

A bad day in the office...

Despite the best laid plans to limit any unanticipated incident to just two hours (worst case scenario), it appears that part of the recovery delay that brought the central bank [perilously close to delaying a welfare payments run](#) in August 2018 flowed from a confluence of super-high security ... and just plain bad luck.

The 67 page tome is a brutal lesson on how fire control system control test can go very horribly wrong when a facility is purposely hardwired to prevent intrusions of all kinds (literally a Fort Knox scenario).

Three hours offline might not sound cataclysmic. But [if you cut all power to a central bank at around 11am in the middle of a busy trading day when a pension run slated for the evening, it really doesn't get much worse.](#)

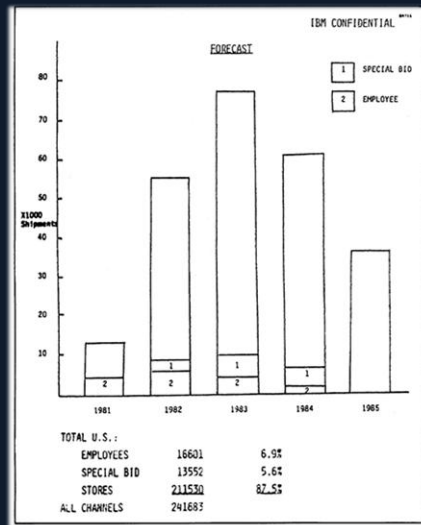
The outage economy

When the RBA's big iron tanks for a protracted period, especially its core Reserve Bank Information and Transfer System (RITS), it isn't just bad; it's potentially economy-outage bad in an age of electronic inter-dependence.

Among other things, failing security controls delayed operational restoration of services... Public communications triggered large-scale bot scanning of perimeters....

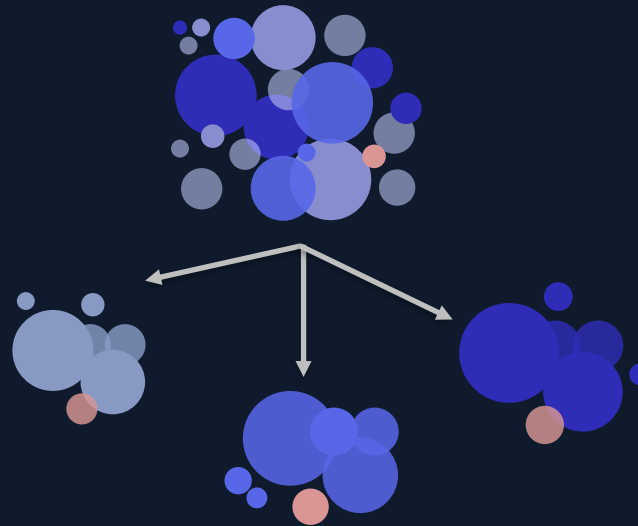
Moving from a risk to resilience mindset

IBM's PC Market Forecast
in the late 1970s



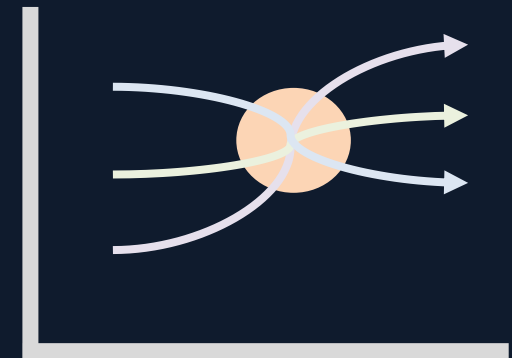
Predictions are fragile in periods of high volatility and uncertainty

In fields of high volatility and uncertainty...



