

The State of IoT, 2026 and Beyond

Michela Menting, Vice President, ABI Research
Syed 'Z' Hosain, Co-Founder, Chief Evangelist, Aeris

ABIresearch
THE TECH INTELLIGENCE EXPERTS™

aeris

CONTENTS

Introduction 1

2025: A Brief Retrospective..... 2

2026: Structuring for the Future..... 5

2027–2028: The Autonomy Inflection Point 7

2029 and Beyond: IoT for the Benefit of All 10

Conclusion and Call to Action 13

INTRODUCTION

The Internet of Things (IoT) is the next global technological revolution shaping our future. What began as simple device connectivity more than 3 decades ago has exploded into a vast, intelligent ecosystem reshaping industries, infrastructure, and everyday life.

Billions of devices now sense, analyze, and act in real time, and their numbers are accelerating at an almost unbelievable pace. Powered by breakthroughs in Artificial Intelligence (AI) and edge computing, and using next-generation connectivity such as 5G, Low-Power Wide Area (LPWA), and satellite networks, as well as expanded use of short-range wireless, IoT solutions are evolving from passive data collectors into autonomous decision makers at the edge.

This extraordinary expansion carries equally extraordinary risk. Every new connected device expands the attack surface. As IoT deployments scale into tens of billions of devices, security must become foundational.

Governments worldwide are responding with sweeping regulations and stricter standards, while enterprises face mounting pressure to design, deploy, and maintain secure-by-design solutions in a rapidly shifting landscape.

This whitepaper examines the key IoT advancements in 2025, and what lies ahead in 2026 and beyond, in a future once imagined only in science fiction. IoT is now connecting intelligence to a physical world where machines collect data and act in real time. This future depends on trust, where security, identity, resilience, and responsible governance must be built in from the start. In time, IoT will transform how humanity moves, heals, produces, and protects the planet. By understanding where the ecosystem is headed, organizations can move from reactive compliance to strategic leadership and harness IoT's immense potential.

2025: A BRIEF RETROSPECTIVE

The year 2025 was when IoT connectivity matured into a highly orchestrated, multi-layered ecosystem, and started deepening security integrations. Enterprises no longer asked "Which network?" or "Why security?" Rather, they started to ask "Which mix of networks, optimized for which IoT workload, and how secure?"

The Expanding 5G IoT Spectrum

The 5G family of cellular standards continued to diversify into clearly defined device classes. At the low-power end, Narrowband IoT (NB-IoT) and LPWAN remain essential for static and widely dispersed sensors, ideal for environmental monitoring, smart agriculture, and low-data telemetry. At the other extreme, full 5G New Radio (NR) supports bandwidth-intensive, low-latency applications such as industrial automation and connected mobility.

But the real momentum in 2025 centered on the middle tier. The 3rd Generation Partnership Project's (3GPP) Release 18 enabled commercialization of 5G Reduced Capability (RedCap), also known as NR-Light, bridging the gap between NB-IoT and higher Long Term Evolution (LTE) categories. RedCap delivers lower complexity, reduced power consumption, and cost efficiency, while maintaining meaningful throughput. In 2025, RedCap transitioned from specification to deployable device standards.

Building on this, 3GPP Release 19 further optimized RedCap for practical large-scale deployments and introduced refinements that made it increasingly attractive for smart metering, asset tracking, wearables, and industrial sensors.

Ambient IoT: Power Without Batteries

A forward-looking development emerging through Release 19 is Ambient IoT (A-IoT), designed for ultra-low-power, energy-harvesting, or even battery-less devices.

A-IoT introduces new authentication, integrity protection, and anti-replay mechanisms tailored to extremely constrained devices. This is significant: security is being embedded not only in high-performance devices, but also in passive tags and sensors that may never require manual servicing. It marks a shift to scalable, secure identification of billions of lightweight endpoints.

Satellite Integration Goes Mainstream

Perhaps one of the most transformative developments of 2025 was the introduction of Non-Terrestrial Network (NTN) support within the 5G standards.

Satellite connectivity is no longer a niche overlay and is becoming part of the unified 5G architecture. Devices ranging from smartphones to vehicles to remote industrial sensors can now leverage standardized satellite connectivity support within the 3GPP ecosystem.

