

SAC132

نظام اسم النطاق يعمل باستخدام البرمجيات المجانية المفتوحة المصدر (FOSS)

تقرير من اللجنة الاستشارية للأمن والاستقرار (SSAC) التابعة لمؤسسة ICANN  
25 سبتمبر/أيلول 2025

## تمهيد

هذا تقرير مقدم إلى كل من مجلس إدارة ICANN ومؤسسة ICANN ومجتمع ICANN، وعلى نطاق أوسع، إلى مجتمع الإنترنت من اللجنة الاستشارية للأمن والاستقرار (SSAC) التابعة لمؤسسة ICANN حول الطرق التي يعتمد بها نظام اسم النطاق (DNS) على البرامج المجانية مفتوحة المصدر (FOSS).

تركز اللجنة الاستشارية للأمن والاستقرار SSAC على المسائل المتعلقة بأمن وسلامة أنظمة تخصيص أسماء وعناوين الإنترنت. ويتضمن هذا المسائل المتعلقة بالتشغيل (مثل ما يتعلق بالتشغيل الصحيح والموثوق لنظام نشر منطقة الجذر)، ومسائل الإدارة الفنية (مثل ما يتعلق بتخصيص العناوين وتخصيص أرقام الإنترنت)، ومسائل التسجيل (مثل ما يتعلق بخدمات السجل وأمين السجل). تشترك اللجنة الاستشارية للأمن والاستقرار SSAC في نشاط متواصل لتقييم التهديدات وتحليل المخاطر التي تحيق بخدمات التسمية وتخصيص عناوين الإنترنت للوقوف على ممكن التهديدات الرئيسية التي يواجهها الاستقرار والأمن، وتقديم توصياتها إلى مجتمع ICANN طبقاً لذلك. ولا تتمتع اللجنة الاستشارية للأمن والاستقرار SSAC بسلطة تنظيم أو إنفاذ أو إصدار القرارات. فهذه الوظائف منوطة بجهات أخرى، ويجب تقييم المشورة المقدمة هنا بناءً على مزاياها. ويشارك أعضاء لجنة SSAC بصفتهم أفراد، وليس بصفتهم ممثلين للجهات التي يعملون لديها أو لمنظمات أخرى. يحصل توافق آراء اللجنة الاستشارية للأمن والاستقرار SSAC على وثيقة ما عندما يتفق محررو الوثيقة المدرجون على المحتوى والتوصيات بدون أي اعتراضات نهائية من بقية أعضاء SSAC، باستثناء أي انسحابات مدرجة في نهاية الوثيقة.

## قائمة المحتويات

2	تمهيد
3	قائمة المحتويات
4	قائمة المخططات
4	قائمة الجداول
5	ملخص تنفيذي
6	1 مقدمة
7	2 مقدمة DNS
10	2.1 التسلسل الهرمي لنظام DNS
11	2.2 تسجيل اسم النطاق ونشره
12	2.3 حل نظام DNS
13	3 نموذج البرمجيات المجانية مفتوحة المصدر FOSS: الخصائص الرئيسية والآثار
13	3.1 الأدوار الرئيسية في منظومة FOSS
14	3.2 المبادئ الأساسية لنموذج تطوير برمجيات FOSS
16	3.3 الأنظمة الاحتكارية تعتمد على برمجيات FOSS
16	3.4 نقاط القوة الكامنة في برمجيات FOSS في منظومة نظام اسم النطاق DNS
19	3.5 المخاطر الكامنة في نموذج برمجيات FOSS
24	4 انتشار برمجيات FOSS في البنية التحتية لنظام DNS وتسجيل أسماء النطاقات
24	4.1 برمجيات FOSS في البنية التحتية لتسجيل أسماء النطاقات
26	4.2 برمجيات FOSS في البنية التحتية لنشر نظام DNS (الخوازم الرسمية)
28	4.3 برمجيات FOSS في البنية التحتية لاسترجاع نظام DNS (المُحلّلات)
30	5 حالات معاصرة في ضوابط برمجيات FOSS
31	5.1 توزيع المسؤولية على أصحاب المصلحة الأكثر قدرة على العمل
31	5.2 تحفيز التعاون بين الصناعات المختلفة في مجال الصيانة المستدامة
32	5.3 تجنب متطلبات أمن سلسلة التوريد بافترض وجود برامج احتكارية
33	5.4 تجنب الأنظمة الإقليمية المتضاربة لمجتمعات برمجيات FOSS العالمية
33	6 النتائج الرئيسية
34	7 مبادئ توجيهية قابلة للتنفيذ لصانعي السياسات
35	8 الإقرارات والإفصاح عن المصالح والانسحابات
35	8.1 الشكر والعرفان
36	8.2 الإفصاح عن المصلحة
36	8.3 الانسحابات
37	الملحق أ: المصطلحات والمختصرات
37	أ.1 مسرد المصطلحات
38	أ.2 الاختصارات المستخدمة في هذا التقرير
39	الملحق ب: منهجية البحث في انتشار برمجيات FOSS ونتائجها
39	ب.1 النهج العام والتحديات
39	ب.2 البنية التحتية لتسجيل اسم النطاق
40	ب.3 البنية التحتية لنظام DNS
42	الملحق ج: استطلاع لوجهات نظر مشغلي نظام اسم DNS بشأن برمجيات FOSS وضوابط البرمجيات
43	ج.1 التعليقات المفتوحة (مخاوف محددة)

## قائمة المخططات

- المخطط 1: منظومة الإنترنت. كيث درازيك ..... 9
- المخطط 2: التسلسل الهرمي لنظام DNS ..... 10
- المخطط 3: مكونات URL واسم النطاق ..... 11
- المخطط 4: حل نظام DNS التقليدي ..... 12

## قائمة الجداول

- الجدول 1: أنظمة برمجيات FOSS المستخدمة في عمليات التسجيل ..... 25
- الجدول 2: أنظمة السجلات المبنية على مكونات برمجيات FOSS ..... 25
- الجدول 3: برمجية FOSS في وكلاء ضمان البيانات ..... 26
- الجدول 4: استخدام برمجيات FOSS في نظام خادم الجذر ..... 27
- الجدول 5: أنظمة برمجيات FOSS الشائعة الاستخدام لتطبيقات خادم نظام DNS ..... 29
- الجدول 6: أمثلة على خدمات نظام DNS التجارية التي تتضمن برمجيات FOSS ..... 30
- الجدول 7: مكتبات برمجيات FOSS المستخدمة في تطبيقات البنية التحتية لنظام DNS ..... 30
- الجدول 8: ملخص للمناهج التنظيمية المعاصرة لبرمجيات FOSS ..... 31

## ملخص تنفيذي

نظام اسم النطاق (DNS) هو نظام موزع عالميًا، وهرمي، وغير مركزي، حيث تشكل المعلومات التي يحتويها أساس كل تفاعل عبر الإنترنت تقريبًا. والهدف الأساسي منه هو ربط أسماء النطاقات سهلة الاستخدام بعناوين IP السهلة للكمبيوتر المطلوبة لتحديد الموارد على الشبكة. وسواء كنت تتصفح الويب أو ترسل بريدًا إلكترونيًا أو تستخدم تطبيقًا من تطبيقات الهاتف الجوال، فإن كل اتصال عبر الإنترنت يعتمد على المعلومات التي تنشأ من نظام اسم النطاق ويتم تنظيمها من خلاله.

النتيجة الأساسية لهذا التقرير هي أن نظام DNS مبني ومستدام على البرمجيات المجانية المفتوحة المصدر (FOSS). وهذه ليست ممارسة خاصة، بل هي الواقع السائد. فالبرامج المجانية مفتوحة المصدر FOSS هي المعيار للمكونات الأساسية للبنية التحتية لنظام اسم النطاق DNS. على سبيل المثال، تستخدم ما لا يقل عن تسعة من أصل 12 منظمة مستقلة تدير نظام خادم الجذر (RSS) للإنترنت حصريًا برمجيات FOSS، ويستخدم تسعة من أصل أكبر 10 موفري خدمات نطاقات المستوى الأعلى (TLD) برمجيات FOSS. وتتبع هذه الهيمنة من نقاط القوة المتأصلة في نموذج تطوير برمجيات FOSS، الذي يجمع بين الكفاءة الاقتصادية والتبني منخفض العوائق مع الشفافية والأمن التعاوني والمرونة التشغيلية الأساسية للبنية التحتية الحيوية.

