Internet Society

Path to 2025: Mid-Term Update

2025 Strategy – Midterm Status Report

We believe in a world where the Internet means opportunity. We care about its future.

In 2019, in collaboration with the Board of Trustees, staff, and global community, the Internet Society developed a five-year strategy centered around three pillars: Build, Promote, and Defend.

To help grow the Internet, we work to close the digital divide. We bring together the people and technology needed to give everyone the access they need. In an increasingly connected world, the Internet has become a critical resource providing those with access virtually infinite opportunities to innovate and work together for the collective good. This did not happen by accident. The Internet owes its strength, resilience, and success to its open architecture. It was built to be built upon.

To make the Internet stronger, we advocate for a secure, trustworthy, and more resilient Internet. We defend the Internet from those who could make it less secure, less resilient, and less open.

As we approach the midpoint of our five-year strategy, we've gathered information about progress made so far to make the Internet bigger and stronger. This report outlines that progress.

Build

Extend the Internet to communities that do not have it and need it most.

2025 Target

By 2025, we will have built and extended connectivity to 50 communities.

Midterm Status

In 2020 and 2021, we built and extended connectivity to communities in 49 countries in total.

Midterm Progress Update

In 2020, we built or strengthened 22 Community Networks (CNs) in a total of 18 countries.

1. Argentina (El Cuy)
2. Canada (Toronto)
3. Colombia (Cauca)
4. Dominica (Kalinago)
5. Ecuador (Galapagos)
6. Georgia (Tusheti)
7. Greece (Sarantaporo)
8. Guyana (Amelia's Ward Linden)
9. Guyana (Golden Grove Village)
10. India (Sittilingi)
11. Italy (Valli di Lanzo)
12. Kenya (Lanet Umoja)
13. Mexico (Reyeshogpan)
14. Nigeria (Kaduna State)
15. Pakistan (Pakpattan)
16. United States (New York)
17. United States (New Jersey)
18. United States (Washington)
19. United States (Washington D.C. area)
20. South Africa (Mankosi Community, Western Cape)
21. Uganda (Gulu District, Northern Uganda)
22. Zimbabwe (Murambinda, Buhera District)

In 2021, we built or strengthened 28 CNs in a total of 21 countries.

1. Armenia (Shaghap Village)
2. Bolivia (Puesto García)
3. Brazil (Espirito Santinho)
4. Canada (Manitoba)
5. Colombia (Cauca)
6. Democratic Republic of the Congo (Idjwi.)
7. Ecuador (Galapagos)
8. Georgia (Ucha)
9. Guyana (Amelia's Ward Linden)
10. Guyana (Golden Grove Village)
11. India (Chirala)
12. India (Orissa)
13. Kenya (Kisumu)
14. Kenya (Lanet Umoja)
15. Kyrgyzstan (Enilchek)
16. Kyrgyzstan (Zardaly)
17. Mexico (Oaxaca)
18. Morocco (Ait Izdeg)
19. Namibia (Groot Aub)
20. Nepal (Uttargaya)
21. Pakistan (Pākpattan)
22. Papua New Guinea (Gaba Gaba Village)
23. Paraguay (Santa Rosa)
24. South Africa (Mamaila)
25. United States (Nationwide initiative called Gigabit Libraries Network)
26. United States (Seattle, Washington)
27. United States (Waianae, Hawaii)
28. United States (Kipahulu, Hawaii)

In 2020, we built or strengthened 22 Internet Exchange Points (IXPs) in a total of 21 countries.

1. Albania (ANIX)
2. Angola (ANG-IXP)
3. Bolivia (PIT Bolivia)
4. Bosnia (BHNIX)
5. Burkina Faso (BFIX)
6. Canada (YYCIX)
7. Canada (OGIX)
8. Democratic Republic of the Congo (KINIX)
9. Dominican Republic (IX-DO)
10. El Salvador (IXSal)
11. Guatemala (IXP.GT)
12. Haiti (AHTIC-IX)
13. Kenya (KIXP)
14. Malawi (MIX)
15. Mauritius (MIXP)
16. Nepal (npIX)
17. Rwanda (RINEX)
18. Saint Vincent & the Grenadines (SVGIX)
19. South Africa (JINX)
20. Tanzania (TIX)
21. Thailand (bkNIX)
22. Togo (TGIX)

In 2021, we built or strengthened 24 IXPs in 21 a total of countries.

