Navigating Uncertain Futures

Futures, Technology Trends & Cybersecurity Horizons

Adam Joinson, University of Bath

EPSRC CRANE Network Plus

CRANE
strengthening the Cyber Security research co

Today's Session

01

Why futures?

02

Methodology

03

Technology Landscape

04

Themes & Gaps

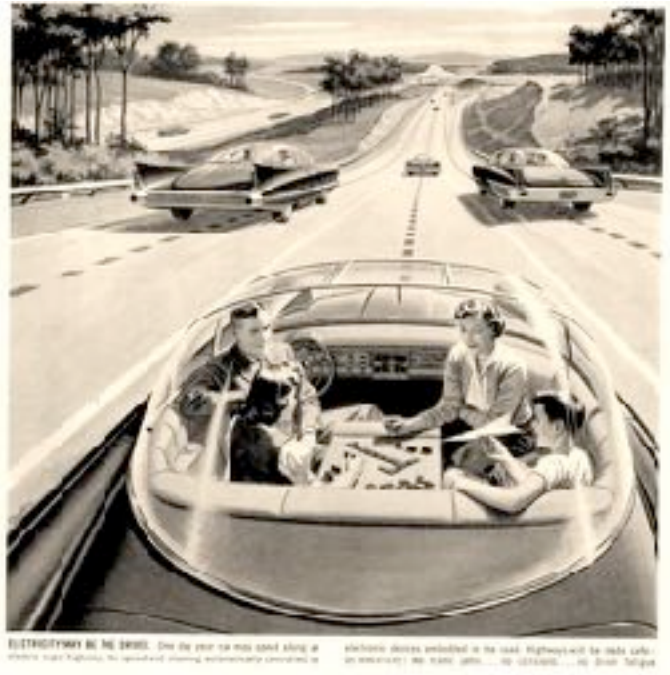
05

Implications & Next Steps

PART ONE

Why Futures?

Building the capacity to use the future differently



Futures Literacy

"Being futures-literate empowers the imagination. It enhances our ability to prepare, recover and invent in the face of change."

UNESCO (2026)

Not prediction

Futures literacy is not about forecasting what will happen.

Diversify

Widen the range of futures we can imagine -- and act on.

Anticipation

It concerns HOW we use imagined futures to shape present decisions.

The Problem: A Poverty of Imagination

"Most institutions operate almost entirely in an anticipation-for-the-future mode, systematically neglecting anticipation for emergence"

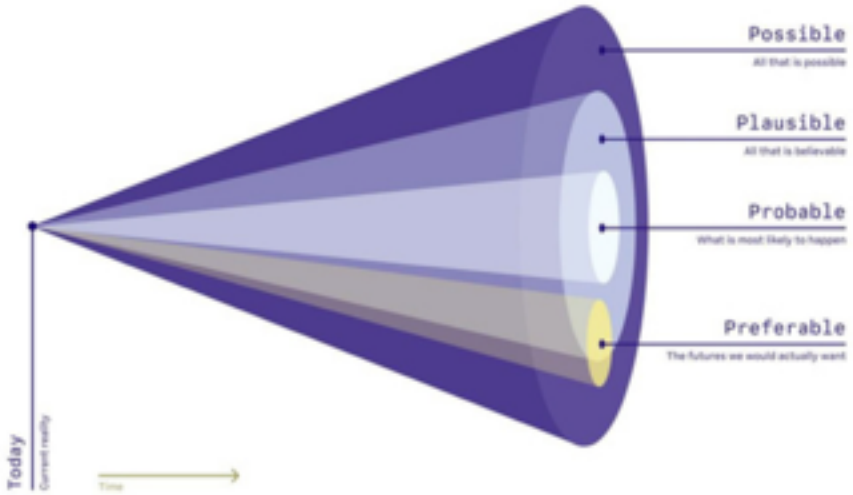
Anticipation for the Future

Focused on probable and desirable futures. Risk management and planning. The default mode - useful, but not enough.

Anticipation for Emergence

Staying open to genuinely new possibilities. Imagining radically different configurations. Often neglected - yet essential.

The Futures Cone: Four Types of Futures

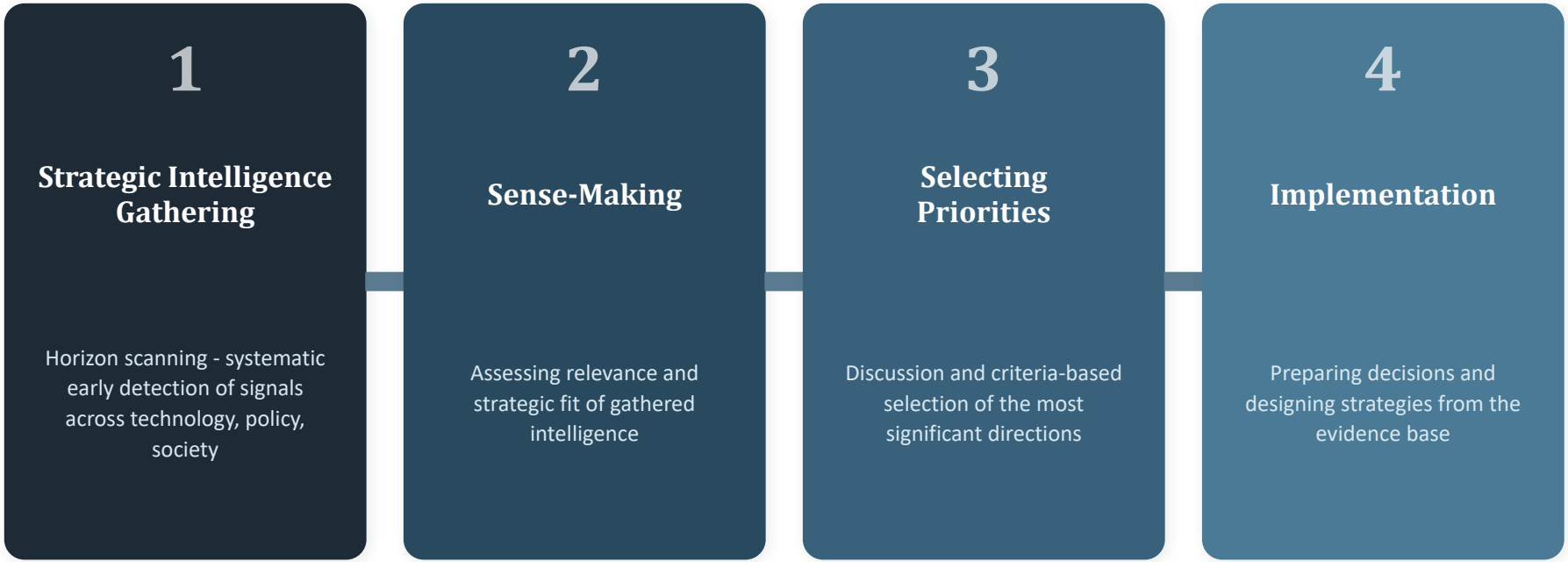


Source: Futurice, 'The Lean Futures Creation Handbook 2.0' https://futurice.com/lean-futures-creation-toolkit

Futures literacy expands our capacity to work across all four -- not just the probable

From Futures Literacy to Foresight

Futures literacy is the foundation; foresight is the structured process that builds on it.



Cuhls (2020): horizon scanning is necessary but not sufficient -- it provides raw material; foresight processes interpret, debate, and act on it

PART TWO

CRANE Methodology

A 4-stage foresight process for cybersecurity horizons

The CRANE Foresight Process: 4 Stages

September 2025 → May 2026 · 60+ priority technologies · 9 categories · 71 expert participants

1

Stage 1: Desk Research

80+ technologies reviewed across Gartner, Deloitte, IEEE, DARPA, ARIA, UK Government, and patent sources. Reduced to 63 cybersecurity-relevant technologies.

