Balancing Technological Advancements with Ethical and AI Security Issues

PUBLIC ECONOMICS
CONFERENCE

Prof. Uche M. Mbanaso
Department of Computer Science, Nasarawa State University, Keffi, Nigeria

3–5 SEPTEMBER
2024

TECHNOLOGY AND DATA
FOR ENHANCED GOVERNMENT SERVICE DELIVERY

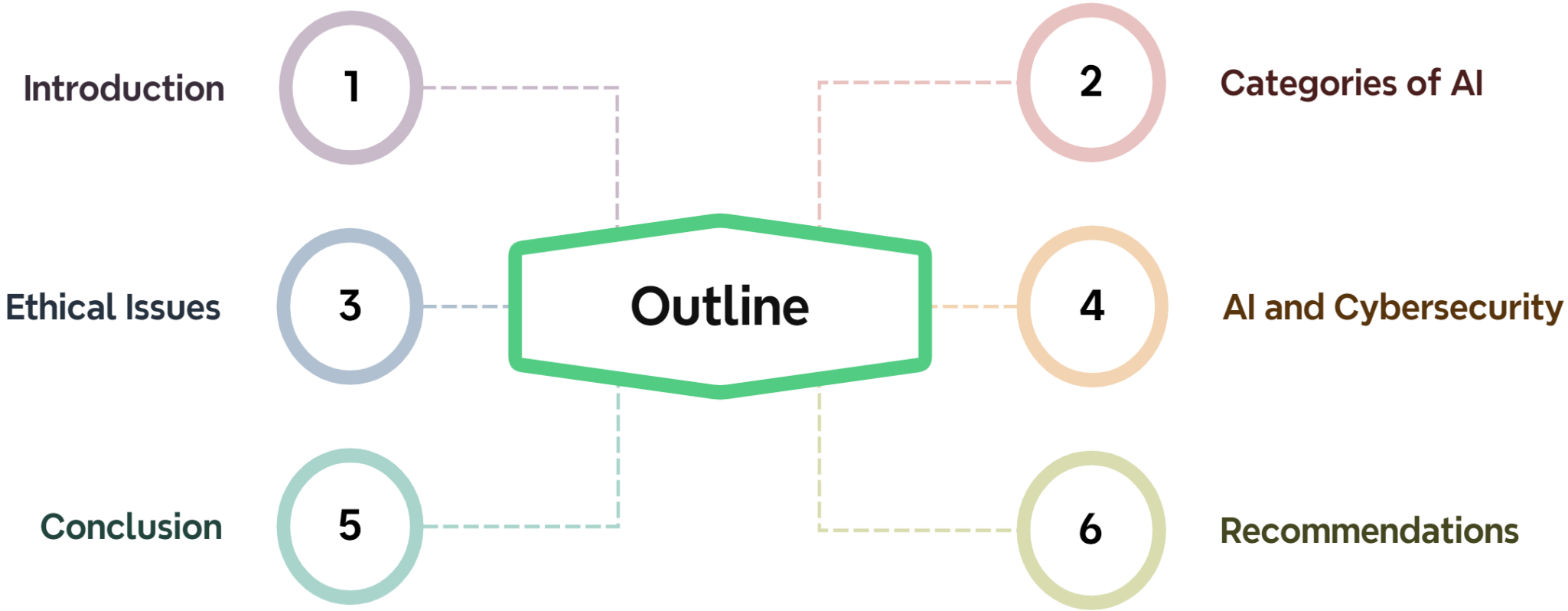
GTAC Analyse Assess Activate Strategic & Technical Advisory
National Treasury REPUBLIC OF SOUTH AFRICA

national treasury
Department: National Treasury
REPUBLIC OF SOUTH AFRICA

public economics WINTERSCHOOL

SAVINGS@WORK
GOVERNMENT SPENDING REVIEWS

Balancing Technological Advancements with Ethical and AI Security Issues



• Introduction

1. AI is significantly transforming our lives, society, our environment and the planet.

3. AI possesses the potential to drive inclusive growth and support scientific and technological advancements that improve the conditions of the world in which we live.

