SAC132

Le système des noms de domaine repose sur des logiciels libres et à code source ouvert (FOSS)

Rapport du Comité consultatif sur la sécurité et la stabilité de l’ICANN (SSAC)
25 septembre 2025

Préface

Le présent rapport du Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC) s'adresse au Conseil d'administration de l'ICANN, à l'organisation ICANN, à la communauté de l'ICANN et, plus largement, à l'ensemble de la communauté Internet. Il met en lumière la dépendance du système des noms de domaine (DNS) à l'égard des logiciels libres et à code source ouvert (FOSS).

Le SSAC se concentre sur des questions liées à la sécurité et à l'intégrité des systèmes de nommage et d'allocation d'adresses Internet. Ceci inclut des questions opérationnelles (par exemple se rapportant au fonctionnement correct et fiable du système de publication de la zone racine), des questions liées à l'administration technique (par exemple se rapportant à l'allocation d'adresses et à l'attribution de numéros sur Internet), et des questions liées à l'enregistrement (par exemple se rapportant aux services des registres et des bureaux d'enregistrement). Le SSAC procède de façon continue à l'évaluation des menaces et à l'analyse des risques auxquels sont confrontés les services de nommage et d'allocation d'adresses Internet afin de déterminer les principales menaces à la sécurité et à la stabilité, et conseille la communauté de l'ICANN en conséquence. Il n'est pas habilité à adopter ou à faire appliquer des règles, ni à statuer. Ces fonctions relèvent d'autres entités, et l'avis donné ici doit être examiné sur le fond. Les membres du SSAC participent à titre individuel et non pas en tant que représentants de leurs employeurs ou d'autres organisations. Il y a consensus du SSAC sur un document lorsque les auteurs se mettent d'accord sur le contenu et les recommandations sans objections finales de la part du reste des membres du SSAC, à l'exception des désistements indiqués à la fin du document.

Table des matières

Liste des figures

Liste des tableaux

Résumé analytique

Le système des noms de domaine (DNS) est un système mondial, hiérarchique et décentralisé, dont les informations sous-tendent la quasi-totalité des interactions en ligne. Sa fonction première est d'établir une correspondance entre les noms de domaine, intelligibles pour l'utilisateur, et les adresses IP, exploitables par les ordinateurs et indispensables pour localiser les ressources sur le réseau. Qu'il s'agisse de naviguer sur le Web, d'envoyer un courriel ou d'utiliser une application mobile, toute connexion en ligne s'appuie sur des informations émanant du DNS, qui en assure également la structuration.

Le constat fondamental de ce rapport est le suivant : le DNS est construit et maintenu grâce à des logiciels libres et à code source ouvert (FOSS). Il ne s'agit pas d'une pratique marginale, mais bien de la réalité dominante. Les FOSS constituent la norme pour les composants les plus essentiels de l'infrastructure du DNS. À titre d'exemple, au moins neuf des douze organisations indépendantes qui exploitent le système des serveurs racine de l'Internet (RSS) ont exclusivement recours à des implémentations FOSS, tout comme neuf des dix plus grands fournisseurs de services pour les domaines de premier niveau (TLD). Cette prédominance s'explique par les atouts intrinsèques du modèle de développement des FOSS, qui conjugue efficacité économique et simplicité d'adoption avec la transparence, la sécurité collaborative et la résilience opérationnelle indispensables à toute infrastructure critique.

Bien que le modèle de développement des FOSS soit radicalement différent de celui des logiciels propriétaires, les FOSS ne sont pas intrinsèquement plus ou moins sécurisés. La sécurité d'un projet logiciel, quel qu'il soit, dépend de la qualité de ses processus de développement et de maintenance, et non de la visibilité de son code source. À l'inverse des logiciels commerciaux, les FOSS sont le fruit d'un effort collaboratif mondial articulé autour de quatre libertés fondamentales : utiliser, étudier, partager et modifier. Cet écosystème repose sur un réseau planétaire de mainteneurs et de contributeurs, pour la plupart bénévoles. Cela dit, l'espace du DNS a la particularité de reposer également sur une poignée d'organisations de maintenance pérennes. Il en résulte un modèle fondé sur la collaboration communautaire plutôt que sur les contrats commerciaux d'une chaîne d'approvisionnement logicielle classique, ce qui introduit des risques spécifiques : la précarité financière pour les organisations de maintenance et l'épuisement pour les mainteneurs bénévoles.

Ces particularités signifient que les cadres réglementaires conçus pour les logiciels propriétaires peuvent se révéler mal adaptés aux FOSS et risquent donc d'avoir de graves conséquences involontaires sur la stabilité des infrastructures critiques de l'Internet. Afin de d'assimiler cette complexité et de promouvoir un écosystème numérique sûr, le Comité consultatif sur la sécurité et la stabilité (SSAC) formule les recommandations suivantes à l'intention des décideurs :

- **Reconnaître le rôle critique des FOSS :** les décideurs devraient reconnaître explicitement, dans tout texte législatif ou réglementaire pertinent, que les infrastructures critiques de l'Internet dépendent des FOSS et que l'usage de ces derniers constitue un atout à préserver.

- **Consulter la communauté des FOSS :** l'élaboration des lois et règlements doit se nourrir de consultations menées auprès de toutes les composantes de l'écosystème FOSS, des mainteneurs individuels aux organisations à but non lucratif et aux entreprises.
- **S'inspirer des exemples contemporains en matière de réglementation des FOSS :** les décideurs trouveront, dans le rapport, des études de cas récents sur des approches novatrices qui tiennent compte des spécificités du modèle de développement des FOSS.
- **Favoriser la pérennité des FOSS :** encourager les contributions des secteurs public et privé aux projets FOSS d'importance critique, en les considérant comme une forme d'investissement dans un bien public commun.
- **Répondre collectivement aux risques systémiques :** promouvoir et financer des solutions collaboratives à l'échelle de l'écosystème, afin d'atténuer les risques découlant des dépendances partagées, plutôt que d'en imposer la charge aux mainteneurs individuels.

1 Introduction

Le présent rapport fait écho à la volonté croissante des décideurs de s'associer aux efforts que déploie le secteur pour réduire les vulnérabilités logicielles des infrastructures numériques. À l'heure où gouvernements et organismes de réglementation s'efforcent, partout dans le monde, de sécuriser la chaîne d'approvisionnement logicielle, il est impératif que ces démarches reposent sur une compréhension précise de la conception et de la maintenance des systèmes fondamentaux de l'Internet. À titre d'exemple, plusieurs interventions réglementaires (proposées) ont récemment visé à atténuer ces vulnérabilités :

- le code de bonnes pratiques volontaire en matière de sécurité logicielle, à l'intention des éditeurs de logiciels au Royaume-Uni[1] ;
- l'auto-attestation, par le secteur, de pratiques de développement logiciel sécurisées, à l'usage du gouvernement des États-Unis[2] ;
- les conditions d'accès au marché (« Règlement sur la cyberrésilience » ou CRA) pour les produits numériques (y compris les logiciels) au sein de l'UE[3] ;
- les obligations de gestion des risques et de signalement incombant aux fournisseurs d'infrastructures numériques dans l'UE (« Directive NIS 2 »)[4] ;
- 'intégration des communautés « code source ouvert » est indiquée comme objectif de développement dans le plan quinquennal de la Chine pour les technologies de l'information[5,6].

Si les logiciel libres et à code source ouvert (FOSS) représentent aujourd'hui la norme dominante en matière de développement logiciel, leurs spécificités sont souvent négligées dans le discours politique. Or, toute intervention réglementaire décidée sans comprendre le modèle unique de développement et de distribution des FOSS risquerait de compromettre la sécurité et la stabilité des infrastructures critiques qui en dépendent, notamment les systèmes de routage et de noms de

[1] « *Software Security Code of Practice* » [Code de bonnes pratiques concernant les logiciels]. Ministère de la Science, de l'Innovation et de la Technologie du Royaume-Uni, 7 mai 2025. https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice.
[2] « *Secure Software Development Attestation Form* » [Formulaire d'attestation de développement de logiciel sécurisé]. Agence de cybersécurité et de sécurité des infrastructures (CISA) des États-Unis, https://www.cisa.gov/secure-software-attestation-form.
[3] « Règlement sur la cyberrésilience : les députés adoptent la loi renforçant la sécurité des produits numériques », Communiqué de presse du Parlement européen, 12 mars 2024, https://www.europarl.europa.eu/news/fr/press-room/20240308IPR18991/les-deputes-adoptent-la-loi-sur-la-cyber-resilience.
[4] « Règlement sur la cyberrésilience : les députés adoptent la loi renforçant la sécurité des produits numériques ». Communiqué de presse. Parlement européen, 12 mars 2024. https://www.europarl.europa.eu/news/fr/press-room/20240308IPR18991/les-deputes-adoptent-la-loi-sur-la-cyber-resilience.
[5] « *14th Five-Year Plan for the Software and Information Technology Services Industry* » [14e plan quinquennal pour le secteur des services informatiques et logiciels]. Conseil des affaires d'État de la République populaire de Chine, Ministère de l'Industrie et des Technologies de l'information, décembre 2021. https://www.gov.cn/zhengce/zhengceku/2021-12/01/5655205/files/a44b507d67c74591ad4f5e55b98c4518.pdf.
[6] *Traduction en anglais : « 14th Five-Year Plan for National Informatization* ». DigiChina Project, Université de Stanford, 24 janvier 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

domaine de l'Internet. Ce rapport a pour vocation d'apporter cet éclairage contextuel indispensable.

Contrairement aux pratiques en vigueur dans d'autres secteurs, l'essentiel des logiciels régissant le fonctionnement de l'Internet est diffusé sous licence de droit d'auteur FOSS. Ces licences ne sont pas une question de coût, mais de liberté. Concrètement, les licences FOSS garantissent aux opérateurs d'infrastructures quatre libertés fondamentales : utiliser, étudier, modifier et partager le logiciel — dans sa version originale ou modifiée — avec tous. Bien plus que de simples logiciels « gratuits » [7], les FOSS constituent un modèle de développement qui est le socle de l'effort collaboratif mondial par lequel est bâtie et maintenue une grande partie de l'infrastructure critique de l'Internet.

La structure de ce rapport vise à offrir aux décideurs une vision exhaustive du rôle des FOSS au sein du système des noms de domaine (DNS) et de l'écosystème d'enregistrement des noms de domaine.

- La section 2 propose une introduction non technique au DNS, dont elle expose les composants et les fonctions clés.
- La section 3 détaille le modèle FOSS, ses caractéristiques essentielles, ses atouts intrinsèques et les risques qui lui sont propres par rapport aux logiciels propriétaires.
- La section 4 présente les travaux de recherche du Comité consultatif sur la sécurité et la stabilité (SSAC) quant à la prévalence des FOSS, et met en évidence leur prépondérance dans les segments les plus critiques du DNS.
- La section 5 examine plusieurs cas d'actualité (États-Unis, Royaume-Uni, Union européenne) illustrant la manière dont les décideurs adaptent la réglementation sur la cybersécurité aux réalités singulières de l'écosystème des FOSS.
- La section 6 synthétise l'analyse du rapport en une série de conclusions ; celles-ci constituent la base factuelle des recommandations énoncées à la section 7.
- La section 7 formule, à l'intention des décideurs, des recommandations concrètes et pratiques.

[7] Les FOSS peuvent être utilisés à n'importe quelle fin et sont exempts de restrictions telles que l'expiration de licence ou les limitations géographiques. Leur code peut être étudié par quiconque, sans accord de non-divulgation ou restriction similaire. Ils peuvent être partagés et copiés à un coût quasi nul. De plus, les FOSS peuvent être modifiés par quiconque, et les améliorations ainsi apportées peuvent être partagées publiquement. La restriction ou l'absence d'une seule de ces libertés signifie qu'une application est propriétaire, et donc qu'il ne s'agit pas d'un logiciel à code source ouvert. Les quatre libertés sont conférées par une licence logicielle. Les licences logicielles définissent les conditions dans lesquelles un programme peut être utilisé et réutilisé. Pour qu'un logiciel soit libre, le texte de la licence doit contenir au moins ces quatre libertés. La Free Software Foundation (https://www.gnu.org/licenses/license-list.html), l'Open Source Initiative (https://opensource.org/licenses) et le projet Debian (https://wiki.debian.org/DFSGLicenses) tiennent à jour des listes de licences examinées et approuvées. Une application ne peut généralement pas être considérée comme FOSS si sa licence ne figure pas dans l'une de ces listes.

2. Introduction au DNS

L'envoi d'un courriel, la consultation d'une page Web ou les échanges par messagerie instantanée impliquent l'envoi et la réception, par votre appareil (ordinateur, téléphone, tablette), de milliers d'informations. Ces informations sont comparables à une carte postale numérique : elles comportent l'adresse de l'expéditeur, celle du destinataire et un contenu. Tout appareil connecté à l'Internet se voit attribuer au moins une adresse de protocole Internet (IP) unique. La mémoire humaine retenant plus aisément les noms que les suites de chiffres, le DNS agit comme l'annuaire de l'Internet : il assure la liaison entre l'adresse IP et le nom de domaine pour faciliter la navigation de tous[8,9]. Le DNS est un système critique, garant de la stabilité, la sécurité et l'interopérabilité continues de l'Internet mondial.

Il assure la correspondance entre des noms de domaine intelligibles pour l'utilisateur (ex. : icann.org) et des adresses IP numériques exploitables par les ordinateurs (ex. : 192.0.43.7 ou 2001:db8::1). L'ensemble de ces correspondances forme un espace de nommage mondial. Pour qu'un site Web ou un compte de messagerie soit accessible via un nom de domaine, le titulaire de ce dernier doit publier les correspondances relatives au service. Cette publication dans le DNS rend accessible à tout internaute le lien entre le nom de domaine et l'adresse IP du service.

Comme l'illustre la figure 1, l'écosystème du DNS comporte trois parties principales :

- L'enregistrement des noms de domaine (encadré bleu clair) : le cadre administratif et contractuel régissant l'acquisition des noms de domaine.
- L'infrastructure du DNS (encadré vert) : les systèmes techniques qui rendent les noms de domaine opérationnels sur Internet en les traduisant en adresses IP.
- L'utilisateur final et les services de contenu (encadrés orange et bleu foncé) : les services que les personnes exploitent en bout de chaîne, tel que les sites Web et les messageries électroniques.

Ce rapport se concentre sur l'enregistrement des noms de domaine et l'infrastructure du DNS, qui constituent ensemble une couche de l'infrastructure critique de l'Internet. La fonction de recherche d'informations dans l'espace des noms mondial n'est généralement pas monétisée ; elle est fournie « gratuitement » aux clients. L'infrastructure assurant ce service mondial distribué, considéré comme un « bien public non marchand », est ici qualifiée d'« infrastructure du DNS ». Ce système, largement réparti sur Internet, se compose de multiples éléments gérés par de nombreuses organisations indépendantes, chacune jouant un rôle précis. L'interopérabilité de ces systèmes est assurée par la normalisation des détails techniques nécessaires à leurs interfaces et communications, sous l'égide du Groupe de travail de génie Internet (IETF).

[8] ICANN. « Le système des noms de domaine », 13 septembre 2022. https://www.icann.org/resources/pages/dns-2022-09-13-en.
[9] Cloudflare. « Qu'est-ce que le DNS ? | Fonctionnement du DNS » https://www.cloudflare.com/learning/dns/what-is-dns/.

Il convient de distinguer cette infrastructure critique du contenu qu'elle achemine. L'enregistrement d'un nom de domaine n'est pas à confondre avec la création d'un site Web, pas plus que la publication d'un nom de domaine dans le DNS (pour le rendre repérable) n'est à confondre avec la publication du contenu d'un site Web. Le présent rapport examine le logiciel fondamental qui fait fonctionner l'annuaire, et non les informations inscrites sur ses pages.

