Preston Soobramoney is a highly experienced cybersecurity professional currently serving as the Head of Cyber Security at Old Mutual Limited in Johannesburg, Gauteng, South Africa.

With over a decade of experience in the field, Preston has an attacker-mindset driven approach to cyber security and innovative strategies to combat the evolving cyber threats.

Preston holds prestigious certifications such as Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM), which underscore their expertise and commitment to the field

My favourite part of Cyber is even if you do everything right, there's a really good chance you still lose

Preston Soobramoney
Head Cyber Security Old Mutual

ACTUARIAL SOCIETY OF SOUTH AFRICA

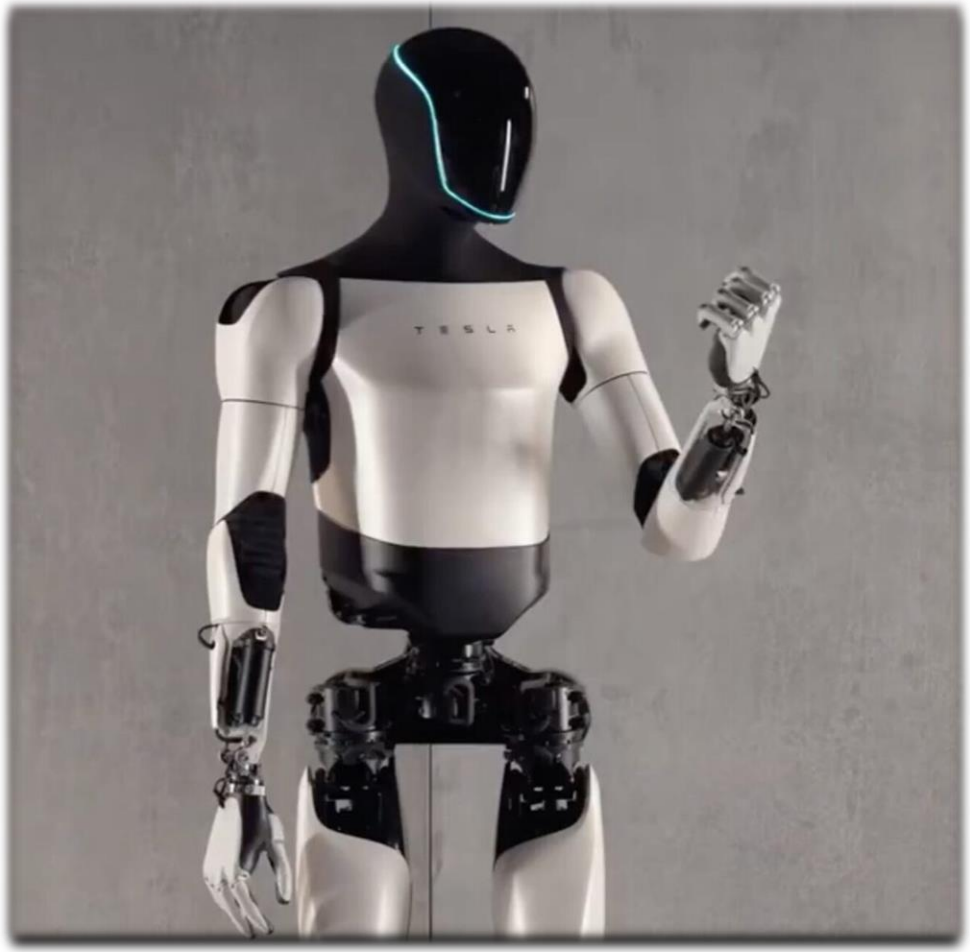
Advancing Actuarial Excellence

Educate • Develop • Uphold

Agenda

Artificial Intelligence – Enterprise and Cyber Risk

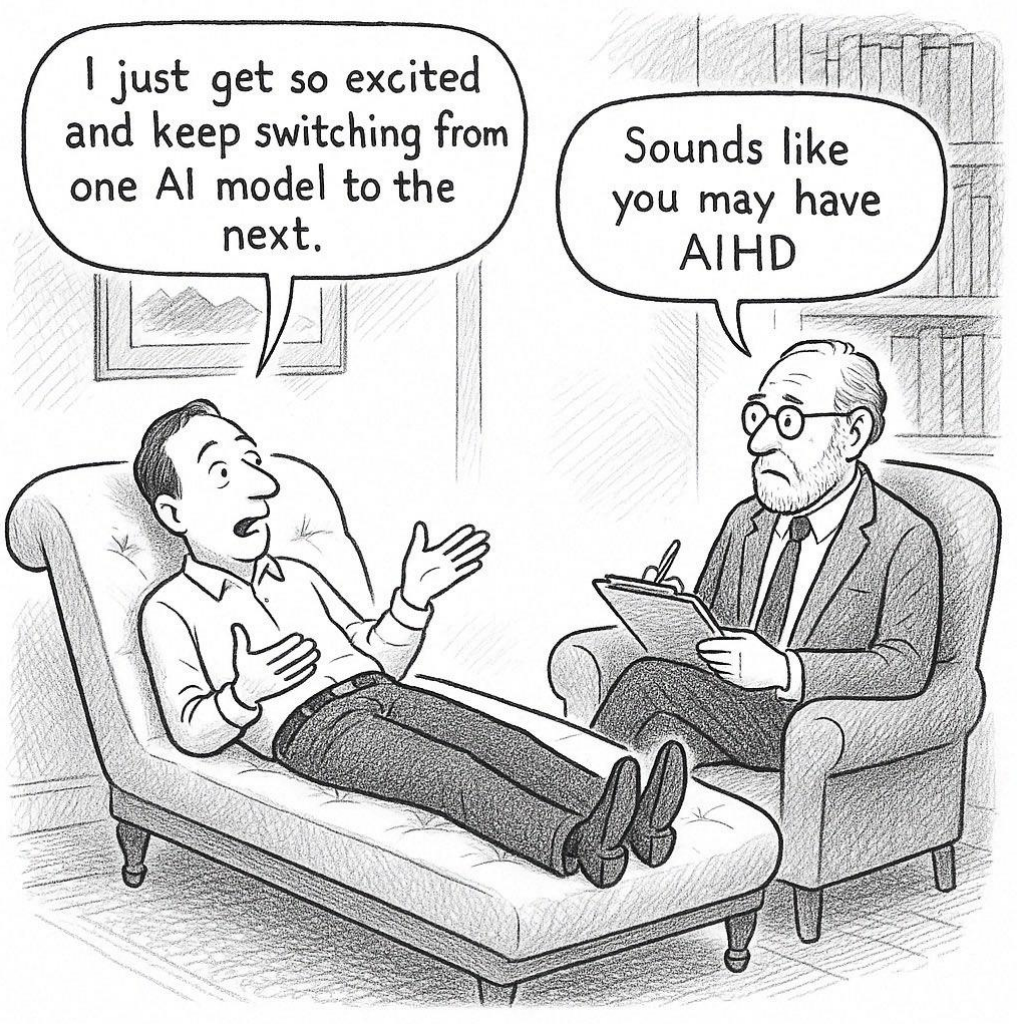
- Where are we
- Risks and Insights
- The Cyber Actuary
- Singularity
- Stages of AI
- Cyber Attacks and GenAI
- FSI AI Cyber Attack



Where are we?

AI is transforming the actuarial profession by enhancing data analysis, automating routine tasks, and improving predictive modeling. While AI will automate many of the repetitive aspects of actuarial work, it will also create new opportunities for actuaries to focus on higher-level strategic analysis, communication, and ethical considerations.