Artificial Intelligence (AI)

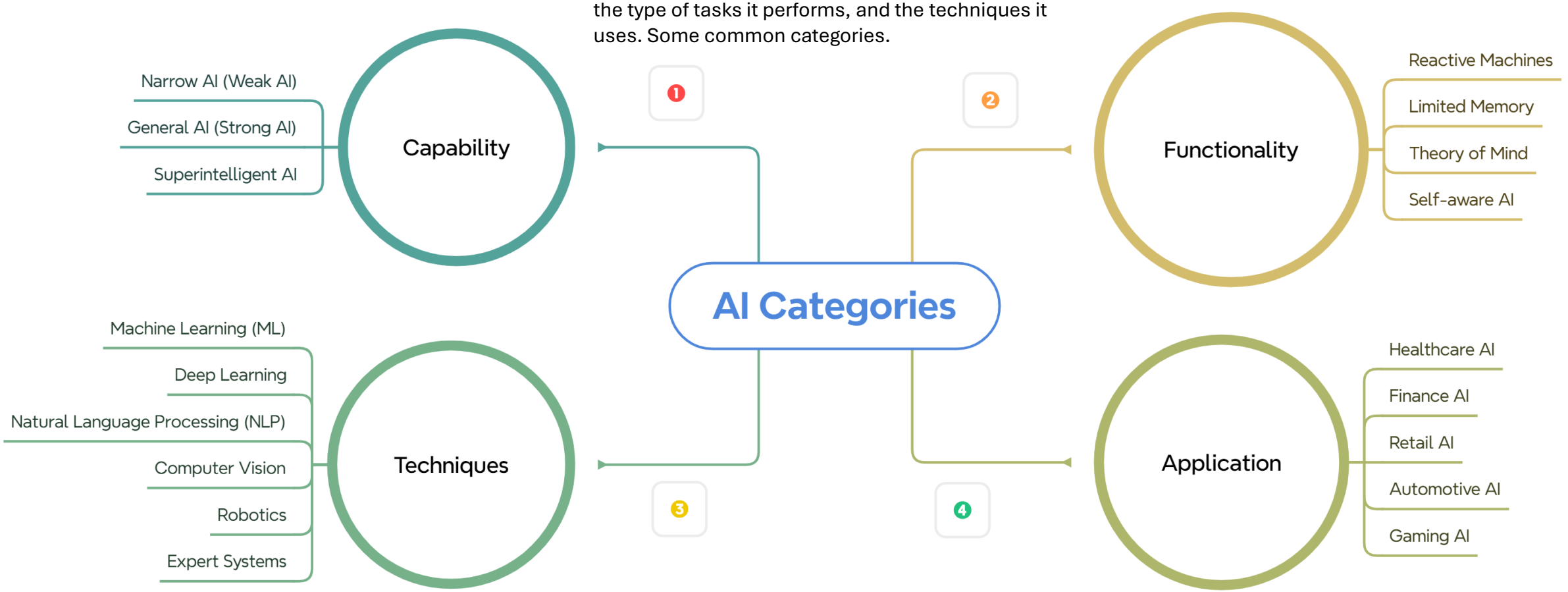
2. AI applicability extends from complex to simple tasks, impacting all aspects of our lives and sectors of the economy.

4. AI systems, however, also pose risks that can negatively impact individuals, groups, organisations, communities, society, the environment and the planet in unforseen ways.

Like any technology, AI poses ethical, security, and safety concerns that can manifest in various ways, characterized by long-term or short-term, high or low probability and impact risks.

