




# Future Scenarios Project Report

2024



## Contents

<b>Introduction</b>	<b>2</b>
<b>Considerations</b>	<b>4</b>
<b>Scenarios</b>	<b>5</b>
 <b>State of Alert</b>	<b>6</b>
 <b>Ecological Civilisation</b>	<b>10</b>
 <b>The Price is Right</b>	<b>14</b>

### Disclaimer

The scenarios presented in this paper are not intended to be projections or forecasts of the future, nor expressions of desired future states. Each scenario envisages a context from which new internet standards, protocols, and governance models might evolve or replace the structures we know in 2024.

Our scenarios, including the scenarios contained in this content, are not auDA's strategy or business plan. They are designed to challenge complacency. They are designed to stretch us to consider those events that are plausible but may seem only remotely possible.

# Introduction

auDA administers the .au domain in the public interest and ensures it is a secure, accessible and trusted Australian critical asset for all internet users.

Our work means we regularly think about the way Australians use and depend on the internet and how technologies and their use might evolve. This includes thinking about the key role of the domain name system (DNS), the challenges it might face and how best to manage the .au domain, so that it supports Australia's economy and community needs and expectations into the future.

As auDA's 2021-25 Strategy draws to an end, we need to undertake long term, deep thinking about our future operating environment and what it might mean for Australians, the .au domain and auDA. We must challenge ourselves and ensure there is no complacency in our approach.



**Rosemary Sinclair AM**  
auDA Chief Executive Officer

**In an industry that is little more than 30-years old and defined by innovation, disruption and dynamism, we know our future will be markedly different to our past. We are committed to thinking about what that future might be and how it will impact auDA's operations.**

To support auDA's future scenarios project, we engaged the expertise of strategy and foresight practitioner, Dr Matthew Finch, Principal of Mechanical Dolphin and Associate Fellow of Saïd Business School at the University of Oxford.

**The scenarios set out in this paper are intended to challenge current assumptions and forecasts, pressing us to consider plausible and relevant possible futures that we may experience in years to come.**

They will provide auDA – and other organisations – with the opportunity to navigate ambiguity, disruption and change, to drive innovation and manage future complexity by thinking about it in advance.

These scenarios have been built using an adapted form of the Oxford Scenario Planning Approach developed at the Saïd Business School. These scenarios are grounded in auDA's current business environment, including the wider global internet governance ecosystem (known knowns), and the uncertainties that surround this environment (known unknowns).

They have been built iteratively over a period of months with a core team at auDA and a diverse set of local and global expert participants representing the public, private and not-for-profit sectors, across a range of industries, communities and stakeholders.

The scenarios were tested for plausibility, relevance and contrast, and were benchmarked against a series of surveys and interviews that both established and challenged pre-existing perspectives and expectations about the future of our networked world.

auDA has prepared this document as a public resource. We hope it will be useful and thought-provoking for those who work in the domain name field, the broader information, communications and technology sector and those sectors who use the internet as critical underlying infrastructure. We hope it might also support the industry to work towards a shared future.

We thank those who have generously engaged with us throughout the process, within and outside auDA. Each participant provided great input into our scenario models and allowed us to stress test their plausibility. We are pleased to have built these scenarios with you and with the benefit of your expertise and consideration.

# Considerations

**For each scenario, we encourage you to consider the impact on the internet, its underlying infrastructure, governance and protocols.**

**These considerations could include:**

- How are future communications platforms and networks (including the various layers of the internet) owned and governed in each scenario?
- How would each scenario affect trust in, and use of, the internet?
- If the scenarios were ahead of us, what interventions might be required to ensure the security, openness and global interoperability of the internet into the future?
- If we could be sure each scenario would unfold as set out in this document, what would we expect to see in the near term?
  - What actions might we need to take in anticipation of key issues and opportunities arising?
  - What work is required to prepare for these futures?
- In each scenario, what new skills or capabilities might be required to manage the various layers of the internet into the future?
- If we look back on the present with hindsight from the 2044 presented in each of these scenarios, what fresh perspective do the scenarios offer on the world as it is in 2024?
  - How would people in each scenario judge the work being done and the decisions being made today?

# Scenarios





2044 – Scenario 1

# State of Alert



## National security is the priority in a world of global tensions

Over the 2020s, geopolitical tensions continued to rise, driven by competition for resources under the increasingly severe impacts of climate change. In this new atmosphere of fear and risk aversion, national and personal security became more important than liberty to citizens around the world.

The 2030s grew increasingly turbulent, with representative democracy seen to have failed and elected politicians unable or unwilling to find avenues for consensus at home or overseas.

