Internet Society

Stratégie 2025 : Rapport de situation à mi-parcours

Stratégie 2025 - Rapport de situation à mi-parcours

Nous croyons en un monde où Internet est synonyme d'opportunité. Nous nous soucions de son avenir.

En 2019, en collaboration avec le conseil d'administration, le personnel et la communauté mondiale, l'Internet Society a élaboré une stratégie quinquennale axée sur trois piliers : construire, promouvoir et défendre.

Pour contribuer à la croissance d'Internet, nous nous efforçons de réduire la fracture numérique. Nous rassemblons les gens et la technologie nécessaires pour donner à tout le monde l'accès nécessaire. Dans un monde de plus en plus connecté, Internet est devenu une ressource essentielle offrant à ceux qui y ont accès des possibilités quasi infinies d'innover et de travailler ensemble pour le bien collectif. Ce n'est pas le fruit du hasard. Internet doit sa force, sa résilience et son succès à son architecture ouverte. Il a été conçu pour servir de base à d'autres conceptions.

Afin de renforcer Internet, nous préconisons un Internet sécurisé, fiable et plus résilient. Nous défendons Internet contre ceux qui pourraient le rendre moins sûr, moins résilient et moins ouvert.

Alors que nous approchons de la mi-parcours de notre stratégie quinquennale, nous avons rassemblé des informations sur les progrès réalisés jusqu'à présent pour rendre Internet plus grand et plus fort. Ce rapport décrit ces progrès.

Construire

Étendre l'accès à Internet aux communautés qui n'en disposent pas et qui en ont le plus besoin.

Objectif 2025

D'ici 2025, nous aurons construit et étendu la connectivité à 50 communautés.

Situation à mi-parcours

En 2020 et 2021, nous avons construit et étendu la connectivité à des communautés de 49 pays en tout.

Mise à jour des progrès à mi-parcours

En 2020, nous avons construit ou renforcé 22 réseaux communautaires (RC) dans un total de 18 pays.

1. Argentine (El Cuy)
2. Canada (Toronto)
3. Colombie (Cauca)
4. Dominique (Kalinago)
5. Équateur (Galapagos)
6. Géorgie (Tusheti)
7. Grèce (Sarantaporo)
8. Guyana (Amelia's Ward Linden)
9. Guyana (village de Golden Grove)
10. Inde (Sittilingi)
11. Italie (Valli di Lanzo)
12. Kenya (Lanet Umoja)
13. Mexique (Reyeshogpan)
14. Nigéria (État de Kaduna)
15. Pakistan (Pakpattan)
16. États-Unis (New York)
17. États-Unis (New Jersey)
18. États-Unis (Washington)
19. États-Unis (région de Washington DC)
20. Afrique du Sud (Communauté Mankosi, Cap-Occidental)
21. Ouganda (district de Gulu, nord de l'Ouganda)
22. Zimbabwe (Murambinda, district de Buhera)

En 2021, nous avons construit ou renforcé 28 RC dans un total de 21 pays.

1. Arménie (village de Shaghap)
2. Bolivie (Puesto García)
3. Brésil (Espirito Santinho)
4. Canada (Manitoba)
5. Colombie (Cauca)
6. République démocratique du Congo (Idjwi)
7. Équateur (Galapagos)
8. Géorgie (Ucha)
9. Guyana (Amelia's Ward Linden)
10. Guyana (village de Golden Grove)
11. Inde (Chirala)
12. Inde (Orissa)
13. Kenya (Kisumu)
14. Kenya (Lanet Umoja)
15. Kirghizistan (Enilchek)
16. Kirghizistan (Zardaly)
17. Mexique (Oaxaca)
18. Maroc (Ait Izdeg)
19. Namibie (Groot Aub)
20. Népal (Uttargaya)
21. Pakistan (Pakpattan)
22. Papouasie-Nouvelle-Guinée (village de Gaba Gaba)
23. Paraguay (Santa Rosa)
24. Afrique du Sud (Mamaila)
25. États-Unis (initiative nationale appelée Gigabit Libraries Network)
26. États-Unis (Seattle, Washington)
27. États-Unis (Waianae, Hawaï)
28. États-Unis (Kipahulu, Hawaï)

En 2020, nous avons construit ou renforcé 22 points d'échange Internet (IXP) dans un total de 21 pays.