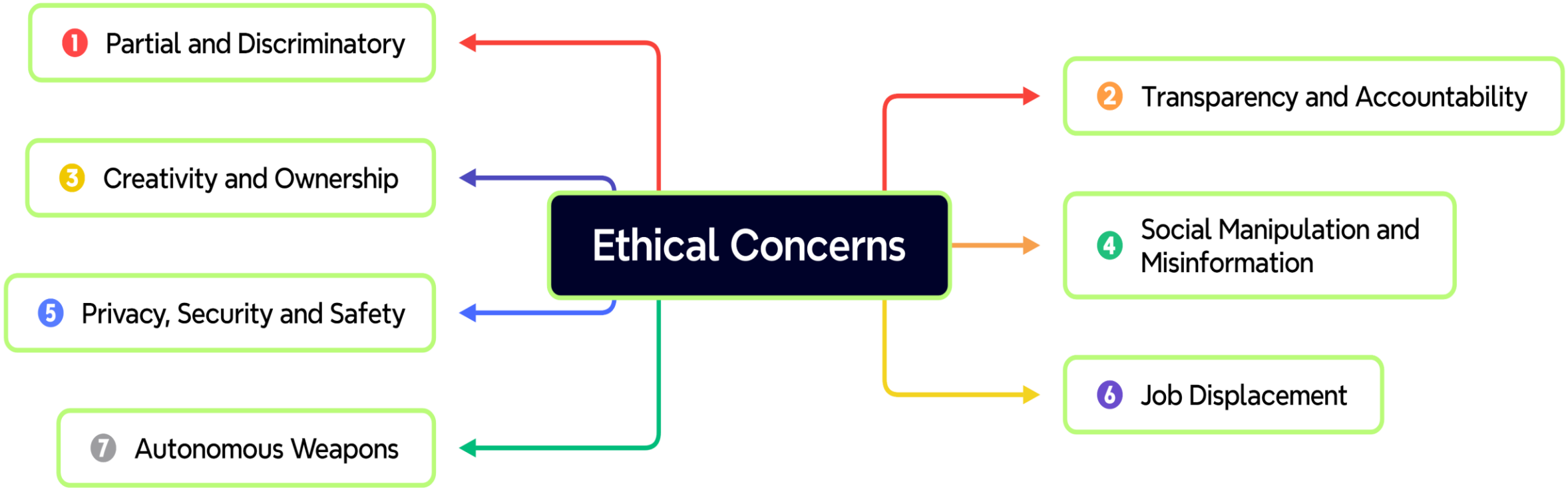
Categories of AI

Artificial Intelligence (AI) can be categorised in several ways, depending on the level of capability, the type of tasks it performs, and the techniques it uses. Some common categories.



GTAC Analyse Assess Activate Strategic & Technical Advisory
national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA
public economics WINTERSCHOOL
SAVINGS@WORK GOVERNMENT SPENDING REVIEWS
PUBLIC ECONOMICS CONFERENCE
3-5 SEPTEMBER 2024

Ethical Issues



GTAC Analyse Assess Activate Strategic & Technical Advisory
national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA
public economics WINTERSCHOOL
SAVINGS@WORK GOVERNMENT SPENDING REVIEWS
PUBLIC ECONOMICS CONFERENCE
3–5 SEPTEMBER 2024