By 2044, a variety of new forms of governance, perceived to be more fair and stable, are enabled by advanced artificial intelligence (AI) and surveillance technologies. Local and global policy makers debate the parameters and principles coded into these largely autonomous governance systems, but there are fewer “humans in the loop” with each passing year.

Citizen assemblies, chosen by AI algorithms so they are demographically representative, provide guidance and approval to government. While their powers are largely advisory, they allow governments to say they understand and respect the will of the people.

Critical infrastructure and manufacturing have been nationalised in almost all jurisdictions. Technology is primarily a tool of control. Governments exercise their will and manage dissent through the power to digitally

deny access to education and health services, transit, resources, telecommunications and financial transactions.

Attempting to secure precious resources and assert dominance, nation-states have expanded or developed alliances beyond their traditional physical borders to encompass virtual spaces, orbital platforms and installations on both the seabed and sea surface.

Domestic circular economies have developed, and as AI-empowered supply chains emphasise “just-in-case” resilience over “just-in-time” cost efficiency, there is a trend towards shoring up supply chains within geopolitical blocs (“friend-shoring”). Consumerism moves away from goods and towards experiences, including virtual ones.

The global internet has split along geopolitical lines with regional “drawbridges” to allow connections when necessary, as a fragile and uneasy peace is maintained between rivals who cannot afford to lose access to rare materials. The fear of geopolitical tensions escalating into physical conflict means that covert cyber skirmishes are frequent. These incidents, often conducted by proxies, are an open secret.

Decentralised and distributed energy control systems, managed via digital networks, become a key part of decarbonised energy supply and represent major points of vulnerability.

Cybernetics advance as a by-product of military research and development; computer chip implants are now commonplace among the general public. Digital twins are increasingly built for systems at all levels, from climate and logistics to individual human biology. Recognising that humans are always the weakest link in cyber security, governments encourage the public to maintain a perpetual state of alert. People are expected to be "citizen-soldiers", doing their patriotic duty in the fight against climate catastrophe as well as keeping watch against foreign adversaries. In the networked nations of 2044, we are warned that all spaces are potential battlespaces.

By giving service, citizens obtain government issued "social credits", validated through personal data shared with the state and its agencies. These credits, which affect one's prospects in everything from education to dating apps, are then added to digital passports. These passports are now standard issue and important for monitoring the rise in climate refugees, who have increased in number as sea levels and global temperatures have risen. Such passports are also required for software, enabling users to understand the software's genesis and verify its legitimacy.

Due to the decreased range and capacity of sustainably powered aircraft and the volatility of hydrogen powered craft, air travel becomes punitively expensive. Ocean travel is increasingly dangerous due to global tensions and increasingly unpredictable weather systems impacting the security of the high seas. Citizens increasingly retreat into advanced virtual worlds for learning and leisure.

Censorship in these spaces is widespread. Misinformation and disinformation are heavily policed, though online gaming expands and e-gaming communities become significant forces in society. Dissidents who are unable to take to the streets express their views online, using continually updated puns and coded language in game chats, leading an endless game of cat-and-mouse against censors armed with AI.

There is also a revival in UFO sightings worldwide, as satellite congestion and space debris increase. New conspiracy theories abound regarding forces that are capable of reading one's private thoughts and eluding even the most advanced digital surveillance.

## IN THIS SCENARIO

**Information** is the property of the state and it is citizens' duty to produce it.

**Identity** is biometrically linked and easily available for government scrutiny, with a single identifier for each user within a national system; citizens who wish to assert alternative identities seek to do so within gaming communities.

