



Intro

Thanks for attending!

Next month's event is July 25th @ 17:45

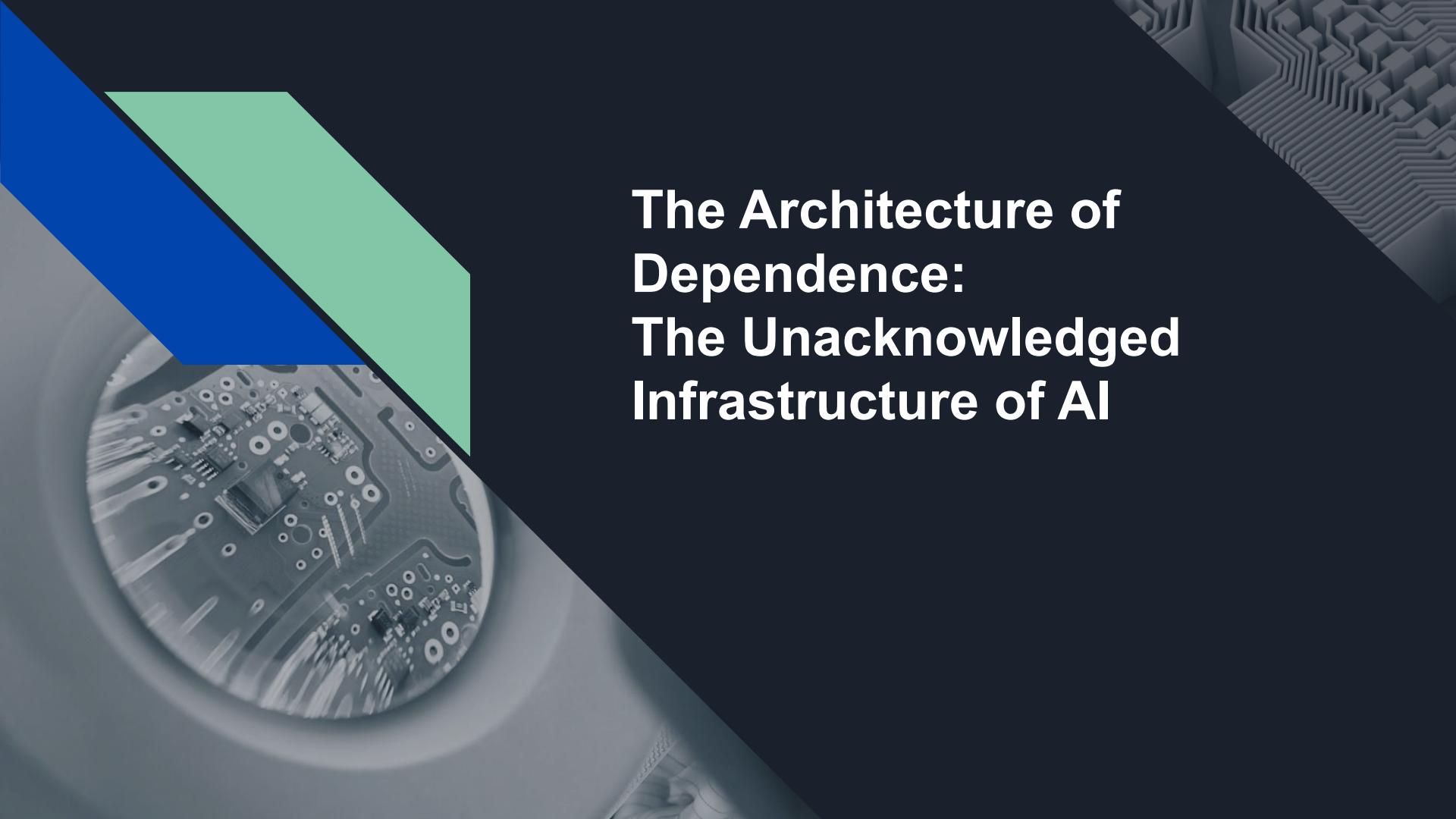
Want to speak at a future event? Have a question?

talk@winnisec.life

Skullspace Discord #events

DC204 #events





The Architecture of Dependence: The Unacknowledged Infrastructure of AI

TOC

Intro - Clever Hans

Human Labour, Disguised as AI

Fauxtomatication

Dangers of AI

Environment

Clever Hans, 1895 - 1916

- Horse that appeared to perform arithmetic and other intellectual tasks during exhibitions in Germany
- Wilhelm von Osten, who was a mathematics teacher, an amateur horse trainer
- Psychologist Carl Stumpf formed a panel of 13 people, concluded there were no “tricks”
- Oskar Pfungst, Carl's assistant, investigated further, found out about subtle, involuntary cues
- Clever Hans effect describes a phenomenon where an algorithm seems to make correct predictions without having the relevant data and/or by using incorrect reasoning





