

Le guide pratique de l'utilisateur final averti, construire un Internet sain.



Le moteur invisible.

On se réveille, et c'est déjà là. Avant même d'avoir versé la première tasse de café, la plupart d'entre nous avons déjà utilisé la machine la plus complexe jamais conçue par l'humanité. On consulte la météo, on parcourt les gros titres, ou on fait défiler un flux de visages, familiers ou inconnus. C'est presque magique : une couche invisible et éthérée qui se superpose à notre réalité physique.

Mais internet n'est pas magique. C'est un **moteur** .

C'est un moteur colossal, mondial et largement invisible qui alimente nos économies, nos vies sociales et, de plus en plus, notre perception même de la vérité. Pendant des décennies, nous nous sommes contentés d'être passagers, profitant de la rapidité et du confort sans jamais nous interroger sur son fonctionnement. Mais comme nous l'avons constaté ces dernières années, lorsque le moteur commence à fumer – lorsque la vie privée s'érode, que la désinformation se propage et que la dimension « sociale » du web prend un tournant résolument antisocial – être un simple passager ne suffit plus.

Le passage du consommateur à l'architecte

Le livre que vous tenez entre vos mains, * *The Smart End-Users Playbook* *, paraît à un moment charnière de notre histoire numérique. Nous passons de l'ère du « faire vite et prendre des risques » à une ère qui exige de nous une réflexion approfondie et une construction de qualité.

Le principe fondamental de ce guide est simple mais profond : **un internet sain n'est pas quelque chose qui nous arrive ; c'est quelque chose que nous créons par nos choix quotidiens.**

Être un « utilisateur averti », c'est reprendre le contrôle de sa vie. Cela signifie dépasser le rôle passif de simple donnée collectée par les algorithmes et devenir un acteur de l'écosystème numérique. Il s'agit de comprendre les mécanismes de ce « moteur invisible » afin de l'orienter vers

un avenir au service de l'humanité, et non uniquement du profit.

Feuille de route pour le citoyen moderne

Le guide « L'utilisateur averti » ne vous demande pas de devenir informaticien ou expert en cybersécurité. Il vous invite simplement à être **attentif**. Il vous fournit les outils nécessaires pour naviguer dans le monde numérique en toute connaissance de cause, en vous apprenant à déceler les forces invisibles – les algorithmes et les modèles économiques – qui façonnent votre expérience en ligne.

Une fois ces chapitres terminés, le « Moteur invisible » vous semblera moins mystérieux. Vous comprendrez mieux vos droits, vos responsabilités et votre pouvoir.

Internet est le plus formidable outil de connexion et de créativité que nous ayons jamais créé. Il est temps d'apprendre à bien l'utiliser.

Bienvenue au volant.

Table des matières		
Le moteur invisible.		i – ii
Chapitre 1 :	Démystifier le noyau – Qu’est-ce que l’ICANN ?	01
Chapitre 2 :	Le Comité consultatif général (ALAC) et ses structures.	04
Chapitre 3 :	Le cycle des politiques publiques : comment un clic devient une règle.	08
Chapitre 4 :	Protéger le terrain de jeu – Le contrôle de santé DNS.	10
Chapitre 5 :	L’acceptation universelle – Un Internet pour tous.	16
Chapitre 6 :	Le guide pratique en action : comment participer à la conversation.	19
Conclusion:	Le pouvoir de votre voix dans le modèle multipartite.	21
Glossaire:	Parler le « jargon de l'ICANN »	23

Chapitre 1

Démystifier le noyau – Qu'est-ce que l'ICANN ?

Chaque matin, des milliards de personnes se réveillent et accomplissent une série de rituels invisibles. Nous consultons nos courriels, accédons à nos comptes bancaires, suivons des cours en ligne et prenons des nouvelles de nos proches, même à l'autre bout du monde. Nous naviguons dans cet immense univers numérique avec une confiance aveugle, pour le moins stupéfiante. Nous supposons que les routes seront ouvertes, que la signalisation nous indiquera le bon chemin et que les quartiers que nous visiterons seront sûrs.

Mais vous êtes-vous déjà demandé **qui s'occupe de la carte ?**

Pour la plupart d'entre nous, internet est comme un service essentiel, au même titre que l'eau ou l'électricité. On ne s'en aperçoit que lorsqu'il tombe en panne. Cependant, contrairement à l'eau ou à l'électricité, internet n'est pas géré par un gouvernement mondial unique ni par une seule entreprise. C'est une ressource partagée, régie par un processus unique et participatif, conçu pour garantir qu'aucune entité ne puisse la couper complètement.

