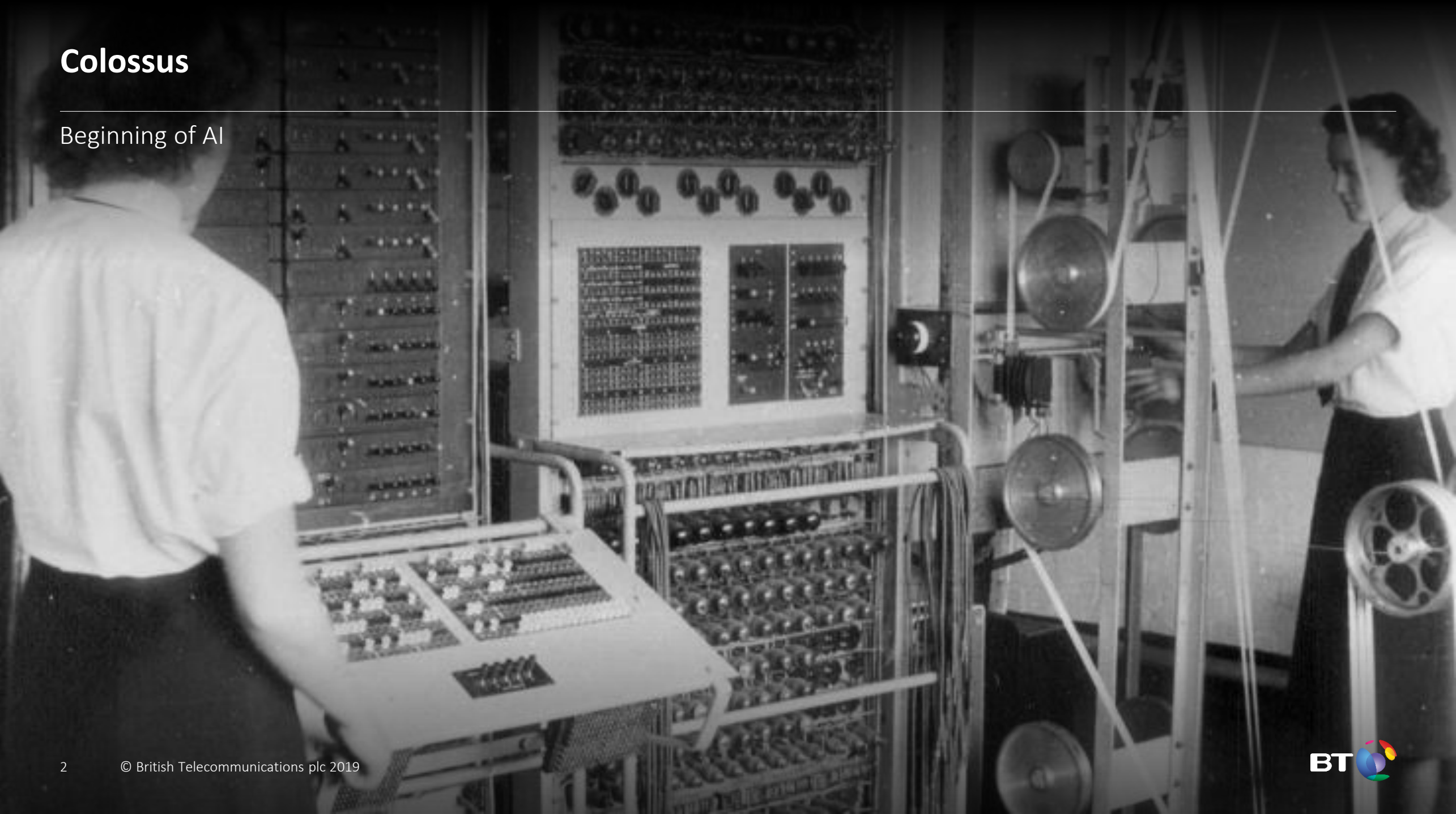
AI History and Future

Dr Robert Hercock
Senior Researcher in Disruptive Technologies

Colossus

Beginning of AI



AI in fiction

1927	1950	1968	1984	2013	2017
Fritz Lang's Metropolis	Isaac Asimov's I, Robot	2001: A Space Odyssey	The Terminator	Her	Ghost in the Shell