1. Albanie (ANIX)
2. Angola (ANG-IXP)
3. Bolivie (PIT Bolivia)
4. Bosnie (BHNIX)
5. Burkina Faso (BFIX)
6. Canada (YYCIX)
7. Canada (OGIX)
8. République démocratique du Congo (KINIX)
9. République dominicaine (IX-DO)
10. El Salvador (IXSal)
11. Guatemala (IXP.GT)
12. Haïti (AHTIC-IX)
13. Kenya (KIXP)
14. Malawi (MIX)
15. Maurice (MIXP)
16. Népal (npIX)
17. Rwanda (RINEX)
18. Saint-Vincent-et-les-Grenadines (SVGIX)
19. Afrique du Sud (JINX)
20. Tanzanie (TIX)
21. Thaïlande (bkNIX)
22. Togo (TGIX)

En 2021, nous avons construit ou renforcé 24 IXP dans un total de 21 pays.

1. Albanie (ANIX)
2. Bangladesh (BDIX)
3. Bolivie (PIT Bolivia)
4. Bosnie (BHNIX)
5. Canada (VANIX)
6. République démocratique du Congo (GOMIX)
7. République démocratique du Congo (LUBIX)
8. Haïti (AHTIC-IX)
9. Inde (Amravati)
10. Inde (Guwahati)
11. Inde (Kolkata IX)
12. Indonésie (Cloud Exchange)
13. Liban (Beirut-IX)
14. Macédoine (IXP.mk)
15. Malawi (MIX)
16. Mexique (IXSY, Yucatán)
17. Pakistan (PKIX Lahore)
18. Pérou (PIT Peru, Arequipa)
19. Rwanda (RINEX)
20. Saint-Vincent-et-les-Grenadines (SVGIX)
21. Afrique du Sud (DINX)
22. Togo (TGIX)
23. Ouganda (UIXP)
24. Zimbabwe (HIX)

Promouvoir

P1 Promouvoir le mode de fonctionnement du réseau Internet comme modèle à privilégier.

Objectif 2025

D'ici 2025, le mode de fonctionnement du réseau Internet sera prépondérant.

Situation à mi-parcours

Le modèle Internet semble être dominant. Nos indicateurs proxy montrent sa prédominance dans les domaines de l'autonomie des réseaux, de l'accessibilité du réseau partagé et de la libre circulation des données. Cependant, la liberté de déploiement est clairement limitée dans plus d'un quart des pays du monde.

Mise à jour des progrès à mi-parcours

L'Internet Society surveille quatre domaines qui, collectivement, permettent de déterminer si le mode de fonctionnement du réseau Internet est privilégié. Ces domaines sont l'autonomie des réseaux, l'accessibilité du réseau partagé, la libre circulation des données et la liberté de déploiement.

Autonomie des réseaux

Sur Internet, les réseaux participent sur une base volontaire et peuvent prendre des décisions indépendantes, libres de toute autorité centrale qui pourrait dicter des arrangements d'interconnexion ou de routage. Les atteintes à la capacité des réseaux à se connecter selon diverses modalités et à prendre des décisions indépendantes constituent une atteinte au modèle.

Pour accompagner cela, nous surveillons le niveau d'inégalité dans la distribution de l'approvisionnement en amont de l'accès à Internet en utilisant une statistique appelée coefficient de GINI de l'hégémonie des systèmes autonomes (SA). Ce suivi est assuré sur la plateforme Pulse de l'Internet Society avec l'indice de résilience Internet.[1] Le coefficient de GINI de l'hégémonie des SA indique le niveau d'inégalité dans la répartition des fournisseurs en amont dans un pays.

De 2020 à 2021, le coefficient de GINI moyen de l'hégémonie des SA dans tous les pays est resté constant avec une légère baisse vers 2021, passant de 0,5195 à 0,5160. Cela indique qu'en moyenne et pour tous les pays, il n'y a pas eu de changement majeur dans la dépendance vis-à-vis d'un ensemble spécifique de fournisseurs, ce qui montre que le mode de fonctionnement du réseau Internet n'a pas été affecté et qu'il n'y a pas eu de grands changements dans l'autonomie générale des réseaux.