Nous sommes nombreux à utiliser Internet comme une voiture : on tourne la clé et on s'attend à ce que ça démarre. Mais qui décide de la construction des

infrastructures et qui obtient les autorisations nécessaires ? Ce livre s'intéresse aux personnes qui œuvrent dans l'ombre – la **communauté au sens large** – pour garantir la stabilité, la sécurité et, surtout, l'adéquation d'Internet aux besoins de chaque utilisateur.

Le déficit de gouvernance

Trop longtemps, les discussions sur le fonctionnement d'Internet se sont déroulées dans des cercles d'ingénieurs, d'avocats et de lobbyistes. Il en résulte un « déficit de gouvernance ». D'un côté, les experts techniques prennent les décisions concernant le système de noms de domaine (DNS) ; de l'autre, l' **utilisateur final** , celui dont la vie est concrètement impactée par ces décisions.

« **Le guide pratique de l'utilisateur final averti** » a pour but de combler cette lacune.

Le cœur du système : l'ICANN et le grand public

Au cœur de cet univers se trouve **l'ICANN** (Internet Corporation for Assigned Names and Numbers). La mission de l'ICANN est de garantir le bon fonctionnement du modèle multipartite d'Internet, en assurant la stabilité, la sécurité et l'interopérabilité du réseau.

Mais l'ICANN sait qu'un système technique n'est efficace que s'il est bien servi. C'est là qu'intervient la **Communauté des utilisateurs. Composée de centaines de structures**

à grande échelle (ALS) réparties dans le monde entier et de membres individuels, cette communauté est la voix désignée de chaque internaute. Que vous soyez étudiant à Nairobi, entrepreneur à Buenos Aires ou retraité à Berlin, la Communauté des utilisateurs veille à la protection de vos droits et de vos intérêts .

Pourquoi ce guide est important maintenant

Nous sommes à la croisée des chemins. Alors qu'Internet s'étend pour inclure le prochain milliard d'utilisateurs, les défis se multiplient :

- **Sécurité** : Comment empêcher les acteurs malveillants de détourner les « adresses » auxquelles nous faisons confiance ?
- **Accessibilité** : Comment garantir l'accès à Internet pour tous, quelle que soit la langue parlée ou l'écriture utilisée ?
- **Agence** : Comment faire en sorte que la politique ne soit pas simplement quelque chose qui nous *arrive* , *mais quelque chose que nous contribuons à créer* ?

Ce que vous trouverez à l'intérieur

Ce livre n'est pas un manuel technique ; c'est un **guide pour prendre votre vie en main**. Nous allons éliminer le jargon et le jargon technique de l'ICANN pour vous montrer :

1. Comment fonctionne réellement l'« annuaire téléphonique » d'Internet.
2. Comment utiliser votre **structure locale d'élus locaux** pour influencer la politique mondiale.
3. Mesures concrètes pour construire un internet plus « sain » — un internet plus sûr, plus inclusif et plus transparent.

Internet est le plus grand laboratoire de connexion humaine jamais créé. Mais il nécessite de l'entretien. Il a besoin de défenseurs. Et surtout, il a besoin **de vous** .

Bienvenue dans la communauté. Commençons à construire.

Chapitre 2

Le Comité consultatif général (ALAC) et ses structures.

Pour vous aider à vous orienter dans le paysage mondial de l'ICANN, il est essentiel de savoir dans quel « voisinage » vous vous trouvez. L'ICANN divise le monde en cinq **organisations régionales (RALO)**.

Ces structures servent de centres régionaux qui rassemblent les structures locales à vocation générale (ALS) pour discuter des politiques et défendre leurs besoins locaux spécifiques.

La force du collectif : le rugissement des 250+

Il est facile d'avoir l'impression qu'une voix se perd dans le brouhaha numérique. Dans un écosystème mondial, une seule personne qui proteste contre une hausse de prix risque de ne pas convaincre un membre du conseil d'administration. Mais le **Comité consultatif général (ALAC)** change la donne.

- **Le réseau ALS** : Il existe plus de **250 structures à grande échelle (ALS)** dans le monde entier — des groupes représentant des utilisateurs individuels d'Internet, de Nairobi à New York.
- **Amplification** : Lorsque ces plus de 250 groupes

s'unissent, ils représentent des millions d'utilisateurs.

C'est **la force du collectif**.

- **Le consensus comme monnaie d'échange :**
dans ce modèle, plus le consensus est fort, plus l'argument a de poids. Lorsque la communauté au sens large s'exprime d'une seule voix, il ne s'agit pas d'une simple suggestion, mais d'un **impératif** que les acteurs techniques et commerciaux ne peuvent ignorer.

