report by Bloomberg intelligence, the AI market is poised to catapult to US$1.3 trillion over the next 8-10 years, with a range of specialised software and services emerging to meet growing demand.

To begin with, what exactly is AI?

As a definition, AI refers to the science of simulating human intelligence in machines, with the aim to enable them to emulate human thought processes and actions. This enables AI to execute certain tasks that were traditionally within the domain of human intelligence, with the added benefit of minimising errors typically made by humans. Consequently, this enables AI to outperform its natural counterparts in certain scenarios.

This characteristic has led AI to revolutionise numerous industries worldwide, and India is notably among those experiencing significant transformation. Cloud platforms and AI-first Software-as-a-Service (SaaS) companies have showcased commendable AI-capability on scale implementations, with their innovative approaches to complex corporate problem statements gaining widescale enterprise confidence. As per a survey by the Data Security Council of India (DSCI), around 97% of Indian organisations have invested in AI/ML technologies while 84% have invested in the Cloud.

Statistically, AI is projected to contribute approximately US$500bn to India’s GDP by 2025, by way of both increased productivity and employment generation.

Having said that, AI isn't just about propelling industries forward; it's also about safeguarding the cyberspace it interacts with.

Introduction
PDF series

Piecing AI and cybersecurity together

The pace of AI-enabled cybersecurity is growing more than ever. A recent research report estimates the global market for AI-based cybersecurity products will surge to roughly US$135bn by 2030.

AI is increasingly being integrated in a multitude of cybersecurity processes ranging from antivirus protection to fraud detection and even risk management. Its unique ability to analyse vast datasets and recognise patterns makes it particularly effective in:

- Increasing accuracy in the detection of cyberattacks
- Flagging suspicious emails in phishing campaigns
- Minimising false positives to a reasonable degree
- Simulating social engineering attacks for vulnerability assessment
- Prioritising responses based on actual risks
- Analysing large volumes of incident-related data for prompt threat containment

This macro-PDF series examines the opportunities brought about by the use of AI in cybersecurity from a People, Development and Financial angle.

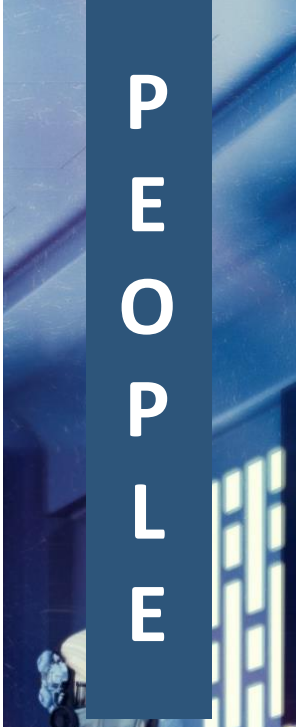
People **D**evelopment **F**inancial

AI is particularly focused upon restructuring the cybersecurity chain to improve factors such as usability, safety and quality, as well as reduce the risk of cyber-attacks for societies. It has direct benefits for a range of stakeholders (the "people"), be it regulators, governments, organisations or "common users."

A key component of AI is behavioural analytics, which holds considerable importance in streamlining largescale citizen data in a country like India. It examines patterns of user and entity behaviour and adeptly detects irregularities indicative of hacking attempts. For organisations seeking to fortify their own security measures to computer emergency response teams establishing proactive cyber-defense mechanisms across the public and private spheres, this information system is invaluable. Moreover, given the rapid expansion of the digital payments ecosystem in India (i.e., UPI and mobile wallets), the use of AI-enabled data analytics for fraud detection and prevention greatly benefits the security of merchants and consumers alike.

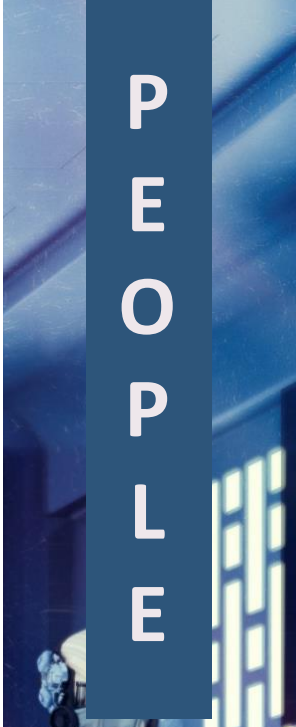
Deep learning technology, a subset of machine learning and a component of the broader AI field, is highly critical for running real-time image and video analysis, and thereby enhancing surveillance capabilities. It possesses the ability to provide accurate and context-aware image recognition in a short of amount of time, which enables security teams and organisations to swiftly detect and respond against suspicious activities.

