Internet Society
Ukraine Chapter

GIGABIT
CHAPTER 2025

Огляд трендів розвитку Інтернет у 2026 році

Виклики для державних органів та операторів

Трансформація, яка неминуча

Огляд підготовлений ГО «Українське відділення всесвітньої Інтернет спільноти»
(ISOC Ukraine Chapter)

Зміст

Вступ

2026 рік став роком змін самої архітектури Інтернету та стратегічного зсуву від простих змін, пов'язаних просто з набором окремих технологічних новин.

Internet Society (ISOC) розглядає Інтернет як глобальну, відкриту, інтероперабельну та децентралізовану інфраструктуру, яка має перетворити ринок цифрових сервісів.

Ринок цифрових сервісів формується непросто як набір доступних сервісів окремих операторів, бо як єдина екосистема, що дозволяє користувачам формувати свої персоналізовані системи необхідних послуг.

У зв'язку з цим величезною проблемою стає питання створення системи довіри до Інтернету, тому що довіра до Інтернету падає – шахрайство, AI-контент, блокування тощо. фактори сприяють цьому.

Не випадково у 2026 році в центрі стратегії ISOC знаходяться два системні виклики: глобальна нерівність та падіння довіри до Інтернету.

Інтернет у 2026 році вступає у новий етап свого розвитку. Якщо протягом попередніх десятиліть його ключовою функцією було забезпечення глобального зв'язку та доступу до інформації, то сьогодні Інтернет стає базовою інфраструктурою економіки, державного управління, штучного інтелекту, критичних сервісів та повсякденного життя суспільства. Одночасно змінюється сама архітектура цифрового простору: стрімко зростають обсяги машинного та AI-трафіку, розвивається розподілена обчислювальна інфраструктура, посилюється роль дата-центрів, хмарних платформ, магістральних та транскордонних мереж, а питання кібербезпеки, стійкості та довіри стають невіддільними від фун.

Ці технологічні зміни відбуваються на тлі посилення геополітичної фрагментації та конкуренції за контроль над цифровою інфраструктурою. Держави прагнуть забезпечити цифровий суверенітет, локалізувати критичні дані та обчислювальні ресурси, знизити залежність від зовнішніх постачальників та захистити національну інфраструктуру від кібератак та фізичних загроз. Однак надмірна централізація та фрагментація цифрового простору створюють новий ризик – поступове руйнування тих властивостей, які зробили Інтернет глобальною системою: відкритості, інтероперабельності, розподіленості та можливості вільної взаємодії різних мереж та учасників.

Саме в цьому контексті особливого значення набуває позиція Internet Society (ISOC), що розглядає Інтернет як глобальну, відкриту, надійну та стійку інфраструктуру, розвиток якої має ґрунтуватися на інтероперабельності, розподіленості, безпеці та багатосторонньому управлінні. На порядку денному ISOC 2026 року особливе місце займають значне місце зв'язність (коннективіті), доступність та надійність інфраструктури, розвиток локальних IXP, безпека маршрутизації, довіра до Інтернету, захист відкритої архітектури мережі та протидія її фрагментації.

Для України ці глобальні зміни мають не лише технологічне, а й стратегічне значення. В умовах війни стійкість електронних комунікацій безпосередньо

пов’язана з національною безпекою, функціонуванням економіки, державних сервісів, енергетики, логістики та соціальної інфраструктури. Одночасно інтеграція України до Європейського цифрового ринку відкриває можливість перейти від моделі периферійного підключення до європейської інфраструктури до формування повноцінних транскордонних цифрових коридорів та регіональних вузлів зв’язку.

Тому стратегічне завдання України на наступному етапі полягає не лише у відновленні пошкодженої інфраструктури чи збільшенні пропускної спроможності мереж. Необхідно сформувати таку архітектуру національної Інтернет-інфраструктури, яка одночасно забезпечувала б стійкість, інтероперабельність, безпеку, довіру та здатність до технологічного розвитку, зберігаючи при цьому повноцінну інтеграцію України до європейського та глобального Інтернету.

У зв’язку з цим цифровий суверенітет України доцільно розглядати не як ізоляцію від глобального цифрового середовища, а як здатність самостійно забезпечувати безперервність функціонування критичної цифрової інфраструктури, обирати між альтернативними постачальниками та маршрутами, забезпечувати захист власних ресурсів та одночасно зберігати сумісність із глобальними та європейськими технологічними стандартами. Інакше кажучи, стратегічною метою стає не «суверенний Інтернет», а суверенітет через інтероперабельність.

Саме такий підхід дозволяє сформувати нову стратегічну рамку розвитку українського Інтернету: від відновлення окремих мереж до побудови розподіленої та сталої інфраструктури; від локального доступу – до повноцінного європейського зв’язку; від традиційних телекомунікаційних мереж – до інфраструктури, готової до AI та кіберфізичних систем; від переважно захисної моделі до створення Trusted Internet Infrastructure.

У цій перспективі Україна має можливість не лише адаптуватися до глобальних змін, а й зайняти більш значущу позицію у європейській цифровій екосистемі – як країна з розвиненою системою IXP, транскордонних оптичних маршрутів, дата-центрів, розподіленою обчислювальною інфраструктурою та компетентною технічною спільнотою.

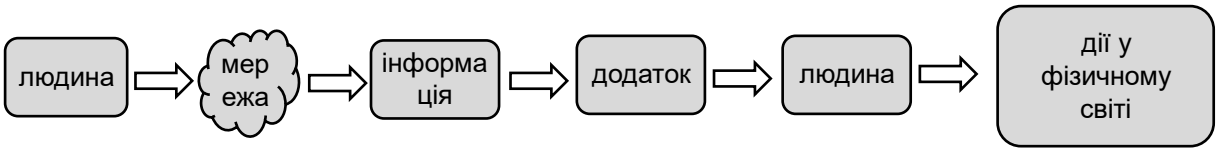
Відтак питання найближчих років полягає вже не в тому, як підключити Україну до глобального Інтернету, а в тому, як зробити Україну стійкою, інтероперабельною та довіреною частиною європейської та глобальної Інтернет інфраструктурою в епоху AI, цифрового суверенітету та геополітичної фрагментації.

