TransRe Forum

(Literaturhaus München)

April 17th 2024

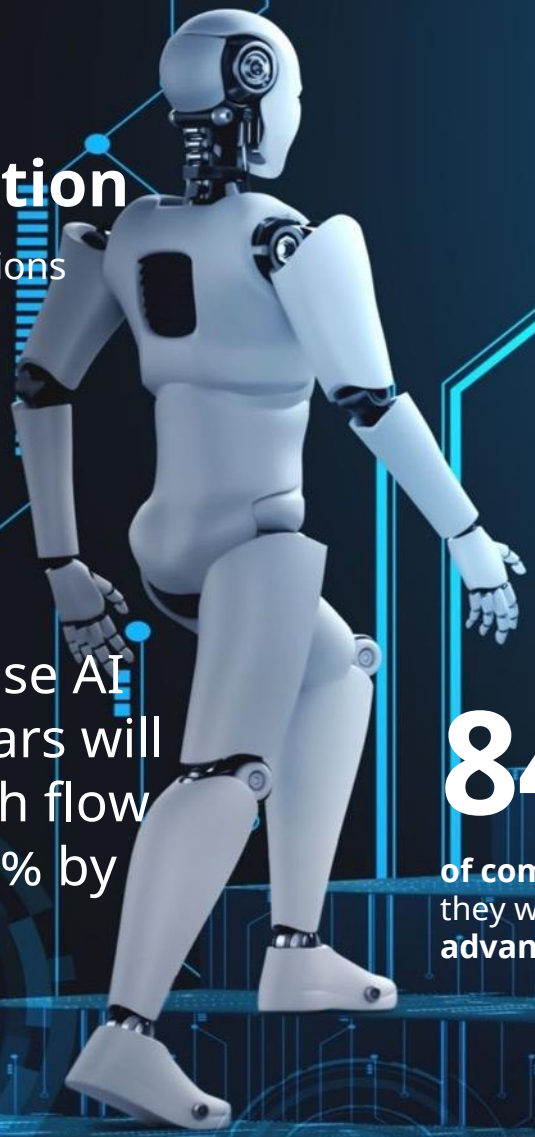
"It's all about AI - opportunities and challenge swithin regulations in artificial intelligence"

Andy Schweiger, SVP Cyber Security, DEKRA

AI in speculative figures

75% **AI application**

within commercial software applications



$15.7 trillion

AI could contribute to the global economy by 2030 - Source: PWC sizing the prize

Companies that use AI in the next 5-7 years will increase their cash flow by more than 120% by 2030

84%

of companies assume that they will achieve **competitive advantages** through AI

Source: Source: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

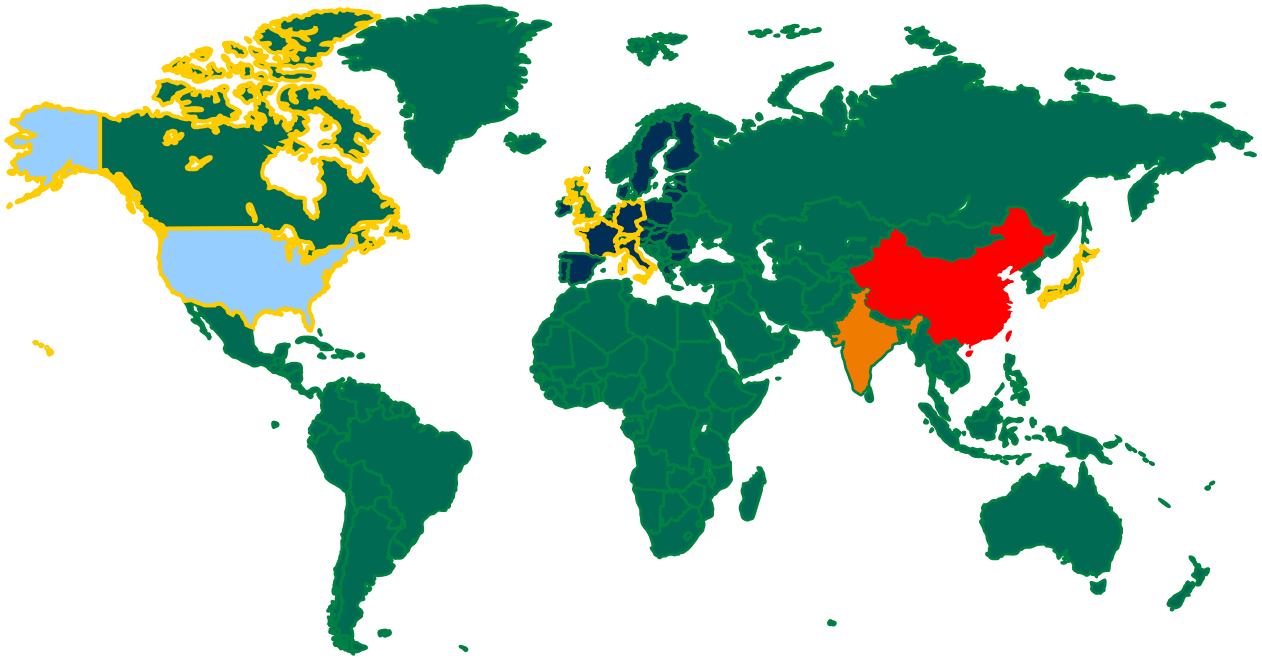
TransRe Forum – Literaturhaus München, April 2024
-Andy Schweiger, Senior Vice President, CFA Cyber Security, DEKRA

