AI in cybersecurity:

A double-edged sword

In an era where the digital landscape evolves at breakneck speed, the quest for security has taken centre stage. The interconnectedness of our modern world has opened unprecedented opportunities for innovation and communication, but it has also exposed us to a growing array of cyber threats. As businesses and individuals rely more than ever on digital technologies, the vital role of cybersecurity cannot be emphasized enough.

The digital frontier

Imagine a world where our every move, our every thought, lives in the digital realm. Our thoughts are shared openly on social media platforms, capturing our emotions, ideas, and opinions for the world to see. Our physical presence is captured through check-ins, travel updates, and real-time location sharing, creating a digital trail of our journeys. In this interconnected landscape, the line between the logical and physical worlds blurs into our identity, seamlessly merging our digital persona with our real-life experiences. It's a frontier where security battles exploitation, defining our digital era.

AI's role in the battle

Enter artificial intelligence (AI), a technological marvel that has promised to revolutionize cybersecurity. With its ability to process vast amounts of data, recognize patterns, and make split-second decisions, AI offers the potential to bolster our digital defences. But, like any powerful tool, AI can be a double-edged sword. It holds the key both to fortifying our security and to unleashing new forms of cyber threats.

Overview of the journey

In this article, we embark on a journey through the paradoxical realm of AI in cybersecurity. We'll begin by exploring the promises AI holds, from supercharging threat detection to automating security tasks. But stay with us as we venture deeper, for the path of AI in cybersecurity is not without its shadows. We'll uncover the darker side of AI, where it empowers cybercriminals, raises ethical dilemmas, and challenges the regulatory landscape. As we navigate these dualities, one thing will become clear: AI in cybersecurity is a potent force, capable of both safeguarding and endangering our digital world.

The promise of AI in cybersecurity

In an ever-evolving digital landscape where cyber threats are a constant presence, AI stands as a beacon of hope for bolstering our defences. This section explores the potential benefits of AI in the realm of cybersecurity, shedding light on how this powerful technology can transform our approach to digital protection.

Improved threat detection and response times

At the forefront of AI's contribution to cybersecurity lies its unparalleled capacity for threat detection and rapid response. Unlike rule-based systems that struggle to keep pace with the evolving tactics of cybercriminals, AI employs machine learning algorithms to analyze vast datasets in real-time. It excels at identifying anomalies and potential threats, allowing for lightning-fast detection and swift, proactive responses. This capability is critical in preventing data breaches and minimizing the impact of cyberattacks.

69%

of enterprises believe AI is necessary for cybersecurity due to increasing number of threats that cybersecurity analysts can handle.[1]

15%

average decrease in the median dwell time - the time between an attacker accessing their victim's systems and the attack being detected or executed.[2]

Enhanced automation for routine security tasks

AI-powered cybersecurity solutions offer a significant advantage by automating routine security tasks that once demanded substantial human effort. Activities such as continuous monitoring of network traffic, identifying vulnerabilities, and applying security patches can be handled efficiently by AI-driven tools. This not only reduces the workload on cybersecurity teams but also minimizes the risk of human error in these repetitive processes.

Scalability and adaptability

In the face of ever-evolving cyber threats, scalability and adaptability are paramount. AI-driven security systems exhibit the ability to effortlessly scale to handle increasing data volumes and a growing number of connected devices. Moreover, they possess the inherent capability to adapt and learn from new threat patterns, continuously improving their ability to safeguard digital environments. This adaptability is essential in an environment where cyber threats continually mutate and evolve.