Відповідь на це питання вимагає переходу від окремих інфраструктурних проектів до комплексної стратегії, що об’єднує державну політику, розвиток електронних комунікацій, транскордонну інфраструктуру, IXP, кібербезпеку, цифрову довіру, AI-інфраструктуру, науково-освітній потенціал та принципи багатостороннього управління Інтернетом (мультістейкхолдеризм).

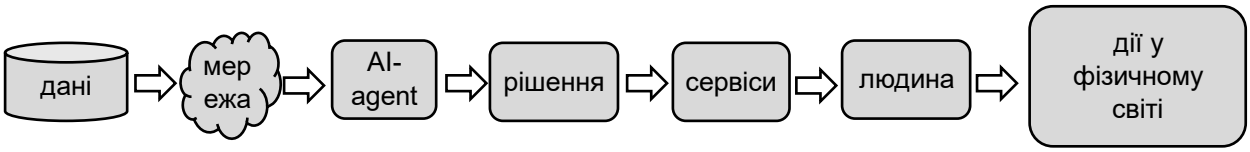
1. Головні тренди 2026 року

1.1. Інтернет переходить від «мережі інформації» до «інфраструктури прийняття рішень»

Класична взаємодія в Інтернеті можна було умовно описати як систему взаємодії



У 2026 році формується нова модель взаємодії:



Це важливий перехід.

AI стає не просто додатком поверх Інтернету. Він починає визначати:

- які дані будуть отримані;
- які послуги будуть викликані;
- який маршрут чи ресурс буде обрано;
- яке рішення буде ухвалено;
- які дії будуть автоматично виконані.

Тому AI поступово стає новим споживачем та водночас новим оператором Інтернет-інфраструктури.

IEEE також характеризує 2026 як перехід до інтелектуальної, програмно-керованої зв'язності (intelligent, software-driven connectivity), де AI інтегрується безпосередньо в управління мережами. (IEEE Standards Association)

Головним об'єктом конкуренції стає вже не просто доступ до Інтернету, а поєднання факторів:

обчислення + зв'язність + дані + ШІ + енергетика

(compute + connectivity + data + AI + energy)

1.2. AI перетворюється на інфраструктурний шар Інтернету

У 2026 році можна виділити три послідовні стадії:

Період	AI-модель
2023–2024	Generative AI
2025	Agentic AI

2026	Distributed AI / AI inference infrastructure

Відбувається перехід від «де знаходиться модель?» до «де у реальному часі виконується inference?»

Це означає розвиток:

- edge AI;
- AI PoP;
- regional inference;
- GPU clusters;
- AI-ready data centers;
- distributed compute;
- AI networking;
- високошвидкісні міжконтакти.

IDC 2026 року прямо зазначає, що для телеком-сектору критичний перехід походить від навчання моделей до real-time distributed inference, що змушує операторів переглядати архітектуру інфраструктури.

Наслідком цього є те, що телекомунікаційна мережа поступово стає інфраструктурою обчислювального зв'язку (Compute Connectivity Infrastructure), а не просто транспортом IP-пакетів.

1.3. Інтернет стає фізично обмеженим

Це одна з найбільш недооцінених тенденцій.

AI вимагає величезної кількості:

- електроенергії;
- GPU;
- охолодження;
- оптичних каналів;
- дата-центрів;
- міжнародних магістралей.

Тому виникає нова залежність:

AI → ЦОД → енергетика → ВОЛЗ → зв'язок

Тобто, цифрова економіка знову стає залежною від фізичної інфраструктури.

Це змінює стратегічне значення:

- підводних кабелів
- DWDM
- наземних ВОЛЗ
- IXP

- технологій об'єднання дата-центрів (Data Center Interconnect – DCI)
- дата-центрів
- регіональних PoP
- питання енергогенерації.

Саме тому сьогодні дата-центр не можна розглядати лише як IT-об'єкт, він стає частиною критичної інфраструктури держави.

1.4. Централізація Інтернету стає одним із головних системних ризиків

ISOC зазвичай вважає небезпекою надмірну концентрацію інфраструктури, послуг і контролю у кола небагатьох суб'єктів.

У 2026 році це проявляється відразу в кількох шарах:

Шар або сервіс інфраструктури	Загроза
Cloud	Декілька глобальних hyperscalers
AI	Обмежена кількість компаній контролює найбільш потужні моделі та GPU-інфраструктуру
DNS/CDN	Концентрація значної частини інфраструктури у великих глобальних гравців
Peering	Зростання залежності від великих транзитних та cloud-провайдерів
Platforms	Концентрація користувача та інформаційного середовища

ISOC у своїх матеріалах 2026 року окремо звертає увагу на ризики централізації та, наприклад, аналізує проблему централізованого та віртуального пірингу як загрозу стійкості Інтернету. (Internet Society)

1.5. IXP – вже не просто економічний інструмент

Класична логіка розвитку та роботи IXP:

IXP → локальний трафік → менша затримка → менші транзитні витрати

Нова логіка:

IXP → локальний трафік → стійкість → цифровий суверенітет → безперебійність роботи критично важливих служб

Саме тому ISOC в Action Plan 2026 прямо пов’язує:

місцева інфраструктура пірінгу → доступність → надійність → відмовостійкість

local peering infrastructure → affordability → reliability → resilience

та планує підтримку та розвиток локальних IXP, навчання технічних спільнот та локалізацію трафіку. (Internet Society)

Тобто IXP стає елементом національної архітектури відмовостійкості.

Для України це особливо суттєво і формула:

IXP + кілька точок присутності (PoP) + кілька оптоволоконних маршрутів + регіональне міжмережеве з’єднання

може розглядатися як механізм створення розподіленого національного відмовостійкого Інтернету.

1.6. Цифровий суверенітет

Тренд на цифровий суверенітет (Digital Sovereignty) породжує дуже цікавий конфлікт, коли держави кажуть:

«Нам потрібна цифрова незалежність»

а на практиці відбувається перетворення цифрового суверенітету на фрагментацію Інтернету.

ISOC безпосередньо розглядає зростання політики, яка намагається встановити географічні кордони для глобального Інтернету.

Виникає суттєва суперечність, коли державна логіка розглядає суверенітет як контроль та управління, а логіка технологічного середовища та середовища управління (Internet Governance) Інтернету розглядає суверенітет як комбінацію спрямовану на створення середовища:

вибір + стійкість + сумісність

choice + resilience + interoperability

Це різні концепції.

