Internet Society
Ukraine Chapter

GIGABIT
CHAPTER 2025

Overview of Internet development trends in 2026

Challenges for government agencies and operators

A transformation that is inevitable

The review was prepared by the ISOC Ukraine Chapter

2026

Content

Scope....4
1. Main trends of 2026....6
1.1. The Internet is moving from an “information network” to a “decision-making infrastructure”....6
1.2. AI is becoming the infrastructure layer of the Internet....6
1.3. The Internet is becoming physically limited....7
1.4. Centralization of the Internet is becoming one of the main systemic risks 8
1.5. IXP is no longer just an economic tool....8
1.6. Digital sovereignty....9
1.7. The emergence of a new concept: "sovereignty without isolation"....9
1.8. The Internet is becoming multilayered....10
1.9. Satellite Internet is changing the concept of the "last mile"....11
1.10. Sustainability becomes more important than speed....12
1.11. Trust becomes infrastructure....12
1.12. Encryption becomes a geopolitical issue....13
1.13. Internet outages are becoming a separate global risk....13
1.14. AI is creating a new type of internet traffic....13
1.15. Combining the Internet + IoT + AI triad and forming the Cyber-Physical Internet....14
2. The main conflict of 2026....14
3. Final analytical formula for 2026....16
4. What does this mean for Ukraine?....17
4.1. Implementation steps....18
4.1.1. Implementation of the principle of "Sovereignty through Interoperability"....18
4.1.2. Moving from “network recovery” to a national Internet resiliency architecture....19
4.1.3. Creating a Distributed Internet Interconnection System....19
4.1.4. Integration into the European fiber optic network architecture....20
4.1.5. Integration of Ukrainian regulation not only legally, but also technically....20
4.1.6. Creating a Trusted Internet Architecture....21
4.1.7. Preparing for the AI Internet....22
4.2. Practical steps towards implementing approaches to regulating the EU electronic communications market....23

4.3. Creating a national Internet Governance 2.0 system 24

Scope

2026 has become a year of changes to the very architecture of the Internet and a strategic shift away from simple changes associated simply with a set of individual technological innovations.

The Internet Society (ISOC) views the Internet as a global, open, interoperable, and decentralized infrastructure that should transform the digital services market.

The digital services market is not simply being formed as a set of available services from individual operators, but as a single ecosystem that allows users to form their own personalized systems of necessary services.

In this regard, the issue of creating a system of trust in the Internet becomes a huge problem, because trust in the Internet is falling - fraud, AI content, blocking, etc. factors contribute to this.

It is no coincidence that in 2026, two systemic challenges are at the center of ISOC's strategy: global inequality and declining trust in the Internet.

The Internet in 2026 is entering a new stage of its development. While in previous decades its key function was to provide global connectivity and access to information, today the Internet is becoming the basic infrastructure of the economy, government, artificial intelligence, critical services, and everyday life of society. At the same time, the very architecture of the digital space is changing: the volume of machine and AI traffic is growing rapidly, distributed computing infrastructure is developing, the role of data centers, cloud platforms, backbone and cross-border networks is increasing, and issues of cybersecurity, resilience, and trust are becoming inseparable from the fun.

These technological changes are taking place against a backdrop of increasing geopolitical fragmentation and competition for control over digital infrastructure. States are seeking to ensure digital sovereignty, localize critical data and computing resources, reduce dependence on external providers, and protect national infrastructure from cyberattacks and physical threats. However, excessive centralization and fragmentation of the digital space create a new risk – the gradual destruction of the properties that made the Internet a global system: openness, interoperability, distribution, and the ability of different networks and participants to interact freely.

It is in this context that the position of the Internet Society (ISOC) becomes particularly important, considering the Internet as a global, open, reliable and resilient infrastructure, the development of which should be based on interoperability, distribution, security and multilateral governance. Connectivity, accessibility and reliability of infrastructure, development of local IXPs, routing security, trust in the Internet, protection of open network architecture and counteraction to its fragmentation occupy a special place on the ISOC 2026 agenda.

For Ukraine, these global changes are not only technological, but also strategic. In wartime, the stability of electronic communications is directly related to national security, the functioning of the economy, public services, energy, logistics, and social infrastructure. At the same time, Ukraine's integration into the European digital market opens up the opportunity to move from a model of peripheral connection to the

European infrastructure to the formation of full-fledged cross-border digital corridors and regional communication nodes.

Therefore, Ukraine's strategic task at the next stage is not only to restore damaged infrastructure or increase network capacity. It is necessary to form an architecture of the national Internet infrastructure that would simultaneously ensure stability, interoperability, security, trust, and the ability to technological development, while maintaining Ukraine's full integration into the European and global Internet.

In this regard, it is advisable to consider Ukraine's digital sovereignty not as isolation from the global digital environment, but as the ability to independently ensure the continuity of critical digital infrastructure, choose between alternative suppliers and routes, ensure the protection of its own resources, and at the same time maintain compatibility with global and European technological standards. In other words, the strategic goal is not a "sovereign Internet", but sovereignty through interoperability.

It is this approach that allows us to form a new strategic framework for the development of the Ukrainian Internet: from the restoration of individual networks to the construction of a distributed and sustainable infrastructure; from local access to full-fledged European connectivity; from traditional telecommunication networks to an infrastructure ready for AI and cyber-physical systems; from a predominantly defensive model to the creation of a Trusted Internet Infrastructure.