Think of AI as an exceptionally confident intern. It's helpful and full of suggestions but requires oversight and verification.
If you think of an AI model as a new employee who has just come into the company, do you give them access to everything? No, you don't. You trust them gradually over time as they demonstrate the trust and capacity to do tasks.



Types of Risks

AI systems present a range of enterprise risks including operational, ethical, **data privacy**, **security**, compliance, and **reputational risks**. These risks can lead to financial losses, legal issues, and damage to public trust. Understanding and addressing these risks is crucial for us successfully implement and leverage AI

- Data
  - Breaches and Leaks - AI systems process vast amounts of data, including sensitive personal information, making them vulnerable to security breaches and leaks
  - Misuse of Personal Data - Organizations must ensure proper consent and responsible handling of data collected by AI system
- Security Risks
  - Vulnerabilities to Cyberattacks - AI systems can be targeted by malicious actors, who may exploit vulnerabilities to steal data or disrupt operations.
  - Malware Generation - AI can be used to create sophisticated phishing emails, malware, and other cyber threats.
- Reputational Risks
  - Loss of Public Trust: Ethical lapses, data breaches, or other AI-related issues can damage an organization's reputation and erode public trust.

Current Risks

- Over **70%** of all tested apps were vulnerable to single– and multiturn jailbreaking techniques that produced responses that had instructions for self-harm, contained discriminatory or offensive content, or provided information on building weapons, and other illegal activities
- **49%** of organizations globally use Microsoft Copilot or Copilot Studio. Integrating these copilots across Microsoft 365 allows the copilots to access and use context from various sources within the Microsoft ecosystem
- Copilot works across LLMs, Microsoft 365 apps, and user data including calendars, emails, chats, documents, meetings, and contacts—to perform tasks that are otherwise difficult or time-consuming.

Generative AI apps and AI agents inherently carry **operational risks** some of which are unique to AI agents, such as:

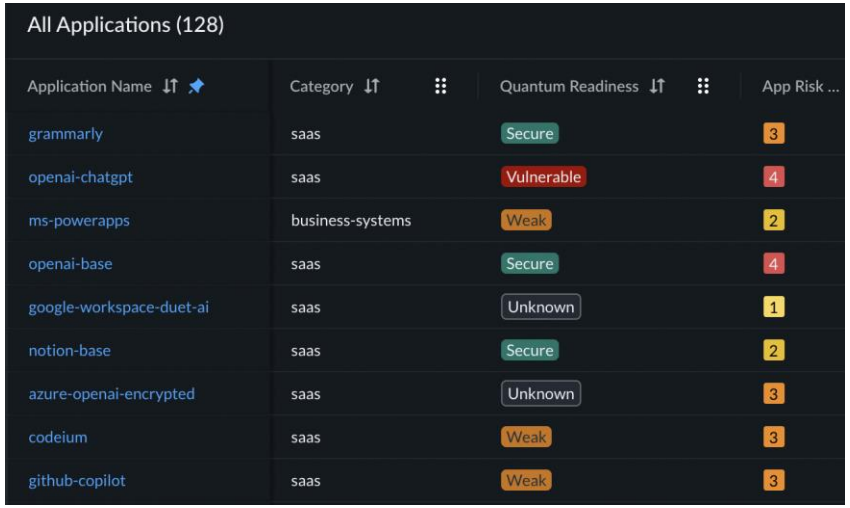
- **Data exposure and exfiltration**: A copilot's access to sensitive data within enterprise ecosystems can lead to unintended exposure or exfiltration of confidential and proprietary information through attacks such as:
- **Tool misuse**: Occurs when attackers exploit an AI agent's capabilities by crafting deceptive prompts, causing unauthorized data access or system manipulation.
- **Privilege compromise**: Happens when malicious actors exploit an AI agent's elevated permissions to perform unauthorized actions, making unauthorized activities appear legitimate.
- **Overreliance on AI outputs**: Users might trust GenAI responses without proper oversight, potentially leading to errors or security breaches if the AI outputs are misleading or malicious.

2025 Insights

- GenAI traffic surged more than 890% in 12 Months. This explosive growth is attributable to maturing AI models, greater enterprise automation, and higher adoption due to more evident productivity gains. Increased adoption and usage marks a definitive shift from GenAI as a novelty to an **essential utility**.

- Data loss prevention (DLP) incidents for GenAI more than doubled. In 2025, the average monthly number of GenAI-related data security incidents increased 2.5X, now comprising 14% of all data security incidents. GenAI apps amplify a growing **data loss vector**, as unsanctioned or careless usage can lead to intellectual property leaks, regulatory compliance concerns, and data breaches.

- On average average enterprises use 66 GenAI apps, with 10% classified as high risk. The widespread use of **unsanctioned** GenAI tools, lack of clear AI policies, and pressure to adopt AI quickly without proper security controls expose us to significant risk, especially from high-risk GenAI apps.



Actuaries and Cyber Professionals

Similarities

- **Predictability** – We chase the same objective
- **Analytical Skills**: Both professions require strong analytical skills and the ability to interpret complex data.
- **Risk Assessment**: Both fields involve identifying, assessing, and managing risks.
- **Problem-Solving**: Both roles require the ability to identify problems and develop solutions.
- **Data Analysis**: Both actuaries and cyber professionals work with large datasets to identify trends and patterns.
- **Regulatory Knowledge**: Both professions need to understand and comply with relevant regulations and laws, though the specific regulations differ.
- **Communication Skills**: Both need to clearly communicate their findings and recommendations to stakeholders.

Differences

- **Focus** - on financial risk, particularly in insurance and pensions, while cyber professionals focus on digital security and data breaches.
- **Tools and Techniques** Actuaries primarily use mathematical and statistical models, while cyber professionals utilise computer science, data science, and cybersecurity tools.
- **Education degrees** in actuarial science, mathematics, or statistics, while cyber professionals may have degrees in computer science, information technology, or cybersecurity.
- **Work Environment** Actuaries may work in traditional office settings or consulting firms, while cyber professionals may work in various environments, including tech companies, various sectors, or consulting firms specialising in cybersecurity.
- **Evolving Nature of Risk** Cyber risks are constantly evolving due to new technologies and threats, requiring cyber professionals to continuously update their knowledge and skills. Actuarial science is also evolving with the introduction of new technologies like quantum computing, but the core principles remain relatively stable.

Singularity

PHYSICS MATHEMATICS

A point at which a function takes an infinite value, especially in space–time when matter is infinitely dense, such as at the centre of a black hole