History of AI

1940s	1950s	1960s	1980s	1990s	2000s
Programmable computers	Symbolic AI	Neural networks	Behaviour-based robotics Shifted focus onto non-symbolic reasoning	Deep neural networks	Big data / GPU / deep learning

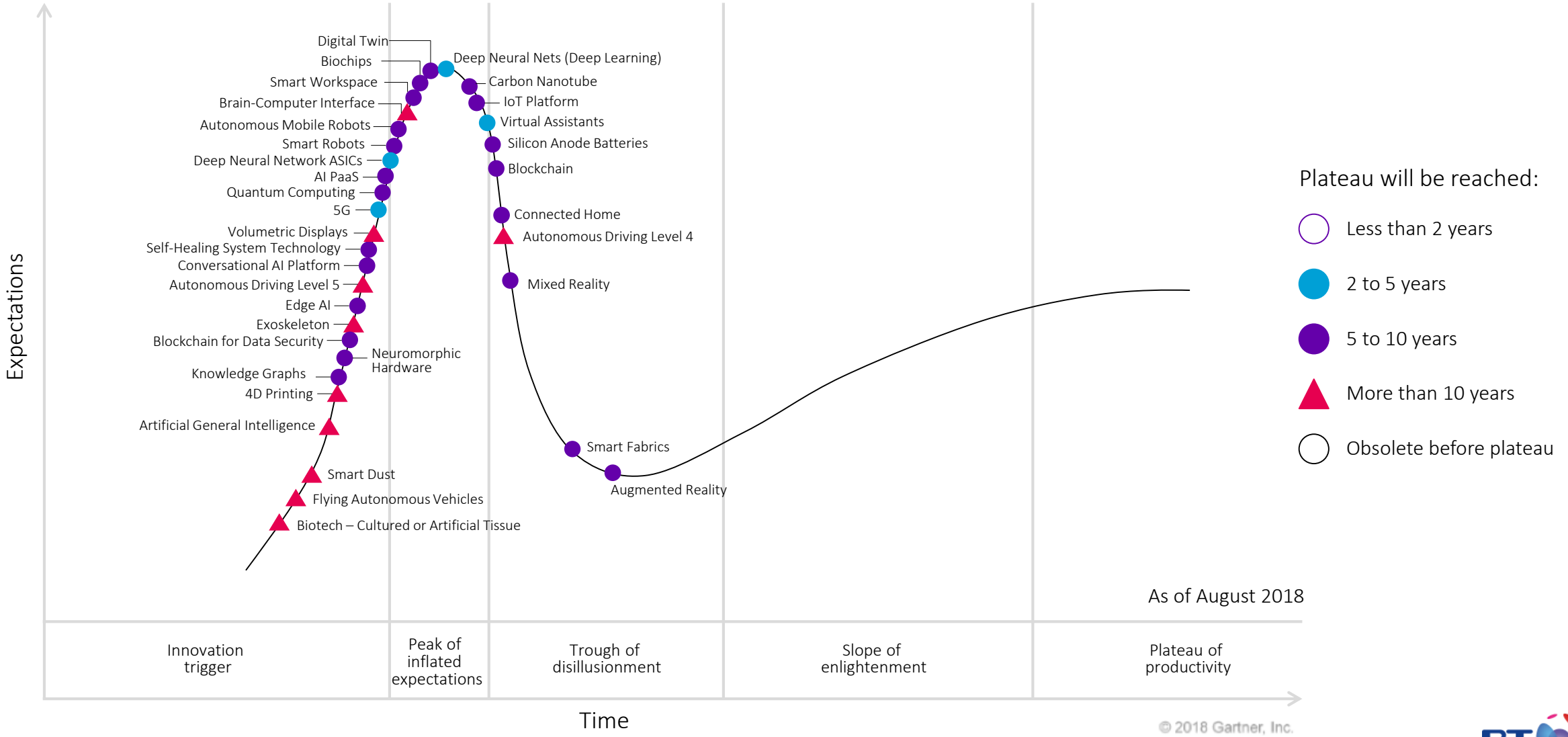
AI economic value

Accenture has estimated that new AI applications could add up to £654bn to the UK economy by 2035.