Trouver sa place : La carte RALO

Utilisez le tableau ci-dessous pour identifier le RALO qui représente vos intérêts en fonction de votre lieu de résidence ou du lieu d'activité de votre organisation :

Nom RALO	Région couverte
AFRALO	Afrique
APRALO	Asie, Australie et Pacifique
EURALO	Europe
LACRALO	Amérique latine et Caraïbes
NARALO	Amérique du Nord

Domaines d'intervention clés

- ✓ Promouvoir la croissance du secteur DNS, l'inclusion numérique et le soutien aux langues locales.
- ✓ Gestion de la région linguistique la plus diversifiée ; forte priorité accordée à l'acceptation universelle (IDN).
- ✓ Forte priorité accordée aux droits numériques, à la protection de la vie privée (conformité au RGPD) et à la transparence pour l'utilisateur final.
- ✓ Réduire la fracture numérique et garantir un accès internet abordable et sécurisé dans toute la région.
- ✓ Protection des consommateurs, politique de cybersécurité et sensibilisation de la société civile.

Quel profil vous correspond ?

Pour vous aider à décider comment vous impliquer, examinez ces trois profils types de « bénévoles ». Lequel vous correspond le mieux ?

1. Le défenseur du numérique (membre de l'ALS)

- **Qui sont-ils ?** Un membre d'une association locale de défense des droits des consommateurs, d'un club technologique universitaire ou d'une section locale d'une société internet.
- **Leur objectif** : veiller à ce que les règles

internationales n'aient pas d'impact négatif sur la capacité de leur communauté locale à accéder à Internet.

- **Action** : Ils rejoignent leur **RALO régional** pour voter sur les déclarations de politique générale et assister aux assemblées régionales.

2. Le passionné de politique technologique (le membre individuel)

- **Profil recherché** : Un professionnel ou un étudiant passionné par la gouvernance d'Internet, mais qui ne fait pas partie d'une organisation formelle.
- **Leur objectif** : apporter leur expertise à des groupes de travail sur des sujets spécifiques tels que **les abus DNS** ou **la protection de la vie privée** .
- **Action** : De nombreuses RALO (comme EURALO et NARALO) permettent **une adhésion individuelle** , vous permettant de participer sans avoir besoin de diriger une organisation.

3. Le citoyen concerné (L'observateur)

- **Qui sont-ils ?** Des personnes qui utilisent quotidiennement Internet et souhaitent rester informées des menaces à la sécurité et de leurs droits.
- **Leur objectif** : comprendre le « pourquoi » des

changements sur Internet et protéger leur santé numérique personnelle.

- **Action** : Ils s'abonnent à la **lettre d'information At-Large** et suivent les périodes de consultation publique qui ont une incidence sur la sécurité des utilisateurs finaux.

Étape suivante : cartographier votre impact

Chaque membre de la SLA, individuellement ou collectivement, commence par une seule personne qui se demande : « *Quel impact cela a-t-il sur ma communauté ?* » Une fois votre RALO identifiée, vous pouvez trouver une liste d'organisations existantes dans votre pays auxquelles adhérer, ou même créer la vôtre.

Chapitre 3

Le cycle des politiques publiques : comment un clic devient une règle.

La politique ne devrait pas être un mystère. L'élaboration des politiques donne souvent l'impression d'être une « boîte noire », dissimulée dans des bureaux lambrissés ou au sein de listes de diffusion complexes. Mais dans le domaine de la gouvernance d'Internet, c'est tout le contraire. Il s'agit du **modèle de consensus ascendant**, un système où les règles qui régissent Internet ne sont pas imposées par un gouvernement ou une entreprise unique, mais élaborées par les internautes eux-mêmes.

1. Identifier le problème : de « C'est agaçant » à « C'est la politique de l'entreprise »

Chaque règle commence par une étincelle. Cela se produit généralement lorsqu'une personne — un propriétaire de petite entreprise, un passionné de technologie ou un défenseur des consommateurs — remarque que quelque chose ne fonctionne pas.

- **Le point sensible** : Prenons l'exemple de **la hausse des prix des noms de domaine**. Lorsqu'un .org ou un .com voit son coût exploser, il ne s'agit pas seulement d'un problème de facturation ; c'est un problème de politique.
- **Prise en compte** : Un problème passe du statut

de simple plainte à celui de sujet d'actualité lorsqu'il est soulevé au sein de la communauté. Grâce **aux groupes de travail** et **aux rapports de problèmes**, la communauté détermine s'il s'agit d'un cas isolé ou d'une tendance systémique nécessitant une nouvelle réglementation.

- **L'élément déclencheur** : Une fois le problème documenté, un processus formel de recherche de solutions est mis en place.