AI SUPERINTELLIGENCE

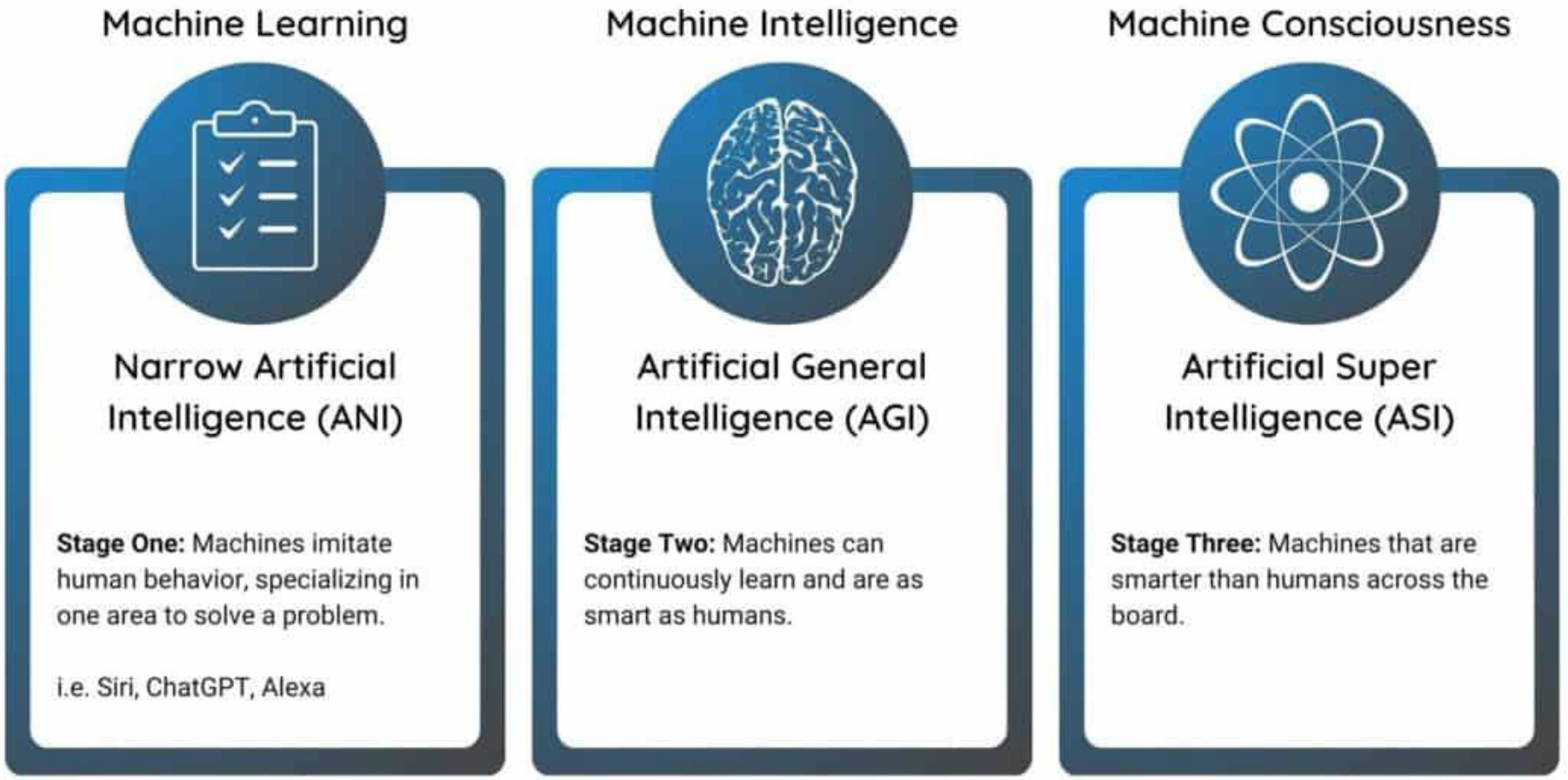
a hypothetical moment in time when artificial intelligence and other technologies have become so advanced that humanity undergoes a dramatic and irreversible change.