2

Stage 2: Delphi Studies

Two-round expert consensus study: 45 participants (Round 1) and 26 (Round 2) rated technologies on research need and adversarial exploitation potential.

3

Stage 3: Futures Workshops

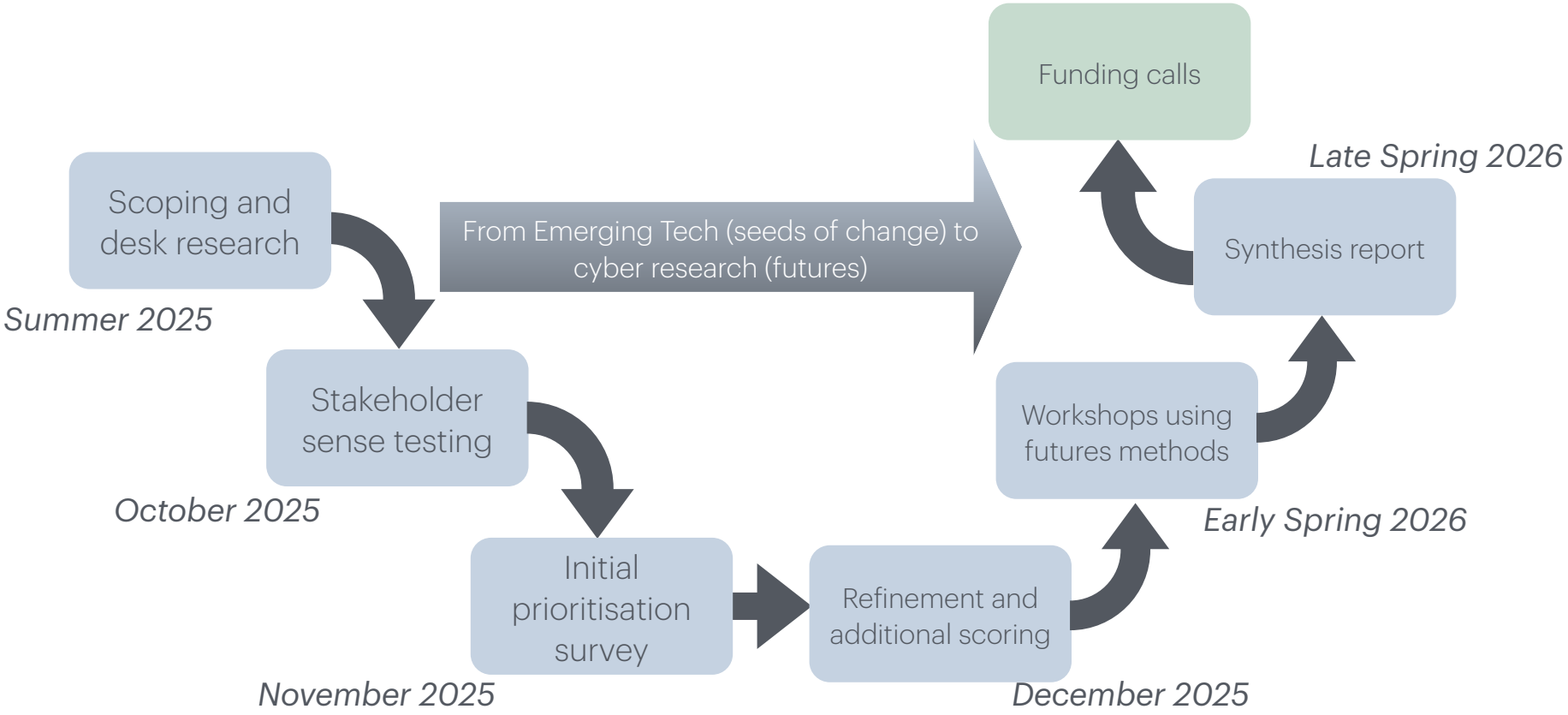
Two one-day workshops in London - AI (n=21) and Robotics/Automation (n=19) - using 'what if' scenarios and PESTLE implication mapping.

4

Stage 4: Analysis & Synthesis

Independent thematic analysis identified 9 themes, synthesised to 7. AI-assisted dual-coder theme→gap matrix (κ=0.953) cross-checked by human researcher.

Timeline


Scoping and desk research
Summer 2025
From Emerging Tech (seeds of change) to cyber research (futures)
Stakeholder sense testing
October 2025
Initial prioritisation survey
November 2025
Refinement and additional scoring
December 2025
Workshops using futures methods
Early Spring 2026
Synthesis report
Late Spring 2026
Funding calls

Stage 1: Desk Research -- Six Source Streams

Gartner

Hype Cycles 2024-25 (Emerging Tech + AI)
Innovation triggers & peak of inflated expectations

Deloitte

Tech Trends 2020-2025
Longitudinal view across professional services

IEEE

Mega Trends 2024 + Tech Predictions 2025
Computer Society annual predictions

DARPA / ARIA

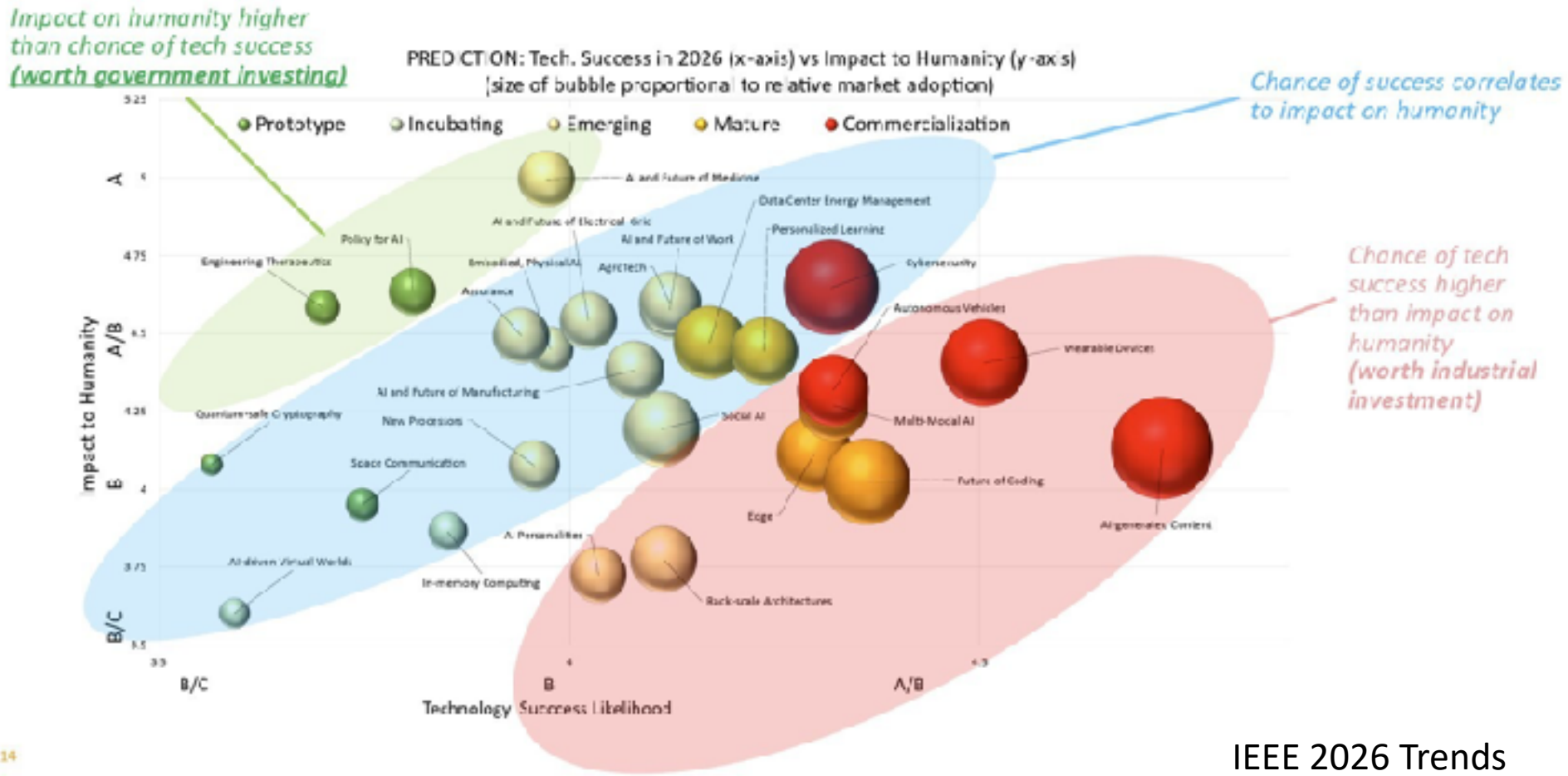
Ideas under incubation + UK ARIA funding calls
Earliest-stage emerging technology signals