In the Fintech sector, > $368m was invested in AI-related Fintech companies in the past year.

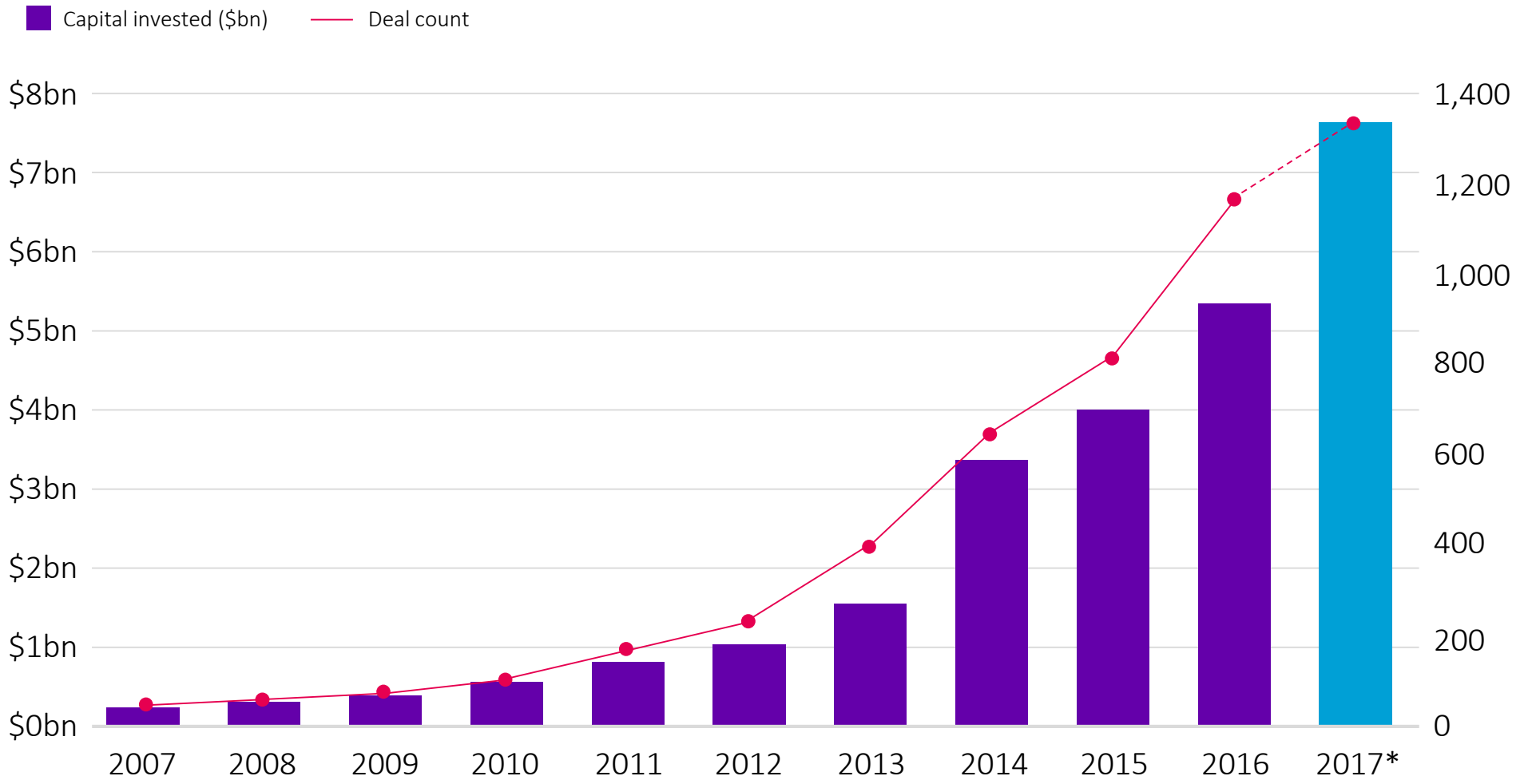
Q. Where are we in the hype cycle?

