Internet
made in France

La lettre n°10

1

Le CENTR : une organisation humaine, technique et stratégique au service des registres européens

Lorsqu'on parle de gouvernance d'internet, on pense souvent à ses acteurs globaux tels que l'ICANN (*Internet Corporation for Assigned Names and Numbers*) pour son rôle global dans la coordination du DNS, ou l'UIT (*Union Internationale des Télécommunications*) pour ses ambitions normatives et ses politiques d'harmonisation de l'utilisation des fréquences. Pourtant, derrière la stabilité du DNS (*Domain Name System*), la gouvernance de l'internet s'organise aussi au niveau régional. En Europe, le CENTR (*Council of European National Top-Level Domain Registries*) joue ainsi le rôle pivot de rassembler les registres nationaux de noms de domaine (les ccTLD pour *country code Top-Level Domains*, comme le .fr en France), de coordonner les actions techniques, faciliter la coopération et contribuer à la résilience globale.

Car si internet est mondial par nature, il n'en reste pas moins décentralisé dans sa gestion quotidienne. Chaque ccTLD reflète une réalité juridique, politique, économique, souvent nationale. Et c'est dans cet entre-deux, entre infrastructure technique et attachement territorial, que le CENTR s'est construit. Basé à Bruxelles, le CENTR réunit aujourd'hui plus de 50 membres, dont la majorité des registres nationaux européens. Son périmètre dépasse toutefois largement les frontières de l'Union européenne : on y retrouve aussi des membres comme l'Australie, Israël, le Canada ou l'Ukraine.

Faire coopérer les registres

Le CENTR fonctionne sur une logique volontaire. Il ne donne pas de directives à ses membres et ne parle pas en leur nom sauf quand ses membres lui en donne le mandat exprès, par exemple dans le cadre d'une prise de position générale sur une nouvelle régulation en cours de discussion à Bruxelles. Il organise, structure, facilite. Ses groupes de travail spécialisés — technique, juridique, sécurité, marketing, recherche et développement… — sont le cœur battant de cette coopération. Ils ne sont pas théoriques, mais des lieux d'échanges concrets, parfois confidentiels, souvent cruciaux. Ils permettent aux registres les plus petits de bénéficier de l'expertise des plus grands, et vice-versa, de faciliter la mutualisation des ressources et des infrastructures (comme les serveurs DNS secondaires) ou encore de coordonner des réponses à des menaces de cybersécurité.

La force du CENTR ne tient pas à son statut juridique ni à un quelconque mandat politique. Elle repose sur une ressource rare : la confiance. Confiance entre personnes qui se connaissent, échangent régulièrement et partagent une même culture technique. Les directeurs techniques, juristes et responsables d'opérations se retrouvent plusieurs fois par an. Les échanges y sont francs, souvent hors micro, mais essentiels. On y parle d'incidents, de jurisprudence, de stratégies. C'est cette confiance interpersonnelle, forgée dans le temps long, qui permet à des registres de pays très différents de s'entraider et de co-construire.

Cette coopération entre pairs est rendue possible par le fait que les ccTLD ne sont pas en concurrence frontale et peuvent donc partager données, bonnes pratiques, outils techniques ou solutions de cybersécurité sans enjeu commercial. L'objectif est ici d'élever collectivement le niveau de robustesse, de qualité de service et de sécurité de l'infrastructure DNS.

Si des organisations similaires existent dans d'autres régions du monde (l'APTLD en Asie-Pacifique, le LACTLD en Amérique latine, l'AFTLD en Afrique) et remplissent des fonctions comparables de coordination entre registres nationaux, aucune n'a atteint le niveau de structuration et d'efficacité du CENTR. Plusieurs raisons à cela : ailleurs, les territoires sont très vastes, les différences de culture et de maturité techniques très marquées entre ccTLD, les modèles économiques très variés. À l'inverse, le CENTR bénéficie d'un environnement plus homogène, où la proximité géographique et une culture technique commune ont permis de construire, dans la durée, un espace de travail partagé, fondé sur la confiance.

Le CENTR n'est ainsi ni un régulateur, ni un organe exécutif, ni un porte-parole. C'est un espace de coopération volontaire entre pairs, avec une structure légère et agile, fondée sur la confiance humaine et le respect de l'autonomie de chaque membre. Le CENTR fonctionne par l'engagement actif de ses membres dans des groupes de travail, ateliers, projets communs, où la transparence, l'entraide et l'intelligence collective priment.

L'évolution des missions du CENTR : partager, former, accompagner

À l'origine, le CENTR est d'abord un espace de partage entre pairs. C'est dans cette logique que l'organisation a vu le jour : permettre à des registres nationaux de trouver, au-delà de leurs frontières, un appui, des retours d'expérience et une forme de solidarité technique. Les premiers échanges ont porté sur des questions très opérationnelles — modèles de gouvernance, résolution DNS, relations avec les bureaux d'enregistrement — mais aussi sur les premiers contentieux liés à la gestion de noms de domaine. Les litiges soulevés dans un pays devenaient des cas d'étude utiles ailleurs. Cette revue collective de la jurisprudence, informelle mais structurante, a permis aux membres du CENTR de mieux anticiper les risques et d'adopter des réponses cohérentes, adaptées à leurs contextes nationaux.

Avec le temps, un deuxième axe est apparu : celui de la formation et de la sensibilisation. Cette évolution ne relève pas d'un changement de cap, mais d'un approfondissement naturel du rôle de facilitateur que joue le CENTR. Face à l'émergence de réglementations européennes touchant aux activités des ccTLD (en matière de cybersécurité, de données personnelles ou de délégation de service public), de nombreux registres ont exprimé le besoin d'être accompagnés. Le CENTR a donc produit des ressources, organisé des séminaires et invité des experts à venir décrypter les textes réglementaires nouveaux ou à venir. Dans le même temps, l'organisation a également commencé à jouer un rôle de pédagogue auprès des institutions européennes, en expliquant ce que sont les registres, comment ils fonctionnent et quelles sont les limites structurelles de leur action. Ce travail de formation et de sensibilisation est devenu un pilier de la présence du CENTR dans les enceintes où se construit aujourd'hui la régulation du numérique.

C'est ce positionnement, à la fois technique et pédagogique, qui a conduit plus récemment à un troisième rôle : l'accompagnement. Le CENTR n'est pas un syndicat ni un organe de représentation politique. Il ne parle pas au nom de ses membres, qui ont chacun leurs réalités et leurs relations nationales. En revanche, il est devenu un point de contact crédible et neutre pour les institutions qui souhaitent comprendre les impacts de leurs décisions sur l'écosystème des ccTLD.

Pour encadrer cette posture, le CENTR a mis en place deux outils qui lui permettent de structurer ses prises de parole tout en respectant l'autonomie de ses membres :

- Le ***Position Paper.*** Adopté à l'unanimité, il exprime une position collective sur un sujet de fond, généralement en lien avec une évolution réglementaire. Il ne représente pas les registres individuellement, mais pose un socle de principes communs, utiles pour éclairer les débats institutionnels.
- Le ***Board Statement.*** Rédigé et adopté uniquement par le conseil d'administration du CENTR, il permet de réagir rapidement à une actualité ou de formuler une contribution sur un point précis, sans engager l'ensemble des membres. C'est un outil souple, bien adapté aux sujets techniques ou à l'expression de préoccupations partagées.

Dans chacun de ces trois rôles — partage, formation, accompagnement —, le CENTR conserve sa ligne : ne pas se substituer à ses membres, mais leur permettre de gagner en cohérence, en lisibilité et en solidité dans un environnement qui devient de plus en plus exigeant. Son évolution est celle d'un organe de coopération qui, sans changer de nature, a su prendre acte de ses responsabilités collectives et évoluer.