1 Veuillez consulter la méthodologie de l'indice de résilience Internet pour une discussion plus approfondie du coefficient de GINI de l'hégémonie des SA : https://pulse.internetsociety.org/wp-content/uploads/2021/11/Internet-Society-Pulse-IRI-Methodology-October-2021-v1.0-Final-EN.pdf

Accessibilité du réseau partagé

Le modèle Internet s'efforce de créer un réseau partagé de connectivité de bout en bout grâce à l'interconnexion de réseaux indépendants. Cela implique une capacité à communiquer de bout en bout en utilisant un protocole commun et un système d'adressage partagé. L'atteinte à cette connectivité de bout en bout est par conséquent une atteinte au mode de fonctionnement du réseau.

Pour suivre cela, nous surveillons l'adoption d'IPv6,[2] qui montre une augmentation de plus de 3 % du nombre de connexions (passant de 27 % en 2020 à 30,7 % en 2021) utilisant le dernier système d'adressage Internet connu sous le nom de protocole Internet version 6 ou **IPv6**. Cela représente une solide augmentation annuelle du nombre de connexions capables de « parler » le dernier langage basé sur les paquets d'Internet requis pour un réseau partagé avec une accessibilité mondiale, sans avoir à utiliser des technologies coûteuses divisant le réseau telles que la traduction d'adresses réseau ou NAT (Network Address Translation).

Libre circulation des données

Le modèle Internet est un réseau technologiquement neutre et polyvalent basé sur la collaboration. Une fois qu'un réseau se connecte à Internet, il fait partie de toutes les parties d'Internet et communique avec elles. Les paquets sont déplacés au mieux sans tenir compte de leur contenu. Les atteintes à cette capacité d'envoyer et de recevoir du trafic à partir de n'importe quelle partie d'Internet (sans tenir compte de son contenu) constituent par conséquent une atteinte au mode de fonctionnement du réseau.

Pour suivre cela, nous surveillons les performances du réseau régional et la récupération de contenu (ou son absence lorsqu'il est bloqué) en mesurant le degré d'anomalies de récupération de contenu au niveau du réseau à travers le monde. Nous utilisons les données de CensoredPlanet.org, qui effectue en permanence des mesures sur une série de sites Web de presque tous les pays du monde en utilisant différentes techniques. Le nombre de « correspondances attendues » (contenu récupéré avec succès) et le nombre « d'anomalies » (de différents types) entraînant une récupération infructueuse ou altérée sont comptés. Nous observons ainsi la médiane des anomalies par rapport aux correspondances attendues, 4 % en 2020 et 2,8 % en 2021, ce qui représente une augmentation de la libre circulation des données à travers le monde. (Nous constatons la même tendance avec les données de l'Open Observatory of Network Interference entre 2020 et 2021 en comptant les anomalies par rapport aux mesures réussies.)

2 L'outil de suivi Enabling Technologies de la plateforme Pulse de l'Internet Society suit longitudinalement les mesures du pourcentage de connexions IPv6 vues par Google, Facebook et APNIC. Chacune de leurs méthodologies est quelque peu complexe et aboutit à un « accord raisonnable » (voir l'analyse de Rene Wilhelm ici : https://labs.ripe.net/author/wilhelm/ipv6-adoption-statistics-a-comparison-of-different-metrics/), nous prenons donc la moyenne des mesures de ces trois pour cet indicateur.

Liberté de déploiement

L'utilisation par le modèle Internet de normes ouvertes aux composants réutilisables, combinée à sa nature décentralisée de réseaux indépendants, permet de déployer librement de nouveaux protocoles et applications sans autorisation. Les atteintes à cette capacité à déployer de nouvelles technologies et à connecter de nouveaux réseaux à Internet constituent par conséquent une atteinte au mode de fonctionnement du réseau.

Pour suivre cela, nous surveillons l'état de préparation à la transformation numérique en termes de maturité des environnements réglementaires et politiques nationaux à l'aide des données fournies par les critères de référence pour la réglementation de cinquième génération (critères de référence G5) de l'UIT. Sur les 193 pays évalués dans les critères de référence G5 2021*, 23 %, soit 44 pays, ont démontré un niveau de préparation faible ou « limité » à la transformation numérique. Cela montre qu'il reste beaucoup de travail à faire pour parvenir à la liberté de déployer librement des protocoles et de nouveaux réseaux dans le monde entier.