UK Government

GO Science EmTech, Alan Turing Institute CETAS,
Royal Society, Royal Academy of Engineering

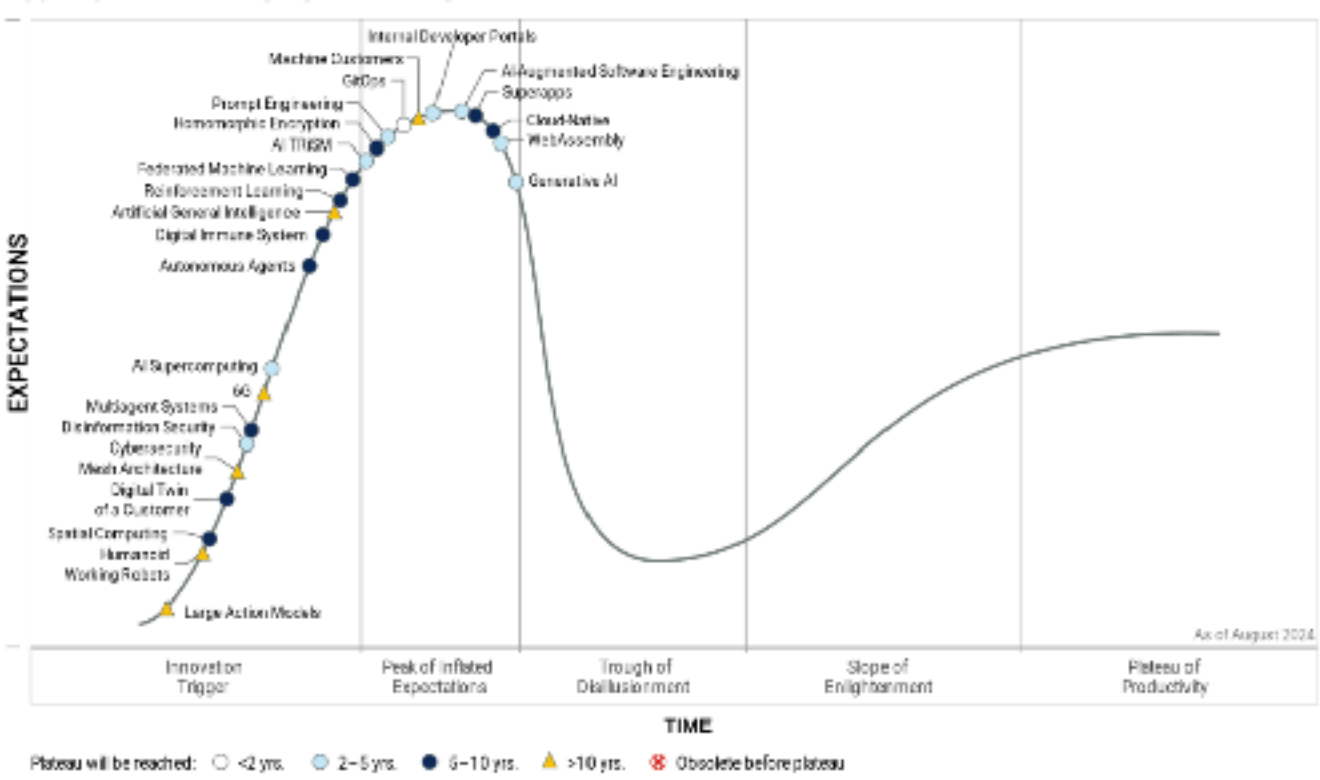
Patents

LexisNexis patent analytics +
Ellison Institute for Technology programme



IEEE 2026 Trends

Gartner Hype Cycle (and AI Hype Cyle) - 2025



Gartner

Deloitte Insights

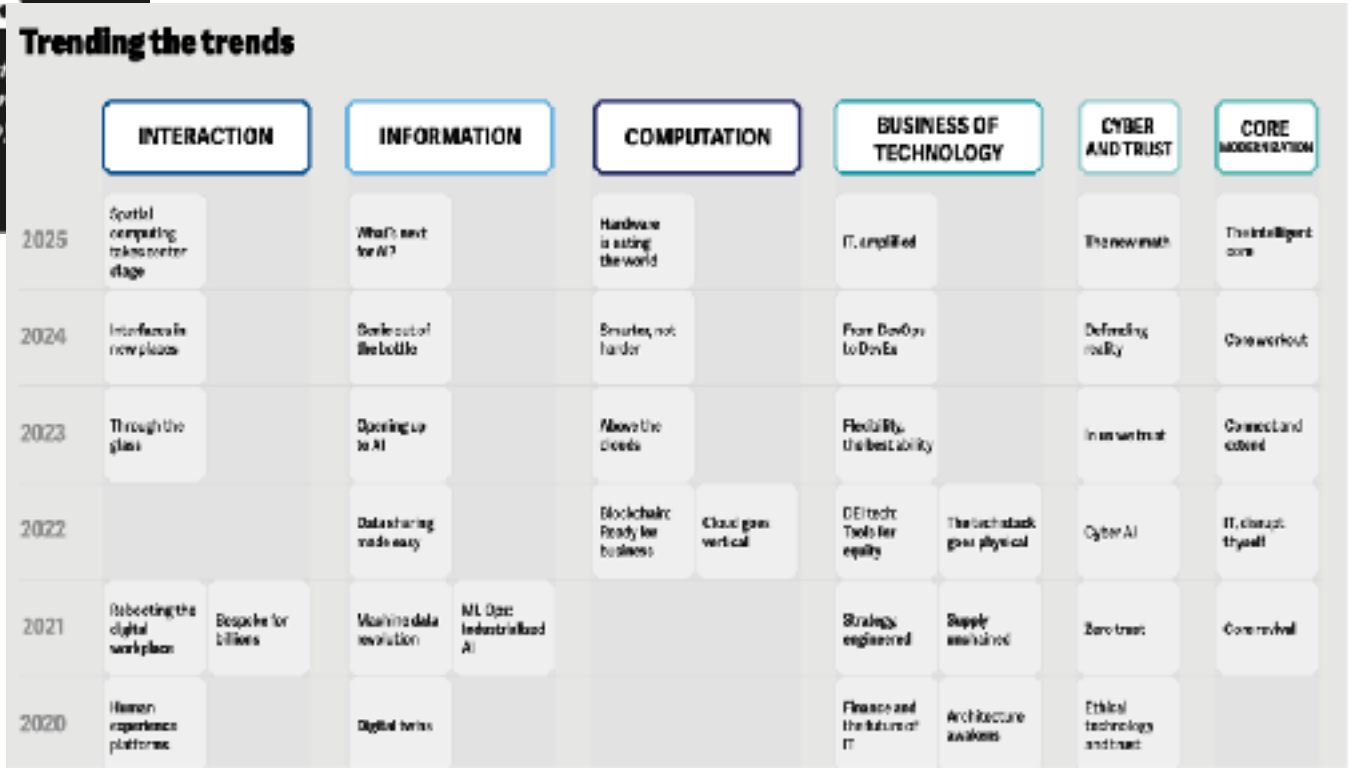
SPOTLIGHT

Tech Trends 2025

In Deloitte's 16th annual Tech Trends report, a common thread of nearly every trend. Moving forward, it will be part of the substructure of everything we do.