Gartner’s hype cycle for emerging technologies 2018



Venture funding for AI startups (Source: PitchBook)

PitchBook *as of 10/12



Democratised AI

AI will become available to the masses – democratised. Movements and trends like cloud computing, the “maker” community and open source will eventually propel AI into everyone’s hands.

This trend is enabled by the following technologies:

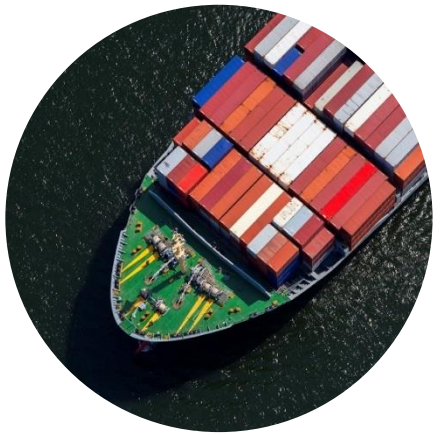
AI platform as a service (PaaS), artificial general intelligence, autonomous driving (Levels 4 and 5), autonomous mobile robots, conversational AI platforms, deep neural networks, flying autonomous vehicles, smart robots, and virtual assistants.

Cyber security costs

NotPetya – June 2017, largest attack so far by cost

$870,000,000

Pharmaceutical company Merck



$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$300,000,000

Danish shipping company Maersk

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Machine learning in cyber security

BT Cyber Security Platform (CSP): the foundation of BT's cyber threat detection systems. Our Big Data analytics platform for Threat Hunting and detecting Advanced Persistent Threats at any scale.

User Entity Behaviour Analytics (UEBA): we use our own data-driven behavioural analytics systems to detect malicious UEBA incidents, looking out for new modes of attack rather than relying on historic patterns of known malware signatures or policies. It's a lot more dynamic and effective.

Domain Generation Algorithms (DGA): command and control domains generated automatically by Malware help Bad Actors' get data from a compromised computer to one they can more easily access. We use machine learning to detect and isolate them before they can do any damage.

DGA domains are difficult to detect via conventional block lists because thousands of them can be generated. Even if you positively identified and blocked one there would still be an unknown number of others out there. With a machine learning approach, the threat is constantly dominated.

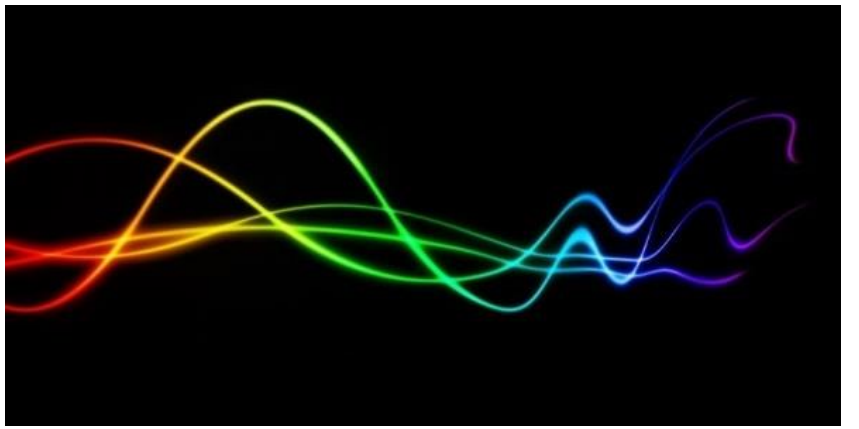
AI as a catalyst

AI is a catalytic technology.