1. Albania (ANIX)
2. Bangladesh (BDIX)
3. Bolivia (PIT Bolivia)
4. Bosnia (BHNIX)
5. Canada (VANIX)
6. Democratic Republic of the Congo (GOMIX)
7. Democratic Republic of the Congo (LUBIX)
8. Haiti (AHTIC-IX)
9. India (Amravati)
10. India (Guwahati)
11. India (Kolkata IX)
12. Indonesia (Cloud Exchange)
13. Lebanon (Beirut-IX)
14. Macedonia (IXP.mk)
15. Malawi (MIX)
16. Mexico (IXSY, Yucatán)
17. Pakistan (PKIX Lahore)
18. Peru (PIT Peru, Arequipa)
19. Rwanda (RINEX)
20. Saint Vincent & the Grenadines (SVGIX)
21. South Africa (DINX)
22. Togo (TGIX)
23. Uganda (UIXP)
24. Zimbabwe (HIX)

Promote

P1 Promote the Internet model of networking as the preferred model.

2025 Target

By 2025, the Internet model of networking will be dominant.

Midterm Status

The Internet model appears to be dominant. Our proxy indicators show its dominance along the axes of autonomy of networks, reachability across shared networks, and free flow of data. However, there is clearly limited freedom to deploy in over a quarter of countries in the world.

Midterm Progress Update

The Internet Society tracks four areas which collectively provide a view of whether the Internet model of networking is preferred. These areas are autonomy of networks, shared network reachability, free flow of data, and freedom to deploy.

Autonomy of networks

On the Internet, networks participate on a voluntary basis and can make independent decisions, free from any central authority that might dictate interconnection or routing arrangements. Infringements on the ability of networks to connect in diverse arrangements and make independent decisions is an infringement on the model.

To track this, we monitor the inequality in distribution of upstream provisioning of Internet access using a statistic called the GINI coefficient of Autonomous System (AS) Hegemony—which we track as part of the Internet Society Pulse Internet Resiliency Index.[1] The GINI coefficient of AS Hegemony indicates the level of inequality in the distribution of upstream providers in a country.

From 2020 to 2021, the average GINI coefficient of AS Hegemony averaged across all countries remained constant with a slight decrease towards 2021—from 0.5195 to 0.5160. This indicates that, on average and for all countries, there has been no major shift in the dependency towards a specific set of providers—which indicates that the Internet model of networking was not affected, and there have not been large changes to the general autonomy of networks.

1 Please see the Internet Resilience Index Methodology for further discussion of the GINI coefficient of AS Hegemony: https://pulse.internetsociety.org/wp-content/uploads/2021/11/Internet-Society-Pulse-IRI-Methodology-October-2021-v1.0-Final-EN.pdf

Shared network reachability

The Internet model strives to create a shared network of end-to end connectivity through the interconnection of independent networks. This implies an ability to communicate end-to-end using a common protocol and shared addressing system. Infringement on this end-to-end connectivity is consequently an infringement on the networking model.

To track this, we monitor IPv6 adoption,[2] which shows a more than 3 percent increase—from 27 percent in 2020 to 30.7 percent in 2021—in the number of connections using the latest Internet addressing system known as Internet Protocol version 6 or **IPv6**. This represents a solid annual rise in the number of connections that can "speak" the latest packet-based language of the Internet required for a shared network with global reachability, without having to use costly and network-splintering technologies such as Network Address Translation (NAT).

Free flow of data

The Internet model is a technology neutral and general-purpose network based on collaboration. Once a network connects to the Internet, they are part of, and communicate with, all parts of the Internet. Packets are moved based on best effort without consideration to their content. Impairments on this ability to send and receive traffic from any part of the Internet (without consideration of its content) is consequently an infringement on the networking model.

To track this, we monitor regional network performance and content retrieval (or lack thereof when it is blocked) by measuring the degree of network-level content retrieval anomalies across the globe. We use data from CensoredPlanet.org, which continuously runs measurements on a series of websites from almost every country of the world using different techniques. They count the number of "expected matches" (successfully retrieved content) and the number of "anomalies" (of different types) that result in unsuccessful or impaired retrieval. As measured in this manner, we observe the median number of anomalies to expected matches ratio in 2020 as 4 percent and in 2021 as 2.8 percent, representing an increase in the free flow of data across the globe. (We see the same tendency with data from Open Observatory of Network Interference across 2020 to 2021 counting anomalies versus successful measurements.)

Freedom to deploy

The Internet model's use of open standards of re-usable building blocks, combined with its decentralized nature of independent networks, enables a freedom to deploy new protocols and applications without permission. Infringements on this ability to

2 The Internet Society Pulse Enabling Technologies tracker longitudinally tracks measures % of IPv6 connections seen by Google, Facebook, and APNIC. Each of their methodologies are somewhat complex and results in "reasonably agreement" (see Rene Wilhelm's analysis here: https://labs.ripe.net/author/wilhelm/ipv6-adoption-statistics-a-comparison-of-different-metrics/), so we take the average of the measurements of these three for this indicator.

deploy new technologies and to attach new networks to the Internet is consequently an infringement on the networking model.