Human Labour, Disguised As AI

AI scrapes millions of images, websites to feed its models/data sets

Not actual reality - but a jumble of images/information that was available (hallucinations)

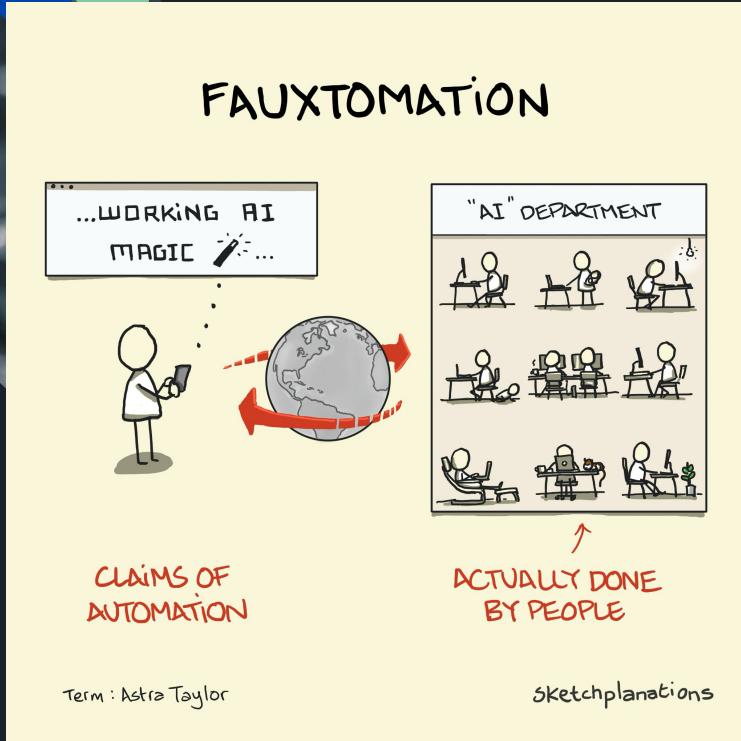
Some humans are used in “training” AI - providing initial data / feedback

But - humans are doing much more work, behind the scenes, doing tasks that make AI seem more intelligent than it really is



Examples - X.AI “Amy”, Amazon AI stores “Just Walk Out”, Mechanical Turk, self driving cars

Fauxtomation



"The process that renders invisible human labour to maintain the illusion that machines and systems are smarter than they are." - Astra Taylor

Crowdsourcing - tagging images, testing algos, refining AI systems

Sifting through suspicious/harmful content could leave psychological trauma

Relocating labour: self checkouts at grocery stores/restaurants

Dangers of AI

Microsoft Co Pilot flaw “EchoLeak” - attack bypasses built in protection

Meta AI searches made public, prompts are put onto a public feed

Hacking using Deepfakes



If a user’s expectations about how a tool functions don’t match reality, you’ve got yourself a huge user experience and security problem.

Humans have built a schema around AI chat bots and do not expect their AI chat bot prompts to show up in a social media style Discover feed — it’s not how other tools function.

Because of this, users are inadvertently posting sensitive info to a public feed with their identity linked, including prompts with:

- exact medical issues
- federal crimes committed
- tax evasion
- home address
- interest in extramarital affairs
- sensitive court details



AI & The Environment

Uses precious metals from the Earth that take billions of years to form

We need to consider the radical depletion of non renewable resources required in the AI system. From network routers, to batters to data centers. From the perspective of deep time, we are extracting Earth's geological history to serve a split second of contemporary technological time, building devices like the Amazon Echo and iPhone that are often designed to only last a few years -
Atlas of AI, Kate Crawford

“Hidden” labour from miners, manufacturers

...But the toxic metals used in their electronics inevitably end up back in the bodies of laborers manning poorly regulated disassembly plants in China. Their bodies are absent from the picture, just as the Chinese bodies of railroad workers are absent from nineteenth-century railroad photographs. - A Prehistory of the Cloud , Tung-Hui Hu



References

<https://www.scientificamerican.com/article/is-there-a-human-hiding-behind-that-robot-or-ai/>

<https://sketchplanations.com/fauxtimation>

<https://logicmag.io/failure/the-automation-charade/>

https://en.wikipedia.org/wiki/Clever_Hans

<https://fortune.com/2025/06/11/microsoft-copilot-vulnerability-ai-agents-echoleak-hacking/>

<https://www.bbc.com/news/articles/c0573lj172jo>