Préserver la coopération dans un environnement sous tension

Si le CENTR repose sur la coopération volontaire, il ne fonctionne pas dans un vide politique. Le contexte international, les évolutions réglementaires européennes ou encore les dynamiques internes entre membres viennent régulièrement éprouver la robustesse de son modèle. Le maintien de la confiance, condition essentielle de l'entraide technique entre registres, dépend aujourd'hui d'un équilibre plus fragile qu'il n'y paraît.

La guerre en Ukraine a conduit, par exemple, à la suspension du registre russe (.ru) du fait de sa dépendance directe au ministère de l'Information du gouvernement russe. Ce n'est pas une exclusion, mais une mise à l'écart effective pour un temps indéfini. Le registre ne participe plus aux réunions, ne bénéficie plus des échanges ni de l'accès aux travaux. La suspension, décidée collectivement, vise à préserver les conditions de coopération technique. Elle traduit une ligne que le CENTR s'efforce de maintenir : ne pas faire de politique, mais ne pas feindre la neutralité quand la confiance n'est plus tenable.

Les tensions sont parfois moins visibles, mais tout aussi structurantes. Elles tiennent à la diversité des membres — de leur taille, de leur modèle économique, de leur rapport à l'État. Certains registres sont intégrés à l'administration, d'autres sont privés, d'autres encore dépendent d'universités ou d'agences parapubliques. Cela crée des asymétries importantes dans leur capacité à s'exprimer publiquement, à s'engager dans les débats réglementaires ou à contribuer à des documents de prise de position. Le CENTR n'impose aucune ligne commune. Il offre des espaces où ceux qui le souhaitent peuvent construire un discours collectif. Mais la cohérence a un prix : les *Position Papers*, notamment, ne peuvent être publiés qu'à l'unanimité, ce qui limite naturellement leur fréquence et leur portée.

Une autre ligne de tension est apparue plus récemment, avec la diversification des activités de certains registres de ccTLD européens. Le développement de services à l'international, l'ouverture à des extensions génériques ou encore la création de structures commerciales distinctes, comme l'alliance commerciale créée entre les registres canadien et néerlandais pour proposer une solution technique de registre qui rentre en concurrence avec la solution commercialisée par l'Afnic (ARS)[1], introduisent des éléments de concurrence partielle entre membres. Cela ne remet pas en cause les principes fondateurs du CENTR, mais cela oblige à clarifier ce qui relève du partage et ce qui, désormais, ne peut plus l'être de façon systématique.

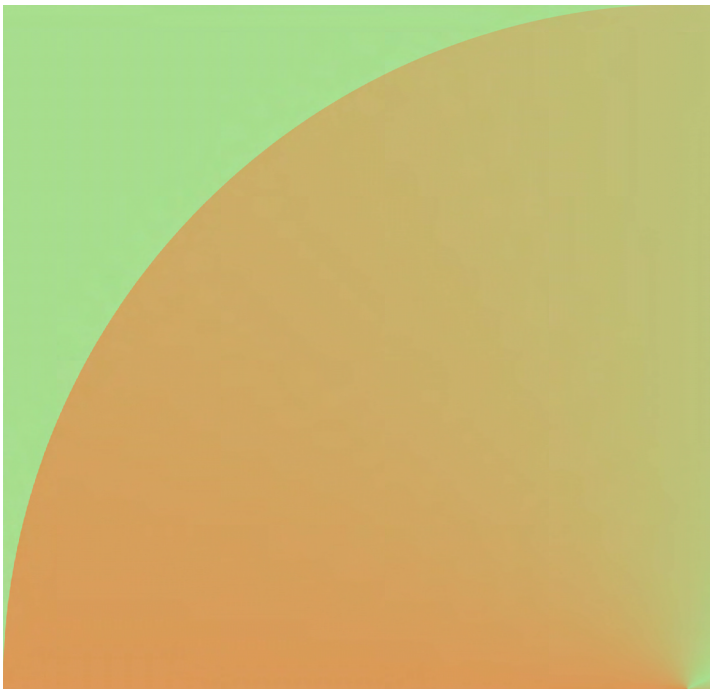
Enfin, les pressions externes, notamment réglementaires, s'intensifient. Le cadre juridique européen évolue vite — NIS 2, CRA, eIDAS 2, RGPD, DNS4EU — avec des implications directes pour les ccTLD. Le CENTR est de plus en plus souvent sollicité par les institutions européennes, parfois dans des délais très courts. Ce dialogue est précieux, mais il oblige l'organisation à structurer sa capacité de réponse sans se substituer aux registres nationaux. L'équilibre est subtil : être audible sans parler au nom des autres, être utile sans être prescripteur.

Ce qui se joue ici, c'est la capacité d'un réseau volontaire à tenir ensemble, dans un contexte fragmenté. Le CENTR ne dispose d'aucun pouvoir contraignant sur ses membres : son autorité repose entièrement sur l'utilité qu'il apporte et sur la confiance que lui accordent ceux qui y participent. À ce titre, il peut difficilement aller plus vite que les membres qu'il réunit, ni se substituer aux rapports bilatéraux qu'ils entretiennent avec leurs propres autorités. Mais il joue un rôle de stabilisateur discret, dont l'utilité devient plus évidente à mesure que l'environnement se tend.

Une coopération ancrée dans le temps long, tournée vers l'avenir

L'histoire du CENTR n'est pas celle d'une montée en puissance spectaculaire. C'est celle d'une organisation technique qui a su, avec méthode et sobriété, faire évoluer ses missions au rythme des besoins de ses membres. D'abord lieu de partage, puis plateforme de formation et de sensibilisation, il est devenu un acteur d'accompagnement, écouté sans être politique, consulté sans être mandaté.

Sa solidité repose sur des choix clairs : rester ancré dans la technique, favoriser la transparence, préserver l'autonomie. Dans un monde où les tensions géopolitiques s'intensifient et où les exigences réglementaires se complexifient, cette posture lui permet de continuer à remplir sa mission : faire vivre une coopération concrète entre registres, dans l'intérêt d'un internet européen stable, résilient et souverain sur le plan technique.



1. https://www.afnic.fr/produits-services/solutions-de-registre/afnic-registry-services/

Retour sur le CENTR Jamboree 2025 à Lyon

Du 21 au 23 mai 2025, l'Afnic a accueilli à Lyon l'édition 2025 du CENTR Jamboree, qui a réuni plus de 260 participants — un record pour cet événement centré sur le partage d'expériences opérationnelles entre équipes des registres. La quasi-totalité des ccTLD européens y étaient représentés et ce sont avant tout les profils techniques, marketing/commerciaux et juridiques qui ont composé leurs délégations.

Des échanges centrés sur les réalités du terrain

Premier axe fort des discussions : la lutte contre les abus liés au DNS. Les échanges ont notamment reflété la diversité des approches dans la mise en œuvre de la directive NIS2, en fonction de la maturité de la culture de l'identité électronique du pays, de la taille des registres et de leur pouvoir de négociation avec les bureaux d'enregistrement. Les discussions sur les méthodes de détection des enregistrements problématiques ont également révélé que presque tous les registres européens s'appuient sur des tiers pour identifier les contenus abusifs. Ces deux dimensions — réglementaire et technique — montrent que la lutte contre les abus implique non seulement des obligations à respecter mais aussi des moyens concrets pour y répondre.

Le projet TLD ISAC (*Top-Level Domain Information Sharing and Analysis Centre*) a également été mis sur le devant de la scène. Officiellement lancé en 2023 sous l'égide du CENTR, ce groupe de travail spécialisé vise à renforcer la cybersécurité des registres de domaines de premier niveau en Europe, en facilitant l'échange d'informations sur les menaces, l'analyse des risques et le développement de mesures proactives. Actuellement, le TLD ISAC est principalement composé de membres du CENTR. Cependant, la question de son élargissement à d'autres types de TLD, tels que les gTLD, a été soulevée lors du Jamboree de Lyon. Cette ouverture favoriserait une collaboration plus large pour une meilleure résilience.