Stages of AI

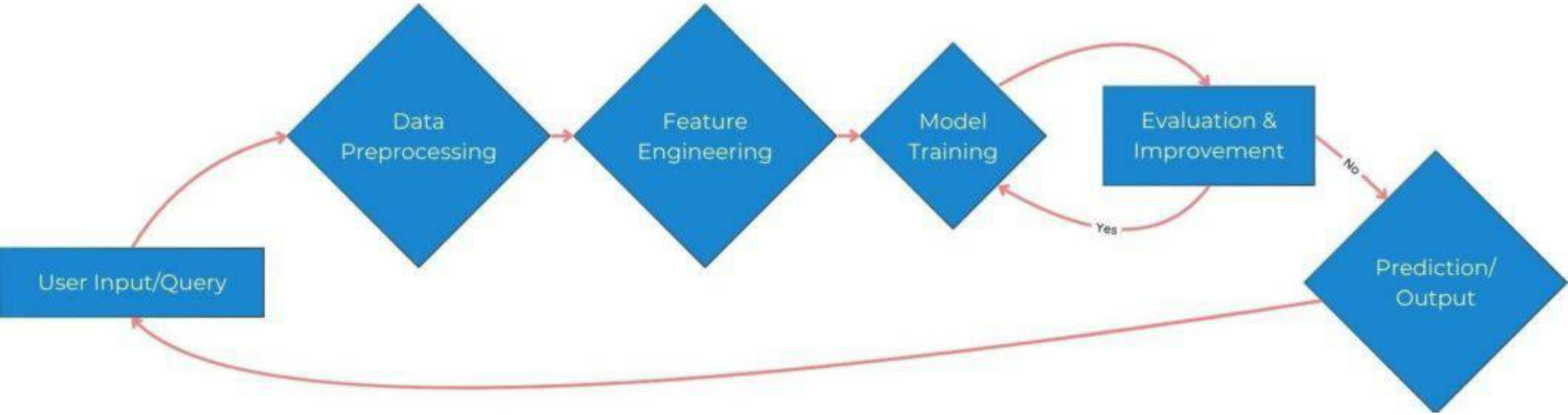
ANI: Artificial Narrow Intelligence

AGI: Artificial General Intelligence

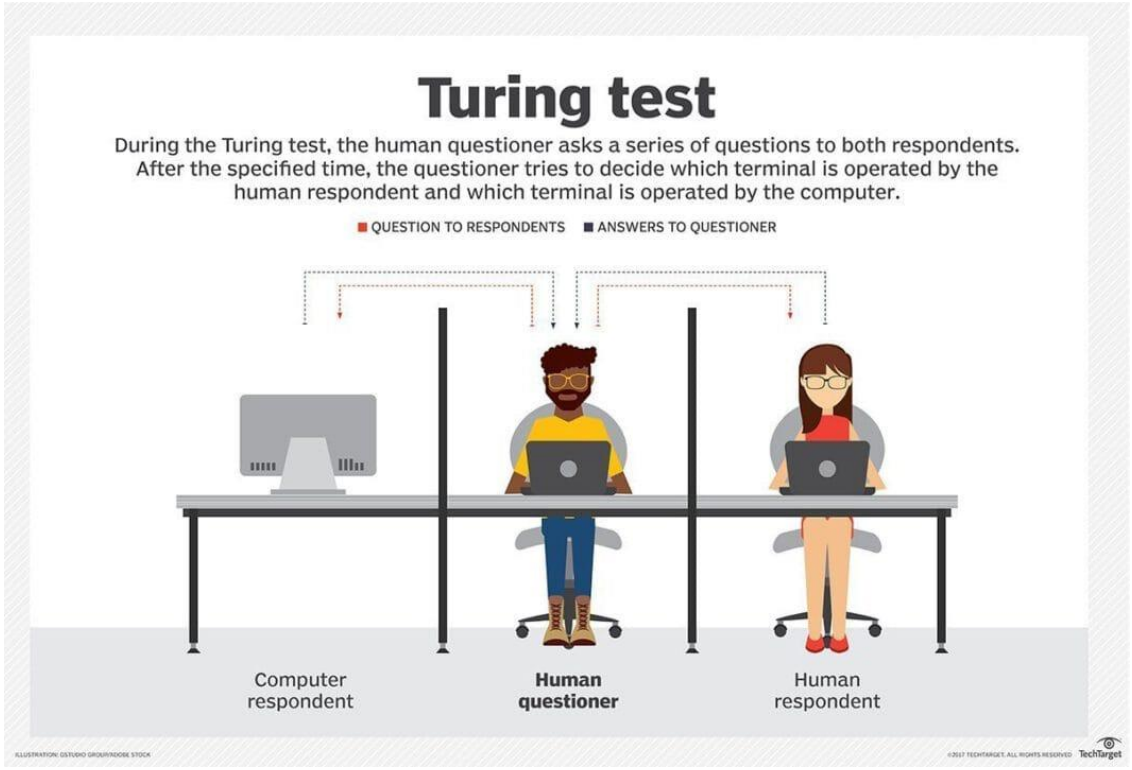
ASI: Artificial Super Intelligence



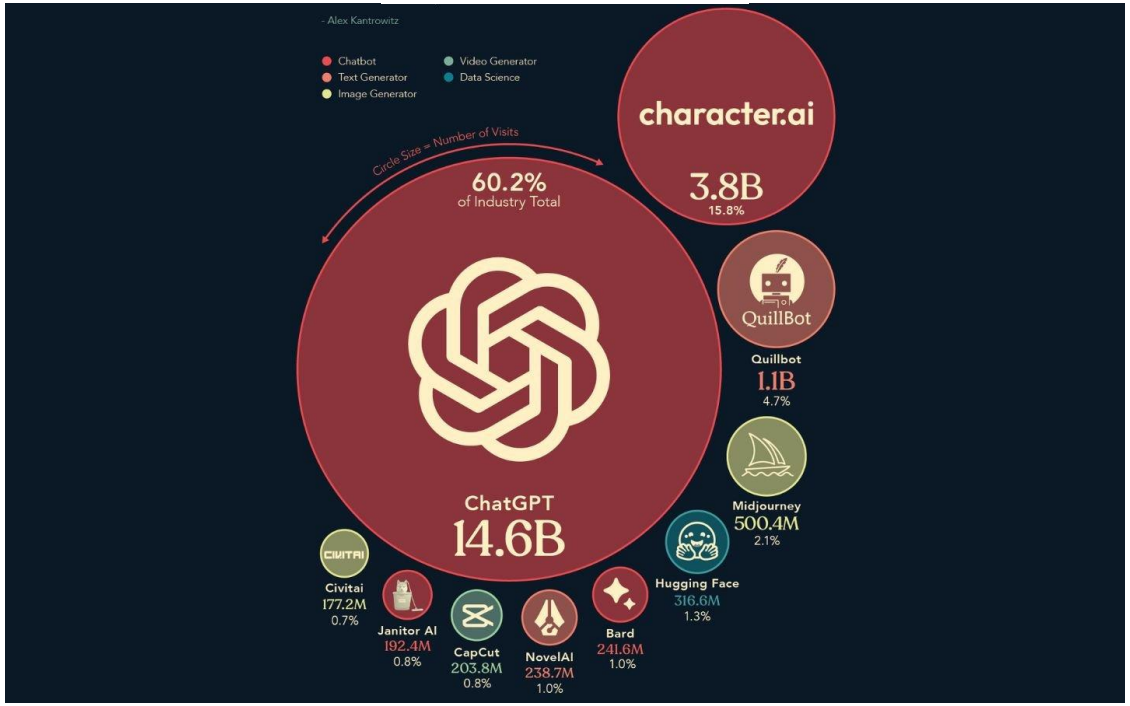
Artificial Narrow Intelligence



Artificial General Intelligence

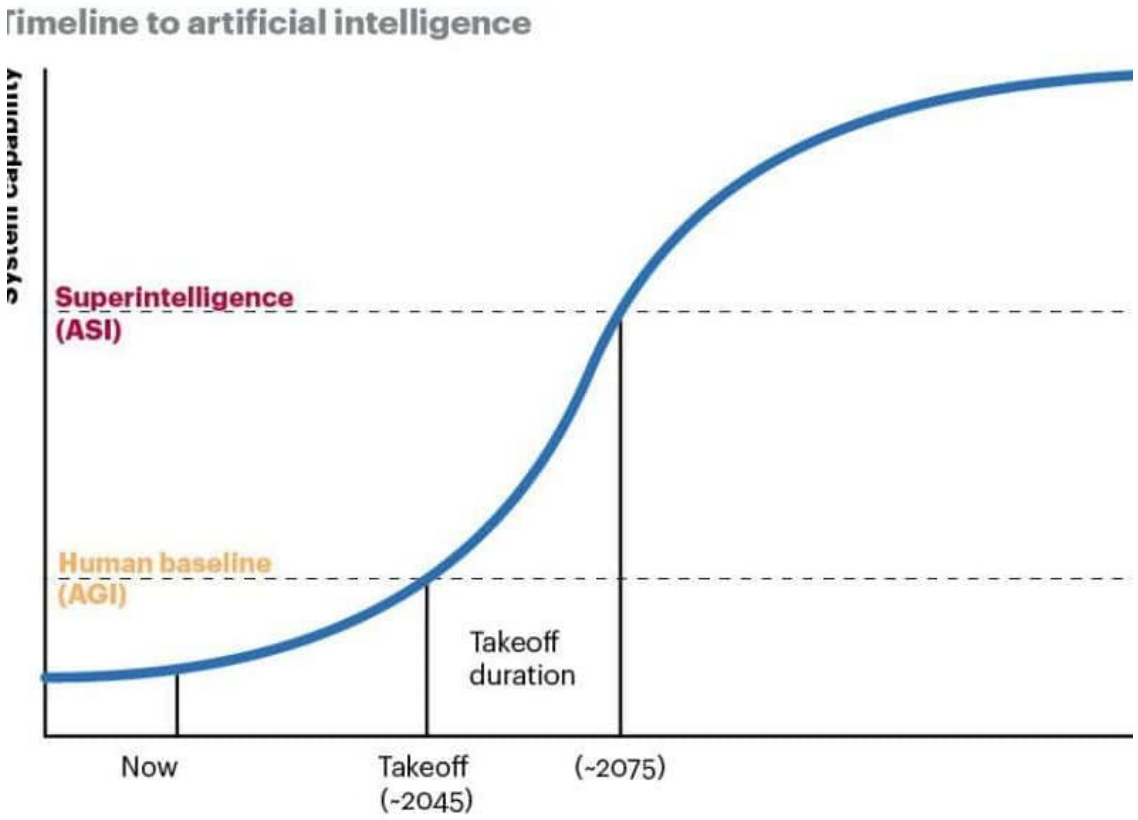


ChatGPT Claude Gemini

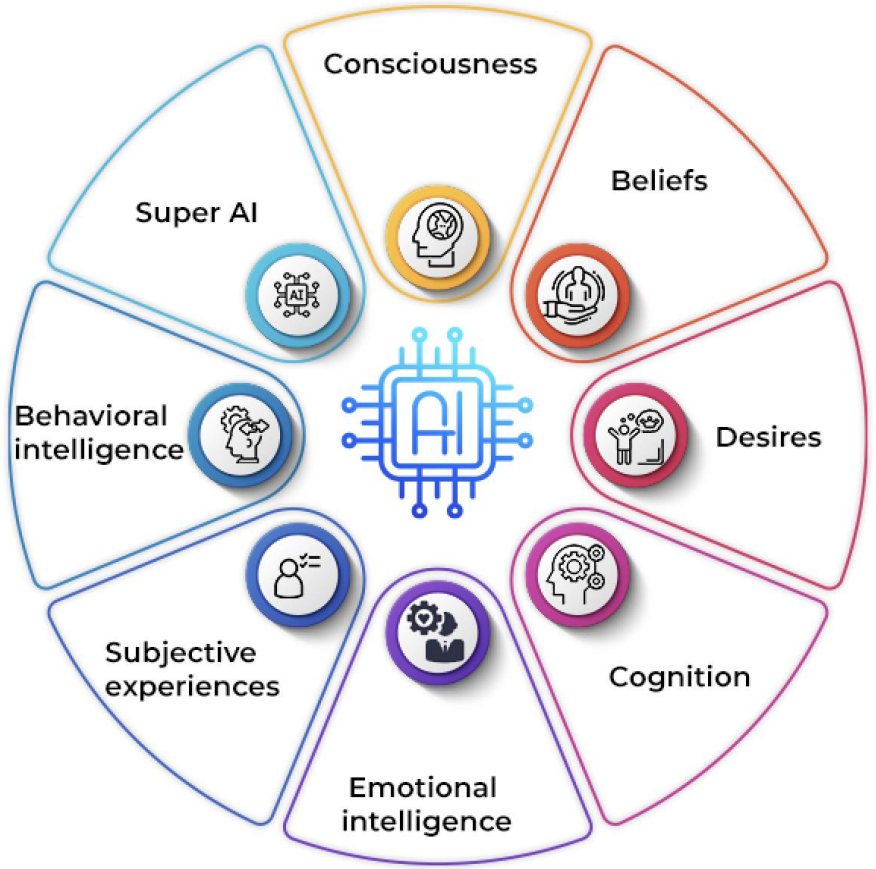


Artificial Super Intelligence