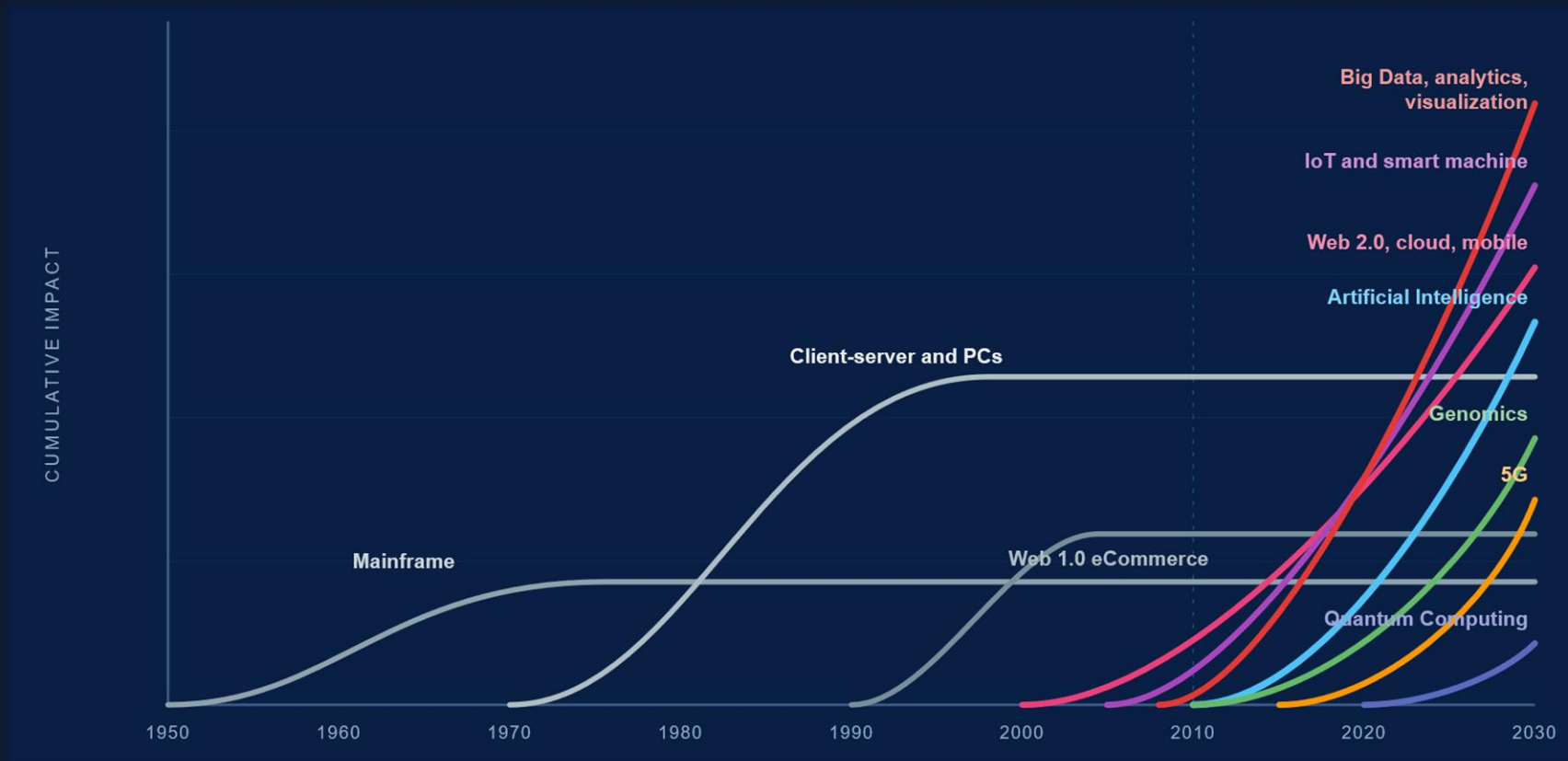
...develop scenarios that address key uncertainties

Look for common likelihoods, take action



Pursue low-cost, near term interventions that provide resilience for multiple scenarios

Converging Innovations. Compounding Risks.