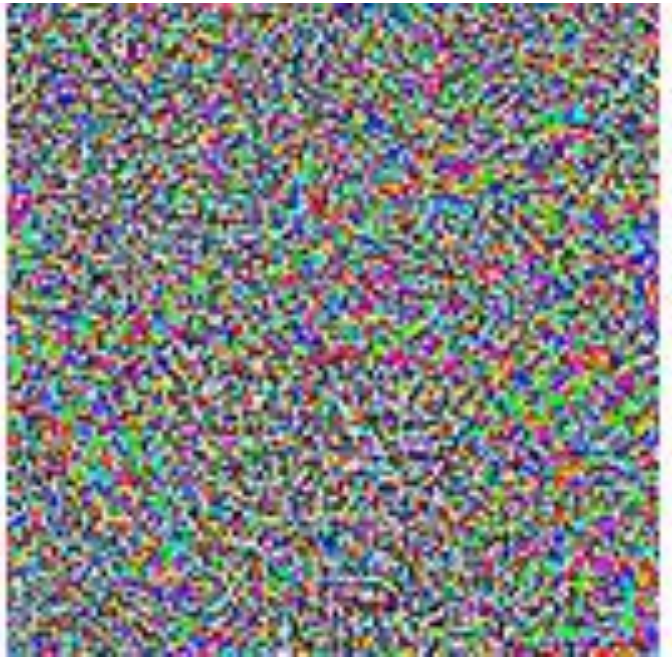
Prior examples:

- Gunpower
- Printing press
- Steam engines
- Vacuum tubes
- Computers.

All revolutionised warfare and security.



