

From Communication Intelligence to a Trustworthy Internet

Edge–Core Convergence and AI-Driven Network Control

Eduard Cristian Popovici

SAIM Lab · Telecommunications Department · ETTI Faculty · POLITEHNICA Bucharest

AI does not just use the Internet. It is redesigning it.



Is the Web still mainly for humans?

Automated clients are reshaping what a web request represents.

≈ 60%

**Cloudflare-observed requests for HTML content:
approximately 60% bots in the referenced period.**

This measures HTML requests on Cloudflare's network — not all Internet bytes, and not only AI agents.

[Cloudflare Radar · worldwide · HTML HTTP requests · 28 Aug–06 Oct 2026](#)

The Internet Is Moving from Connection to Coordination

Why this change is happening **now**

- **Users** expect **real-time** services **everywhere**.
- Content, cloud, sensors and applications **spread across the network**.
- Network **pressure changes faster** than manual operations can follow.
- AI becomes necessary because **complexity has exceeded static control**.

The next Internet challenge is not only to connect everything, but to coordinate everything.

From transport network to decision infrastructure

The **Internet** *no longer only carries data*; it **supports decisions**.

COLLECT

Signals, logs, telemetry

CARRY

Packets, streams,
services

PROCESS

Edge and cloud analysis

PROTECT

Security and resilience

DECIDE

Policy and control

- Every **network node** can become a **source of operational intelligence**
- Telemetry turns **connectivity** into **context**
- Context turns **operations** into **faster decisions**

Connectivity is the raw material. Decision is the value.

The next Internet transaction may be an agent workflow

The Web is *evolving* from **page delivery** toward **delegated machine-to-machine actions**.

BEFORE

Human → browser → web page

EMERGING

User goal → AI agent → APIs and tools

THE DESIGN QUESTION

Which identity, permissions and audit trail follow each agent request?

Packets may be generated by delegated actions, not only direct human clicks.

Where should intelligence live?

The answer is architectural, *not just technological*.

AT THE EDGE

When milliseconds matter

IN THE CORE

When coherence matters

IN THE CLOUD

When scale matters

ACROSS THE NETWORK

When learning matters

- **Edge** brings **action closer** to users and applications
- **Core** keeps **global coordination, policies** and **stability**
- **Cloud** provides **scale** for **deeper analysis** and **learning**

The Internet is becoming less centralized, but more coordinated.

AI may reverse a familiar traffic assumption

Uplink is growing faster than downlink for most operators in an Ericsson sample.

43 / 55

17 of the 55 operators saw uplink growth more than 1.5× the downlink growth rate.

Downlink still dominates total volume; emerging AI use cases may put new pressure on uplink.

From static routes to adaptive flow

Traffic control *becomes* more sensitive to context.

OBSERVE

Telemetry

PREDICT

Likely stress

PRIORITIZE

Service needs

ADAPT

Resources

VERIFY

Experience

- **Live telemetry** reveals **patterns before alarms**
- **AI** can detect **early signs** of **congestion** or **degradation**
- **Traffic** can be **adapted before** service **quality drops**
- **Resources follow** application **context**, *not only fixed rules*

The best route is the path that understands the moment.

AI-Driven Traffic Control

From **static** rules to **live network** decisions

- The **network** observes **live traffic conditions**.
- **AI** detects **patterns** and **early signs** of congestion.
- **Traffic** can be **redirected before** service **quality drops**.
- **Resources** can be **adapted** to application **needs**.
- **Anomalies** can be **identified faster** and **more accurately**.

The network learns to react before the problem becomes visible to the user.

Networks must learn before they break

The **goal** is to **reduce impact**, *not only to repair faster*.

REACTIVE MODEL incident → alarm → diagnosis → response → repair

PREDICTIVE MODEL observe → pattern → warning → preventive action → reduced impact

The goal is not to fix faster. The goal is to fail less visibly.

Machine-speed attacks demand machine-speed resilience

Quarter-over-quarter increase in network-layer DDoS attacks >1 Tbps (Q2 vs Q1 2026).

+519%

Cloudflare reports 935 DDoS attacks above 1 Tbps mitigated during H1 2026.

Rapid detection, controlled mitigation and fast recovery are architectural requirements.

Automation with accountability

Autonomous networks *must remain visible, bounded and reversible.*

VISIBILITY

Operators **see** what the system **recommends**.