Contrary to popular belief, AI presents a huge opportunity for the working-class – i.e., the backbone of the demographic dividend in India. While this technology automates repetitive tasks, it does open up new avenues for human research and innovation.



Ultimately, while AI can simulate human thought processes it cannot entirely replace human creativity. Hence, its integration in cybersecurity opens new skill sets for cyber professionals to learn, necessitating proficiency with machine learning, big data analysis and AI-driven security systems. Humans will be needed to develop, train, implement, maintain and secure AI, which means job roles such as AI security analysts or machine learning security engineers will become very much in demand. This presents a strong footing for the youth in India to equip themselves with contemporary profiles and pursue value-added growth in cybersecurity.

However, this is merely scratching the surface. AI has the potential to take care of the entire value spectrum of cybersecurity services – from detection to predictive analysis, knowledge consolidation, vulnerability assessment, risk mitigation and beyond. While the initial utilisation of data will aid security professionals and regulators with their oversight duties, the ultimate prevention of large-scale cyber-attacks will benefit all users significantly.



AI has the potential to effectively address the entire value spectrum of cybersecurity services – from detection to predictive analysis, knowledge consolidation, vulnerability assessment, risk mitigation and beyond.

Development
PDF series

Given the multi-stakeholder opportunities – as well as the swift digital transformation in India that is being propelled by a host of government initiatives, a dynamic startup ecosystem, and advancements in technologies like 5G and AI/ML – the rising pace of investment in AI-enabled cybersecurity is inevitable. It has a strong role to play in advancing India's long-term digitalisation vision and instilling order and confidence in the market. In this regard, AI is increasingly being integrated into various government initiatives, which includes being channelised to build the robust platforms needed for cyber-monitoring as well as for enforcing contemporary regulations and laws.

Public-support and encouragement has been growing every year. In 2022, the government of India outlined 75 priority projects related to utilising AI in defence. These include areas such as data processing and analysis, cybersecurity, simulation and autonomous systems, particularly drones. Meanwhile, the application of AI for underwater domain awareness and border security is also under exploration.

A key milestone was marked in August 2023 when India unveiled its highly anticipated Digital Personal Data Protection Act, 2023 (DPDPA). This legislation extends the rights of citizens beyond the Information Technology (IT) Rules, including the right to information, correction, erasure, grievance redressal, and the ability to nominate a representative in case of incapacity. As per the Ministry of Electronics and Information Technology (MeitY), the DPDPA will soon be accompanied by a Digital India Act (DIA), which is set to replace the existing IT Rules.

AI-powered tools are instrumental in forwarding the objectives of the DPDPA, given their focus on the identification and mitigation of data breaches, as well as regulation and compliance with data protection standards and trust-based governance.

However, the synergy that AI plays in India's cybersecurity development is itself dependent on the pace of AI-integration across sectors. This underscores the employment opportunities created by AI, as it necessitates the emergence of new cyber professions to manage and secure new technological landscapes. The industry requires more experts in AI and ML cybersecurity with proficiency in relevant programming, who can conduct regular maintenance and adjustment of the network.

To address this, the government has been carrying out various skill development programs to date, which includes the launch of the Future Skills Prime initiative in 2021. This is a collaborative initiative by the Ministry of Electronics & Information Technology (MeitY) and NASSCOM, which aims to establish an upskilling/reskilling ecosystem in ten emerging technologies, including artificial intelligence, IoT, blockchain, 3D printing, AR/VR, cyber security, and cloud computing. This initiative, involving entities like C-DAC, NIELIT, the National Skills Development Mission of India, NSDC, and AICTE, aims to reskill/upskill about 20 lakh professionals.

Alongside this, the government recognises the importance of responsibility when it comes to using next-gen technologies. It has recommended the establishment of the 'Transparent and Accountable AI and Emerging Technologies Governance Framework', which aims to guide an ethical and responsible deployment of AI tools, shaping a future where innovation aligns seamlessly with accountability.

Overall, these development initiatives highlight the synergy AI has with cybersecurity to usher in a new era of good governance in India, both at the infrastructural and institutional level. The crucial aspect is to ensure alignment of this technology from its inception, ensuring it is developed and managed in tandem with the growth of cybersecurity across the nation.

AI-powered tools are instrumental in forwarding the objectives of the DPDPA, given their focus on the identification and mitigation of data breaches, as well as regulation and compliance with data protection standards and trust-based governance.

Financial
PDF series

Considering its pivotal role in threat identification and response mechanisms, it's easy to see the positive financial impact of AI in cybersecurity.

