Ethical 6G: Identifying Elements of Ethical Framework for 6G and Creating Opportunities for India and Australia

Background and Context:

As technology spreads, cybercrimes increase, making cyberspace a modern battleground where cybersecurity equals national security. Yet, no global rules set minimum standards for securing cyberspace, and a few powerful nations dominate international discussions. To secure cyberspace, dependable telecom networks are seen as crucial. Many countries are rolling out 5th Generation (5G) mobile networks, with early moves towards 6th Generation (6G) mobile networks. India and Australia have also aimed to take a lead in the 6G development.

But 6G's development and deployment might bring unforeseen challenges. Hence, it must prioritise safe, secure, and accessible cyberspace. Creating an ethical framework is vital for ensuring safety, security, global trade and investment. Recently, India and Australia boosted cooperation in the digital economy, especially in cyber governance, security, and critical tech. They share a goal of an open, secure, and rules-based cyberspace aligned with international law. Compliance raises the need for global vigilance.

This project, part of the Australia-India Cyber and Critical Technology Partnership (AICCTP), seeks to shape global discussions on cyber and critical tech, strengthen ties between Australian and Indian researchers, businesses, and governments, and enhance cyber resilience and best practices in the Indo-Pacific and beyond.

Vulnerabilities and Risks in 6G (including virtual nations)

Too often when considering risks about anything, a ‘process mentality’ results based on a tick-box, routine, shelf exercise for supposedly good governance, ending with items sitting in a risk register, attended by silo-centric mitigation strategies. Risks are ‘identified’ by internal focus groups. The register is visited occasionally, assuming all risks are linear and behave rationally. Thus, overall, a mandatory ‘process’ is carried out.

A new approach to risk has been needed and has emerged, overcoming failures from the above-described approach, and secondly, by recognising that risk thinking ‘must adjust’ to be relevant in today’s transformative and increasingly disruptive world. Adjustment must capture presently ‘invisible’ risk discovery means, replacing out-dated methods.

In essence, rather than being a static, internal, limited and reactive process, risk must form an unavoidable part of effective decision-making by leaders, that is, producing informed and pre-emptive decisions.

The first premise of new risk thinking is to recognise the real world we now live in, and secondly, to introduce an approach to see the totality of every situation, including recognising sudden change, to place leaders in a position of constantly having the “right information on the right issue, at the right time.” This is the essence of Strategic Risk Policy® as the new frontline approach to consideration of risk and building resilience.

The world today is interconnected, interdependent and interactive like never before. It comprises a meta-grid of systems. We must therefore view the world as whole systems and

operate on the basis that information now resides in networks. The world is subject to rapid deterioration but not at the same time nor same place nor for the same reason.

Some challenges today have never been seen before. Some consequences are unimaginable. Old methods will not necessarily solve many of today's main challenges.

None is more significant to the world right now than that published by ARPI in February 2022 that Information Technology was (and still is) the greatest risk to mankind in the history of the world. Fast forward to today, global leaders and professionals are loudly proclaiming Artificial Intelligence (AI) as capable of destroying civilization - and they say within two years. The late Professor Stephen Hawking foreshadowed this.

AI illustrates the situation that some consequences today are unimaginable.

Risk must today be viewed in Qualitative terms because only Qualitative can see the totality of any situation – systems within systems, and to recognise that we must access meta-grid network information, requiring total leadership paradigm change. Quantitatively, it can be easily proven that 4=2. Qualitatively, context and perspective produce the true explanation of this formula.

To further illustrate, the need to enhance resilience of critical global infrastructure – which AI and 5G/6G are fundamental pillars of, requires corporate as well as government leadership paradigm change, to move from cost-minimisation meaning minimum or unprotected vulnerability, to "Protection Against Foreseeable Vulnerabilities" This is ARPI's new global definition of resilience which was announced and welcomed at the Renewable Resilient Planet (R2) Conference organised by the Electric Infrastructure Security Council (EIS Council) and held at the Imperial College in London on 17-19 April 2023.

EIS Council remit now extends well beyond electricity and is leading into a global-scale Human Continuity Project™, of which ARPI is a Founding Partner. It will cover gas, electricity, water, bushfires, floods, communications, medicines, transport and fuels.

Leadership paradigm change needed is therefore founded upon the identity that "It is no longer the cost of resilience, but the avoided cost (to society) of failure that counts."