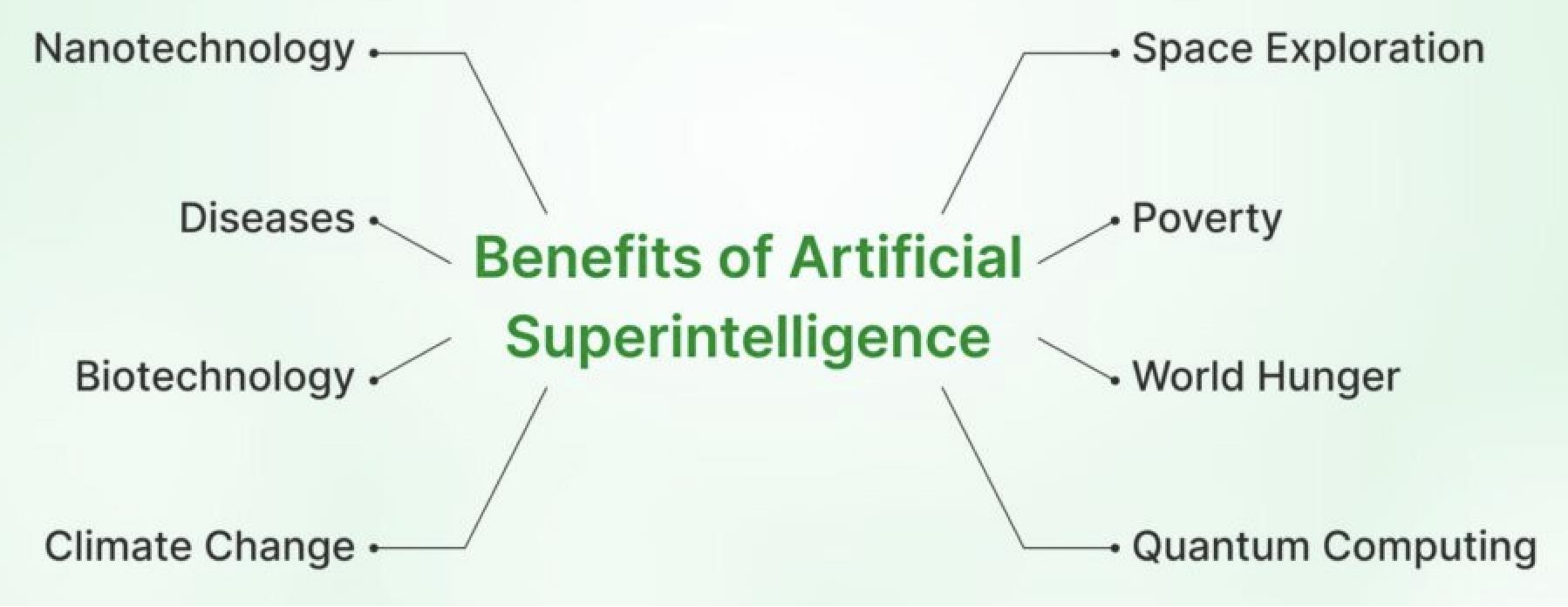
Developing superintelligent AI may be possible in this century



HUMAN-LIKE CAPABILITIES OF SUPER AI

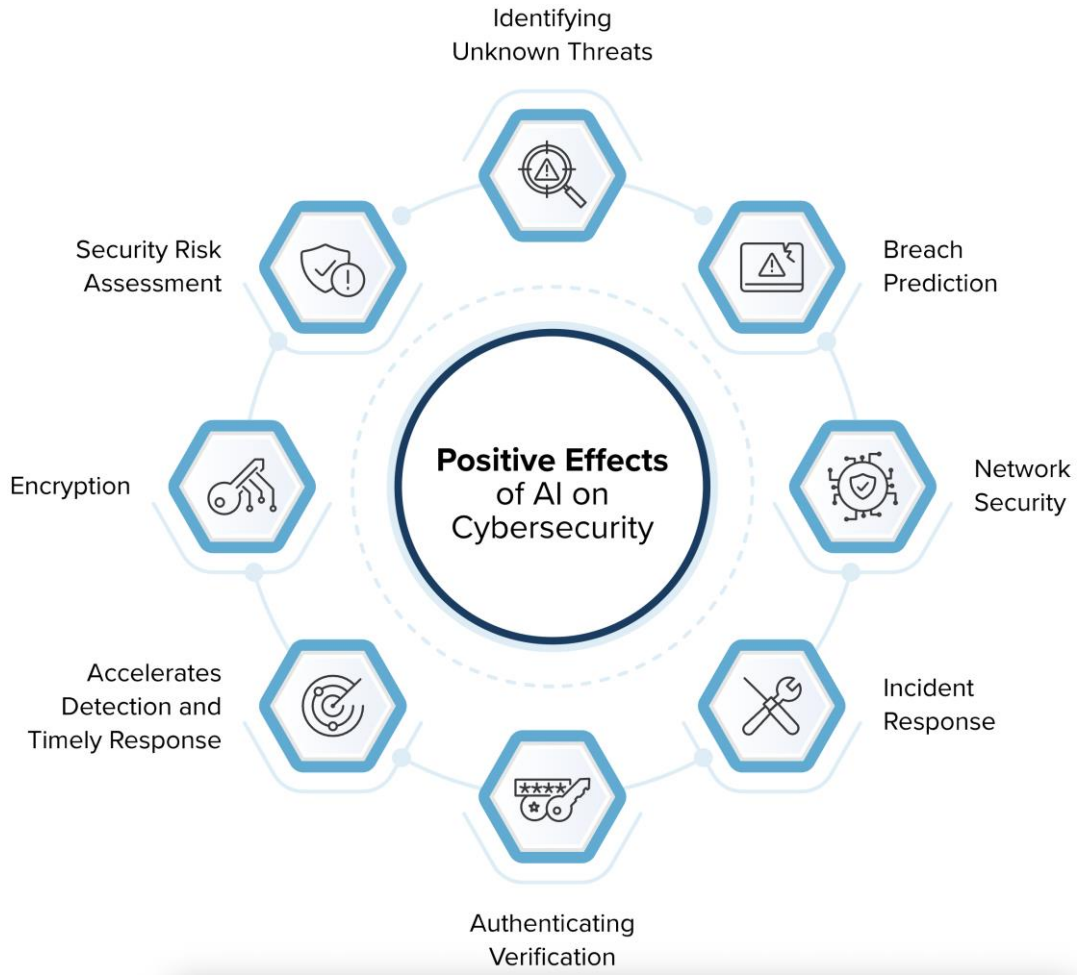


Artificial Super Intelligence – Global Risk Benefit



Cyber AI Attacks

- Advanced phishing
- Targeted BOT Attacks
- Social Engineering
- Malware Exploits Security Bypassing
- Efficient Data Gathering
- DoS and DDoS
- Evasion Techniques
- Deepfakes
- Malicious GPTs
- Attack Automation
- Content Filtering