وعلى الرغم من أن نموذج تطوير البرمجيات المجانية المفتوحة المصدر FOSS يختلف بشكل أساسي عن نموذج تطوير البرمجيات المملوكة، إلا أنها ليست بطبيعتها أكثر أو أقل أمانًا. ويتم تحديد أمان أي مشروع برمجي من خلال جودة عمليات التطوير والصيانة الخاصة به، وليس من خلال وضوحية كود المصدر الخاص به. وعلى عكس البرمجيات التجارية، فإن برمجيات FOSS هي جهد تعاوني عالمي مبني على أربع حريات أساسية: الاستخدام، والدراسة، والمشاركة، والتغيير. وتعتمد هذه المنظومة على شبكة عالمية من المسؤولين والمساهمين الذين غالبًا ما يكونون متطوعين يعملون بدون أجر. وفي الوقت الذي يكون فيه العديد منهم متطوعون بدون أجر، فإن فضاء نظام اسم النطاق فريد من نوعه لأنه يعتمد أيضًا على عدد قليل من منظمات الصيانة المخضمة. ويؤدي هذا إلى إنشاء نموذج يعتمد على التعاون المجتمعي بدلًا من العقود التجارية التي تحدد سلسلة توريد البرامج التقليدية، مما يؤدي إلى نشوء مخاطر فريدة تتعلق بالاستدامة المالية لمنظمات الصيانة وإرهاق المسؤول عن صيانتها للمتطوعين العاملين.

وتعني هذه الخصائص الفريدة أن الأطر التنظيمية المصممة للبرمجيات المملوكة قد لا تكون مناسبة للبرمجيات المجانية المفتوحة المصدر FOSS، وبالتالي قد يكون لها عواقب وخيمة غير مقصودة على استقرار البنية الأساسية الحيوية للإنترنت. وللتغلب على هذه التعقيدات وتعزيز منظومة رقمية آمنة، تقدم اللجنة الاستشارية للأمن والاستقرار (SSAC) المبادئ التوجيهية التالية لصناع السياسات:

- **الاعتراف بالدور الحاسم لبرمجيات FOSS:** يتعين على صناع السياسات أن يعترفوا صراحة في أي تشريع أو لائحة ذات صلة بأن البنية التحتية الحيوية للإنترنت تعتمد على البرمجيات المجانية المفتوحة المصدر FOSS، وأن استخدامها يشكل قوة يجب الحفاظ عليها.
- **التشاور مع مجتمع برمجيات FOSS:** ينبغي أن يتم وضع التشريعات واللوائح من خلال التشاور مع جميع أجزاء منظومة البرمجيات المجانية المفتوحة المصدر FOSS، من المسؤولين الأفراد إلى المنظمات غير الربحية والشركات.
- **الاستفادة من الحالات المعاصرة في تنظيم برمجيات FOSS:** يستطيع صناع السياسات الرجوع إلى دراسات الحالة الأخيرة في تقرير النهج المعاصرة التي تتضمن الخصائص الفريدة لنموذج تطوير البرمجيات المجانية المفتوحة المصدر FOSS.
- **تحفيز استدامة برمجيات FOSS:** تشجيع مساهمات القطاعين العام والخاص في مشاريع البرمجيات المجانية المفتوحة المصدر FOSS الهامة كشكل من أشكال الاستثمار في منفعة عامة مشتركة.
- **معالجة المخاطر النظامية بشكل جماعي:** تعزيز وتمويل الحلول التعاونية على مستوى المنظومة للتخفيف من المخاطر الناجمة عن التبعيات المشتركة بدلًا من إلقاء كاهل المسؤولين الأفراد.

## 1 مقدمة

يأتي هذا التقرير في ضوء المشاركة المتزايدة لصناع السياسات في جهود الصناعة الرامية إلى تقليل الثغرات الأمنية في البرمجيات في البنية التحتية الرقمية. وبينما تسعى الحكومات والهيئات التنظيمية في جميع أنحاء العالم إلى تأمين سلسلة توريد البرمجيات، فمن الأهمية بمكان أن تستند هذه الجهود إلى فهم واضح لكيفية بناء وصيانة أهم أنظمة الإنترنت. وتشمل الأمثلة الحديثة للتدخل التنظيمي (المقترح) لتقليل الثغرات الأمنية في البرمجيات في البنية التحتية الرقمية ما يلي:

- مدونة ممارسات أمن البرمجيات الطوعية لموردي البرمجيات في المملكة المتحدة.<sup>1</sup>
- إقرار ذاتي من الصناعة لممارسات تطوير البرمجيات الآمنة للاستخدام من قبل حكومة الولايات المتحدة.<sup>2</sup>
- متطلبات دخول السوق ("قانون المرونة السيبرانية (CRA)") للمنتجات الرقمية (بما في ذلك البرامج) في الاتحاد الأوروبي.<sup>3</sup>
- التزامات إدارة المخاطر والإبلاغ لموفري البنية التحتية الرقمية في الاتحاد الأوروبي ("NIS2 IA").<sup>4</sup>
- تمت تسمية مجتمعات المصدر المفتوح باسم الهدف التنموي في الخطة الخمسية لتكنولوجيا المعلومات في الصين.<sup>5,6</sup>

على الرغم من أن البرمجيات المجانية المفتوحة المصدر (FOSS) هي ممارسة تطوير البرمجيات السائدة اليوم، إلا أن خصائصها الخاصة غالبًا ما يتم تجاهلها في الخطابات المتعلقة بالسياسات. فإن قام صناع السياسات بتقديم مداخلات تنظيمية دون فهم نموذج التطوير والتوريد الفريد للبرمجيات المجانية المفتوحة المصدر FOSS، فإنهم يخاطرون بتهديد أمن واستقرار البنية التحتية الحيوية التي تعتمد عليها، بما في ذلك نطاق الإنترنت وأنظمة التوجيه. ويهدف هذا التقرير إلى توفير ذلك السياق الضروري.

وعلى عكس ما هو معتاد في القطاعات الأخرى، فإن معظم البرامج التي تشغل الإنترنت متاحة بموجب تراخيص حقوق الطبع والنشر الخاصة ببرمجيات FOSS. ولا تتعلق هذه التراخيص بالتكلفة في المقام الأول؛ بل تتعلق بالحرية. وعلى وجه التحديد، تمنح تراخيص برمجيات FOSS مشغلي البنية التحتية أربع حريات أساسية: الاستخدام والدراسة والتغيير ومشاركة البرمجيات –

<sup>1</sup> "مدونة ممارسات أمن البرمجيات". وزارة العلوم والابتكار والتكنولوجيا بالمملكة المتحدة، 7 مايو/أيار 2025. <https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice>

<sup>2</sup> "Secure Software Development Attestation Form". الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية <https://www.cisa.gov/secure-software-attestation-form>

<sup>3</sup> "قانون المرونة السيبرانية الأوروبي: أعضاء البرلمان الأوروبي يعتمدون خططًا لدعم أمن المنتجات الرقمية"، بيان صحفي للبرلمان الأوروبي، في 12 مارس/آذار 2024، على الرابط - <https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products>

<sup>4</sup> "قانون المرونة السيبرانية الأوروبي: أعضاء البرلمان الأوروبي يعتمدون خططًا لدعم أمن المنتجات الرقمية". بيان صحفي. البرلمان الأوروبي، في 12 مارس/آذار 2024. على الرابط - <https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products>

<sup>5</sup> "الخطة الخمسية الرابعة عشر لصناعة الخدمات البرمجية والمعلوماتية والتكنولوجية". مجلس الدولة في جمهورية الصين الشعبية، وزارة الصناعة وتكنولوجيا المعلومات، في ديسمبر/كانون الأول 2021. على الرابط - <https://www.gov.cn/zhengce/zhengceku/2021-12/files/a44b507d67c74591ad4f5e55b98c4518.pdf/5655205/01/12>

<sup>6</sup> "ترجمة: الخطة الخمسية الرابعة عشر للمعلوماتية الوطنية". مشروع DigiChina، جامعة ستانفورد، 24 يناير/كانون الثاني 2022. على الرابط <https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>

معدلة أو غير معدلة – مع الجميع. وهذا نموذج تطوير، وليس مجرد برنامج "مجاني"،<sup>7</sup> ويشكل الأساس للجهد التعاوني العالمي الذي يبني ويحافظ على معظم البنية الأساسية الحيوية للإنترنت.

تم إعداد هذا التقرير لتزويد صناعات السياسات بفهم شامل لدور البرمجيات المجانية والمفتوحة المصدر FOSS في نظام اسم النطاق (DNS) ومنظومة تسجيل اسم النطاق.