Release 19 enhancements to NR-NTN refined coexistence between terrestrial and satellite links, with RedCap positioned as a practical enabler for remote industrial IoT deployments. For transportation logistics, energy, maritime, and rural infrastructure, ubiquitous coverage is shifting from aspiration to architectural assumption.

eSIM Evolution: Connectivity Without Friction

Aeris single SKU eSIM simplifies device portfolio and multi-network access without hardware changes, with effective eSIM orchestration enabling lower total cost of ownership.

Beyond radio evolution, device lifecycle management also advanced.

Certification efforts for GSMA SGP.32 accelerated in 2025, enabling standardized remote Subscriber Identity Module (SIM) provisioning for IoT embedded Universal Integrated Circuit Cards (eUICCs). Unlike earlier consumer-focused specifications, SGP.32 is purpose-built for IoT, particularly for devices without user interfaces.

This development simplifies manufacturing and global deployments by allowing a single hardware Stock Keeping Unit (SKU) to be produced and provisioned dynamically for different operators or regions. It also strengthens alignment between IoT infrastructure and mainstream mobile ecosystems, reducing fragmentation and operational complexity.

From RedCap's emergence as the "Goldilocks" IoT category in 5G to satellite-native integration, to battery-less A-IoT, and seamless embedded SIM (eSIM) orchestration, wireless technologies expanded in both capability and architectural coherence.

The year 2025 also saw a deeper relationship emerge with security. As evolving wireless standards determined how IoT would scale, regulation defined what secure IoT must achieve.

A Transitional Year for Policy & Regulation

In 2025, IoT security shifted from voluntary best practices to enforceable regulatory requirements, with governments mandating device-level protections and laying out rules penalizing noncompliance around the world.

Regulatory confidence through the BOM management pipeline in Aeris IoT Watchtower™, a security platform for cellular IoT, and demand for a unified experience with one control plane across global CMPs, eliminating dependence on third-party overlays, is driving competitive advantage.

REGULATIONS

(GDPR, CRA, RED, NIS2, UK PSTI, US 2020 Cybersecurity Improvement Act)



The European Union (EU) led the regulating shift as new Radio Equipment Directive (RED) provisions and the Cyber Resilience Act (CRA) established the first binding cybersecurity baseline for connected products, influencing global manufacturers.

MANDATES

(NIST CSF, NIST SP 800-213, NIST IR 8259 Series, US FDA Cybersecurity in Medical Devices)



In the United States, the National Institute of Standards and Technology (NIST) frameworks and sector specific rules evolved into de facto mandates emphasizing secure by design processes, Software Bill of Materials (SBOM), and lifecycle accountability.

SCHEMES

(U.S. Cyber Trust mark, Japan JC-STAR, Singapore & Malaysia Draft consumer IoT cybersecurity frameworks)



At the same time, security labeling schemes such as the U.S. Cyber Trust Mark, Japan's JC STAR, and emerging programs in Southeast Asia signaled a global move toward standardized IoT security expectations.

The IoT industry entered 2026 with a new reality: compliance is no longer a simple checkbox for products and is an architectural constraint. Organizations that internalized this shift began transforming security into a competitive advantage. Those that did not now face a rapidly closing deadline to adapt.

Zero Trust & Identity Access Management Take Center Stage

Aeris IoT Watchtower reduces mean time to detection for anomalous device behavior, enabling OTA patching synchronized with CSP connectivity management, and real-time telemetry.

As standards matured and regulations solidified into enforceable baselines, Zero Trust and Identity and Access Management (IAM) moved from abstract concepts to operational necessities, driving requirements for strong cryptographic device identities, authenticated onboarding, integrity verification, least-privilege access, and continuous behavioral monitoring.

This transition leveraged adaptive, context-aware enforcement, supported by AI-driven behavioral analytics, focusing on identifying anomalies to respond rapidly at scale.

At the same time, forward-looking manufacturers began preparing for a post-quantum future, recognizing that long-lived IoT devices require cryptographic agility, robust update mechanisms, and early planning to ensure resilience against emerging quantum-era threats.

2026: STRUCTURING FOR THE FUTURE

If 2025 was about preparation, 2026 will be about execution. This is the year when IoT security shifts permanently from "feature" to "foundational requirement" and regulatory theory meets operational reality.