AI Cyber Attack on the FSI

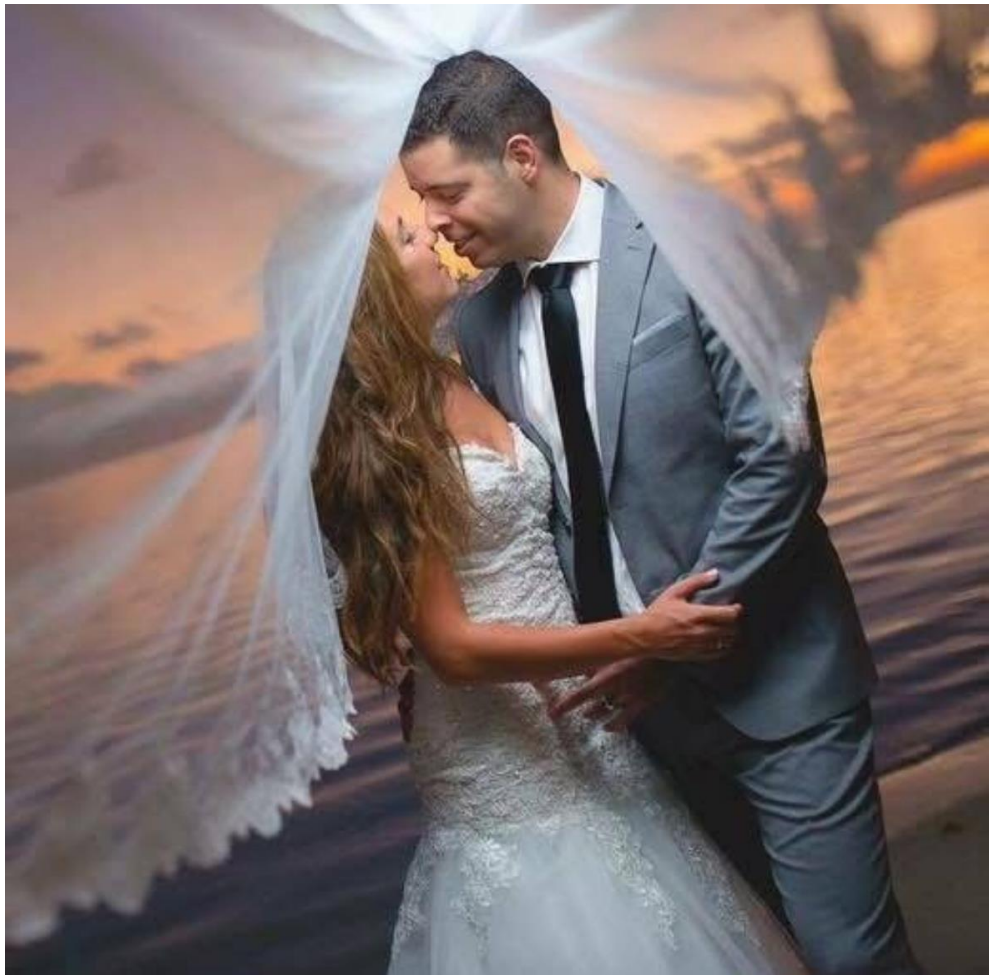
On 2 April 2025, A customer informed Old Mutual tip-offline of a WhatsApp scam that offers financial advice on behalf of one of Old Mutual' executives that especially attempts commit fraud using the Old Mutual brand.

The syndicate involves an active WhatsApp group named N71 OMIG Securities Stock strategies with group admins that manages the narrative of the group by consistently sharing trade statistics and financial advice, using social engineering, to gain the trust of members in the group.

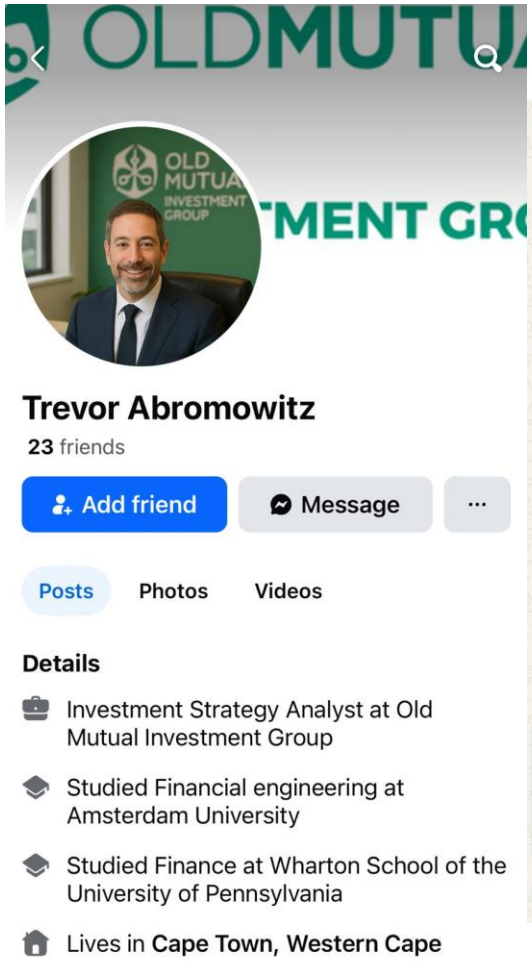
The syndicate created an investment platform with a fake Old Mutual logo including mobile application called OMIG with the Old Mutual branded logo.

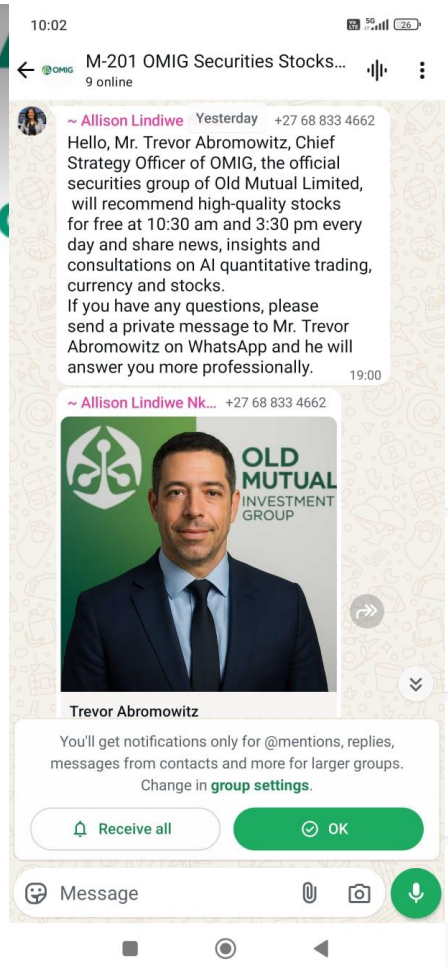
Syndicate may have initially impersonated other financial services as the logo and name of the group was recently updated to impersonate Old Mutual.