- يقدم القسم 2 مقدمة غير تقنية لنظام اسم النطاق، ويشرح المكونات والوظائف الرئيسية لهذه البنية التحتية الحيوية.
- يقدم القسم 3 تفاصيل نموذج البرمجيات المجانية المفتوحة المصدر FOSS، ويشرح خصائصه الرئيسية ونقاط القوة المتأصلة والمخاطر الفريدة مقارنة بالبرمجيات المملوكة.
- يقدم القسم 4 البحث الأساسي الذي أجرته اللجنة الاستشارية للأمن والاستقرار (SSAC) حول انتشار برمجيات FOSS، مما يدل على هيمنتها في الأجزاء الأكثر أهمية لنظام اسم النطاق DNS.
- يتناول القسم 5 العديد من الحالات المعاصرة من الولايات المتحدة والمملكة المتحدة والاتحاد الأوروبي والتي توضح كيف يقوم صناعات السياسات بتكليف لوائح الأمن السيبراني مع الحقائق الفريدة لمنظومة برمجيات FOSS.
- يقوم القسم 6 بتوحيد التحليل الأساسي للتقرير في سلسلة من النتائج التي تشكل أساس الأدلة للمبادئ التوجيهية التي تتبع في القسم 7.
- يقدم القسم 7 مبادئ توجيهية مباشرة وقابلة للتنفيذ لصناعات السياسات.

## 2 مقدمة DNS

عندما ترسل بريداً إلكترونيًا، أو تتصفح صفحة ويب، أو تتحدث مع الأصدقاء، وما إلى ذلك، فإن جهازك (مثل الكمبيوتر أو الهاتف أو الجهاز اللوحي) يرسل ويستقبل آلاف المعلومات. ويمكنك التفكير في هذا الأمر مثل بطاقة بريدية رقمية، تحتوي على عنوان المرسل، وعنوان المستقبل، والمحتوى. يحتوي كل جهاز متصل بالإنترنت على الأقل على عنوان بروتوكول إنترنت (IP) فريد ومرتبطة به. وبالنسبة للبشر، فإنه من الأسهل عليهم تذكر الأسماء مقارنة بالأرقام. نظام اسم النطاق DNS هو بمثابة دفتر عناوين الإنترنت. حيث يقوم بربط عنوان IP باسم النطاق بحيث يمكن لأي شخص التنقل عبر الإنترنت بسهولة أكبر.<sup>8,9</sup> ويعد نظام اسم النطاق نظامًا بالغ الأهمية وضروريًا لاستمرار الإنترنت العالمي المستقر الآمن والقابل للتشغيل المتبادل.

يوفر نظام اسم النطاق ربطاً بين أسماء النطاقات سهلة الاستخدام (على سبيل المثال، [icann.org](http://icann.org)) وعناوين IP العديدة سهلة الاستخدام للكمبيوتر (على سبيل المثال، 192.0.43.7 أو 1::db8:2001). وتشكل هذه التعيينات مجتمعة مساحة اسم عالمية. ولأجل الحصول على موقع ويب أو حساب بريد إلكتروني يمكن الوصول إليه عبر اسم النطاق، يجب على صاحب النطاق نشر

<sup>7</sup> يمكن استخدام البرمجيات المجانية المفتوحة المصدر FOSS لأي غرض وهي خالية من القيود مثل انتهاء صلاحية الترخيص أو القيود الجغرافية. ويمكن لأي شخص دراسة الكود الخاص به، دون الحاجة إلى اتفاقيات عدم الإفصاح أو قيود مماثلة. ويمكن مشاركتها ونسخها بتكلفة شبه معدومة. بالإضافة إلى ذلك، يمكن أن يتم تعديل برمجيات FOSS من قبل أي جهة، ويمكن مشاركة هذه التحسينات علناً. إن غياب أو إضعاف واحدة على الأقل من هذه الحريات يعني أن التطبيق احتكاري (مملوك من قبل جهة معينة)، أي أنه ليس برنامجاً مفتوح المصدر. يتم منح الحريات الأربع من خلال ترخيص البرمجيات. وتعرّف تراخيص البرامج الشروط التي يمكن بموجبها استخدام البرنامج وإعادة استخدامه. ولكي يكون البرنامج مجانياً، يجب أن يحتوي نص الترخيص على الحريات الأربع على الأقل. تحتفظ مؤسسة Free Software Foundation على الرابط <https://www.gnu.org/licenses/license-list.html>، ومؤسسة Open Source Initiative على الرابط <https://opensource.org/licenses>، وDebian Project على الرابط <https://wiki.debian.org/DFSGLicenses> بقوائم التراخيص التي تمت مراجعتها والموافقة عليها. ولا يمكن عادةً اعتبار التطبيق برنامجاً مجانياً ومفتوح المصدر إذا لم يظهر ترخيصه في إحدى هذه القوائم.

<sup>8</sup> ICANN. "نظام أسماء النطاقات"، 13 سبتمبر/أيلول 2022. <https://www.icann.org/resources/pages/dns-2022-09-13-en>.

<sup>9</sup> منصة Cloudflare. "ما المقصود بنظام أسماء النطاقات؟ | كيف يعمل نظام أسماء النطاقات"، <https://www.cloudflare.com/learning/dns/what-is-dns/>.

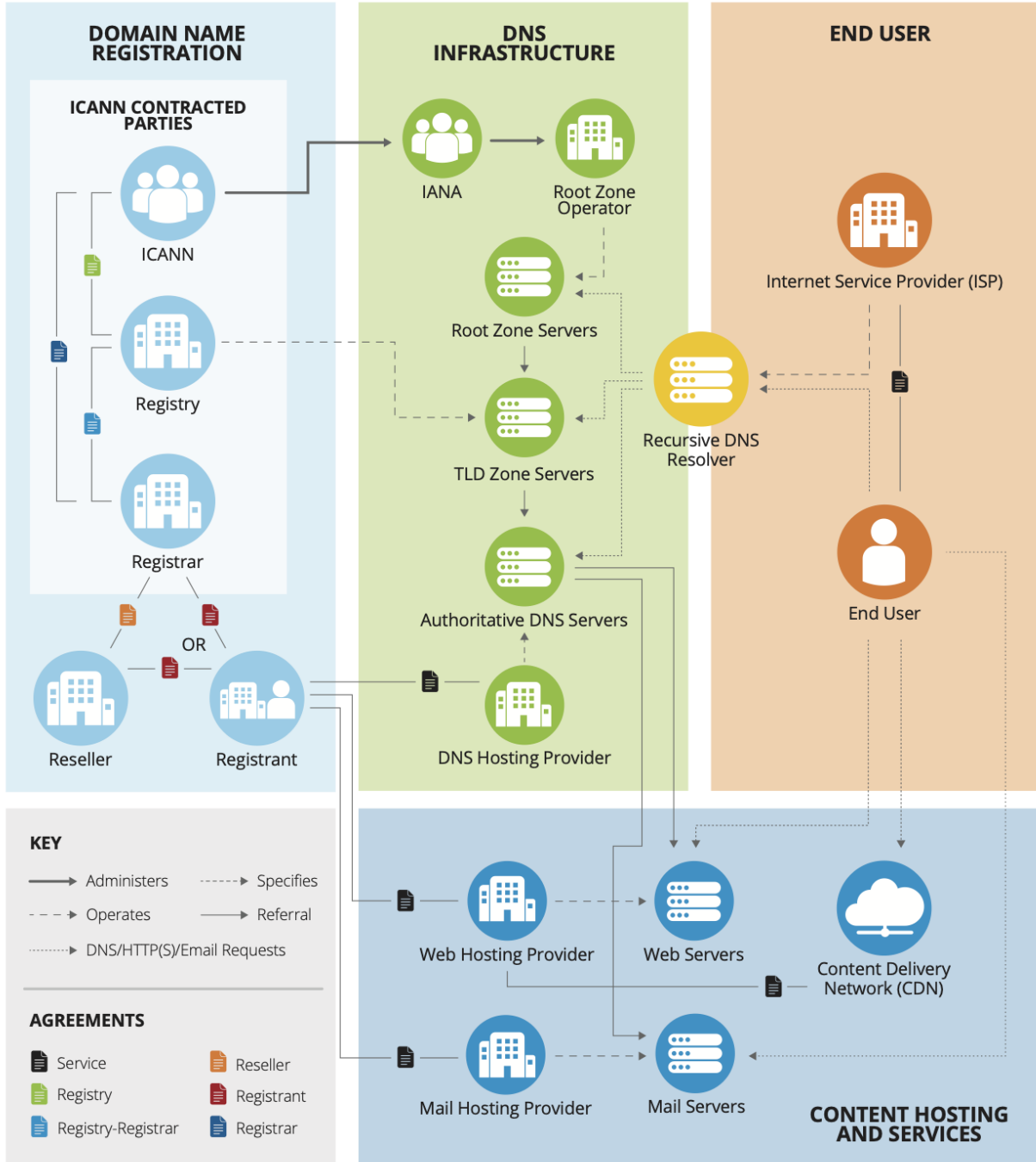
التعيينات الخاصة بتلك الخدمة. ويؤدي هذا المنشور في نظام اسم النطاق إلى جعل الاتصال بين اسم النطاق وعنوان IP الخاص بالخدمة متاحًا لأي شخص على الإنترنت.