What I learned from
NASA *about*
balancing risk with
research & innovation



Being innovative with a low risk tolerance *is hard*



Moon and Mars

Safety + Innovation is critical

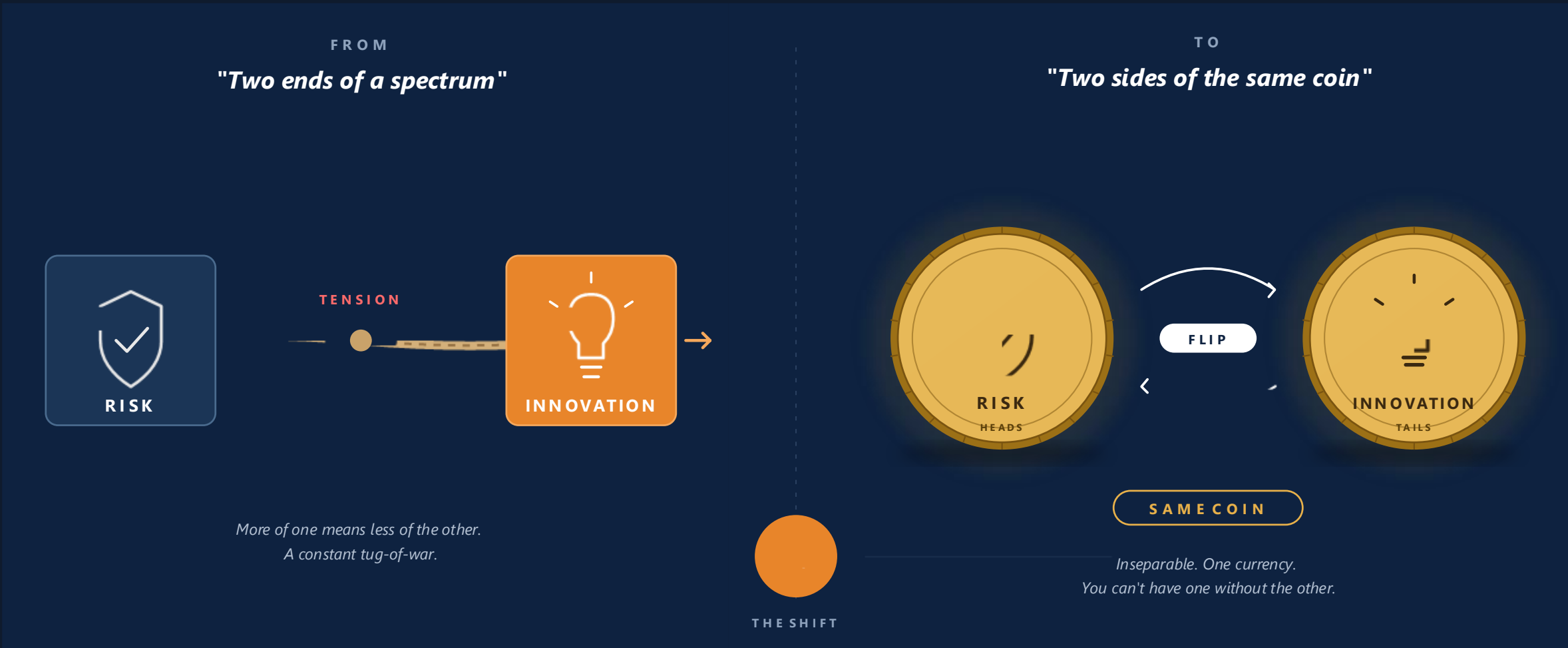


99.995%

real-time payments availability

Resilience + Innovation is necessary

Risk and Innovation: shifting the perspective

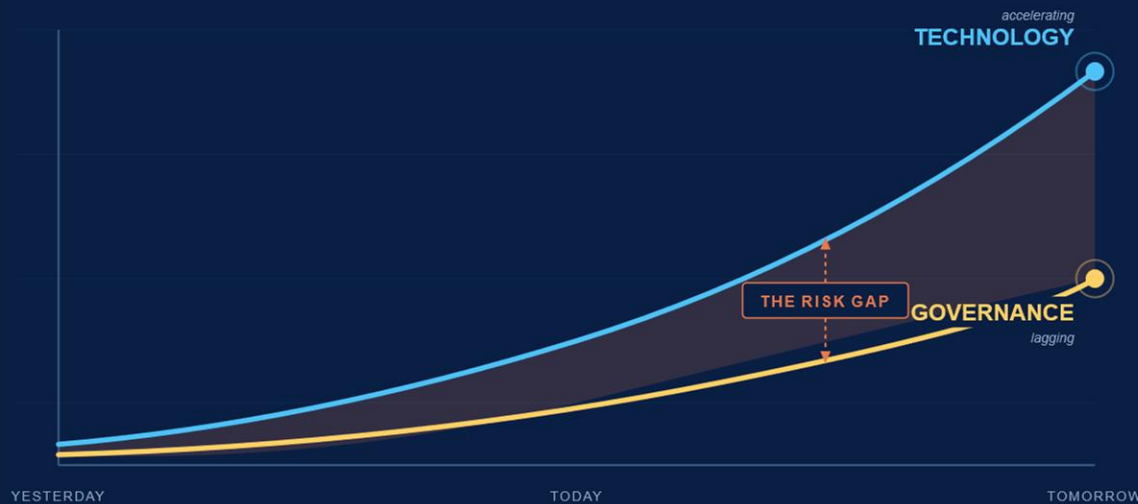


What industry is teaching us about about security, governance and research

Technology innovation scales faster than its governance

Scale technology. Scale governance.