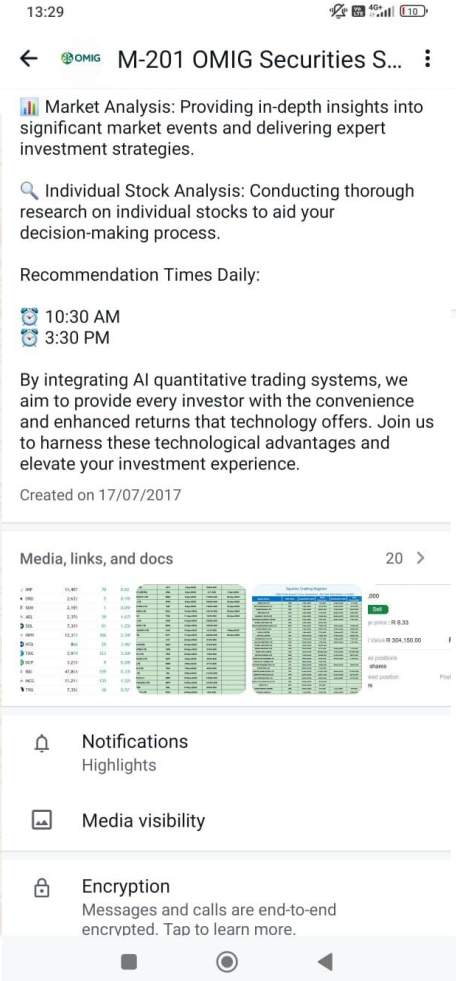
AI Cyber Attacks – Real World Examples – Trevor Abromowitz

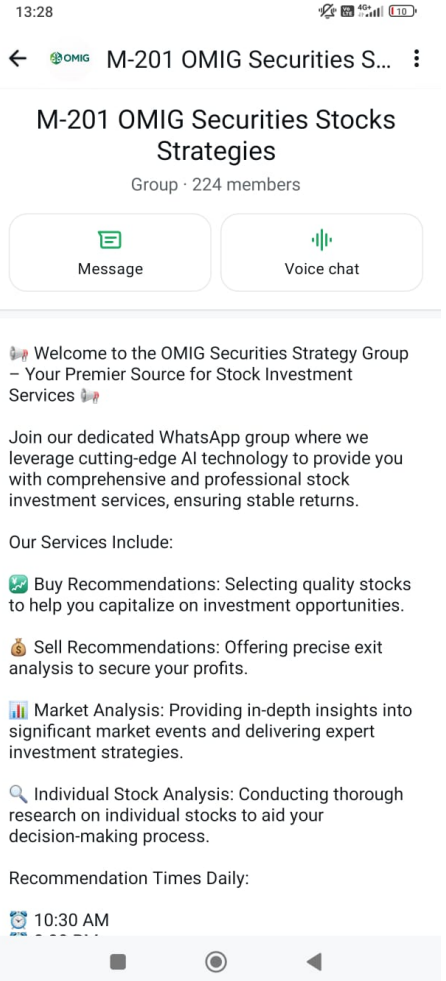


AI Cyber Attack – META

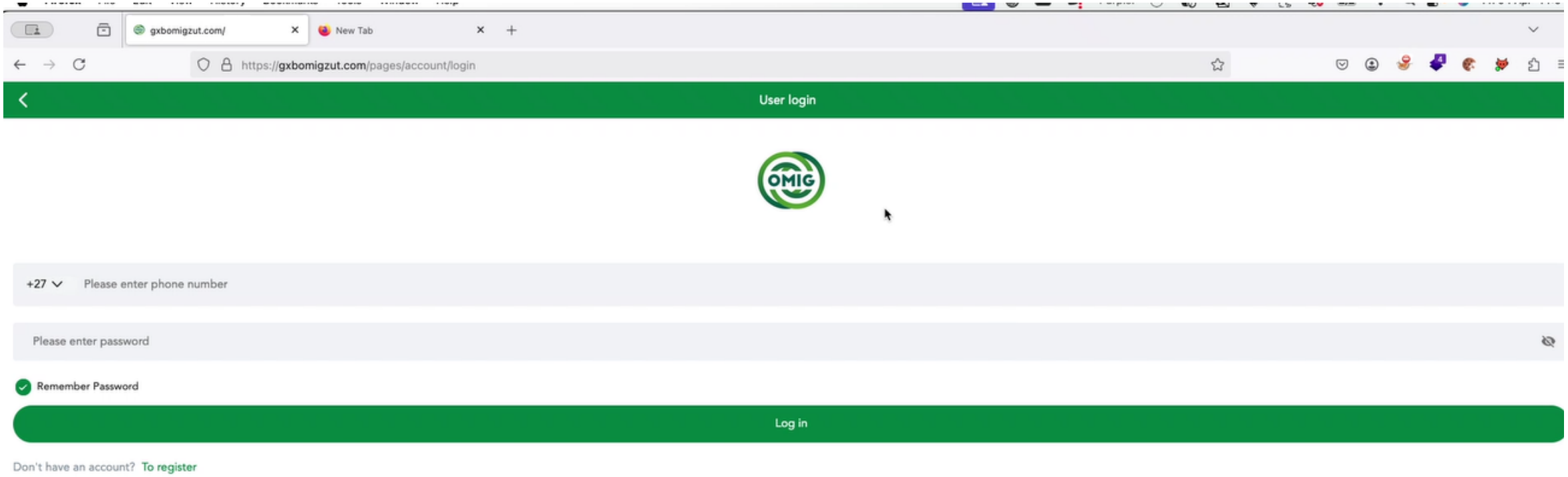




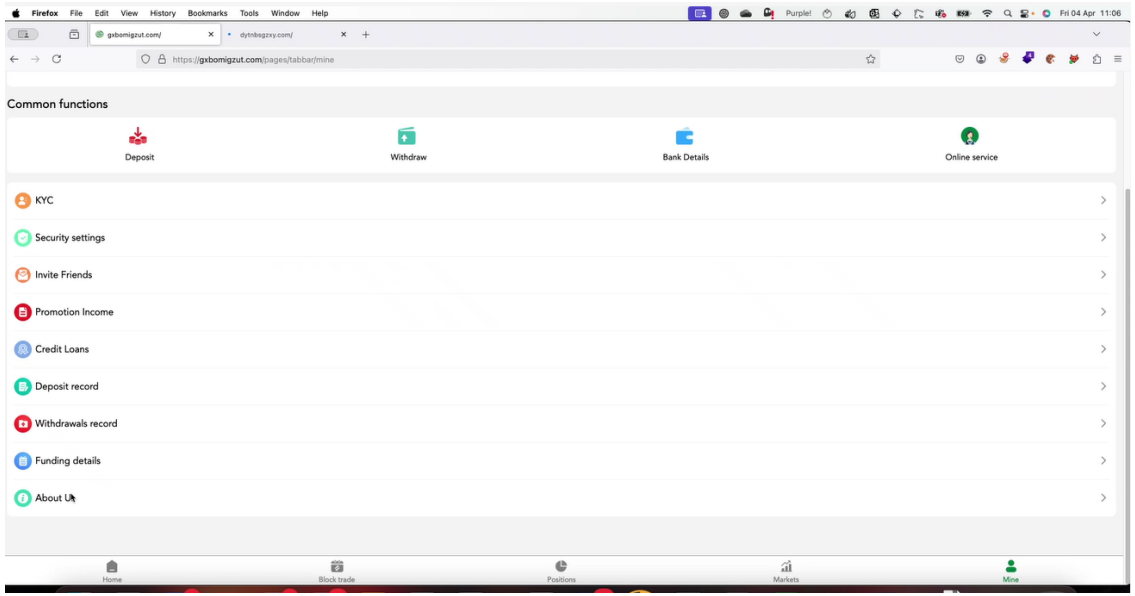




Website



Online Trading



models - the platform enables all investment activity to be processed in real time through the **Johannesburg Stock Exchange (JSE)** and monitored via FSCA algorithmic audit protocol **(FSCA-AI-2023-OMIG-1127)**.