1.7. Виникнення нової концепції: «sovereignty without isolation»

Одна з найважливіших концептуальних тенденцій 2026 року.

Сильна цифрова система – це не ситуація, коли ми все побудуємо самі, а ми здатні продовжувати роботу, навіть якщо частина зовнішньої інфраструктури недоступна.

Тобто:

суверенітет ≠ ізоляція

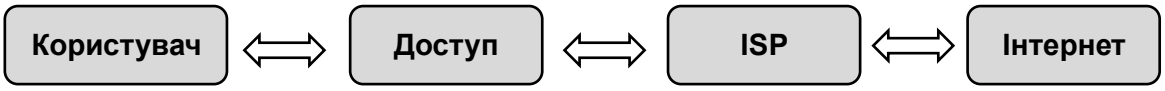
а:

суверенітет = здатність вибирати + здатність перемикатися + здатність взаємодіяти

Саме таку логіку можна побачити і в дискусіях ISOC Chapters щодо sovereign technology: контроль над власною інфраструктурою має поєднуватися із збереженням відкритих дверей для співпраці. (Internet Society Singapore Chapter)

1.8. Інтернет стає багатошаровим

Архітектурно в 2026 році Інтернет все менше схожий на просту модель:



Формується кілька структурних шарів (Рисунок 1).

Шар AI / Agents – найвищий рівень: додатки та сервіси (включаючи AI та агентів), які працюють поверх мережевої інфраструктури. Це споживачі, що забезпечують нижні шари.

Шар Cloud/SaaS – хмарні платформи та програмне забезпечення як послуга, на яких працюють програми верхнього шару.

Шар Data/Identity – рівень даних та ідентифікації (управління доступом, ідентифікація, авторизація та аутентифікація, зберігання та обробка даних).

Шар Internet – ключова точка, звідки мережа розходиться на два основні шляхи доступу до користувачів:

- Mobile та Satellite – мобільні мережі, включаючи супутниковий доступ.
- Fixed Fiber та Local PoP – фіксовані оптоволоконні мережі через місцеві точки присутності (Point of Presence).

Шар IXP/Peering, де оператори обмінюються даними безпосередньо

Шар Regional backbone – регіональна магістральна мережа, що поєднує трафік на рівні регіону.

International backbone – міжнародні оптоволоконні магістралі, що зв'язують регіони за допомогою підводних та наземних кабелів та є фізичною основою глобального зв'язку між континентами.

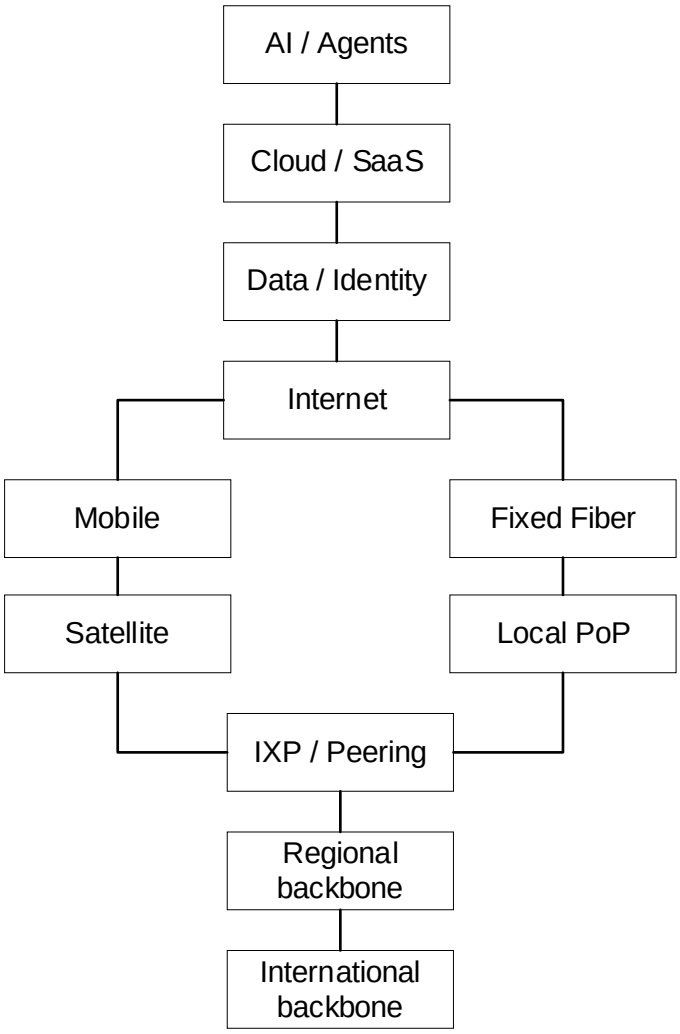


Рисунок 1. Схема структурних шарів Інтернету

При цьому кожен шар стає потенційною «пляшковою шийкою».

1.9. Супутниковий інтернет змінює поняття «останньої милі»

У 2026 році наземний, мобільний та супутниковий зв'язок починають розглядатися не як конкуруючі технології, а як єдина гібридна архітектура підключення, для якої особливо важливі:

- низькоорбітальні супутники (LEO);
- пряме підключення до супутників (direct-to-device)
- супутниковий магістральний зв'язок (satellite backhaul)
- наземна інфраструктура ВОЛЗ (terrestrial fiber)
- технології 5G/5G Advanced
- майбутня 6G архітектури.

Таким чином, доступ до інтернет перестає бути прив'язаним до одного фізичного рішення в даній точці для даного користувача.

Це надзвичайно важливо для України в умовах необхідності вирішення завдань:

- відновлення зв'язку після стихійних лих та руйнувань
- забезпечення зв'язку у сільських районах

- забезпечення морського зв’язку
- забезпечення зв’язку у надзвичайних ситуаціях.

1.10. Стійкість стає важливішою за швидкість

Це, мабуть, головне зрушення у філософії Інтернет-інфраструктури.

Період	Головний критерій
У 2010-х	Наскільки швидка мережа?
У 2020-х	Наскільки безпечною є ця мережа?
У 2026	Чи зможе мережа продовжувати роботу за умов навантаження?