Strategic Risk Policy® can deliver a positive, network-centric "New Systems Theory" for informed and pre-emptive decision-making. Strategic Risk Policy® is recognised as Risk 4.0 and speaks to the evolving "Leadership 5.0 in the Age of Digital Transformation."

Following ARPI's warning last year, ARPI accelerated advanced Research and Development on the counterfoil to AI, with the area of science known as Intelligence Augmentation ('IA') – to rebalance the 'Intelligence Equation.' IA not only exposes areas within AI of danger but also manages areas which AI presently does not cover and may never be able to cover, such as situational awareness and sudden change. ARPI has access to R&D models addressing over 30 critical areas – all essential for informed and pre-emptive decision-making. IA must dominate and govern the global 'Intelligence Equation' – as recent military exercises have graphically confirmed.

In summary, Strategic Risk Policy® 'achieves risk purpose' by adjusting risk thinking and introducing new approaches and frames. These are critical to understand 'risk today' and apply it meaningfully in developing an Ethical, Governance Frame for 6G. Without this adjustment

and simply installing a traditional risk management approach, would severely devalue policy attempts by governments, corporates and academia to take risk into meaningful consideration to optimise benefits of technological innovation while ensuring effective protection against identifiable thus foreseeable vulnerabilities. “Risk today is based in Vulnerability and concerned with Consequences” – an ARPI Principle.

Furthermore, ARPI divides the term ‘vulnerability’ to include exposure, which brings a different decision-making mindset to bear.

Strategic Risk Policy® looks at network-informed ‘potentiality’ or ‘possibility’ of strategic risks – which occurs at an earlier point in time than relying on managing ‘existing’ risks and operates at a higher organisational level, in a totally new manner, to ‘protect against’ vulnerability – thus ensuring and assuring supply chains for example, rather than trying to recover through risk mitigation. An existentially more resilient and sustainable approach. 6G must be viewed through Strategic Risk Policy® theory.

Protecting against potential or possible strategic risks results in identifying ‘80:20’ improvement opportunities ‘upfront’ as well as reducing the number and severity of any downstream risks to manage – as well as reducing/preventing left-field crises and wicked problems, missed by focusing only on silo-centric, reactive risk management.

In conclusion, Strategic Risk Policy® is a living process, its richness hence value predicated on network awareness and access. A primary, overriding, global potential strategic risk for 6G is the “consequence of the conjunction of threat and threat actors” – those entities unwilling to be distracted from the race to produce 6G technology – for both corporate and military ends, underpinned by Intellectual Property rights and secrecy, and the currently overlooked need for paradigm change to accept that “Innovation without Governance” can be a global existential risk. 6G is ‘wonderful’ but potentially ‘dangerous.’

A change is needed, for example, by panicked AI laboratories rushing to find risk management mitigation strategies, instead to understand the new risk paradigm presented by Strategic Risk Policy® and embrace ‘informed decision-making’ incorporating ‘Protection Against Foreseeable Vulnerabilities.” This translates to First Principles of 6G policy and applying Strategic Risk Policy® for strategic guidance and protection.

For 6G, this is the change needed in the AI landscape, well recognised now as the most fundamental, existential risk in the world. Would 6G applied to AI accelerate the risk of global destruction? This question is underpinned by various experts around the world holding diametrically opposing views on whether 6G will ever happen (!) and whether there are either no health/safety risks or that energy requirements will produce greatly increased health/safety risks.

Strategic Risk Policy® also reinstates the now too often overlooked part of policy development and implementation called ‘Implementation Analysis.’ ARPI suggests that this omission should be the first cause examined upon failure of new policy or new legislation.

AI is a global ‘Systemic Risk’ and must be viewed in that context and perspective, and managed in a formal, global, collaborative environment, else it will quickly become a Wicked Problem. Consideration of risk and regulation of 6G must be similarly considered as inextricably interconnected and interdependent on AI. Regulation of 6G is a continuum.

To assist an understanding of the difference of 'Vulnerability' – 'Risk' – Live Issue' as depicted in ARPI's New Risk Landscape – the only known such 'executive dashboard' - which tracks whole-of-life risk, measures appetite and tolerance, as well as providing a forensic capacity for regression analysis, learning and auditing, the following summary is provided:

Vulnerability:

Defined: Today risk is based on vulnerability and concerned with consequences. Vulnerability as in the ordinary dictionary meaning, should include 'Exposure' so the reader will already appreciate that these two terms create new thinking, requiring a different mindset to identify and consider each.