2. Périodes de commentaires du public : Votre place à la table des questions

Si le cycle d'élaboration des politiques est un dialogue, la **période de consultation publique** est le moment où la parole vous est donnée. C'est la partie la plus transparente du processus, et pourtant souvent la plus sous-utilisée.

- **La période d'influence** : avant qu'une recommandation ne devienne une règle, elle doit être publiée pour être soumise à l'examen du public. Il ne s'agit pas d'une simple formalité, mais d'une obligation légale et procédurale.
- **Pourquoi votre avis compte** : Les décideurs politiques sont souvent des spécialistes qui peuvent avoir du mal à appréhender la réalité du terrain. En soumettant un commentaire, vous leur fournissez les

données concrètes dont ils ont besoin pour comprendre les conséquences d'une réglementation proposée.

- **Transparence** : Chaque commentaire est archivé et pris en compte. Votre voix est inscrite de façon permanente dans les archives publiques, ce qui permet de responsabiliser les décideurs.

Les politiques d'Internet définissent notre manière de vivre ensemble en ligne. Comprendre ce processus vous permet de passer du statut d'utilisateur passif à celui d'acteur de la construction de l'avenir numérique. **Ce guide d'initiation au processus d'élaboration des politiques de l'ICANN fait partie de notre série.**

Chapitre 4

Protéger le terrain de jeu : le contrôle de santé du DNS.

Un internet sain repose sur un « annuaire » DNS sain. Dans le monde de l'ICANN, **l'abus DNS** n'est pas un simple dysfonctionnement technique ; il s'agit d'une utilisation malveillante et intentionnelle du système de noms de domaine à des fins nuisibles. Bien que l'infrastructure d'internet soit complexe, les signes d'une « fuite » sont souvent visibles si l'on sait où chercher.

Les « cinq grands » abus de DNS

L'ICANN et ses partenaires contractuels (les personnes qui vendent et gèrent les noms de domaine) se concentrent sur cinq types de préjudices spécifiques. Connaître ces catégories vous aide à comprendre à quoi vous êtes confronté :

1. **Hameçonnage** : vous inciter à divulguer vos mots de passe ou vos informations de carte de crédit en se faisant passer pour une marque de confiance (par exemple, un courriel provenant d'une « banque »).
2. **Logiciel malveillant** : logiciel malveillant qui s'infiltrer sur votre appareil via un domaine pour voler des données ou verrouiller vos fichiers (ransomware).
3. **Botnets** : Un réseau « zombie » d'ordinateurs infectés contrôlé par un seul attaquant, souvent utilisé pour faire planter d'autres sites web.

4. **Pharming** : Une attaque plus sophistiquée qui vous redirige vers un faux site web même si vous avez saisi la bonne adresse dans votre navigateur.
5. **Spam** : Courriels non sollicités envoyés en masse, en particulier ceux utilisés comme « véhicule de livraison » pour les quatre autres types d'abus mentionnés ci-dessus.

Votre bilan de santé en 5 points « signaux d'alarme »

Avant de cliquer sur un lien ou de saisir vos données, passez mentalement en revue cette liste de vérification. Voici les signes distinctifs d'un domaine utilisé à des fins abusives :

- **[] Le test du « like-alike » (typosquatting) :**
L'URL semble-t-elle légèrement différente ? Les attaquants utilisent souvent `micros0ft.com` (avec un zéro) ou `paypal-support-security.com` au lieu du domaine officiel.
- **L' astuce du survol :** Sur un ordinateur, survolez un lien avec votre souris sans cliquer. Regardez dans le coin inférieur de votre navigateur. L'adresse affichée correspond-elle au texte du lien ? Si le lien indique « Votre banque » mais que le texte au survol affiche « `totallement-réel- site.xyz` », c'est un piège.

- **[] Le sentiment de panique** : les abus prospèrent grâce à l'urgence. Si un domaine ou un courriel prétend que votre compte sera supprimé dans « 2 heures » à moins que vous ne cliquiez immédiatement, il s'agit probablement d'une tentative de contourner votre esprit critique.
- **[] Analyse du sous-domaine** : Les entreprises légitimes placent généralement leur nom juste avant le `.com` ou le `.org`. Méfiez-vous des longues chaînes de caractères comme `account-update.verification.security.official-bank.com.randomsite.net`. Le véritable domaine est ici `randomsite.net`, et non celui de la banque.
- **Les erreurs linguistiques** : De nombreuses campagnes d'abus internationales utilisent la traduction automatique. Soyez attentif aux formulations étranges, aux fautes de grammaire ou à une formule de salutation générique (comme « Cher client ») là où vous vous attendez normalement à votre nom.