A real-life example

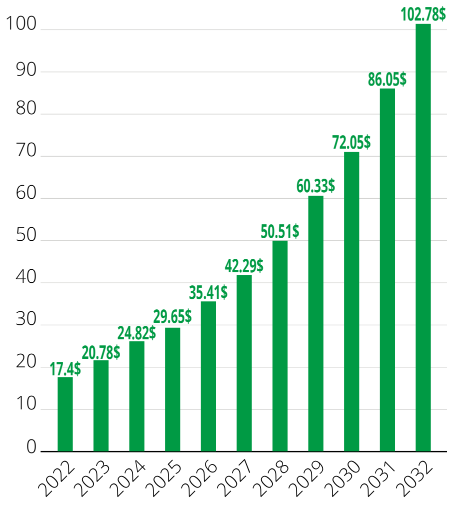
One particular case study exhibited how a leading technology company helped a global industrial supplier deploy an integrated set of managed security services that use AI to provide 100% visibility and the ability to process millions of events per day.[3]

The industrial supplier faced challenges such as increasing complexity and sophistication of cyber threats, lack of visibility and control over its global IT infrastructure, high cost and effort of managing multiple security tools and vendors, and limited availability and expertise of security analysts. The technology company helped the industrial supplier implement a comprehensive security solution that covered security monitoring and analytics, security orchestration and automation, security testing and optimization, and security services for cloud.

The solution used cognitive computing to augment human intelligence and automate the analysis of security incidents, AI to orchestrate and automate incident response actions, continuous testing and optimization of the security posture, and cloud security services. The benefits of the AI-based security solution for the industrial supplier included improved detection and prevention of cyberattacks, reduced time to respond and remediate incidents, enhanced visibility and control over the IT infrastructure, optimized security operations and reduced costs, and increased efficiency and productivity of security analysts.

This case study demonstrates how AI can help improve cybersecurity by enhancing automation for routine security tasks, improving threat detection and response times, and reducing human errors and biases.

The benefits are evident in the forecasts of the global AI in cybersecurity market size,[4] which was evaluated at US$17.4 billion in 2022 and is expected to hit around US$102.78 billion by 2032, growing at a CAGR of 19.43% between 2023 and 2032.



Source: www.precedenceresearch.com

Figure 1: Artificial intelligence (AI) in cybersecurity market size, 2022 to 2032 (US$ billion)

AI-powered threats: The dark side

While AI holds the promise of fortifying our digital defences, it also presents a dark and ominous facet. In this section, we venture into the shadowy realm of AI-powered cyber threats, where technology originally designed to protect can be turned into a potent weapon by malicious actors.

The emergence of AI-driven cyber threats

The rapid advancement of AI technology has given rise to a new breed of cyber threats. Attackers now harness the power of AI to craft more sophisticated and evasive attacks. AI-driven malware, for instance, can adapt to the target environment, making it exceptionally difficult to detect and mitigate. Similarly, AI can be employed in social engineering attacks, where it generates convincing phishing messages tailored to exploit individual vulnerabilities leveraging a new technique referred to as "deepfake."

AI in action

These threats are not theoretical; they have materialized in various forms, highlighting the potency of AI in the hands of malicious actors.

- Earlier this year, hackers used AI to bypass Bitfinex's biometric authentication system, which required users to verify their identity with their face and voice. The hackers injected fake video streams into the verification process, fooling the system into thinking that they were the legitimate users. The hackers also used deepfake technology to create realistic facial images that matched the voice and behavior of the victims. The hackers stole US$150 million worth of various digital assets, including Bitcoin, Ethereum, and Tether.[5]
- In 2021, a cyber espionage campaign dubbed Operation Diànxùn was uncovered by researchers from McAfee.[6] The campaign used AI to create phishing emails that targeted telecommunications companies around the world. The emails used natural language generation to craft convincing messages that appeared to come from legitimate sources, such as job recruiters or industry experts. The emails contained malicious attachments or links that delivered malware to the victims' devices.
- In 2020, a cryptocurrency platform was targeted by a voice-spoofing attack that used AI to impersonate the CEO's voice and tricked an employee into transferring US$243,000 to a fraudulent account.[7]

These examples underscore the alarming reality of AI-driven threats. As we delve into the statistics that illuminate the prevalence of such attacks, it becomes evident that these incidents are not isolated; they represent a growing trend in the world of cybersecurity.

According to a report from Webroot, more than 90% of cybersecurity professionals are concerned that hackers will use AI in cyberattacks against their company that are more sophisticated and harder to detect. Similarly, a survey by CyberArk found that 93% of cybersecurity professionals expect AI-enabled threats to impact their organization. Finally, based on research conducted by Checkpoint,[8] the average weekly cyberattacks per organization by region shows a significant increase across all regions in 2022 compared to 2021 thanks to generative AI models.