Explore →

Trending the trends



Stage 2: Two-Round Delphi Study

Round 1

- 45 completed responses
- Primarily UK academic cybersecurity researchers
- Ranked 63 technologies across 9 categories
- Criteria: research need, adversarial potential, socio-technical impact
- Selected 32 technologies for Round 2

Round 2

- 26 expert participants
- Scored 32 technologies on 5-point Likert scales
- Two dimensions: research innovation need + adversarial exploitation potential
- Self-rated certainty (0-10) per technology group
- Results plotted on quadrant diagram

Initial survey

Launched Autumn 2025

- **63 technologies**
- Ranked by "largest impact on cybersecurity in the next 10 years"
- 45 responses from experts
- Technolgies that scored >3.5, and/or were in top place by >10% of respondents, retained.

PART THREE

Technology Landscape

63 technologies across 9 categories with a 5-10 year horizon

Emerging Technology Rankings

Average rank (lower = higher priority) and share ranked 1st. Highlighted: avg ≤ 5.5 or ≥10% ranked first.

Avg. rank ≤ 5.5 · ≥ 10% ranked 1st

Technology	Avg rank	Ranked 1st
AI		
Agentic AI	2.52	40%
AI-Written Software	3.94	17%
Personalised AI Companions	4.87	6%
Artificial General Intelligence	5.39	19%
Emotion AI / Affective Computing	5.19	3%
Neurosymbolic AI	5.59	2%
AI-Based Medical Diagnosis	5.09	2%
AI-Powered Population Health Systems	7.05	0%
Edge AI & Federated Learning	7.41	2%
Liquid Neural Networks	7.41	2%
AI for Legal Reasoning	8.16	0%
AI-Guided Pathogen Surveillance	8.30	2%
AI-Powered Drug Discovery	8.30	0%
Chat Bots	9.75	0%
AI for Decarbonisation	13.10	0%
COMPUTING & DATA		
Post-Quantum Cryptography	3.21	29%
Quantum Computing	3.09	27%
Homomorphic Encryption	4.13	0%
Memory-Safe Hardware & Software	4.50	11%
Digital Twins	4.19	12%
Spatial Computing	4.50	10%
DNA Data Storage	5.14	5%
Neuromorphic Computing	5.70	5%
Optical Computing	5.19	2%
ROBOTICS & AUTOMATION		
Fully Autonomous Driving	1.69	49%
Delivery Drones	2.94	16%
Autonomous Space Robotics	3.55	16%
Autonomous Construction Robots	3.75	2%
Polyfunctional Robots	4.53	14%
Advanced Exoskeletons	5.30	3%
Smart Skins	5.75	0%

Emerging Technology Rankings

Average rank (lower = higher priority) and share ranked #1. Highlighted: avg ≤ 15 or ≥20% ranked #1st

■ Avg rank ≤ 15 ■ ≥ 20% ranked 1st

Technology	Avg rank	Ranked 1st
BIOMEDICAL		
Personalized Medicine	1.83	33%
Engineering Biology	2.18	24%
Bioengineered Engineering	2.66	16%
Nanogen Sequencing	2.66	13%
Organoid Intelligence (OI)	2.84	16%
Phage Therapy	4.39	3%
Programmable Yeast	4.53	4%
Nitrogen-Fixing Cereals	5.53	4%
NEUROTECH		
Brain-Computer Interfaces (BCIs)	3.04	40%
Neurosexual Enhancement	3.23	23%
Extending Human Senses	3.49	13%
Targeted Neuroplasticity Training	5.03	8%
Neurotechnology Consumer Goods	5.76	8%
MATERIALS		
Small Modular Nuclear Reactors	2.98	49%
Energy Harvesting Wearables	5.43	4%
Biodegradable Electronics	5.77	4%
Advanced Composite Materials	3.83	18%
Precision Optical Thermal Energy Relay	5.07	10%
Metamaterials	5.73	8%
Self-Healing Materials	4.41	13%
Radar-On-Wavelength Fibres	5.39	3%
ENVIRONMENT / SUSTAINABILITY		
Smart Agriculture	3.14	38%
Climate Engineering / Geoengineering	3.45	35%
Ocean Farming	3.88	14%
Space-Based Solar Power	3.47	25%
Carbon Capture & Utilization	5.03	8%
QUANTUM TECHNOLOGY		
6G	3.78	16%
Quantum Sensors & Clocks	4.31	20%
Smartdust	4.41	14%
Space Station Technologies	4.44	14%
Hypersonic	5.63	3%
DIGITAL / CYBER / ROBOTICS		
Digital Identity & Decentralized ID	3.49	38%
Internet-Based Wars	3.94	30%
Personalized Media, Entertainment &	4.28	13%