L'évolution du marché des noms de domaine a aussi été abordée, les statistiques confirmant une forme de ralentissement — car si la création de noms de domaine reste dynamique, le nombre de suppressions progresse nettement. Certaines extensions, parmi lesquelles le .com, perdent même du stock. Plusieurs facteurs ont été évoqués, sans pouvoir expliquer à eux seuls la tendance : une économie morose qui voit la baisse des créations et l'augmentation des défaillances d'entreprises, mais aussi un possible désengagement des grandes marques sur les stratégies d'enregistrement défensif — la confiance qu'elles accordent au renforcement des mécanismes de lutte contre les abus des registres réduisant leur besoin de précaution. Face à cette érosion du stock, il est probable que certains registres envisagent des hausses tarifaires pour préserver leur capacité d'investissement, notamment en cybersécurité.

Enfin, l'intelligence artificielle s'est invitée dans les débats. Un consensus s'est rapidement dégagé sur l'intérêt de l'IA pour anticiper les usages malveillants et lutter contre les abus, en repérant des schémas d'enregistrement inhabituels, en analysant le comportement des résolveurs DNS ou encore en croisant des signaux faibles issus de données RDAP/Whois ou de serveurs de noms. Beaucoup de registres s'interrogent toutefois sur l'usage d'IA publiques, pratiques mais hors de contrôle en termes de confidentialité des données ; alors que développer sa propre IA offrirait davantage de maîtrise et de garanties, mais nécessiterait des ressources humaines et financières dont les registres ne disposent pas. La question est donc moins « est-ce utile ? » que « dans quelles conditions, avec quelles données et à quel coût ? ».

Le développement durable, grand absent des échanges

À noter que les questions de développement durable dans l'écosystème DNS n'ont été que peu, voire pas du tout évoquées. C'est un regret pour l'Afnic, en tant qu'hôte de l'événement, qui aurait souhaité voir ces enjeux mis à l'agenda. Mais les thématiques du Jamboree sont issues d'un appel à propositions adressé aux participants et, cette année, les soumissions ont convergé vers les autres priorités évoquées ci-dessus. Cela reflète certes les préoccupations actuelles des équipes des ccTLD européens, mais souligne aussi combien il reste difficile, pour les équipes en première ligne, d'inscrire des objectifs sociétaux dans des feuilles de route déjà largement captées par les exigences réglementaires et opérationnelles.

2

Cryptographie post-quantique : préparer l'infrastructure internet à une transition technique inévitable

L'informatique quantique n'est pas encore une réalité industrielle, mais elle ne relève plus du domaine de la science-fiction. De nombreux États et entreprises privées y investissent massivement. Cette course à la technologie, encore très expérimentale dans ses applications concrètes, a toutefois une conséquence bien réelle : elle oblige à repenser dès aujourd'hui certaines fondations techniques d'internet.

L'informatique quantique ne remet pas en cause l'ensemble des communications sur internet, mais cible spécifiquement les mécanismes cryptographiques. Ce sont principalement les systèmes de chiffrement et de signature asymétriques — utilisés pour établir des connexions sécurisées, gérer des certificats ou authentifier des échanges — qui sont concernés. En volume, cela ne représente qu'une partie des échanges. Mais c'est cette partie qui assure la confidentialité, l'intégrité et la confiance dans les services numériques les plus sensibles.

La principale menace porte donc sur la cryptographie. Les systèmes actuels de chiffrement et de signature pourraient être rendus vulnérables par la puissance de calcul des futurs ordinateurs quantiques. En réaction, un chantier international s'est ouvert autour de la « cryptographie post-quantique » : il s'agit d'identifier, normaliser et préparer des algorithmes capables de résister à cette nouvelle donne.

Mais si la transition est engagée dans les laboratoires et les instances de normalisation, elle est encore largement absente des infrastructures en production. Le sujet est pourtant loin d'être secondaire. Pour des acteurs comme les registres, les fournisseurs d'accès ou les opérateurs de services, cette mutation soulève des défis concrets en matière de performance, d'interopérabilité, d'architecture, voire de gouvernance technique.

Ce que l'on sait et ce que l'on ne sait pas de la « menace » quantique

L'existence d'une menace cryptographique liée à l'informatique quantique ne fait plus débat. De nombreuses démonstrations théoriques, dont l'algorithme de Shor[2], ont montré qu'un ordinateur quantique suffisamment puissant permettrait de casser des systèmes de chiffrement aujourd'hui considérés comme sûrs, tels que RSA (du nom de ses inventeurs *Rivest–Shamir–Adlema*n, basé sur la difficulté de factoriser de grands nombres premiers) ou ECC (*Elliptic Curve Cryptography*, fondée sur des équations de courbes elliptiques). Cela concernerait directement la majorité des mécanismes de sécurité utilisés sur internet, qui assurent l'authenticité, l'intégrité et la confidentialité de nombreuses communications, que ce soit dans le cadre du protocole TLS, des signatures DNSSEC, des tunnels SSH, des certificats numériques ou des échanges d'e-mails sécurisés.

Ce que l'on ne sait pas encore, en revanche, c'est quand une telle machine existera. Les estimations varient selon les sources, les méthodologies et les intérêts. Certaines prévisions parlent d'une décennie, d'autres d'un horizon plus lointain. Il est également possible que le premier acteur capable de faire fonctionner un ordinateur quantique suffisamment avancé pour menacer la cryptographie actuelle choisisse de ne pas le rendre public immédiatement, voire de l'exploiter en toute confidentialité à des fins stratégiques ou malveillantes. La prudence impose donc de raisonner non pas en termes de probabilité, mais de conséquences.

Car même si ces machines n'existent pas encore, les enjeux qu'elles soulèvent peuvent dès aujourd'hui poser problème. Des échanges chiffrés peuvent être interceptés, stockés, puis déchiffrés ultérieurement, lorsque la puissance de calcul nécessaire sera disponible. Ce scénario, désormais bien identifié, justifie à lui seul une anticipation sérieuse.

Des standards en cours de définition, une mise en œuvre encore lointaine

La réponse à la menace posée par l'informatique quantique ne repose pas sur un algorithme miracle, mais sur un processus long, collectif et itératif. Depuis 2016, le NIST (*National Institute of Standards and Technology*) pilote ainsi un programme international visant à sélectionner des algorithmes dits « post-quantiques », c'est-à-dire capables de résister aux attaques permises par un ordinateur quantique, tout en restant compatibles avec les architectures actuelles.

Lors du lancement de cette initiative, certains observateurs s'attendaient à des résultats rapides. Mais les cycles de la cryptographie sont longs, prudents et passent par plusieurs phases d'analyse, d'expérimentation et de validation. En 2022, après six années d'évaluation, le NIST a annoncé la sélection de quatre algorithmes en vue de leur standardisation : un pour l'échange de clés (CRYSTALS-Kyber) et trois pour la signature numérique (CRYSTALS-Dilithium, Falcon, SPHINCS+). D'autres candidats restent en cours d'étude, notamment pour diversifier les approches mathématiques et mieux couvrir des cas d'usage spécifiques.

Ces algorithmes ne sont pas encore intégrés dans les infrastructures en production, loin de là. Leur spécification mathématique n'est qu'une première étape. Il faut encore évaluer leur robustesse dans des conditions réelles, vérifier leur compatibilité avec les protocoles existants et les intégrer dans les bibliothèques cryptographiques de référence — ces composants logiciels (comme OpenSSL ou BoringSSL) qui assurent, en pratique, la mise en œuvre du chiffrement, des signatures et des échanges de clés dans la majorité des services numériques. La prudence reste donc de mise : la sélection d'un algorithme ne garantit ni sa fiabilité opérationnelle, ni sa sécurité une fois déployé.