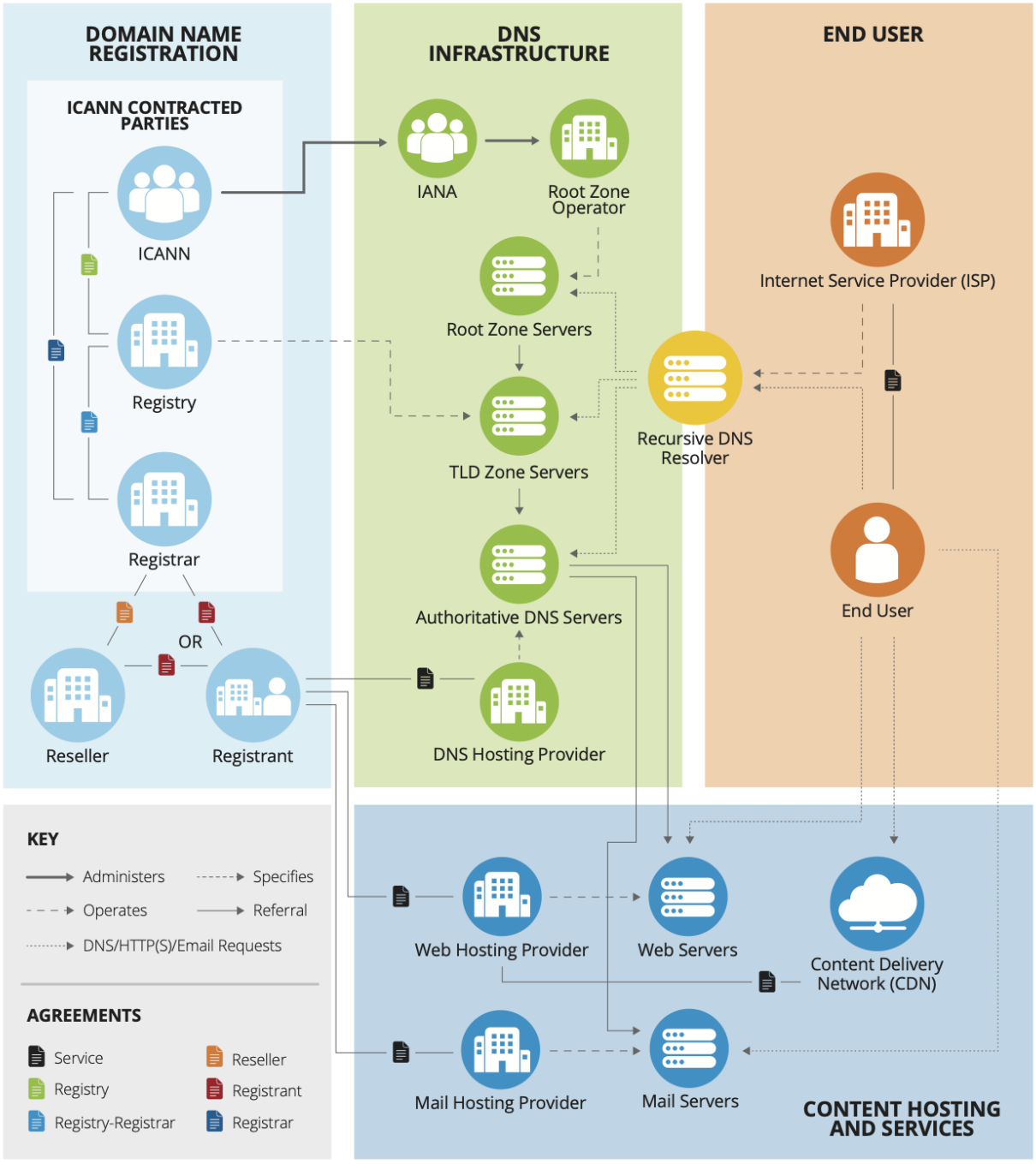

Figure 1 : *L'écosystème de l'Internet* Drazek, Keith. « *DNS Security: Ongoing Community Work to Mitigate Domain Name System (DNS) Security Threats* » [Sécurité du DNS : travail communautaire continu pour atténuer les menaces à la sécurité du système des noms de

domaine] Blog de Verisign, 7 décembre 2021. https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/.

2.1 Hiérarchie du DNS

Le DNS est un système distribué, hiérarchique et réparti à l'échelle mondiale. Désigné par le terme « Infrastructure du DNS » à la figure 1, il est conçu pour la résilience, garantissant ainsi l'absence de point de défaillance unique pour l'Internet mondial.

La figure 2 illustre la structure hiérarchique de l'espace de noms du DNS.

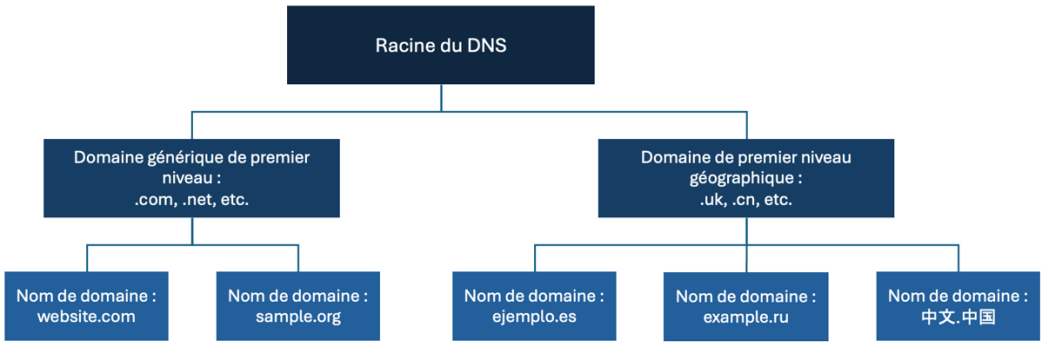

Figure 2: *Hiérarchie du DNS*

La racine du DNS (.) trône au sommet de la hiérarchie ; elle est desservie par le système des serveurs racine (SSR)[10]. La racine pointe vers les serveurs faisant autorité pour les différents domaines de premier niveau (TLD). Les TLD constituent le suffixe des noms de domaine et se divisent en deux grandes catégories :

- les TLD génériques (gTLD), qui sont des domaines à vocation générale tels que .com, .org, .xyz et .shop[11] ;
- les TLD géographiques (ccTLD), réservés aux pays, territoires et lieux géographiques figurant sur la liste des codes de pays de la norme ISO 3166-1[12]. Les ccTLD peuvent baser leurs noms sur les codes de pays à deux lettres définis par la norme ISO 3166-1 (ex. : .jp pour le Japon, .fr pour la France, .ke pour le Kenya), ou représenter un nom de

[10] Le système de serveurs racine est composé de serveurs dispersés dans le monde entier et exploités par 12 organisations indépendantes. Pour en savoir plus sur les opérateurs de serveurs racine, consulter le « RSSAC023v2 : Histoire du système des serveurs racine ». Comité consultatif du système des serveurs racine de l'ICANN (RSSAC), 17 juin 2020. https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf.

[11] ICANN. « Termes et acronymes, domaine générique de premier niveau (gTLD) », https://www.icann.org/fr/icann-acronyms-and-terms/generic-top-level-domain-fr.

[12] Organisation internationale de normalisation. « ISO 3166 — Codes des noms de pays », https://www.iso.org/fr/iso-3166-country-codes.html.

pays ou de territoire dans des scripts autres que les caractères ASCII[13]. Ce dernier concept, connu sous le nom de « nom de domaine internationalisé (IDN) », est mis en œuvre par l'ICANN depuis 2009.

Sous les TLD se trouvent les noms de domaine individuels. Un nom de domaine consiste en une série de segments de texte séparés par des points. Comme le montre la figure 3, un nom de domaine se construit de droite à gauche, en commençant par le TLD. Ainsi, dans icann.org, le TLD est .org et le domaine de second niveau est icann ; ensemble, ils forment un nom de domaine unique. Dans le second exemple, bbc.co.uk, le TLD est .uk et le domaine de second niveau est .co. Ce système hiérarchique et décentralisé assure la robustesse et la résilience de l'Internet mondial.

Le nom de domaine représente un nom unique qui forme la base de l'adresse universelle (URL) utilisée pour accéder à une ressource spécifique sur Internet. Le nom de domaine lui-même désigne une adresse bien précise sur Internet, qui correspond à une entité telle qu'une entreprise, une organisation, une institution ou un particulier[14].

[13] ICANN. « Termes et acronymes, domaine de premier niveau géographique (ccTLD) », https://www.icann.org/fr/icann-acronyms-and-terms/generic-top-level-domain-fr.
[14] ICANN. « Termes et acronymes, nom de domaine », https://www.icann.org/fr/icann-acronyms-and-terms/domain-name-fr.

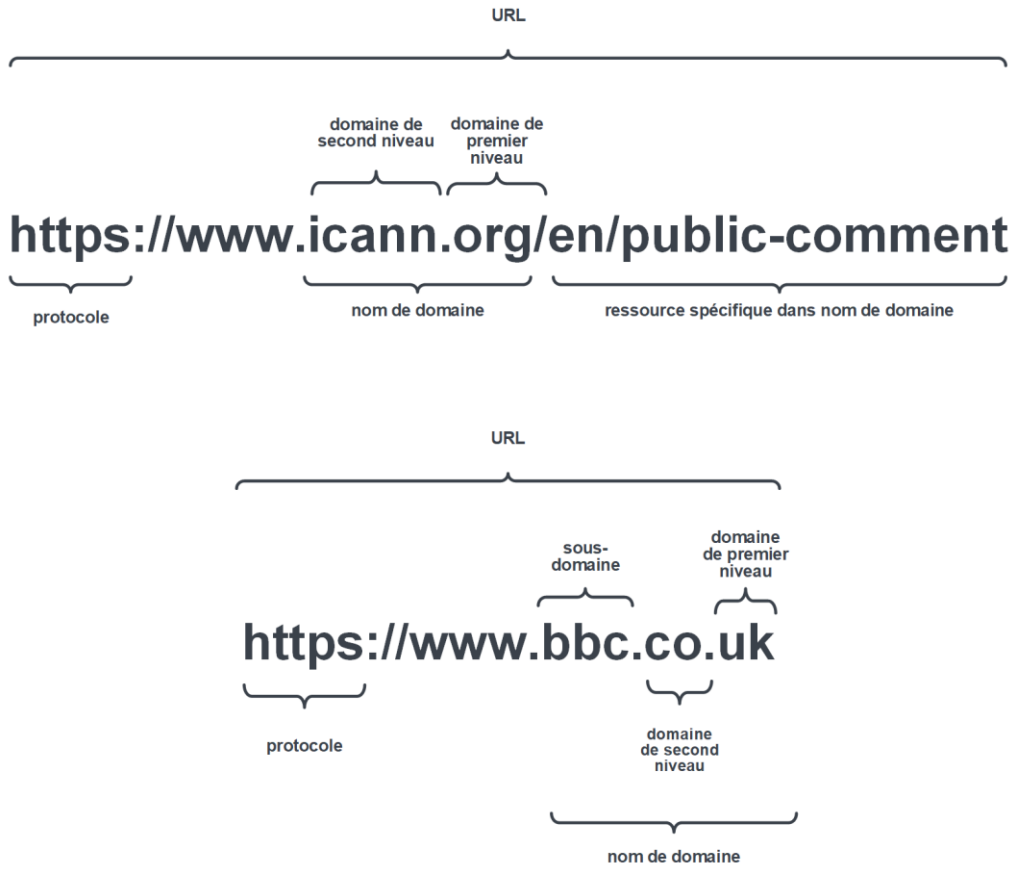

Figure 3 : *Composantes d'une URL et d'un nom de domaine*

2.2 Enregistrement et publication des noms de domaine

L'infrastructure d'enregistrement des noms de domaine désigne les systèmes qui facilitent l'acquisition d'un nom de domaine unique. Ce mécanisme, illustré dans la section « Enregistrement de nom de domaine » de la figure 1, mobilise plusieurs acteurs clés autour de deux processus distincts : l'enregistrement et la publication.

L'enregistrement consiste à réserver un nom de domaine. Le titulaire de nom de domaine est la personne physique ou morale qui enregistre un nom de domaine spécifique et en détient les droits. Pour enregistrer un nom sous un TLD donné, le titulaire doit passer par un bureau d'enregistrement. Ce dernier est une organisation, en interface directe avec le public, qui agit comme revendeur de noms de domaine. Les bureaux d'enregistrement constituent de fait le canal de distribution des enregistrements ; ils gèrent les paiements, les renouvellements et autres informations administratives. Ils interagissent ensuite avec un registre, la base de données principale faisant autorité pour l'ensemble des noms d'un TLD. L'organisation qui maintient cette base de données est appelée l'opérateur de registre. Pour automatiser les millions de transactions qui s'opèrent entre eux, les bureaux d'enregistrement et les opérateurs de registre utilisent le protocole d'avitaillement extensible (EPP), protocole normalisé régissant l'enregistrement, le renouvellement et le transfert des noms de domaine.

Tout enregistrement réussi aboutit à la publication des enregistrements DNS du domaine sur les serveurs faisant autorité de l'infrastructure du DNS, rendant le domaine accessible sur Internet. La publication est le processus technique de mise à disposition des enregistrements DNS sur les serveurs de noms faisant autorité. Ces serveurs contiennent la correspondance entre les noms de domaine intelligibles pour l'utilisateur et les adresses IP exploitables par les machines, une fonction critique pour la localisation et l'authentification des sites Web, serveurs de messagerie et autres ressources Internet.

2.3 Résolution du DNS

La saisie d'un nom de domaine tel que www.example.com dans un navigateur déclenche la « résolution du DNS ». Ce processus repose sur la synergie de deux composants de l'infrastructure : les résolveurs récursifs et les serveurs faisant autorité (voir Figure 4).

Figure 4: *Résolution classique du DNS*

Les serveurs faisant autorité sont les composants qui publient les informations du domaine. Ils détiennent l'enregistrement officiel et définitif d'un domaine donné et le rendent consultable. Ces serveurs de noms sont exploités par des particuliers, des entreprises, des universités, des fournisseurs de services et des entités gouvernementales. Les serveurs de noms des TLD, par exemple, publient les données techniques de tous les domaines individuels de leur registre. De nombreuses organisations disposent de services DNS locaux qui fournissent exclusivement des informations propres à leur organisation interne, comme la localisation de sites Web départementaux sur un intranet. Ce pan important du DNS reste invisible depuis l'Internet ouvert.

Si certains utilisateurs finaux et petites entreprises confient la publication de leurs données de domaine à leur bureau d'enregistrement ou aux services faisant autorité de leur hébergeur, il est fréquent que les administrations publiques et les entreprises gèrent leurs serveurs séparément, soit en interne, soit en externalisation. La fiabilité et la redondance étant des préoccupations majeures, les administrateurs des informations de « zone » publiées sous un domaine souscrivent souvent des « services DNS faisant autorité secondaires » auprès de fournisseurs tiers. Ces fournisseurs publient les mêmes données que les serveurs DNS faisant autorité primaires. Bon

nombre des organisations proposant ces services sont celles qui fournissent également des services DNS faisant autorité pour les TLD.

Les résolveurs facilitent l'extraction des informations du DNS. Ils agissent pour le compte de l'appareil utilisateur (le « client », tel qu'un smartphone) pour trouver la bonne adresse IP. Dans un souci d'efficacité, les résolveurs maintiennent un « cache », base de données constamment actualisée des recherches récentes. En pratique, il est courant que les résolveurs répondent à jusqu'à 90 % des requêtes à partir de leur cache local, ce qui est beaucoup plus rapide que d'interroger des serveurs Internet distants. En l'absence de réponse en cache, ils doivent interroger les serveurs faisant autorité. Le fort volume de trafic, qui assure le rafraîchissement continu du cache, fait des résolveurs des systèmes particulièrement sollicités.

Il existe des millions de résolveurs à travers le monde. La fonction de résolveur peut être locale (au sein du réseau de l'utilisateur ou du fournisseur d'accès) ou hébergée dans le nuage (soit comme service distinct hébergé sur Internet, soit conjointement avec d'autres services en nuage). Quelle que soit la configuration du service, il importe de veiller à ce que seuls les utilisateurs prévus puissent l'interroger. Un service ouvert à quiconque sur Internet risque d'être détourné par des acteurs malveillants, par exemple lors d'attaques par déni de service distribué (DDoS). La configuration de l'appareil de l'utilisateur détermine généralement le fournisseur privilégié. Outre les résolveurs locaux fournis par les universités, entreprises et fournisseurs de services Internet (FSI), il existe des services en nuage prisés comme Google (8.8.8.8), Quad9 (9.9.9.9) et Cloudflare (1.1.1.1). Le choix du fournisseur de résolveur dépend de facteurs clés tels que la politique organisationnelle, les politiques de filtrage ou de liste de blocage du résolveur, et la disponibilité de transports DNS chiffrés. Le processus de résolution (Figure 4) illustre l'interaction de ces composants au sein de la hiérarchie du DNS.

3 Le modèle FOSS : caractéristiques clés et enjeux

Après avoir dressé, dans la section précédente, le tableau de l'infrastructure du DNS et de l'enregistrement des noms de domaine, systèmes vitaux pour la navigation sur Internet, il convient d'examiner dans la présente section la construction et la maintenance de cette infrastructure critique. Les logiciels qui sous-tendent cette infrastructure sont majoritairement des logiciels libres et à code source ouvert (FOSS). Ce type de logiciel obéit à une logique de développement et à un modèle économique radicalement différents de ceux des logiciels propriétaires. Toute discussion éclairée sur les politiques exige donc une parfaite compréhension de ces caractéristiques uniques.