Standardization & Certification as Growth Multipliers

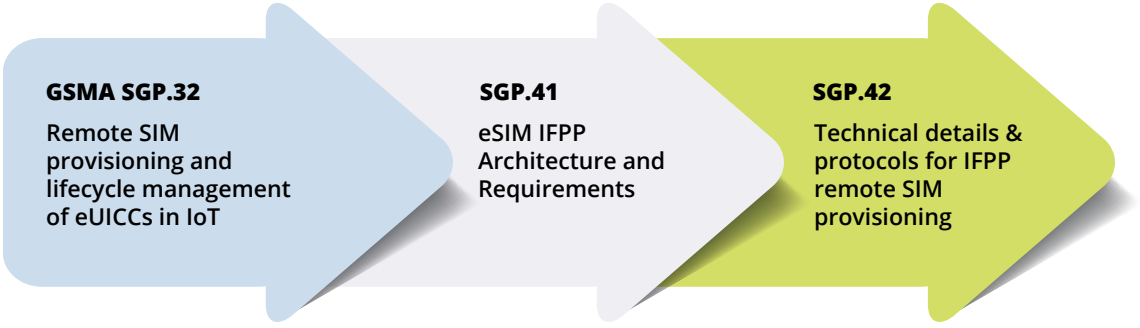
Aeris' SM-DP+ as-a-Service and IAM-as-a-Service serve as reference models for eSIM orchestration.

In industrial IoT, massive Machine-Type Communications (mMTC) over 5G will expand further into grid modernization and smart city infrastructure. Second-generation 5G RedCap chipsets, building on 3GPP Release 19 enhancements, are expected to reduce cost and complexity, making mid-tier 5G IoT commercially scalable.

At the same time, NTN satellite integrations will move from pilot programs into structured early deployments, particularly in remote utilities, logistics, and asset monitoring. As connectivity diversifies, unified security models, with consistent identity, remote lifecycle management, and cross-network policy enforcement, will become essential to prevent fragmentation.

In the consumer market, the Connectivity Standards Alliance's (CSA) Matter ecosystem will continue gaining acceptance. Its device attestation certificates, strong authenticated onboarding, encrypted communications, and structured update models indirectly reinforce secure-by-design architectures across consumer IoT portfolios.

eSIM orchestration will start scaling through GSMA SGP specifications, driving commercial deployments and influencing manufacturing pipelines, and eventually pushing vendors to start planning how to design hybrid fleets that can accommodate evolving specifications across device lifecycles.



Commercial deployments of GSMA SGP.32 are expected to scale significantly in 2026, enabling remote SIM provisioning purpose-built for IoT. Standardization efforts around in-factory provisioning, guided by GSMA SGP.41 requirements, will influence manufacturing pipelines. Meanwhile, strategic alignment planning for SGP.42 will begin in earnest, as vendors design hybrid fleets that can accommodate evolving specifications across device lifecycles.

Regulatory Deadlines Drive Market Forces

By the end of 2026, security will no longer be a competitive differentiator in IoT; it will be a baseline condition for market access.

The Cyber Resilience Act (CRA) becomes applicable to many products with digital elements in the European Union (EU) market. The recently updated Radio Equipment Directive (RED) requirements must also now integrate seamlessly with software, cloud, and lifecycle security requirements under the CRA. Simultaneously, enforcement of the Network and Information Systems 2 Directive (NIS2) will accelerate as remaining Member States complete their legal requirements.

Energy grids, transport networks, telco infrastructure, and cloud operators will face heightened expectations for supply chain security, pulling IoT vendors directly into critical infrastructure compliance.

As a result, IoT procurement teams will increasingly require structured documentation. Quality standards for Software Bill of Material (SBOM) generation, attestation, and update synchronization are likely to tighten. Automated SBOM validation and vulnerability correlation, increasingly assisted by Artificial Intelligence (AI), will become common in both compliance and defensive workflows.

The concept of a Cryptographic Bill of Materials (CBOM) will gain traction. As organizations inventory cryptographic assets in preparation for quantum-safe transitions, CBOMs will support transparency into algorithm usage, key lengths, certificate chains, and hardware security dependencies.

Additional documentation efforts, such as Artificial Intelligence BOM (AIBOM) and Hardware BOM (HBOM), will also begin appearing, although there is still much work remaining for these to be widely understood and used.