C'est précisément cette phase d'intégration que traitent aujourd'hui plusieurs groupes de travail de l'IETF, qui examinent les adaptations nécessaires dans des protocoles comme TLS, SSH, IPsec ou DNSSEC. Les discussions sont encore toutefois à un stade préliminaire. Les travaux les plus avancés portent en effet sur la terminologie, avec une première RFC attendue prochainement[3]. D'autres groupes explorent parallèlement des pistes plus concrètes, telles que des approches hybrides combinant un algorithme classique et un algorithme post-quantique dans un même échange, afin de garantir une transition sans perte de sécurité[4] ; ou la mise à jour du protocole IKEv2 pour supporter la cryptographie post-quantique[5].

2. Publié dès 1994 par Peter Shor, l'algorithme de Shor permet, en théorie, de factoriser de grands entiers et de calculer des logarithmes discrets très rapidement sur un ordinateur quantique. Il serait ainsi capable de casser les bases mathématiques de nombreux systèmes cryptographiques actuels, notamment RSA et ECC. Pour aller plus loin : https://interstices.info/lalgorithme-quantique-de-shor/
3. *Terminology for Post-Quantum Traditional Hybrid Schemes*, draft du groupe de travail PQUIP (*Post-Quantum Use In Protocols*), en attente de publication (*RFC Editor Queue*) : https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/
4. *Hybrid key exchange in TLS 1.3*, draft du groupe de travail TLS (*Transport Layer Security*) : https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design
5. *Post-quantum Hybrid Key Exchange with ML-KEM in IKEv2*, draft du groupe de travail IPSECME (*IP Security Maintenance and Extensions*) : https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-mlkem/

Un autre draft encore, destiné aux ingénieurs, prend un peu plus de hauteur sur l'ensemble de ces enjeux, en proposant une synthèse pédagogique des implications techniques de la cryptographie post-quantique dans les protocoles internet[6].

Un défi d'infrastructure, de coordination… et de temps

Si les travaux théoriques et normatifs progressent, leur mise en œuvre future soulève des enjeux très concrets pour l'infrastructure actuelle de l'internet. À la différence d'une simple mise à jour logicielle, l'adoption d'algorithmes post-quantiques affecte des couches profondes du réseau : serveurs DNS, systèmes de gestion de certificats, équipements réseau, protocoles d'interconnexion, etc.

Cette transition est d'autant plus complexe qu'elle concerne un écosystème distribué, hétérogène et composé d'acteurs multiples : éditeurs, opérateurs, fournisseurs de services, gestionnaires d'infrastructure, autorités de certification, registres, etc. Aucun acteur n'a la capacité d'imposer à lui seul un basculement global. La coordination, les tests d'interopérabilité et le déploiement progressif devront donc se faire dans un cadre souple mais structuré, avec des références communes.

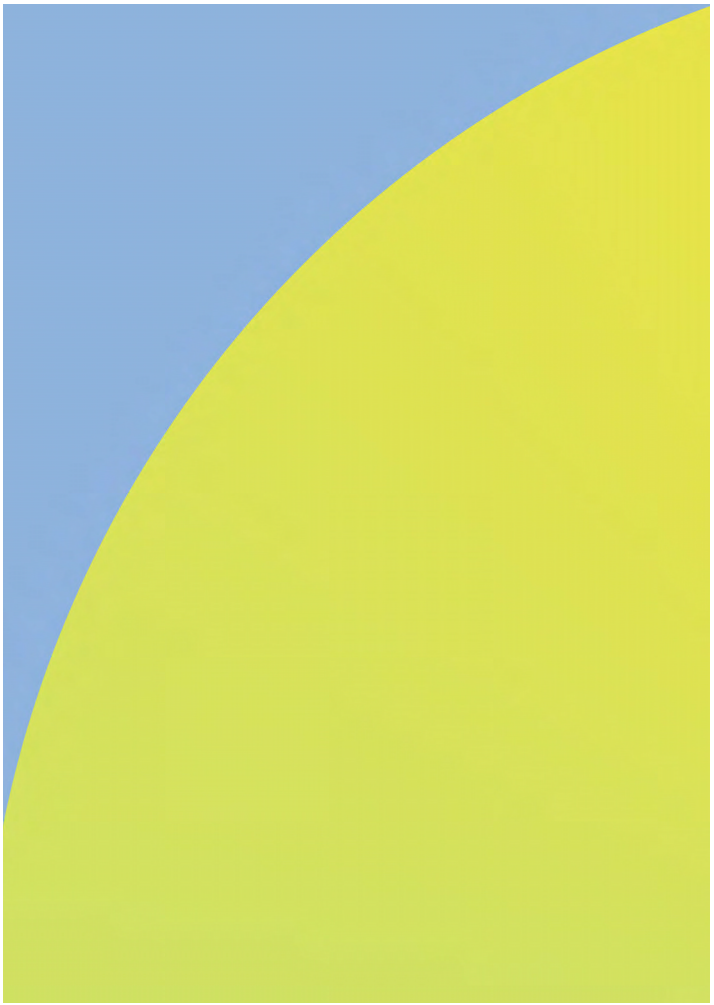
Le DNS, en particulier, illustre bien ces difficultés. Le mécanisme DNSSEC permet de signer les zones pour garantir l'authenticité des réponses. Ces signatures sont aujourd'hui générées par des machines spécifiques, souvent protégées par des modules matériels de sécurité et stockées dans des formats optimisés pour limiter leur taille. L'introduction d'algorithmes post-quantiques, dont les clés et les signatures seront significativement plus volumineuses, modifie ces équilibres. Pour l'ensemble des registres et opérateurs de zones DNS signées, cela signifie des zones plus lourdes, des temps de traitement plus longs et un impact sensible sur le volume de données échangées avec les résolveurs.

Enfin, même si l'ordinateur quantique capable de casser la cryptographie actuelle n'existe pas encore, la complexité de la transition ne laisse pas de place à l'attentisme. Adapter les infrastructures, revoir les chaînes de confiance, mettre à jour les logiciels, tester les interopérabilités : cela ne se résume pas à activer une option ou remplacer quelques lignes de code. Ce sont des évolutions lentes, parfois coûteuses, qui impliquent une coordination entre de nombreux acteurs et une planification rigoureuse. L'expérience du passage à IPv6 ou du déploiement de DNSSEC montre à quel point ces changements, même consensuels, peuvent s'étendre sur plus d'une décennie.

Anticiper collectivement une transition inévitable

L'informatique quantique ne menace pas internet dans son ensemble, mais compromet directement la confidentialité, l'intégrité et la confiance dans les échanges assurés par les mécanismes cryptographiques déployés. Ce risque, bien que toujours théorique, est pris au sérieux par l'ensemble de la communauté technique. Non pas parce que la menace est imminente, mais parce que les réponses techniques, toujours en développement, nécessiteront ensuite encore du temps pour être déployées.

La cryptographie post-quantique ne pourra pas être adoptée en quelques mois, ni même en quelques années. Elle implique des évolutions techniques et organisationnelles longues à mettre en œuvre et qui ne pourront réussir qu'à l'échelle collective. Elle suppose une transformation profonde des standards, des outils et des pratiques, ainsi qu'une coordination entre de nombreux acteurs. Et c'est le décalage entre une menace encore peu visible et une transformation technique déjà nécessaire qui en fait un sujet complexe et stratégique.