3.1 Les rôles clés dans l'écosystème des FOSS

À la différence du modèle classique de logiciels à code source fermé, où le développement est centralisé au sein d'une entité juridique unique, le modèle FOSS est ouvert et distribué. Les rôles, loin de s'exclure mutuellement, peuvent être endossés par quiconque, en tout lieu. Aux fins du présent rapport, la terminologie suivante est retenue :

- **Mainteneur :** Personne ou groupe responsable de l'orientation générale d'un projet FOSS. En leur qualité de gardiens du projet, les mainteneurs ont autorité pour accepter ou rejeter les contributions à la version officielle, gage de qualité et de cohérence.
- **Contributeur :** Personne physique ou morale proposant des améliorations (soumission de code, documentation, signalement de bogues). Ces apports sont soumis à l'examen d'un mainteneur avant toute intégration au projet officiel.
- **Utilisateur ou opérateur :** Personne physique ou morale déployant et exploitant le logiciel. Dans le contexte du DNS, l'« opérateur » gère des composants d'infrastructure, tels que les serveurs faisant autorité ou les résolveurs. Les utilisateurs et les opérateurs constituent une partie essentielle de l'écosystème, car ils fournissent des retours d'expérience et donnent une raison d'être au projet.

Dans un souci de clarté, ce rapport privilégie les termes « mainteneur » et « contributeur » à celui, plus générique, de « développeur », un individu pouvant écrire du code en tant que mainteneur, contributeur, ou à titre indépendant.

3.2 Principes fondamentaux du modèle de développement FOSS

La nature du modèle FOSS découle des droits conférés par ses licences. Pour qu'un programme soit qualifié de FOSS, sa licence doit garantir aux utilisateurs quatre libertés fondamentales[15,16] :

- la liberté ***d'utiliser*** le logiciel à toutes fins, sans restrictions (durée de licence, limitation géographique, etc.) ;
- la liberté ***d'étudier*** le fonctionnement du programme, ce qui implique l'accès au code source sans accord de confidentialité ;
- la liberté ***de partager*** le logiciel, c'est-à-dire de le redistribuer et de le copier à un coût quasi nul ;
- la liberté ***de modifier*** le programme et de rendre publiques les améliorations qui y ont ainsi été apportées.

La restriction ou l'absence d'une seule de ces libertés relègue le logiciel au rang de solution propriétaire. Ces libertés fondent les caractéristiques intrinsèques des FOSS, qui le distinguent nettement des logiciels propriétaires. Des organisations comme la Free Software Foundation[17], l'Open Source Initiative[18] et le Projet Debian[19] tiennent à jour des listes de licences logicielles examinées et approuvées comme répondant à ces critères.

[15] Système d'exploitation GNU. « Qu'est-ce que le logiciel libre ? », https://www.gnu.org/philosophy/free-sw.html.
[16] Une autre définition courante de ce qui constitue une licence FOSS est celle donnée par l'Open Source Initiative dans son document « *Open Source Definition* » [Définition du code source ouvert] https://opensource.org/osd.
[17] Système d'exploitation GNU. « Licences commentées », https://www.gnu.org/licenses/license-list.html.
[18] Open Source Initiative. « *OSI Approved Licenses* » [Licences approuvées par l'OSI], https://opensource.org/licenses.
[19] Wiki de Debian. « *DFSGLicenses* », https://wiki.debian.org/DFSGLicenses.

Ces quatre libertés ne sont pas de simples principes abstraits ; elles constituent le socle du modèle unique de développement et des particularités économiques des FOSS, décrits ci-après.

3.2.1 Le modèle FOSS permet un développement collaboratif mondial

En autorisant l'étude, la modification et le partage du code, les licences FOSS favorisent une collaboration ouverte de développement logiciel à l'échelle planétaire. Aucune condition arbitraire ne vient brider la participation au développement des FOSS, ce qui permet à tout individu d'apporter sa pierre à l'édifice. Les contributions peuvent provenir d'un large éventail de personnes physiques ou morales, parfois dans le cadre du développement d'un produit par une entreprise, parfois sur une base individuelle bénévole.

Le produit qui en résulte est mis à la disposition de tous, gratuitement, pas dans n'importe quel but (y compris commercial) mais pour être développé davantage. Cette ouverture fluidifie l'évolution du logiciel : la réintégration des modifications dans le produit logiciel accélère l'ajout de fonctionnalités ainsi que la correction des bogues et des failles de sécurité. La nature collaborative des FOSS est un vecteur de transparence et d'innovation rapide. De plus, les contributions elles-mêmes sont normalement ouvertes, permettant à des tiers d'inspecter les propositions et de commenter leur pertinence ainsi que l'intérêt de leur intégration dans le logiciel.

Cependant, il est rare que toutes les contributions soient acceptées sans un certain niveau d'inspection et d'acceptation. Ces contrôles visent à réduire le risque d'inclusion d'un code incohérent, erroné ou malveillant qui pourrait compromettre le logiciel. L'acceptation des contributions est par ailleurs soumise à certaines conditions courantes, notamment la nécessité de préserver les droits d'auteur et la propriété intellectuelle. Règle d'or des FOSS : aucune contribution collaborative ne peut imposer de contraintes supplémentaires d'utilisation, de droit d'auteur ou de propriété intellectuelle en sus de celles régissant déjà la base logicielle existante.

Outre la contribution directe, les licences FOSS offrent la possibilité de créer un projet dérivé (*fork*) plutôt que de travailler sur le projet original (en amont). Cette faculté de bifurquer sans autorisation stimule la rapidité d'innovation, certains dérivés devenant parfois plus prisés que leur projet parent. Elle peut néanmoins être source de confusion et disperser les capacités de révision nécessaires à la détection d'erreurs ou d'ajouts malveillants.

Enfin, les logiciels peuvent être autonomes ou dépendre de bibliothèques tierces pour construire les fonctionnalités nécessaires. Ces bibliothèques, essentiellement des composants de code externes, peuvent changer d'une manière moins visible pour les développeurs du code, ce qui risque d'entraîner des comportements imprévus. La facilité d'intégration des FOSS comme composant dans d'autres logiciels (y compris propriétaires) tend à accroître la fréquence de ce type de risque, bien qu'il ne soit pas exclusif aux FOSS.

3.2.2 L'absence de liens contractuels dans le modèle FOSS

Le modèle d'approvisionnement FOSS se distingue par l'absence, généralement, de relation contractuelle entre les parties, contrairement à la chaîne logistique des biens matériels, où les contrats entre fabricants et distributeurs permettent d'imposer des politiques ou des obligations de conformité. Dans l'univers FOSS, les opérateurs acquièrent les logiciels par divers canaux. Bien que le code source soit souvent téléchargeable auprès du mainteneur, la distribution passe majoritairement par des intermédiaires proposant des paquets installables (ex. : projet Debian) ou des produits et services. L'opérateur n'est que rarement lié par contrat à ces intermédiaires, au-delà des conditions de la licence libre. De même, les contrats avec les mainteneurs sont l'exception et concernent généralement le support technique, non le logiciel lui-même.

3.2.3 Le découplage entre financement et utilisation

Contrairement aux biens matériels, un logiciel est une information pure qui ne présente pas de coût matériel inhérent par unité supplémentaire produite. Les droits d'utilisation et de partage conférés par les licences FOSS n'exigent aucune contrepartie financière. Les utilisateurs, y compris les opérateurs d'infrastructure Internet, peuvent financer le développement et la maintenance des FOSS s'ils le souhaitent, mais n'y sont nullement tenus par la licence ; le financement des développeurs est indépendant de l'utilisation de leur logiciel.

3.2.4 Les FOSS n'ont souvent pas d'entité juridique unique responsable

Dans le monde des biens physiques, on suppose généralement qu'il existe une entité juridique responsable pouvant faire l'objet d'une politique ou porter une obligation de conformité. À l'inverse, la distribution mondiale de logiciels via l'Internet à un coût négligeable, voire nul, permet à des individus ou groupes informels de développer ou de diffuser gratuitement des logiciels sans constituer de personne morale. Le projet Debian[20], dont les logiciels sont utilisés dans le nucléaire, le ferroviaire, l'automatisation industrielle ou la santé, est un exemple très médiatisé de projet code source ouvert sans entité juridique associée. Si certains projets FOSS sont adossés à une structure juridique leur assurant une gouvernance, un parrainage ou même un emploi, la plupart en sont dépourvus. Nous verrons plus loin que le DNS est atypique à cet égard, avec quatre petites organisations assurant professionnellement la maintenance de logiciels FOSS.

3.3 Les systèmes propriétaires dépendent des FOSS

Les caractéristiques des FOSS s'avèrent également pertinentes pour les systèmes dits propriétaires (non FOSS). En effet, les systèmes propriétaires modernes reposent souvent sur des FOSS pour fonctionner. Les outils et bibliothèques FOSS sont omniprésents dans le développement et le déploiement de logiciels propriétaires. À titre d'exemple, rares sont les logiciels produits sans compilateurs ou environnements d'exécution ; de même, un logiciel ne peut stocker d'objets ou de données structurées sans magasins d'objets ou bases de données, ni

[20] Debian. « *Notre philosophie : pourquoi nous le faisons et comment nous le faisons* », https://www.debian.org/intro/philosophy.

communiquer avec d'autres composants sans système de transmission de messages. Or, ces fonctions back-end sont, pour l'essentiel, assurées par des FOSS.

Dans le cas spécifique du DNS, Cloudflare offre un exemple probant. Cloudflare exploite un service de résolveur DNS public largement utilisé, le « 1.1.1.1 ». Initialement, ce service était assuré à l'aide de Knot Resolver, un FOSS ; il a depuis été remplacé par un logiciel propriétaire développé en interne[21]. Toutefois, ce logiciel propriétaire, cœur du service 1.1.1.1, est écrit en Rust, langage de programmation dont les spécifications, l'implémentation de référence et le compilateur sont fournis sous licence FOSS par une fondation à but non lucratif[22]. Il s'appuie sur « tokio »[23], un environnement d'exécution asynchrone qui est également un logiciel FOSS, et tourne sous Linux, système d'exploitation FOSS. Le tout est entouré d'une vaste gamme de composants FOSS qui garantissent l'observabilité et autres nécessités opérationnelles[24]. En somme, si le logiciel propriétaire de Cloudflare utilisé par 1.1.1.1 fonctionne à grande échelle, c'est grâce aux FOSS, et non en dépit de leur utilisation.

3.4 Les atouts intrinsèques des FOSS dans l'écosystème du DNS

Loin d'être une construction théorique, le modèle FOSS offre, du fait de ses principes, des avantages tangibles qui l'ont imposé comme le paradigme dominant pour les logiciels d'infrastructure du DNS. La liberté d'étudier, de partager et de perfectionner collectivement les logiciels instaure un environnement propice à la transparence, à la résilience et à l'innovation. Il ne s'agit pas là de retombées fortuites, mais bien de forces inhérentes au modèle FOSS, particulièrement en phase avec les exigences qu'imposent la mise en place et la maintenance d'une infrastructure Internet critique. Les sections qui suivent détaillent ces points forts spécifiques.

3.4.1 Transparence et sécurité collaborative

Au sein du DNS, les implémentations à code source ouvert bénéficient de la transparence. En effet, la disponibilité de codes sources pour les implémentations FOSS permet à une communauté mondiale de développeurs, chercheurs et opérateurs de déceler et de corriger les vulnérabilités, souvent avec une célérité supérieure à celle observée dans les systèmes propriétaires. Ces logiciels font l'objet d'études actives de la part des milieux universitaires et de

[21] Wen, Anbang, et Marek Vavruša. « *How Rust and Wasm Power Cloudflare's 1.1.1.1* ». Le blog de Cloudflare, 28 février 2023. https://blog.cloudflare.com/big-pineapple-intro/.
[22] La Rust Foundation. « *About Us - Mission, Leadership, Board* »[À propos de la Fondation Rust - Mission - Direction - Conseil d'administration], https://rustfoundation.org/about/.
[23] Tokio. « Tutorial », https://tokio.rs/tokio/tutorial.
[24] Graham-Cumming, John. *« CloudFlare And Open Source Software: A Two-Way Street »* [Cloudflare et les logiciels à code source ouvert : un échange dans les deux sens]. Blog de Cloudflare, 7 octobre 2013. https://blog.cloudflare.com/open source-two-way-street/.

la sécurité [25], ce qui mène au signalement de failles tant dans le protocole DNS que dans ses implémentations à code source ouvert[26].

Lorsqu'une vulnérabilité est décelée, l'étroite collaboration entre ces trois groupes permet de remédier rapidement à toute vulnérabilité grave et de coordonner la divulgation des vulnérabilités ainsi que la diffusion des correctifs. Les serveurs DNS critiques (notamment les serveurs racine) sont ainsi pleinement sécurisés avant même que l'information ne devienne publique, et tous les autres serveurs sont mis à jour sans délai.

Dans le cadre d'une enquête menée auprès des opérateurs d'infrastructures DNS (voir Annexe C), ceux-ci ont jugé très utile la transparence de leur chaîne d'approvisionnement. Ils voient dans cette transparence un levier puissant pour accélérer l'application de correctifs aux vulnérabilités affectant les dépendances logicielles des services DNS qu'ils exploitent. Voici quelques réponses illustrant ce point[27] :

> Le code source ouvert expose RAPIDEMENT toute faille — de sécurité ou autre — et les correctifs sont déployés et diffusés bien plus vite que par n'importe quelle entité commerciale.
>
> De grandes entités commerciales comme [expurgé], [expurgé] et [expurgé] ont souvent, au fil des ans, publié des correctifs de sécurité bien APRÈS la découverte de la vulnérabilité.
>
> Nous soutenons toujours que l'utilisation des FOSS est dans l'intérêt de tous — utilisateurs et consommateurs de nos services. Cela leur permet de vérifier que nous utilisons des composants logiciels sains. Dans les rares cas où une faille de sécurité est détectée, elle est discutée ouvertement et corrigée à vitesse maximale, contrairement à ce que l'on observe avec les logiciels propriétaires.
>
> Les exemples de logiciels propriétaires présentant des failles de sécurité et affichant un bilan médiocre en matière de transparence et de fourniture de correctifs ne manquent pas. Sur ces deux plans, la communauté FOSS a fait mieux que la plupart des fournisseurs.

L'utilisation et la gestion des logiciels FOSS du DNS font l'objet de discussions actives et ouvertes entre les opérateurs. Chacun des principaux systèmes logiciels du DNS dispose d'une

[25] Voir par exemple l'article de Paul Vixie, « *DNS and BIND Security Issues* » [Problèmes de sécurité du DNS et sur BIND], Actes du 5e symposium USENIX sur la sécurité UNIX, Salt Lake City, UT, 1995 https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/vixie.pdf.

[26] Pour illustrer la notion d'« objet d'études actives », voir, par exemple, le résumé des conclusions de 23 articles de recherche publiés en 2024 sur la sécurité du DNS, présenté par Chaoyi Lu, « *Summarizing DNS & Security Academic Papers Published in 2024* » [Résumé des articles universitaires sur le DNS et la sécurité publiés en 2024] (présentation, ICANN82, Seattle, WA, 12 mars 2025), https://static.sched.com/hosted_files/icann82/7b/1.1%20chaoyi-dnspapers2024-0304.pdf.

[27] Comité consultatif sur la sécurité et la stabilité (SSAC) de l'ICANN, « *ICANN SSAC Survey on the Anticipated Impacts of Open Source Regulation on the DNS Infrastructure* » [Enquête sur les impacts anticipés de la réglementation des logiciels à code source ouvert sur l'infrastructure du DNS], communication personnelle, février 2025.

liste de diffusion publique d'utilisateurs[28], ainsi que d'une base de données sur les bogues et les incidents, librement consultable [29]. La communauté du DNS collabore sur les opérations et la recherche par l'intermédiaire de l'organisation sectorielle Centre d'analyse et de recherche pour les opérations DNS (DNS-OARC)[30]. Cette culture de communication ouverte contribue à une connaissance plus rapide et plus large des problèmes opérationnels, des bogues logiciels, des incompatibilités entre implémentations, ainsi que des erreurs commises par les opérateurs et susceptibles d'affecter d'autres parties du système.

3.4.2 Stabilité et support à long terme

En général, la maintenance des FOSS repose largement sur le bénévolat ; elle est souvent assurée par une seule personne. Dans le cas du DNS, quatre solutions à code source ouvert phares sont portées par quatre organisations distinctes (trois à but non lucratif, une commerciale), basées dans plusieurs pays et territoires d'Amérique du Nord et d'Europe[31]. Nées aux débuts de l'Internet grand public, ces quatre structures ont acquis une stabilité organisationnelle et financière éprouvée. Chacune pilote le développement de son logiciel en écrivant du nouveau code et en validant les contributions issues de communautés actives réparties dans le monde entier. L'engagement à long terme de ces organisations parraines et le contrôle technique centralisé des modifications logicielles concourent à atténuer les préoccupations habituelles liées à la qualité ou la sécurité des projets FOSS moins bien encadrés techniquement. De plus, la culture de la communauté technique code source ouvert du DNS est telle qu'il faudrait un effort soutenu de longue haleine pour qu'un « infiltré » puisse tisser les liens et se forger la réputation nécessaires à l'obtention d'un rôle de confiance.