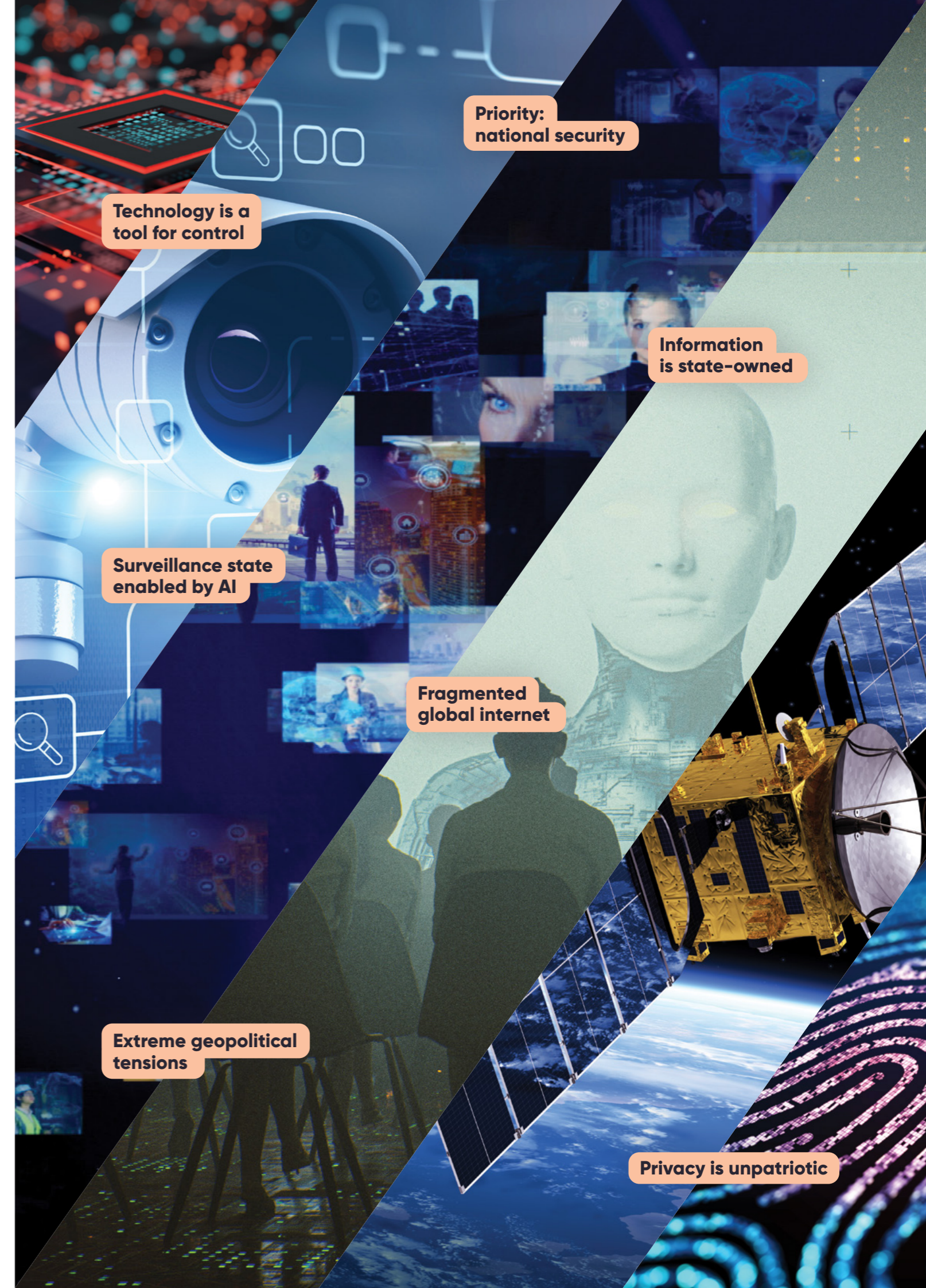
**The internet** is a critical national security asset, divided along geopolitical lines; protocols are designed to maximise security within each bloc and sharpen competitiveness against international rivals.

**Individuals** earn their rights (and access to new technological developments) through citizen service.

**Privacy** is unpatriotic and impedes one's upward social mobility; sharing your data is an accepted cultural norm.

### Technology implications include:

- Domain registries are nationalised and the ability to register a domain name is linked to a government issued digital ID
- Network protocols see that all data packets incorporate the unique digital ID of the person sending and receiving the packets
- Governments have access to a directory of digital IDs that delivers them insights on all communications and content created
- AI software constantly monitors communications and stored data, and looks for patterns of dissent and changes from usual behaviour
- New dark webs exist outside of the government-controlled cloud.



**Priority:  
national security**

**Technology is a  
tool for control**

**Information  
is state-owned**

**Surveillance state  
enabled by AI**

**Fragmented  
global internet**

**Extreme geopolitical  
tensions**

**Privacy is unpatriotic**



2044 – Scenario 2

# Ecological Civilisation



**Collective resilience is the priority  
in a world where climate catastrophe  
can no longer be ignored**

In the 2020s, the world's geopolitical and economic centres of power moved rapidly eastwards, as the region took the lead in the production of electric vehicles, solar panels, wind turbines and sustainable building materials. At the same time, climate events that were previously expected to occur "once a century" became the widespread norm, drastically impacting human civilisation as it lurched from one worldwide crisis to another. This led to a growing recognition that humanity must pull together to respond to this systemic and existential threat.