6. *Post-Quantum Cryptography for Engineers*, draft du groupe de travail PQUIP (*Post-Quantum Use In Protocols*) : https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/

03

Le SSAC enquête sur la place des logiciels libres dans l'infrastructure DNS

Le SSAC (*Security and Stability Advisory Committee*), l'organe de conseil technique de l'ICANN (*Internet Corporation for Assigned Names and Numbers*) spécialisé dans la sécurité et la stabilité du système des noms de domaine, vient de clore une importante phase de collecte d'informations sur l'utilisation des logiciels libres et open source dans l'infrastructure du DNS et des services d'enregistrement de noms de domaine. Une analyse est en cours, dont les résultats seront rendus publics cette année.

L'objectif de cette initiative, qui avait été présentée l'année dernière lors de l'ICANN80 à Kigali au Rwanda, est simple : comprendre où, comment et à quelle échelle les logiciels libres structurent l'écosystème DNS. Et surtout, en mesurer les conséquences en termes de stabilité, de sécurité et de responsabilité juridique dans un contexte de régulation de plus en plus dense.

Pourquoi cette étude ?

Les infrastructures critiques de l'internet, à commencer par le DNS, dépendent largement de logiciels open source. Si ce constat est largement partagé et admis par la communauté technique, il reste encore peu documenté. Avec son enquête, le SSAC entend ainsi dresser pour la première fois un état des lieux objectif et chiffré de l'utilisation de logiciels libres dans l'écosystème DNS.

Le sujet a notamment été motivé par l'adoption du *Cyber Resilience Act* (CRA) en Europe, qui pose la question de la responsabilité des composants logiciels dans les chaînes critiques. L'idée n'est pas de remettre en cause l'open source, mais d'en comprendre les dépendances réelles et les risques induits, afin de guider les décideurs publics dans un cadre de régulation plus informé.

Une enquête internationale pour cartographier l'usage du logiciel libre dans l'écosystème DNS

Pour y parvenir, le SSAC a mené une consultation internationale de six mois, aujourd'hui close, sous la forme d'un questionnaire adressé aux opérateurs DNS, registres, bureaux d'enregistrement, fournisseurs de services DNS, communautés de développeurs et toute autre organisation utilisant ou déployant de l'open source dans les couches critiques du DNS.

L'analyse des données, actuellement en cours, devrait permettre d'identifier les logiciels open source utilisés dans des fonctions telles que les serveurs faisant autorité (y compris racine et TLD), les résolveurs DNS, les logiciels d'enregistrement de noms, les interfaces Whois/RDAP, les outils de signature DNSSEC, ou encore les services de supervision, de monitoring et d'analyse DNS.
Le questionnaire portait également sur les politiques de mise à jour, les pratiques de gestion des vulnérabilités, le soutien financier ou communautaire aux projets utilisés, ainsi que les difficultés rencontrées pour s'adapter à de nouvelles obligations réglementaires.

Le DNS repose largement sur l'open source, mais sur qui reposent les logiciels libres ?

Les résultats devraient confirmer ce que beaucoup dans la communauté technique pressentent : une large majorité de l'infrastructure DNS s'appuie sur des logiciels libres, choisis pour leur efficacité, leur interopérabilité, leur transparence, mais parfois maintenus par des équipes très réduites, voire bénévoles.

C'est là que le risque s'installe : un projet critique, faiblement maintenu, peut devenir un point de défaillance majeur si une vulnérabilité est exploitée ou si le projet cesse brutalement. Le CRA se concentrant sur les responsabilités respectives des acteurs concernés, il a la vertu de mettre à jour d'éventuelles faiblesses dues au nombre parfois restreint de développeurs affectés à tel ou tel projet, et à la faible surface financière des organisations qui les portent. Ainsi, en provoquant l'enquête du SSAC, le CRA nous semble être une opportunité pour les acteurs opérant des infrastructures et services critiques de l'internet d'identifier les logiciels et les projets qu'il convient de mieux soutenir, à la fois en termes de compétences mises à disposition, ou encore de contribution budgétaire.

Informer les régulateurs pour nourrir leurs réflexions en amont

Pour le SSAC, il est essentiel que les régulateurs comprennent la nature distribuée et communautaire de l'open source dans l'infrastructure DNS. Les modèles de responsabilité classiques ne s'appliquent pas bien à ces logiciels. Les développeurs ne sont pas des fournisseurs, les licences excluent toute garantie, et pourtant les utilisateurs en tirent des bénéfices. Ce serait donc dans ce cas aux utilisateurs de ces logiciels d'assumer la responsabilité juridique d'éventuelles défaillances, dès lors qu'ils ne se donneraient pas les moyens ou ne donneraient pas les moyens à ces « éditeurs » de maintenir convenablement les logiciels en question.

L'étude du SSAC veut fournir une base factuelle pour penser des mécanismes de responsabilité partagée. L'enjeu est d'éviter que des mesures bien intentionnées ne provoquent des effets contre-productifs : retrait de certains projets, renoncement à la mise à disposition de code libre, affaiblissement de la diversité et de la qualité logicielles via moins de contributions.

Protéger ce qui fait tourner l'internet

À travers cette enquête, dont les conclusions devraient être dévoilées lors de l'ICANN84 qui se tiendra du 25 au 30 octobre 2025 à Dublin, le SSAC souhaite mettre en lumière une réalité technique encore trop peu visible : l'internet d'aujourd'hui, dans ses fondations mêmes, repose sur des logiciels libres souvent fragiles, parfois sous-financés, mais toujours essentiels. À l'heure où les régulations s'intensifient, il devient urgent de repenser les modèles de responsabilité, non pour freiner l'innovation ouverte, mais pour la protéger. Il ne s'agit pas seulement de cartographier les usages, mais d'initier un dialogue lucide entre développeurs, opérateurs et régulateurs. Car garantir la stabilité et la sécurité du DNS, c'est aussi garantir un avenir durable à l'open source dans l'infrastructure d'internet.

04

DINRG : un groupe de recherche engagé pour la décentralisation d'internet

Internet connaît depuis plusieurs années un mouvement de centralisation sans précédent. Quelques grandes plateformes dominantes concentrent l'essentiel du trafic et des données, tandis que des fournisseurs cloud et réseaux de distribution de contenu centralisent de plus en plus l'infrastructure du réseau. Face à ces phénomènes de consolidation d'internet, la communauté technique a réagi en créant un espace dédié à l'analyse et à la contre-mesure de cette centralisation galopante. C'est ainsi qu'a vu le jour en 2017 le DINRG (*Decentralization of the Internet Research Group*) au sein de l'IRTF (*Internet Research Task Force*), l'organe de recherche de l'IETF (*Internet Engineering Task Force*). Ce groupe de recherche a pour mission d'étudier en profondeur les causes et effets de la centralisation de l'internet et d'explorer des pistes techniques pour en renforcer la décentralisation.

Aux origines du DINRG : comprendre la centralisation de l'internet

Depuis une dizaine d'années, l'écosystème internet est marqué par une concentration croissante des applications, des services en ligne et même de certaines infrastructures. Quelques grandes plateformes et fournisseurs captent une part toujours plus importante du trafic et des données, menaçant le caractère ouvert et distribué du réseau. Cette centralisation — c'est-à-dire la situation où une entité unique ou un petit groupe contrôle ou surveille un élément clé de l'internet — soulève des enjeux majeurs en termes d'innovation, de concurrence, de résilience et de liberté d'expression. Elle va à l'encontre de la nature originelle de l'internet conçu comme un « réseau de réseaux » sans monopole ou position dominante.

C'est dans ce contexte qu'a été fondé le DINRG. Ce groupe de recherche fait partie de l'IRTF — le pendant orienté recherche de l'IETF, l'organisme international de standardisation de l'internet. Le DINRG offre un forum ouvert à la communauté ingénierie et recherche pour discuter du phénomène de centralisation d'internet et des menaces associées, et coordonner les efforts visant à en identifier les causes et proposer des solutions. Autrement dit, sa mission est à la fois analytique et prospective : comprendre pourquoi et comment l'internet se centralise, et explorer comment le décentraliser de nouveau.