3.4.3 La résilience opérationnelle grâce à la diversité

La haute disponibilité qu'exigent les services DNS impose la mise en place de redondances et la suppression de tout point unique de défaillance. Pour de nombreux opérateurs, cela passe par l'exploitation parallèle de plusieurs implémentations DNS indépendantes dans les logiciels. Les opérateurs qui externalisent peuvent de même adopter une stratégie multifournisseurs. Cela crée une demande intrinsèque en faveur d'une pluralité de solutions, afin que les opérateurs de services hautement fiables puissent en exploiter au moins deux en parallèle et éviter ainsi de

[28] Voir par exemple les listes de diffusion publiques de CZnic (https://lists.nic.cz/postorius/lists/knot-resolver-users.lists.nic.cz/), NLnet Labs (https://www.nlnetlabs.nl/support/mailing-lists/) et PowerDNS (https://mailman.powerdns.com/mailman/listinfo/).

[29] Voir par exemple le suivi des failles pour CoreDNS (https://github.com/coredns/coredns/issues) et BIND 9 (https://gitlab.isc.org/isc-projects/bind9/-/issues/).

[30] Centre d'analyse et de recherche pour les opérations DNS. « Introduction au DNS-OARC », 3 juillet 2008. https://www.dns-oarc.net/oarc/info.

[31] Par ordre alphabétique : CZNIC, une association tchèque de fournisseurs de services Internet (« FSI ») fondée en 1998 ; Internet Systems Consortium, Inc. (« ISC »), une société à but non lucratif établie aux États-Unis en 1994 et expressément créée pour soutenir les logiciels et systèmes à code source ouvert de l'infrastructure de l'Internet ; NLnet Labs, une organisation néerlandaise à but non lucratif fondée en 1999 pour développer des normes ouvertes et des logiciels à code source ouvert pour le DNS et le routage interdomaine ; et PowerDNS, une société néerlandaise fondée en 1999 pour soutenir le développement de logiciels DNS spécialisés destinés aux FSI.

dépendre d'un seul développeur de logiciels ou d'être vulnérables aux failles d'un produit unique. La disponibilité de logiciels DNS FOSS abaisse le seuil d'entrée pour les organisations souhaitant gérer leur propre infrastructure et offre un moyen d'échapper à la concentration et à la centralisation du marché[32].

3.4.4 Vecteur de croissance économique et d'innovation

Il est avéré que les FOSS constituent un puissant levier de croissance[33,34]. Comme indiqué précédemment, une multitude de produits à code source ouvert sont disponibles gratuitement, en libre accès, à l'échelle mondiale pour quiconque a besoin de logiciels DNS. Au rang des utilisateurs potentiels figurent les FSI, les opérateurs de registre de noms de domaine et les bureaux d'enregistrement de noms de domaine, ainsi que les internautes eux-mêmes. Particuliers, organismes à but non lucratif, jeunes pousses et experts en la matière, qui peineraient à assumer le coût de licences de logiciels propriétaires, peuvent ainsi se doter gratuitement des outils dont ils ont besoin. Un répondant à l'enquête auprès des opérateurs du DNS (voir Annexe C) résume ainsi la situation : « Ma préoccupation majeure tient au volume de composants à code source ouvert que nous utilisons dans les segments non critiques de notre pile technologique, sans contrat de maintenance ; au total, le coût des licences serait pour nous prohibitif, à supposer même qu'elles soient disponibles ».[35]

L'existence de multiples solutions FOSS pour le DNS favorise le développement technique et commercial des usages d'Internet, ainsi que des logiciels et services en ligne, qu'ils soient libres ou propriétaires. De nombreux systèmes propriétaires et services hébergés sont tributaires de composants à code source ouvert pour assurer leurs fonctions critiques ; c'est notamment le cas de maintes plateformes en nuage et services en ligne qui intègrent des composants FOSS pour le DNS[36]. Parallèlement, l'infrastructure DNS repose largement sur des bibliothèques

---

[32] Nottingham, Mark. « *RFC 9518 : Centralization, Decentralization, and Internet Standards* » [Centralisation. décentralisation et normes sur Internet] Appel à commentaires. Groupe de travail de génie Internet, 18 décembre 2023. https://datatracker.ietf.org/doc/rfc9518/.

[33] « L'analyse estime un rapport coût-bénéfice supérieur à 1:4 et prédit qu'une augmentation de 10 % des contributions aux logiciels à code source ouvert (OSS) générerait annuellement 0,4 % à 0,6 % de PIB supplémentaire ainsi que plus de 600 start-ups TIC supplémentaires dans l'UE. Des études de cas révèlent qu'en achetant des OSS plutôt que des logiciels propriétaires, le secteur public pourrait réduire le coût total de possession, éviter l'enfermement propriétaire et ainsi accroître son autonomie numérique. » Extrait de la Commission européenne. Direction générale des réseaux de communication, du contenu et des technologies. *The Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy: Final Study Report.* [L'impact des logiciels à code source ouvert et des matériels libres sur l'indépendance technologique, la concurrence et l'innovation dans l'économie de l'UE : Rapport d'étude final] LU: Office des publications, 2021. https://data.europa.eu/doi/10.2759/430161.

[34] Wright, Nataliya Langburd, Frank Nagle, et Shane Greenstein. *« Open Source Software and Global Entrepreneurship »* [Logiciels à code source ouvert et entrepreneuriat mondial]. Politique de recherche *52, no. 9* (2023) : 104846. https://doi.org/10.1016/j.respol.2023.104846.

[35] Comité consultatif sur la sécurité et la stabilité (SSAC) de l'ICANN, « *ICANN SSAC Survey on the Anticipated Impacts of Open Source Regulation on the DNS Infrastructure* » [Enquête sur les impacts anticipés de la réglementation des logiciels à code source ouvert sur l'infrastructure du DNS].

[36] À ce jour, aucune citation indépendante unique ne vient corroborer cette affirmation. Toutefois, l'enquête menée collectivement par les auteurs du présent document permet de l'avancer avec certitude. Des contraintes de

cryptographiques FOSS telles qu'OpenSSL. De même, Linux, système d'exploitation à code source ouvert, constitue le socle d'une part significative de l'infrastructure en nuage, des environnements serveurs et des appareils de l'Internet des objets (IoT). Ce rôle fondamental souligne l'influence déterminante des FOSS sur l'innovation technologique. Les logiciels propriétaires intègrent souvent ces cadres FOSS tout en greffant des applications ou des fonctionnalités à code source fermé, ce qui instaure une relation symbiotique entre les deux modèles[37].

3.4.5 Contribution à l'autonomie numérique

L'usage des FOSS ne requérant généralement pas le versement de redevances ni de rémunération, les capitaux nécessaires au lancement de nouvelles entreprises numériques sont souvent moindres qu'avec des logiciels propriétaires. En outre, la liberté d'étude, de modification et de redistribution du code inhérente aux FOSS stimule l'acquisition de connaissances et de savoir-faire locaux, ce qui ouvre la voie à de nouveaux projets de recherche et à de nouvelles activités commerciales. Les adaptations locales ou les développements ultérieurs ne sont soumis à aucune autorisation ni à aucun accord préalable des auteurs originaux. Enfin, aucun service basé sur des FOSS ne saurait être entravé par des détenteurs étrangers de droits d'auteur, les licences étant irrévocables ; la disponibilité du code reste ainsi garantie, y compris en cas de conflit commercial ou d'embargo.

3.5 Les risques inhérents au modèle FOSS

Bien que le modèle FOSS présente des avantages considérables, ses caractéristiques uniques comportent également un ensemble distinct de risques qui diffèrent de ceux associés aux logiciels propriétaires traditionnels. Il ne s'agit pas de défauts du modèle lui-même, mais plutôt de compromis inévitables qui doivent être compris et gérés, en particulier lorsque le logiciel est utilisé dans des infrastructures critiques. Le modèle économique, la nature distribuée du développement et l'absence de relations contractuelles classiques ont des implications pour la viabilité et la sécurité opérationnelle à long terme. Ces risques inhérents sont décrits en détail ci-après.

3.5.1 Viabilité financière et le surmenage du mainteneur

Le problème général de la viabilité financière des FOSS est l'une des principales menaces qui pèsent sur le DNS. En dissociant le financement de l'utilisation (section 3.2.3), ce modèle favorise certes une adoption massive, mais encourage également le phénomène du

confidentialité empêchant de révéler publiquement quelle plateforme utilise quel service, nous précisons que cet énoncé est fondé bien que non documenté formellement.

[37] Gortmaker, Jeff. *« Open source software policy in industry equilibrium »* [Politique sur les logiciels à code source ouvert dans l'équilibre du secteur] . *Working paper, Tech. Rep*, 2024. https://jeffgortmaker.com/files/Open_Source_Software_Policy_in_Industry_Equilibrium.pdf.

« profiteur »[38], créant une situation où le monde entier dépend de logiciels financés par une poignée d'acteurs[39,40].

Le Broadband Internet Technology Advisory Group [Groupe de travail technique sur l'Internet bande large] (BITAG) dresse le constat suivant :

> Il existe un décalage entre l'achat d'équipements de réseaux assortis de coûteux contrats de maintenance et l'absence de financement des logiciels libres dont ces équipements sont, bien souvent, tributaires. Fréquemment, les équipes techniques des opérateurs de réseaux souhaiteraient soutenir le développement, mais se heurtent à la structure de leur entreprise : ces logiciels ne sont pas des produits que l'on achète dans une boîte sous emballage plastique, accompagnés d'un contrat de support. Parrainer le développement d'une fonctionnalité peut s'avérer problématique, car les services juridiques partent du principe que tout développement logiciel confère au commanditaire la propriété intellectuelle [exclusive], une notion incompatible avec le modèle du logiciel libre et à code source ouvert[41].

Bien que les quatre principales implémentations DNS à code source ouvert soient maintenues par des organisations qui ont atteint une stabilité financière et structurelle durable, ces structures restent de taille modeste. La moindre menace pesant sur leur financement ou toute imposition de contraintes réglementaires dont elles ne pourraient absorber le coût pourrait suffire à les déstabiliser. Qu'un de ces systèmes à code source ouvert majeurs vienne à souffrir d'un défaut de maintenance ou devienne inopérant, et les répercussions sur le DNS pourraient être considérables.

Cela est particulièrement vrai pour les outils fondamentaux qui exigent une maintenance constante mais sont déconnectés du cœur de métier de leurs utilisateurs. Les quatre implémentations DNS à code source ouvert les plus prisées reposent sur des équipes de développement ne dépassant guère une douzaine d'ingénieurs ; dès lors, l'ajout d'exigences réglementaires mobilisant, par exemple, un équivalent temps plein (ETP) représenterait une charge conséquente.

---

[38] Johnson, Justin Pappas. *« Essays in Microeconomic Theory »* [Essai sur la théorie microéconomique]. Thèse, Massachusetts Institute of Technology, 1999. http://hdl.handle.net/1721.1/9518.

[39] Kristoff, John, Alexander Band, Ondrej Filip et Jeff Osborn. *Panel : Core Systems OSS Panel [Panel sur les OSS dans les systèmes centraux]* . NANOG 84, 2022. https://www.youtube.com/watch?v=vWiW-3jMw7w.

[40] Par exemple, un rapport souligne le déséquilibre entre l'utilisation d'un logiciel essentiel de routage et les contributions financières à son développement : « Nous illustrons, au moyen de deux exemples, … la pertinence de ce déséquilibre entre le financement et l'utilisation. Sur un nombre total estimé de 2 000 installations du logiciel Routinator RP et de 1 400 réseaux utilisant le logiciel CA délégué Krill, moins de dix en financent le développement. La majorité des opérateurs dépendent de la stabilité, de la pérennité et du développement futur du logiciel, sans toutefois contribuer en rien à cette fin ». Groupe de travail technique du Broadband Internet Technical Advisory Group (BITAG), « *Security of the Internet's Routing Infrastructure* » [Sécurité du système de routage Internet], 2 novembre 2022, 26, https://www.bitag.org/documents/BITAG_Routing_Security.pdf.

[41] Groupe de travail technique du BITAG, « *Security of the Internet's Routing Infrastructure* » [Sécurité du système de routage Internet], 26.

Le financement de mainteneurs rémunérés emprunte des voies parfois inattendues. Outre l'acceptation de dons et l'offre d'assistance technique personnelle, certains projets offrent à leurs mécènes un accès anticipé aux correctifs, une maintenance des versions en fin de vie, le développement prioritaire de fonctionnalités, ou encore l'accès à des paquets précompilés et à des services de sécurité additionnels[42,43,44,45]. Les régulateurs doivent veiller à ne pas interdire par inadvertance l'un de ces leviers de financement essentiels aux opérations des mainteneurs de FOSS.

Les FOSS appliqués au DNS font figure d'exception par l'existence même d'organisations pérennes employant des mainteneurs. Pour ces structures, l'enjeu est la viabilité *financière*. En règle générale, cependant, le risque est avant tout lié à l'essoufflement. L'écrasante majorité des FOSS est maintenue par des individus isolés, pendant leur temps libre[46]. C'est le cas de Dnsmasq, logiciel DNS le plus souvent embarqué dans les petits routeurs bon marché utilisés par les particuliers et les petites entreprises. Il est principalement maintenu par un unique bénévole, pour l'essentiel non rémunéré[47]. De même, plusieurs bibliothèques logicielles éprouvées, essentielles à la programmation du DNS, sont maintenues par des individus seuls, pendant leur temps libre[48]. CoreDNS, autre implémentation DNS prisée, ainsi que la bibliothèque DNS sous-jacente en langage Go s'appuient respectivement sur des efforts communautaires et sur un unique mainteneur bénévole (expert). Ces exemples soulignent une caractéristique intrinsèque de l'écosystème du logiciel : une petite organisation ou un développeur isolé peut jouer un rôle critique dans l'écriture d'un logiciel pour une infrastructure numérique mondiale, tout en étant totalement dissocié des dépenses d'investissement ou d'exploitation liées au fonctionnement de ce logiciel. Pour ces mainteneurs bénévoles isolés, tant que cette activité n'est pas financée comme emploi principal, à temps plein, le risque n'est pas la viabilité financière, mais l'épuisement. Les régulateurs devraient prendre garde à ne pas imposer de fardeaux supplémentaires excédant la capacité et la volonté de ces mainteneurs à investir leur temps libre

[42] L'Internet Systems Consortium propose, par exemple, un service de signalement anticipé des vulnérabilités. Voir Internet Systems Consortium, « *Early Vulnerability Notification* (EVN) » [Notification précoce des vulnérabilités], https://www.isc.org/evn/.

[43] NLnet Labs assure, par le truchement de sa filiale Open NetLabs, des prestations de formation, de conseil, d'assistance technique et de développement de logiciels. Voir NLnet Labs, « *Open Netlabs Services - Consultancy* » [Services Open Netlabs - Conseil], https://nlnetlabs.nl/services/consultancy/.

[44] PowerDNS offre un large éventail de produits et services dont PowerDNS Protect, une solution de sécurité intégrant des listes de blocage de protection. Voir « *PowerDNS Protect* », https://www.powerdns.com/powerdns-protect.

[45] Pour une vue d'ensemble des différents modèles organisationnels de l'univers code source ouvert, voir « *Open Source Archetypes: A Framework For Purposeful Open Source* » [Archétypes du code source ouvert : cadre pour un code source ouvert utile], Open Tech Strategies, Mozilla Corporation, 28 octobre 2019, https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf.

[46] Bressers, Josh. *« Open Source Is One Person »* [Le code source ouvert, c'est une seule personne]. Open Source Security, 28 août 2025. https://opensourcesecurity.io/2025/08-oss-one-person/.

[47] « *Dnsmasq - Network Services for Small Networks* » [Dnsmasq - Services réseaux pour petits réseaux], https://thekelleys.org.uk/dnsmasq/doc.html.

[48] Citons à titre d'exemple *Net::DNS* pour le langage de programmation Perl ou encore *miekg/dns*, une bibliothèque DNS en langage Go utilisée par Kubernetes, Docker et l'autorité de certification Let's Encrypt. D'autres exemples de bibliothèques sont présentés dans le tableau 7.

dans ce qui demeure, essentiellement, des projets personnels. Ce sujet fait l'objet d'études actives et les décideurs gagneraient à prendre en compte les recommandations formulées par les travaux de recherche[49].