Default Zero Trust Suffused with AI

Aeris IoT Watchtower will expand its scope to include application performance monitoring and advanced OTA policy enforcement.

Buoyed by more clearly-defined structure, 2026 will mark the acceleration of Zero Trust as the implicit IoT security model. Device fleets will be managed not only for connectivity, but for cryptographic integrity and behavioral compliance.

Device identity will increasingly rely on hardware roots of trust, secure boot, attestation, and protected credential storage. Continuous authentication and least-privilege enforcement will become embedded assumptions, rather than simple upgrades. AI will be leveraged extensively to enable greater automation and real-time management.

Edge AI, in particular, will further distribute trust enforcement, enabling anomaly detection and policy decisions closer to the device layer, particularly in RedCap and remote NTN deployments.

The first concrete steps toward post-quantum readiness will be made as IoT vendors begin piloting hybrid cryptographic implementations that combine classical and post-quantum schemes. The transition will be cautious. New Post-Quantum Cryptography (PQC) standards are not yet battle-tested for IoT on a global scale.

2027–2028: THE AUTONOMY INFLECTION POINT

By 2027–2028, IoT will stop being a collection of connected devices and start becoming a secure, distributed autonomous system. This period is less about adding more endpoints and more about redefining what those endpoints are allowed to do, and under what conditions they are trusted to act independently.

Where integration with a single carrier can take years, Aeris delivers in months. Recent partnerships show that its unprecedented approach solves backend security challenges while enabling simultaneous connectivity across 30 carriers. This positions Aeris as a critical enabler of an interoperable AI-driven IoT ecosystem, where latency, bandwidth, and reliability are non-negotiable.

Autonomous IoT systems powered by AI will demand a network capable of delivering near-instant responsiveness, constant connectivity reliability, and seamless interoperability across multiple carriers. In this emerging landscape, the infrastructure acts as the nervous system with AI as the brain, from lightweight small models running on devices, to latency-critical models at the network edge, and deep-thinking large language models in the cloud.

Compliance With Security Regulations

Compliance windows will close permanently as the CRA and other instruments apply fully. Transition periods will end without any further grace-period assumptions and the first visible enforcement actions are likely to emerge.

More importantly, procurement ecosystems will internalize regulatory and policy alignment as a baseline filter for tenders, especially in critical infrastructure and industrial deployments.

Connectivity Choice Is Expected

By 2028, multi-provider connectivity will not be a differentiator; it will be expected. The single-SKU eSIM model will be deeply embedded in manufacturing strategies, with production lines assuming post-deployment profile flexibility by default.

Solutions based on GSMA SGP.32 will have matured through real-world scaling. Operational lessons from early deployments will shape the refinement of orchestration models, ownership structures, and lifecycle accountability.

Follow-on GSMA SGP.42 specifications will target ultra-low-power and form factor-constrained devices that remain underserved by SGP.32 activation flows. If finalized on schedule, SGP.42 could trigger an inflection in battery-constrained and 5G-Advanced IoT categories, including RedCap and early NTN deployments.

RedCap Becomes the Default Transport

By 2028, 5G RedCap, refined through 3GPP Release 19 and beyond, will solidify as the default migration path for many LTE CAT-1 and CAT-4 use cases. Smart grids, industrial telemetry, Point of Sale (POS) systems, surveillance, and select automotive applications will increasingly converge on RedCap.

However, its success will hinge on sufficient 5G standalone coverage in industrial-heavy regions. Without infrastructure density, migration slows. With it, RedCap becomes the connective tissue of mid-tier IoT.

A-IoT, meanwhile, will begin appearing in early commercial chipsets. Volumes will remain niche (e.g., retail tags, smart building sensors, logistics markers), but the idea of disposable, energy-harvesting endpoints will no longer be experimental.

The long-term implication is profound: when sensors become nearly free and maintenance-free, instrumentation density explodes.

The Autonomy Threshold

The most significant shift will not be regulatory or radio-based however; it will be behavioral.

With Zero Trust architectures maturing, IAM normalized, SBOM and CBOM transparency improving, and post-quantum transition planning underway, IoT ecosystems will begin trusting devices not just to report, but to decide and act using Agentic AI mechanisms.

Autonomous fleets, coordinated industrial robots, and AI-assisted medical devices will move beyond controlled pilot environments into operational normalcy.