In this perspective, Ukraine has the opportunity not only to adapt to global changes, but also to take a more significant position in the European digital ecosystem - as a country with a developed IXP system, cross-border optical routes, data centers, distributed computing infrastructure, and a competent technical community.

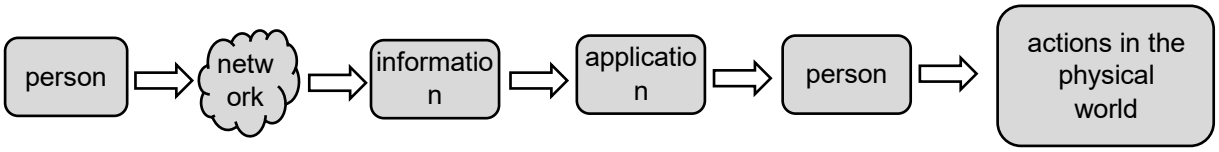
Therefore, the question of the coming years is no longer how to connect Ukraine to the global Internet, but how to make Ukraine a sustainable, interoperable, and trusted part of the European and global Internet infrastructure in the era of AI, digital sovereignty, and geopolitical fragmentation.

The answer to this question requires a transition from individual infrastructure projects to a comprehensive strategy that combines public policy, the development of electronic communications, cross-border infrastructure, IXPs, cybersecurity, digital trust, AI infrastructure, scientific and educational potential, and the principles of multilateral Internet governance (multistakeholderism).

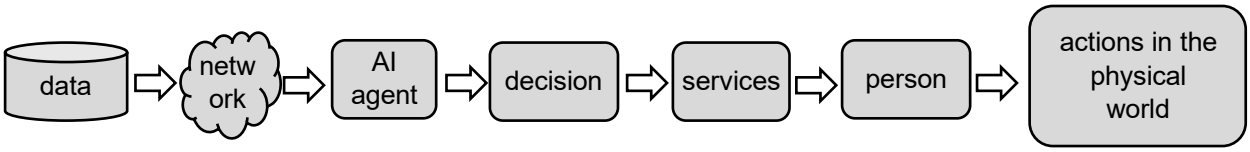
1. Main trends of 2026

1.1. The Internet is moving from an “information network” to a “decision-making infrastructure”

Classical interaction on the Internet could be conditionally described as a system of interaction



In 2026, a new model of interaction is taking shape:



This is an important transition.

AI is becoming more than just an application on top of the Internet. It is starting to define:

- what data will be obtained;
- what services will be called;
- which route or resource will be chosen;
- what decision will be made;
- which actions will be automatically performed.

Therefore, AI is gradually becoming a new consumer and at the same time a new operator of the Internet infrastructure.

IEEE also characterizes 2026 as a transition to intelligent, software-driven connectivity, where AI is integrated directly into network management. (IEEE Standards Association)

The main object of competition is no longer just Internet access, but a combination of factors:

computing + connectivity + data + AI + energy

1.2. AI is becoming the infrastructure layer of the Internet

In 2026, three consecutive stages can be distinguished:

Period	AI model
2023–2024	Generative AI

2025	Agentic AI
2026	Distributed AI / AI inference infrastructure

There is a shift from “where is the model?” to “where is the inference performed in real time?”

This means developing:

- edge AI;
- AI PoP;
- regional inference;
- GPU clusters;
- AI-ready data centers;
- distributed computing;
- AI networking;
- high-speed intercontacts.

IDC 2026 explicitly states that for the telecom sector, a critical transition comes from model training to real-time distributed inference, forcing operators to reconsider their infrastructure architecture.

The consequence of this is that the telecommunications network is gradually becoming a Compute Connectivity Infrastructure, rather than simply a transport of IP packets.

1.3. The Internet is becoming physically limited

This is one of the most underestimated trends.

AI requires a huge amount of:

- electricity;
- GPU;
- cooling;
- optical channels;
- data centers;
- international highways.

Therefore, a new dependency arises:

AI → Data center → energy → FOCL → communication

That is, the digital economy is once again becoming dependent on physical infrastructure.

This changes the strategic meaning:

- submarine cables
- DWDM

- terrestrial fiber optic cables
- IXP
- Data Center Interconnect (DCI) technologies
- data centers
- regional PoPs
- energy generation issues.

That is why today a data center cannot be considered only as an IT facility; it becomes part of the critical infrastructure of the state.

1.4. Centralization of the Internet is becoming one of the main systemic risks

ISOC usually considers excessive concentration of infrastructure, services, and control in a few entities to be a danger.

In 2026, this manifests itself in several layers at once:

Infrastructure layer or service	Threat
Cloud	Multiple global hyperscalers
AI	A limited number of companies control the most powerful models and GPU infrastructure
DNS/CDN	Concentration of a significant part of the infrastructure in large global players
Peering	Growing dependence on large transit and cloud providers
Platforms	Concentration of the user and the information environment

ISOC in its 2026 materials specifically draws attention to the risks of centralization and, for example, analyzes the problem of centralized and virtual peering as a threat to the stability of the Internet. (Internet Society)

1.5. IXP is no longer just an economic tool

The classic logic of IXP development and operation:

IXP → local traffic → lower latency → lower transit costs

New logic:

IXP → local traffic → resilience → digital sovereignty → continuity of critical services

That is why ISOC in Action Plan 2026 directly links:

local peering infrastructure → availability → reliability → fault tolerance

local peering infrastructure → affordability → reliability → resilience

and plans to support and develop local IXPs, train technical communities, and localize traffic. (Internet Society)

That is, the IXP becomes an element of the national fault tolerance architecture.