$+\epsilon$



$=$

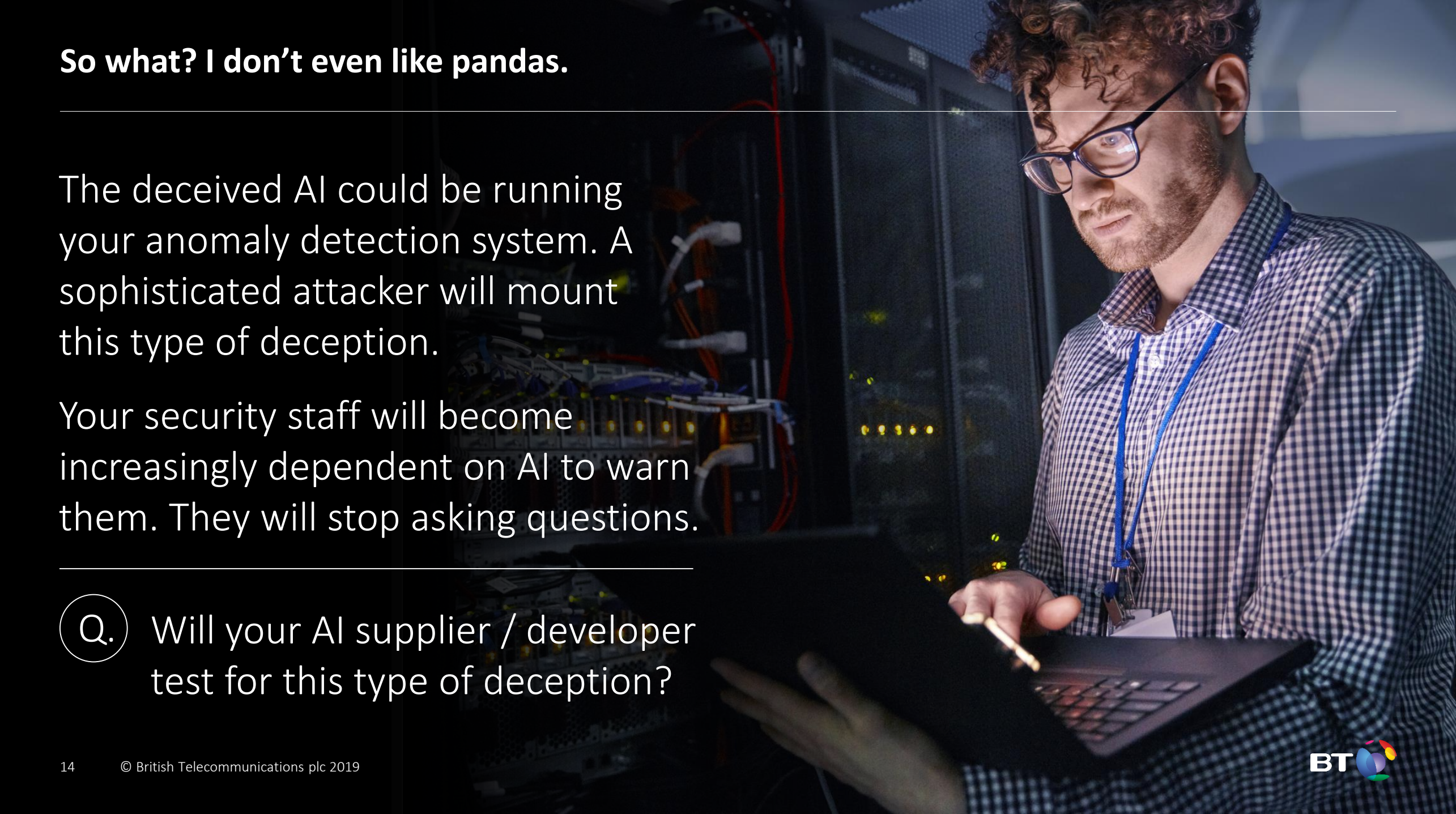
“Panda”
57.7% confidence

“Gibbon”
99.3% confidence

https://blog.openai.com/adversarial-example-research/

BT

So what? I don’t even like pandas.