Amélioration de la sécurité de 2024

Depuis **avril 2024**, l'ICANN a mis en œuvre de nouvelles règles plus strictes pour les bureaux d'enregistrement (les entreprises qui vendent des noms de domaine). Ces

derniers sont désormais **contractuellement tenus** d'agir lorsqu'ils reçoivent des preuves concrètes d'abus commis par les cinq principaux acteurs du secteur.

Concrètement, cela signifie que vos appels ne sont plus vains. Si vous signalez un site d'hameçonnage à un registraire, celui-ci est légalement tenu par l'ICANN d'enquêter et, si l'hameçonnage est avéré, de le fermer.

Le rôle de la SLA : votre garde communautaire

Vous n'avez pas besoin d'être un expert en cybersécurité pour lutter contre les abus DNS. C'est là que votre **La structure At-Large (ALS)** se présente sous la forme :

- **Éducation** : De nombreux ALS organisent des ateliers pour enseigner ces signes avant-coureurs aux personnes âgées, aux étudiants et aux propriétaires de petites entreprises.
- **Plaidoyer**: Les ALS recueillent des données sur les tendances locales en matière d'abus et les soumettent à l'ICANN pour élaborer ses politiques, en veillant à ce que la notion de « preuve exploitable » soit définie de manière à protéger réellement l'utilisateur final.
- **Assistance** : Si vous découvrez une campagne d'hameçonnage massive ciblant votre communauté locale, votre ALS peut vous aider à transmettre le

signalement aux autorités régionales compétentes et au service de conformité de l'ICANN.

La boîte à outils du reporting : transformer la sensibilisation en action

Savoir repérer les abus ne représente que la moitié du chemin. Pour construire un internet sain, il est tout aussi important de savoir les signaler efficacement. Ce guide propose une démarche claire en quatre étapes pour vous permettre d'agir concrètement lorsque vous constatez un problème.

Préparation du rapport : Rassemblez vos preuves

Avant de contacter qui que ce soit, vous devez « geler la situation ». Les bureaux d'enregistrement et l'ICANN exigent **des preuves concrètes** pour suspendre un domaine.

- **L'URL complète** : non pas simplement « le site web de la banque », mais la chaîne de caractères exacte (par exemple, `http://verify-bank-secure.top/login`).
- **Captures d'écran** : Preuve visuelle de la page d'hameçonnage ou de l'avertissement relatif aux logiciels malveillants.
- **En-têtes de courriel** : Si l'abus a eu lieu par

courriel, les en-têtes techniques (et pas seulement la ligne « De ») permettent d'en remonter à la source.

- **Horodatage** : Quand avez-vous constaté les abus ?

Phase 1 : Identifier le « propriétaire » (La recherche)

Vous ne pouvez pas signaler un domaine si vous ne savez pas qui le gère.

1. Allez à [Outil de recherche de données d'enregistrement ICANN](#).
2. Saisissez le nom de domaine suspect.
3. Recherchez le « **Registraire parrain** » et l'« **Adresse électronique de contact en cas d'abus** ».

Remarque : Si le domaine se termine par un code pays (comme `.uk`, `.br` ou `.in`), il s'agit d'un **ccTLD**. L'ICANN n'a aucune autorité contractuelle sur ces domaines. Vous devez vous renseigner auprès du gestionnaire. [Base de données de la zone racine IANA](#).

Phase 2 : Le rapport direct (le registraire)

En vertu des **amendements contractuels de 2024**, tous les bureaux d'enregistrement accrédités par l'ICANN sont désormais tenus d'enquêter et de prendre des mesures

d'atténuation lorsqu'ils reçoivent des rapports « bien étayés » d'abus du DNS.

- **Action** : Envoyez vos preuves à l'adresse électronique de contact en cas d'abus que vous avez trouvée lors de la phase 1.
- **À quoi s'attendre** : Vous devriez recevoir une confirmation automatique. Un registraire pourrait suspendre le domaine (le rendant inaccessible) si l'abus est avéré.
- **Patience** : accordez au registraire un « délai raisonnable » pour enquêter (généralement 24 à 48 heures pour les menaces urgentes comme le phishing).

Phase 3 : Escalade (Conformité contractuelle à l'ICANN)

Si le bureau d'enregistrement ignore un rapport bien étayé ou refuse d'agir face à un cas flagrant d'abus DNS, il est temps de passer à l'étape supérieure.

1. Visitez le [Portail de conformité contractuelle de l'ICANN](#).
2. Choisissez le formulaire « **Abus** » .
3. **Important** : Vous devez joindre la preuve que vous avez déjà essayé de contacter le registraire

(votre courriel envoyé et toute réponse ou absence de réponse).