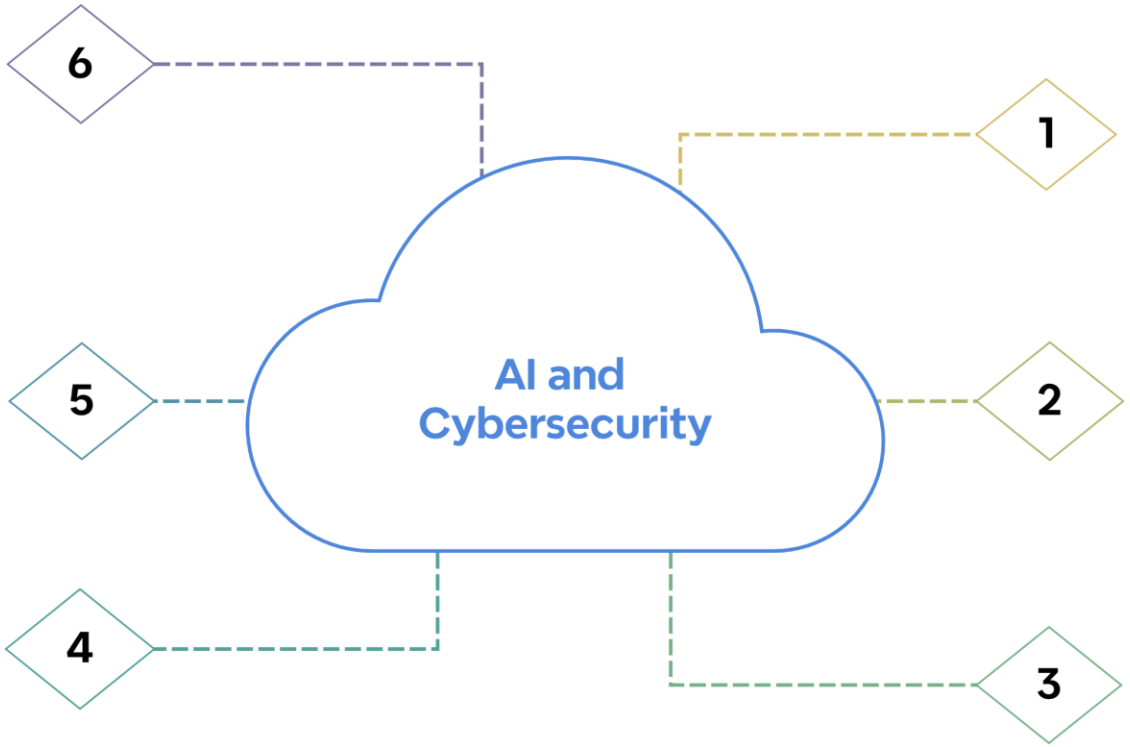
AI and Cybersecurity

• AI and Cybersecurity

The dual-edged nature of AI and cybersecurity creates paradoxes, complexities, challenges, and opportunities in the digital domain. While AI offers unprecedented opportunities to enhance cybersecurity, it also empowers attackers to launch more sophisticated and damaging cyberattacks, yet AI has its threat landscape.

AI and Cybersecurity are symmetric and asymmetric.
.

Vulnerabilities in AI can arise from various sources, such as the design, implementation, and deployment of AI systems, as well as from the data they use and the environments in which they operate.