For Ukraine, this is especially important and the formula:

IXP + multiple points of presence (PoP) + multiple fiber routes + regional interconnect

can be seen as a mechanism for creating a distributed national fault-tolerant Internet.

1.6. Digital sovereignty

The trend towards Digital Sovereignty creates a very interesting conflict when states say:

"We need digital independence"

and in practice, digital sovereignty is being transformed into Internet fragmentation.

ISOC directly addresses the rise of policies that attempt to establish geographical boundaries for the global Internet.

A significant contradiction arises when the state logic views sovereignty as control and management, while the logic of the technological environment and the Internet Governance environment views sovereignty as a combination aimed at creating an environment:

choice + resilience + interoperability

These are different concepts.

1.7. The emergence of a new concept: "sovereignty without isolation"

One of the most important conceptual trends of 2026.

A strong digital system is not a situation where we build everything ourselves, but where we are able to continue working even if part of the external infrastructure is unavailable.

That is:

sovereignty ≠ isolation

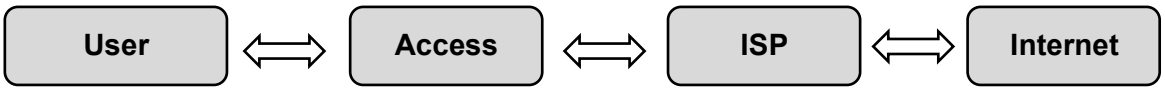
and:

sovereignty = ability to choose + ability to switch + ability to interact

This logic can be seen in the ISOC Chapters' discussions on sovereign technology: control over one's own infrastructure must be combined with keeping the door open for cooperation. (Internet Society Singapore Chapter)

1.8. The Internet is becoming multilayered

Architecturally, the Internet in 2026 looks less and less like a simple model:



Several structural layers are formed (Figure1).

AI/Agents Layer – the highest level: applications and services (including AI and agents) that run on top of the network infrastructure. These are the consumers that power the lower layers.

Cloud/SaaS layer – cloud platforms and software as a service on which top-tier applications run.

Data/Identity layer – data and identification layer (access control, identification, authorization and authentication, data storage and processing).

The Internet layer is the key point from where the network diverges into two main paths to access users:

- Mobile and Satellite – mobile networks, including satellite access.
- Fixed Fiber and Local PoP – fixed fiber optic networks through local points of presence (Point of Presence).

IXP/Peering layer, where operators exchange data directly

The Regional backbone layer is a regional backbone network that connects traffic at the regional level.

International backbone – international fiber optic highways that connect regions using submarine and terrestrial cables and are the physical basis of global communication between continents.

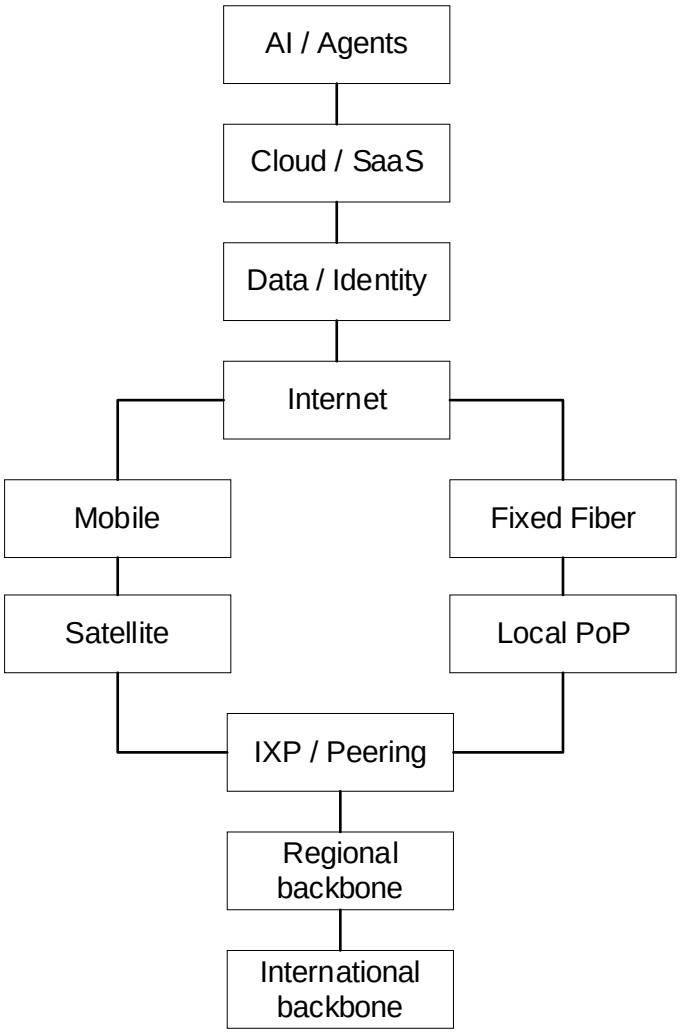


Figure1. Diagram of the structural layers of the Internet

In this case, each layer becomes a potential "bottleneck."