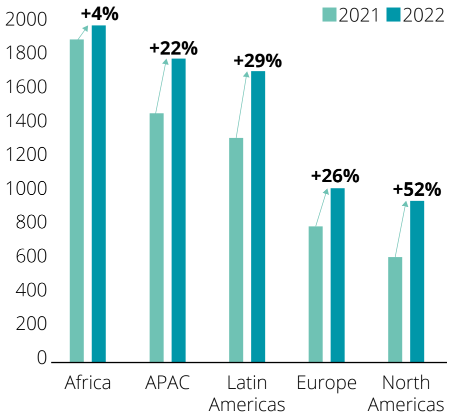


Figure 2: Average weekly cyberattacks per organization per region

These statistics highlight the growing concern within the cybersecurity community about the potential for AI-powered threats.

The regulatory landscape

The regulatory landscape surrounding AI in cybersecurity is a critical aspect of ensuring responsible and secure AI implementation.

Examination of current regulations

Governments and regulatory bodies worldwide are increasingly recognizing the need to establish guidelines and regulations for AI in cybersecurity. These regulations aim to address the ethical, privacy, and security concerns associated with AI technologies. The field of AI regulation is still evolving globally; therefore, businesses should respond proactively to AI regulations by developing a robust AI governance program that informs the AI lifecycle.

In recent years, several countries and regions have issued or proposed AI-related laws and regulations covering various aspects such as data protection, human rights, accountability, transparency, and safety. Some of the notable examples are:

- The EU's Artificial Intelligence Act, which is a comprehensive legislative proposal that aims to create a harmonized legal framework for AI in the EU. The proposal defines four categories of AI systems based on their risk level and sets out different requirements and obligations for each category. The proposal also establishes a European Artificial Intelligence Board to oversee the implementation and enforcement of the rules.
- The US's National Artificial Intelligence Initiative Act, which is a law that establishes a coordinated federal initiative to accelerate AI research and development, promote public-private partnerships, foster education and workforce development, and ensure ethical and trustworthy AI. The law also creates a National Artificial Intelligence Advisory Committee to provide advice and recommendations to the federal government.

From the perspective of the Middle East, Saudi Arabia has specific regulations and policies related to AI. The Saudi Data and Artificial Intelligence Authority (SDAIA) is responsible for the country's AI regulations. The SDAIA has created a data governance framework at the national level that outlines the laws and regulations for national data management and governance, as well as the protection of personal data. This framework includes:

- Data Management and Personal Data Protection Regulations and Standards
- National Data Governance Policies
- Data Classification Policy and Regulations
- Personal Data Protection Law and The Implementing Regulation
- Data Sharing Policy and Regulations

In addition to this, the Saudi Food & Drug Authority has published guidance on AI and 'Big Data' in the context of medical devices. These regulations aim to ensure that AI is used responsibly and ethically, while also promoting innovation and growth in the field.

While in the United Arab Emirates (UAE) regulators and organizations, such as the UAE's Ministry of AI and Smart Dubai, have taken a soft approach to regulation, mostly in the form of non-binding guidelines. These guidelines are intended to foster the development and uptake of AI in an ethical, transparent, and responsible manner while minimizing pitfalls such as discrimination and algorithmic bias.

Industry standards and compliance

Government regulations are not the only factors influencing the role of AI in cybersecurity. Industry-specific standards and compliance frameworks are equally crucial. These guidelines, which organizations follow to ensure their AI systems align with industry best practices, are continually evolving. For instance, the NIST AI Risk Management Framework (AI RMF), launched on 26 January, 2023, is a key standard in this domain. This framework, developed through public-private collaboration, is designed to enhance trustworthiness in the design, development, use, and evaluation of AI products and services.

In the same vein, the ISO/IEC AWI 27090 is another significant standard under development that addresses security threats and failures in AI systems. It aims to equip organizations with a better understanding of the implications of security threats to AI systems throughout their lifecycle and offers strategies for detecting and mitigating such threats.