З’являється поняття інженерія забезпечення відмовостійкості Інтернету (Internet resilience engineering), яке включає:

- різноманітність маршрутів (diversity of routes)
- різноманітність провайдерів (diversity of providers)
- IXP;
- локальний піринг (local peering)
- множинність ап-стрімів (multiple upstreams)
- резервування DNS (redundant DNS)
- резервоване електроживлення (redundant power)
- розподілені точки присутності (distributed PoPs)
- резервне супутникове з’єднання (satellite backup)
- кіберстійкість (cyber resilience)
- мережі спільнот (community networks)

ISOC фактично ставить стійкість (resilience) поряд з доступністю зв’язку та зв’язністю (connectivity) та ціновою доступністю (affordability). В Action Plan прямо підкреслюється роль IXP у збереженні бізнесу онлайн та стійкості інфраструктури.

1.11. Довіра стає інфраструктурою

ISOC ясно формулює, що Інтернет повинен бути не тільки доступним, але й безпечним, надійним і заслуговує на довіру, тому в 2026 році недостатньо мати зв’язність.

Тому довіра (trust) поступово стає інфраструктурною властивістю, яка комплексно має включати:

- шифрування (encryption)
- RPKI (Resource Public Key Infrastructure)
- безпечну маршрутизацію (secure routing)
- безпека системи доменних імен (DNS security)
- приватність та конфіденційність (privacy)
- ідентифікацію (identity)

- боротьбу із шахрайством (anti-fraud)
- кіберстійкість (cyber resilience)
- безпека програмного забезпечення (secure software)
- безпека штучного інтелекту (AI safety).

Іншими словами, безпека перестає бути окремим сервісом, а стає частиною самої архітектури мережі.

1.12. Шифрування стає геополітичним питанням

Internet Society продовжує розглядати шифрування як фундаментальний елемент довіри в екосистемі Інтернету та прямо пов'язує шифрування з конфіденційністю та безпекою.

Проблему 2026 року можна сформулювати в цьому аспекті, як держава хоче контролювати злочинність, тероризм, AI, дезінформацію, а користувач повинен мати захищену комунікацію.

Це породжує постійний тиск на:

- наскрізне шифрування (end-to-end encryption)
- зашифрований обмін повідомленнями (encrypted messaging)
- анонімність (anonymity)
- технології, що підвищують рівень конфіденційності (privacy-enhancing technologies)

1.13. Відключення інтернету стає окремим глобальним ризиком

Дуже показово, що у серпні 2026 року Internet Society випустила окремий матеріал: **Shutdown Trends from 2019 to 2025: Where Do We Go from Here**.

ISOC розглядає відключення вже не як виняткові політичні події, а як системну загрозу глобальному Інтернету.

Актуальним стає важлива концепція: мережа availability becomes a human-rights and economic continuity issue (доступність мереж стає питанням правами людини і забезпечення безперервності економічної діяльності).

Тобто відключення Інтернету означає не просто, наприклад, ситуацію що «люди не можуть зайти до Facebook», а породжує ланцюжок переривання нормального життєзабезпечення сучасної людини:

платіжні системи → логістика → охорона здоров'я → державні органи → освіта → бізнес → служби екстреної допомоги тощо

1.14. AI створює новий тип інтернет-трафіку

Історично Інтернет був орієнтований на трафік, що генерується людьми. Тепер швидко зростає трафік, що генерується самою "системою машин", джерелом якого є:

- ШІ-агенти (AI agents)
- пошукові роботи (crawlers)
- процедури для машинного виведення та резолвінгу (inference)
- процедури взаємодії «машина-машина» (machine-to-machine)
- IoT;
- автономні системи (autonomous systems)

Через війну з'являється Інтернет автономних агентів.

І тут постає зовсім нове питання – хто є суб'єктом Інтернет-комунікації: людина? додаток? AI-агенти? IoT пристрої? автономні транспортні засоби? процедури цифрової ідентифікації?

Те, що було юридичним питанням прав та довіри до контенту, стає питанням архітектури.

1.15. Об'єднання тріади Інтернет + IoT + AI та формування кіберфізичного Інтернету (Cyber-Physical Internet)

Кіберфізичний Інтернет (Cyber-Physical Internet) сприймається як наступна стадія розвитку Інтернет. Відбувається об'єднання технологій та засобів обробки інформації та прийняття рішень, що дозволяє перейти від тріади Internet + IoT + AI перейти до якісно нового етапу розвитку у вигляді кіберфізичних систем (Cyber-Physical Systems)

Тобто Інтернет починає керувати:

- автомобілями;
- енергетикою;
- промисловістю;
- логістикою;
- роботами;
- медичними пристроями;
- розумні міста.

Тому помилка 2026 року вважати Інтернет виключно комунікаційною інфраструктурою, тому що Інтернет стає інфраструктурою управління реальною економікою.

2. Головний конфлікт 2026 року

Якщо звести світові тенденції до однієї діаграми (Рисунок 2), яка ілюструє дилему розвитку інтернету: чи буде майбутнє побудовано за принципами централізації (зручність для гігантів) чи принципах розподіленості (рівноправності учасників). Будь-який шлях визначає прагнення до цифрового суверенітету, який можна досягти через контроль і фрагментацію, або через свободу вибору і сумісність. Кінцева мета обох підходів – стійка мережа, у якій реалізовано властивість та середовище довіри.

Ключова думка, яку ілюструє діаграма – напруга між цілісністю відкритої мережі та зростаючим прагненням до національного та корпоративного контролю,

запитуючи: чи можна зберегти довіру та стійкість, не пожертвувавши при цьому відкритістю?