1.9. Satellite Internet is changing the concept of the "last mile"

In 2026, terrestrial, mobile, and satellite communications begin to be viewed not as competing technologies, but as a single hybrid connectivity architecture, for which the following are particularly important:

- low-orbit satellites (LEO);
- direct-to-device connection to satellites
- satellite backhaul
- terrestrial fiber infrastructure
- 5G/5G Advanced technologies
- future 6G architecture.

Thus, Internet access ceases to be tied to a single physical solution at a given point for a given user.

This is extremely important for Ukraine in the context of the need to solve the following tasks:

- restoring communication after natural disasters and destruction

- providing communications in rural areas
- ensuring maritime communications
- ensuring communication in emergency situations.

1.10. Sustainability becomes more important than speed

This is perhaps the most significant shift in the philosophy of Internet infrastructure.

Period	Main criterion
In the 2010s	How fast is the network?
In the 2020s	How secure is this network?
In 2026	Will the network be able to continue operating under load conditions?

The concept of Internet resilience engineering appears, which includes:

- diversity of routes
- diversity of providers
- IXP;
- local peering
- multiple upstreams
- DNS redundancy (redundant DNS)
- redundant power
- distributed points of presence (distributed PoPs)
- satellite backup
- cyber resilience
- community networks

ISOC effectively places resilience alongside connectivity and affordability. The Action Plan explicitly highlights the role of IXPs in keeping businesses online and infrastructure resilient.

1.11. Trust becomes infrastructure

ISOC clearly states that the Internet must not only be accessible, but also safe, secure, and trustworthy, so in 2026, simply being connected is not enough.

Therefore, trust is gradually becoming an infrastructural property that should comprehensively include:

- encryption
- RPKI (Resource Public Key Infrastructure)
- secure routing
- Domain Name System security (DNS security)
- privacy and confidentiality
- identification (identity)
- anti-fraud

- cyber resilience
- software security (secure software)
- artificial intelligence safety (AI safety).

In other words, security ceases to be a separate service and becomes part of the network architecture itself.

1.12. Encryption becomes a geopolitical issue

Internet Society continues to view encryption as a fundamental element of trust in the Internet ecosystem and directly links encryption to privacy and security.

The problem of 2026 can be formulated in this aspect, how the state wants to control crime, terrorism, AI, disinformation, and the user must have secure communication.

This creates constant pressure on:

- end-to-end encryption
- encrypted messaging
- anonymity
- privacy-enhancing technologies

1.13. Internet outages are becoming a separate global risk

It is very telling that in August 2026, the Internet Society released a separate article:**Shutdown Trends from 2019 to 2025: Where Do We Go from Here**.

ISOC views outages no longer as exceptional political events, but as a systemic threat to the global Internet.

An important concept is becoming relevant: network availability becomes a human-rights and economic continuity issue.

That is, turning off the Internet does not simply mean, for example, a situation where "people cannot access Facebook," but generates a chain of interruptions to the normal life support of modern people:

payment systems → logistics → healthcare → government → education → business → emergency services, etc.

1.14. AI is creating a new type of internet traffic

Historically, the Internet has been focused on human-generated traffic. Now, traffic generated by the “machine system” itself is rapidly growing, originating from:

- AI agents
- search engines (crawlers)
- procedures for machine inference and resolving
- machine-to-machine interaction procedures
- IoT;
- autonomous systems

The war gives rise to the Internet of autonomous agents.

And here a completely new question arises – who is the subject of Internet communication: a person? an application? AI agents? IoT devices? autonomous vehicles? digital identification procedures?

What was a legal issue of rights and trust in content becomes a question of architecture.

1.15. Combining the Internet + IoT + AI triad and forming the Cyber-Physical Internet

Cyber-Physical Internet is perceived as the next stage of Internet development. There is a combination of technologies and means of information processing and decision-making, which allows moving from the triad Internet + IoT + AI to a qualitatively new stage of development in the form of Cyber-Physical Systems.

That is, the Internet begins to rule:

- cars;
- energy;
- industry;
- logistics;
- robots;
- medical devices;
- smart cities.

Therefore, it is a mistake in 2026 to consider the Internet solely as a communication infrastructure, because the Internet is becoming the infrastructure for managing the real economy.

2. The main conflict of 2026

If we reduce global trends to a single chart (Figure 2), which illustrates the dilemma of the development of the Internet: whether the future will be built on the principles of centralization (convenience for giants) or on the principles of distribution (equality of participants). Any path determines the desire for digital sovereignty, which can be achieved through control and fragmentation, or through freedom of choice and interoperability. The ultimate goal of both approaches is a stable network in which the property and environment of trust are implemented.

The key idea illustrated by the diagram is the tension between the integrity of an open network and the growing desire for national and corporate control, asking: can trust and resilience be maintained without sacrificing openness?