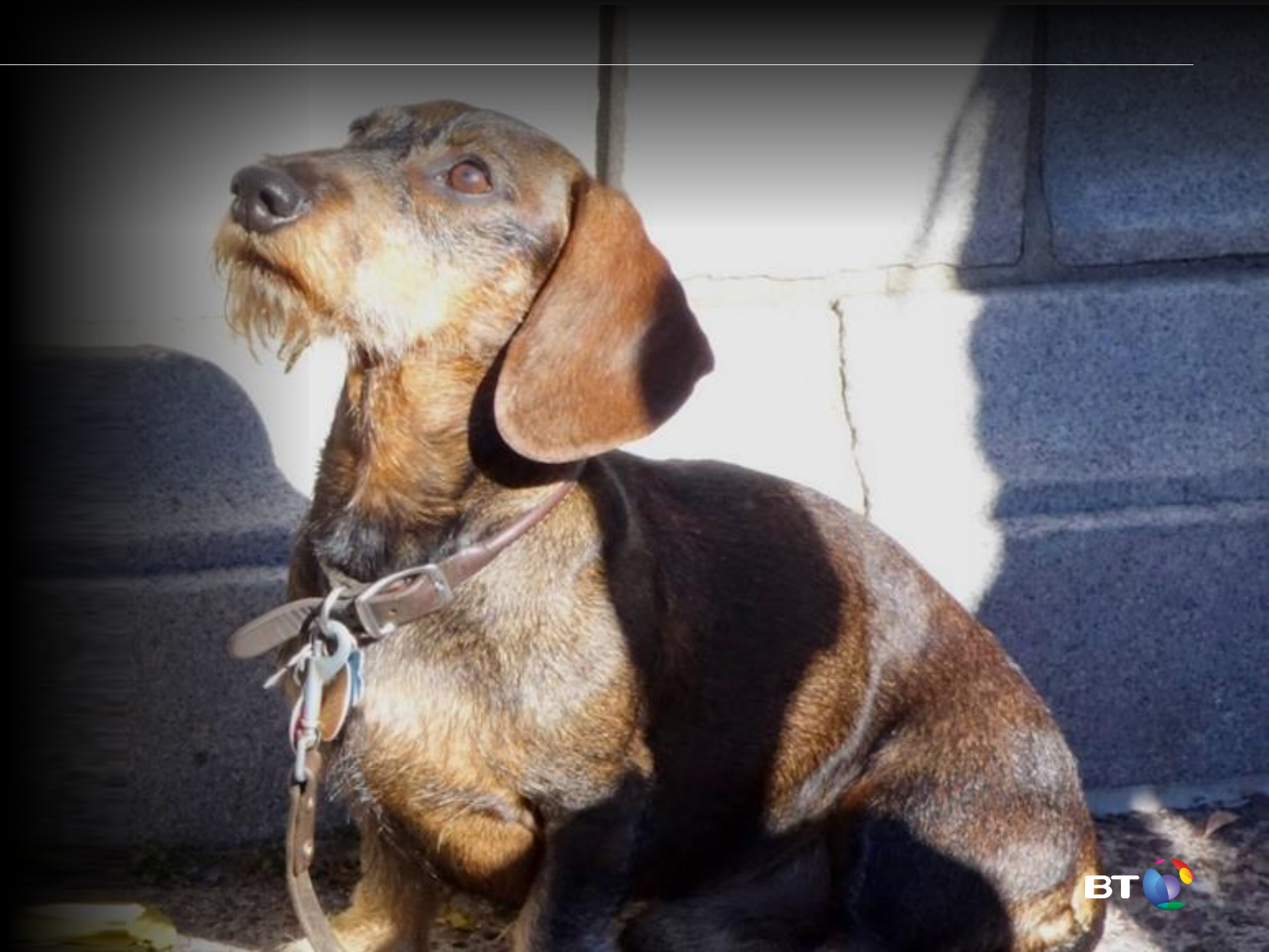


The deceived AI could be running your anomaly detection system. A sophisticated attacker will mount this type of deception.

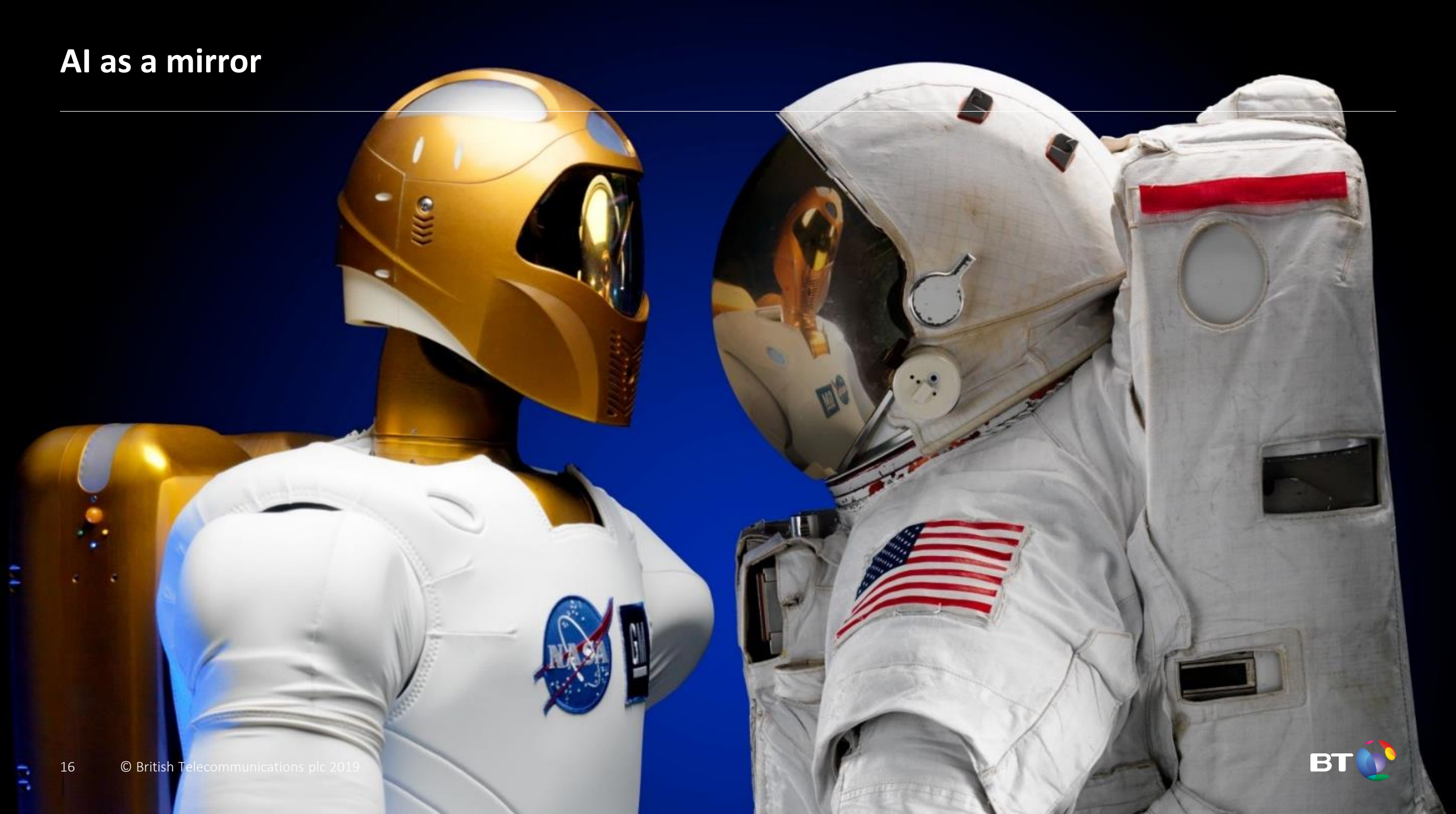
Your security staff will become increasingly dependent on AI to warn them. They will stop asking questions.

