The Marconi Society

EXECUTIVE INSTITUTES FORUM

Driving cross-sector alignment on the most pressing technology challenges in Advanced Wireless, Internet Resilience, and AI

ADVANCED WIRELESS INSTITUTE

AI INSTITUTE

INTERNET RESILIENCE INSTITUTE

April 28, 2026 | marconisociety.org

Marconi Society Executive Institutes Forum

April 28, 2026

Executive Summary

The 2026 Marconi Society Executive Institutes Forum brought together senior leaders from industry, academia, policy, and nonprofit sectors across its three Institutes (**Advanced Wireless**, **Internet Resilience**, and **Artificial Intelligence**) to evaluate the most pressing technology challenges warranting collective action ahead of its flagship convening November 4-6, 2026, in San Francisco.

The Forum signified the importance for directional alignment on three core topics: **Internet Resilience**, **Trust and Safety**, and **Infrastructure and Energy Transformation**. The outcomes identified herein reflect a broader recognition that the most consequential technology challenges of this era spanning AI, connectivity, and wireless innovation no longer exist in isolation, and require cross-sector collaboration to address effectively and reliably.

Session I: Internet Resilience

Society's dependence on digital infrastructure has expanded dramatically, but preparedness has not kept pace. Participants framed this not as a niche engineering concern, but as a systemic risk with direct implications for public safety, economic continuity, and equitable access to essential services.

A critical and underappreciated mismatch surfaced: while network capacity appears abundant, digital systems continuously consume whatever bandwidth is available, leaving institutions from enterprises to public agencies far more vulnerable to prolonged outages than commonly assumed. Modern workflows are optimized for convenience, scale, and always-on connectivity – not for austere network conditions.

The 5% Bandwidth Scenario

To translate the abstract risk into operational terms, participants were asked to consider, *what would your organization do if it had access to only 5% of its normal bandwidth for two weeks* – a deliberate shift from thinking about brief outages to modeling severe, sustained degradation.

The exercise was notably effective and generated a wide range of responses that revealed several critical vulnerabilities:

- **Cloud dependency exposure**: Many organizations have offloaded critical functions to cloud platforms and external repositories without maintaining viable offline or hybrid alternatives.
- **Complexity as a liability**: Modern digital workflows have become so layered and interdependent that meaningful resilience requires not only backup systems, but also simplification of core processes; prioritization of the most important systems would be needed.
- **Testing gaps**: Multiple participants acknowledged that failover systems exist on paper but are rarely tested under genuinely constrained conditions, raising serious questions about whether they would function when needed.
- **Uneven resilience across sectors**: Large infrastructure organizations with extensive fiber capacity and redundant failover systems reported lower perceived vulnerability, underscoring that

resilience preparedness varies significantly by organizational scale and technical maturity – leaving smaller institutions, public agencies, and critical service providers disproportionately exposed.

Stakeholder-Specific Mitigation Responsibilities
One of the session's most actionable contributions was mapping resilience responsibilities across distinct stakeholder communities. Rather than treating resilience as a monolithic technical challenge, participants organized response strategies by actor type:

- **Enterprises & Content Delivery Networks**: Deploy backup systems, diversify suppliers, implement hybrid cloud/on-premises architectures, enforce graceful degradation strategies, and conduct rigorous, repeated testing of failover systems under austere network conditions.
- **Telecommunications & Infrastructure Operators**: Strengthen critical interconnection points and subsea cable infrastructure; establish emergency access protocols in advance of crisis conditions.
- **Regulators & Policymakers**: Ensure resilience governance is driven by technical evidence rather than political considerations; engage proactively with the policy dimensions of network disruption.
- **Standards Bodies & Browser/Platform Stakeholders**: Address the absence of a widely adopted standard for critical information delivery under low-bandwidth conditions; advance lightweight, text-first delivery architectures for crisis scenarios.

Session II: Trust and Safety

All too often AI governance is framed either as a technical compliance exercise or as a debate about future existential risk, missing the people already affected by current systems, especially those with little influence over how systems are designed or deployed. In this framing, trust and safety work has centered the needs and assumptions of already well-served groups, while people outside that profile are often treated as secondary considerations.