Phase 4 : Le filet de sécurité communautaire (Le rôle de la SLA)

Parfois, un seul signalement ne suffit pas à stopper une attaque de grande envergure. C'est là que **les structures à grande échelle (ALS)** deviennent des plateformes puissantes :

- **Signalement groupé** : Si un agent de liaison scolaire (ALS) constate que des dizaines de personnes dans sa région sont ciblées par la même campagne, il peut lancer une « alerte collective » à son responsable régional de liaison (RALO).
- **Commentaires sur les politiques** : Si vous trouvez le processus de signalement trop difficile, votre ALS peut transmettre directement ces commentaires à l' **ALAC (Comité consultatif général)** , qui conseille le Conseil d'administration de l'ICANN sur la façon de rendre le système plus convivial.

Tableau récapitulatif : Qui dois-je contacter ?

Si le problème est...	Contact...	Pourquoi?

Hameçonnage / Logiciels malveillants	Le registraire	Ils peuvent « désactiver » le nom de domaine globalement.
Contenu illégal / Droit d'auteur	Le fournisseur d'hébergement	Ils contrôlent les fichiers sur le serveur (le contenu).
Inaction du registraire	Conformité à l'ICANN	Ils veillent à ce que le greffier respecte leur contrat.
Arnaques/fraudes locales	Police locale / CERT	Pour les enquêtes criminelles et les alertes publiques locales.

Chapitre 5

L'acceptation universelle – Un Internet pour tous.

Un internet véritablement mondial ne peut exister s'il oblige la moitié de la population mondiale à apprendre une deuxième langue rien que pour saisir une adresse web. L'acceptation universelle (AU) est le mouvement technique et social qui garantit que tous les noms de domaine et adresses électroniques valides — quels que soient le système d'écriture, la langue ou la longueur des caractères — puissent être utilisés par toutes les applications, tous les appareils et tous les systèmes connectés à internet.

Au-delà de l'alphabet latin : présentation des IDN

Pendant des décennies, le système de noms de domaine (DNS) s'est limité au sous-ensemble « LDH » (lettres, chiffres, traits d'union) de l'alphabet latin. Cela a créé une barrière numérique pour des milliards de personnes dont la langue maternelle utilise des alphabets non latins.

Les noms de domaine internationalisés (IDN) résolvent ce problème en autorisant les noms de domaine dans les langues et les systèmes d'écriture locaux, tels que :

- **Arabe:** شبكة. (dot- shabaka)
- **Chinois :** .网络 (réseau de points)
- **Dévanagari :** . भारत (point-Inde)

Pour rester compatibles avec l'infrastructure DNS existante, ces scripts sont convertis dans un format lisible par machine appelé **Punycode** (qui ressemble à `xn -- [chaîne]`). Tandis que l'ordinateur interprète le code, l'utilisateur voit sa langue maternelle, ce qui lui permet de naviguer sur Internet comme à la maison.

Objectif : Fonctionnalité sans faille

Le critère ultime de l'acceptation universelle est la parité.

Nous aspirons à un monde où :

- **utilisateur@email.thailand** (un domaine de premier niveau non ASCII)
- **用户@例子.中国**(une adresse e-mail en script complet)
- **contact@business.photography** (un long TLD « nouveau »)

Tous les noms de domaine doivent être traités avec la même fiabilité que **user@email.com** . Actuellement, de nombreux systèmes anciens rencontrent des dysfonctionnements face à ces adresses : ils les rejettent comme invalides dans les formulaires d'inscription ou ne parviennent pas à acheminer les courriels. La mise en œuvre de l'UA implique la mise à jour des logiciels à l'échelle mondiale afin d' **accepter, de valider, de traiter, de stocker et d'afficher** tous les noms de domaine de manière cohérente.

Le rôle d'ALS : Plaidoyer pour le citoyen du monde

Au sein de l'écosystème ICANN, les **structures At-Large (ALS)** représentent la voix de chaque internaute. Leur rôle dans l'acceptation universelle est crucial car l'UA n'est pas qu'une simple solution technique : c'est une question d'équité numérique.

Comment les organisations spécialisées dans la SLA impulsent le changement :

- 1· Sensibilisation locale :** Informer les développeurs de logiciels et les entreprises de la région sur l'importance de mettre à jour leurs systèmes pour prendre en charge les scripts locaux.
- 2· Influence politique :** Faire pression pour que les services numériques gouvernementaux adoptent les IDN, afin de garantir que les citoyens puissent interagir avec leur gouvernement dans leur langue maternelle.
- 3· Tests et signalements :** identifier les sites Web ou les applications « défectueux » qui n'acceptent pas les adresses électroniques locales et les signaler au Groupe de pilotage de l'acceptation universelle (UASG).