Urban mobility will include robotaxis operating alongside public transit. Warehouses, airports, factories, and retail spaces will rely on Automated Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs) as standard infrastructure. These systems will increasingly operate with minimal human oversight, making real-time decisions based on sensor fusion and local AI inference.

Edge Intelligence Everywhere

With systemic AI integration, edge computing will be embedded at every tier.

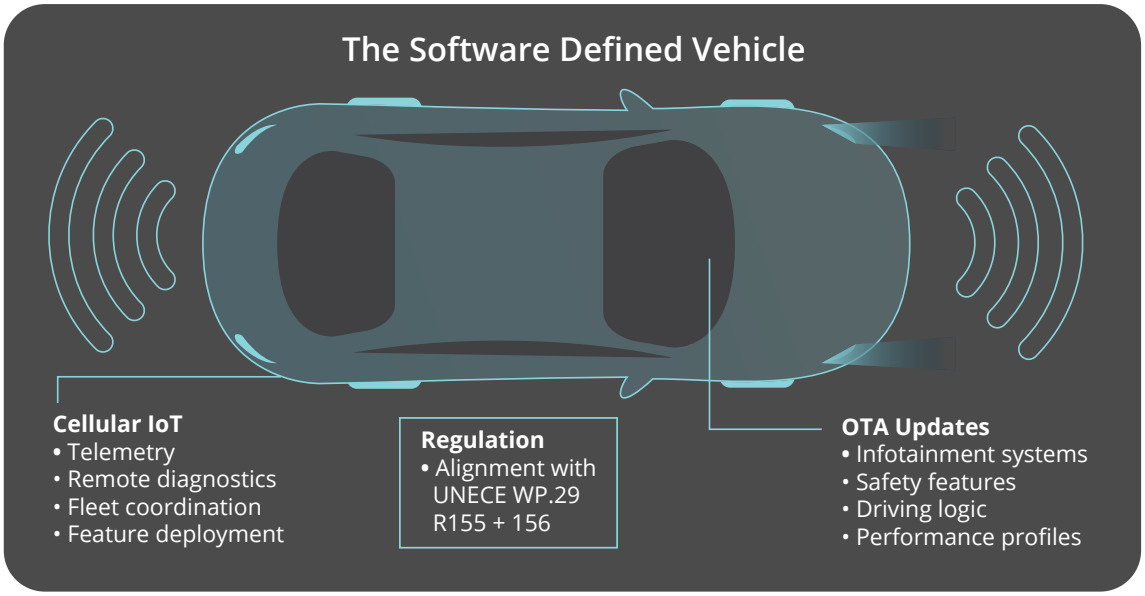
Cameras, Light Detection and Ranging (LiDAR), radar, and thermal sensors will proliferate not only in machines, but in infrastructure itself. As camera modules shrink and improve, and vertically-specialized Vision Language Models (VLMs) mature, machine perception will become a default capability.

Smart parking systems will not just count vehicles, they will classify behavior. Elder care systems will go beyond detecting motion to inferring anomalies. Smart meters will still record consumption, but they will also detect environmental context.

The volume of AI-driven decision-making pushed to the edge will dramatically reduce dependency on centralized cloud processing. Importantly, it will shift security responsibility outward.

The Connected Car Becomes a Software Platform

The automotive sector may illustrate this transition most clearly.



Connected vehicles are already standard. By 2027–2028, software-defined vehicles will dominate new model launches. Over-the-Air (OTA) updates will modify not just infotainment systems, but safety features, driving logic, and performance profiles.

Regulatory alignment with frameworks such as UNECE WP.29 R155 and R156 will enforce cybersecurity management systems and secure update governance.

Vehicles will increasingly resemble rolling distributed computing platforms. They will be reliant on cellular IoT connectivity for telemetry, remote diagnostics, fleet coordination, and feature deployment.

The Bigger Question: Who Governs Autonomous Trust?

As one of the largest providers of connectivity and solutions to the auto industry, Aeris will continue to add new features to its automotive solution, as well as use its Aeris IoT Watchtower system to monitor vehicles.

By the end of 2028, the industry will face a deeper question: when billions of devices operate semi-autonomously, across heterogeneous networks, and under overlapping regulatory regimes, who will govern trust?