Rising nations of the global majority eclipsed the dominant powers of the 20<sup>th</sup> century and a new international coalition formed in the face of the climate catastrophe. At the same time, within the formerly dominant nations, new co-operatives arose from the environmental movement, forming a globally networked, online, eco-focused community of mutual aid. What once was considered radical climate activism, came to be seen as common sense in the face of near environmental collapse.

Over the 2030s, western governments adopted a more deliberative approach to governance, with greater attention to shared responsibility, evidence-based responses, consultation and co-design within these co-operatives. This also contributed to more inclusive forms of governance and civic debate.

The global order of 2044 is more multi-polar than in the early 2000s, but the world tends to look to the economic centres of the East for political leadership. The United Nations and other institutions have evolved to meet the climate crisis. International governance now includes a negotiated rebalancing of excess energy and resource use between nations, aiming to bring the global economy back into balance with the natural world. Crimes against the environment come under the purview of the International Criminal Court; a new global asylum covenant has been established; and institutions like the World Trade Organization have transformed to suit a planet where economics must reconcile sustainability with profit. "Blue helmet" peacekeepers are deployed to pacify resource conflicts, enforce international environmental agreements and address the growing problem of permanently displaced climate refugees.

Digital infrastructure is built for resilience, redundancy and adaptability in adverse and unpredictable environmental conditions. By 2044, it is beginning to incorporate the natural world, so that the Internet of Things has become the Internet of Everything, including networked flora, fauna and objects in outer space. This increasingly feels like a dialogue, where new modes of animal-computer interaction are available, biochemical computation is a major research field and nature itself has increasing access to digital spaces.

In turn, learning from these innovations feeds back to novel forms of human-computer interaction, including developments such as a tactile internet. It also supports a “One Health” approach, pursuing optimal health outcomes by recognising the interconnection between people, animals, plants and their shared environment. The Hippocratic Oath now applies to the entire planet. Local communities take increasing responsibility for the natural and built environment, including online spaces, as well as local digital and critical infrastructure which may be vulnerable to extreme weather events.

The ability of social networks to communicate with each other inspired a new generation of free, open-source, independent and interoperable platforms. The internet is regarded as a tool for climate solutions and digital interactions are regulated for energy use and climate impact. The dollar-based financial system has given way to a new generation of digital currencies that evolved from the cryptocurrency era. Within this new financial system, a culture of radical transparency has developed, with individual tax returns publicly available online, strict climate auditing and robustly enforced environmental sustainability standards. Next-generation AI, built on vast datasets and under the regulatory environments of different nations, has proved a powerful global tool for environmental intervention, resource management and enforcement.

The trusted educational content needed to support climate action is also seen as critical infrastructure; open access is the norm and there has been widespread democratisation of education through digital media. The misinformation and disinformation which proliferated in the 2020s is recognised as a deeply harmful and divisive contributor to the climate crisis. Grassroots anti-disinformation corps, citizen journalists and local media have since arisen within the new global green movement, “rewilding” the polluted news ecosystem and shaming those who falsify environmental credentials or try to gain influence by manipulating information.

## IN THIS SCENARIO

**Information** is open wherever possible – wherever and whoever you are, you and your community should have the tools and resources you need to play your part in the climate battle.

**Identity** is totally transparent to all.

**The internet** is federalised, serving as the basis for global climate debate and solutioneering; protocols are designed for resilience, interoperability and open scrutiny.

**Individuals** must put the community's needs first and be mindful of their place in a fragile wider ecosystem.

**Privacy** is a matter of abstinence from the digital environment. Reducing voluntary digital interactions reduces one's digital footprint as well as one's impact on the environment.

### Technology implications include:

- Inexpensive, miniaturised receivers and storage devices are embedded in individual items at the point of origin to improve the granularity of information
- Network protocols effectively transmit and receive information from billions of devices on a continuous basis
- Network protocols see that all data packets incorporate information on the use of resources to produce that data
- Blockchain technology tracks the path of resources through the end-to-end value chain
- The dark web supports encrypted applications facilitating the use of scarce resources without accountability.



