

# Un cadre stratégique pour un Internet ouvert et digne de confiance

## Une approche pour renforcer la confiance dans un environnement ouvert\*



Mars 2017

### Synthèse

- Une confiance qui diminue est un défi pour l'Internet. Pour protéger les opportunités d'Internet, nous devons contrer cette baisse de confiance.
- Des violations de données à une grande échelle, des incertitudes sur la façon dont nos données sont utilisées, la cybercriminalité, la surveillance et les autres menaces en ligne ont impacté la confiance des utilisateurs, la façon dont ils utilisent Internet, et gêné l'adoption de l'Internet.
- Les décideurs font face à un important défi aujourd'hui : comment appréhender totalement la révolution numérique et en même temps garantir la sûreté et la sécurité de leurs citoyens.
- L'Internet Society est convaincue qu'Internet a besoin de solides fondations en termes de confiance pour atteindre son plein potentiel. La confiance est la pierre angulaire de toutes les stratégies de connectivité réussies, tant dans les pays en voie de développement que dans les pays développés. Cela ne peut être réalisé qu'à travers une responsabilité collective et une collaboration.
- Un « Internet ouvert et digne de confiance » est un Internet globalement interopérable qui cultive l'innovation et crée des opportunités pour tous. Ses fondations reposent sur la confiance des utilisateurs, des technologies de confiance, des réseaux de confiance et un écosystème digne de confiance.
- Ce cadre stratégique dessine une approche pour aborder les complexités d'une construction de la confiance dans un environnement ouvert tel que l'Internet. Il décrit quatre dimensions de la confiance interdépendantes et qui doivent être prises en compte lors du développement de politiques pour l'Internet et offre des principes pour aider à construire un Internet digne de confiance.

## Introduction

L'Internet ouvert offre des opportunités économiques et sociales pour tous. Toutefois, le plein potentiel de l'Internet ne sera obtenu que si la confiance est l'une de ses solides fondations. Une étude récente aux Etats-Unis a montré que 45 % des utilisateurs ont changé leur comportement en ligne du fait de leurs peurs. Des articles provenant du monde entier nous indiquent les mêmes préoccupations. Les utilisateurs d'Internet sont inquiets de la façon dont leurs données sont utilisées par les gouvernements et les entreprises. Ils ressentent un manque de contrôle et s'inquiètent du profilage et de la discrimination. Ils craignent aussi de devenir les victimes de violations de données, de vols d'identité et d'autres formes de cybercriminalité. Pour certains, ce scénario s'est déjà mué en réalité. Les utilisateurs d'Internet sont aussi très troublés par l'impact qu'une surveillance générale a sur leur vie privée et leurs autres droits.

De nombreux gouvernements sont en train d'évaluer les effets d'Internet sur la société. Certains sont inquiets de la capacité d'Internet à permettre, voire à amplifier les menaces de criminels, d'autres états et même de leurs propres citoyens. Ils y répondent par des contrôles gouvernementaux plus importants, comme restreindre l'accès à divers contenus et entraver l'utilisation des médias sociaux. Certains ont imposé des mesures de localisation des données pour conserver un trafic Internet à l'intérieur de leurs frontières. D'autres ont considéré bannir les technologies de confiance clés (par ex., le cryptage) ou forcer les fournisseurs de technologies à créer des faiblesses dans leurs produits car ils croient que ces technologies entravent la capacité à faire appliquer les lois pour combattre le crime. Toutefois, sans cryptage ou autres technologies de confiance, il n'y aurait pas d'opérations bancaires sécurisées ni de communications confidentielles pour *n'importe* quel utilisateur d'Internet. Ces politiques ont le résultat inverse de ce qui est en réalité nécessaire : elles endommagent la confiance des utilisateurs, suppriment des opportunités et étouffent l'innovation.