3.5.2 Risques pour la chaîne d'approvisionnement liés aux dépendances partagées

Une grande partie des logiciels critiques, qu'ils soient commerciaux ou FOSS, reposent sur les mêmes composants FOSS. La présence d'un bogue grave dans une bibliothèque cryptographique FOSS très répandue[50] pourrait ainsi compromettre la totalité des implémentations DNS[51]. Cela concerne aussi d'autres composants plus discrets, couramment réutilisés. Il s'agit là d'une vulnérabilité potentielle majeure qui ne se limite ni au DNS ni aux FOSS, mais touche l'écosystème du logiciel dans son ensemble[52]. Les risques pour la viabilité décrits à la section 3.5.1 s'appliquent également à ces composants partagés, ce qui ne fait qu'aggraver la menace.

Ce risque est aggravé par le fait que des contributeurs aux FOSS mal intentionnés peuvent insérer, à l'insu de tous, du code malveillant dans des projets à code source ouvert ou dans leurs composants, que ce soit en manipulant les référentiels de paquets ou via des contributions directes aux projets. Une vigilance accrue dans la vérification et la surveillance des dépendances s'impose donc pour prévenir toute intégration de code malveillant dans les projets logiciels.

3.5.3 Les logiciels FOSS gratuits sont fournis sans aucune garantie ni aucun engagement d'assistance

La gratuité des logiciels libres constitue un atout indéniable — l'acquisition se résumant souvent à un simple téléchargement. Toutefois, l'absence de garantie et de promesse d'assistance technique comporte des risques. Par défaut, aucun contrat ne lie le fournisseur du produit FOSS à l'utilisateur, hormis l'accord de licence libre[53]. À moins que l'utilisateur ne prenne ses propres

[49] Eghbal, Nadia. « Sur quoi reposent nos infrastructures numériques ? Le travail invisible des faiseurs du web ». Fondation Ford, 14 juillet 2016. https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/.

[50] OpenSSL constitue l'archétype de la bibliothèque cryptographique incontournable. L'ampleur de la dépendance à son égard est bien illustrée par l'épisode de la faille « *Heartbleed* » dans OpenSSL. À ce moment-là, on estimait que 17 % des serveurs Web de l'Internet, certifiés par des autorités de certification reconnues, étaient vulnérables à des attaques. Netcraft, « *Half a Million Widely Trusted Websites Vulnerable to Heartbleed Bug* » [Un demi-million de sites largement utilisés vulnérables au bogue Hartbleed], Netcraft News, 8 avril 2014, https://web.archive.org/web/20141119102520/http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html.

[51] À l'instar des logiciels du DNS, la conception de logiciels cryptographiques relève d'une expertise pointue. Si certains outils cryptographiques FOSS sont établis de longue date, leur diversité et leur qualité restent un sujet de préoccupation.

[52] Pour un exemple de tentative de cartographie des dépendances communes, voir « *Census III of Free and Open Source Software* », [Rapport Census III sur les logiciels libres et à code source ouvert] de la Linux Foundation, décembre 2024 : https://www.linuxfoundation.org/research/census-iii

[53] On croit souvent à tort qu'il existe des relations contractuelles entre mainteneurs et opérateurs ; cette idée reçue est abordée à la section 3.2.2.

dispositions de maintenance avec le mainteneur du logiciel ou des tiers, il ne dispose d'aucune garantie de maintenance active ou d'assistance technique.

En cas de faille de sécurité, qu'elle soit accidentelle (comme le bogue Heartbleed d'OpenSSL[54] ou malveillante (comme la porte dérobée de xz Utils[55]), nul n'est tenu d'y apporter un correctif. Certes, il est techniquement possible pour quiconque, y compris l'utilisateur, de copier le code source pour corriger le problème manuellement ; toutefois, la création d'une telle version dérivée requiert une expertise pointue en génie logiciel et des ressources opérationnelles conséquentes. De fait, l'utilisateur se trouve souvent sans prise réelle sur la disponibilité des correctifs. Ce problème est particulièrement grave lorsqu'il touche des paquets omniprésents, comme OpenSSL et xz, pour lesquels il n'existe aucun substitut immédiat. Les risques associés à la monoculture ne sont pas propres au code source ouvert, mais cela peut être une des raisons pour lesquelles ces risques généraux s'appliquent aux FOSS.

Une baisse de l'intérêt communautaire pour la maintenance d'un logiciel FOSS peut favoriser l'entrée en lice d'organisations proposant une maintenance sous contrat. Cependant, les modifications apportées par ces entités sont généralement reversées au projet FOSS d'origine pour minimiser la charge de gérer la maintenance d'une base de code distincte. Ce mécanisme permet à d'autres acteurs de profiter de cette maintenance sans en assumer le coût, ce qui conduit au problème du « profiteur » : lorsqu'un fournisseur de services exploite un logiciel FOSS sans contribuer à la maintenance, il peut le faire à moindre coût qu'un concurrent contributeur, ce qui lui permet de pratiquer des prix inférieurs[56].

Il est possible de pallier cette absence de garantie intrinsèque. Les opérateurs peuvent former et retenir une expertise interne, financer ou embaucher des mainteneurs[57], ou conclure des contrats d'assistance technique pour accéder à l'expertise de mainteneurs ou de contributeurs experts[58]. Le rapport du BITAG cité à la section 3.5.1 illustre les obstacles organisationnels qui empêchent les opérateurs de prendre ces mesures.

---

[54] « *Heartbleed Bug* », https://heartbleed.com/.

[55] Goodin, Dan. « *What We Know about the xz Utils Backdoor That Almost Infected the World* » [Ce que nous savons sur la porte dérobée xz Utils qui a failli infecter le monde entier]. Ars Technica, 1er avril 2024. https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/.

[56] Une association professionnelle allemande regroupant des développeurs de logiciels FOSS a ainsi signalé l'existence de ce problème dans le cadre des marchés publics de logiciels FOSS. Voir le Groupe de travail des services d'acquisition de l'Open Source Business Alliance, « *Selection Criteria for the sustainable Procurement of Open Source Software* » [Critères de sélection pour un approvisionnement durable en logiciels à code source ouvert], Open Source Business Alliance, 11 février 2025, https://osb-alliance.de/publikationen/veroeffentlichungen/selection-criteria-for-the-sustainable-procurement-of-open source-software.

[57] Valsorda, Filippo. « *I'm Now a Full-Time Professional Open Source Maintainer* » [Je suis désormais mainteneur de logiciels à code source ouvert professionnel à plein temps] , 2 février 2023. https://words.filippo.io/full-time-maintainer/.

[58] Des contrats d'assistance technique sont disponibles pour plusieurs des systèmes FOSS décrits dans le présent rapport.

3.5.4 Risques opérationnels liés au déploiement

La nature distribuée des FOSS engendre des défis opérationnels concernant l'authenticité des logiciels, l'application des correctifs et la pénurie de main-d'œuvre qualifiée.

Vérification de l'authenticité des logiciels

Les FOSS étant distribués librement sur Internet, ils sont exposés aux risques de détournement, ou encore de substitution par du code contrefait. Pour parer à cette menace, les mainteneurs signent systématiquement leurs logiciels FOSS à l'aide de méthodes cryptographiques robustes, signatures que l'utilisateur peut vérifier pour s'assurer de l'intégrité du code. Dans l'infrastructure Internet, toutes les implémentations DNS prisées de type FOSS sont signées. Cependant, les utilisateurs ne vérifient pas toujours ces signatures ou acquièrent le logiciel via des intermédiaires qui ne vérifient pas ou ne maintiennent pas l'intégrité du logiciel.

Manque d'informations sur les déploiements et la rapidité des correctifs

La communauté des chercheurs s'investit activement dans la recherche de vulnérabilités dans les logiciels DNS FOSS ; elle parvient fréquemment à en trouver et à les signaler. De leur côté, tous les principaux fournisseurs de logiciels DNS se conforment aux meilleures pratiques en matière de traitement, de correction et de divulgation des vulnérabilités. Il manque toutefois une source d'information fiable permettant de déterminer si — et à quel rythme — les utilisateurs migrent vers les nouvelles versions corrigées.

Pour les FOSS en général, les données permettant d'évaluer ce risque restent limitées. Le fait que les consommateurs reçoivent souvent le logiciel via un tiers — un empaqueteur de système d'exploitation ou un passionné de logiciels FOSS qui a copié et redistribue le logiciel — complique d'autant plus le suivi des mises à jour. Ce risque pourrait être traité par une réglementation imposant aux opérateurs une sorte de rapport centralisé sur les logiciels critiques de leur infrastructure de production.

Externalisation et déficit de compétences

La complexité inhérente à l'exploitation correcte des FOSS pose problème car dans certaines régions du monde, il existe une pénurie d'opérateurs qualifiés. Ce double défi — criticité et complexité — pousse certains décideurs à l'externalisation vers des services en nuage, ce qui peut affaiblir la diversité et la nature distribuée du système, réduisant potentiellement sa résilience et sa sécurité. À titre d'exemple, si tous les acteurs d'une région choisissent par commodité le même service de messagerie hébergée plutôt que de construire, d'exploiter et de maintenir leurs propres serveurs, la disponibilité du courrier électronique dans cette région se trouve alors tributaire de la stabilité d'un seul fournisseur.

On observe par ailleurs un changement générationnel au sein des entreprises et des petits fournisseurs de services : le personnel en début de carrière, de plus en plus tributaire des services en nuage, maîtrise moins l'exploitation de ses propres services réseaux. Bien que des organisations comme l'APNIC, le NSRC ou PCH proposent des formations à l'intention des

opérateurs afin de renforcer les compétences en gestion du DNS et des réseaux, et que les projets FOSS s'efforcent de remédier à la situation en proposant des paquets précompilés et des fonctionnalités facilitant l'utilisation, il reste difficile de rivaliser avec les offres de type « logiciel en tant que service ».

4 Prépondérance des FOSS dans l'infrastructure du DNS et de l'enregistrement des noms de domaine

Les FOSS jouent un rôle crucial et prépondérant dans l'exploitation technique des systèmes de noms de domaine et d'enregistrement de l'Internet. Dans les maillons les plus critiques de cette infrastructure, les FOSS sont la norme et les logiciels propriétaires sont l'exception. Les recherches menées dans le cadre du présent rapport établissent que l'infrastructure mondiale et distribuée du DNS est tributaire des FOSS : au moins 9 des 12 opérateurs du système des serveurs racines (RSS) d'Internet utilisent exclusivement des implémentations DNS de type FOSS. De même, 9 des 10 plus importants fournisseurs de services pour les TLD utilisent des FOSS. Dans le secteur de l'enregistrement des noms de domaine, bien que de nombreux grands systèmes soient propriétaires, ils reposent néanmoins majoritairement sur des composants FOSS. Il en va de même pour les principaux fournisseurs de services d'entiercement de données auxquels recourent les opérateurs de registre et les bureaux d'enregistrement. Les sections ci-après détaillent la prépondérance des FOSS dans chacun des composants de cette infrastructure critique. La méthodologie employée est décrite à l'annexe B.

4.1 Les FOSS dans l'infrastructure d'enregistrement des noms de domaine

L'infrastructure d'enregistrement s'entend des systèmes qui facilitent l'enregistrement des noms de domaine et rendent les noms enregistrés accessibles dans le DNS public. Bien que l'on ne dispose pas de données précises sur l'ampleur exacte de l'utilisation des FOSS, les éléments dont on dispose attestent d'une forte dépendance à l'égard des FOSS, tant sous forme de systèmes complets que de composants fondamentaux.

Un certain nombre d'opérateurs de registre exploitent une infrastructure d'enregistrement entièrement FOSS (Tableau 1). Par exemple, il est établi que la plateforme de registre FRED est utilisée par au moins 12 registres de ccTLD, et que la plateforme Nomulus est utilisée par plusieurs registres de gTLD.

Tableau 1 : Systèmes FOSS utilisés pour les opérations de registre

Système logiciel	Licence code source ouvert	Utilisateurs
FRED	GPLv3	FRED est utilisé notamment par les ccTLD des territoires suivants : Albanie, Angola, Argentine, Bosnie-Herzégovine, Costa Rica, Lesotho, Macao, Malawi, Macédoine du Nord, Paraguay, République tchèque et Tanzanie.
Registre du domaine Internet ee	MIT	ccTLD de l'Estonie (.ee).
Namingo	MIT	Système conçu pour la prochaine série du programme des nouveaux gTLD.
Nomulus	Apache 2.0	Registres gTLD Google, notamment .app, etc.

Tableau 2 : Systèmes de registre bâtis sur des composants FOSS

Système de registre/Service back-end	Exemples de composants à code source ouvert utilisés	Registre utilisé par
Afnic	Serveur Web, base de données	20 TLD, dont le .fr
CIRA / SIDN / Registre Hello	Base de données, serveur Web, serveur d'application, production de rapports, frontal	6 ccTLD, 6 gTLD, dont .ca et .ie
CoCCA	Serveur Web, serveur d'application, base de données	56 ccTLD
CORE Association	Serveur Web, base de données, bibliothèques Java	1 ccTLD, 21 gTLD
Registre GoDaddy	Base de données, serveurs d'application, production de rapports, surveillance, journalisation, tests, frontal, DNS	Plus de 200 TLD
Identity Digital	Base de données	250 gTLD et ccTLD, dont .au, .me et .pr
Nominet	Base de données, serveur d'application, analyse syntaxique, journalisation, tests, frontal, serveur de noms	Plus de 85 TLD, dont le .uk
Services de registre TANGO	Serveur Web, base de données, bibliothèques Java	8 gTLD
Registre Tucows	Base de données, logiciel DNS et outils accessoires, serveurs Web et de messagerie, files d'attente de messages, orchestration et virtualisation d'infrastructure, système d'exploitation	222 « TLD », y compris des SLD gérés comme des TLD (ex. : .my et com.my)

Système de registre/Service back-end	Exemples de composants à code source ouvert utilisés	Registre utilisé par
Verisign[59]	(non communiqué)	.com, .net, .edu et autres TLD

[59] Aux fins du présent rapport, Verisign a fourni la déclaration suivante : « Verisign exploite sa plateforme propriétaire de résolution DNS *Advanced Transaction Lookup and Analysis System* (ATLAS) [Système avancé de recherche et d'analyse des transactions]. Verisign utilise également une infrastructure d'enregistrement et de résolution dédiée qui intègre, à des fins de redondance, un ensemble diversifié et rigoureusement sélectionné de composants logiciels commerciaux et à code source ouvert ».

À l'inverse, les opérateurs de registre et les registres back-end de grande envergure privilégient souvent des solutions propriétaires. Il convient toutefois de noter que ces systèmes ne sont généralement pas développés de zéro ; ils s'articulent le plus souvent autour d'extensions propriétaires personnalisées intégrant des composants — bases de données et serveurs Web, notamment — majoritairement issus du monde FOSS (Tableau 2).

Cette dépendance aux FOSS s'observe également dans les services d'entiercement de données, qui assurent le stockage sécurisé de copies des données d'enregistrement. Les trois plus grands fournisseurs de ces services, desservant opérateurs de registre et bureaux d'enregistrement, ont conçu leurs systèmes en s'appuyant, au moins en partie, sur des composants FOSS (Tableau 3).

Tableau 3 : Utilisation de logiciels FOSS par les agents d'entiercement de données

Agent d'entiercement de données	Pour les registres	Pour les bureaux d'enre-gistrement	Intégration des FOSS aux fonctions clés ?
Beilong Zedata (Beijing) Data Technology Co., Ltd	✓	✓	Non
Centre d'information de réseaux de Chine (CNNIC)	✓	✓	Non
China Organizational Name Administration Center (CONAC)	✓	✓	Non
DENIC Services GmbH & Co. KG	✓	✓	Oui, partiellement
Escrow4All	✓		Oui
Joint Stock Company Internet Exchange "MSK-IX"	✓	✓	Inconnu
NCC Group	✓		Oui, partiellement
Centre d'information de réseaux de Taïwan (TWNIC)	✓		Non

Dans le cadre du présent rapport, l'infrastructure des bureaux d'enregistrement n'a fait l'objet d'aucune évaluation métrologique ni enquête. Il y est toutefois probable que les bureaux d'enregistrement ont régulièrement recours à des extensions propriétaires sur mesure et des composantes essentiellement FOSS. Certains emploient, par exemple, les logiciels de serveur Web nginx ou Apache pour administrer les portails Web destinés aux titulaires de noms de domaine, et font appel à des solutions FOSS pour leurs besoins en matière de surveillance, d'analyse de données ou de gestion de code, entre autres.

4.2 Les FOSS dans l'infrastructure de publication du DNS (serveurs faisant autorité)

C'est au sein de l'infrastructure de publication des données de domaine que la prédominance des FOSS est la plus manifeste. Aux échelons supérieurs de la hiérarchie du DNS — la racine et les TLD — les FOSS sont quasi omniprésents.