كما يوضح المخطط 1، تتكون منظومة اسم النطاق من ثلاثة أجزاء رئيسية:

- تسجيل اسم النطاق (المربع الأزرق الفاتح): هذا هو الإطار الإداري والتعاقدى للحصول على أسماء النطاقات.
- البنية التحتية لنظام DNS (المربع الأخضر): هذه هي الأنظمة التقنية التي تجعل أسماء النطاقات تعمل على الإنترنت عن طريق ترجمتها إلى عناوين IP.
- خدمات المستخدم النهائي والمحتوى (المربعات البرتقالية والأزرق الداكن): هذه هي الخدمات التي يستخدمها الأشخاص في نهاية المطاف، مثل مواقع الويب والبريد الإلكتروني.

يركز هذا التقرير على تسجيل أسماء النطاقات والبنية الأساسية لنظام DNS، والتي تشكل معًا طبقة من البنية الأساسية الحيوية للإنترنت. إن البحث عن المعلومات في مساحة اسم النطاق العالمي لا يحقق في الغالب ربحاً منه ويتم تقديمه "مجانيًا" للعملاء دون مقابل. وإن البنية التحتية التي تمكن هذه الخدمة العالمية الموزعة باعتبارها "منفعة عامة غير استغلالية" هي ما يشير إليه هذا التقرير باسم "البنية التحتية لنظام DNS". ويتم توزيع النظام على نطاق واسع عبر الإنترنت ويتكون من مكونات متعددة، يتم تشغيلها من قبل العديد من المنظمات المستقلة التي تلعب أدوارًا محددة مختلفة في هذا النظام. وتتفاعل هذه الأنظمة بعضها مع بعض لأن التفاصيل الفنية اللازمة لواجهاتها واتصالاتها يتم توحيدها من خلال فريق عمل هندسة الإنترنت (IETF).

تعتبر هذه البنية التحتية الحيوية منفصلة عن المحتوى الذي يتم تقديمه من خلالها. وإن تسجيل اسم النطاق لا يعني إنشاء موقع ويب. وإن نشر اسم النطاق في نظام اسم النطاق حتى يمكن إيجاده لا يشبه نشر محتوى موقع الويب. ويتناول هذا التقرير البرمجيات الأساسية التي تجعل دفتر العناوين يعمل، وليس المعلومات المكتوبة على صفحات هذا الدفتر.

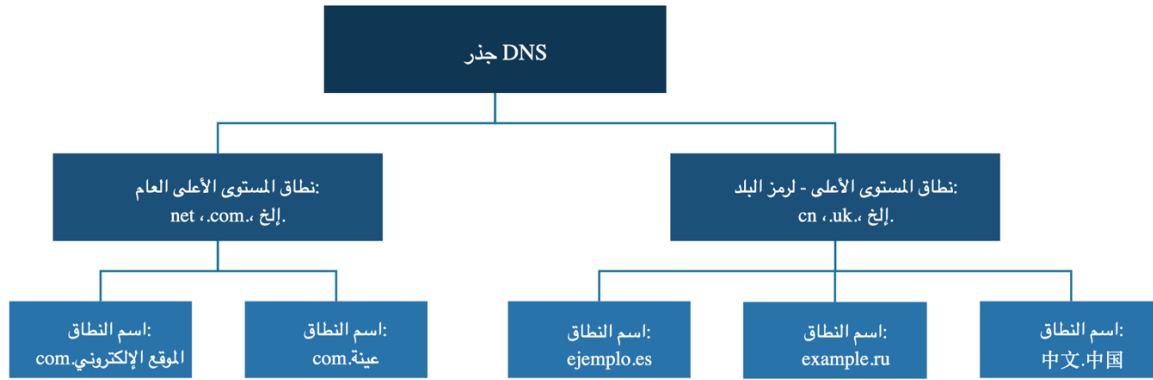


**المخطط 1: منظومة الإنترنت.** كيث درازيك. "أمان نظام اسم النطاق DNS: العمل المجتمعي الجاري للتخفيف من حدة التهديدات الأمنية لنظام اسم النطاق (DNS)." مدونة Verisign، في 7 ديسمبر/كانون الأول 2021. على الرابط <https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/>.

## 2.1 التسلسل الهرمي لنظام DNS

إن نظام اسم النطاق DNS هو نظام موزع عالميًا، وهرمي، وغير مركزي. تم تصميم هذا النظام، الموضح في المخطط 1 باسم "البنية الأساسية لنظام اسم النطاق DNS"، ليكون مرناً، مما يضمن عدم حدوث تعطل للإنترنت العالمي من نقطة أو مركز فردي واحد.

يوضح المخطط 2 كيفية تكون مساحة اسم نظام DNS هرمية.



### المخطط 2: التسلسل الهرمي لنظام DNS

في أعلى التسلسل الهرمي يوجد جذر نظام DNS (.)، والذي يخدمه نظام خادم الجذر (RSS).<sup>10</sup> ويشير الجذر إلى الخوادم الرسمية لمختلف نطاقات المستوى الأعلى (TLD). وتعتبر نطاقات المستوى الأعلى هي نهايات أسماء النطاقات ويتم تصنيفها على نطاق واسع إلى نوعين:

- نطاقات المستوى الأعلى العامة (gTLD): هذه هي النطاقات ذات الأغراض العامة مثل .com، .org، وxyz.
- نطاقات المستوى الأعلى لرموز البلدان (ccTLD): هذه مخصصة للاستخدام من قِبل البلدان والأقاليم والمواقع الجغرافية المحددة في قائمة رموز البلدان 1-3166 ISO.<sup>12</sup> ويمكن أن تستند أسماء نطاقات المستوى الأعلى لرموز البلدان على رموز البلدان المكونة من حرفين والتي حددها معيار ISO 3166-1 (على سبيل المثال، .jp لليابان، و.fr لفرنسا، و.ke لكينيا)، أو يمكنها تمثيل اسم بلد أو إقليم بنصوص من غير أحرف ASCII.<sup>13</sup> وتُعرف هذه بأسماء النطاقات المدوّلة (IDN)، وهو مفهوم نفذته ICANN منذ عام 2009.

<sup>10</sup> يتألف نظام خادم الجذر من خوادم موزعة عالميًا يتم تشغيلها من قبل 12 منظمة مستقلة. ولمزيد من المعلومات حول مشغلي خادم الجذر، راجع "RSSAC023v2: تاريخ نظام خادم الجذر". اللجنة الاستشارية لنظام خادم الجذر (RSSAC) في ICANN، بتاريخ 17 يونيو/حزيران 2020. على الرابط <https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf>

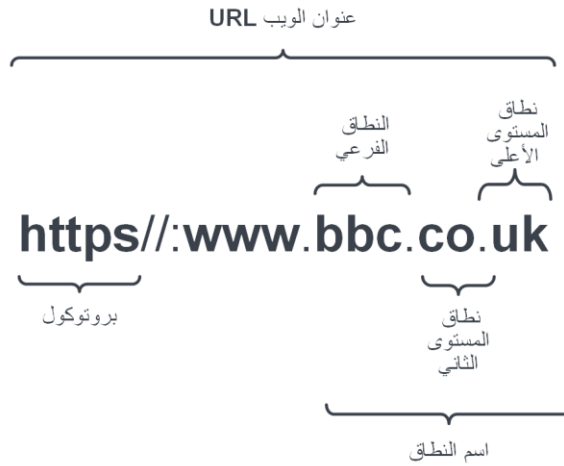
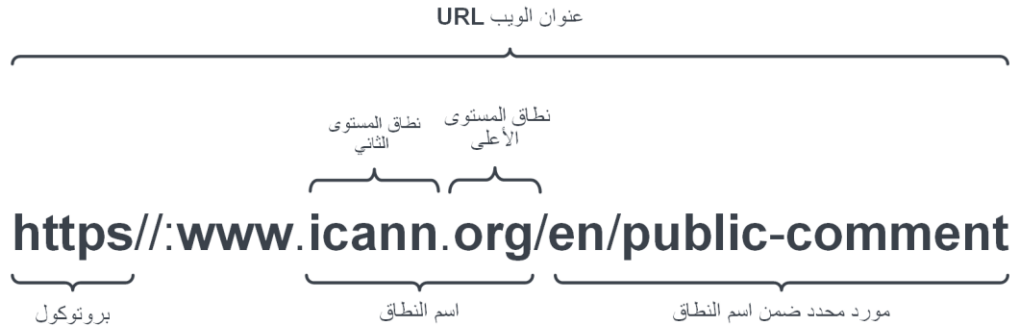
<sup>11</sup> ICANN. "الاختصارات والمصطلحات، نطاق المستوى الأعلى العام (gTLD)" على الرابط <https://www.icann.org/en/icann-acronyms-and-terms/generic-top-level-domain-en>