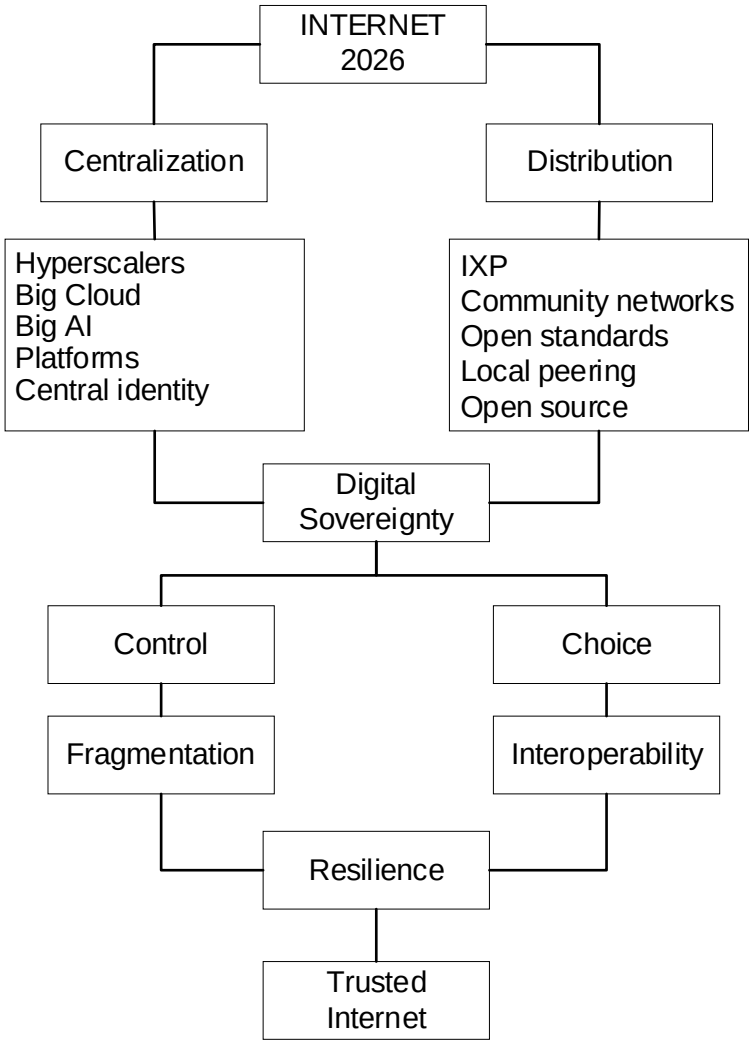


Рисунок 2. Діаграма ілюстрації дилеми розвитку інтернет

На першому рівні розглядається конфлікт між централізацією та розподіленістю. Це головна розвилка – два протилежні шляхи подальшого розвитку мережі.

Централізація, коли один центр керує всім, визначає домінування:

- Hyperscalers – гігантські хмарні провайдери (Amazon, Google, Microsoft)
- Big Cloud – великі хмарні платформи
- Big AI – великі гравці у сфері ШІ
- Platforms – домінуючі платформи (соцмережі, маркетплейси та сервісні екосистеми)
- Central identity – єдина система ідентифікації під одним контролем

Розподіл, коли влада розосереджена між учасниками, визначає управління елементами:

- IXP – точки обміну інтернет-трафіком (де мережі з'єднуються безпосередньо)
- Community networks – локальні мережі, керовані спільнотами

- Open standards – відкриті технічні стандарти
- Local peering – прямі з'єднання між сусідніми мережами без посередників
- Open source – програмне забезпечення з відкритим кодом

Другий рівень у аналізованої діаграмі пов'язані з потенціалом цифрового суверенітету (Digital Sovereignty), коли обидві гілки конфлікту сходяться у спільній точці.

Це означає, що незалежно від обраного шляху, держави та спільноти прагнуть цифрового суверенітету та контролю над своїми даними, технологіями та інфраструктурою.

На третьому рівні розглядається конфлікт між управлінням (Control) та вибором (Choice), що є ще одним розвилкою всередині суверенітету.

Шлях контролю (суверенітет через обмеження) визначає дії уряду та регулятора як спрямовані на фрагментацію, тобто. роздробленість (різні регіони з несумісними системами)

Шлях вибору (суверенітет через повноваження) визначає дії уряду та регулятора як спрямовані на интероперабельность, тобто. здатність систем взаємодіяти один з одним

Обидві гілки (управління та вибір) ведуть до спільної мети, але вони визначають реалізацію державних регуляторних політик у підсумкових точках:

- resilience – стійкість (здатність мережі переживати збої, атаки та кризи)
- trusted Internet – інтернет-середовище з екосистемою довіри

У визначенні вибору між або поєднанням політик централізації та розподіленості розвиватиметься Інтернет найближчих 5–10 років.

Тому ISOC фактично захищає не «старий Інтернет», а певну архітектурну модель майбутнього Інтернету, яка має відповідати архітектурним принципам:

Принцип	Сенс	Властивості майбутнього Інтернету
Open	відкритий Інтернет	1. community networks 2. IXP 3. open standards 4. encryption 5. multistakeholder governance 6. local Internet infrastructure 7. meaningful connectivity
Global	глобальна зв'язність	
Interoperable	інтероперабельність	
Distributed	розподіленість	
Trusted	безпека та довіра	

Це не окремі напрямки. Це є елементи однієї архітектурної моделі. (Internet Society)

3. Підсумкова аналітична формула 2026 року

Світова трансформація Інтернету:

Період	Формула розвитку	У чому успіх
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 у 2026 році фактично пропонує відповідь на глобальну тенденцію централізації:

Не боротися з технологічним розвитком, а не дозволити технологічному розвитку зруйнувати архітектурні властивості Інтернету

Ключові пріоритети, які розглядає ISOC за підсумками 2026 року, можна звести до чотирьох:

1. Connect

Підключити тих, хто залишається поза Інтернетом

2. Localize

Розвивати локальну інфраструктуру, IXP та піринг

3. Protect

Захищати шифрування, конфіденційність, безпеку та довіру в Інтернеті

4. Keep Open

Не допустити фрагментації Інтернету під виглядом цифрового суверенітету

4. Що це означає для України

Для України ці світові тренди складаються особливо цікаво.

Україна може бути не лише споживачем глобальної цифрової інфраструктури, а й регіональним елементом європейської Інтернет-інфраструктури.

Стратегічно найперспективніша модель, що реалізує трансформацію інтернет простору України в один із центрів цифрового зв'язку ЄС з компонентами IXP,

регіональних PoP, південно-західний перехід до Румунії, Болгарії та Балкан з подальшою інтеграцією в європейський бекбон.

Це дозволить розглядати дії, спрямовані на реалізацію такої моделі, вже не просто як телеком-проекти, а позиціонувати їх як:

Регіональна інфраструктура забезпечення відмовостійкості Інтернету

Regional Internet Resilience Infrastructure

і одночасно:

Цифровий суверенітет через взаємодію та сумісність систем

Digital Sovereignty through Interoperability

Якщо перекласти це мовою стратегічного планування, то головне питання вже не

Як підключити Україну до Інтернету?