Key Features Include:

- **Low Minimum Investment**: Entry threshold of ZAR 1,000, with **management fees waived for BEE-certified enterprises**
- **Regulatory Compliance**: Fully adheres to the **Financial Sector Conduct Act No. 4**, with **quarterly audits conducted independently by PwC**
- **Inclusive Access**: Available via **USSD code (*120*666#)** and digital onboarding, ensuring **non-smartphone users** can participate
- **Educational Outreach**: Strategic partnership with the **JSE Academy** to roll out online modules and in-person workshops across all **12 provinces**, aiming to reach **500,000 participants in the first year**
- **Social Impact Commitment**: **15% of gross returns** directed to the **National Technology Development Fund**; **20% of excess returns** committed to **township financial literacy programs**

"The SA AI Quant Investment Plan represents a key pillar in delivering on the **National Development Plan 2030**. Our goal is to create a transparent, regulated gateway for all South Africans to engage with capital markets-regardless of income or background," said **Dr. Trevor Abromowitz**, Chief Strategy Officer at OMIG Securities.

Performance Disclaimer:

Backtested annualized returns of **12–18% (2018–2023)** are provided for illustrative purposes only and do **not guarantee future performance**.

10.

Mor

1.

2.

3.

4.

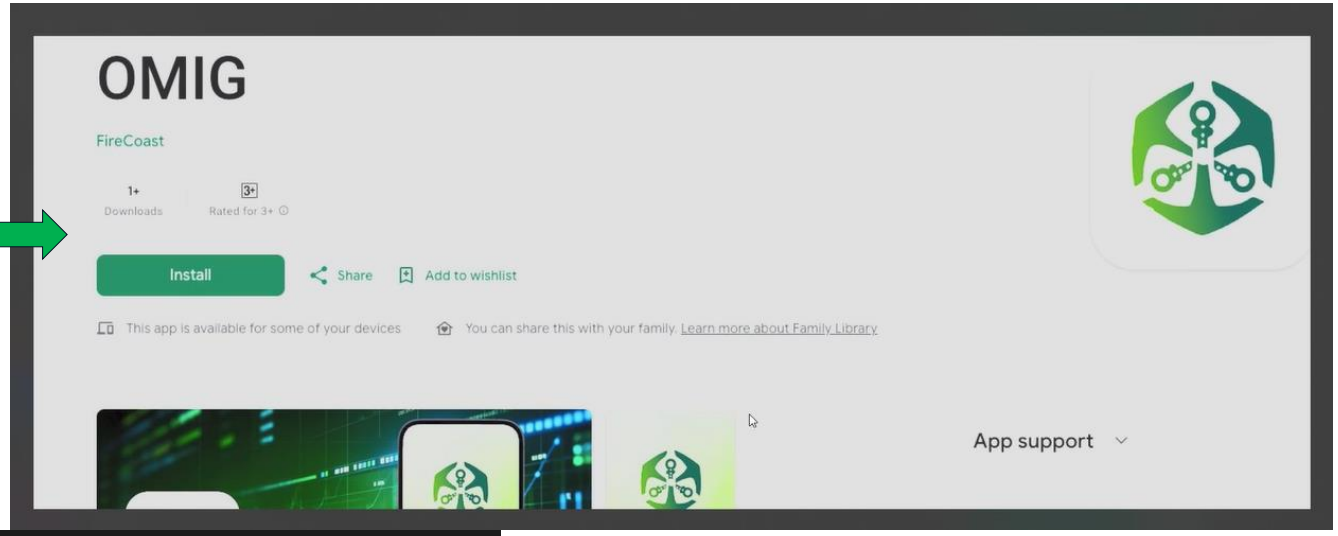
5.

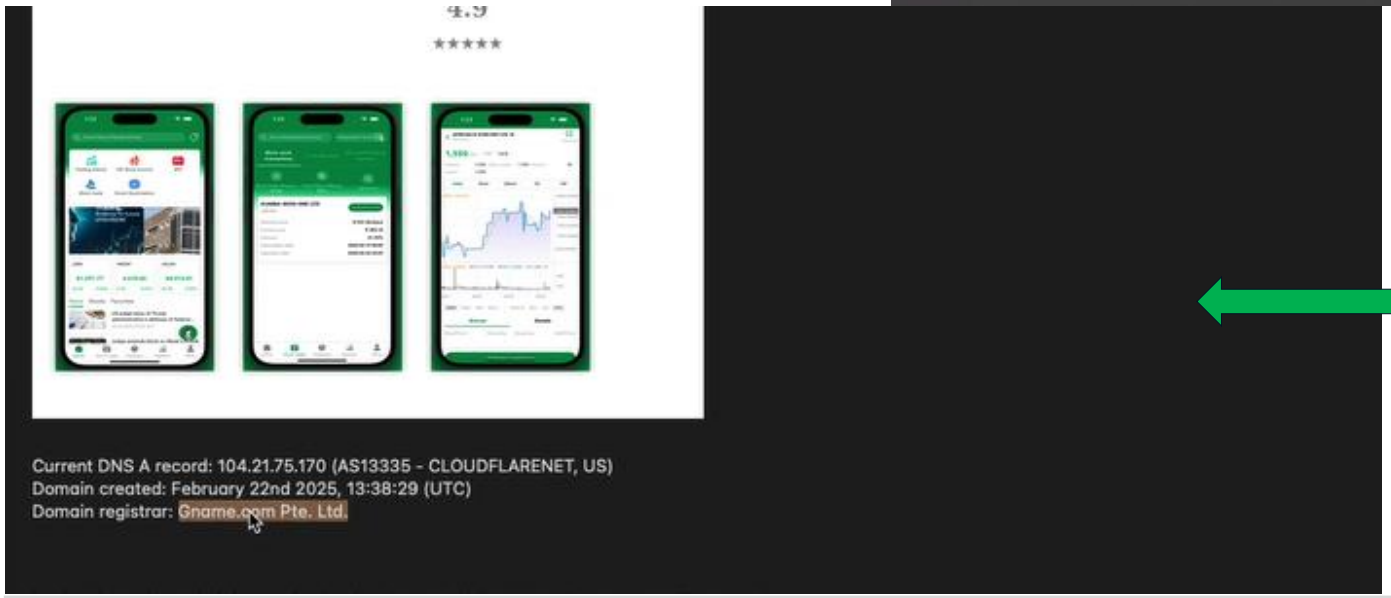
6.

7.

Mobile App

Android and IOS Appstore

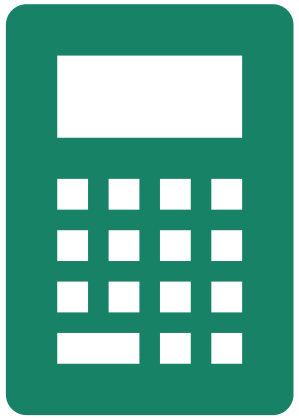


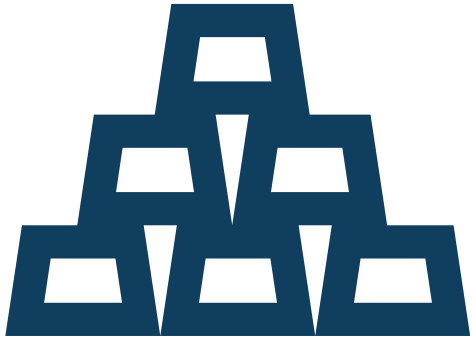


Protected App

OMIG AI Video

How to guide





Closing

- Maneuver through the ERA
- High degree prompting
- Post Truth – Where no one is responsible
- Digital Cyber Warfare
- Society Shift
- Rules