## L'Internet a besoin de solides fondations en termes de confiance pour réaliser son plein potentiel.

Aujourd'hui, les décideurs doivent choisir la route à prendre dans le développement des politiques Internet. Une route conduit à un Internet ouvert et digne de confiance avec l'ensemble des bénéfices sociaux et économiques qu'il apporte. L'autre route conduit à un réseau sans confiance et qui se referme de plus en plus, incapable de susciter de la croissance. Une route conduit aux opportunités, l'autre à la stagnation. La clé en est la confiance et la façon de maintenir l'Internet comme un espace fondamentalement dynamique et digne de confiance.

## L'Internet : la confiance dans un environnement ouvert

Un « Internet ouvert et digne de confiance » est un réseau de réseaux répartis mondialement et interopérables, qui cultive l'innovation et crée des opportunités pour tous. Ses fondations reposent sur la confiance des utilisateurs, des technologies de confiance, des réseaux de confiance et un écosystème digne de confiance. Il offre une gouvernance complète, est construit sur des principes politiques robustes et cherche à mettre les intérêts des utilisateurs d'Internet au cœur des décisions.

Un « Internet digne de confiance » n'est pas une utopie, coupée des menaces du monde. Il existera toujours des risques et des inconvénients à un système de réseaux ouvert. Des acteurs malveillants trouveront toujours des façons d'exploiter les vulnérabilités. Les technologies et les capacités que nous développons pour améliorer une partie de la vie peuvent en impacter négativement une autre. Mais les menaces peuvent être atténuées, les risques répartis, les faiblesses partagées et surmontées. L'ouverture de l'Internet est aussi le moyen de le protéger.

Toutes les parties prenantes ont un rôle positif à jouer pour entretenir un Internet ouvert et digne de confiance. Nous devons travailler à sécuriser les aspects centraux de l'infrastructure Internet, à protéger la confidentialité et l'intégrité des données qui la traversent et à nous assurer que les bonnes politiques sont en place pour soutenir les technologies, les réseaux et les acteurs qui font fonctionner l'Internet. Nous réaliserons cela en étant responsables collectivement et en collaborant.

Une des fondations utiles peut être trouvée dans les principes de la [Sécurité Collaborative](#) : faire naître la confiance et protéger les opportunités ; responsabilité collective ; propriétés et valeurs fondamentales ; évolution et consensus ; penser globalement, agir localement.

Le cadre stratégique de l'Internet Society pour un Internet ouvert et digne de confiance dessine une approche pour gérer les complexités de la construction de la confiance dans un environnement ouvert tel que l'Internet. Cette approche est décrite au travers de quatre dimensions interdépendantes de la confiance qui doivent être prises en considération lors du développement de politiques pour l'Internet, et fournit les principes pour bâtir un Internet fiable.

Ce cadre stratégique pour un Internet fiable regroupe les importantes et précieuses différences qui confèrent à notre monde sa riche diversité. Il n'existe pas de solution « unique » pour les prises de décisions en ce qui concerne l'Internet. Les politiques pro-Internet peuvent prendre de nombreuses formes, s'adaptant ainsi aux besoins spécifiques de chaque pays. Mais une chose les unit ; leur point de départ est la question : *comment construisons-nous la confiance dans un environnement ouvert tel que l'Internet ?*



Fig. 1 Les quatre dimensions pour un Internet ouvert et digne de confiance

**Confiance des utilisateurs** : comment et pourquoi les utilisateurs d'Internet, y compris les gouvernements, le secteur privé et les citoyens, font confiance à l'Internet, et comment bâtir cette confiance.

**Des technologies pour la confiance** : les blocs de constructions techniques pour établir et maintenir des réseaux, des applications et des services dignes de confiance.

**Réseaux de confiance** : la force de l'Internet repose sur sa collection en éternelle évolution de réseaux interconnectés avec une propriété et un contrôle bien distribués. La confiance est le ciment qui conserve les réseaux connectés et les données échangées.

**Écosystème digne de confiance** : comment l'Internet est-il gouverné et comment sont gérées les questions posées par l'Internet.