Une mission alliant technique, économie et régulation

Le DINRG aborde la centralisation de l'internet comme un sujet multidimensionnel en prenant en compte ses implications techniques, économiques et politiques. Parmi ses objectifs figurent l'investigation des causes profondes de la centralisation – qu'elles relèvent des protocoles, des choix de conception techniques, des dynamiques de marché ou encore de régulations et réglementations. Le groupe s'attache également à mesurer la centralisation de l'internet et ses impacts sociétaux, ainsi qu'à identifier les différentes formes que prend ce mouvement de consolidation. Un travail important de définition est mené afin d'établir une terminologie commune autour de la (dé)centralisation, tant il est vrai que ces notions recouvrent des réalités multiples (techniques, économiques, géographiques, etc.).

Fort de ce diagnostic, le DINRG explore des pistes de solutions pour favoriser la décentralisation de l'internet. Ces solutions peuvent être techniques (nouvelles architectures, protocoles alternatifs, outils favorisant l'interopérabilité et la distribution des services) ou politiques (incitations réglementaires, bonnes pratiques de gouvernance, cadres juridiques adaptés). Le groupe ne s'enferme pas dans une approche unique : il se veut une plateforme ouverte à différentes technologies, sans parti-pris pour l'une ou l'autre. L'objectif est de mieux cerner le pour et le contre de chaque approche : quelles promesses offrent-elles réellement ? Quels sont leurs contraintes ou effets de bord ?

Surtout, le DINRG garde à l'esprit que la centralisation est un phénomène complexe qu'aucune solution miracle ne viendra résoudre à elle seule. Les premiers travaux du groupe ont mis en évidence que la centralisation d'internet n'est pas uniquement imputable à la technologie. Ce sont avant tout les dynamiques économiques qui poussent à la concentration, la technique et la régulation n'ayant pas toujours permis d'en limiter les effets. En d'autres termes, même les meilleurs protocoles ne suffiront pas si le contexte économique incite à la concentration, ou si des menaces comme des cyberattaques encouragent le regroupement des ressources pour y faire face.

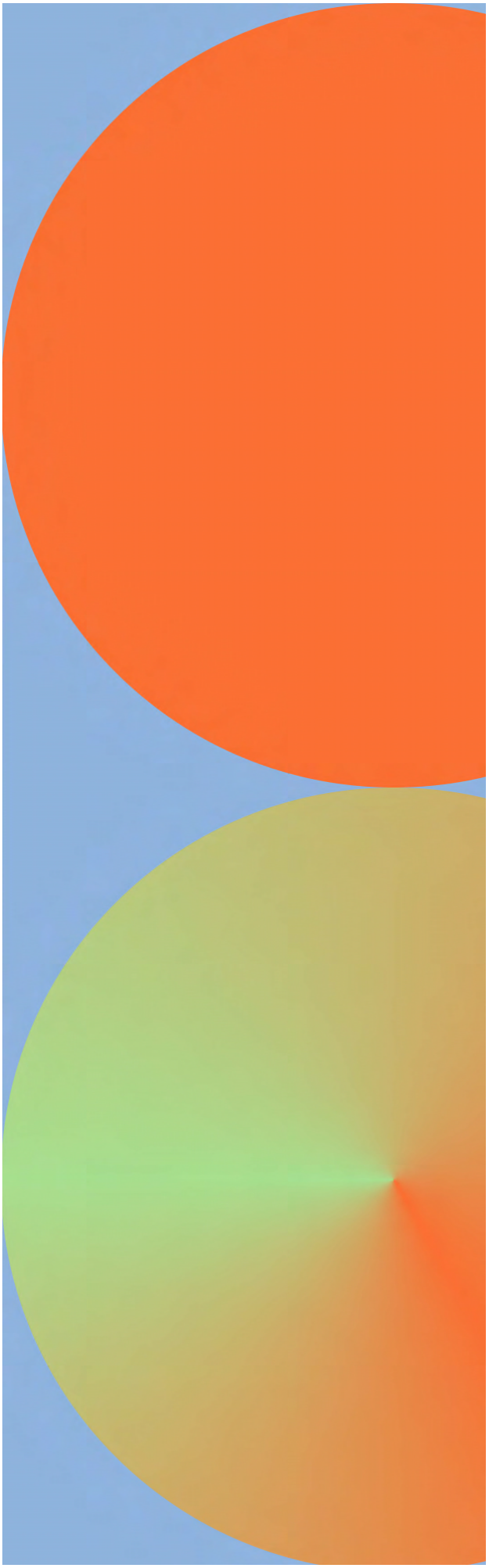
C'est cette analyse réaliste qui a conduit le DINRG à prôner une approche holistique : conjuguer avancées techniques et évolutions réglementaires pour renverser le déséquilibre actuel. Les régulateurs ont un rôle décisif à jouer pour restaurer un marché plus réparti, et la communauté technique a la responsabilité de les éclairer sur ce qu'il convient de faire et comment. Le DINRG se positionne précisément comme un lieu d'élaboration d'une telle vision équilibrée.

Un fonctionnement ouvert et interdisciplinaire

En tant que groupe de recherche de l'IRTF, le DINRG fonctionne de manière ouverte et collaborative, sur le modèle des groupes de travail de l'IETF. Toute personne intéressée — que sa spécialité soit l'ingénierie réseau ou la recherche, qu'elle soit juriste, économiste ou décideur public — peut suivre les travaux du groupe et y contribuer.

Le groupe se réunit lors des grandes conférences IETF (en principe au moins une fois par an en marge des trois rencontres annuelles de l'IETF) et organise au besoin des réunions additionnelles, ateliers ou panels thématiques. Ces événements permettent d'approfondir certaines questions avec une diversité d'intervenants, selon les sujets : chercheurs en réseaux, experts en droit et politiques du numérique, militants des droits numériques. Ce dialogue interdisciplinaire est encouragé par le DINRG, convaincu que les problèmes de centralisation doivent être abordés sous toutes leurs facettes. Le groupe prévoit d'ailleurs explicitement d'impliquer des communautés non techniques — autorités de régulation, chercheurs en sciences économiques et sociales — et d'organiser des tables rondes élargies afin de croiser les points de vue.

En pratique, les réunions de DINRG alternent exposés de travaux de recherche, discussions ouvertes et élaboration de documents. Les sujets traités couvrent un large spectre : analyses d'architectures existantes, études de cas concrets, présentations de nouvelles idées de protocoles ou encore réflexions sur l'impact de telle ou telle politique publique sur la décentralisation d'internet. Cette variété illustre le rôle de passerelle que joue le DINRG entre le monde technique et le monde de la gouvernance. Le groupe se situe à l'interface de communautés qui interagissent peu habituellement : il crée un espace où ingénieurs, universitaires et régulateurs peuvent échanger librement, confrontant les contraintes techniques aux exigences juridiques et économiques. Pour les autorités publiques, notamment en Europe, le DINRG offre ainsi une ressource précieuse pour alimenter la réflexion sur la gouvernance du numérique, et plus particulièrement d'internet : ses travaux fournissent des éléments concrets et une expertise neutre pour éclairer les décisions en matière de politique internet.



Des thèmes de travail illustrés par des exemples concrets

Même s'il relève de la recherche exploratoire, le DINRG aborde aussi des questions très concrètes, en prise avec l'actualité des technologies internet. Plusieurs exemples de thèmes étudiés par le groupe permettent de mieux saisir les défis de la décentralisation.

Le paradoxe IPFS. L'IPFS (*InterPlanetary File System*) est souvent mis en avant comme une solution de stockage de fichiers décentralisée, alternative aux plateformes cloud classiques. IPFS repose en effet sur un réseau pair-à-pair où les fichiers peuvent être distribués sur de multiples nœuds au lieu d'un serveur central.