Le système des serveurs racines (RSS) constitue le sommet de cette hiérarchie. Sur les 12 organisations indépendantes exploitant les serveurs racines, au moins 9 utilisent exclusivement des implémentations DNS de type FOSS pour répondre aux requêtes (Tableau 4).

Tableau 4 : Utilisation des FOSS dans le système des serveurs racines

Identificateurs de serveur racine	Logiciels	Code source ouvert[60]
A, J	ATLAS (propriétaire) NSD	Partiellement[61]
B	Knot BIND9	Oui[62,63]
C	BIND9	Oui
D	NSD	Oui
E	*Inconnu* (FOSS), *interne* (propriétaire)[64]	Partiellement[65]
F	BIND9, *interne* (propriétaire)[66]	Partiellement
G	BIND9	Oui
H	NSD	Oui
I	*Confidentiel*	Oui[67]

[60] Willem Toorop et al., « *RSSAC028 Implementation Study Report* » [Rapport d'étude de mise en œuvre du RSSAC028] (rapport, NLnet Labs et Stichting Internet Domeinregistratie Nederland (SIDN), 27 septembre 2023), 15, https://www.icann.org/en/system/files/files/rssac028-implementation-study-report-27sep23-en.pdf.

[61] Extrait de la déclaration de Verisign sur les attentes de service des serveurs racines (RSSAC001v2) : « Verisign utilise deux bases de code distinctes pour le service racine du DNS : 1) notre plateforme de résolution propriétaire et brevetée ATLAS, et 2) le logiciel à code source ouvert Name Server Daemon (NSD) de NLnet Labs. L'une ou l'autre de ces implémentations, voire les deux, peuvent être utilisées à tout moment », https://a.root-servers.org/aroot-rssac001v2-expectations.pdf.

[62] « *USC/ISI's DNS Root Server* » [Serveur racine DNS de l'USC/ISI], https://b.root-servers.org/.

[63] « RSSAC023v2 : Histoire du système des serveurs racine ». Comité consultatif du système des serveurs racine de l'ICANN (RSSAC), 17 juin 2020. https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf.

[64] Grant, Dani. « *Delivering Dot* » [Lancement du Dot]. Blog de Cloudflare, 10 septembre 2017 https://blog.cloudflare.com/f-root/.

[65] Bischof, Ralph. « *E-Root Instance in San Francisco Servfails?* » [Instance du serveur racine E dans les pannes de serveur à San Francisco ?], 19 juin 2025. https://lists.dns-oarc.net/pipermail/dns-operations/2025-June/022899.html.

[66] Grant, « Delivering Dot » [Lancement du Dot].

[67] Communiqué avec la permission de Netnod dans une correspondance avec le SSAC datée du 13 décembre 2024.

Identificateurs de serveur racine	Logiciels	Code source ouvert[60]
K	BIND9 Knot NSD	Oui
L	Knot NSD	Oui
M	BIND9	Oui[68]

L'examen conjoint des ccTLD et des gTLD révèle que 9 des 10 principaux opérateurs assurant un service faisant autorité pour les registres de TLD utilisent des FOSS à cette fin.[69]

Sous la racine et les TLD, les serveurs de noms faisant autorité sont exploités par une vaste gamme d'acteurs, notamment des particuliers, des entreprises, des universités et des gouvernements. Même en l'absence de données exhaustives sur cet ensemble hétéroclite, il est avéré que bon nombre des systèmes FOSS utilisés à la racine et pour les TLD sont également le choix privilégié de ces opérateurs. Bien souvent, les organisations proposant un DNS secondaire sont celles-là mêmes qui fournissent des services DNS faisant autorité pour les TLD. Les tableaux 5 et 6 recensent les systèmes FOSS et les produits commerciaux adaptés aux implémentations DNS faisant autorité.

Les serveurs de noms faisant autorité sont fréquemment intégrés à des systèmes d'approvisionnement afin de simplifier la mise à jour des informations de zone et de mettre en œuvre les autorisations et les contrôles adéquats sur la maintenance de ces enregistrements. Certains des systèmes d'approvisionnement les plus répandus sont des FOSS[70].

Une large part des contenus les plus prisés sur Internet est hébergée sur quelques grands réseaux de contenu, tel YouTube (Google), qui utilise un système DNS propriétaire. Bien qu'un certain nombre de grands opérateurs de services faisant autorité pour le deuxième niveau et les échelons inférieurs de la hiérarchie utilisent des FOSS (notamment ceux qui desservent aussi la racine ou les zones de TLD), le manque de déclarations publiques empêche toute enquête fiable ou toutes statistiques sur l'usage qu'ils en font[71]. Pour en savoir plus, consulter les tableaux ci-après. Il s'agit là d'une lacune notable dans les données accessibles, car quatre très grands fournisseurs

[68] « *M-Root DNS Server* » [Serveur DNS racine M], https://m.root-servers.org/.
[69] Principaux opérateurs par nombre de TLD desservis. Voir l'annexe B pour une description de la méthodologie utilisée.
[70] Parmi les systèmes prisés figurent VinylDNS (https://www.vinyldns.io/), géré par Comcast, et OctoDNS, géré par Amazon et Oracle. Autre système de configuration très répandu, DNS Control gère le DNS à la fois sur les systèmes auto-hébergés et les services en nuage, notamment Cloudflare, le service Route53 d'Amazon et Gandi, un bureau d'enregistrement DNS et fournisseur d'hébergement.
[71] Il est difficile de mesurer de manière fiable l'adoption des FOSS. Daniel Stenberg avance plusieurs raisons à cela dans « *What We Can't Measure* » [Ce que l'on ne peut pas mesurer], Daniel : //Stenberg : // (blog), 5 juin 2025, https://daniel.haxx.se/blog/2025/06/05/what-we-cant-measure/.

pourraient traiter à eux seuls plus de la moitié des requêtes visant des noms faisant autorité visibles sur Internet[72].

4.3 Les FOSS dans l'infrastructure d'extraction du DNS (résolveurs)

La prépondérance des FOSS ne se limite pas à la publication des données DNS ; elle s'étend également à l'infrastructure assurant l'extraction de ces informations : l'écosystème diversifié des résolveurs DNS. Les FOSS occupent une place importante dans l'ensemble de cet écosystème, depuis les réseaux locaux jusqu'aux plateformes en nuage mondiales.

La majorité des utilisateurs dépendent de résolveurs locaux exploités par leurs FSI, leurs entreprises ou leurs établissements d'enseignement. Les recherches estiment à moins de 20 % la part mondiale des utilisateurs desservis par des résolveurs en nuage, les 80 % restants ayant recours à divers types de résolveurs locaux.[73] Bon nombre des systèmes FOSS les plus courants assurent indifféremment des fonctions de serveur faisant autorité et de résolveur (Tableau 5).

Tableau 5 : Systèmes FOSS couramment utilisés pour les applications de serveur DNS

Système logiciel	Licence code source ouvert	Application — Exemples d'utilisateurs
BIND9	MPL 2.0	Faisant autorité, résolveurs — CIRA, NIC.BR, Visionary Broadband
CoreDNS	Apache 2.0	Kubernetes, faisant autorité — Meta
dnsdist	GPL 2.0	Équilibrage de charge DNS
Dnsmasq	GPL 2 ou 3	Principalement résolveurs — courant dans les systèmes embarqués, tels qu'OpenWRT, passerelles domestiques
Knot DNS	GPL 3.0	Faisant autorité — TLD .cz
Résolveur Knot	GPL 3.0	Résolveur — DNS4EU
NSD	BSD à 3 clauses	Faisant autorité — Rcode Zero
PowerDNS	GPL 2.0	Faisant autorité — Rakuten
PowerDNS Recursor	GPL 2.0	Résolveur — British Telecom
Unbound	BSD à 3 clauses	Résolveur — Quad9, Let's Encrypt
YADIFA	BSD à 3 clauses	Faisant autorité — TLD .eu

[72] Huston, Geoff. *« Looking at Centrality in the DNS » [Regard sur la centralité dans le DNS]*. Blog de l'APNIC (blog), 22 novembre 2022. https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/.
[73] Huston, *« Looking at Centrality in the DNS » [Regard sur la centralité dans le DNS]*.

Nonobstant l'existence de nombreux produits commerciaux sur ce marché, la majeure partie d'entre eux intègrent une ou plusieurs solutions FOSS en tant que composant DNS central de leur offre (Tableau 6).

Dans le nuage, les plateformes informatiques à très grande échelle, telles que Microsoft Azure, Google Cloud et AWS d'Amazon, exploitent toutes d'importantes infrastructures de résolution à l'appui de leurs services. Au moins quatre des principaux fournisseurs à très grande échelle s'appuient sur des FOSS pour la résolution DNS[74], tandis que d'autres ont mis au point des solutions propriétaires fondées sur des bibliothèques DNS de type FOSS (Tableau 7).

Enfin, certains utilisateurs finaux configurent leurs systèmes de manière à contourner le résolveur fourni par leur opérateur de réseau au profit de résolveurs publics ouverts. Si deux des services publics les plus prisés (le 8.8.8.8 de Google et le 1.1.1.1 de Cloudflare) ont recours à des logiciels propriétaires, d'autres résolveurs publics majeurs, tels que Quad9 (9.9.9.9) et DNS4EU, reposent sur des FOSS. De plus amples détails sont disponibles à l'annexe B.

Tableau 6 : Exemples de services DNS commerciaux intégrant des FOSS

Fabricant	Produit	Candidature	Intègre des FOSS
Akamai	Edge DNS	Résolveur en nuage hybride et service faisant autorité	Non
Bluecat Networks	Integrity, Micetro	Faisant autorité, résolveur	Oui
Cygna Labs	VitalQIP, DiamondIP	Faisant autorité, résolveur	Oui
EfficientIP	SolidServer DDI	Faisant autorité, résolveur, boîtier et nuage	Oui
F5	BIG-IP DNS	Résolveur	Oui
IBM	NS1 Connect	Service faisant autorité basé sur le nuage	Inconnu
InfoBlox	Universal DDI et NIOS DDI	Faisant autorité, résolveur, boîtier et nuage	Oui
Knipp	IronDNS	Faisant autorité	Partiellement
Microsoft	Serveur DNS de Windows	Faisant autorité, résolveur, utilisé dans les réseaux d'entreprise, s'intègre à Active Directory	Non
	Azure DNS	Service de résolveur en nuage	Oui
Netgate	pfSense	Résolveur	Oui
Oracle	OCI DNS	Service en nuage faisant autorité	Oui
TCPWave	DDI Management	Boîtier faisant autorité	Oui

[74] Conception vague pour des raisons de confidentialité.

Tableau 7 : Bibliothèques FOSS utilisées pour les applications d'infrastructure du DNS

Système logiciel	Langage de programmation	Application — Exemples d'utilisateurs
c-ares	C	libcurl, curl, NodeJS
dnsjava	Java	Systèmes back-end de registre (propriétaires)
dnspython	Python	Mailman, Samba, Ansible
domain	Rust	Cascade
miekg/dns	Go	Let's Encrypt, CoreDNS, Docker
ldns	C	Zonemaster, dnstap, serveurs de noms (propriétaires)
libunbound	C	Open vSwitch, libreswan, opendkim
Net::DNS	Perl	Spamassassin, Mail::DMARC, Mail::DKIM, Mail::SPF

5 Exemples contemporains de réglementation des FOSS

Cette section se penche sur plusieurs exemples récents (États-Unis, Royaume-Uni, Union européenne) illustrant l'adaptation, par les décideurs, de la réglementation en matière de cybersécurité à la réalité singulière de l'écosystème des FOSS. Le tableau 8 synthétise ces approches ; on y observe une tendance générale à exonérer les mainteneurs bénévoles de toute responsabilité directe pour cibler plutôt celle des entités commerciales assurant l'intégration ou le déploiement des FOSS. Ces cas sont analysés plus en détail ci-après.

Tableau 8 : Synthèse des approches réglementaires contemporaines applicables aux FOSS

Section	Axe principal	Exemple de réglementation	Traitement des FOSS
5.1	Répartition des responsabilités	Stratégie de cybersécurité des États-Unis (2023), Code du Royaume-Uni (2025)	Exonération des mainteneurs de toute responsabilité, ciblage des entités commerciales
5.2	Incitation à la collaboration	Règlement européen sur la cyberrésilience	Création d'un rôle facultatif d'« intendant » pour stimuler le soutien

5.3	Distinction avec le modèle propriétaire	Acte d'exécution de la directive européenne NIS 2	Absence de contrat = absence de fournisseur direct ; encouragement au soutien
5.4	Prévention des conflits entre régimes juridiques	Directive européenne NIS 2	Évitement des doublons pour les éléments mondiaux (serveurs racines)

5.1 Confier la responsabilité aux acteurs les mieux placés pour agir

La stratégie nationale de cybersécurité des États-Unis (2023)[75] a cherché à déplacer la responsabilité pour les produits et services logiciels non sécurisés (objectif stratégique 3.3). Elle a énoncé un principe directeur selon lequel « les éditeurs de logiciels doivent être libres d'innover, mais aussi répondre de leurs manquements au devoir de diligence envers les consommateurs, les entreprises ou les fournisseurs d'infrastructures critiques ». D'emblée, cette stratégie a réservé un traitement plus nuancé aux mainteneurs de logiciels FOSS : « La responsabilité incombe aux acteurs les mieux à même de prévenir les incidents, et non aux utilisateurs finaux — qui subissent souvent les conséquences des failles logicielles — ni au développeur d'un composant libre intégré ultérieurement à un produit commercial. »

Dans le même esprit, le Code de bonnes pratiques pour la sécurité des logiciels (Royaume-Uni, 2025)[76], d'application volontaire, a pour vocation d'« aider les fournisseurs de logiciels et leurs clients à réduire la probabilité et l'impact des attaques visant la chaîne d'approvisionnement et autres incidents affectant la cyberrésilience ». Son champ d'application cible lui aussi les fournisseurs de logiciels commerciaux : « S'agissant des logiciels libres, le développeur ou le mainteneur n'a aucune obligation formelle envers sa chaîne d'approvisionnement en aval ou pour la maintenance et la sécurité continues du code. Il appartient aux utilisateurs finaux ou aux développeurs de solutions propriétaires intégrant du code libre de gérer les risques y afférents. »

5.2 Encourager la collaboration intersectorielle au service d'une maintenance durable

Le règlement européen sur la cyberrésilience (CRA)[77] entend corriger le « faible niveau de cybersécurité des produits comportant des éléments numériques », lequel se traduit par « des vulnérabilités généralisées et une fourniture insuffisante et incohérente de mises à jour de

[75] Président des États-Unis. *« National Cybersecurity Strategy » [Stratégie nationale de cybersécurité]*. Washington, DC : La Maison-Blanche, 1er mars 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[76] « *Software Security Code of Practice* » [Code de bonnes pratique pour la sécurité des logiciels].

[77] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 relatif aux exigences horizontales de cybersécurité pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (Règlement sur la cyberrésilience), JO 2024 (L 2024/2847) 1, https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

sécurité pour y remédier ». S'il exonère pareillement de toute responsabilité les mainteneurs ne tirant pas profit de leurs FOSS, ce texte encourage la collaboration intersectorielle sur la maintenance durable des FOSS en introduisant un nouvel acteur juridique (« intendant de logiciels à code source ouvert ») chargé de « fournir un soutien continu au développement » et d'assurer « la viabilité de ces produits ». Le rôle d'intendant, facultatif et encore peu répandu, s'adresse aux organisations auxquelles les mainteneurs de logiciels FOSS peuvent s'associer comme moyen de canaliser les ressources des fabricants ou des opérateurs d'infrastructures essentielles tributaires des FOSS. Si le volume de logiciels FOSS actuellement soutenu par ce type d'organisation « intendant » demeure pour l'heure modeste, le CRA pourrait favoriser l'essor de cette pratique, qui semble du reste applicable à certaines organisations assurant la maintenance de logiciels DNS. Dernière innovation réglementaire : l'option future d'« attestations de sécurité volontaires », qui permettra une collaboration intersectorielle en matière de diligence raisonnable.

5.3 Éviter d'imposer à la chaîne d'approvisionnement des exigences de sécurité fondées sur le modèle propriétaire

La directive européenne NIS 2 vise à « atténuer les menaces pesant sur les réseaux et les systèmes d'information servant à fournir des services essentiels dans des secteurs clés[78] ». Elle classe l'infrastructure numérique comme « secteur hautement critique », définit les responsabilités de gestion en matière de cybersécurité et impose des « mesures de gestion des risques », précisées dans un acte d'exécution[79]. Ces mesures englobent « la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ». L'annexe énonçant ces exigences s'inspire des contrôles de la norme ISO/IEC 27002:2022 ; au mépris de la réalité des FOSS (voir section 3.2.2), elle présuppose l'existence d'une chaîne d'obligations contractuelles remontant jusqu'au développeur du logiciel.