Cette division trouve son origine dans la nature modulaire et stratifiée de l'Internet. Un réseau de réseaux de confiance permet une portée globale, alors qu'un ensemble de technologies de confiance permet des applications qui utilisent l'Internet pour offrir confidentialité, intégrité et capacité d'authentification. Avec ces branches techniques en place, un écosystème digne de confiance permet une confiance systémique, où la confiance de l'utilisateur est le moteur de toute la créativité et l'innovation que l'on trouve sur l'Internet.

La confiance n'est pas simplement une belle idée. C'est un ensemble de choix, d'outils et de capacités déjà enchâssés dans l'Internet ouvert.

## Confiance des utilisateurs

Toute personne qui utilise Internet est un « utilisateur de l'Internet », qu'elle soit représentant gouvernemental, publicitaire, enseignant, agent de voyages, étudiant ou artiste. Nous décidons chaque jour la façon dont nous faisons confiance (ou non) à l'Internet pour nos interactions sociales, professionnelles, financières ou autres.

La confiance des utilisateurs est importante pour le succès futur de l'Internet parce que si les utilisateurs ne font pas confiance à l'Internet, ils en restreindront l'utilisation, et pourront même cesser de l'utiliser pour certaines activités. Cela pourrait avoir un sérieux impact sur l'évolution de l'Internet, son utilisation et sa croissance.

En remontant à 1996, l'Assemblée pour l'organisation de l'Internet, l'organisation supervisant le développement des protocoles techniques d'Internet, reconnaît que la croissance de l'Internet dépend de la confiance qu'ont les utilisateurs que le réseau protégera leurs informations et communications ([RFC 1984](#)).

Toutefois, inspirer confiance aux utilisateurs ne signifie pas simplement rassurer les gens en espérant un résultat positif. Inspirer confiance aux utilisateurs signifie mettre en place la bonne infrastructure (réseaux de confiance), permettre aux utilisateurs de protéger leurs activités (technologies de confiance), mettre en place les politiques justes, et fournir un environnement souple qui répond correctement aux craintes fondées des utilisateurs (écosystème digne de confiance).

Les principes politiques pour améliorer la confiance des utilisateurs permettent aux particuliers et aux organisations de prendre des décisions rationnelles et informées sur la façon dont ils utilisent Internet.

Nous sommes tous, gouvernement, secteur privé, société civile et citoyens, des utilisateurs d'Internet. Si nous commençons par nous demander « que peut-on faire pour rendre l'Internet meilleur pour nous en tant qu'utilisateurs ? » nous serons déjà à mi-chemin dans la construction d'un Internet digne de confiance.

### Principes de politique pour maintenir la confiance des utilisateurs

**Droits de l'Homme :** les droits de l'Homme doivent être intégrés dans les politiques Internet au fur et à mesure de leur développement, et non ajoutés après coup. Les droits individuels doivent être protégés sur l'Internet.

**Confidentialité des communications :** les politiques de l'Internet doivent maintenir le principe que les utilisateurs de l'Internet doivent pouvoir communiquer de manière confidentielle en ligne. Ils devraient également encourager l'innovation et l'utilisation d'outils pour faciliter les communications confidentielles (par ex., le cryptage).

**Confidentialité :** les droits individuels à une vie privée et les attentes liées doivent être protégés sur Internet, indépendamment de la nationalité ou du lieu de résidence. Il ne doit pas y avoir de surveillance générale des communications Internet. Les individus doivent avoir la possibilité de communiquer de manière anonyme ou avec un pseudonyme.

**Protection du consommateur :** les droits des consommateurs doivent être respectés dans l'ensemble de l'Internet. Les gouvernements doivent soutenir la confiance des consommateurs en faisant voter et en appliquant des lois de protection des consommateurs pour les affaires réalisées sur leur territoire ou sous leur contrôle. Ils doivent aussi s'engager dans une coopération internationale au-delà des frontières pour s'assurer que les droits des consommateurs sont protégés, quel que soit l'endroit où ils résident.