Will it be centralized in cloud platforms? Distributed across hardware roots of trust? Abstracted into AI-driven risk engines? Or encoded into regulatory compliance artifacts?

Autonomy amplifies consequences. It compresses response times. It reduces human checkpoints.

If IoT in 2025 was about securing devices, and 2026 about operationalizing compliance, then 2027–2028 will be about whether the ecosystem can securely scale autonomy without collapsing under its own complexity.

This is not just an expansion phase. It is a stress test of architecture, governance, and digital resilience.

2029 AND BEYOND: IoT FOR THE BENEFIT OF ALL

By the end of this decade, IoT will no longer be just a "technology sector." It will be infrastructure as fundamental and invisible as electricity.

The shift will not simply be about more devices. It will be about a world in which physical systems in vehicles, hospitals, farms, factories, and homes operate as coordinated, AI-native networks.

The defining theme of the 2029 and beyond horizon: ubiquitous autonomy, governed by embedded trust.



Autonomous Mobility Becomes Normal

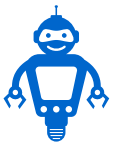
Advanced driver-assistance and partial automation (as defined in SAE J3016) will be standard in most new vehicles globally. SAE Level 2 will be a minimum baseline; Level 3 and Level 4 will be commercially routine in defined operating domains.

SAE Level 4 autonomy, with its high automation within constrained geographies, is likely to expand significantly before Level 5 (full automation under all conditions) becomes mainstream. And this transition will not be purely technical; it will be infrastructural.

During the coexistence period of autonomous and human-driven vehicles, projected safety outcomes may temporarily destabilize. Highly automated vehicles are designed to compensate for predictable environments. Human unpredictability introduces corner cases where automation is likely to struggle.

One possible response: restricted autonomous zones within urban regions where only highly automated vehicles are permitted. These zones would simplify the behavioral matrix and allow self-driving systems to operate at their highest safety performance.

Within these zones, Vehicle-to-Everything (V2X) ecosystems may finally flourish. Instead of deploying costly universal Vehicle-to-Infrastructure (V2I) upgrades everywhere, cities may selectively digitize autonomous regions and corridors. Vehicles, bikes, wearables, traffic systems, and logistics drones could operate in coordinated mesh networks, creating real-time cooperative mobility systems.



Robotics Leaves the Factory Floor

Autonomy will expand beyond vehicles into humanoid robotics, drones, and distributed industrial agents.

Heterogeneous System-on-Chip (SoC) architectures, optimized for safety, inference, power efficiency, and edge AI, will proliferate across robotaxis, delivery drones, warehouse automation, and service robotics.

Factories, airports, hospitals, and retail environments, will deploy fleets of semi-autonomous machines as default operational infrastructure.

The key inflection: these systems will no longer be isolated automation islands. They will coordinate across shared AI frameworks, real-time connectivity, and cloud-to-edge orchestration.

Robotics becomes an extension of IoT, and IoT becomes the nervous system of robotics.



Healthcare Moves "Inward"

Healthcare may experience one of the most profound IoT transformations.

Data-driven healthcare models are already expanding. By 2030, persistent monitoring, via wearables, ingestibles, and subdermal implants, could normalize continuous health telemetry.

Remote diagnostics will expand beyond telehealth video calls. Robotic-assisted remote procedures, immersive Augmented Reality (AR) diagnostics, and AI-assisted triage systems could extend specialist-level care into rural and underserved regions.

Satellite-enabled connectivity will play a role in ensuring continuity of care in remote regions. Combined with advanced edge AI and breath Volatile Organic Compound (VOC) sensors already in development, medical IoT systems may detect epidemiological anomalies earlier, potentially reshaping pandemic detection and timely response.

The concept of "Innerspace", i.e., embedded sensor networks inside the human body, will raise ethical and governance questions as quickly as it expands medical capabilities.

Healthcare IoT will demand the strictest identity, encryption, and lifecycle guarantees ever deployed at scale.



Edge AI Becomes the Default Model

By the early 2030s, centralized cloud processing alone will not scale economically or physically for the density of sensor networks deployed.

AI at the edge will become commonplace. Cameras, LiDAR, radar, acoustic, thermal, and biochemical sensors will increasingly include embedded AI acceleration. These systems will process, filter, and act locally in near-instant time, transmitting only contextual or aggregated insights upstream.