LIMITS

Critical actions follow approved **policies**.

OVERSIGHT

Humans remain **responsible** for high-**impact** changes.

ROLLBACK

Automated actions can be **reversed safely**.

Autonomy is not the absence of human control. It is human control built into the system.

AI infrastructure is becoming the new exposed edge

Internet-exposed AI infrastructure grew *during the nine months assessed* by Censys.

+63%

Internet-facing AI tools and services increase the importance of visibility, identity and access controls.

Exposure is not automatically a vulnerability — but it expands the observable attack surface.

No network is intelligent alone

AI increases the need for **cooperation**, *not only automation*.

INTERNET PROVIDERS

Adaptive capacity and **network operations**

INTERNET EXCHANGES

Interconnection and **shared visibility**

CONTENT PLATFORMS

Placement and **delivery decisions**

CLOUD & EDGE

Distributed compute and **network coordination**

- Security **response depends** on **shared visibility**
- Trust **depends** on **coordination across actors**

In the AI era, no network is intelligent alone.

Designing a trustworthy AI-powered Internet

Intelligence *must be* architectural, operational and governable.

OBSERVABLE

By **design**

PREDICTIVE

But **explainable**

AUTOMATED

But **governed**

DISTRIBUTED

But **coherent**

RESILIENT

**Before users
notice** failure

Trustworthy infrastructure means intelligent infrastructure with accountable control.

AI does not just use the Internet. AI is redesigning it.

The next Internet architecture will be *adaptive by design*.

- It **changes where** Internet **decisions** are made
- **Edge** and **core** become **part of the same decision loop**
- **Traffic control** becomes **adaptive** and **context-aware**
- **Architecture, operations** and **trust** *evolve together*

Communication becomes context. Context becomes prediction. Prediction becomes action.

Thank you!

From communication intelligence to Internet intelligence.

Edge–Core Convergence and AI-Driven Network Control

Eduard Cristian Popovici · SAIM Lab · RITE 2026



Why this matters now

Complexity is moving faster than manual network control.

- **Traffic** is more **dynamic, distributed** and b
- **Applications** depend on **fast decisions**, not only fast connections
- **Centralized cloud** is **not enough** for **every real-time use case**
- **AI** allows **networks** to **observe, predict** and **adapt**

CONNECTIVITY

CONTEXT

PREDICTION

ACTION

The new bottleneck is the speed of understanding.

The New Architecture: Edge, Core and AI

Where should intelligence live?

EDGE

Fast local action close to users, devices and events.

CORE

Coordination, stability, policy and **global visibility**.

CLOUD

Scale, storage, training and **deeper analysis**.

AI

Prediction, prioritization and **adaptive control**.

OBSERVE
state

PREDICT
future

CONTROL
action

LEARN
feedback

The architecture is no longer a line. It is a living loop.

Distributed intelligence, coherent control

Local speed and global stability must be *designed together*.

EDGE

Local action — reacts close to events

CORE

Global coordination — keeps policy and coherence

- AI links local *adaptation* with global control
- Traffic control becomes shared across layers

The edge is not replacing the core. It is forcing the core to become smarter.

Networks Must Learn Before They Break

From reactive operations to predictive operations

- **Traffic patterns** reveal **early stress**.
- **Service degradation** often **has warning signs**.
- **AI** can **support preventive** capacity **decisions**.
- **Operations teams** move **from firefighting to orchestration**.
- **Predictive networks** buy **time** for **better decisions**.

Prediction is most valuable when it changes the outcome, not just the report.

Automation with Accountability

Intelligent networks must remain governable

- AI can **recommend actions**.
- **Some actions** may be **automated**.
- **Critical changes** need **clear policies** and **human oversight**.
- **Network decisions** must be **visible, explainable** and **reversible**.
- **Trust** comes from **control**, *not from blind automation*.

Policy · Visibility · Audit · Rollback

Impact on the Internet Ecosystem

The **transformation** goes **beyond** a single network.

- Internet **providers** need **more predictive operations**.
- Internet **exchange points** may see **more dynamic traffic behavior**.
- **Content platforms** need **smarter placement** and **delivery**.
- **Cloud** and **edge providers** become **part of the same architecture**.
- **Users** will **judge** the Internet **by continuity, speed** and **trust**.

The Internet ecosystem is becoming an ecosystem of shared decisions.