the tension between AI & cyber security

	AI	Cybersecurity
Potential for improvement	• Automation of security solutions (threat detection, incident response) • Improved anticipation, proactive responses to threats • Accelerated pattern recognition	• Improved learning about attack patterns • Bridging or resolving personnel bottlenecks
New risks	• Manipulation of automation • Relatively high susceptibility of training data to interference	• Too strong a focus on machine support • Manipulation and sabotage of security solutions can be automated

Global approaches/measures for AI regulations

Overview



EU - AI Act

China - AI Governance Framework

G7 - AI Code of Conduct

US - Executive Order

India - "Non-regulatory" approach to AI

TransRe Forum – Literaturhaus München, April 2024

-Andy Schweiger, Senior Vice President, CFA Cyber Security, DEKRA

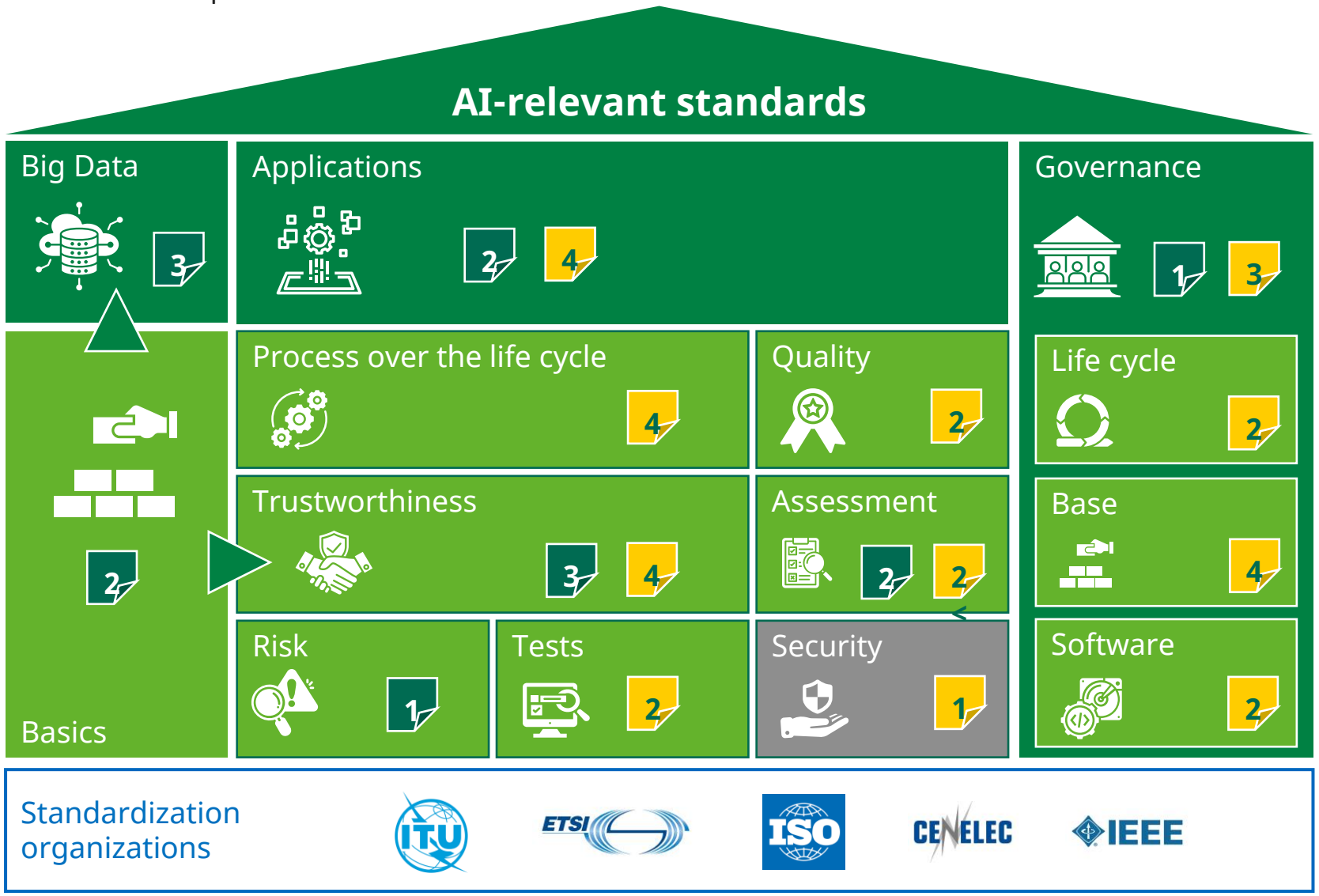
AI standardization - a major "construction"...