Remarque : 2021 est la première année de collecte de données des critères de référence G5 de l'UIT. Nous espérons que dans les années à venir, nous observerons une diminution continue du pourcentage de pays dont le niveau de préparation à la transformation numérique est faible, augmentant ainsi directement la liberté de déploiement dans le monde.

P2 Convaincre les gouvernements du monde entier d'adopter des politiques privilégiant le mode de fonctionnement du réseau Internet et améliorant la connectivité.

Objectif 2025

D'ici 2025, les principaux gouvernements du monde entier auront adopté des politiques « privilégiant » le mode de fonctionnement du réseau Internet et améliorant la connectivité.

Situation à mi-parcours

En 2020 et 2021, un total de six gouvernements de pays avec lesquels l'Internet Society s'est engagée, ont adopté des politiques « privilégiant » le mode de fonctionnement du réseau Internet et améliorant la connectivité.

Mise à jour des progrès à mi-parcours

En Afrique,

- **Le Kenya** a adopté en 2021 une politique relative à l'octroi de licences et au partage du spectre pour les réseaux communautaires. L'Internet Society a contribué au processus de consultation publique pour influencer ce résultat.
- **Le Zimbabwe** a adopté en 2020 un nouvel instrument statutaire sur les licences et la réglementation des télécommunications, comprenant une licence pour les services spéciaux : les systèmes d'accès sans fil haut débit fixes en milieu rural (réseaux communautaires). L'Internet Society a contribué au processus de consultation publique pour influencer ce résultat.

En Asie-Pacifique,

- **Samoa** a adopté une politique IXP nationale. L'Internet Society a été directement impliquée dans ce changement de politique par le biais de son partenariat/ engagement avec l'UNESCAP sur les travaux des IXP du Pacifique.

Au Moyen-Orient et en Afrique du Nord,

- **Oman** a adopté des politiques IXP conformes à nos recommandations pour les IXP neutres. L'Internet Society a travaillé en étroite collaboration avec les régulateurs des télécommunications et les principaux réseaux pour influencer ce résultat.
- **L'Irak** a adopté des politiques IXP conformes à nos recommandations pour les IXP neutres. Cela se reflétait en partie dans le contrat avec un IXP en tant que fournisseur de services. L'Internet Society a travaillé en étroite collaboration avec les régulateurs des télécommunications et les principaux réseaux pour influencer ce résultat.

En Amérique du Nord,

- La ville d'I**nuvik, dans les Territoires du Nord-Ouest, au Canada**, a adopté une politique IXP favorisant le déploiement des IXP en tant qu'initiative communautaire. L'Internet Society était l'organisateur de la réunion publique, réunissant différentes parties prenantes, notamment des FAI, des responsables municipaux et des collèges. Le maire d'Inuvik a invité l'Internet Society à parler aux élus et à présenter les arguments en faveur du déploiement d'un nouvel IXP. En conséquence, la ville d'Inuvik a publié une lettre de soutien invitant toutes les parties prenantes à participer au déploiement et à la connectivité du nouvel IXP.

P3 Promouvoir le déploiement de technologies et de protocoles qui assurent l'interconnexion de réseaux indépendants.

Objectif 2025

D'ici 2025, les technologies de sécurité promues par l'Internet Society auront assuré la résilience, la stabilité, la disponibilité, la confidentialité et l'intégrité des réseaux qui souhaitent s'interconnecter.

Situation à mi-parcours

De 2020 à 2021, nous avons observé une augmentation de l'adoption et du déploiement des technologies de sécurité promues par l'Internet Society.

Mise à jour des progrès à mi-parcours

L'Internet Society suit l'adoption et le déploiement de cinq types de technologies de sécurité, qui fournissent collectivement une idée générale de l'amélioration du déploiement et de l'adoption de technologies de sécurité importantes. Ces technologies sont : IPv6, TLS, DNSSEC, ROA et ROV.

Nous avons observé une augmentation de plus de 3 % (de 27 % en 2020 à 30,7 % en 2021) du nombre de sites Web parmi les 1 000 principaux utilisant le dernier système d'adressage Internet connu sous le nom de protocole Internet version 6 ou **IPv6**. Cela signifie qu'en 2021, plus d'un tiers des 1 000 meilleurs sites Web ont adopté l'utilisation d'IPv6, ce qui permet à Internet de gérer de nombreux autres appareils, tels que des ordinateurs et des téléphones, qui peuvent communiquer directement entre eux.