En théorie, ce système élimine le besoin d'un stockage centralisé. En pratique, cependant, le DINRG a observé que l'écosystème IPFS tend vers une certaine centralisation. Une étude de 2023[7] a ainsi révélé que 5 % des nœuds IPFS les plus actifs servaient jusqu'à 95 % du trafic, et qu'un seul fournisseur cloud (Amazon Web Services) générait à lui seul 96 % des requêtes de résolution de contenu.

L'exemple d'IPFS illustre que même une architecture conçue pour être décentralisée peut, dans la pratique, se recentraliser. En cause : des mécanismes économiques classiques comme la concentration des acteurs ou la recherche d'efficacité.

Bluesky et les réseaux sociaux fédérés. Lancé en 2023, le réseau social Bluesky s'est présenté comme une alternative décentralisée à Twitter, fondée sur un protocole ouvert (*Authenticated Transfer Protocol* ou *AT Protocol*). L'une des innovations de Bluesky réside dans les identifiants décentralisés (*Decentralized IDentifier* ou DID) : chaque utilisateur possède une identité indépendante qui peut être déplacée d'un serveur à un autre, offrant une portabilité et évitant d'être lié à vie à un fournisseur.

Toutefois, là encore, la réalité technique impose des compromis. Le modèle de Bluesky n'est pas une fédération pure à la Mastodon ; il implique des nœuds « *relay* » chargés d'agréger et de distribuer les messages à l'échelle du réseau. Or, il s'avère que le déploiement de ces relais exige une puissance de stockage et de bande passante considérable. Selon la propre documentation technique de Bluesky, il est probable que seuls quelques grands nœuds relais assureront la majeure partie du trafic du réseau, aux côtés de nombreux autres relais plus petits couvrant des communautés spécifiques. En d'autres termes, l'architecture Bluesky, malgré sa promesse d'auto-souveraineté des identités, risque de reproduire une dépendance à une infrastructure centralisée (quelques opérateurs majeurs de relais). De fait, durant sa phase initiale, Bluesky n'a fonctionné qu'avec un serveur principal opéré par l'entreprise elle-même, limitant de facto la décentralisation. Fin 2024, la fédération complète commence à s'ouvrir avec la possibilité pour des tiers de déployer leur propre serveur Bluesky, mais il reste à voir si cela se traduira par une véritable distribution du pouvoir ou simplement par une centralisation élargie à un petit nombre de fournisseurs.

7. Balduf, S., Korczyński, M., Castro, I. et Tyson, G., IPFS in the Wild : A Measurement Perspective, IMC 2023 : https://mkorczynski.com/IMC2023Balduf.pdf

Ce cas souligne l'importance d'examiner concrètement les architectures : une solution annoncée comme « décentralisée » peut cacher des points de centralisation subtile, que ce soit au niveau technique (infrastructure indispensable) ou organisationnel (gouvernance par une entité dominante).

Le DNS, la décentralisation méconnue. À l'inverse, un exemple souvent cité par le DINRG comme une infrastructure déjà décentralisée est le bon vieux DNS (*Domain Name System*). Le DNS est la colonne vertébrale de l'internet pour la résolution des noms de domaine : il s'agit d'un annuaire mondial réparti en une hiérarchie (racine, domaines de premier niveau, domaines de second niveau, etc.) avec des serveurs gérés par une multitude d'acteurs à travers le monde.

En pratique, le DNS fonctionne de manière distribuée depuis plus de 35 ans : aucun serveur ni aucune organisation ne contrôle seul l'ensemble du système. Pourtant, cette décentralisation opérationnelle du DNS est souvent mal perçue ou sous-estimée. À l'heure où fleurissent des systèmes de nommage alternatifs basés sur la blockchain (tels que l'*Ethereum Name Service* pour les noms en « .eth »), beaucoup affirment que le DNS serait obsolète et trop centralisé.

Le DINRG apporte un contrepoint nuancé sur ce sujet. Dans une étude[8] présentée au sein du groupe, des chercheurs ont comparé la gouvernance et l'architecture du DNS avec celles de solutions blockchain comme ENS. Le constat est instructif : le DNS, bien qu'imparfait en la matière, offre déjà un haut degré de décentralisation du contrôle des noms (répartition des responsabilités entre l'ICANN, les registres, les bureaux d'enregistrement, les opérateurs DNS, etc.), là où les solutions blockchain comportent d'autres formes de centralisation (dépendance à un petit nombre de mineurs ou validateurs, nécessité de plateformes pour accéder aux registres, coûts d'utilisation élevés, etc.). Autrement dit, remplacer le DNS par une blockchain ne garantit pas une meilleure décentralisation ; dans certains cas, le remède pourrait même s'avérer moins soutenable ou plus coûteux que le système actuel. Ce qui manque au DNS, finalement, c'est davantage une perception publique de sa nature distribuée qu'une refonte totale.

Cette analyse nuancée illustre bien l'approche de DINRG : aller au-delà des idées reçues et examiner les faits pour guider les décideurs vers des choix éclairés, plutôt que de céder aux effets de mode technologiques.

Contributions et influence du DINRG : vers des standards plus ouverts

Depuis sa création, le DINRG a produit une série de documents et d'analyses qui contribuent à faire évoluer les mentalités au sein de la communauté internet. Si le groupe n'édicte pas directement de normes (ce rôle revient à l'IETF), il exerce une influence indirecte en alimentant les discussions stratégiques et en formulant des recommandations à l'attention des concepteurs de technologies internet.

Une contribution marquante en ce sens est la publication fin 2023 du RFC 9518[9], intitulé « *Centralization, Decentralization, and Internet Standards* ». Ce document, nourri de deux années de débats au sein de l'IETF (notamment au sein du DINRG), dresse un panorama des enjeux de centralisation et suggère ce que les organismes de standardisation technique peuvent — et ne peuvent pas — faire pour y remédier. Le RFC 9518 souligne que les standards ouverts sont nécessaires pour éviter la centralisation, mais qu'ils ne suffisent pas à eux seuls étant donné que de nombreux facteurs de centralisation échappent à la seule dimension technique.

En ce sens, il invite les ingénieurs et architectes à intégrer la préoccupation de la décentralisation dès la conception des protocoles (par exemple, éviter de créer des points de contrôle uniques, favoriser l'interopérabilité, permettre la portabilité des données…). Mais parallèlement, il tempère l'idée qu'une norme technique puisse à elle seule garantir un écosystème décentralisé si le contexte ne s'y prête pas. Ce réalisme est précieux : il évite de tomber dans l'utopie du « tout technique » et rappelle la nécessité d'actions complémentaires (régulation, vigilance des acteurs). Le document formule ainsi une série de questions et de pistes à l'intention des *protocol designers*. Notamment, il les incite à se demander, lors de tout nouveau design, « Qui aura le pouvoir sur cette fonction ? », ou encore « Pourrait-on, involontairement, créer une concentration ? ».

En outre, le RFC 9518 s'adresse non seulement aux techniciens mais aussi aux décideurs publics : il propose une grille de lecture pour identifier les abus liés à des architectures centralisées et évaluer les remèdes possibles. Ce type de passerelle entre le monde des standards et celui des politiques publiques est au cœur de la raison d'être du DINRG. En encourageant la rédaction et la diffusion de telles analyses, le groupe contribue à orienter l'écosystème vers davantage de décentralisation, de manière lucide et documentée.

Par ailleurs, le DINRG se montre vigilant face aux engouements technologiques rapides tels que la blockchain et le Web3. Il ne s'agit pas de rejeter ces innovations, mais de chercher plutôt à en évaluer objectivement les apports et les limites. Les analyses qui en résultent montrent que les solutions de décentralisation les plus en vogue peuvent se heurter à des obstacles concrets (performances, coûts, recentralisation indirecte) qui nécessitent une approche mesurée.