Compass for navigating through a diverse standard landscape

12 **available Standards**

30 **Standards in Development**

These standards originate from a heterogeneous landscape of standardization institutions that need to be must be classified in the specific context of companies!



EU-AI Act of 9.12.2023 - key content

Horizontal legislation on AI regulation within the EU, 5 main pillars:

Risk classification & neutral testing obligation

Binding regulations (general AI)

Special obligations for simulation of human behavior

Fines for non-compliance

EU authority structure

The goal: AI safely and responsibly in society and the environment!

AI that supports people in a meaningful, value-adding way and must not endanger them!

ethically sound and safe Applications for our society

fair, transparent, competition-oriented & growth-promoting

TransRe Forum – Literaturhaus München, April 2024
-Andy Schweiger, Senior Vice President, CFA Cyber Security, DEKRA

A View onto our work bench ...

DEKRA

TRAININGS & PRE-ASSESSMENTS

KI Training & Consulting

- AI risk awareness
- AI regulations and standards
- Trustworthiness & ethics
- Maturity assessment (DEKRA KI maturity level scoring)

ASSESSMENTS

AI tests

- Data Quality (ISO 5259)
- Model Robustness (ISO 24029)
- AI Bias & Fairness (ISO 24027)
- AI cyber security

KI Audits & Certification

- Management systems (ISO 42001)
- AI risk management (ISO 23894)
- Road vehicle safety & AI (ISO 8800)
- Data Labeling (ISO 5259-4)
- A-Spice machine learning

Thank you very much!

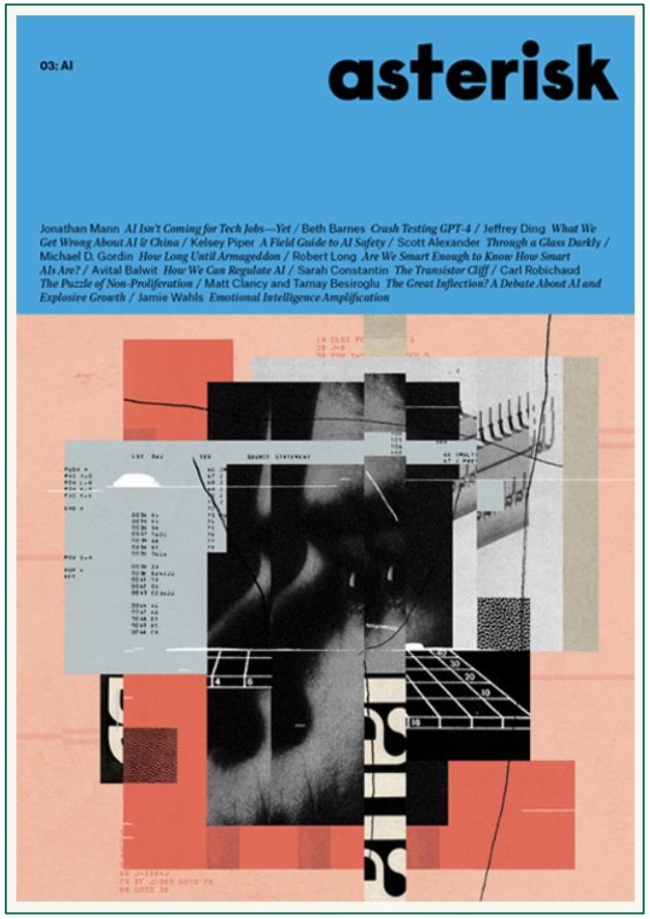
Andy Schweiger
SVP Cyber Security Services
DEKRA