This session focused on **AI trust through a human-centered design lens**, challenging the default assumption of who counts as the "human" in technology design. Participants were asked to consider *how do we move from designing for humans to designing with humans, embedding lived experience and participatory design into the technologies that shape daily life?* Trust cannot be built only with system operators or enterprise customers; it must also include those whose information, opportunities, or outcomes are shaped by the systems, often without their active participation.

Participants repeatedly returned to the breadth of AI's impact. Virtually everyone is directly or indirectly affected by AI systems, whether as users, data subjects, employees, or members of communities shaped by AI-enabled decisions. A particularly vivid example involved an online staffing marketplace breach in which highly sensitive applicant materials were exposed, including interview recordings, background-check information, and other personal data. The implications discussed went beyond a standard data leak: participants highlighted the risks created when voice samples, tax information, and identity data are combined into high-fidelity profiles that can later be exploited, risks that were taken on by particularly vulnerable people–those seeking employment. This case illustrates how trust is not an abstract principle; it is closely tied to data stewardship, security design, and the downstream effects of failure.

Human and Institutional Dimensions of Trust
Companies often invest heavily in training employees to recognize email spoofing and other traditional cybersecurity threats, while providing far less guidance on safe and appropriate AI tool usage. This gap becomes more serious when personal and professional uses of AI systems blur together, such as when employees use the same tools or environments for work research and sensitive personal questions. Many users do not understand how data is stored, separated, or reused across systems, making it difficult for them to make informed decisions about trust. This suggests that AI governance is not only a policy issue at the executive or regulatory level, but also an operational issue involving employee behavior, literacy, and everyday workflow design.

Policy and Governance Dimensions
Participants also explored the difficulty of governing AI because of its uneven and unpredictable capabilities. One concept that resonated was the "jagged frontier" problem: AI can perform at an expert level in some domains while failing in surprisingly basic ways in others. This unpredictability complicates oversight, because the boundaries of competence and failure are not always visible in advance. The group discussed whether governance should rely more on proactive testing, stronger certification mechanisms, and incentives for organizations to identify failure modes before public harm occurs. While some companies already have reputational incentives to reduce bias and hallucinations, the conversation suggested that market incentives alone are unlikely to be enough, especially when the effects of failure are distributed across people with little power to demand accountability.

The session closed with a practical challenge to participants: review their own organizations' AI governance policies and ask two questions. First, do those policies genuinely represent the interests of all the populations affected by the organization's AI-related activities? Second, if someone is harmed by an AI system connected to the organization, is there a meaningful path for redress, or only informal public complaint? This closing reframed AI governance as an institutional responsibility rather than merely a technical or theoretical issue, pushing participants to evaluate whether their policies are inclusive in design and accountable in practice.

Session III: Infrastructure and Energy Transformation

The rapid expansion of digital infrastructure driven by AI workloads, advanced wireless deployment, and growing cloud demand has placed unprecedented pressure on energy systems and physical infrastructure. This session surfaced infrastructure sustainability and energy transformation as a global priority with direct implications for resilience, economic competitiveness, and long-term technological viability.

Energy Demand as a Strategic Constraint
Data center expansion, AI model training, and the proliferation of connected devices are driving energy consumption at a pace that existing grid infrastructure and energy policy were not designed to accommodate. Participants discussed the limits of continuing with current energy generation models and pointed to nuclear, fusion, and expanded solar as the main categories of alternatives that could support future AI growth. Across these ideas, the shared view was that sustaining AI growth will require both new energy sources and more serious planning around how generation capacity is developed and deployed.

Infrastructure Resilience and Physical Vulnerabilities

Digital resilience is only as strong as the physical systems that underpin it. Vulnerabilities in power grids, subsea cables, and national interconnection points represent compounding risks that are often addressed in isolation rather than as an integrated system. The consensus was clear: physical and digital infrastructure must be viewed as a unified, interdependent ecosystem.

Security and resilience should be considered just as critically as efficiency. Highly centralized infrastructure can create attractive single points of failure, particularly when energy generation and computing resources are concentrated together. Participants noted a more distributed model may potentially be better for resilience, even if it introduces tradeoffs in cost or efficiency.

Efficiency gains need to happen across the full AI stack, not only at the model level. Hardware, packaging, system design, software, and operational practices were all discussed as areas where incremental improvements could produce meaningful aggregate impact. Sustainable AI growth will depend not just on building more power capacity, but also on creating stronger incentives for efficiency, optimization, and resilience throughout the ecosystem.