**Contrôle sur les données :** les utilisateurs d'Internet doivent pouvoir avoir la maîtrise de leurs données. Ils doivent avoir la possibilité de transférer leurs données d'un service à l'autre.

**Transparence dans la politique nationale :** les gouvernements doivent être ouverts et transparents concernant leurs décisions, leurs politiques, lois et pratiques. Ils doivent impliquer de façon active les parties prenantes dans le développement des politiques de l'Internet.

**Sécurité juridique :** les gouvernements doivent s'assurer que les lois sont claires, faciles à comprendre et accessibles à tous. Ils doivent s'abstenir d'utiliser leurs pouvoirs législatifs et judiciaires de manière capricieuse ou arbitraire.

**Applications et réparations :** les gouvernements doivent s'assurer que les autorités réglementaires possèdent les ressources nécessaires et l'indépendance requise pour offrir aux utilisateurs d'Internet un respect de la loi et des réparations, dans le cas où ils ont subi des pertes, des préjudices ou toute autre forme de dommages.

**Non-discrimination :** les gouvernements doivent s'assurer que leurs lois et politiques empêchent l'Internet d'être utilisé pour discriminer une personne selon le groupe, la classe ou la catégorie à laquelle cette personne ou objet est perçu(e) comme appartenant ; ou sur la base de profilage des données.

**Agences de surveillance et lanceurs d'alerte :** toutes les parties prenantes doivent reconnaître la valeur que les agences de surveillance ou les particuliers donneurs d'alerte apportent à la société et leur porter assistance.

## Technologies de confiance

Les technologies de confiance sont les blocs de constructions techniques pour établir et maintenir des réseaux, des applications et des services de confiance. Elles sont les fondements techniques pour un Internet digne de confiance.

Une technologie de confiance communément utilisée est la Transport Layer Security (TLS), un protocole cryptographique utilisé pour fournir confidentialité et intégrité aux communications, par ex. entre un appareil d'un utilisateur et un serveur de site Web. TLS a été développé par un processus ouvert par le groupe de travail d'ingénierie Internet (IETF). Aujourd'hui, pratiquement toutes les banques et tous les services gouvernementaux en ligne utilisent TLS.

Les technologies de confiance sont importantes pour permettre de renforcer la confiance sur l'Internet car elles constituent les outils techniques qui permettent aux utilisateurs d'Internet de communiquer de manière privée (confidentialité), de savoir avec qui ils communiquent (authentification), de savoir que l'information qu'ils envoient ou reçoivent n'a pas été altérée en transit (intégrité), de restreindre l'accès à leurs données ou communications (autorisation), et de savoir si leur appareil ou technologie a été falsifié (détection et résistance à la falsification).

Les technologies de confiance sont utilisées pour sécuriser les réseaux, les applications et les services que nous utilisons tous les jours. Sans les technologies de confiance telles que TLS et ses prédécesseurs, nous n'aurions jamais vu l'explosion du commerce en ligne qui stimule la croissance du PIB et qui diffuse des opportunités globalement. Sans le cryptage des communications, les gouvernements, les sociétés et les individus ne seraient pas capables de garder leurs communications confidentielles et leurs informations en sécurité.

Les technologies de confiance ont évolué grâce à une caractéristique clé de l'Internet ouvert - l'innovation qui ne demande pas de permission préalable ou d'autorisation spéciale provenant d'une autorité. L'innovation sans permission a construit l'Internet et est essentielle à la future bonne santé de l'Internet et des économies qui en dépendent.

Les menaces continuent d'émerger et de croître, nous devons ainsi nous assurer que nous possédons tous les outils nécessaires à la vie privée, la sécurité et, finalement, les opportunités économiques et sociales.

Nous avons besoin de politiques qui favorisent plutôt qu'entravent le développement, la disponibilité et l'utilisation des technologies de confiance.