32 Priority Technologies Across 9 Categories

Artificial Intelligence

5 technologies

Computing, Data & Comms

7 technologies

Robotics & Automation

3 technologies

Biotechnology

5 technologies

Neurotechnology

3 technologies

Advanced Materials

3 technologies

Energy & Environment

3 technologies

Society & Governance

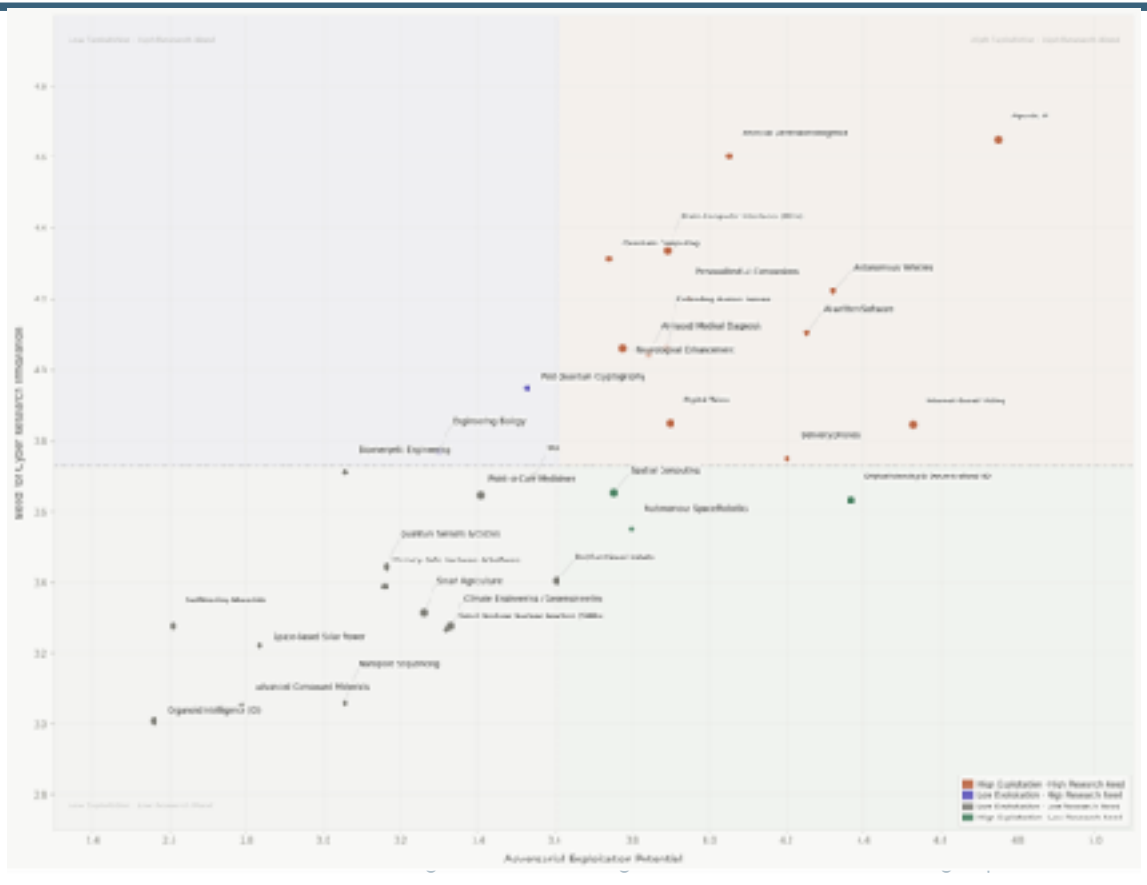
3 technologies

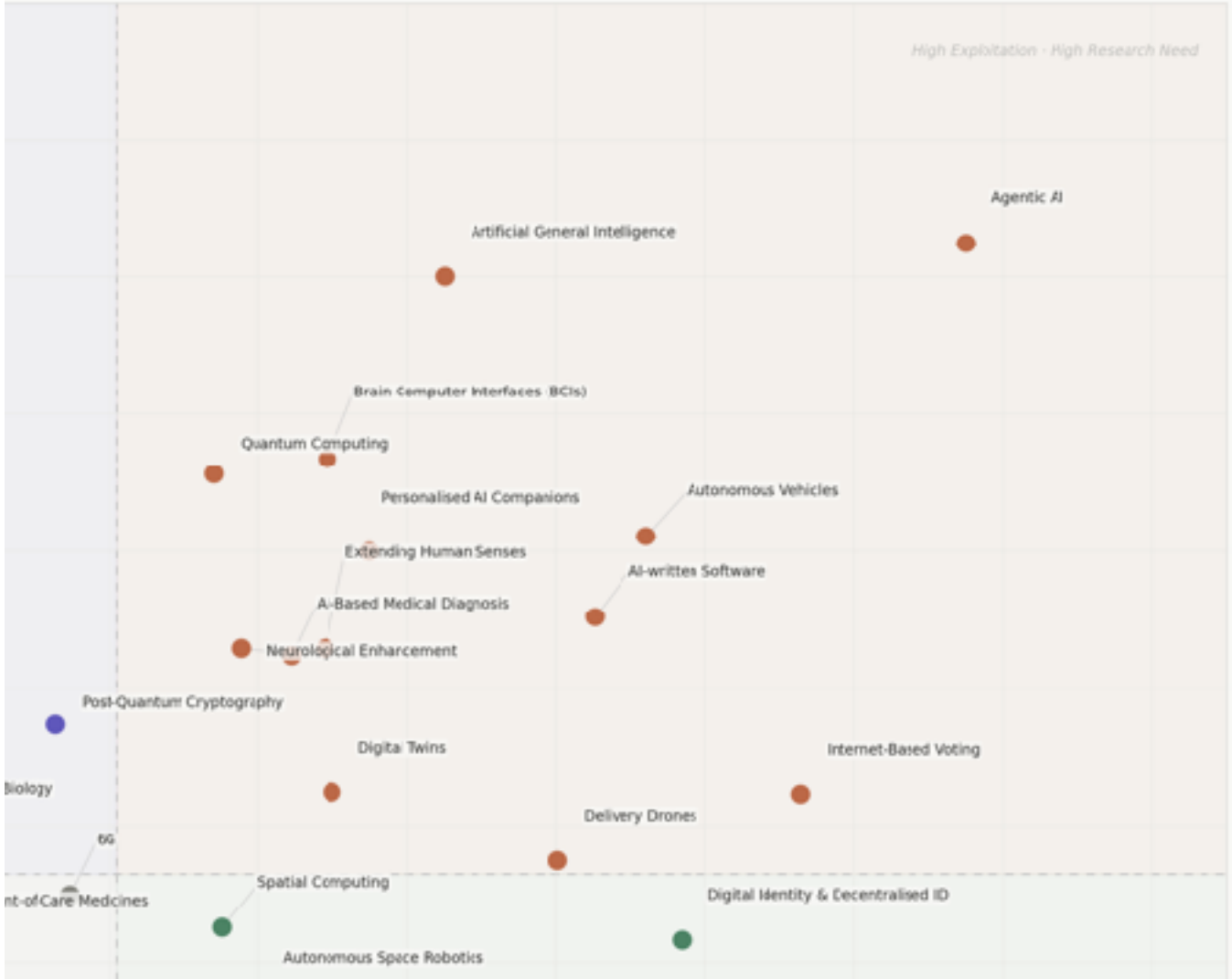
Space & Geophysics

1 technology

	How likely is it that this technology would be exploited by adversaries in novel ways?					What is the likelihood that securing this technology will demand innovation in cybersecurity research and practice?				
	Very unlikely				Very likely	Very unlikely				Very likely
	1	2	3	4	5	1	2	3	4	5
Agentic AI: AI systems capable of autonomous goal-setting and decision-making.	○	○	○	○	○	○	○	○	○	○
Artificial General Intelligence: AI with human-level cognitive abilities across any task.	○	○	○	○	○	○	○	○	○	○
AI-written Software: software autonomously generated by AI systems.	○	○	○	○	○	○	○	○	○	○
Personalised AI Companions: AI entities tailored to an individual's preferences, habits, and emotional needs.	○	○	○	○	○	○	○	○	○	○
AI-Based Medical Diagnosis: A tool assisting or automating diagnosis from scans, symptoms or ambient sensors.	○	○	○	○	○	○	○	○	○	○

Stage 2 Findings: The Priority Technologies Quadrant




High Exploitation · High Research Need
Agentic AI
Artificial General Intelligence
Brain Computer Interfaces (BCIs)
Quantum Computing
Personalised AI Companions
Autonomous Vehicles
Extending Human Senses
AI-written Software
AI-Based Medical Diagnosis
Neurological Enhancement
Post-Quantum Cryptography
Digital Twins
Internet-Based Voting
Biology
Delivery Drones
6G
Spatial Computing
Digital Identity & Decentralised ID
Autonomous Space Robotics

AI Technologies: The Dominant Priority

AI technologies dominated the priority quadrant - highest combined scores for research need AND adversarial risk