A-IoT will benefit significantly. Ultra-low-power sensors paired with intelligent gateways will enable contextual awareness without requiring heavy on-device compute power.



The Rise of Machine Data Economies

As connected systems proliferate, a new economic layer will emerge: machine-native data markets.

Autonomous vehicles, drones, environmental sensors, industrial machines, and consumer IoT solutions, will continuously generate high-value contextual data.

With appropriate governance and privacy constraints, shared sensor and data insights could improve any number of processes, from autonomous navigation models to infrastructure planning, environmental forecasting, and energy optimization, to disaster response.

A key question will arise about who owns machine-generated data? Manufacturers? Operators? Cities? Individuals? The governance models chosen here may shape geopolitical influence in the AI era.



Environmental Stewardship at Planetary Scale

Perhaps the most globally transformative application of IoT will be environmental management.

Drones and autonomous monitoring platforms could continuously inspect forests, agricultural fields, coastlines, and wildlife habitats.

Sensor networks combining visual, acoustic, thermal, and atmospheric analysis could perform any number of activities, using satellite backhaul, integrated into standardized 5G and 6G NTN to ensure planetary-scale coverage.

Any number of activities could be tracked, including monitoring crop health and water usage, tracking biodiversity changes, and optimizing distributed renewable energy grids.

Long-life, energy-efficient sensors will expand instrumentation density across natural environments. IoT will become not just an efficiency engine, but a planetary stewardship tool.

The Trust Question Becomes Existential

By 2030, the promise of IoT everywhere is extraordinary, from efficient transportation to accessible healthcare to sustainable resource management.

But the enabling condition is durable trust: cryptographic, architectural, regulatory, and societal. The industry will face defining challenges that will need to be addressed:



Beyond 2030, IoT will not simply connect the world. It will coordinate it. And whether that coordination empowers humanity broadly, or concentrates power narrowly, will depend on the governance, security, and design decisions being made today.

CONCLUSION AND CALL TO ACTION

Aeris' three pillars—Choice and Flexibility, Unified Experience, and Value Beyond Connectivity—provide a case study in aligning technology delivery with the sector's evolving demands.

We are entering a moment that once belonged only to science fiction.

The Internet connects people to information. The IoT is connecting to the physical world itself. Sensors, machines, and AI are turning cities, infrastructure, and industries into systems that can sense, respond, and adapt in real time.

This is the long-envisioned future of intelligent environments: cities that think; infrastructure that anticipates needs; and machines that collaborate with humans rather than simply serve them.

But this future will only succeed if it is built on trust. As billions of devices begin interacting autonomously with the physical world, security, identity, resilience, and responsible governance must become foundational design principles...not afterthoughts. The systems we build today will shape how safely and equitably this connected future unfolds.

The call to action is clear: continue to expand the IoT to be secure, interoperable, and trustworthy from the start.

If we succeed, IoT will become more than a technological revolution. It will quietly transform how humanity moves, heals, produces, and protects the planet, bringing us closer to a world once imagined in futuristic visions, where intelligent technology works seamlessly in the background to make life safer, smarter, and better for everyone.

157 Columbus Avenue
New York, NY 10023
www.abiresearch.com

3979 Freedom Circle, #520
Santa Clara, CA 95054
www.aeris.com

Published May 2026

About Aeris

For more than three decades, Aeris has been a trusted IoT leader enabling the biggest IoT programs and opportunities across automotive, utilities and energy, fleet management and logistics, medical devices, and manufacturing. Our IoT technology expertise serves a global ecosystem of 7,000 enterprise customers, nearly 30 mobile network operator partners, and more than 100 million IoT devices across the world. Aeris, the largest orchestrator of eSIMs for IoT, powers today's connected smart world with innovative technologies and borderless connectivity that simplify management, enhance security, optimize performance, and drive growth at scale. To learn how Aeris IoT Accelerator platform can secure and supercharge your critical IoT programs, visit aeris.com and follow us on LinkedIn.
©2026 Aeris Communications, Inc. All Rights Reserved.

About ABI Research

We Empower Technology Innovation and Strategic Implementation.
ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers.

©2026 ABI Research. Used by permission. ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. The opinions of ABI Research or its analysts on any subject are continually revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.