<sup>12</sup> المنظمة الدولية للتقييس. "ISO 3166 — أكواد الدول"، <https://www.iso.org/iso-3166-country-codes.html>

<sup>13</sup> ICANN. "الاختصارات والمصطلحات، نطاق المستوى الأعلى لرمز البلد (ccTLD)"، على الرابط <https://www.icann.org/en/icann-acronyms-and-terms/country-code-top-level-domain-en>

توجد أسفل نطاقات المستوى الأعلى أسماء النطاقات الفرعية. يتكون اسم النطاق من جزأين أو أكثر من الأجزاء النصية المفصولة بنقاط. كما هو موضح في المخطط 3، يتم إنشاء اسم النطاق من اليمين إلى اليسار، بدءًا من TLD. على سبيل المثال، في `icann.org`، نطاق المستوى الأعلى هو `org`. ونطاق المستوى الثاني هو `icann`. ويشكلان معًا اسم النطاق الفريد. في المثال الثاني، `bbc.co.uk`، نطاق المستوى الأعلى هو `uk`. ونطاق المستوى الثاني هو `co`. ويتيح هذا النظام الهرمي واللامركزي تحقيق شبكة إنترنت عالمية قوية ومرنة.

اسم النطاق هو اسم فريد يشكل أساس المحددات الموحدّة لمصدر المعلومات (URL) التي يستخدمها الأشخاص لإيجاد الموارد على الإنترنت. إن اسم النطاق يحدد عنوانًا محددًا على الإنترنت ينتمي إلى كيان مثل شركة أو منظمة أو مؤسسة أو فرد.<sup>14</sup>



المخطط 3: مكونات URL واسم النطاق

## 2.2 تسجيل اسم النطاق ونشره

تشير البنية التحتية لتسجيل اسم النطاق إلى الأنظمة التي تسهل الحصول على اسم نطاق فريد. وتتطوي هذه العملية، الموضحة في قسم "تسجيل اسم النطاق" في المخطط 1، على العديد من الجهات الفاعلة الرئيسية واثنين من العمليات المميزة: التسجيل والنشر.

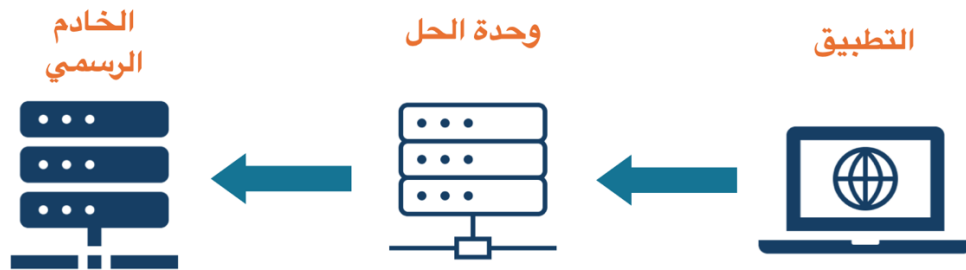
<sup>14</sup> ICANN. "المختصرات والمصطلحات، اسم النطاق،" <https://www.icann.org/en/icann-acronyms-and-terms/domain-name-en>

إن التسجيل هو عملية حجز اسم النطاق. والمسجل هو الفرد أو المنظمة التي تسجل وتحمل الحقوق الخاصة باسم نطاق معين. لتسجيل اسم نطاق تحت نطاق محدد من نطاق المستوى الأعلى، يجب على المسجل أن يستخدم أمين سجل. وأمين السجل هو منظمة عامة تعمل بمثابة بائع تجزئة لأسماء النطاقات. ويعتبر أمناء السجلات في الواقع بمثابة قناة توزيع للتسجيلات وإدارة المدفوعات والتجديدات وغيرها من المعلومات الإدارية. ثم يتفاعل أمين السجل مع سجل. والسجل هو قاعدة البيانات الرئيسية الرسمية لجميع أسماء النطاقات ضمن نطاق المستوى الأعلى المذكور. وتسمى المنظمة التي تحافظ على قاعدة البيانات هذه بمشغل السجل. لأنتمة ملايين المعاملات فيما بينها، يستخدم أمناء السجلات والسجلات بروتوكول التزويد المرن (EPP)، وهو بروتوكول موحد لتسجيلات أسماء النطاقات وتجديدها ونقلها.

إن نتيجة التسجيل الناجح هي نشر سجلات نظام اسم النطاق الخاصة بالنطاق على الخوادم الرسمية التي تعد جزءاً من البنية التحتية لنظام DNS، مما يجعل النطاق قابلاً للوصول على الإنترنت. والنشر هو العملية الفنية المتمثلة في جعل سجلات نظام اسم النطاق الخاصة بالنطاق متاحة على خوادم الأسماء الرسمية. تحتوي هذه الخوادم على قوائم أسماء النطاقات سهلة الاستخدام لعناوين IP السهلة للكمبيوتر المقابلة لها، وهو أمر بالغ الأهمية لتحديد مواقع الويب وخوادم البريد وموارد الإنترنت الأخرى والتحقق من صحتها.

## 2.3 حل نظام DNS

عندما تقوم بكتابة اسم نطاق مثل [www.example.com](http://www.example.com) في متصفح الويب، تبدأ عملية تسمى "حل نظام اسم النطاق". وتعتمد هذه العملية على نوعين من مكونات البنية الأساسية لنظام اسم النطاق التي تعمل معاً: المُحلّلات التكرارية والخوادم الرسمية (انظر المخطط 4).



### المخطط 4: حل نظام DNS التقليدي

الخوادم الرسمية هي المكونات التي تنشر معلومات النطاق. وهي التي تحمل السجل الرسمي النهائي لنطاق معين وتجعله متاحاً للاسترجاع. ويتم تشغيل خوادم الأسماء الرسمية من قبل الأفراد والمؤسسات والجامعات وموفري الخدمات والجهات الحكومية. على سبيل المثال، تنشر خوادم أسماء نطاقات المستوى الأعلى البيانات الفنية لجميع النطاقات الفردية ضمن سجلها. وتتمتع العديد من المؤسسات بخدمات محلية لنظام اسم النطاق DNS توفر فقط المعلومات التي تنطبق على مؤسساتها الداخلية، مثل تحديد مواقع الويب الخاصة بالإدارات على شبكة الإنترنت. وهذا جزء كبير من نظام اسم النطاق الذي لا يمكن رؤيته من الإنترنت المفتوح.

يعتمد بعض المستخدمين النهائيين والشركات الصغيرة على الخدمات الرسمية من أمين سجل اسم النطاق أو مستضيف الويب لنشر معلومات نطاقهم، ولكن من الشائع أن تقوم الشركات والحكومات والمؤسسات بتشغيل خوادمها الرسمية بشكل منفصل، إما داخلياً أو خارجياً. وتتمثل المخاوف الرئيسية في الموثوقية والتكرار؛ وبالتالي، فإن مسؤولي معلومات "المنطقة" المنشورة ضمن نطاق ما غالباً ما يشتركون "خدمات نظام اسم النطاق الثانوية الرسمية" من موفري خدمات خارجيين. وينشر هؤلاء

الموفرين نفس البيانات مثل خوادم نظام اسم النطاق الرسمية الأساسية. العديد من المنظمات التي تقدم هذه الخدمات هي نفسها التي تقدم خدمات نظام اسم النطاق الرسمية لنطاقات المستوى الأعلى TLD.