Q. Will your AI supplier / developer test for this type of deception?

AI and regulation

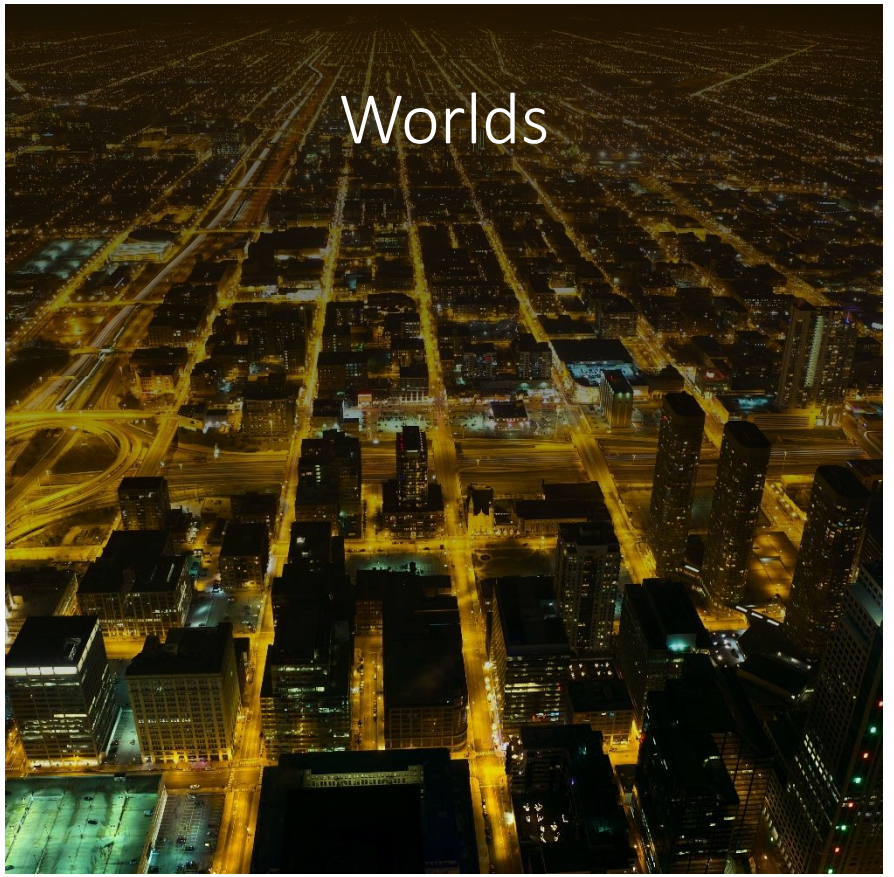


AI as a mirror



AI future?

HAL



Iron Man

Terminator

Watson

Summary

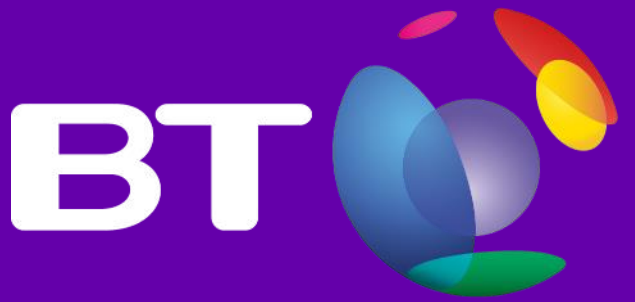
AI is reshaping cyber security at all levels

It will have a major impact on society: i.e. employment and wealth balance

Q. Is your AI biased, has it been deceived?

Longer term: the HAL problem – AI can be benign, but has conflicting instructions

Key development – explainable AI required


BT