L'idée clé : lorsque nous parviendrons à une acceptation universelle, nous ne corrigerons pas seulement un bug technique ; nous libérerons le potentiel d'Internet pour le prochain milliard d'utilisateurs, garantissant ainsi que le « World Wide Web » soit enfin à la hauteur de son nom.

Chapitre 6

Le guide pratique en action : comment participer à la conversation.

Les chapitres précédents de ce guide ont éclairci les enjeux et les raisons de la gouvernance d'Internet. Nous abordons maintenant l'essentiel : **le « comment »**. Le savoir est un outil, mais la participation est le moteur du changement. Ce dernier chapitre vous servira de guide d'intégration au sein de la communauté des citoyens engagés.

1. Trouvez votre scène

Vous n'êtes pas seul dans cette aventure. Partout dans le monde, des centaines de **personnes**, d'organisations à but non lucratif, de groupes de défense des consommateurs et d'établissements universitaires représentent les intérêts des internautes.

Votre première étape : Visitez le [Consultez le site web de l'ICANN At-Large](#) et utilisez l'annuaire.

2. Rejoignez un groupe de travail

Il n'est pas nécessaire d'être un expert technique pour contribuer. Les travaux d'ICANN sur les politiques sont menés au sein **de groupes de travail** où l'aspect humain d'Internet est débattu. Que vous soyez avocat, enseignant, étudiant ou retraité, votre point de vue est précieux.

- **Élaboration de politiques :** Contribuer à définir les règles relatives aux noms de domaine et à la protection de la vie privée des utilisateurs.

- **Technologie** : Discutez de l'impact des nouvelles technologies comme l'IPv6 ou la blockchain sur les utilisateurs finaux.
- **Sensibilisation et mobilisation** : Aidez à traduire le jargon complexe en un langage compréhensible par votre communauté locale.
- **Médias sociaux et communication** : Utilisez vos compétences créatives pour sensibiliser le public aux droits numériques.

3. Participer à une réunion (physiquement ou virtuellement)

L'ICANN organise chaque année trois réunions publiques mondiales dans différentes villes du monde. Ces réunions sont gratuites et ouvertes à tous.

- **En personne** : Postulez pour une **bourse** ou le programme **NextGen@ICANN** , qui finance la participation des leaders émergents.
- **En ligne** : chaque session est diffusée en direct avec interprétation simultanée et accès à un chat. Vous pouvez lever la main et poser une question depuis votre salon ; elle sera enregistrée comme si vous étiez physiquement présent(e) dans la salle.

Le credo de l'utilisateur final

« Internet n'appartient à personne et à tous. Ma participation n'est pas seulement un droit ; c'est la garantie qui préserve un monde numérique ouvert, libre et sûr pour la prochaine génération. »

Conclusion

Le pouvoir de votre voix dans le modèle multipartite .

Nous avons entamé ce voyage en considérant Internet comme un vaste moteur invisible, que nous tenons souvent pour acquis jusqu'à ce qu'il dysfonctionne. Grâce à ce guide, nous avons levé le voile sur le jargon technique pour révéler une vérité simple et profonde : **Internet n'est gouverné ni par un seul roi, ni par une multinationale, ni par un groupe de gouvernements éloignés. Il est gouverné par vous.**

La place à table

Le secret d'un internet stable et ouvert réside dans le **modèle multipartite** . Contrairement aux organisations internationales traditionnelles où seuls les gouvernements ont voix au chapitre, le modèle de l'ICANN garantit que chaque voix compte.

En tant qu'utilisateur final, votre voix est représentée par le **Comité consultatif général (ALAC)** . Cette structure garantit que, lors de l'élaboration des politiques techniques, l'impact sur un étudiant dans un village rural ou un consommateur dans une métropole animée est pris en compte. Sans votre participation, l'équilibre est rompu ; grâce à vous, Internet demeure une ressource mondiale et équilibrée.

Un Internet sain est une responsabilité partagée.

Construire un « internet sain » n'est pas un aboutissement, mais un processus continu d'hygiène, de sensibilisation et

de participation. En lisant ce guide, vous avez déjà franchi la première étape pour devenir un **citoyen numérique (urbain ou rural)** plutôt qu'un simple consommateur.

- Vous êtes désormais en mesure de **détecter les abus DNS** et de protéger votre communauté.
- Vous comprenez la **procédure à suivre pour signaler les problèmes** via la boîte à outils de reporting.
- Vous connaissez votre **quartier**, d'AFRALO à NARALO.