تسهل المُحلّلات استرجاع معلومات نظام اسم النطاق DNS. إنها تعمل نيابة عن جهاز المستخدم ("العميل"، مثل هاتفك الذكي) للعثور على عنوان IP الصحيح. وللقيام بذلك بكفاءة، تحتفظ المُحلّلات بقاعدة بيانات محدثة باستمرار للعمليات البحثية الأخيرة، والتي تسمى ذاكرة التخزين المؤقت. في الممارسة العملية، يكون من الشائع أن تجيب المُحلّلات على ما يصل إلى 90% من الاستعلامات من ذاكرة التخزين المؤقت المحلية الخاصة بها، وهو ما يعد أسرع بكثير من الاستعلام من الخوادم عبر الإنترنت. وبالنسبة للإجابات التي لا يملكونها مخزنة مؤقتًا، فيجب عليها الاستعلام من الخوادم الرسمية. وعادةً ما تكون المُحلّلات مشغولة للغاية ومحملة بشكل كبير، ويرجع ذلك جزئيًا إلى أن مستوى حركة مرور البيانات المرتفع الثابت يضمن ذاكرة تخزين مؤقتة يتم تحديثها باستمرار.

هناك الملايين من المُحلّلات حول العالم. ويمكن أن تكون وظيفة المُحلّل محلية، ضمن شبكة المستخدم أو شبكة موفر خدمة الوصول، أو في السحابة الإلكترونية، إما كخدمة منفصلة مستضافة على الإنترنت أو بالاشتراك مع خدمات سحابية أخرى. وبغض النظر عن كيفية إعداد الخدمة، فمن المهم التأكد من أن المستخدمين المقصودين فقط هم القادرين على الاستعلام عن الخدمة. وإذا كانت الخدمة متاحة لأي شخص على الإنترنت، فمن الممكن إساءة استخدامها، على سبيل المثال، هجمات الحجب المنتشر للخدمة (DDoS). وعادةً ما يحدد التكوين في جهاز المستخدم موفر الخدمة المفضل. وتوفر العديد من الجامعات والمؤسسات وموفري خدمات الإنترنت (ISP) مُحلّلات محلية للمستخدمين على شبكاتهم، وهناك خدمات سحابية شائعة مثل Google وهو (8.8.8.8)، وQuad9 وهو (9.9.9.9)، وCloudflare وهو (1.1.1.1). تشمل العوامل الرئيسية في تحديد موفر المُحلّل الذي يجب استخدامه السياسة التنظيمية، وسياسات التصفية أو القائمة المحظورة للمُحلّل، وتوافر عمليات نقل نظام اسم النطاق المشفرة. وتظهر عملية الحل (المخطط 4) كيفية عمل هذه المكونات معًا وفقًا للتسلسل الهرمي لنظام اسم النطاق.

### 3 نموذج البرمجيات المجانية مفتوحة المصدر FOSS: الخصائص الرئيسية والآثار

تناول القسم السابق مقدمة عن البنية التحتية لنظام اسم النطاق وتسجيل اسم النطاق، وهي الأنظمة الأساسية التي تسمح للمستخدمين بالتنقل عبر الإنترنت. وسوف يوضح هذا القسم كيفية بناء هذه البنية التحتية الحيوية وصيانتها. وإن البرمجيات التي تدعم معظم هذه البنية التحتية هي البرمجيات المجانية المفتوحة المصدر، والتي تعمل على نموذج تطوير واقتصاد مختلف تمامًا عن البرمجيات الاحتكارية التقليدية. وتتطلب مناقشة السياسة المستنيرة فهم هذه الخصائص الفريدة

#### 3.1 الأدوار الرئيسية في منظومة FOSS

على عكس البرمجيات التقليدية مغلقة المصدر حيث يتم التعامل مع التطوير داخليًا ومن قبل كيان قانوني واحد، فإن نموذج برمجيات FOSS مفتوح وموزع. والأدوار لا تتعارض مع بعضها البعض، ويمكن لأي شخص، في أي مكان، أن يقوم بها. ولأغراض هذا التقرير، سيتم استخدام المصطلحات التالية:

- **المسؤول:** الفرد أو المجموعة المسؤولة عن التوجيه العام لمشروع برمجيات FOSS. ولدى المسؤولين السلطة لقبول أو رفض المساهمات في النسخة الرسمية للبرمجيات، مما يضمن الجودة والاتساق. وهم المشرفون على المشروع.
- **المساهم:** فرد أو منظمة تقدم تحسينات لمشروع ما، مثل إرسال الأكواد أو الوثائق أو تقارير الأخطاء. ويتم مراجعة هذه المساهمات من قبل أحد المسؤولين قبل إدراجها في المشروع الرسمي.
- **المستخدم أو المشغل:** الفرد أو المنظمة التي تنشر البرمجيات وتستخدمه. وفي سياق نظام اسم النطاق DNS، فإن "المشغل" هو كيان يقوم بتشغيل مكونات البنية التحتية لنظام DNS، مثل الخوادم أو المُحلّلات الرسمية. ويُعد المستخدمون والمشغلون جزءًا حيويًا من المنظومة، حيث يقدمون الملاحظات ويمنحون المشروع غرضًا.

ولتجنب الغموض، يستخدم هذا التقرير المصطلحين المحددين "المسؤول" و"المساهم" بدلاً من المصطلح الأكثر عمومية "المطور"، حيث قد يقوم فرد ما بتطوير الكود كمسؤول أو مساهم أو بشكل مستقل.

## 3.2 المبادئ الأساسية لنموذج تطوير برمجيات FOSS

يتم تعريف نموذج برمجيات FOSS من الحقوق الممنوحة من خلال تراخيص حقوق النشر الخاصة بها. ولكي يتم اعتبار برنامج FOSS، يجب أن يمنح ترخيصه للمستخدمين أربع حريات أساسية:<sup>15،16</sup>

- حرية *استخدام* البرمجيات لأي غرض، دون قيود مثل انتهاء صلاحية الترخيص أو القيود الجغرافية.
- حرية *دراسة* كيفية عمل البرمجيات، الأمر الذي يتطلب الوصول إلى الكود المصدر دون اتفاقيات عدم الإفصاح.
- حرية *مشاركة* البرمجيات، مما يعني أنه يمكن إعادة توزيعها ونسخها دون أي تكلفة تقريباً.
- حرية *تغيير* البرمجيات ونشر هذه التحسينات للعمامة.

إن غياب أو إضعاف أي من هذه الحريات يعني أن البرنامج مملوك، وليس برنامجاً مجانياً مفتوح المصدر FOSS. وتشكل هذه الحريات الأساس للخصائص العامة للبرمجيات المجانية المفتوحة المصدر، والتي تختلف بشكل كبير عن البرمجيات الاحتكارية (المملوكة). تحتفظ منظمات مثل Free Software Foundation<sup>17</sup> و Open Source Initiative<sup>18</sup>، و Debian Project<sup>19</sup> بقوائم تراخيص البرامج التي تمت مراجعتها والموافقة عليها باعتبارها تلبى هذه المعايير.

لا تعد هذه الحريات الأربع مجرد مبادئ مجردة؛ بل إنها تشكل الأساس لنموذج التطوير الفريد والخصائص الاقتصادية للبرمجيات المجانية المفتوحة المصدر FOSS، والموصوفة في الأقسام الفرعية التالية.

### 3.2.1 نموذج برمجيات FOSS يسمح بالتطوير التعاوني العالمي

نظرًا لأن تراخيص برمجيات FOSS تمنح أي شخص حرية دراسة الكود وتعديله ومشاركته، فإنها تسهل التعاون العالمي المفتوح في تطوير البرمجيات. ولا توجد مجموعة عشوائية من الشروط المسبقة التي يتم تطبيقها على المساهمين في تطوير برمجيات FOSS، مما يسمح لأي فرد بتقديم مساهمات إلى البرنامج. يمكن أن تأتي المساهمات من مجموعة متنوعة من الأفراد والمنظمات، في بعض الأحيان كجزء من التطوير المؤسسي لمنتج ما، وفي بعض الأحيان على أساس فردي تطوعي.

المنتج الناتج متاح مجانًا لأي شخص ليس فقط لأي استخدام (بما في ذلك الاستخدام التجاري)، ولكن لمزيد من التطوير. يؤدي هذا إلى تقليل المصادمات المحتملة الحدوث خلال تطوير البرمجيات، وخاصةً عندما يتم دمج التعديلات مرة أخرى في منتج البرمجيات، مما يساهم في تسريع تطوير الميزات وحل أخطاء البرمجيات وقضايا الأمان. وتعمل الطبيعة التعاونية لبرمجيات FOSS على تعزيز الشفافية والابتكار السريع. علاوة على ذلك، فإن المساهمات نفسها تكون مفتوحة أيضًا عادةً، مما يسمح للآخرين بفحص المساهمات المقترحة والتعليق على مدى ملاءمتها للمساهمة ومزايا دمج المساهمة في منتج البرنامج.