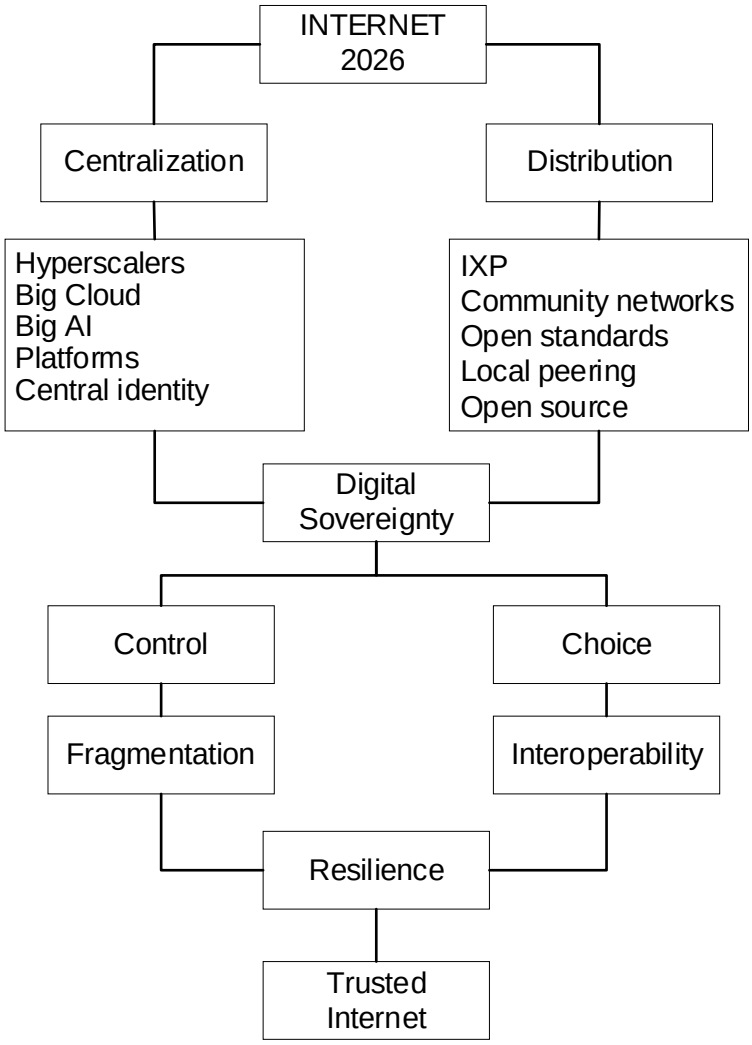


Figure 2. Diagram illustrating the dilemma of internet development

The first level considers the conflict between centralization and distribution. This is the main fork – two opposing paths for the further development of the network.

Centralization, when one center controls everything, determines dominance:

- Hyperscalers – giant cloud providers (Amazon, Google, Microsoft)
- Big Cloud – large cloud platforms
- Big AI – big players in the field of AI
- Platforms – dominant platforms (social networks, marketplaces and service ecosystems)
- Central identity – a single identification system under one control

Distribution, where power is dispersed among participants, determines the management of the elements:

- IXPs – Internet Exchange Points (where networks connect directly)
- Community networks – local networks managed by communities

- Open standards – open technical standards
- Local peering – direct connections between neighboring networks without intermediaries
- Open source – open-source software

The second level in the analyzed diagram is related to the potential of digital sovereignty, when both branches of the conflict converge at a common point.

This means that regardless of the path chosen, states and communities seek digital sovereignty and control over their data, technology, and infrastructure.

The third level considers the conflict between Control and Choice, which is another fork within sovereignty.

The path of control (sovereignty through constraints) defines the actions of the government and the regulator as aimed at fragmentation, i.e. fragmentation (different regions with incompatible systems)

The path of choice (sovereignty through authority) defines the actions of the government and the regulator as aimed at interoperability, i.e. the ability of systems to interact with each other.

Both branches (management and choice) lead to a common goal, but they determine the implementation of state regulatory policies at the final points:

- resilience – stability (the ability of a network to survive failures, attacks and crises)
- trusted Internet – an Internet environment with an ecosystem of trust

The Internet will evolve over the next 5–10 years in determining the choice between or a combination of centralization and distribution policies.

Therefore, ISOC actually protects not the “old Internet”, but a certain architectural model of the future Internet, which must comply with the architectural principles:

Principle	Sense	Properties of the future Internet
Open	open Internet	1. community networks 2. IXP 3. open standards 4. encryption 5. multi-stakeholder governance 6. local Internet infrastructure 7. meaningful connectivity
Global	global connectivity	
Interoperable	interoperability	
Distributed	distribution	
Trusted	security and trust	

These are not separate directions. These are elements of one architectural model. (Internet Society)

3. Final analytical formula for 2026

The global transformation of the Internet:

Period	Development formula	What is success?
Until 2010	Internet = access	better access → better Internet
2010–2020	Internet = connectivity	more bandwidth → better Internet
2020–2025	Internet = digital economy infrastructure	control access + more bandwidth → better Internet
2026–2030	Internet = critical socio-economic function + AI + cyber-physical infrastructure	connectivity + resilience + interoperability + trust + compute + energy

ISOC in 2026 actually offers an answer to the global trend of centralization:

Not fighting technological development, but not allowing technological development to destroy the architectural properties of the Internet

The key priorities that ISOC is considering for 2026 can be summarized into four:

1. Connect

Connect those who remain offline

2. Localize

Develop local infrastructure, IXPs and peering

3. Protect

Protect encryption, privacy, security, and trust online

4. Keep Open

Prevent Internet fragmentation under the guise of digital sovereignty

4. What does this mean for Ukraine?

For Ukraine, these global trends are particularly interesting.