La santé d'Internet repose sur l'engagement de ses utilisateurs. Vous avez les outils, votre place est à table, et le dialogue est déjà engagé. **Bienvenue !**

Dernier appel à l'action : Vos prochaines étapes

Ne vous arrêtez pas là. La santé d'Internet dépend de l'engagement de ses utilisateurs. Voici votre liste finale de vérification pour un impact maximal :

1. **Trouvez votre communauté** : Visitez le [Consultez le site web ICANN At-Large](#) et trouvez un représentant ALS dans votre pays ou région. Contactez-le.
2. **Exprimez-vous** : suivez les **débats publics** . Nul besoin d'être ingénieur pour dire : « *Cette politique rend l'accès à Internet plus difficile pour les membres de ma communauté.* »
3. **Aidez les autres** : partagez les sections « Bilan de santé » et « Outils de signalement » de ce livre avec une personne susceptible d'être vulnérable aux menaces numériques.

Conclusion

Internet a été bâti sur l'idée révolutionnaire que nous pouvons tous être connectés. Il prospère grâce à l'inclusion et reste sûr grâce à notre vigilance. En rejoignant la communauté At-Large, vous ne protégez pas seulement un réseau ; vous protégez le plus grand laboratoire mondial du potentiel humain.

Le plan de jeu est désormais entre vos mains. Utilisez-le à bon escient.

Glossaire : Parler « l'anglais de l'ICANN »

Comprendre le monde de la gouvernance d'Internet peut s'apparenter à l'apprentissage d'une langue étrangère. Ce glossaire explique les acronymes et les termes les plus courants que vous rencontrerez au sein de la communauté des acteurs d'Internet.

Le « Who's Who » de la gouvernance

Terme	Ce que cela représente	Définition en langage clair
ALAC	Comité consultatif général	L'organe de 15 membres qui représente la voix des utilisateurs individuels d'Internet au sein de l'ICANN.
SLA	Structure en pleine expansion	Une organisation locale ou régionale

		(comme un groupe de consommateurs ou un club technologique) officiellement accréditée par l'ICANN.
ICANN	Société Internet pour l'attribution de noms et de numéros	L'organisation mondiale à but non lucratif qui coordonne le « répertoire d'adresses » d'Internet (le DNS).
RALO	Organisation régionale à grande échelle	Les cinq pôles régionaux (Afrique, Asie/Pacifique, Europe, Amérique latine/Caraïb

		es, Amérique du Nord) qui organisent les ALS .
--	--	--

La « plomberie » technique

- **DNS (Domain Name System)** : Le système qui traduit les adresses web conviviales pour les humains (comme `google.com`) en adresses IP conviviales pour les ordinateurs (comme `192.0.2.1`).
- **gTLD (Domaine générique de premier niveau)** : L'extension d'une adresse web qui n'est pas liée à un pays, comme `.com`, `.org` ou les extensions plus récentes comme `.photography`.
- **ccTLD (domaine de premier niveau de code pays)** : extensions de domaine réservées aux pays ou territoires, comme `.uk` (Royaume-Uni), `.jp` (Japon) ou `.ng` (Nigeria).
- **IDN (Nom de domaine internationalisé)** : Noms de domaine utilisant des alphabets locaux comme l'arabe, le chinois ou le cyrillique, permettant aux internautes de naviguer sur le web dans leur langue maternelle.
- **Bureau d'enregistrement** : Une entreprise (comme GoDaddy ou Namecheap) où vous pouvez

acheter et enregistrer un nom de domaine.

- **Registre** : L'organisation qui gère la liste principale de tous les noms de domaine sous un TLD spécifique (par exemple, Verisign gère le registre `.com`).

Politiques et sécurité

- **Abus de DNS** : activité intentionnelle et malveillante qui utilise le système de noms de domaine pour causer des dommages (hameçonnage, logiciels malveillants, réseaux de zombies, pharming ou spam).
- **multipartite** : un cadre organisationnel dans lequel toutes les parties – y compris les gouvernements, le secteur privé, la société civile et les utilisateurs finaux – collaborent sur un pied d'égalité.
- **Consultation publique** : Période du processus d'élaboration des politiques durant laquelle l'ICANN invite le grand public à soumettre ses opinions sur les changements proposés.
- **UA (Acceptation universelle)** : L'objectif est de garantir que tous les noms de domaine et adresses électroniques valides – quelle que soit leur longueur ou leur syntaxe – fonctionnent parfaitement dans toutes les applications compatibles avec Internet.
- **WHOIS / RDAP** : Protocoles utilisés pour rechercher des informations sur le propriétaire ou le

gestionnaire d'un nom de domaine spécifique.

Conseil de pro : Si vous entendez un terme lors d'une réunion de l'ICANN qui ne figure pas sur cette liste, n'hésitez pas à poser des questions !

La communauté At-Large est réputée pour être le point d'entrée le plus accueillant pour les nouveaux arrivants.