innovating safety & security

BACKUP

other sources with noteworthy considerations on AI evolutions …

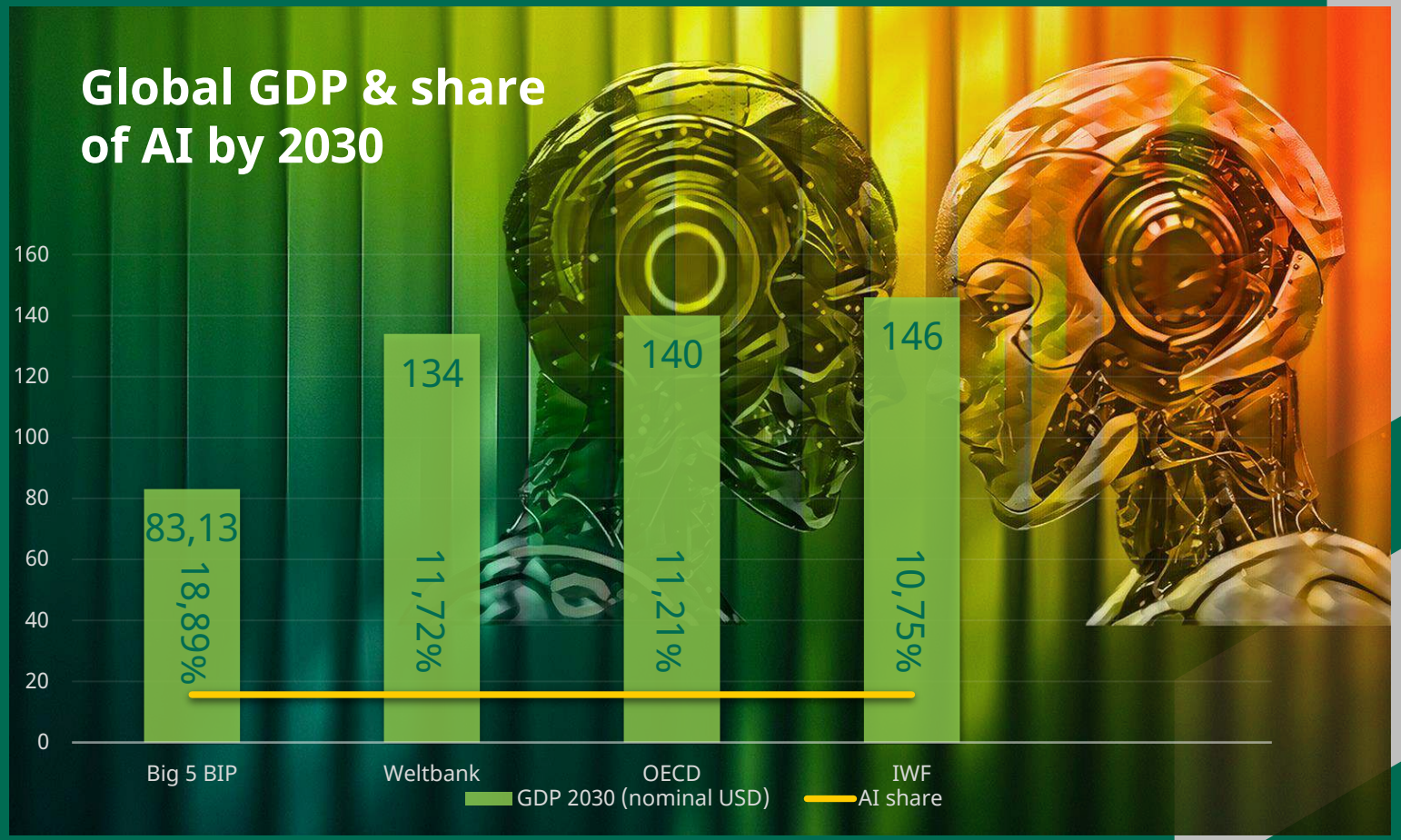
please use internally only



asteriskmag
June 2023 Issue
exclusively on

Andrew Marantz
March 2024 Issue
on AI Doomsayers

by 2030 - AI* to account for over 10% of GDP worldwide**!?



Sources:
* PWC sizing the prize
** Forecasts World Bank, IMF & OECD

...This is not just about regulation ...
Why do we need AI assessments and certifications?

1

Conformity to new standards

- Violations are severely punished
- Assumption of liability in the event of of compliance violations

2

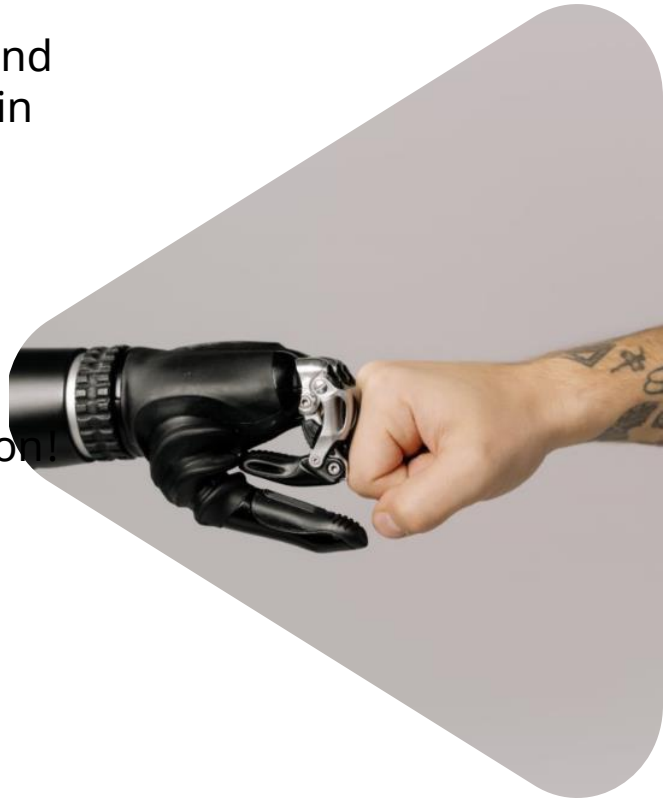
Quality assurance and reduction of economic risks

- Incorrectly functioning AI can result in considerable economic damage due to incorrect decisions, consequential damage and liability

3

Building trust with customers and users

- Prove that your solution is secure and sustainable and gain the trust of customers and users
- Set yourself apart from the from the competition!



Testing service providers are part of the solution …

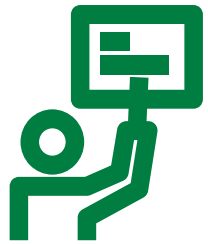
… when it comes to protecting our society and its companies

indispensable in the legal text

- globally binding rules
- Consideration of TIC companies in conformity assessments (Art. 6 (1))/Art. 43 (3)
- Integration TIC context in Art. 52c - 52d

our contribution:

- neutral know-how
- Digital protection mechanisms
- Confidence in new products & services