Dans ses orientations techniques de mise en œuvre destinées aux entités réglementées[80], l'Agence de l'Union européenne pour la cybersécurité (ENISA) clarifie la notion de « fournisseur et prestataire de services directs » au regard des FOSS : « S'agissant des logiciels libres et à code source ouvert (FOSS), les communautés et projets qui assurent le développement, la maintenance et la distribution publics de logiciels ne sauraient être considérés comme des fournisseurs ou prestataires de services directs en l'absence de relation contractuelle entre l'entité concernée et le projet libre hormis l'adhésion à une licence de droit d'auteur normalisée, ou

[78] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (Directive NIS 2), JO 2022 (L 333) 80, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[79] Règlement d'exécution (UE) 2024/2690 de la Commission du 22 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2024/2847 du Parlement européen et du Conseil, JO 2024 (L 2024/2690) 1, https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj.

[80] Agence de l'Union européenne pour la cybersécurité (ENISA), *NIS2 Technical Implementation Guidance* [Orientations relatives à la mise en œuvre technique de la directive NIS 2] (rapport, Office des publications de l'Union européenne, 2025), https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

lorsque la relation contractuelle est établie avec un intendant de logiciels à code source ouvert. » Elle recommande plutôt d'« envisager de soutenir les communautés qui développent et maintiennent des FOSS et d'investir dans une relation mutuellement bénéfique ». Le cas échéant, cela peut passer par des relations avec l'intendant de logiciel OSS compétent qui « fournit un soutien durable au développement et assure la viabilité de ces produits ».

Un rapport commandé en 2025 par le Ministère britannique de la science, de l'innovation et de la technologie a recensé les pratiques du secteur en matière de code source ouvert et de risque lié à la chaîne d'approvisionnement[81]. Le rapport recommande notamment aux organisations d'« établir une politique interne relative aux OSS afin d'en gérer l'adoption des composants » et de « promouvoir un engagement actif auprès de la communauté OSS afin de […] garantir la qualité des composants et la pérennité de l'écosystème des OSS ». A contrario, une réglementation de sécurité inadaptée aux FOSS contraindrait les opérateurs à imposer des vérifications d'antécédents aux mainteneurs, considérés à tort comme des « fournisseurs » alors même que les FOSS ne font l'objet d'aucun achat. Une telle réglementation, malavisée, risquerait de pousser les talents du modèle FOSS à délaisser leurs projets ; la pénurie ou la compétence moindre des mainteneurs qui en résulterait entraînerait inévitablement une baisse de qualité. Un résultat qui va à l'encontre même de l'effet recherché par la réglementation sur la sécurité de la chaîne d'approvisionnement.

5.4 Éviter les conflits entre régimes régionaux pour les communautés mondiales des FOSS

La réglementation directe du développement logiciel et son application dans les infrastructures critiques demeure une pratique peu répandue. Le modèle FOSS reposant sur une collaboration mondiale (section 3.2.1), les futurs régimes réglementaires devront se garder d'instaurer, en fonction de la localisation physique des mainteneurs, des exigences qui se chevauchent ou entrent en conflit.

À cet égard, la directive européenne NIS 2[82] (citée plus haut) a pris grand soin d'éviter une situation similaire de régimes qui se chevauchent dans ses exigences à l'égard des fournisseurs de services DNS en excluant les serveurs de noms racines de son champ d'application, évitant ainsi aux opérateurs de serveurs racine d'être assujettis à des régimes régionaux concurrents, voire contradictoires[83].

[81] *« Open Source Software Best Practices and Supply Chain Risk Management »* [Meilleures pratiques en matière de logiciels à code source ouvert et gestion des risques liés à la chaîne d'approvisionnement].
[82] Directive NIS 2.
[83] On trouvera un résumé des arguments de Bert Hubert dans l'article « *Dear EU: Please Don't Ruin the Root* » [Chère UE, ne détruisez pas la racine], du 10 mai 2021. https://berthub.eu/articles/posts/dont-ruin-the-root/.

6 Principales conclusions

La présente section synthétise l'analyse du rapport en une série de conclusions ; celles-ci constituent la base probante sur laquelle s'appuient les recommandations opérationnelles présentées plus loin.

Conclusion 1 : Les FOSS constituent le socle de l'infrastructure critique du DNS. À l'heure où décideurs et organismes de réglementation s'emploient, partout dans le monde, à sécuriser la chaîne d'approvisionnement logicielle, il est impératif que leurs démarches reposent sur une compréhension précise des modalités réelles de construction et de maintenance des systèmes fondamentaux de l'Internet. Les recherches menées pour ce rapport confirment que l'infrastructure mondiale du DNS se trouve aujourd'hui en situation de dépendance massive à l'égard des FOSS. Dans les maillons les plus critiques de cette infrastructure, les FOSS sont la norme et les logiciels propriétaires sont l'exception. C'est notamment le cas du RSS, au sein duquel au moins 9 opérateurs sur 12 utilisent exclusivement des implémentations DNS de type FOSS, ainsi que des TLD, où 9 des 10 plus grands fournisseurs de services y ont recours.

Conclusion 2 : Le modèle de développement FOSS se distingue fondamentalement du logiciel propriétaire. Si le logiciel propriétaire est généralement le produit interne d'une organisation unique, le modèle FOSS est ouvert et distribué. Il repose sur quatre libertés cardinales garanties par ses licences : utiliser, étudier, partager et modifier le logiciel. Ce cadre a permis l'éclosion d'un écosystème unique de mainteneurs, de contributeurs et d'opérateurs qui, pour la plupart, s'affranchissent des liens contractuels propres aux chaînes d'approvisionnement commerciales classiques.

Conclusion 3 : Les FOSS ne sont ni intrinsèquement plus sûrs, ni moins sûrs que les logiciels propriétaires ; la sécurité tient aux processus et à la maintenance, non à la visibilité du code source. Les implications de ce modèle ouvert en matière de sécurité doivent s'appréhender à la lumière d'un débat vieux de plusieurs décennies, resté sans réponse tranchée. Comme le résume Ross Anderson, chercheur en ingénierie de la sécurité, la visibilité du code source des systèmes vastes et complexes profite à parts égales aux attaquants et aux défenseurs. À long terme, le caractère ouvert ou fermé d'un système n'a qu'une incidence mineure sur la sécurité de celui-ci. L'occultation du code source n'est pas un gage de sécurité supplémentaire ; la sûreté d'un système découle bien davantage de la qualité du développement et de la rigueur des processus de révision et de maintenance.

Conclusion 4 : L'écosystème FOSS du DNS possède des atouts uniques favorisant la stabilité et la résilience. Si l'ouverture est en soi un facteur neutre, le processus collaboratif qu'elle autorise s'avère particulièrement efficace pour bâtir et maintenir l'infrastructure critique de l'Internet. La transparence inhérente aux FOSS permet à une communauté mondiale de développeurs, chercheurs et opérateurs d'étudier le code source et de remédier collectivement aux vulnérabilités, garantissant souvent un déploiement des correctifs plus rapide que dans les systèmes propriétaires. Il en résulte des atouts intrinsèques : une sécurité concertée renforcée,

une résilience opérationnelle accrue par la diversité logicielle, et une stabilité remarquable assurée par le soutien à long terme d'organisations dédiées, commerciales ou à but non lucratif.

Conclusion 5 : Le modèle FOSS comporte des risques inhérents qui exigent une approche sur mesure, non uniforme, en matière de politiques. Les caractéristiques qui font la force de ce modèle introduisent aussi des risques spécifiques appelant, sur le plan des politiques, une réponse adaptée. Du fait que le modèle FOSS dissocie le financement de l'utilisation, les projets peuvent se heurter à des problèmes de viabilité financière et d'épuisement des mainteneurs ; ainsi, une infrastructure critique peut reposer sur le travail bénévole et non financé d'une poignée d'individus. En outre, la réutilisation généralisée de composants FOSS engendre un risque de dépendances partagées : une vulnérabilité dans une seule bibliothèque peut alors avoir des répercussions en cascade sur l'ensemble de l'écosystème. Ce type de problèmes ne saurait être résolu par des réglementations conçues pour le marché du logiciel commercial et propriétaire.

Conclusion 6 : L'imposition de nouvelles responsabilités juridiques et financières liées au développement et à la distribution des FOSS exige la plus grande prudence, sous peine de déstabiliser l'environnement qui a permis l'essor de cet élément fondamental de l'infrastructure Internet. L'absence, dans les projets FOSS, d'entité juridique unique et responsable ou de chaîne contractuelle classique rend l'application des cadres classiques de responsabilité aussi impraticable que risquée. Le modèle de développement FOSS repose sur des bénévoles et de petites organisations qui ne disposent que de financements minimes. Faire peser un lourd fardeau réglementaire sur ces mainteneurs risquerait de décourager leur engagement, de brider l'innovation et de conduire à l'abandon de logiciels pourtant vitaux pour l'infrastructure critique de l'Internet.

Conclusion 7 : Les FOSS sont un levier essentiel pour l'entrée de nouveaux fournisseurs sur le marché des services Internet ; il offre aux décideurs l'opportunité d'encourager le développement de services locaux et de réduire la dépendance aux fournisseurs d'informatique en nuage étrangers. Au-delà de sa fonction technique, le modèle FOSS est un vecteur de croissance économique, d'autonomie numérique et de concurrence. En éliminant les frais de licence, le modèle de développement FOSS réduit le coût d'entrée sur le marché pour les nouvelles entreprises. Cette accessibilité favorise l'innovation et les compétences locales ; elle offre aux décideurs un levier puissant pour diversifier l'écosystème numérique et réduire la dépendance aux services en nuage étrangers.

7 Recommandations pratiques à l'intention des décideurs

S'appuyant sur les constats du rapport, cette section énonce des recommandations directes et pratiques à l'intention des décideurs. L'objectif est de favoriser l'élaboration de réglementations efficaces et inoffensives, capables de renforcer — au lieu de fragiliser — un écosystème FOSS indispensable à la sécurité et à la stabilité du fonctionnement de l'Internet.

Recommandation 1 : Reconnaître le rôle critique des FOSS. Le présent rapport établit que l'infrastructure mondiale du DNS se trouve en situation de dépendance à l'égard des FOSS. Dans

les maillons les plus critiques de cette infrastructure, les FOSS sont la norme et les logiciels propriétaires sont l'exception. Il convient dès lors que les décideurs reconnaissent expressément, dans tout texte législatif ou réglementaire pertinent, que les FOSS constituent l'assise de l'infrastructure critique de l'Internet et que leur utilisation est un atout à préserver. Cette reconnaissance doit orienter la réglementation dès sa conception, afin de ne pas causer de préjudice involontaire à l'écosystème.

Recommandation 2 : Consulter la communauté FOSS. Ouvert et distribué, le modèle de développement FOSS diffère radicalement de celui du logiciel propriétaire. Cet écosystème rassemble mainteneurs, contributeurs et opérateurs généralement affranchis des liens contractuels propres aux chaînes d'approvisionnement commerciales classiques. Il est donc primordial d'associer l'ensemble des acteurs de cet écosystème — entreprises, associations, mainteneurs individuels et institutions communautaires — à toutes les étapes de l'élaboration des politiques. Cette démarche garantit une réglementation adaptée aux réalités opérationnelles, évitant ainsi de porter préjudice à l'écosystème des FOSS et, par ricochet, à l'infrastructure critique de l'Internet.

Recommandation 3 : S'inspirer des exemples contemporains en matière de réglementation des FOSS. Comme l'indique la section 5, des initiatives réglementaires récentes ont commencé à intégrer les spécificités des FOSS, tout en faisant avancer les objectifs essentiels de leurs politiques. Ces précédents offrent un cadre de référence précieux pour l'élaboration de nouvelles politiques taillées sur mesure pour l'écosystème des FOSS. Appliquer ces enseignements implique de concevoir des politiques et réglementations qui :

- imputent la responsabilité aux acteurs les mieux placés pour agir. Le devoir de protection incombe alors aux entités qui déploient le logiciel dans des produits commerciaux ou des infrastructures critiques, et non aux développeurs bénévoles de logiciels FOSS qui en créent les composants ;
- encouragent la collaboration intersectorielle au service d'une maintenance durable. La viabilité des produits FOSS critiques passe par des modèles juridiques innovants, tel l'« intendant de logiciels à code source ouvert », qui permet de canaliser des ressources depuis le secteur ;
- évitent d'imposer à la chaîne d'approvisionnement des exigences de sécurité fondées sur le modèle propriétaire. Rappelons que, dans le modèle FOSS, il n'existe souvent aucun lien contractuel direct entre le mainteneur et l'opérateur, hormis la licence code source ouvert elle-même ;
- préviennent les conflits entre régimes régionaux pour les communautés mondiales des FOSS. Il convient de proscrire les obligations concurrentes ou contradictoires imposées aux projets FOSS mondiaux, afin d'éviter la fragmentation du développement et l'affaiblissement de la sécurité.

Recommandation 4 : Favoriser la pérennité des FOSS. Le modèle FOSS dissocie le financement de l'utilisation, ce qui constitue fréquemment une source de précarité financière et d'épuisement pour les mainteneurs. Des infrastructures critiques peuvent ainsi reposer sur de petites structures ou sur le travail bénévole et non rétribué d'une poignée d'individus. Pour

pallier ce risque, les décideurs sont invités à instaurer des politiques incitatives qui stimulent les contributions des secteurs public et privé aux projets FOSS d'importance critique, en considérant ce type de contributions comme une forme d'investissement dans un bien public commun.

Recommandation 5 : Répondre collectivement aux risques systémiques. La réutilisation généralisée de composants FOSS engendre un risque de dépendances partagées : une vulnérabilité dans une seule bibliothèque peut se répercuter en cascade sur tout l'écosystème, affectant aussi bien les logiciels FOSS que propriétaires. Comme ce risque systémique est inhérent à tout développement logiciel moderne, les politiques devraient promouvoir et financer des solutions collaboratives à l'échelle de l'écosystème — outils de sécurité améliorés, recherche indépendante — plutôt que de faire peser l'intégralité de la charge sur les épaules des mainteneurs bénévoles.

8 Remerciements, déclarations d'intérêt et désistements

Par souci de transparence, les sections suivantes fournissent au lecteur des informations relatives à certains aspects du processus du SSAC. La section Remerciements donne la liste des membres du SSAC, des spécialistes externes et du personnel de l'ICANN qui ont coécrit ce document spécifique, qui y ont directement contribué ou qui en ont assuré des révisions. La section Déclarations d'intérêt comprend un lien vers les biographies des membres du SSAC, dans lesquelles sont indiqués les éventuels sujets susceptibles d'engendrer un conflit d'intérêts (qu'il soit réel, présumé ou possible) en raison de la contribution d'un membre à ce rapport. La section Désistements indique quelles sont les personnes qui ont choisi de ne pas participer aux débats concernant le sujet du présent rapport. Tous les membres du SSAC, à l'exception de ceux cités dans la section Désistements, approuvent le présent document.

8.1 Remerciements

Le Comité tient à remercier les membres du SSAC indiqués ci-dessous, les invités d'honneur et le personnel de l'ICANN pour leur temps, leurs contributions et leurs révisions.

Membres du SSAC
Joe Abley
Maarten Aertsen (coprésident de l'équipe de travail)
Gautam Akiwate
Tim April
Nabil Benamar
KC Claffy
Hadia Elminiawi
Ondrej Filip (membre du SSAC jusqu'au 31 décembre 2024)
James Galvin
Robert Guerra
Russ Housley
Matthias Hudobnik

Geoff Huston
Layal Jebran
Merike Kaeo (membre du SSAC jusqu'au 31 décembre 2024)
Andrei Kolesnikov
Warren « Ace » Kumari
Barry Leiba (coprésident de l'équipe de travail)
John Levine
Russ Mundy
Ram Mohan
Matt Thomas
Peter Thomassen
Tara Whalen
Suzanne Woolf
Jiankang Yao

Invités d'honneur :
Vittorio Bertola
Merike Kaeo (invité d'honneur à compter du 1er janvier 2025)
Vicky Risk
Raffaele Sommese

Personnel de l'ICANN
John Emery (éditeur)
Daniel Gluck
Gustavo Lozano Ibarra
Michael Puckett
Carlos Reyes
Danielle Rutherford (éditeur, auteur contributeur)
Kathy Schnitt
Steve Sheng (membre du personnel de soutien du SSAC jusqu'au 30 novembre 2024)

8.2 Déclarations d'intérêt

Les biographies et les déclarations d'intérêt des membres du SSAC, au moment de la publication, sont disponibles à l'adresse suivante : https://www.icann.org/en/ssac/members/archive/16-05-2025.