The Role of Policy and Investment
The infrastructure and energy transformation agenda requires alignment across the private sector, government, and regulatory bodies. The pace of private investment in data centers and wireless infrastructure is outpacing public policy frameworks for energy planning, environmental impact, and grid modernization. Without proactive policy engagement, the sector risks creating infrastructure bottlenecks that could constrain technological progress.

Participants further explored the pace of AI expansion and whether the current rate of investment is sustainable. Deployment appears to be moving faster than historical computing efficiency trends, while usage remains supported by subsidized economics and large flows of capital. One concept the group suggested was “tokens per watt” as a more practical way to think about AI efficiency. Rather than measuring progress only through larger systems and higher throughput, participants reiterated the importance of understanding how much useful output can be produced per unit of energy consumed.

Ultimately, who should bear the cost of the supporting infrastructure? Participants underscored the need for AI companies and data center operators to contribute meaningfully to the costs of generation and grid upgrades associated with their growth. Grid modernization will likely require stronger public-private coordination, and future projects will depend in part on whether local communities believe the benefits and burdens are being shared fairly.

Conclusion

The 2026 Marconi Society Executive Institutes Forum delivered a clear strategic signal: the most consequential technology challenges of this moment are not confined to disciplinary or institutional boundaries. Critical topics such as Internet resilience, trust and safety, and infrastructure and energy transformation are deeply interconnected, and addressing them effectively requires the kind of cross-sector, expert convening that is the Marconi Society’s defining strength. The Marconi Awards Gala & Institute Forums this November 4-6, 2026, represents a high-value opportunity to build upon the Forum’s momentum by driving actionable solutions, building coalitions, and securing commitments among leading academics, executives, and technologists serving the broader technology ecosystem.

2026 Executive Institutes Forum Participants

- **Fay Arjomandi**–Founder & CEO, mimik
- **Tina Austin**–Professor, UCLA
- **Victor Bahl**–Technical Fellow - Research, Microsoft
- **John Cioffi**–CEO, ASSIA & Marconi Society Board Director
- **Andrew Coward**–Principal Consultant, Kirin Solutions
- **Paul Dawes**–CEO, More.AI
- **Mischa Dohler**–VP Emerging Technologies, Ericsson
- **Mo Elbashir**–Self
- **Taher Elgamal**–CTO, Salesforce & Marconi Society Board Director
- **Mingxi Fan**–SGM, Wireless Communication Technology and System Design, MediaTek
- **Gillian R. Hayes***–Vice Provost, UC Irvine
- **John Janowiak**–President and CEO, Marconi Society
- **Anton Monk**–SVP Strategy, Cohere Technologies
- **Michael Munsey***–VP Semiconductor Industry, Siemens
- **Ramakant Pandrangi**–SVP, Architecture and Engineering, Verisign
- **Anand Raghavan**–Chief Product Officer, Snorkel AI
- **Vinay Ravuri**–CEO & Founder, EdgeQ
- **Puneet Sharma**–Fellow, VP, Director of NDSL, HPE Labs
- **Neel Sundaresan**–GM of Automation and AI, IBM Software, IBM
- **Mimi Tam**, Author & Adjunct Professor Computer Science, Boston College
- **Shanker Trivedi**, Self
- **Caleb Queern***–Managing Director, Cyber, KPMG & Co-Founder, Texas Cyber Alliance
- **Andreas Zoll**–Chief Strategy Officer, Maverick Power
- **Hao Zou**–CEO, Abundy & Marconi Society Board Director

**The Marconi Society extends its gratitude to Caleb Queern, Gillian R. Hayes, and Michael Munsey for their expertise and invaluable contributions as session moderators.*

Marconi Society Contacts

John R. Janowiak
President and CEO
john@marconisociety.org

Flora Tromelin
VP for International Engagement
ftromelin@marconisociety.org

Marina Pappas
Institute Director
mpappas@marconisociety.org

Barry Sullivan
Institute Director
bsullivan@marconisociety.org

Elizabeth Hibbler
Institute Director
ehibbler@marconisociety.org

Yeimidy Lagunas
Director, Communications and Membership
ylagunas@marconisociety.org

Jaymee Bohannon
Executive Relations
jbohannon@marconisociety.org