With Vulnerability or Exposure, there is no existing risk, hence a probability of occurring of zero but rather, there is a Potentiality or Possibility of a strategic risk arising in the future – based on considered information and judgement.

Existing Risk:

Defined: ARPI has redefined 'risk' under Strategic Risk Policy® for today's world, which definition aligns with the concept of Vulnerability:

1. Impact of decisions or non-decisions;
2. Implications of decisions or non-decisions on networks; and
3. Implementation analysis of policy development and policy introduction.

Live Issue:

Defined: Live issue is when a risk materialises or happens, Probability reaches 100% or '1', it requires a range of reactions including 'crisis management' through to management of a 'wicked problem'.

The following table outlines high-level Vulnerabilities, Risks and Issues facing 6G - as at this point in time, and in the above context and perspective.

Vulnerabilities	Strategic and Systemic Risks	Issues to Wicked Problems
Unknown or undisclosed 'Information Technology' impacts and implications x threats x threat actors	Inadequate global state of awareness, commitment, prevention, protection against and responsiveness to for example, BlackSky™ events	The future of AI and its immediate implications – vulnerabilities, risks and live issues facing the development and introduction of 6G.
Unawareness by society in general to consider risk at an earlier juncture and thus seek to protect against vulnerabilities, rather than wait and manage risks.	Unawareness that the distinction between vulnerability and risk is the greatest public policy challenge in the world.	Corporate and military pursuits of defence and domination underway, to develop and deploy 6G as the adjunct to AI – with or without awareness and governance

Emerging acceptance of or indifference to existential risks of AI and potentially accelerated impact of 6G	World is subject to the risk of rapid deterioration – absence of collective leadership and planning	Previous attempts to create an underground, unregulated global financial sector creating virtual nations.
Opposing expert views on health, safety and energy science concerning 6G	Unawareness that AI hence 6G are global Systemic Risks requiring collaborative and formal management	IP – patents, Trade Secrets, commercial and security products vis a vis to situations such as global 'hotspots.'
Unwillingness of society (on scale) – governments, organisations, professionals - to express comment about 6G for fear of criticism of ignorance	Failure to realise that risk today resides in vulnerability and is concerned with consequences	Present attention to the need to regulate AI must go back to First Principles concerning policy implications especially areas which AI may never address.
Unknown state of actual global R&D on 6G	Risk management equation of likelihood x consequence is no longer safe to apply to AI or 6G - consequence must govern the equation	Restoration of an Intelligence Equilibrium between Artificial Intelligence (AI) and (Real) Intelligence Augmentation (IA)
Global assessment using Strategic Risk Policy® architecture is lacking to consider various impacts including both Vulnerability and Risk Domino and Convergence scenarios.	Global commitment is required to the planned global scale Human Continuity Project™ to enhance resilience of critical infrastructure.	Information Technology must be viewed as 'whole systems' which is not the case at the moment – this must trigger redesigns
Differential technology infrastructure across regions of the world	Weaponised political diversion e.g. failure of the developed world to meet the urgent resilience needs of the Global South	Regulation of AI (thus affecting the safe and unsafe application of 6G) is presently and likely to continue onan individual national basis.
Exponential technology growth with limited visibility of the future especially in the context of quantum computing, machine intelligence and robotization	Failure to address AI concerns means 6G is a potential global Systemic Risk e.g. quantum hacking	

The following three tables identify specific technical, consumer and regulatory vulnerabilities, risks and issues:

Technical/Infrastructural			
Vulnerabilities	**Risks**	**Live Issues**	**Recommendations**
Terahertz (THz) Frequency Interaction	Potential Security Concerns in proximal communication and edge communication	Interference with IoT communication and associated network intrusions	1. Availability of incredibly wide bandwidths
Lack of adequate rural telecom infrastructure will pose a complex challenge for 6G to be inclusive and scalable.	Limited Access to Services	Digital divide and poor connectivity in rural and semi-urban areas	1. Deploy an optimal mix of non-terrestrial and terrestrial modes 2. Reliance on Low-Earth Orbit (LEO) satellites for inclusive access 3. Fibre-Broadband Connectivity 4. Achieving high data rates
Antenna Deployment Challenges; Sensitivity to Obstacles (Millimetre & Terahertz).	Limited Network Coverage	Interference, and poor connectivity for mission critical applications	
Limited Fibre Optic Connectivity.	Insufficient Infrastructure for Efficient 6G Deployment	Lack of guaranteed quality of service and quality of experience	
Capacity Challenges in Backhaul.	Inadequate Support for Heavy Traffic	Poor quality of real time super high speed communication resulting in loss of safety and security	
Use of molecular communication for human-machine communication	Inadequate testing and lack of standards	Threats to human safety	
Interconnectedness of IoT Devices	Escalation of Security Threat Vectors	Hacking of IoT devices	1. Security by Design
Vulnerability of Current Cryptographic Mechanisms	Compromised Authentication and Access Control	Crypto hacking using distributed network resources	1. Flexible and self-healing network 2. Global cyber-

Attacks on AI Systems, Especially ML Systems	Risks Include Poisoning, Data Injection, Manipulation, etc.	Spoofing using Big Data	security assurance and certification
Ransomware Attacks on Critical Infrastructures	Compromised National Security	Attacks on critical information infrastructure threatening closures and hijacking of national infrastructure	
Data-intensive technologies	Requiring a massive power supply	Increasing carbon emissions and pollution levels	1. The need for research to develop a sustainable future around 6G.
Adequate security testing	Minimum user authentication	Hijacking of devices and of IoTs, and Internet of Everything	1. Redesign IoT

Consumer Protection			
Vulnerabilities	**Risks**	**Live Issues**	**Recommendations**
Increase in Data Generation and Uses	High Energy Consumption in Data Storage Centres	Imbalance in supply of power to other sectors including healthcare, transportation	1. Reassessment of telecom operations wet environmental targets 2. Reduce dependency on batteries
Personal Data Theft/Loss (Identity, Location, Reactions, Emotions)	Potential Privacy Violations	Identity attacks, privacy and reputational harms	1. Confidential Computing 2. Use of privacy preserving technologies
Security and integrity of data when employing Intelligent Edges (IE) powered by Artificial Intelligence (AI) or	Security breaches, including data tampering, evasion, and privacy violations.	Inadequate software vulnerability management, security patching and incidence management	1. Develop robust security protocols and encryption mechanisms

Machine Learning (ML) algorithms at the network edge.			tailored to the unique requirements of IE-enabled 6G networks 2. Federated Learning Security
Distributed computation, communication, caching, and control resources.	Susceptible to various risks, particularly concerning data security at the network's edge.	Security attacks nearer to users and devices	1. Robust security measures at the network edge.
Failure to comply with the Consumer Bill of Rights 2023 – as updated by ARPI.	Inadequate transition to enhanced sustainability	Failure to provide choice of technology to consumers, technology obsolescence	1. Allowing consumers the right to choose repairers

Regulatory			
Vulnerabilities	**Risks**	**Live Issues**	**Recommendations**
Lack of Harmonisation with other Global Standards	Potential Fragmentation of Global Standards	Difference of stands between IEEE, 3GPP, ITU	1. Adopting global collaborative and harmonised standards 2. Policy coherence and regulatory clarity
Tension Between Telecom and Software Firms	Incompatibility and Interoperability	Difference in approach by the Internet firms, especially Over The Top firms and Telcos	
Spectrum Scarcity	Limited Network Capacity	Competing spectrum usage amongst mobile operators, defence, and utility firms	1. Spectrum reuse and sharing 2. Reassessment of spectrum Sharing practices 3. Alternate spectrum signals
Congestion and Competition in Spectrum Allocation	Frequency Interference and Inefficiencies	Inadequate harmonization across geographies especially on spectrum bands for commercial mobile	

		communication services	
High Cost of Spectrum	Financial Sustainability of Telecom Operators	Huge sunk cost for operators and hence lesser capital for providing 6G services	
Network Slicing	Net Neutrality	Strong alliances between telcos and content providers	1. Ensuring net neutrality while balancing it with the business models through effective regulations.
Sufficiently uniform effective global regulation	Recognition that an ISO Standard is a Guideline only and thresh-hold regulation	Differences in capacity of regulators across countries	1. IP ownership require an holistic approach to regulation