а

Як зробити український сегмент стійкою, інтероперабельною та довіреною частиною європейської та глобальної інфраструктури інтернету в епоху ШІ, цифрового суверенітету та геополітичної фрагментації?

У логіці реалізації це може бути національна програма стійкості та інтероперабельності Інтернету, що об'єднує державу, операторів, IXP, технічну спільноту, університети та бізнес.

Причому Україна вже має хорошу відправну точку: у 2025 році затверджено Стратегію розвитку електронних комунікацій до 2030 року, яка передбачає gigabit connectivity, 5G, цифрову стійкість та інтеграцію до EU Digital Single Market. А з 1 січня 2026 року Україна вже перебуває в режимі EU Roam Like at Home – тобто інтеграція перестала бути лише декларативною (digital-strategy.ec.europa.eu).

4.1. Кроки реалізації

4.1.1. Імплементація принципу «Суверенітет через взаємодію та сумісність» (Sovereignty through Interoperability)

Імплементація принципу «Суверенітет через взаємодію та сумісність» – ідеологічний центр цифрової політики країни. Відкритий та глобальний Інтернет повинен зберігати інтероперабельність, одночасно стаючи більш стійким та довіреним.

Відхід від принципу «Країна повинна мати власний Інтернет» та перехід до принципу «Країна повинна мати можливість вибирати, перемикатися та продовжувати роботу без втрати сумісності з глобальним Інтернетом»:

Область	Вимога суверенітету
DNS	кілька незалежних рівнів
Transit	≥3 незалежні напрямки
IXP	розподілені
Cloud	мультихмарна
Fiber	різноманітність маршрутів
Data centers	географічне розмаїття
AI	розподілені обчислення
Identity	сумісні принципи
DNS/CDN	кілька постачальників
Mobile	кілька операторів
Satellite	резервне підключення

4.1.2. Перехід від «відновлення мереж» до національної архітектури забезпечення відмовостійкості Інтернету

Завдання: побудувати розподілену, надмірну та здатну до автономної роботи Інтернет-інфраструктуру України.

Це означає створення національної карти критичних Інтернет-ресурсів:

- магістральні ВОЛЗ
- міжнародні переходи
- підводні/наземні маршрути
- IXP
- дата-центри
- DNS інфраструктура
- хмарна інфраструктура
- інфраструктура штучного інтелекту
- мобільний зв’язок
- критичні PoP
- Значення енергетики.

Для кожного елемента необхідно визначити primary, secondary, emergency маршрути з N-1 / N-2 стійкістю, тобто. здатністю продовжувати роботу після відмови одного чи кількох незалежних елементів.

4.1.3. Створення системи розподіленого міжмережевого з’єднання в Інтернеті (Distributed Internet Interconnection)

Україна має мати багато «національних IXP», які утворюють розподілену систему взаємопов'язаних IXP/PoP.

Функціонально IXP повинен розглядатися як майданчик, який забезпечує роботу:

- розподіленого пірингу (distributed peering)
- BGP
- RPKI
- серверів маршрутизації (route server)
- IPv4/IPv6
- BGP communities
- пом'якшення наслідків DDoS
- аналізу трафіку
- міжхмарного з'єднання (cloud interconnection)
- CDN з'єднання (CDN interconnection).

Це повністю відповідає логіці розвитку надійності та стабільності Інтернету, коли локальний піринг підвищує доступність, надійність та стійкість Інтернету.

4.1.4. Інтеграція в європейську архітектуру оптоволоконних мереж

Україна не має бути кінцевою точкою європейської мережі Інтернет, а має стати транзитним регіональним вузлом.

Особливо важливими є коридор південний захід (south-west corridor), що включає маршрут Ukraine – Danube – Romania – Balkans – Central Europe, та західний коридор (western corridor), що включає маршрут Ukraine – Poland – Germany / Baltic region

Це означає розвиток:

- крос-граничні телеком-переходи
- DWDM;
- різноманітних маршрутів оптоволоконних ліній
- крос-граничні PoP
- об'єктів, незалежних від операторів зв'язку
- міжнародних IXP
- з'єднань між дата-центрами.

Фактично, постановка завдання визначає створення «Коридор цифрової стійкості ЄС – Україна» (EU – Ukraine Digital Resilience Corridor).

4.1.5. Інтеграція українського регулювання не лише юридично, а й технічно

Використати досвід інтеграції в EU роумінг, який став першим прикладом застосування внутрішнього ринку ЄС до України у цифровій сфері (digital-strategy.ec.europa.eu)

Наступний рівень – це перехід від правового узгодження (legal alignment) до політики нормативної та технічної сумісності (regulatory + technical interoperability).

Пріоритети	Напрями, завдання
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

У 2026 році розпочалися дії щодо імплементації Україною положень Interoperable Europe Act; серед напрямів визначено національну рамку інтероперабельності, транскордонних цифрових послуг та інтеграції рішень до європейської екосистеми. (НІСД/NISS)

4.1.6. Створення довірчої Інтернет-архітектури (Trusted Internet Architecture)

Фундаментальна вимога без якої неможлива реалізація нової архітектури інтернету, яка має на меті перехід від поняття “кібербезпека як засіб захисту” (cybersecurity as protection) до поняття “довіра, закладена в архітектуру Інтернету” (trust embedded into Internet architecture).

Мінімальні та вихідні вимоги для реалізації такого підходу до архітектури включають створення процедур, що визначають довіру щодо:

- IPv4/IPv6
- DNS (DNSSEC, TLS)
- BGP (RPKI)
- захист від DDoS
- суворої ідентифікації
- ведення журналів/моніторингу
- реагування на інциденти

Особливо важливо зробити RPKI практично обов'язковим елементом професійної мережевої інфраструктури з реалізацією ланцюжка дій:

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

яка описує стандартний процес захисту глобальної маршрутизації в інтернеті від перехоплення трафіку (BGP Hijacking) та витоків маршрутів (Route Leaks), гарантуючи, що трафік піде лише легітимними маршрутами

А також створити національну систему моніторингу роботи Інтернет, що покриває моніторинг BGP, DNS аномалії, моніторинг затримок та збоїв у роботі мережі, трафіку IX та крос-граничних переходів

4.1.7. Підготовка до AI Internet

Це те, чого поки що недостатньо у традиційній українській стратегії розвитку електронних комунікацій.