As the integration of AI in cybersecurity becomes more prevalent, experts across the field emphasize the pressing need for robust, enforceable policies. Many argue for the establishment of stringent laws and regulations to govern the ethical and secure usage of AI. Striking the delicate balance between fostering innovation and implementing necessary regulations stands as a pivotal challenge as we advance into an increasingly digital future.

Striking the right balance: Mitigating risks

Striking the right balance in the use of AI in cybersecurity is a formidable task, akin to walking a tightrope. On one side, we have the transformative potential of AI, which promises to revolutionize cybersecurity with unprecedented levels of protection and resilience. On the other side, we face the risks of misuse and unintended consequences, which could amplify existing threats or create new vulnerabilities.

Navigating this delicate equilibrium demands a proactive and dynamic approach. Organizations need to stay abreast of the latest advancements in AI and continually assess and address the evolving landscape of risks associated with its use. It's about making informed decisions, leveraging AI's strengths to enhance cybersecurity defences while taking calculated measures to minimize its potential pitfalls.

However, adopting AI in cybersecurity is not just about harnessing its power; it's about doing so responsibly and judiciously. This is where continuous education and awareness come into play. As AI continues to evolve at a rapid pace, so too does the complexity of the risks associated with its use in cybersecurity. This dynamic landscape necessitates a commitment to ongoing learning and awareness at all levels of an organization.

Continuous education empowers individuals and organizations to stay ahead of the curve, equipping them with the knowledge and skills to leverage AI effectively and safely. It fosters a culture of vigilance, where potential risks are identified and mitigated proactively rather than reactively. Moreover, awareness plays a crucial role in ensuring that all stakeholders understand the implications of AI in cybersecurity. It promotes informed decision-making and encourages responsible use of AI.

In essence, striking the right balance between reaping AI's benefits in cybersecurity and mitigating its risks isn't a one-time effort. It's a continuous journey that requires constant education, heightened awareness, and an unwavering commitment to navigate the ever-evolving landscape of AI in cybersecurity responsibly and effectively.

Concrete steps to be taken include: Firstly, defining a controls framework is crucial. This involves establishing a comprehensive set of policies, standards, guidelines, and best practices that govern the development, deployment, and use of AI systems within an organization. It sets the foundation for responsible and secure AI usage.

Secondly, developing a defensible security architecture is key. This means designing and implementing a robust and resilient architecture capable of protecting AI systems from both internal and external threats. It's about building fortifications around AI assets.

Thirdly, implementing tailored security solutions for AI can provide an added layer of protection. Specialized tools and platforms specifically crafted for testing, validating, monitoring, and moderating AI solutions can help ensure their integrity and reliability.

Lastly, bolstering defense by harnessing AI threat intelligence is essential. With the emergence of new AI-specific cyber threats, adopting a proactive and holistic approach to secure AI systems and applications becomes paramount. It's about staying one step ahead of potential threats.

In conclusion, securing AI in cybersecurity is a multifaceted challenge that requires a strategic blend of policy-making, architectural design, specialized solutions, and threat intelligence. It's a journey that demands continuous effort, vigilance, and adaptation.

By **Tamer Charife**, Cyber Emerging Technologies Leader, Cyber Risk Services and **Michael Mossad**, Cyber Emerging Technologies Director, Deloitte Middle East

As AI continues to evolve at a rapid pace, so too does the complexity of the risks associated with its use in cybersecurity. This dynamic landscape necessitates a commitment to ongoing learning and awareness at all levels of an organization.

Endnotes

1. https://zipdo.co/statistics/ai-use-in-cyber-security/.
2. https://securityintelligence.com/news/global-median-dwell-time-drops-to-record-low/.
3. https://www.ibm.com/case-studies/andritz.
4. Artificial Intelligence (AI) Market Size, Growth, Report By 2032 (precedenceresearch.com).
5. Bitfinex Owner Offers $150M Buyback to Bitcoin (BTC) Hack Victims - Bloomberg.
6. https://blog.avast.com/deepfake-voice-fraud-causes-243k-scam.
7. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-dianxun-cyberespionage-campaign-targeting-telecommunication-companies/.
8. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - Check Point Blog.