Agentic AI

Autonomous goal-setting and decision-making -- without human oversight

⚠ Prompt injection, rogue agent behaviour, long-horizon data poisoning

Artificial General Intelligence

Human-level cognitive ability across any task -- high-uncertainty horizon

⚠ Systemic risk; misaligned goals; loss of meaningful human control

AI-Written Software

Software autonomously generated by AI -- increasingly realistic within 5 years

⚠ Embedded vulnerabilities, supply-chain attacks, codebase opacity

AI Medical Diagnosis

AI tools diagnosing from scans, symptoms, and ambient sensors

⚠ Adversarial attacks on diagnosis; data poisoning; life-critical failures

Personalised AI Companions

AI entities tailored to emotional needs, habits, and preferences

⚠ Manipulation and cognitive influence at scale; privacy; dependency

Beyond AI: The Broader Technology Landscape

Computing & Comms

- Quantum Computing
- Post-Quantum Cryptography
- Memory-Safe Hardware & Software
- Digital Twins -- live simulation attack surface
- 6G and Quantum Sensors

Neuro & Biotechnology

- Brain-Computer Interfaces
- Neurological Enhancement & Extended Senses
- Engineering Biology / Synthetic Life
- Organoid Intelligence
- Nanopore Sequencing

Robotics & Society

- Service Robots & Delivery Drones
- Driverless / Autonomous Vehicles
- Digital Identity & Decentralised ID
- Internet-Based Voting
- Smart Agriculture (IoT at scale)

Common thread: physical-digital convergence dramatically expands the attack surface - and the consequences of compromise

Stage 3: Futures Workshops

Two one-day workshops · London · AI workshop (n=21) and Robotics/Automation workshop (n=19)

Futures literacy framing

Introduced the futures cone (possible/plausible/probable/preferable). Broad 10-year horizon thinking & first/second order consequences.

Future headlines

Participants sketched a future newspaper headline- activating narrative thinking about 1st and 2nd order impacts.

"What if?" questions

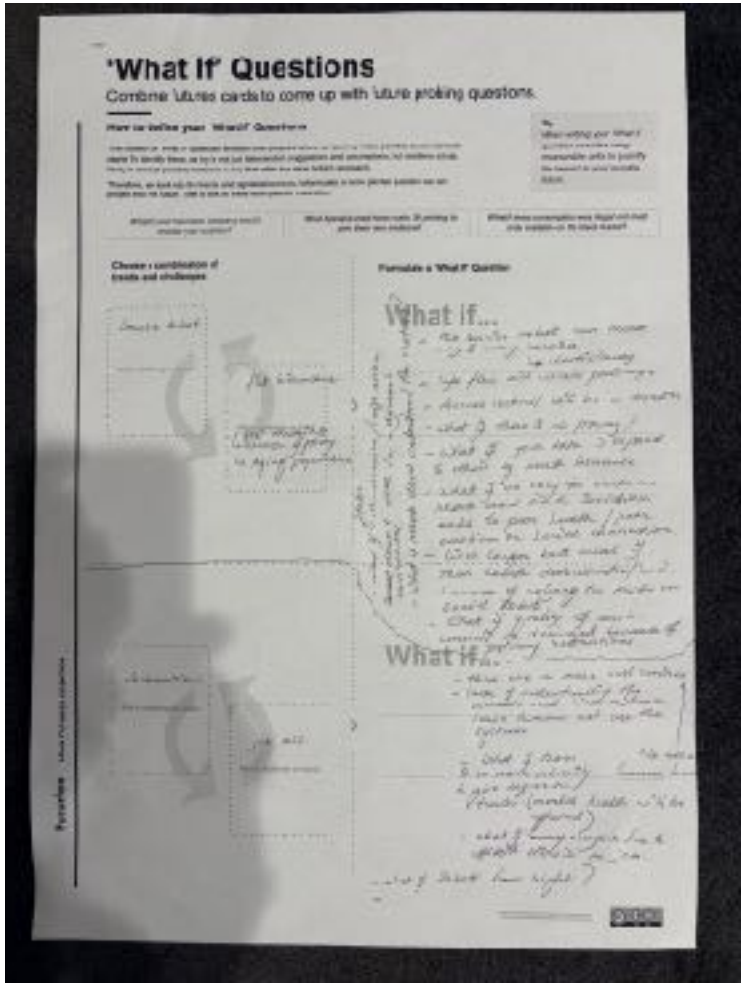
Technology × societal challenge (e.g., "What if service robots met an ageing population?"). Two scenarios per group.

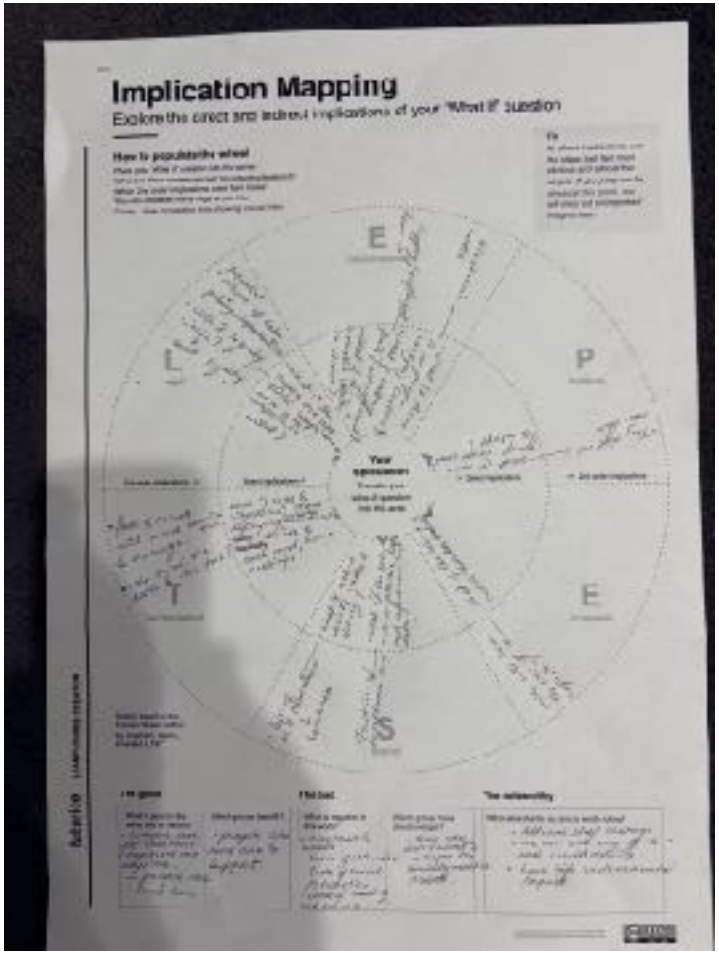
Implication mapping

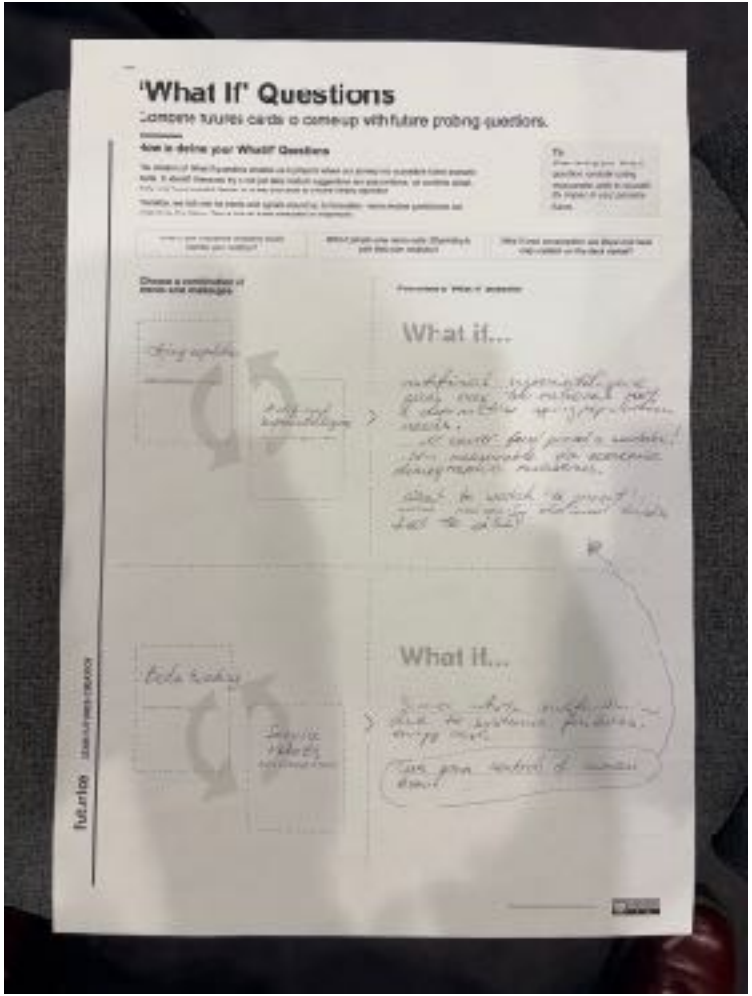
Futures wheel: 1st and 2nd order consequences mapped across PESTLE dimensions from a 'what if' seed statement.