Le rôle du DINRG est ainsi d'apporter une voix équilibrée dans le débat : ni technophilie naïve, ni rejet systématique, mais une évaluation rigoureuse de chaque option. Cette capacité à produire une vision réaliste et nuancée de la décentralisation est sans doute l'une des valeurs ajoutées les plus importantes du groupe.

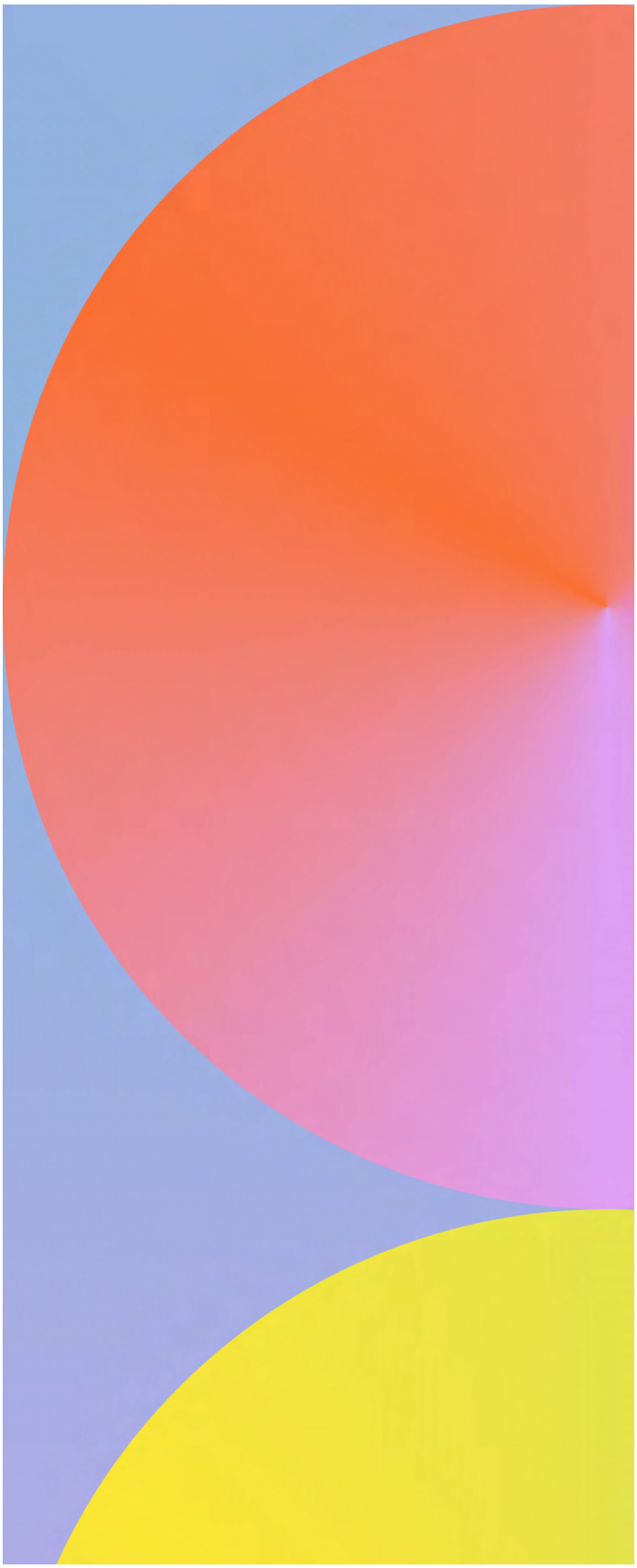
8. Yekta Kocaogullar, Eric Osterweil, Lixia Zhang, Towards a Decentralized Internet Namespace, atelier DIN@CoNEXT 2024 : https://dl.acm.org/doi/10.1145/3694809.3700746
9. https://datatracker.ietf.org/doc/html/rfc9518

Un pont entre technologie et gouvernance pour les décideurs publics

En quelques années, le DINRG s'est affirmé comme un lieu d'échange privilégié entre la sphère technique de l'internet et le monde des décideurs et régulateurs. Le groupe de recherche a conscience que la problématique de la centralisation touche à des questions de politique publique (concurrence, souveraineté numérique, protection des données, etc.) et que les solutions ne pourront émerger que d'une collaboration étroite entre toutes les parties prenantes. À cet égard, le DINRG se pose en interface pour faciliter cette collaboration. Il ouvre la communauté IETF/IRTF à des acteurs externes et, réciproquement, fait connaître au monde de la régulation les enjeux techniques souvent complexes qui sous-tendent la centralisation du réseau.

Concrètement, ce pont entre technique et politique s'illustre par les interactions régulières entre le DINRG et des organismes tels que l'IAB (*Internet Architecture Board*), qui a un pied dans la standardisation et un pied dans la réflexion stratégique, mais aussi par les passerelles créées lors des ateliers de travail avec les représentants d'autorités ou d'instances de gouvernance. Le discours porté par le DINRG commence également à résonner au-delà de la communauté IETF. On voit par exemple des références à ses travaux dans des discussions sur les réglementations du numérique, ou dans des forums traitant de la souveraineté technologique. Pour les décideurs publics européens, en particulier, qui cherchent des voies pour réguler les grandes plateformes tout en préservant l'innovation, les analyses du DINRG offrent un éclairage précieux. Elles permettent de distinguer, parmi les solutions avancées (interopérabilité obligatoire, promotion des logiciels ouverts, soutiens aux alternatives décentralisées, etc.), lesquelles sont techniquement réalistes et susceptibles d'avoir un impact positif.

En synthèse, le DINRG joue un rôle à la fois de vigie et d'éclaireur sur la question de la centralisation du réseau. En documentant les tendances de fond, en démontant certaines idées reçues et en proposant des recommandations concrètes, il aide à orienter l'écosystème internet vers un modèle plus équilibré. Son approche, qui marie expertise technique et compréhension fine des leviers économiques et réglementaires, en fait un interlocuteur de choix pour accompagner les pouvoirs publics dans la définition d'une vision stratégique du numérique. À l'heure où l'Europe s'interroge sur la régulation des « géants du Net » et la promotion d'un internet plus ouvert et diversifié, le DINRG apparaît comme une source d'informations et d'analyses à haute valeur ajoutée, susceptible d'alimenter une gouvernance du numérique éclairée et efficace.



Les prochains événements auxquels l'Afnic participe :

- **9 et 10 septembre**
UIT, Réunion des groupes de travail et d'experts du Conseil sur le SMSI
Genève, Suisse

- **12, 15 et 16 septembre 2025**
UIT, Réunion des groupes de travail et d'experts du Conseil sur Internet
Genève, Suisse

- **16 et 17 septembre 2025**
LoRa Alliance Technical Committee Meeting
Portsmouth, États-Unis

- **30 septembre au 3 octobre 2025**
CEPT Committee for ITU Policy
Athènes, Grèce

- **16 et 17 octobre 2025**
French-japanese conference on Internet Governance
Tokyo, Japon

- **20 au 24 octobre 2025**
RIPE 91
Bucarest, Roumanie

- **25 au 30 octobre 2025**
ICANN 84, réunion générale annuelle
Dublin, Irlande

- **1er au 7 novembre 2025**
IETF 124
Montréal, Canada

- **13 novembre 2025**
Forum français sur la gouvernance de l'Internet
Paris, France

- **14 novembre 2025**
JCSA
La Défense, France

- **17 au 28 novembre 2025**
Conférences mondiales de développement des télécommunications
Bakou, Azerbaïdjan

afnic
Internet made in France

Votre contact

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
7 avenue du 8 Mai 1845,
78280 Guyancourt