ومع ذلك، فمن غير المعتاد أن يتم قبول كل هذه المساهمات دون مستوى معين من الفحص والقبول. تهدف مثل هذه الفحوصات إلى تقليل مخاطر تعرض البرامج للخطر من خلال تضمين تعليمات (أكواد) برمجيات غير متسقة أو غير صحيحة أو ضارة. وهناك بعض الشروط المشتركة لقبول المساهمات، بما في ذلك ضرورة الحفاظ على حقوق النشر واعتبارات الملكية الفكرية. إن الممارسة الشائعة في برمجيات FOSS هي أن جميع المساهمات التعاونية لا يمكنها فرض قيود إضافية على استخدام

<sup>15</sup> نظام التشغيل GNU. "ما المقصود بالبرمجيات المجانية؟"، <https://www.gnu.org/philosophy/free-sw.html>

<sup>16</sup> التعريف البديل والشائع لما يمثل ترخيص برمجيات FOSS هو "تعريف المصدر المفتوح" لمبادرة المصدر المفتوح، <https://opensource.org/osd>

<sup>17</sup> نظام التشغيل GNU. "تراخيص مختلفة وتعليقات حولها"، <https://www.gnu.org/licenses/license-list.html>

<sup>18</sup> مؤسسة Open Source Initiative. "الترخيص المعتمدة من OSI"، على الرابط <https://opensource.org/licenses>

<sup>19</sup> Debian Wiki. "DFSGLicenses"، على الرابط <https://wiki.debian.org/DFSGLicenses>

البرمجيات تتجاوز الشروط المرتبطة بالفعل بالبرمجيات، ولا يمكنها فرض قيود إضافية تتعلق بحقوق النشر أو الملكية الفكرية على قاعدة البرمجيات الموجودة.

وكبديل للمساهمة، تتيح تراخيص برمجيات FOSS أيضًا للمساهمين بدء مشتق خاص بهم (مشروع فرعي)، بدلاً من العمل مع المشروع الأصلي (المنبع). ويتيح التفرع بدون تصريح الابتكار السريع. وقد أصبحت بعض المشروعات الفرعية أكثر شعبية من المشروع الأصلي المشتقة منه. ولكنها قد تؤدي أيضًا إلى خلق حالة من الارتباك، وتقسيم قدرة المراجعة المتاحة لتحديد الأخطاء أو الإضافات الضارة.

ويمكن أن يكون البرنامج مستقلاً بذاته، أو يمكنه الاعتماد على مكتبات برامج أخرى لبناء الوظائف الضرورية. ويمكن أن تتغير مثل هذه المكتبات، والتي تعد في الأساس مكونات خارجية للكود، بطرق أقل وضوحًا لمطوري الكود، وقد يؤدي هذا الموقف إلى إنتاج سلوكيات غير مقصودة. وتتمتع برمجيات FOSS بحاجز دخول منخفض للغاية لاستخدامها كمكون في برمجيات أخرى (بما في ذلك البرمجيات الاحتكارية)، وهو ما يجعل تكرار حدوث مثل هذه المخاطر أعلى، على الرغم من أنها ليست فريدة من نوعها بالنسبة لبرمجيات FOSS.

### 3.2.2 نموذج برمجيات FOSS يعمل بدون علاقات تعاقدية

أحد أهم مميزات نموذج توريد برمجيات FOSS هو أن هذه الأطراف عادةً لا تربطها علاقة تعاقدية. ويتناقض هذا مع سلسلة التوريد الخاصة بالسلع المادية، حيث يكون لدى المصنعين والموزعين عقود يمكن الاستفادة منها لربط السياسات أو نقل التزامات الامتثال. ومع ذلك، ففي نموذج توريد برمجيات FOSS، يحصل المشغلون على البرمجيات من خلال مسارات متعددة. وفي الوقت الذي يقوم فيه المسؤول بتوفير البرمجيات على شكل مصدر متاح للتنزيل العام، إلا أن الأكثر شيوعًا توزيعه من خلال وسطاء يوفرون حزمًا قابلة للتثبيت (على سبيل المثال، "Debian Project") أو على شكل منتجات أو خدمات. وبعيدًا عن شروط ترخيص المصدر المفتوح الذي يمنحه المسؤول، فإنه نادرًا ما يكون لدى المشغل عقد مع مثل هذا الوسيط. يوجد فقط عقد جزئي مع المسؤولين. عندما توجد علاقة تعاقدية، فعادةً ما تكون للدعم الفني، وليس لبرمجيات FOSS بحد ذاتها.

### 3.2.3 نموذج برمجيات FOSS يفصل بين التمويل والاستخدام

على عكس السلع المادية، فإن البرمجيات هي مجرد معلومات وليس لها تكلفة مادية جوهرية لكل وحدة إضافية يتم إنتاجها. إن حرية استخدام ومشاركة برمجيات FOSS تعني أن التراخيص تمنح الحقوق دون الحاجة إلى تبادل الأموال. ويمكن للمستخدمين، بما في ذلك مشغلي البنية التحتية للإنترنت، تمويل تطوير وصيانة برمجيات FOSS إذا رغبوا في ذلك، ولكن الترخيص لا يلزمهم بذلك، وبالتالي فإن تمويل المطورين غير مرتبط باستخدام برامجهم.

### 3.2.4 غالبًا ما لا يوجد لدى برمجيات FOSS كيان قانوني مسؤول واحد

في عالم السلع المادية، من الشائع جدًا افتراض وجود كيان قانوني مسؤول واحد، والذي بدوره يمكن أن يكون خاضعاً لسياسة، أو يتحمل عبء الامتثال. وعلى عكس السلع المادية، فإن توزيع البرامج عالميًا يحدث غالبًا بتكلفة منخفضة جدًا أو بدون تكلفة عبر الإنترنت. ويتيح هذا للأفراد، أو مجموعات من الأفراد، كتابة وتوزيع البرامج دون مقابل ودون إنشاء كيان قانوني. يعد Debian Project<sup>20</sup> مثالاً بارزاً لمشروع مفتوح المصدر بدون كيان قانوني مرتبط به. يتم استخدام برمجيات Debian في مجالات مثل الطاقة النووية، والنقل بالسكك الحديدية، والأتمتة الصناعية، ومعدات الرعاية الصحية. وفي الوقت التي تتمتع فيه بعض مشاريع برمجيات FOSS بكيان قانوني يوفر الحوكمة أو الرعاية أو حتى التوظيف، إلا أن معظمها لا يتمتع بهذا الكيان. وسوف نرى لاحقاً أن نظام اسم النطاق غير عادي في هذا الصدد، حيث تقوم أربع منظمات صغيرة بصيانة برمجيات FOSS بشكل احترافي.

<sup>20</sup> مؤسسة Debian. "فلسفتنا: لماذا وكيف نقوم بذلك"، على الرابط <https://www.debian.org/intro/philosophy>

### 3.3 الأنظمة الاحتكارية تعتمد على برمجيات FOSS

لقد ثبت أن خصائص برمجيات FOSS تنطبق على الأنظمة التي هي في حد ذاتها احتكارية (وليس البرمجيات المجانية المفتوحة المصدر FOSS). ويرجع ذلك إلى حقيقة أن الأنظمة الاحتكارية الحديثة تعتمد غالبًا على برمجيات FOSS للعمل. وأصبحت أدوات ومكتبات برمجيات FOSS موجودة في كل مكان في تطوير ونشر البرمجيات الاحتكارية. على سبيل المثال، لا يتم إنتاج معظم البرمجيات بدون ترجمات برمجية أو بيئات وقت التشغيل؛ ولا يمكن للبرامج تخزين الكائنات أو البيانات المنظمة بدون مخازن الكائنات أو قواعد البيانات؛ ولا يمكن للبرامج التواصل مع المكونات الأخرى بدون تسهيل تمرير الرسائل. ويتم توفير هذه الوظائف الخلفية عادةً بواسطة برمجيات FOSS.