У 2026 році Кабінет Міністрів України та Мінцифри включили питання про перехід до стратегії зв'язності для ШІ (Agentic State) та AI security як пріоритетні для цифрової повістки.

Для цього потрібно створювати інфраструктурний шар AI Connectivity Strategy, який визначає технологічний та організаційний розвиток як єдину розподілену архітектуру:

Data Center → IXP → Backbone → Cloud → AI Compute

Пріоритетами розвитку з технологічної точки зору визначаються:

Пріоритет	Роль
Обчислювальний рівень	
Регіональні обчислювальні ресурси ШІ	Донавчання моделей (Fine-Tuning) під конкретні локальні ринки/мови та для ресурсомісткого інференсу з низьким часом відгуку, локалізація даних, розвантаження центральних хабів
Кластери GPU (GPU clusters)	Об'єднання безлічі графічних процесорів в єдиний мережевий суперкомп'ютер
Периферійний ШІ (edge AI)	Забезпечення миттєвого інференсу для критично важливих програм: безпілотний транспорт, розумні заводи, камери безпеки, медичне обладнання
Дата-центри, готові до навантажень ШІ (AI-ready data centers)	Забезпечення охолодження Direct-to-Chip для гарячих GPU, безперебійного живлення та архітектури залів, оптимізоване під надщільне прокладання оптичних кабелів

Пріоритет	Роль
Мережевий рівень	
Високошвидкісна оптична комутація всередині ЦОД (high-speed optical interconnect)	З'єднання GPU всередині стійок і між ними з використанням оптичних трансіверів для передачі терабіти даних з мінімальним тепловиділенням та енергоспоживанням, за винятком мережевих заторів при паралельних обчисленнях
400G/800G	Перехід на порти 400Gbps та 800Gbps, а в перспективі і 1,6T та скорочення кількості фізичних кабелів та портів на комутаторах, спрощуючи архітектуру мережі Spine-Leaf
Зв'язок між ЦОД (Data Center Interconnect)	Розподіл фаз навчання чи інференсу між різними ЦОД, зв'язність ЦОД на величезних швидкостях та резервування маршрутів
Маршрути з мінімальною затримкою (low-latency routes)	Використання найкоротших оптичних трас (пряме волокно без зайвих транзитних вузлів) та оптимізацію протоколів маршрутизації з метою прискорення синхронізації GPU та зменшення загального часу навчання моделі

4.2. Практичні кроки щодо реалізації підходів до регулювання ринку електронних комунікацій ЄС

Адаптація європейського підходу до регулювання ринку електронних комунікацій в Україні має розглядатись не як механічне перенесення окремих положень законодавства ЄС, а як послідовна трансформація самої моделі регулювання.

Причому сама модель регулювання передбачає два аспекти:

- технічне регулювання, яке має на меті вирішення питань роботи мережі та забезпечення в ній сумісності, безпеки та якості надання послуг.
- організаційно-адміністративне регулювання, яке визначає на яких умовах та за якими процедурами учасники ринку будують, використовують свої мережі та надають послуги для забезпечення умов ефективної конкуренції та стимулювання довгострокових інвестицій

Основне завдання полягає у переході від переважно національного та операторо центричного регулювання до моделі, орієнтованої на розвиток конкурентної інфраструктури, стимулювання довгострокових інвестицій, забезпечення стійкості мереж та формування єдиного європейського простору електронного зв'язку.

Європейський підхід, сформований Європейським кодексом електронних комунікацій (EECC), уже продемонстрував таку логіку:

- попереднє регулювання застосовується насамперед там, де існують стійкі конкурентні вузькі місця («пляшкові шийки»), а з розвитком конкуренції воно має скорочуватися
- регулювання має одночасно створювати стимули для інвестицій у мережі надвисокої пропускної спроможності (VHCN), забезпечувати доступ до інфраструктури та захищати інтереси кінцевих користувачів.

У 2026 році ця модель отримує подальший розвиток у положеннях Digital Networks Act (DNA). Його принципова відмінність полягає у зміщенні акценту від регулювання національних ринків електронних комунікацій до створення більш інтегрованого європейського ринку можливостей підключення (connectivity), здатного підтримувати AI, хмарні та космічні (супутникові) технології та інші інфраструктурно-ємні цифрові сервіси. Одночасно DNA спрямована на зниження фрагментації ринку, розвиток транскордонної діяльності операторів, підвищення безпеки та стійкості інфраструктури.

Для України це означає необхідність розгляду кількох взаємопов'язаних практичних напрямів:

1) перехід до регулярного аналізу ринків та регулювання лише стійких конкурентних проблем на основі принципу "evidence-based regulation"
2) перехід від регулювання послуг до регулювання інфраструктурних "пляшкових шийок", коли ключовий об'єкт регулювання повинен поступово зміщуватися від окремих послуг до інфраструктури, яку неможливо економічно ефективно дублювати
3) перенесення центру тяжкості з цінового регулювання на стимулювання інвестицій та створення правильного балансу між двома цілями регулювання – competition та investment, тобто реалізація моделі Investment-friendly regulation + effective competition safeguards
4) запровадження географічно диференційованих політик регулювання з урахуванням принципів:
   - competitive areas, тобто для територій, де є кілька незалежних мереж і операторів.
   - emerging competition areas, тобто для територій, де інфраструктура розвивається, але конкуренція ще недостатня
   - non-competitive/high-cost areas, тобто для територій, де комерційне будівництво економічно обмежене
   - critical / resilient areas, тобто для територій, де першорядне значення має безперервність зв'язку
5) створення механізму співінвестування одним із основних інструментів розвитку розгортання мереж надвисокої пропускної спроможності розгортання мереж надвисокої пропускної спроможності на принципі – оператори спільно створюють інфраструктуру, а конкурують на рівні послуг та сервісів
6) створення єдиного режиму доступу до фізичної інфраструктури в рамках національної системи доступу до пасивної інфраструктури
7) розвиток cross-border connectivity як окремого об'єкта регулювання в рамках єдиного ринку можливостей підключення (connectivity) у рамках напрямків:

- Ukraine → Rumania → Bulgaria → Balkans → EU
- Ukraine → Poland → Central Europe