To track this, we monitor readiness for digital transformation in terms of maturity of national regulatory and policy environments using data provided by the ITU's Benchmark for Fifth Generation Digital Collaborative Regulation (G5 Benchmark). Of the 193 countries assessed in the 2021* G5 Benchmark, 23 percent—or 44 countries—scored low or "limited' readiness for digital transformation. This shows a lot of work remains to be done to achieve freedom to deploy protocols and new networks freely around the world.

Note: 2021 is the first year of the ITU's G5 Benchmark data collection. We hope in future years to observe continued decrease in the percentage of countries with low levels of readiness for digital transformation, directly increasing the freedom to deploy globally.

P2 Convince leading governments of the world to adopt policies that favor the Internet model and improve Internet connectivity.

2025 Target

By 2025, leading governments of the world will have adopted policies that "favor" the Internet model and improved Internet connectivity.

Midterm Status

In 2020 and 2021, a total of **six** leading governments—with which Internet Society engaged—have adopted policies that "favor" the Internet model and improved Internet connectivity.

Midterm Progress Update

In Africa,

- **Kenya** adopted in 2021 a Licensing and Shared Spectrum Framework for Community Networks policy. The Internet Society contributed to the public consultation process to influence this outcome.
- **Zimbabwe** adopted in 2020 a new Statutory Instrument on Telecommunications licensing and regulations, that include License for Special Services: Rural Fixed Broadband Wireless Access Systems (community networks). The Internet Society contributed to the public consultation process to influence this outcome.

In Asia Pacific,

- **Samoa** adopted a domestic IXP policy. The Internet Society had direct involvement in this policy change through its partnership/engagement with UNESCAP on Pacific IXP work.

In the Middle East and Northern Africa,

- **Oman** adopted IXP policies that are consistent with our recommendations for neutral IXPs. The Internet Society worked closely with telecom regulators and key networks to influence this outcome.
- **Iraq** adopted IXP policies that are consistent with our recommendations for neutral IXPs. That was reflected in part in the contract with an IXP as a service provider. The Internet Society worked closely with telecom regulators and key networks to influence this outcome.

In North America,

- The city of **Inuvik in North-West Territories, Canada** adopted an IXP policy promoting the deployment of IXPs as a community-driven initiative. The Internet Society was the convener of the Town Hall meeting, bringing together different stakeholders, including ISPs, city officials, and colleges. The Mayor of Inuvik invited the Internet Society to speak to the elected officials and present the case for a new IXP deployment. As a result, the City of Inuvik issued a letter of support, inviting all stakeholders to participate in the new IXP deployment and connectivity.

P3 Promote the deployment of technologies and protocols that secure the interconnection of independent networks.

2025 Target

By 2025, security technologies promoted by the Internet Society will have provided resiliency, stability, availability, confidentiality, and integrity for networks that want to interconnect.

Midterm Status

From 2020 to 2021, we observed increases in the adoption and deployment of security technologies promoted by the Internet Society.

Midterm Progress Update

The Internet Society tracks the adoption and deployment of five types of security enabling technologies, which collectively provide a general sense of whether there is improvement in deployment and adoption of important security technologies. These technologies are: IPv6, TLS, DNSSEC, ROA, and ROV.

We observed a more than 3 percent increase—from 27 percent in 2020 to 30.7 percent in 2021—in the number of top-1000 websites using the latest Internet addressing system known as Internet Protocol version 6 or **IPv6**. This means that, as of 2021, more than a third of the top 1000 websites have adopted the use of IPv6, which allows for an Internet that can handle many more devices like computers and phones that can directly talk to one another.

We observed an 8 percent increase in the number of top 1000 websites that enabled the latest in advanced secure web communication protocol known as **TLS** (Transport Layer Security) 1.3. This is an increase from 56 percent in 2020 to 64 percent in 2021. This greatly enhances secure communications for visitors to these top 1000 websites. This is a progressive achievement for a new technology that only became available in 2018.

We observed that as of 2021, 33 percent of all country code Top Level Domain (ccTLD) operators—such as .uk, .za, .de, etc.—have enabled secure domain name resolution by implementing the Domain Name System Security Extensions (**DNSSEC**) technology, which verifies the authenticity of a DNS lookup, similar to a "verified" phone book. This was a 3 percent increase from 2020.

As of 2021, 33 percent of all global networks have used a new technique known as Route Origin Authorization (**ROA**) Generation, to enable other networks to validate the legitimacy of the Internet routing directions to them. This was a 5 percent increase from the previous year.