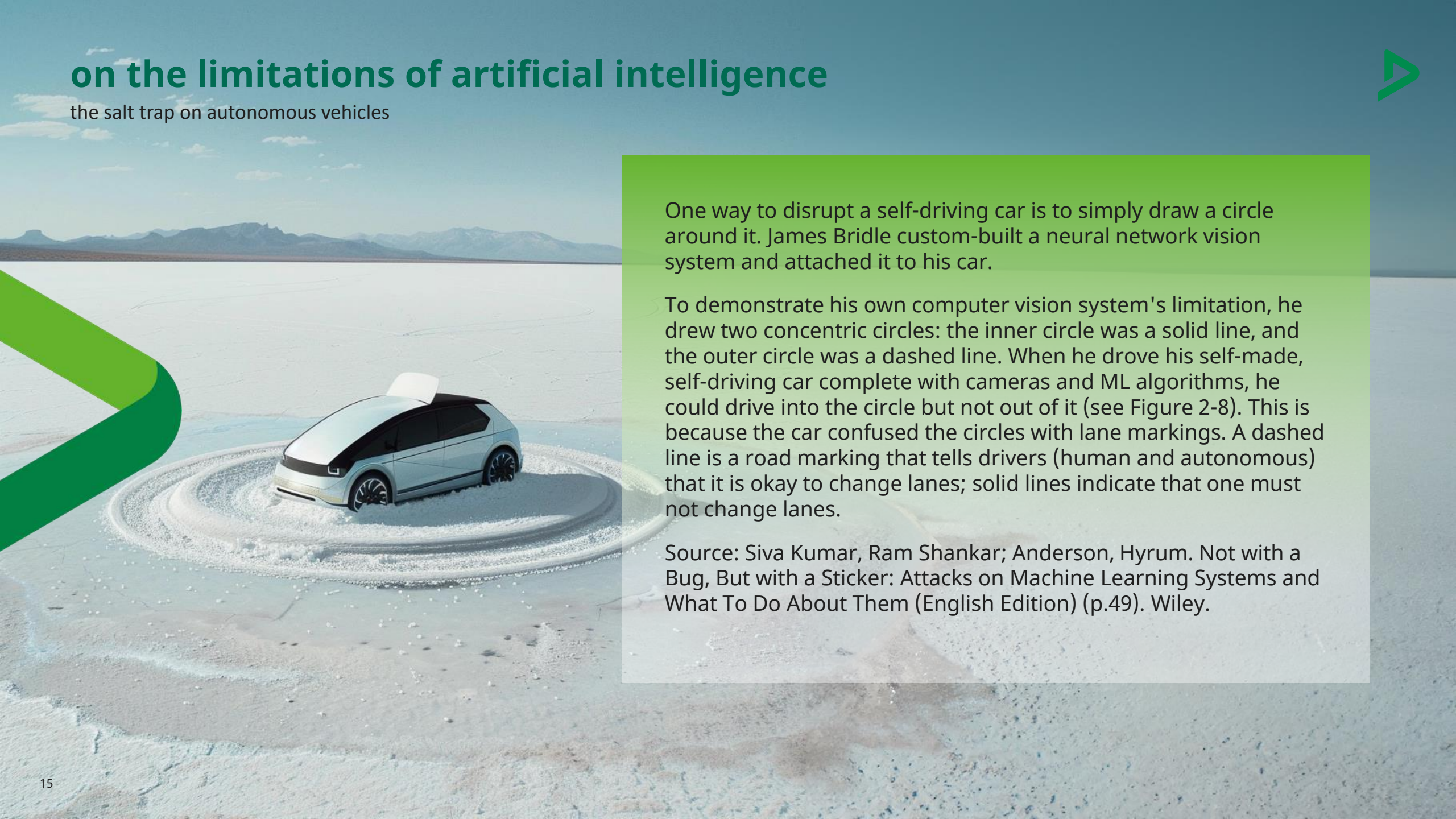


our requirement for the legislative process:

- Strong state rules for inspection obligations
- Clear legal requirements on the AI testing obligation
- Binding guidelines for the accreditation of neutral third parties (TIC provider)

on the limitations of artificial intelligence

the salt trap on autonomous vehicles



One way to disrupt a self-driving car is to simply draw a circle around it. James Bridle custom-built a neural network vision system and attached it to his car.

To demonstrate his own computer vision system's limitation, he drew two concentric circles: the inner circle was a solid line, and the outer circle was a dashed line. When he drove his self-made, self-driving car complete with cameras and ML algorithms, he could drive into the circle but not out of it (see Figure 2-8). This is because the car confused the circles with lane markings. A dashed line is a road marking that tells drivers (human and autonomous) that it is okay to change lanes; solid lines indicate that one must not change lanes.

Source: Siva Kumar, Ram Shankar; Anderson, Hyrum. Not with a Bug, But with a Sticker: Attacks on Machine Learning Systems and What To Do About Them (English Edition) (p.49). Wiley.

The biggest fears
in relation to AI