8) перехід від оцінки доступності Інтернету (Internet accessibility) до оцінки значущості та цінності зв'язку та підключення (meaningful connectivity)
9) формування розуміння, що стійкість мережі є самостійним об'єктом регулювання на принципі – розподілена стійкість до відмов замість централізованого управління
10) формування розуміння, що IXP є частиною національної політики регулювання та IXP слід розглядати як елемент конкурентної та стійкої архітектури ринку, при тому, що IXP не може перетворюватися на регульовану державну монополію, а його цінність саме у нейтральності та добровільній взаємодії учасників
11) підготовка ринку електронних комунікацій до того, що потенціал можливостей підключення визначає фундамент для розвитку AI, cloud та edge infrastructure

4.3. Створення національної системи Internet Governance 2.0

Європейська модель регулювання у сфері можливості підключення (connectivity) стає дедалі складнішою: одночасно вирішуються питання інфраструктури, доступу, інвестицій, конкуренції, сталого розвитку, штучного інтелекту, хмарних технологій та транскордонних з'єднань. У 2026 році BEREC прямо орієнтує свою діяльність на послідовне застосування європейського регулювання, можливості підключення, Єдиного цифрового ринку, відкритої цифрової екосистеми та взаємодії зі стейкхолдерами.

У рамках цього підходу можна говорити про принципове положення, коли відбувається відокремлення поняття та діяльності «Governance» від поняття та діяльності «Regulation».

Сьогодні українська цифрова політика фактично розподілена між кількома регуляторними та інституційними сферами:

держава	регулювання та безпека в цілому
НКЕК	регулювання електронних комунікацій
Держспецзв'язку	кібербезпека та стійкість
Мінцифри	цифрова трансформація
НЦУ	операційний контур стійкості
оператори	інфраструктура та послуги
технічна спільнота	протоколи, маршрутизація, IX, DNS
академічне середовище	дослідження та кадри
IGF-UA	багатосторонній діалог

Сьогодні в рамках чинної системи за участю різних зацікавлених сторін (multistakeholderism) на платформі IGF-UA діє принцип **один раз на рік** винесення та висвітлення накопичених проблемних питань, їх подальшого обговорення на панелях форуму, проведення консультацій та розробки рекомендацій у рамках форуму, які не завжди втілюються в практику роботи акторів ринку. Умовно кажучи це система Internet Governance 1.0

Тому є актуальним створення інституціолізованої багатосторонньої системи формування та реалізації державної політики у сфері Інтернету, в якій рішення щодо інфраструктури, регулювання, безпеки, стандартизації та цифрової трансформації ухвалюються на основі **постійної взаємодії** держави, бізнесу, технічної та академічної спільнот, асоціацій, громадянського суспільства тощо, умовно кажучи системи Internet Governance 2.0.

Тобто створення повного постійно діючого циклу формування політики:

дані → експертний аналіз → консультація → спільне рішення щодо політики → реалізація політики → KPI → моніторинг → коригування політики

Формування **нейтральної технічної та мультистейкхолдерної дорадчої платформи**, наприклад, у рамках нової структури – Ради із забезпечення сталості інтернету України (Ukraine Internet Resilience Council) за участю центральних органів виконавчої влади, бізнесу та індустрії, технічної спільноти, наукової (академічної) спільноти, профільних громадських організацій та асоціацій.

Основою національної системи Internet Governance 2.0 є, як і раніше, МУЛЬТИСТЕЙКХОЛДЕРИЗМ, але з одним базовим доповненням – його реалізація неможлива без створення СЕРЕДОВИЩА ДОВІРИ, тобто. ТРАСТА

МУЛЬТІСТЕЙКХОЛДЕРИЗМ за умов відсутності ТРАСТУ не працює

Роль платформи має полягати у забезпеченні нейтральної архітектури постійного діалогу на базі довіри між тими, хто регулює Інтернет, і тими, хто його насправді будує та експлуатує.

Ця платформа має основну організаційну мету – стати нейтральним майданчиком, який допоможе:

- пов’язувати українську державну цифрову політику, операторів, IXP, технічну спільноту з європейською інтернет-екосистемою,
- знайти шляхи реалізації стратегії “від підключення до стійкості до відмови → від цифрового суверенітету до взаємодії → від доступу до Інтернету до надійної інфраструктури штучного інтелекту”

за основними напрямками роботи:

- Національна мережа «Універсальний доступ» (National Universal Access Connect),

- Національна стійкість Інтернету (National Internet Resilience),
- Сумісна цифрова інфраструктура України та ЄС (Interoperable Ukraine and EU Digital Infrastructure),
- Середовище довіри в українському Інтернеті (Trusted Ukrainian Internet),
- Інтернет-інфраструктура штучного інтелекту в Україні (Ukraine AI Internet Infrastructure)

Принципи роботи ради:

Принцип роботи	**Предмет**
Мультістейкхолдеризм	Рівноправний діалог та облік інтересів усіх сторін – держави, бізнесу, операторів зв'язку, технічних експертів, науковців, профільних громадських організацій, асоціацій тощо
Технологічний нейтралітет	Ухвалення рішень на основі відкритих інженерних стандартів інтернету, незалежно від конкретних вендорів або політичної кон'юнктури
Колегіальність та прозорість	Відкритий характер обговорень, консенсусний механізм прийняття рішень та публічність вироблених рекомендацій
Інклюзивність	Забезпечення балансу між національною безпекою, економічними інтересами операторів та захистом прав кінцевих користувачів

Цілі роботи ради:

Мета роботи	**Предмет**
Забезпечення стійкості (Resilience)	Розробка стратегій захисту національної мережі від кібератак, блекаутів, фізичних ушкоджень інфраструктури та зовнішнього деструктивного впливу
Розвиток Internet Governance 2.0	Перехід до сучасної моделі управління інтернетом на національному рівні, гармонізованої з європейськими та світовими стандартами (RIPE, ICANN, ISOC)
Експертна експертиза	Виступ у ролі незалежного консультаційного органу для уряду під час підготовки законів, нормативних актів та регуляторних правил у сфері електронних комунікацій
Координація та раннє попередження	Створення єдиного майданчика для оперативного обміну інформацією щодо загроз зв'язків між державою та приватними провайдерами
Технологічний розвиток	Стимулювання впровадження передових протоколів та практик безпеки (таких як RPKI/ROA, IPv6, DNSSEC) на загальнодержавному рівні