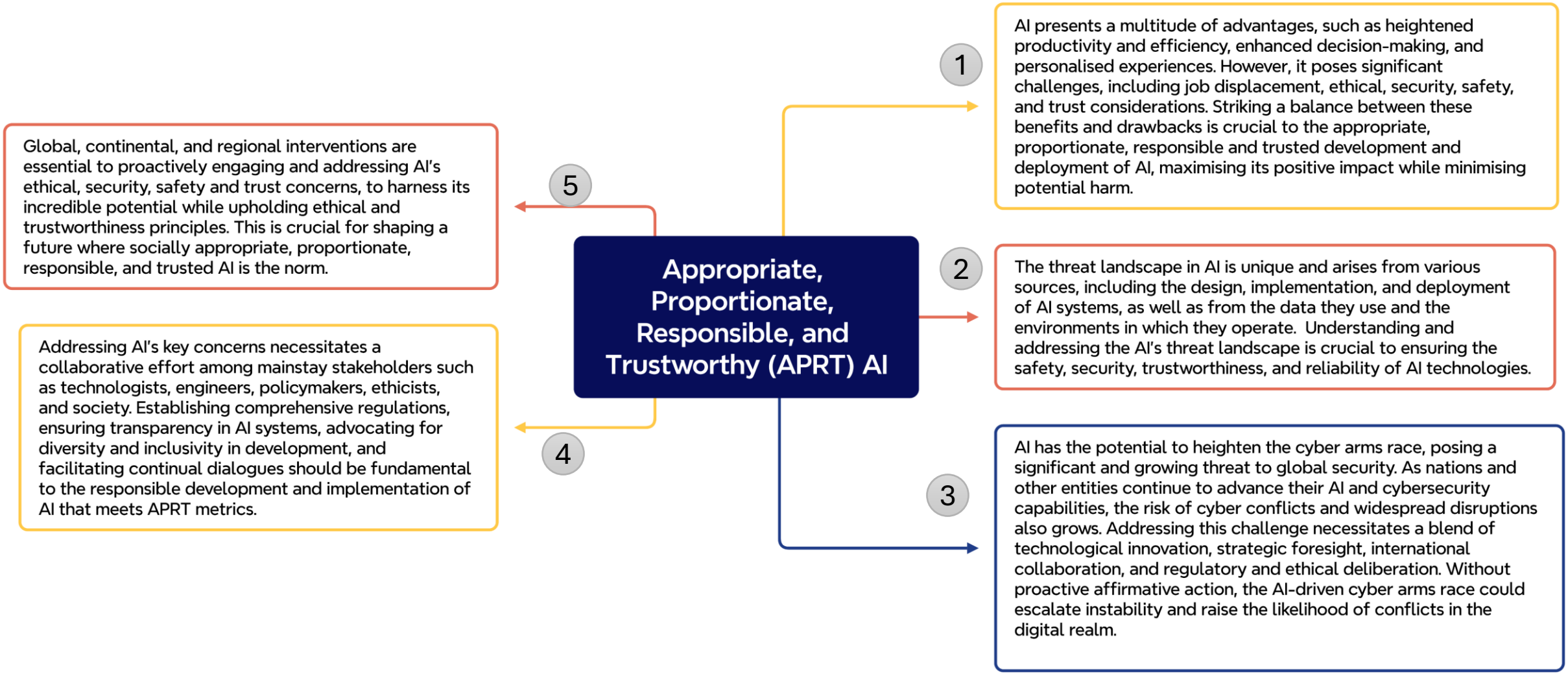


AI and cybersecurity create a crucial paradox because of AI's dual nature: AI is both a powerful tool for enhancing cybersecurity and a potent weapon for cybercriminality.

This paradox delineates a complex and evolving battlefield in which AI-driven technologies can concurrently fortify defenses and facilitate more sophisticated attacks

Like other technologies, AI systems are vulnerable. As software-based artefacts, they have weaknesses or flaws that can be exploited by malicious actors or may lead to unintended and harmful outcomes.

Conclusion


Appropriate, Proportionate, Responsible, and Trustworthy (APRT) AI
1
AI presents a multitude of advantages, such as heightened productivity and efficiency, enhanced decision-making, and personalised experiences. However, it poses significant challenges, including job displacement, ethical, security, safety, and trust considerations. Striking a balance between these benefits and drawbacks is crucial to the appropriate, proportionate, responsible and trusted development and deployment of AI, maximising its positive impact while minimising potential harm.
2
The threat landscape in AI is unique and arises from various sources, including the design, implementation, and deployment of AI systems, as well as from the data they use and the environments in which they operate. Understanding and addressing the AI's threat landscape is crucial to ensuring the safety, security, trustworthiness, and reliability of AI technologies.
3
AI has the potential to heighten the cyber arms race, posing a significant and growing threat to global security. As nations and other entities continue to advance their AI and cybersecurity capabilities, the risk of cyber conflicts and widespread disruptions also grows. Addressing this challenge necessitates a blend of technological innovation, strategic foresight, international collaboration, and regulatory and ethical deliberation. Without proactive affirmative action, the AI-driven cyber arms race could escalate instability and raise the likelihood of conflicts in the digital realm.
4
Addressing AI's key concerns necessitates a collaborative effort among mainstay stakeholders such as technologists, engineers, policymakers, ethicists, and society. Establishing comprehensive regulations, ensuring transparency in AI systems, advocating for diversity and inclusivity in development, and facilitating continual dialogues should be fundamental to the responsible development and implementation of AI that meets APRT metrics.
5
Global, continental, and regional interventions are essential to proactively engaging and addressing AI's ethical, security, safety and trust concerns, to harness its incredible potential while upholding ethical and trustworthiness principles. This is crucial for shaping a future where socially appropriate, proportionate, responsible, and trusted AI is the norm.

Recommendations

1

Continental, regional, and national harmonised frameworks are needed to address the complexities and challenges and to foster collaboration and opportunities.

2

Deliberate and focused workforce reskilling through collaboration between governments, industry and educational institutions.

3

Creating AI awareness and education from primary to tertiary level to understand AI opportunities and risks. Curriculum change is inevitable!

4

Harmonised and coordinated R, I, & D across the continent; establish specific CoE in dedicated tertiary institutions.

5

Establish regulatory and evaluation (or testing) centres for compliance and monitoring of AI's appropriateness, proportionateness, responsibility, and Trustworthiness.

The power of AI lies in our ability to ideate and innovate, but deep learning has the potential to reshape AI's future outcomes.

Thank You!

GTAC Analyse Assess Activate Strategic & Technical Advisory

national treasury
Department: National Treasury
REPUBLIC OF SOUTH AFRICA

public economics WINTERSCHOOL

SAVINGS@WORK GOVERNMENT SPENDING REVIEWS

PUBLIC ECONOMICS CONFERENCE