Nous avons observé une augmentation de 8 % du nombre des 1 000 sites Web les plus performants qui ont activé le dernier protocole avancé de communication Web sécurisé connu sous le nom de **TLS** (Transport Layer Security) 1.3. Le pourcentage a augmenté de 56 % en 2020 à 64 % en 2021. Les communications sécurisées sont ainsi considérablement améliorées pour les visiteurs de ces 1 000 meilleurs sites Web. Il s'agit d'une réalisation progressive pour une nouvelle technologie qui n'est devenue disponible qu'en 2018.

Nous avons observé qu'en 2021, 33 % de tous les opérateurs de domaine de premier niveau de code de pays (ccTLD), tels que .uk, .za, .de, etc., ont activé la résolution sécurisée des noms de domaine en mettant en œuvre la technologie **DNSSEC** (Domain Name System Security Extensions), qui vérifie l'authenticité d'une recherche DNS, similaire à un annuaire téléphonique « vérifié ». Cela représente une augmentation de 3 % par rapport à 2020.

En 2021, 33 % de tous les réseaux mondiaux ont utilisé une nouvelle technique connue sous le nom de création d'autorisation d'origine de route **(ROA)**, pour permettre à d'autres réseaux de valider la légitimité de leur propre annonce de route. Cela représente une augmentation de 5 % par rapport à l'année précédente.

En 2021, 17 % de tous les réseaux mondiaux ont utilisé une nouvelle technique connue sous le nom de Validation de l'origine de la route **(ROV)** pour valider la légitimité des directions qu'ils suivent pour atteindre un réseau Internet spécifié. Cela représente une augmentation de 2 % par rapport à l'année précédente.

Défendre

D1 Influencer les politiques des principaux gouvernements en faveur de la croissance des réseaux indépendants, libres de s'interconnecter.

Objectif 2025

D'ici 2025, les principaux gouvernements du monde entier auront adopté des politiques en faveur de la croissance de réseaux indépendants, libres de s'interconnecter.

Situation à mi-parcours

En 2020 et 2021, un total de **18** gouvernements de pays avec lesquels l'Internet Society s'est engagée, ont adopté des politiques en faveur de la croissance de réseaux indépendants, libres de s'interconnecter.

Mise à jour des progrès à mi-parcours

En Afrique,

- Les 16 États membres qui composent la Communauté de développement de l'Afrique australe ou SADC **(Angola, Botswana, Comores, RDC, Eswatini, Lesotho, Madagascar, Malawi, Maurice, Mozambique, Namibie, Seychelles, Afrique du Sud, Tanzanie, Zambie et Zimbabwe)** ont soutenu la politique des meilleures pratiques consistant à ne pas exiger l'interconnexion des IXP dans la région de la SADC. L'interconnexion d'IXP distincts sur de longues distances et transfrontalières élargit le champ d'application et place les IXP en concurrence directe avec certains de leurs membres qui fournissent des services de transit IP. En conséquence, cela affectera potentiellement la neutralité et la croissance des IXP. L'Internet Society a organisé des ateliers pour les États membres afin d'influencer ce résultat.

En Asie-Pacifique,

- **Samoa a adopté** une politique IXP nationale. L'Internet Society a été directement impliquée dans ce changement de politique par le biais de son partenariat/ engagement avec l'UNESCAP sur les travaux des IXP du Pacifique.

En Amérique du Nord,

- Les **États-Unis ont adopté** la première Rural Tribal Priority Window (TPW). Cette fenêtre spéciale d'application du spectre a permis aux nations tribales rurales de demander des fréquences précieuses pour le service de haut débit éducatif (EBS, Educational Broadband Service) sur leurs terres qui n'avaient jamais été autorisées. L'Internet Society a travaillé en étroite collaboration avec les communautés tribales et les partenaires dans la promotion et la défense de cette initiative cruciale.

D2 Contrer les tentatives des gouvernements d'affaiblir le cryptage.

Objectif 2025

D'ici 2025, nous aurons contré les tentatives d'au moins trois gouvernements d'affaiblir le cryptage.