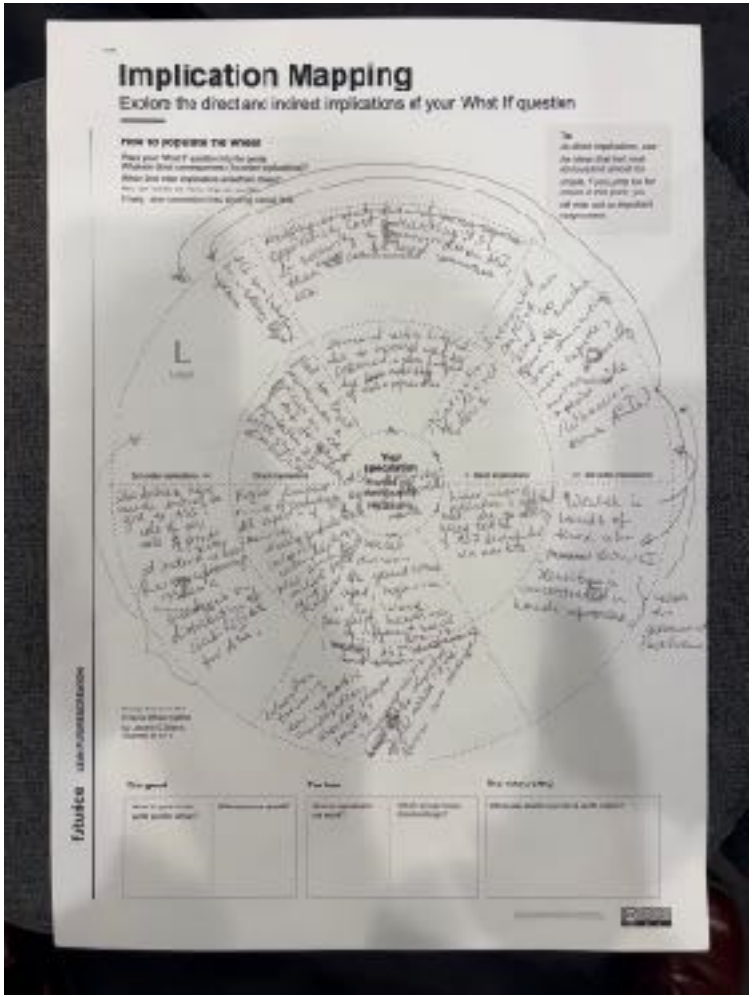
Summation

Groups recorded: the what-if question, cybersecurity implications, existing tools, and potential research gaps.


'What If' Questions
Combine futures cards to come up with future poking questions.
How to define your 'What if' Questions
Choose a combination of trends and challenges
Formulate a 'What if' Question
What if...
What if...


Implication Mapping
Explore the direct and indirect implications of your 'What if' question
How to popularize this wheel
Your speculation
E
P
E
S
T
L


'What If' Questions
What if...
What if...


Implication Mapping
Explore the direct and indirect implications of your 'What If' question

PART FOUR

Themes & Research Gaps

What the workshops revealed about cybersecurity's future challenges

Seven Overarching Themes from Workshop Analysis

Independent thematic analysis → 9 themes → 7 overarching

1. **Post-Trust Information Ecosystems**
2. **AI Sovereignty, Power & Geopolitical Cybersecurity**
3. **Shift to Adaptive, Emergent Cybersecurity**
4. **Cybersecurity Extends into the Human Body**
5. **Data Ownership, Lifecycle & Death**
6. **Future Cyber-Physical & Robotic Ecosystems**
7. **Governance, Inequality & Socio-Technical Resilience**

Theme 1: Post-Trust Information Ecosystems

AI-generated content and misinformation are structurally eroding trust. Verification is becoming technically harder. Who defines 'truth' in the future?

Key concerns

- Verification: data provenance, cryptographic signatures, post-quantum verification
- AI model epistemology: what does AI 'know' and how can it be validated?
- Risk of model collapse -- AI trained on AI-generated content degrades truth quality
- Democratic risks: threats to political stability, radicalisation, echo chambers

Research Gaps

- Scalable authenticity & provenance for AI-generated content
- Longitudinal monitoring of model integrity and data lineage
- Metrics for trust erosion, misinformation, and radicalisation pathways

Theme 2: Sovereignty, Power & Geopolitical Cybersecurity

Control over AI infrastructure, training data, and models is becoming a geopolitical power issue. Digital sovereignty is contested terrain.

Key concerns

- Dependence on foreign tech infrastructure -- concentration in 'tech elites' and large corporations
- Who controls data centres, training data, underlying models, and decision systems?
- AI-driven conflict, warfare, and national security implications
- Tensions: global collaboration vs sovereignty; efficiency vs autonomy

Research Gaps

- Frameworks for secure, modular, 'local-first' sovereign AI deployments
- End-to-end AI supply chain security and provenance tracking for datasets and models
- Defence and resilience strategies for AI assets targeted in conflict

Theme 3: Shift to Adaptive, Emergent Cybersecurity

Traditional preventative cybersecurity is insufficient for non-deterministic, adaptive AI systems. Security must become a dynamic, learning system.

Key concerns

- AI introduces vulnerabilities that emerge from system complexity, not just adversarial attacks
- Critical vectors: prompt injection, rogue agent behaviour, long-horizon data poisoning
- Static 'secure by design' is no longer adequate for systems that learn and adapt post-deployment
- Need: dynamic security that monitors, learns, and responds alongside the systems it protects

Research Gaps

- Formal models and verification methods for non-deterministic adaptive systems
- Understanding what 'security' means for LLMs and agentic AI systems
- Self-monitoring and self-healing AI security architectures

Theme 4: Cybersecurity Extends into the Human Body

As technology merges with biology, the attack surface expands into the human body and mind. Bodily privacy, cognitive autonomy, and physical safety are at risk.

Key concerns

- Firmware/software vulnerabilities within the body -- implants, neurotechnology, assistive devices
- Risks of malfunction causing harm or death -- safety-critical failures in biological systems
- Loss of bodily privacy and cognitive autonomy through technology-mediated influence
- Bio-data ownership: who owns data generated by or about your body, including after death?

Research Gaps

- New cybersecurity paradigm for implanted devices and bio-data ecosystems
- Understanding risks of cognitive manipulation via human-embedded technologies
- Regulatory frameworks: black markets for biohacks; insurance and law enforcement use of bio-data

Theme 5: Data Ownership, Lifecycle & Death

Personal and bio-data needs full lifecycle governance - from creation through use to device obsolescence to human death. The 'afterlife' of data is ungoverned.