According to the 2023 IBM Cost of a Data Breach report, organisations utilising security AI and automation experience lower data breach costs compared to those without AI-based cybersecurity tools. Specifically, organisations extensively leveraging AI and security automation report an average cost of a data breach at US$3.60m, contrasting with US$4.04m for those with limited AI use. Meanwhile, those without any AI and security automation face significantly higher breach costs at US$5.36m.

For India, cost savings here have the potential to yield significant benefits at an enterprise-wide level. As per Surfshark, India ranks 2nd in the world (as of 2022) on the number of data breach cyber-attacks that organisations face; meanwhile, it ranks 14th globally in average data breach costs. The ability to cut through the breach lifecycle and detect a breach in less than 200 days can help an Indian enterprise, on average, save IN₹10 crore (US$1.2m). AI has the power to increase this saving by multiples, as it can help firms analyse and detect cyber threats accurately with low false alarms within a period much less than 200 days.

However, monetary savings aren't the only consideration here; time is also a valuable commodity. By automating threat detection, AI systems save valuable time and resources for organisations and security teams, enhancing accuracy on both a retrospective and prospective level. AI-powered threat intelligence systems monitor and analyse network traffic in near real-time, promptly identifying anomalies and potential threats. This prompt response reduces the time required to mitigate a threat and minimises the impact of attacks.

Financial
PDF series

Essentially, AI has the ability to significantly reduce both costs and time in cybersecurity, through enhanced application security and improvement in threat detection, response, and prevention. While AI enhances security testing accuracy and analysis, it is crucial for organisations to adopt these technologies judiciously, recognising that AI should complement human expertise. Staying updated on AI developments is vital for organisations to fortify their security stance.

Organisations utilising security AI and automation experience lower data breach costs compared to those without AI-based cybersecurity tools.

Road ahead

Overall, the integration of AI in cybersecurity goes beyond just the technology. It possesses the potential to revolutionise processes and usher in a new era of governance through monitoring, addressing, reacting, and proactively anticipating threats.

AI systems can enhance cybersecurity capabilities by incorporating contextual datasets and information to help stakeholders make more informed decisions. It can revolutionise penetration testing, which involves testing the security measures of software and networks to find vulnerabilities beforehand. By developing AI tools capable of scrutinising their own technology, organisations can more effectively identify weaknesses and prevent hackers from exploiting them.

The ironic fact is that this technology aims to solve the very risks it breeds in the first place. For example, major cyber threats utilising AI include brute force attacks, denial of service incidents, AI-generated deepfakes, and social engineering attacks. However, utilising AI-governance against its own generated attacks can help security teams stay ahead of what is coming.

To counter these risks and align with the future of artificial intelligence security, both government and organisational leaders should consider the following steps:

Invest in maintaining a future-focused approach to technology

Supplement teams with AI and ML skillsets to help safeguard systems, rather than replacing them with the system

Regularly update data policies to comply with evolving legislation

Finally, it's crucial to recognise that while the optimal role of AI in cybersecurity entails interpreting patterns established by machine learning algorithms, it doesn't exclude humans from the ecosystem. Instead, contemporary AI must be refined by the creative and spontaneous judgment of cybersecurity professionals, ensuring a balance between being "technologically adept" to identify errors and "flexible enough" to think innovatively.

Contacts

Bharat Dhawan
Managing Partner
bharat.dhawan@mazars.co.in

Shree Parthasarathy
Partner
shree.parthasarathy@mazars.co.in

Rajan Arora
Partner
rajan.arora@mazars.co.in

Manoj Ajgaonkar
Partner
manoj.ajgaonkar@mazars.co.in

Nikunj Garg
Partner
nikunj.garg@mazars.co.in

Kartikeya Raman
Associate Partner
kartikeya.raman@mazars.co.in

Contributor

Ankur Malhotra
Director
ankur.malhotra@mazars.co.in

Rati Acharya
Director
rati.acharya@mazars.co.in

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory and tax services. We operate in more than 105 countries and territories around the world. We draw upon the expertise of more than 50,000 professionals, 33,000+ in Mazars' integrated partnership, 17,000+ via the Mazars North America Alliance and 1500+ professionals in India to assist clients of all sizes through all developing stages. Our professionals possess in-depth experience in the Energy, Telecom, BFSI, Automobiles, Technology, Real Estate, Shipping, Services, Manufacturing and Retail sectors and are located in 7 offices across Bengaluru, Chandigarh, Chennai, Delhi, Gurugram, Mumbai and Pune.

mazars