Nous avons besoin de technologies de confiance tous les jours, pour sécuriser nos réseaux, nos transactions et même nos vies. Elles doivent être aussi robustes et omniprésentes que nous pouvons les rendre.

### Principes politiques pour soutenir l'utilisation de technologies de confiance

#### Les gouvernements doivent :

- permettre aux utilisateurs d'adopter leurs propres mesures techniques de protection pour leurs communications et données sur Internet ;
- encourager le développement ouvert et la liberté d'accès à des outils « faciles à utiliser » qui permettent aux utilisateurs de communiquer de manière confidentielle ;
- encourager les fournisseurs de services en ligne à offrir à leurs consommateurs des solutions de cryptage de bout en bout.

#### En ce qui concerne le cryptage :

*(Ces recommandations résument les principes de l'initiative de [www.securetheinternet.org](http://www.securetheinternet.org), soutenus par de nombreuses sociétés, personnes et organisations, y compris l'Internet Society.)*

Les utilisateurs d'Internet doivent avoir la possibilité d'utiliser, et les sociétés doivent avoir la possibilité d'offrir, le cryptage le plus fort possible, y compris un cryptage de bout en bout, sans crainte que les gouvernements les contraignent à donner accès aux contenus, métadonnées ou clés de cryptage sans procédure officielle ni respect des droits de l'Homme.

Les gouvernements ne doivent pas interdire ou autrement limiter l'accès à du cryptage sous quelque forme que ce soit, ou interdire la mise en place ou l'utilisation de cryptage basée sur son degré ou son type.

Les gouvernements ne doivent pas exiger la conception ou la mise en place de « backdoors » ou de vulnérabilité dans les outils, technologies ou services.

Les gouvernements ne doivent pas exiger que les outils, technologies ou services soient conçus ou développés pour permettre à des tiers l'accès à des données décryptées ou des clés de cryptage.

Les gouvernements ne doivent pas chercher à affaiblir ou saper les normes de cryptage ou influencer intentionnellement l'établissement de normes de cryptage sauf pour promouvoir un plus haut niveau de sécurité de l'information. Aucun gouvernement ne doit exiger des algorithmes de cryptage, des normes, des outils ou des technologies peu robustes.

Les gouvernements ne doivent pas, que ce soit par un accord public ou privé, obliger ou faire pression sur une entité pour qu'elle s'engage dans des activités qui sont incompatibles avec ces principes.

## Réseaux de confiance

L'Internet est une collection de réseaux interconnectés sans propriétaires communs ni contrôle centralisé et en évolution constante. La confiance est le ciment qui conserve les réseaux connectés et les données échangées.

**Établir et maintenir un Internet de confiance signifie que différents acteurs - avec différents rôles et responsabilités - doivent prendre des mesures proches de là où les problèmes se produisent.**

Il n'existe pas de réseau unique mondial, l'Internet est un « réseau de réseaux ». Le trajet des communications n'est pas décidé à l'avance, et il ne respecte pas les frontières nationales. Les utilisateurs de l'Internet ne décident pas de la façon dont leurs communications sont acheminées : ils font simplement « confiance » en le fait que les opérateurs de réseaux transmettront les données là où elles doivent aller. C'est une stratégie de transport qui peut apparaître chaotique, mais elle fournit résilience et vitesse à une échelle que l'humanité n'a encore jamais réalisée.

La confiance dans ce contexte n'est ni un espoir ni une opinion ; c'est une façon pratique et réciproque de « faire des affaires ». Les opérateurs de réseau font confiance à leurs pairs pour réaliser les opérations nécessaires pour fournir une communication de bout en bout. Si un opérateur ne respecte pas cette confiance, ses pairs trouveront d'autres façons de faire transiter leur trafic et cesseront simplement de traiter avec lui. Cette approche est importante, car elle offre des options viables et ne permet pas au système de s'effondrer.

La pierre angulaire des réseaux de confiance se trouve être **la responsabilité collective et la collaboration**. Ceci est la notion que toutes les parties prenantes doivent collaborer et partager la responsabilité pour régler les difficultés posées par Internet.