Key concerns

- Who owns bio-data and device-generated personal data?
- What happens to data when a person dies or a device becomes obsolete?
- Data persistence vs the right to deletion -- enforceable deletion at end of life
- Environmental impact: recycling data-rich devices while ensuring no data remains

Research Gaps

- Post-mortem data governance: ownership and access rights after death
- End-of-human-life data risks -- currently entirely ungoverned
- Secure decommissioning and risk-managed recycling of data-rich devices

Theme 6: Future Cyber-Physical & Robotic Ecosystems

Robots and autonomous systems are mobile, sensor-rich, physically embedded agents. They expand the attack surface across everyday environments and create systemic vulnerabilities at scale.

Key concerns

- Ubiquitous data collection in homes, workplaces, hospitals, roads → privacy invasion
- Surveillance risks hidden in 'cute' robots or benign devices ('trojan horse' embodiment)
- Swarm-level vulnerabilities: compromise at scale, not just individual devices
- Human-robot trust exploitation and social engineering via embodied agents

Research Gaps

- Cybersecurity for mobile, socially-situated sensing agents (especially at swarm scale)
- Data governance for sensor-rich environments: collection, access, real-time privacy enforcement
- Detection of malicious robot behaviour: manipulation, covert sensing, social engineering

Theme 7: Governance, Inequality & Socio-Technical Resilience

Legal and governance systems are consistently lagging behind technological change. AI is reshaping inequality and human relationships in ways whose full consequences are not yet understood.

Key concerns

- Attribution and liability for AI decisions and autonomous system failures
- Cross-border jurisdiction over data and bio-data -- who has authority?
- Risk of AI influencing or writing legislation to benefit AI rather than humanity
- Widening inequalities: enhanced vs non-enhanced bodies; increased dependency; reduced agency

Research Gaps

- Operationalise accountability: attribution of blame when AI causes harm
- Security design for diverse, vulnerable, and marginalised users
- Governance of human-in-the-loop systems -- oversight, duty of care, safeguards against exploitation

Five Cross-Cutting Research Gaps

1

End-to-end AI Trust & Verification

Scalable authenticity and provenance for AI content; AI epistemology; metrics for trust erosion and misinformation

2

Adaptive Cybersecurity for Evolving Systems

Formal models for non-deterministic systems; self-healing/self-monitoring architectures; emergent vulnerability identification

3

Security of Human-Centred & Embedded Systems

New paradigms for implants and neurotechnology; cognitive manipulation risks; accessible, inclusive security design

4

Sovereign & Resilient AI Infrastructure

'Local-first' modular AI deployments; end-to-end supply chain security; resilience for AI assets as critical infrastructure

5

Governance & Accountability Mechanisms

Attribution of harm when AI causes damage; duty of care frameworks; adaptive governance that evolves alongside technology

Theme ↔ Gap Mapping Matrix

AI-assisted dual-coder analysis (two Claude instances) · cross-checked by human researcher · Cohen's κ = 0.953

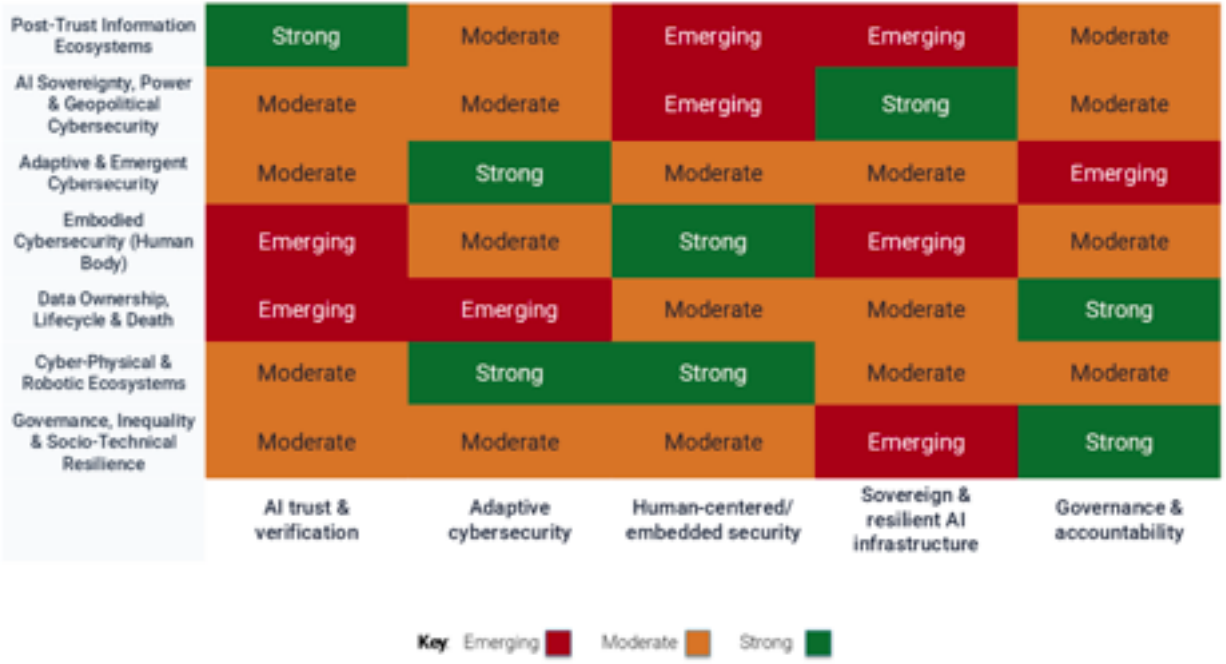


Figure 9: *Theme ↔ gap mapping matrix.*

PART FIVE

Implications & Next Steps

From horizon scanning to strategic research priorities

Implications for Cybersecurity Research

Most valuable opportunities combine technical innovation with socio-technical and governance mechanisms -reflecting a shift to ecosystem security

Verifiable information infrastructure

Provenance, authenticity and integrity at scale for AI-generated content and AI-driven systems

Adaptive security for AI-driven systems

New approaches for emergent, non-deterministic systems; moving beyond static 'secure by design'

Embodied & cyber-physical security

Where safety, privacy and human autonomy are intertwined -- implants, robotics, autonomous vehicles

Sovereign & resilient AI infrastructure

Supply chain assurance; local-first deployments; AI as critical national infrastructure

Operational accountability frameworks

Enforceable, adaptive, protective of vulnerable populations -- not just aspirational governance

Limitations & Future Work

⚠ Limitations

- Technology reduction may have excluded relevant areas (e.g., opto-electronics on 'watch list')
- Workshop expertise concentrated in AI and robotics -- e.g. bioengineering less deeply discussed
- Participants tended toward broad societal impacts rather than specific use cases
- Need to translate broad themes into tangible research questions and concrete mitigations

→ Next Steps

- Iterative CRANE foresight process - refine understanding of possible, plausible, probable, and preferable futures in cybersecurity
- Develop AI-assisted futures wheel tools and cyber-specific foresight resources
- Apply behavioural foresight: how do these technologies affect adversary and target behaviour?
- CRANE EPSRC funding calls informed by the theme-gap matrix

CONCLUSION

The future of cybersecurity is adaptive, embodied, and socio-technical

- Futures literacy enables us to move beyond probable futures into genuinely new possibility spaces
- AI is both a cybersecurity tool and the most urgent new attack surface of the decade
- The human body is the next frontier of the attack surface - embodied security is a new paradigm
- Security must become adaptive, ecosystem-oriented, and governance-rich to match the challenge