THE GAP BETWEEN THEM IS RISK



Completed steps on "The Last Ones" per spent tokens

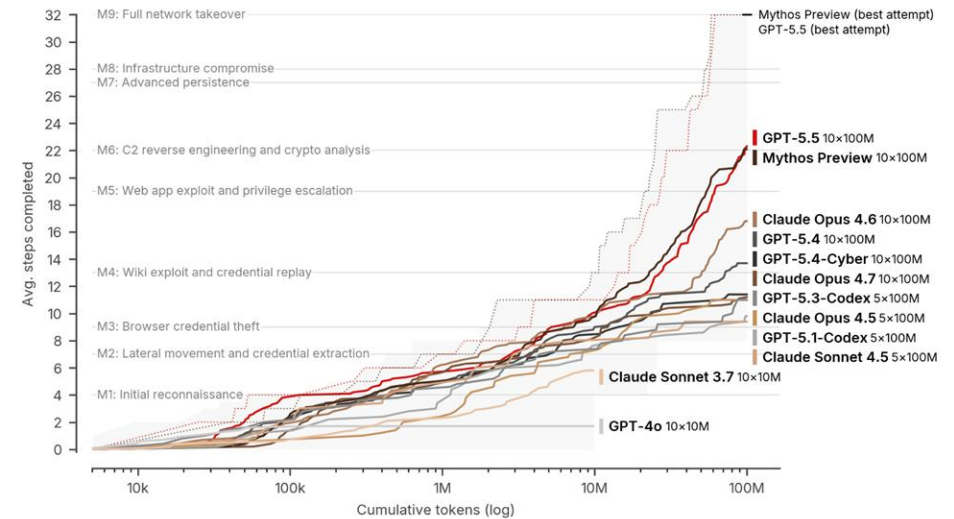


Figure 2: Average number of steps completed on The Last Ones (a 32-step simulated corporate network attack) as a function of total token spend. Each line represents a different model, with the shaded region showing the min-max range across all runs at each token budget. Grey horizontal lines indicate significant milestones in the attack chain.

<https://www.aisi.gov.uk/blog/our-evaluation-of-openai-gpt-5-5-cyber-capabilities>

Different growth drivers

Technology innovation compounds (compute, AI, automation) while governance grows linearly (people, committees, approvals). Excellent governance falls behind.

The security risk gap is a compounding debt

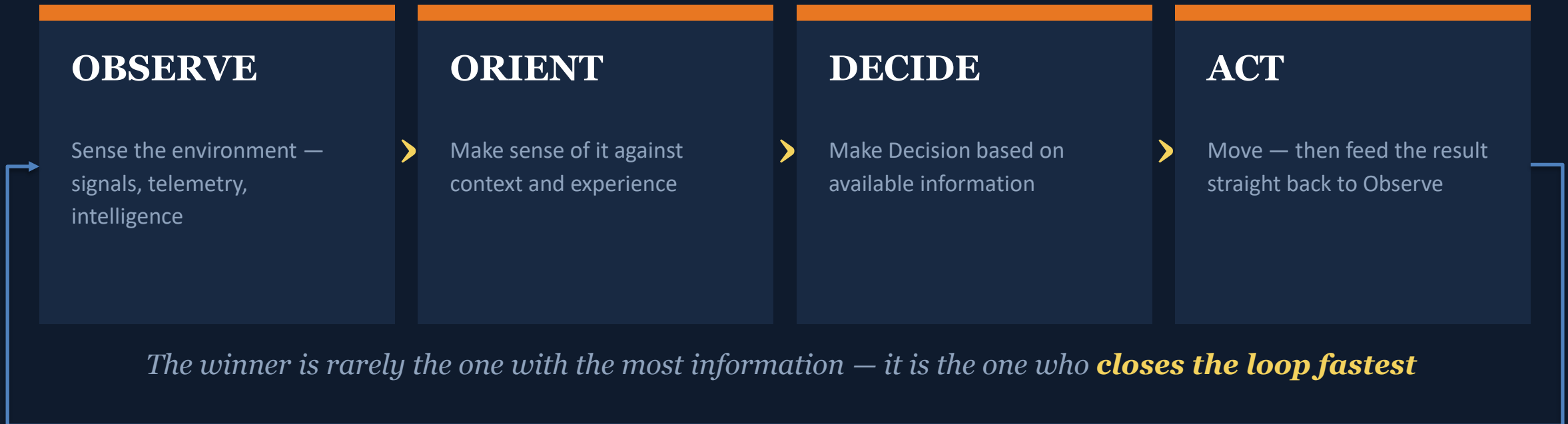
Residual risk doesn't hold steady — each cycle's residual becomes the next cycle's baseline. You can improve governance every year and still lose ground to innovation.

Can only close gap from the governance side

Slowing technology adoption cedes ground to adversaries who won't. The one lever you control is increasing governance responsiveness— decide faster, at volume

Decision speed: close and tighten the OODA loop

If we cannot slow technology innovation down, we have to speed decision and actions up. Boyd's Loop for warfare decision making — Observe, Orient, Decide, Act (OODA) — is a unit of governance efficacy.



Powell's 40-70 rule: Using security research and innovation to scale decisive action

*Colin Powell's Rule: In time-critical contexts, act once you have between **40% and 70%** of the information needed for certainty*



Use Security Research to:

- 1 *Identify new risks and theories*
- 2 *Identify new early signals*
- 3 *De-risk new scenarios*

Three take aways

01

RESEARCH

For many futures

Envisage new future scenarios.

Identify commonalities across scenarios.

02

UNIFY

Risk × Research Innovation

Research and innovate to target risks better

Solve for risks when innovating

03

BRIDGE

Close the gap between technology and risk

Trust declines when adoption > governance

Innovative governance needs to bridge gap

Thank you.