Les éléments fondamentaux pour des réseaux Internet de confiance sont les invariants d'Internet de l'Internet Society et les principes de la Sécurité Collaborative.

L'adoption de ces éléments fondamentaux en tant que fondation pour la prise de décision crée un environnement dans lequel les réseaux de confiance vont continuer à évoluer et s'épanouir.

### Principes de politique pour soutenir des réseaux de confiance

#### Sécurité :

Les stratégies et politiques nationales de cybersécurité doivent promouvoir la prospérité économique et sociale : elles ne doivent pas entraver la croissance, l'innovation ou le développement.

Pour développer des stratégies et des politiques de cybersécurité, les gouvernements doivent regrouper l'expertise de toutes les parties prenantes et travailler avec elles pour développer des solutions collaboratives.

Les politiques de cybersécurité doivent intégrer les droits de l'Homme : elles doivent se battre pour défendre la sûreté et la sécurité, tout en garantissant les droits des particuliers.

Les gouvernements doivent donner l'exemple, mais aussi savoir reconnaître l'expertise de certaines parties prenantes qui peuvent être les leaders dans leur domaine. Quelquefois, les meilleures solutions sont celles qui émergent organiquement sans instructions d'un quelconque gouvernement. Les solutions doivent être définies et mises en place à l'endroit où elles auront le plus d'impact.

La collaboration internationale sera essentielle pour conserver la sécurité et la résilience d'Internet.

#### Connexion des réseaux et circulation du trafic :

Les gouvernements ne doivent pas exiger la localisation des données ou imposer des routes de circulation d'Internet.

Les gouvernements doivent encourager les sociétés régionales et internationales à participer à l'interconnexion locale et à l'environnement de mono gage (par ex., en réduisant les barrières et/ou en fournissant des incitations économiques).

Les gouvernements doivent encourager les investissements dans des infrastructures d'Internet supplémentaires (par ex., des câbles sous-marins, des IXP et des infrastructures nationales) et une meilleure résistance au profit de tout l'écosystème Internet.

Les gouvernements doivent offrir un environnement législatif qui soutienne la compétitivité des marchés pour les services en ligne.

#### Normes techniques ouvertes :

Les politiques doivent défendre un Internet construit sur les normes techniques ouvertes. Les parties prenantes peuvent démontrer leur soutien en secondant et promouvant les principes d'OpenStand.

## Écosystème digne de confiance

Lorsque les gouvernements définissent des politiques pour Internet, ils réfléchissent plus loin que de se poser simplement la question « avons-nous confiance en Internet pour notre propre usage ? ». Ils considèrent également l'impact que l'Internet peut avoir sur la sécurité et le bien-être des citoyens, leur économie, leur souveraineté, ainsi que « qui possède le contrôle ». Équilibrer tous ces intérêts est une équation de confiance bien plus complexe que la confiance de l'utilisateur. Cependant, il est essentiel d'y répondre. Voilà pourquoi les gouvernements accordent tellement d'importance à la fiabilité de l'écosystème Internet et à sa gouvernance.

La fiabilité de l'écosystème Internet découle de la façon dont il a été développé et de ses processus de gouvernance multipartite, où ceux affectés par des décisions ont l'opportunité de faire partie de ceux-ci.

L'Internet est devenu une plate-forme globale pour l'innovation et la croissance économique grâce à des processus participatifs partant de la base, donnant la priorité à la stabilité d'une intégrité de systèmes, et maintenant la nature ouverte des technologies sous-jacentes. Ces principes sont l'« ADN » de l'Internet.

En son sein, la gouvernance multipartite incarne la transparence, l'inclusion, la responsabilité partagée, favorise la responsabilisation, et est efficace en matière de résolution des problèmes communs de l'Internet.

De plus, dans la communauté technique, nous partageons un sentiment de direction collective vis-à-vis du cœur du public de l'Internet et des normes ouvertes sur lesquelles ses technologies et réseaux sont fondés.