Ukraine can be not only a consumer of the global digital infrastructure, but also a regional element of the European Internet infrastructure.

Strategically, the most promising model that implements the transformation of Ukraine's Internet space into one of the EU's digital communication centers with IXP components, regional PoPs, a southwestern transition to Romania, Bulgaria, and the Balkans with further integration into the European backbone.

Overview of Internet development trends in 2026. Challenges for government agencies and operators. Transformation that is inevitable.
ISOC Ukraine Chapter.

This will allow us to consider actions aimed at implementing such a model no longer simply as telecom projects, but to position them as:

Regional Internet Resilience Infrastructure

and at the same time:

Digital sovereignty through interoperability and system compatibility

If we translate this into the language of strategic planning, the main question is no longer

How to connect Ukraine to the Internet?

and

How to make the Ukrainian segment a sustainable, interoperable, and trusted part of the European and global Internet infrastructure in the era of AI, digital sovereignty, and geopolitical fragmentation?

In the logic of implementation, this could be a national sustainability program and interoperable The Internet community, which unites the state, operators, IXPs, the technical community, universities and businesses.

Moreover, Ukraine already has a good starting point: in 2025, it was approved Strategy for the development of electronic communications until 2030, which provides for gigabit connectivity, 5G, digital resilience and integration into the EU Digital Single Market. And since January 1, 2026, Ukraine has already been in the EU Roam Like at Home mode – that is, integration has ceased to be only declarative (digital-strategy.ec.europa.eu).

4.1. Implementation steps

4.1.1. Implementation of the principle of "Sovereignty through Interoperability"

The implementation of the principle of "Sovereignty through Interoperability and Interoperability" is the ideological center of the country's digital policy. An open and global Internet must maintain interoperability while becoming more resilient and trusted.

Moving away from the principle of “A country should have its own Internet” and moving towards the principle of “A country should be able to choose, switch and continue working without losing compatibility with the global Internet”:

Region	The demand for sovereignty
DNS	several independent levels
Transit	≥3 independent directions
IXP	distributed
Cloud	multi-cloud
Fiber	variety of routes
Data centers	geographical diversity
AI	distributed computing
Identity	compatible principles
DNS/CDN	several suppliers
Mobile	several operators
Satellite	backup connection

4.1.2. Moving from “network recovery” to a national Internet resiliency architecture

Task: to build a distributed, redundant, and autonomous Internet infrastructure in Ukraine.

This means creating a national map of critical Internet resources:

- trunk fiber optic cables
- international transfers
- underwater/land routes
- IXP
- data centers
- DNS infrastructure
- cloud infrastructure
- artificial intelligence infrastructure
- mobile communication
- critical PoPs
- The importance of energy.

For each element, it is necessary to define primary, secondary, emergency routes with N-1 / N-2 resilience, i.e. the ability to continue operation after the failure of one or more independent elements.

4.1.3. Creating a Distributed Internet Interconnection System

Ukraine should have many “national IXPs” that form a distributed system of interconnected IXPs/PoPs.

Functionally, an IXP should be considered as a platform that provides the following:

- distributed peering

- BGP
- RPKI
- routing servers (route server)
- IPv4/IPv6
- BGP communities
- DDoS mitigation
- traffic analysis
- cloud interconnection
- CDN interconnection.

This is fully consistent with the logic of developing Internet reliability and stability, where local peering increases the availability, reliability, and resilience of the Internet.

4.1.4. Integration into the European fiber optic network architecture

Ukraine should not be the end point of the European Internet network, but should become a transit regional hub.

Particularly important are the south-west corridor, which includes the route Ukraine – Danube – Romania – Balkans – Central Europe, and the western corridor, which includes the route Ukraine – Poland – Germany / Baltic region.

This means developing:

- cross-border telecom transitions
- DWDM;
- various fiber optic line routes
- cross-border PoPs
- objects independent of telecommunications operators
- international IXPs
- connections between data centers.

In fact, the task statement determines the creation of the “EU – Ukraine Digital Resilience Corridor”.

4.1.5. Integration of Ukrainian regulation not only legally, but also technically

Use the experience of integration into EU roaming, which became the first example of applying the EU internal market to Ukraine in the digital sphere (digital-strategy.ec.europa.eu)

The next level is the transition from legal alignment to regulatory + technical interoperability policy.

Priorities	Directions, tasks
Electronic Communications	• EECC (European Electronic Communications Code) • spectrum • 5G • cross-border connectivity

	• infrastructure sharing • wholesale access • numbering • roaming
Digital identity	• eID • trust services • authentication
Data	• GDPR-compatible mechanisms • cross-border data flows
Cybersecurity	• NIS2-compatible framework • incident reporting • critical infrastructure
Digital services	• EU interoperability

In 2026, actions were initiated to implement the provisions of the Interoperable Europe Act by Ukraine; among the areas identified were a national framework for interoperability, cross-border digital services, and integration of solutions into the European ecosystem. (NISS)

4.1.6. Creating a Trusted Internet Architecture

A fundamental requirement without which the implementation of a new Internet architecture is impossible, which aims to transition from the concept of "cybersecurity as protection" to the concept of "trust embedded into Internet architecture".