As of 2021, 17 percent of all global networks are using a new technique known as Route Origin Validation (**ROV**) to validate the legitimacy of the directions which they follow to reach a specified Internet network. This was an increase of 2 percent from the previous year.

Defend

D1 Shape the policies of leading governments in favor of the growth of independent networks, which are free to interconnect.

2025 Target

By 2025, leading governments of the world have adopted policies that favor the growth of independent networks, which are free to interconnect.

Midterm Status

In 2020 and 2021, a total of **18** leading governments in countries —with which the Internet Society engaged—adopted policies in favor of the growth of independent networks, which are free to interconnect.

Midterm Progress Update

In Africa,

- the 16 member states that make up the Southern Africa Development Community - SADC (**Angola, Botswana, Comoros, DRC, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia and Zimbabwe) upheld** the best practice policy of not requiring the interconnection of IXPs in the SADC region. The interconnection of distinct IXPs over long distances and cross-border expands the scope and places the IXP in direct competition with some of its members who provide IP transit services. As a result, this will potentially affect the IXP's neutrality and growth. The Internet Society facilitated workshops for the member states to influence this outcome.

In Asia Pacific,

- **Samoa adopted** a domestic IXP policy. The Internet Society had direct involvement in this policy change through its partnership/engagement with UNESCAP on Pacific IXP work.

In North America,

- the **U.S. adopted** the first Rural Tribal Priority Window (TPW). This special spectrum application window allowed rural tribal nations to apply for valuable Educational Broadband Service (EBS) frequencies over their lands that had never been licensed. The Internet Society worked closely with tribal communities and partners in the promotion and advocacy of this critical initiative.

D2 Counter attempts by leading governments to undermine encryption.

2025 Target

By 2025, we countered attempts by at least three leading governments to undermine encryption.

Midterm Status

In 2020 and 2021, we countered attempts to undermine encryption by a total of **five** leading governments.

Midterm Progress Update

In Africa,

- In **Mauritius** in 2021, the government's proposed Social Media legislation threatened to force Internet service providers to route social media traffic through a system that would decrypt, read, and then re-encrypt social media data, greatly undermining the security and privacy of users. After a large response from the Internet community, the Mauritian government did not continue to pursue the legislation. The Internet Society coordinated advocacy with allies, published a blog post, and partnered with the Mauritian IGF to make a submission during the public consultation on the legislation highlighting our technical concerns.

In Europe,

- **Germany** - German hacking legislation would have allowed the German government to force over-the-top services (OTTs) and Internet Service Providers (ISPs) to aid them in hacking end points. Ultimately the text of the legislation was changed to explicitly exclude OTTs from the assistance obligations. To influence this outcome, the Internet Society coordinated advocacy with local partners and facilitated Global Encryption Member sign on to an open letter against the legislation.
- **Belgium** - Belgian Data Retention Legislation originally required companies to "turn off" end-to-end encryption on demand. The Belgian Government ultimately removed this obligation from the revised text. To influence this outcome, the Internet Society mobilized the Belgium chapter and the Global Encryption Coalition community as well as advocated to raise awareness about the concerns related to this legislation.

In Latin America and the Caribbean,

- **Brazil** - Brazilian congress considered a disinformation bill with implications for end-to-end encryption. Ultimately encryption related aspects were removed from the draft in 2020. To influence this outcome, the Internet Society

coordinated closely with local partners and advocated to raise awareness about the risks associated with this bill.

In North America,

- In the **U.S.**, the EARN IT Act in 2020 threatened to target platforms that use end-to-end encryption by increasing the risk of being sued because they offer encrypted services to protect the content and communication of their users. The EARN IT Act 2020 failed to pass before the legislative session ended. The Internet Society worked with members of the Global Encryption Coalition to help stop the bill, including through signing an open letter, releasing a blog post, and media outreach.
- In the **U.S.**, the Lawful Access to Encrypted Data Act in 2020 threatened to require companies to build encryption "backdoors" either by default or on demand by law enforcement authorities. The Lawful Access to Encrypted Data Act failed to pass before the legislative session ended. The Internet Society helped stop the bill, including through organizing an open letter and Internet Society blog post highlighting the technical community's grave concerns about the bill.

D3 Defend against shutdowns by increasing cross-border connectivity and resiliency.

2025 Target

Defend against shutdowns by increasing cross-border connectivity and resiliency.

Midterm Status

We have increased resiliency by building and extending connectivity to communities in a total of 49 countries in 2020 and 2021. Further, in 2021, we also began to track resiliency by capturing baseline metrics related to infrastructure, performance, security, and market readiness in Africa with plans to expand tracking to all regions/globally.

Midterm Progress Update

See Build for list of countries where we have increased resiliency by building and extending connectivity. See Internet Resilience Index where we have started tracking resiliency in Africa.