8.3 Désistements

Il n'y a pas eu de désistements.

Annexe A : Glossaire et acronymes

A.1 Glossaire des termes

Serveur faisant autorité : Serveur détenteur des enregistrements DNS officiels et définitifs pour un nom de domaine donné. Il fournit les réponses ultimes aux requêtes DNS concernant ce domaine.

Contributeur : Personne physique ou morale proposant des améliorations à un projet FOSS, notamment par la soumission de code, de documentation ou de signalements d'erreurs.

Entiercement de données : Dépôt d'une copie des données d'enregistrement de domaine auprès d'un tiers accrédité par l'ICANN, à des fins de conservation sécurisée.

Nom de domaine : Nom unique et intelligible (ex. : icann.org) identifiant une adresse spécifique sur Internet et constituant la base des URL.

Système des noms de domaine (DNS) : Système mondial décentralisé faisant office d'« annuaire de l'Internet » ; il convertit les noms de domaine intelligibles en adresses IP numériques, indispensables à la localisation des services et équipements informatiques.

Protocole d'avitaillement extensible (EPP) : Protocole technique normalisé assurant l'automatisation des transactions entre bureaux d'enregistrement et opérateurs de registre (enregistrements, renouvellements, transferts, etc.).

Bifurcation : Nouveau projet logiciel distinct, lancé à partir d'une copie du code source d'un projet FOSS existant.

Logiciels libres et à code source ouvert (FOSS) : Logiciels sous licence garantissant aux utilisateurs quatre libertés fondamentales : l'utilisation, l'étude, le partage et la modification du logiciel. Cette définition renvoie à un modèle de développement collaboratif, et non à la simple gratuité du logiciel.

Adresse de Protocole Internet (IP) : Identifiant numérique unique attribué à tout appareil connecté à un réseau informatique utilisant le protocole Internet pour communiquer.

Nom de domaine internationalisé (IDN) : Nom de domaine dont une ou plusieurs étiquettes contiennent des caractères autres que des lettres ASCII, des chiffres ou des traits d'union.

Mainteneur : Personne ou groupe responsable de l'orientation générale et du contrôle qualité d'un projet FOSS. Ils ont autorité pour accepter ou rejeter les contributions à la version officielle du logiciel.

Opérateur : Personne physique ou morale qui déploie et utilise un logiciel pour assurer un service. Dans le contexte du DNS, l'opérateur est l'entité qui exploite des composants d'infrastructure, tels que des serveurs faisant autorité ou des résolveurs.

Publication (dans le DNS) : Processus technique rendant les enregistrements DNS d'un domaine accessibles sur les serveurs faisant autorité, permettant ainsi la résolution du nom de domaine sur Internet.

Résolveur récursif (ou résolveur) : Serveur, souvent géré par un fournisseur de services Internet (FSI), qui agit pour le compte de l'appareil de l'utilisateur afin de trouver l'adresse IP correspondant au nom de domaine demandé.

Enregistrement (dans le DNS) : Procédure administrative consistant à réserver un nom de domaine unique en l'inscrivant dans la base de données principale faisant autorité (le registre) d'un domaine de premier niveau spécifique.

Titulaire de nom de domaine : Personne physique ou morale qui enregistre un nom de domaine spécifique et en détient les droits.

Bureau d'enregistrement : Organisation servant d'interface commerciale (« détaillant ») pour les noms de domaine ; elle gère les réservations de domaine pour le compte des titulaires.

Opérateur de registre : Base de données principale faisant autorité et regroupant tous les noms de domaine enregistrés sous chaque domaine de premier niveau (ex. : le registre .org). L'entité assurant la maintenance de cette base est l'opérateur de registre.

Système des serveurs racine (RSS) : Ensemble des serveurs situés au sommet de la hiérarchie du DNS, chargés d'aiguiller les requêtes vers les serveurs de domaine de premier niveau appropriés.

Domaine de premier niveau (TLD) : Segment du nom de domaine, situé à droite du dernier point (ex. : .com, .org ou .uk).

Adresse universelle (URL) : Adresse complète permettant de localiser une ressource spécifique sur Internet ; elle comprend généralement un protocole (ex. : https), un nom de domaine et un chemin d'accès (ex. : https://www.icann.org/resources).

A.2 Abréviations employées dans le présent rapport

ccTLD : Domaine de premier niveau géographique
DNS : Système des noms de domaine
EPP : Protocole d'avitaillement extensible
FOSS : Logiciels libres et à code source ouvert
gTLD : Domaine générique de premier niveau
IP : protocole Internet

FSI : Fournisseur de services Internet
RSS : Système des serveurs racine
SSAC : Comité consultatif sur la sécurité et la stabilité
TLD : Domaine de premier niveau
URL : Adresse universelle (URL)
IDN : Nom de domaine internationalisé

Annexe B : Méthodologie et résultats de la recherche sur la prépondérance des FOSS

Cette annexe constitue une synthèse exhaustive et autonome des travaux de recherche originaux du rapport. Elle détaille la méthodologie employée pour établir la prépondérance des logiciels libres et à code source ouvert (FOSS), ainsi que les conclusions qui en découlent, présentées à la section 4 du présent rapport.

B.1 Approche générale et difficultés

Il est difficile de déterminer avec certitude quels logiciels sont utilisés par les opérateurs en conditions réelles. Si certains enregistrements du système des noms de domaine (DNS) (version.bind, authors.bind, id.server, etc.) ont été créés pour permettre aux utilisateurs finaux d'identifier la version du serveur DNS interrogé, leur adoption reste limitée en raison des risques potentiels de sécurité et de la nécessité d'une configuration manuelle. La littérature spécialisée a exploré d'autres méthodes, notamment l'analyse passive et les mesures actives. Toutefois, ces approches ont souvent une portée restreinte — certaines ne permettant d'identifier que l'infrastructure récursive — et se heurtent à des problèmes d'évolutivité.

C'est pourquoi l'approche privilégiée ici cible l'évaluation des grands opérateurs du DNS en fonction de leur part de marché, ce qui a permis de confirmer directement l'utilisation significative de logiciels à code source ouvert.

B.2 Infrastructure d'enregistrement des noms de domaine

B.2.1 Méthodologie

Afin d'évaluer l'utilisation des FOSS dans l'infrastructure d'enregistrement, le Comité consultatif sur la sécurité et la stabilité (SSAC) a mené une enquête auprès des principaux opérateurs de registre et prestataires de services de registre back-end. Pour les services d'entiercement de données, l'enquête a ciblé les agents d'entiercement de données (DEA) approuvés par l'ICANN et répertoriés sur son site Web ; l'accent a été mis sur les logiciels assurant les fonctions clés du service (transfert de données, vérification des signatures et des dépôts, interaction avec l'API des interfaces de déclaration d'enregistrement [RRI]).

B.2.2 Conclusions

L'infrastructure d'enregistrement désigne les systèmes assurant l'enregistrement des noms de domaine individuels et leur publication dans le DNS public. Bien que l'on ne dispose pas de données précises sur l'ampleur exacte de l'utilisation de logiciels FOSS, les éléments recueillis attestent d'une forte dépendance à l'égard de cette technologie, tant sous forme de systèmes complets que de composants fondamentaux.

Nombre d'opérateurs de registre, en particulier dans l'espace des domaines de premier niveau géographiques (ccTLD), gèrent une infrastructure d'enregistrement entièrement basée sur les FOSS (Tableaux 1 et 2). À titre d'exemple, la plateforme de registre FRED est utilisée par au moins 12 registres de ccTLD, tandis que la plateforme Nomulus est utilisée pour plusieurs TLD génériques (gTLD).

À l'inverse, les opérateurs de registre et les fournisseurs de services de registre back-end de grande envergure privilégient souvent des solutions propriétaires. Toutefois, ces systèmes ne sont généralement pas créés de zéro ; il s'agit plutôt d'extensions propriétaires personnalisées intégrant des composants (bases de données, serveurs Web, notamment) majoritairement issus du monde FOSS.

Cette dépendance à l'égard des FOSS s'étend aux services d'entiercement de données (Tableau 3), chargés du stockage sécurisé des copies des données d'enregistrement de domaine. Les principaux fournisseurs de ces services, tant pour les registres que pour les bureaux d'enregistrement, ont bâti leurs systèmes, du moins en partie, sur des composants FOSS.

B.3 Infrastructure du DNS

B.3.1 Méthodologie

Analyse des serveurs faisant autorité : Pour étudier l'utilisation des FOSS dans l'infrastructure des TLD, la procédure suivante a été appliquée :

1. récupération de la zone racine auprès de l'IANA et mise en correspondance des TLD avec les adresses IP de leurs serveurs de noms ;
2. analyse distincte des ccTLD, prenant en compte à la fois les TLD à deux lettres et leurs équivalents étiquette-A (Punycode), afin d'inclure les ccTLD internationalisés (IDN) ;
3. utilisation de la bibliothèque Python ip2asn pour associer ces adresses IP à leurs numéros de système autonome (ASN) et aux noms ASN (opérateurs) correspondants ;
4. calcul de la part de marché, en divisant le nombre de TLD hébergés par un opérateur donné par le nombre total de TLD (étant entendu qu'un TLD peut être hébergé simultanément par plusieurs opérateurs) ;
5. Identification des 25 principaux opérateurs et vérification manuelle de leur utilisation de logiciels à code source ouvert pour leurs serveurs de noms faisant autorité.

Analyse des résolveurs : Il n'existe aucun recensement fiable de l'ensemble du parc installé de résolveurs. Aux fins du présent rapport, l'analyse s'est attachée à recenser les principaux opérateurs et types de déploiements (local, en nuage, public) et à déterminer, sur la base de déclarations publiques et de connaissances directes, s'ils recourent à des logiciels FOSS ou propriétaires.

B.3.2 Conclusions

Serveurs faisant autorité : C'est dans l'infrastructure de publication des données de domaine que la prédominance des FOSS est la plus manifeste. Au sommet de la hiérarchie du DNS — la racine et les TLD — les FOSS sont quasi omniprésents. Le système des serveurs racines (RSS) constitue la clé de voûte du DNS. Sur les 12 organisations indépendantes exploitant les serveurs racines, au moins 9 utilisent exclusivement des implémentations DNS de type FOSS pour répondre aux requêtes (Tableau 4).

Cette tendance se confirme à l'échelon suivant de la hiérarchie, celui des serveurs de noms de TLD (Tableau 5). Les recherches menées pour ce rapport révèlent que 9 des 10 principaux opérateurs fournissant des services DNS faisant autorité aux registres de TLD ont recours aux FOSS. En outre, 20 des 25 principaux opérateurs assurant ce service pour les ccTLD utilisent des logiciels DNS de type FOSS, desservant collectivement 234 ccTLD uniques.

Résolveurs : La prépondérance des FOSS ne se limite pas à la publication des données DNS ; elle s'étend également à l'infrastructure assurant l'extraction de ces informations : l'écosystème diversifié des résolveurs DNS.

La plupart des utilisateurs dépendent de résolveurs locaux gérés par leur fournisseur de services Internet (FSI), leur entreprise ou leur établissement d'enseignement. Si de nombreux produits commerciaux existent sur ce marché, la plupart intègrent une ou plusieurs solutions FOSS comme composant DNS central de leur offre.

Dans le nuage, les plateformes de calcul à très grande échelle, telles que Microsoft Azure, Google Cloud et Amazon Web Services, exploitent toutes une importante infrastructure de résolveurs à l'appui de leurs services. Au moins quatre des principaux acteurs à très grande échelle s'appuient sur les FOSS pour la résolution DNS, tandis que d'autres ont mis au point des solutions propriétaires fondées sur des bibliothèques DNS de type FOSS.

Annexe C : Enquête sur la perception des FOSS et de la réglementation des logiciels par les opérateurs du DNS

Afin d'étayer le présent rapport, le Comité consultatif sur la sécurité et la stabilité (SSAC) a réalisé un sondage informel en ligne portant sur les répercussions prévisibles de la réglementation relative aux logiciels à code source ouvert sur l'infrastructure du DNS. Le choix de l'outil EUSurvey a permis de garantir la confidentialité et l'anonymat des participants[84]. Le sondage a été relayé auprès de la communauté technique du DNS via plusieurs listes de diffusion, notamment celles techniques et juridiques du Conseil des registres de noms de domaine de premier niveau nationaux européens (CENTR), celles des groupes de travail consacrés au DNS et au code source ouvert du Centre de coordination des réseaux IP européens (RIPE-NCC), ainsi que les listes d'utilisateurs de plusieurs systèmes logiciels à code source ouvert du DNS. Le sondage a par ailleurs été réalisé lors de la réunion de février du Centre d'analyse et de recherche pour les opérations DNS (DNS-OARC).

Cette démarche visait principalement à déterminer si les opérateurs techniques du DNS ont connaissance des initiatives réglementaires en cours et à recueillir leur avis sur les effets potentiels d'une réglementation des FOSS. Le sondage, ouvert durant tout le mois de février 2025, a recueilli 98 réponses émanant d'un éventail représentatif des différents rôles au sein de l'infrastructure du DNS.

Les participants ont d'abord été interrogés sur la nature de leur implication dans le DNS : 96 sur 98 ont déclaré être actifs dans l'infrastructure DNS, et 64 ont également indiqué intervenir dans l'infrastructure d'enregistrement des noms de domaine. Vingt-quatre participants ont mentionné la fonction de « développeur/fournisseur de logiciels » parmi leurs rôles, mais aucun ne s'est exprimé exclusivement à ce titre. (La nature ouverte ou propriétaire de leurs logiciels n'a pas fait l'objet d'une question.)

Les répondants étaient des utilisateurs de code source ouvert, assez au fait de la réglementation. La quasi-totalité des répondants (93 %) a déclaré utiliser des logiciels à code source ouvert. Environ un tiers (33 %) a indiqué utiliser également des logiciels propriétaires. Trente pour cent des participants assurent par ailleurs une fonction de conseil pour la mise en œuvre et l'exploitation des FOSS ; ce groupe affichait une connaissance élevée des initiatives réglementaires actuelles. À la question « De quelles initiatives réglementaires avez-vous connaissance ? (cochez toutes les réponses pertinentes) », soumise avec une liste de textes de référence, soixante-dix-sept répondants (soit environ 77 %) ont indiqué en connaître au moins une. Le règlement sur la cyberrésilience (CRA), le règlement sur la cybersécurité et la directive NIS 2 de l'UE sont connus de plus de 40 % des participants. Trente pour cent des répondants ont déclaré également connaître une ou plusieurs initiatives du Gouvernement américain, notamment les décrets présidentiels 14028 et 14144, le programme d'attestation de développement logiciel sécurisé, ou le label « CyberTrust » pour l'Internet des objets (IoT). Parmi les autres réglementations citées figuraient la loi australienne sur la sécurité des infrastructures critiques

[84] « EUSurvey – À propos ». https://ec.europa.eu/eusurvey/home/about?language=fr.

(SOCI), le Règlement général sur la protection des données (RGPD), la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), ainsi que le programme fédéral de gestion des risques et des autorisations (FedRAMP) aux États-Unis et au Canada.

Nous avons demandé : « Quelles sont vos préoccupations spécifiques concernant les répercussions de la réglementation des logiciels sur votre organisation ? », en proposant des options tant positives que négatives. L'ensemble des participants a été en mesure de répondre, y compris ceux qui ne connaissaient aucune des réglementations citées.

- 72 % ont jugé qu'il était raisonnablement probable que certains projets à code source ouvert puissent être abandonnés, ou devenir indisponibles ;
- 66 % ont estimé que la conformité augmenterait le coût des logiciels pour eux ;
- 49 % redoutaient que certains projets à code source ouvert sur lesquels ils comptent puissent passer à une licence propriétaire ;
- 29 % ont pensé que la réglementation empêchera leur organisation de publier des logiciels à code source ouvert ;
- 21 % ont anticipé une amélioration de la sécurité des logiciels à code source ouvert qu'ils utilisent ;
- 7 % ont prévu que la réglementation allégera la charge liée à l'évaluation de la sécurité et de la qualité des logiciels au sein de leur organisation.

Bien que nous ayons expressément sollicité, dans un souci d'équilibre, des commentaires sur les conséquences positives et les opportunités, les répondants se sont montrés majoritairement pessimistes.

C.1 Commentaires libres (préoccupations spécifiques)

Le sondage invitait les participants à formuler des commentaires libres sur leurs préoccupations spécifiques quant aux conséquences de la réglementation, ainsi que sur les opportunités ou retombées positives attendues.

Les préoccupations les plus fréquentes sont les suivantes :

- augmentation des coûts de mise en conformité ;
- ralentissement du déploiement des logiciels ;
- risque d'abandon de certains projets à code source ouvert, face au fardeau réglementaire ;
- complexité juridique accrue en matière de conformité pour les utilisateurs de logiciels à code source ouvert.