The minimum and initial requirements for implementing this architectural approach include establishing procedures that define trust regarding:

- IPv4/IPv6
- DNS (DNSSEC, TLS)
- BGP (RPKI)
- DDoS protection
- strict identification
- logging/monitoring
- incident response

It is especially important to make RPKI a practically mandatory element of a professional network infrastructure with the implementation of a chain of actions:

ROA (Route Origin Authorization) → validation → filtering → secure routing

which describes a standard process for protecting global routing on the Internet from BGP Hijacking and Route Leaks, ensuring that traffic only travels along legitimate routes

And also to create a national Internet monitoring system covering BGP monitoring, DNS anomalies, monitoring of network delays and failures, IX traffic and cross-border transitions

4.1.7. Preparing for the AI Internet

This is something that is still lacking in the traditional Ukrainian strategy for the development of electronic communications.

In 2026 Cabinet of Ukraine and the Ministry of Digital Affairs have included the issue of transitioning to a connectivity strategy for AI (Agentic State) and AI security as priorities for the digital agenda.

To do this, you need to create an infrastructure layer, the AI Connectivity Strategy, which defines technological and organizational development as a single distributed architecture:

Data Center → IXP → Backbone → Cloud → AI Compute

Development priorities from a technological point of view are determined by:

Priority	Role
Computational level	
Regional AI computing resources	Fine-Tuning models for specific local markets/languages and for resource-intensive inference with low response time, data localization, offloading central hubs
GPU clusters	Combining multiple GPUs into a single networked supercomputer
Edge AI	Providing instant inference for mission-critical applications: autonomous vehicles, smart factories, security cameras, medical equipment
AI-ready data centers	Providing Direct-to-Chip cooling for hot GPUs, uninterrupted power, and a room architecture optimized for ultra-dense fiber cabling
Network layer	
High-speed optical interconnect within the data center	GPU connectivity within and between racks using optical transceivers to transfer terabits of data with minimal heat and power consumption, excluding network congestion during parallel computing
400G/800G	Transition to 400Gbps and 800Gbps ports, and in the future 1.6T, and reduction in the number of physical cables and ports on switches, simplifying the Spine-Leaf network architecture

Overview of Internet development trends in 2026. Challenges for government agencies and operators. Transformation that is inevitable.
ISOC Ukraine Chapter.

Priority	Role
Data Center Interconnect	Distribution of training or inference phases between different data centers, data center connectivity at high speeds, and route reservation
Low-latency routes	Using the shortest optical paths (straight fiber without unnecessary transit nodes) and optimizing routing protocols to accelerate GPU synchronization and reduce overall model training time

4.2. Practical steps towards implementing approaches to regulating the EU electronic communications market

The adaptation of the European approach to regulating the electronic communications market in Ukraine should be considered not as a mechanical transfer of individual provisions of EU legislation, but as a consistent transformation of the regulatory model itself.

Moreover, the regulatory model itself provides for two aspects:

- technical regulation, which aims to resolve network operation issues and ensure compatibility, security, and quality of service provision.
- organizational and administrative regulation that determines the conditions and procedures under which market participants build, use their networks and provide services to ensure conditions for effective competition and stimulate long-term investments

The main task is to transition from predominantly national and operator-centric regulation to a model focused on developing competitive infrastructure, stimulating long-term investments, ensuring network sustainability, and forming a single European electronic communications space.

The European approach, shaped by the European Electronic Communications Code (EECC), has already demonstrated the following logic:

- ex ante regulation is applied primarily where there are persistent competitive bottlenecks ("bottlenecks"), and as competition develops it should be reduced
- Regulation should simultaneously create incentives for investment in very high capacity networks (VHCN), ensure access to infrastructure, and protect the interests of end users.

In 2026, this model will be further developed in the Digital Networks Act (DNA). Its fundamental difference is the shift in emphasis from regulating national electronic communications markets to creating a more integrated European connectivity market capable of supporting AI, cloud and space (satellite) technologies and other infrastructure-intensive digital services. At the same time, DNA aims to reduce market fragmentation, develop cross-border activities of operators, and increase the security and resilience of infrastructure.

For Ukraine, this means the need to consider several interrelated practical areas:

1) transition to regular market analysis and regulation of only persistent competition problems based on the principle of “evidence-based regulation”
2) transition from regulation of services to regulation of infrastructure “bottlenecks”, when the key object of regulation should gradually shift from individual services to infrastructure that cannot be economically duplicated
3) shifting the center of gravity from price regulation to investment stimulation and creating the right balance between the two goals of regulation – competition and investment, i.e. implementing the Investment-friendly regulation + effective competition safeguards model
4) introduction of geographically differentiated regulatory policies taking into account the principles of:
    - competitive areas, i.e. for territories where there are several independent networks and operators.
    - emerging competition areas, i.e. for areas where infrastructure is developing, but competition is still insufficient
    - non-competitive/high-cost areas, i.e. for areas where commercial construction is economically limited
    - critical / resilient areas, i.e. for areas where continuity of communication is of paramount importance
5) creation of a co-investment mechanism as one of the main tools for developing the deployment of ultra-high-capacity networks deployment of ultra-high-capacity networks on the principle that operators jointly create infrastructure and compete at the level of services
6) creation of a unified regime for access to physical infrastructure within the framework of the national system of access to passive infrastructure
7) development of cross-border connectivity as a separate regulatory object within the framework of the single market for connectivity in the following areas:
    - Ukraine → Romania → Bulgaria → Balkans → EU
    - Ukraine → Poland → Central Europe
8) transition from assessing Internet accessibility to assessing the significance and value of communication and connection (meaningful connectivity)
9) developing an understanding that network resilience is an independent regulatory object based on the principle of distributed fault tolerance instead of centralized management
10) creating an understanding that IXP is part of the national regulatory policy and that IXP should be considered as an element of a competitive and sustainable market architecture, while IXP cannot turn into a regulated state monopoly, and its value lies precisely in the neutrality and voluntary interaction of participants
11) preparing the electronic communications market so that the potential of connectivity determines the foundation for the development of AI, cloud and edge infrastructure

4.3. Creating a national Internet Governance 2.0 system

The European connectivity regulatory model is becoming increasingly complex, addressing infrastructure, access, investment, competition, sustainability, artificial intelligence, cloud technologies and cross-border connections at the same time. In 2026 BEREC directly focuses its activities on the consistent application of European regulation, connectivity, the Digital Single Market, an open digital ecosystem and engagement with stakeholders.

Within the framework of this approach, we can talk about a principled position when the concept and activity of "Governance" is separated from the concept and activity of "Regulation".

Today, Ukrainian digital policy is actually divided between several regulatory and institutional spheres:

Stakeholder	Spheres
State	regulation and safety in general
National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services	regulation of electronic communications
State Service of Special Communications and Information Protection of Ukraine	cybersecurity and resilience
Ministry of Digital Transformation of Ukraine	digital transformation
National Centre for Operations and Technology Management of Telecommunications Networks	operating stability circuit
Operators	infrastructure and services
Technical community	protocols, routing, IX, DNS
Academic environment	research and staff training
IGF-UA	multilateral dialogue

Today, within the framework of the current system with the participation of various stakeholders (multistakeholderism) on the IGF-UA platform, the principle of presenting and highlighting accumulated problematic issues once a year, their further discussion on the forum panels, conducting consultations and developing recommendations within the forum, which are not always implemented in the practice of market actors, operates. Relatively speaking, this is the Internet Governance 1.0 system

Therefore, it is urgent to create an institutionalized multilateral system for forming and implementing state policy in the Internet sphere, in which decisions on infrastructure, regulation, security, standardization, and digital transformation are made on the basis of constant interaction between the state, business, technical and academic communities, associations, civil society, etc., conventionally speaking, the Internet Governance 2.0 system.

That is, creating a complete, ongoing policy-making cycle:

data → expert analysis → consultation → joint policy decision → policy implementation → KPI → monitoring → policy adjustment

Formation of a neutral technical and multi-stakeholder advisory platform, for example, within the framework of a new structure - the Ukraine Internet Resilience Council with the participation of central executive bodies, business and industry, the technical community, the scientific (academic) community, specialized public organizations and associations.

The basis of the national Internet Governance 2.0 system is, as before, MULTI-STAKEHOLDERISM, but with one basic addition - its implementation is impossible without creating an ENVIRONMENT OF TRUST (TRUST)

MULTISTAKEHOLDERISM does not work in the absence of TRUST.

The role of the platform should be to provide a neutral architecture for ongoing dialogue based on trust between those who regulate the Internet and those who actually build and operate it.

This platform has a primary organizational goal of becoming a neutral venue that will help:

- to connect Ukrainian state digital policy, operators, IXPs, technical community with the European Internet ecosystem,
- find ways to implement the strategy “from connectivity to resilience → from digital sovereignty to interoperability → from Internet access to reliable AI infrastructure”

by main areas of work:

- National Universal Access Connect,
- National Internet Resilience,
- Interoperable Ukraine and EU Digital Infrastructure,
- Trusted Ukrainian Internet,
- Ukraine AI Internet Infrastructure

Principles of the council's work:

Working principle	Subject
Multistakeholderism	Equal dialogue and consideration of the interests of all parties – the state, business, telecommunications operators, technical experts, scientists, specialized public organizations, associations, etc.
Technological neutrality	Making decisions based on open Internet engineering standards, regardless of specific vendors or political circumstances
Collegiality and transparency	Open nature of discussions, consensus decision-making mechanism and publicity of recommendations made
Inclusivity	Ensuring a balance between national security, economic interests of operators and protection of end-user rights

The goals of the council's work:

Purpose of work	Subject
Ensuring Resilience	Development of strategies to protect the national network from cyberattacks, blackouts, physical damage to infrastructure, and external destructive influences
The development of Internet Governance 2.0	Transition to a modern model of Internet governance at the national level, harmonized with European and global standards (RIPE, ICANN, ISOC)
Expert examination	Acting as an independent advisory body to the government during the preparation of laws, regulations and regulatory rules in the field of electronic communications
Coordination and early warning	Creating a single platform for the prompt exchange of information on threats to communications between the state and private providers
Technological development	Promoting the implementation of advanced security protocols and practices (such as RPKI/ROA, IPv6, DNSSEC) at the national level