Internet of Everything

Priority:  
collective resilience

Sustainability  
over profit

Eco-focused community

Technology to support  
climate solutions

Culture of radical  
transparency

Natural disasters  
an existential threat





2044 – Scenario 3

# The price is right



**Profit is the priority in a world where corporations transcend the nation-state**

The 2020s saw a cyber security and misinformation/disinformation “arms race” between actors including rival governments and criminal enterprises. Developments in AI unleashed countless autonomous bots which rendered all spaces dependent on the internet – both digital and physical – highly insecure. Cyber security became the world’s leading challenge at every level, from the individual to the institutional. Citizens, already disillusioned with the effectiveness of their governments, lost trust in the state’s ability to protect them or provide basic services, as public sector databases and infrastructure were continually subject to successful cyber attacks. Meanwhile, a series of corporate innovations in clean energy, privatised medicine and quantum cryptography led to increasing faith in “celebrity tycoons” as saviours of the human race – and a corresponding loss of faith in government.

In the 2030s, the fabric of the nation-state was unravelling, and with it many long-standing allegiances. Former public services were largely privatised and offered by the private sector on a subscription basis. Even law enforcement required victims of crime to hold “investigation insurance” to obtain full justice. Cyber security fell under the purview of private sector cartels. Blockchain-based systems underpinned many transactions, and advanced systems monitoring significantly reduced cyber threats – for those who could afford a subscription.

As the power of the nation-state waned, and that of corporations rose, businesses increasingly set the rules of global governance, focusing on economic stability and light touch regulation to encourage innovation and maximise profit. Political geography included membership of privately owned virtual spaces, and governance involved a tangled web of competition and collaboration among the elite class who sat on the boards of big businesses. Coming of age in an era of hyper-capitalism, AI-supported learning and climate action, youth-led start-ups began to flourish and 12 to 18 year olds became a powerful constituency, demanding equal rights to those of adults, including the right to full economic and political participation.

In 2044, climate change is causing obvious and adverse impacts, which are seen by corporations as a technological research and development challenge, as well as a population-level behavioural science challenge. The focus is on identifying and maintaining more or less hospitable local environments in which to do business; and employees and resources based in zones of high climate vulnerability are a bottom-line threat.

Breakthroughs in cryptography, biotechnology and AI have encouraged a culture of technological solutionism. There is increasing interest in geoengineering as a long-term response to climate change, but there are

significant inequalities in how technological benefits are distributed, both within and between societies worldwide. Innovations and novelties proliferate in this networked world, with different providers offering varieties of holographic communication and elaborate haptic interaction to those who can afford them.

Citizens in developed areas are treated as consumers first and foremost; they must be savvy about managing the multiple short- and long-term subscriptions that provide services to their families. Corporates have taken on social responsibility by bundling basic welfare subscription services with employment. In lower income regions around the world, populations are treated extractively by corporations as sources of raw data and sites for technological experimentation, with the aim of developing them from research subjects into profitable consumers over time. Business interests seek to disrupt or co-opt informal barter arrangements, community exchange and organised labour wherever possible, including by operating profitable privacy brokerage services, through which individuals can buy or sell their data, or that of their dependents.

Misinformation remains widespread, although subscriptions are available to competing “debunking services” that filter and label media according to set criteria and principles. While corporate powers use curated private-access information as the basis for business decisions, the media ecosystem available to the general public is full of “junk food” and “infotainment”. It is widely understood that there is no clear line between news and entertainment.

## IN THIS SCENARIO

**Information** of every kind is a tradable commodity.

**Identity** is multiple, provisional and tied to individual subscriptions, with consumers holding different identities across different platforms – some more valuable than others.

**The internet** is global and vital to commerce, research and development; protocols are designed to maximise opportunities for innovation and profit.

**Individuals** use different personas for different services and must take increasing responsibility for matters which were once the preserve of the state.

**Privacy** is a privilege to be traded by brokers on data exchanges.

### Technology implications include:

- Trusted digital identities allow corporations to “mark” information verified by them
- Digital ID enables users to manage and maintain multiple digital identities and subscriptions in one place, that can be used in multiple systems
- Directory services of trusted corporate identifiers enable independent verification of corporate information
- Network protocols see that a user’s digital ID is incorporated into data packets, enabling the user’s access to be verified against their subscription and costs to be charged back
- The internet search engine is AI driven and delivers information and services directly. Websites and domain names will not be listed.



Priority: profit

Information is a tradable commodity

Internet for innovation and profit

Privatisation of public services

Corporations supersede nation-states

Hyper-capitalism

Inequality within and between societies





**.au Domain Administration Ltd**

**ABN 38 079 009 340**

**PO Box 18315**

**Melbourne VIC 3001**

**info@auda.org.au**

**www.auda.org.au**



The Future Scenarios Project Report 2024 by the .au Domain Administration (auDA) is licensed under CC BY 4.0. The CC license excludes all images and photographs within the report. To view a copy of the license, visit <http://creativecommons.org/licenses/by/4.0>