Situation à mi-parcours

En 2020 et 2021, nous avons contré les tentatives de cinq gouvernements d'affaiblir le cryptage.

Mise à jour des progrès à mi-parcours

En Afrique,

- À **Maurice** en 2021, un projet de loi du gouvernement sur les médias sociaux menaçait d'obliger les fournisseurs de services Internet à acheminer le trafic des réseaux sociaux via un système qui décrypterait, lirait, puis recrypterait les données des réseaux sociaux, compromettant considérablement la sécurité et la confidentialité des utilisateurs. Suite à d'importantes réactions de la communauté Internet, le gouvernement mauricien n'a pas donné suite au projet de loi. L'Internet Society a coordonné le plaidoyer avec des alliés, publié un article de blog et s'est associé à l'IGF mauricien pour se prononcer lors de la consultation publique sur le projet de loi mettant en évidence nos préoccupations techniques.

En Europe,

- **Allemagne** - Un projet de loi allemand sur le piratage informatique aurait permis au gouvernement allemand d'obliger les services par contournement (OTT ou Over-the-top en anglais) et les fournisseurs d'accès Internet (FAI) à les aider à pirater les terminaux. Finalement, le texte de loi a été modifié pour exclure explicitement les OTT des obligations d'assistance. Pour influencer ce résultat, l'Internet Society a coordonné le plaidoyer avec les partenaires locaux et a invité les membres de la Global Encryption Coalition à signer une lettre ouverte contre le projet de loi.
- **Belgique** - Un projet de loi belge sur la conservation des données exigeait à l'origine que les entreprises « désactivent » le cryptage de bout en bout à la demande. Le gouvernement belge a finalement supprimé cette obligation du texte de loi révisé. Pour influencer ce résultat, l'Internet Society a mobilisé le chapitre belge et la communauté de membres de la Global Encryption Coalition et a plaidé pour sensibiliser aux préoccupations liées à cette loi.

En Amérique latine et aux Caraïbes,

- **Brésil** - Le congrès brésilien a envisagé un projet de loi sur la désinformation ayant des implications pour le cryptage de bout en bout. En fin de compte, les aspects liés

au cryptage ont été supprimés du projet en 2020. Pour influencer ce résultat, l'Internet Society a collaboré étroitement avec des partenaires locaux et a plaidé pour une sensibilisation aux risques associés à ce projet de loi.

En Amérique du Nord,

- Aux **États-Unis**, le projet de loi EARN IT de 2020 menaçait de cibler les plateformes utilisant le cryptage de bout en bout en augmentant le risque d'être poursuivi parce qu'elles offrent des services cryptés pour protéger le contenu et la communication de leurs utilisateurs. Le projet de loi EARN IT 2020 a été abandonné avant la fin de la session législative. L'Internet Society a travaillé avec les membres de la Global Encryption Coalition pour aider à contrer le projet de loi, notamment en signant une lettre ouverte, en publiant un article de blog et en sensibilisant les médias.
- Aux **États-Unis**, la loi sur l'accès légal aux données cryptées en 2020 menaçait d'obliger les entreprises à créer des « portes dérobées » de cryptage soit par défaut, soit à la demande des forces de l'ordre. Le projet de loi sur l'accès légal aux données cryptées a été abandonné avant la fin de la session législative. L'Internet Society a contribué à contrer le projet de loi, notamment en organisant la signature d'une lettre ouverte et un article de blog soulignant les graves préoccupations de la communauté technique concernant le projet de loi.

D3 Protéger des coupures en augmentant la connectivité et la résilience transfrontalières.

Objectif 2025

Se prémunir contre les coupures en améliorant la connectivité et la résilience transfrontalières.

Situation à mi-parcours

Nous avons accru la résilience en établissant et en étendant la connectivité aux communautés dans un total de 49 pays en 2020 et 2021. De plus, en 2021, nous avons également commencé à suivre la résilience en capturant des mesures de base liées à l'infrastructure, aux performances, à la sécurité et à la préparation du marché en Afrique avec des plans pour étendre le suivi à toutes les régions et dans le monde entier.

Mise à jour des progrès à mi-parcours

Reportez-vous à la section « Construire » pour la liste des pays où nous avons augmenté la résilience en établissant et en étendant la connectivité. Consultez l'indice de résilience Internet où nous avons commencé à suivre la résilience en Afrique.