Ces caractéristiques renforcent la confiance des parties prenantes dans la façon dont l'écosystème Internet fonctionne et est gouverné

L'Internet ne présente pas de problème de « commande et contrôle ». C'est un défi de coordination. Comment pouvons-nous effectivement travailler avec ceux qui sont responsables pour toutes ces différentes parties, nombre d'entre eux étant au-delà de nos frontières ?

**Écosystème digne de confiance : attributs d'une gouvernance multipartite réussie.**

**Inclusion et transparence : l'inclusion est la base de la légitimité dans la prise de décision collaborative.**

Dans le cadre de la prise d'une décision susceptible d'avoir d'importantes répercussions sur certaines parties prenantes, ces dernières devraient avoir la possibilité de participer au processus. Non seulement l'inclusion est un objectif admirable, mais elle constitue aussi une part essentielle d'un processus efficace. Moins un processus est inclusif, moins il a de chances de gagner la confiance de ceux qui en sont exclus et de les soutenir. La transparence est une condition essentielle pour l'inclusion, car elle intègre des experts ainsi que les groupes affectés dans le processus. La transparence des contributions, du processus et des prises de décisions est essentielle pour l'Internet.

**Responsabilité partagée : toutes les parties prenantes partagent une responsabilité collective pour maintenir la dynamique d'Internet et les avantages qu'il apporte à nos sociétés et à l'économie mondiale.** Dans la communauté technique, nous partageons un sentiment de *direction collective* d'Internet et des normes ouvertes sur lesquelles reposent ses technologies.

**Prise de décision efficace et mise en œuvre : les décisions les plus efficaces sont celles qui s'appuient sur un processus ouvert et délibéré tenant compte d'un vaste éventail de sources d'informations et de perspectives.** Ceci vaut à la fois pour la qualité et pour la mise en œuvre de la décision.

Comme l'Internet est exploité par une variété de parties prenantes du secteur public et du secteur privé ainsi que de la société civile, la réussite de la mise en œuvre des décisions passe par des solutions imaginatives et collaboratives. Ce n'est pas aussi simple que d'adopter une loi nationale. Les parties prenantes qui ont participé au processus déploient leurs meilleurs efforts pour en réussir la mise en œuvre.

**Collaboration, gouvernance répartie et interopérable : pour tirer le meilleur parti des efforts déployés par un grand nombre d'acteurs, la communauté technique a développé des systèmes de gouvernance autonome en s'appuyant sur la collaboration et le respect mutuel.** Les nombreuses organisations impliquées dans la gouvernance de l'Internet ont des rôles complémentaires à jouer. Nous devons reconnaître cette autonomie et maintenir un dialogue et une participation mutuelle dans les domaines qui se recoupent entre les différentes organisations.

C'est un résumé des caractéristiques des approches d'une gouvernance réussie de l'Internet dans la « [Gouvernance d'Internet par l'Internet Society : pourquoi l'approche multipartite fonctionne-t-elle](#) ».



## Conclusion

Pour nous assurer que les bénéfices de l'économie numérique atteignent l'ensemble des personnes dans le monde, et que l'innovation prospère, nous devons construire ensemble un Internet ouvert et digne de confiance. Nous croyons que le cadre de cette politique fournit une approche pour gérer la complexité de la construction de la confiance dans un environnement ouvert tel qu'Internet.

Nous vous demandons de réfléchir à ces différentes dimensions de la confiance et la façon dont elles sont toutes interdépendantes lorsque vous réfléchissez à des politiques liées à l'Internet. Nous encourageons aussi tous les commentaires que vous pourriez avoir sur ce cadre de politique pour un Internet ouvert et digne de confiance. Veuillez envoyer vos commentaires à [trust@isoc.org](mailto:trust@isoc.org).

Un Internet ouvert et digne de confiance est vital au succès de cette économie numérique. Nous devons travailler de manière collaborative pour en faire une réalité.