وفي الحالة الخاصة لنظام اسم النطاق DNS، توفر Cloudflare مثالاً مفيداً. تدير Cloudflare خدمة مُحلِّل نظام اسم النطاق العامة واسعة الاستخدام والتي تُعرف باسم "1.1.1.1". تم تقديم الخدمة في البداية بنجاح باستخدام Knot Resolver، وهو برمجية FOSS؛ ومع ذلك تم استبداله لاحقاً ببرنامج احتكاري تم تطويره داخلياً.<sup>21</sup> تم كتابة البرنامج الخاص الذي يعمل ضمن خدمة 1.1.1.1 بلغة Rust، وهي لغة برمجة يتم توفير مواصفاتها وتنفيذها المرجعي وترجمتها البرمجية كبرمجية FOSS وذلك من قبل مؤسسة غير ربحية.<sup>22</sup> وهو يستخدم tokio،<sup>23</sup> وهو وقت تشغيل غير متزامن وهو أيضاً من برمجيات FOSS. ويتم تشغيله على Linux، وهو نظام تشغيل برمجيات FOSS، وهو محاط بمجموعة كبيرة من مكونات برمجيات FOSS الأخرى التي توفر إمكانية المراقبة وغيرها من الضروريات التشغيلية.<sup>24</sup> ويعمل برنامج Cloudflare الاحتكاري خلف خدمة 1.1.1.1 على نطاق واسع بفضل برمجية FOSS، وليس على الرغم منها.

### 3.4 نقاط القوة الكامنة في برمجيات FOSS في منظومة نظام اسم النطاق DNS

لا يعد نموذج برمجيات FOSS مجرد بناء نظري؛ فمبادئه تترجم إلى فوائد ملموسة جعلته النموذج السائد لبرمجيات البنية التحتية لنظام اسم النطاق. إن الحريات في دراسة البرامج ومشاركتها وتحسينها تعمل بشكل جماعي على خلق بيئة تعزز الشفافية والمرونة والابتكار. وهذه ليست نتائج ثانوية عرضية، بل هي نقاط قوة متأصلة في نموذج برمجيات FOSS والتي أثبتت أنها مناسبة بشكل خاص لمتطلبات بناء وصيانة البنية الأساسية الحيوية للإنترنت. وتوضح الأقسام التالية نقاط القوة المحددة المذكورة.

#### 3.4.1 الشفافية والأمن التعاوني

تستفيد عمليات تنفيذ نظام اسم النطاق مفتوحة المصدر من الشفافية. إن توافر الكود المصدر لعمليات تنفيذ برمجيات FOSS قد مكّن مجتمعاً عالمياً من المطورين والباحثين والمشغلين من تحديد الثغرات الأمنية ومعالجتها، في كثير من الأحيان بشكل أسرع

<sup>21</sup> أنبانغ فين، ومارك فافروسا. "كيف تدعم Rust وWasm خادم الحل 1.1.1.1 المقدم من شركة Cloudflare". مدونة Cloudflare، في 28 فبراير/شباط 2023. <https://blog.cloudflare.com/big-pineapple-intro/>.

<sup>22</sup> مؤسسة Rust Foundation. نبذة عنا - الرسالة، القيادة، مجلس الإدارة. <https://rustfoundation.org/about/>.

<sup>23</sup> موقع Tokio. "نبذة تعريفية" <https://tokio.rs/tokio/tutorial>.

<sup>24</sup> جون غراهام كامينغ "منصة CloudFlare والبرمجيات مفتوحة المصدر: طريق ثنائي الاتجاهات". مدونة Cloudflare، بتاريخ 7 أكتوبر/تشرين الأول 2013. على الرابط <https://blog.cloudflare.com/open-source-two-way-street/>.

من الأنظمة الاحتكارية. لقد كانت موضوعًا مهمة على نحو فعال للدراسة من قبل المجتمعات الأكاديمية والأمنية لعقود من الزمن،<sup>25</sup> مما أدى إلى الإبلاغ عن الثغرات الأمنية في بروتوكول نظام DNS وفي عمليات تنفيذ المصدر المفتوح.<sup>26</sup>

إذا تم تحديد الثغرات الأمنية، فإن الروابط الوثيقة بين المجموعات الثلاث تسمح بمعالجة أي مشكلة خطيرة في الوقت المناسب وتنسيق الإفصاحات وإصدارات التصحيحات، مما يضمن تأمين خوادم نظام DNS المهمة (مثل خوادم الجذر) بشكل كامل قبل نشر المعلومات للعامة، وتحديث جميع الخوادم الأخرى على الفور.

وفي استطلاع بين مشغلي البنية التحتية لنظام اسم النطاق (انظر الملحق ج)، أشار المشاركون إلى أنهم يقدرون الرؤية الواضحة لشفافية سلسلة التوريد الخاصة بهم باعتبارها سمة قوية تسمح لهم بتسريع تصحيح الثغرات الأمنية في تبعيات البرمجيات لخدمة نظام اسم النطاق DNS التي يديرونها. على سبيل المثال، انظر الردود التالية:<sup>27</sup>

يكشف المصدر المفتوح بسرعة عن أي عيوب -- سواء كانت متعلقة بالأمن أو غير ذلك -- ويتم تصحيحها وتوزيع التصحيحات بشكل أسرع بكثير من أي كيان تجاري.

وفي كثير من الأحيان، قامت الكيانات التجارية الكبيرة مثل [مخفي] و [مخفي] و [مخفي] على مدار سنوات بإصدار تصحيحات أمنية بعد فترة طويلة من اكتشاف الثغرة الأمنية.

نحن نؤكد دائمًا أن استخدام برمجيات FOSS هو في مصلحة الجميع، سواء المستخدمين أو المستهلكين لخدماتنا. وهذا يسمح لهم بالتأكد من أننا نستخدم مكونات برمجيات سليمة. وفي الحالات النادرة التي يتم فيها اكتشاف مشكلة أمنية في البرنامج الذي نستخدمه، تتم مناقشتها بشكل مفتوح وإصلاحها بأقصى سرعة -- على عكس ما نراه مع البرامج الاحتكارية.

هناك الكثير من الأمثلة على البرامج الاحتكارية التي تعاني من مشاكل أمنية وسجلات تعقب ضعيفة فيما يتعلق بالشفافية أو الإصلاحات. لقد قام مجتمع برمجيات FOSS بعمل أفضل من معظم البائعين في كلا الأمرين.

وتمت مناقشة استخدام وإدارة برنامج نظام اسم النطاق لبرمجيات FOSS بشكل فعال وعلمي من قبل المشغلين. يحتوي كل نظام من أنظمة برامج نظام اسم النطاق DNS الرائدة على قائمة بريدية عامة مفتوحة للمستخدمين،<sup>28</sup> وقاعدة بيانات عامة قابلة للقراءة عالميًا للأخطاء أو المشكلات.<sup>29</sup> ويتعاون مجتمع نظام اسم النطاق في العمليات والأبحاث عبر منظمات هذه الصناعة، ومركز عمليات وتحليلات وأبحاث نظام اسم النطاق (DNS-OARC).<sup>30</sup> وتساهم ثقافة التواصل المنفتح هذه في زيادة الوعي

<sup>25</sup> على سبيل المثال، راجع الورقة البحثية المقدمة من بول فيكسي، بعنوان "DNS and BIND Security Issues" (نظام أسماء النطاقات ومشكلات أمن BIND) في وقائع الندوة الخامسة لأمن *USENIX UNIX*، في مدينة سولت ليك سيتي بولاية يوتا، في عام 1995 على الرابط [https://www.usenix.org/legacy/publications/library/proceedings/security95/full\\_papers/vixie.pdf](https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/vixie.pdf).

<sup>26</sup> لتوضيح مفهوم "موضوع الدراسة النشط"، انظر، على سبيل المثال، ملخص النتائج من 23 ورقة بحثية نُشرت في عام 2024 حول أمن نظام اسم النطاق، كما قدمها تشاوي لو، بعنوان "Summarizing DNS & Security Academic Papers Published in 2024" (عرض تقديمي في اجتماع ICANN82، في سياتل بواشنطن العاصمة، في 12 مارس/آذار 2025)، على الرابط [https://static.sched.com/hosted\\_files/icann82/7b/1.1%20chaoyi-dnspapers2024-0304.pdf](https://static.sched.com/hosted_files/icann82/7b/1.1%20chaoyi-dnspapers2024-0304.pdf).

<sup>27</sup> اللجنة الاستشارية للأمن والاستقرار التابعة لمؤسسة ICANN، "استطلاع ICANN SSAC حول التأثيرات المتوقعة للوائح مفتوحة المصدر على البنية التحتية لنظام اسم النطاق"، اتصالات شخصية، فبراير/شباط 2025.

<sup>28</sup> على سبيل المثال، راجع قوائم البريد العامة المدرجة من قبل CZnic على الرابط <https://lists.nic.cz/postorius/lists/knot-resolver->، و NLnet Labs على الرابط <https://www.nlnetlabs.nl/support/mailling-lists/>، و PowerDNS على الرابط <https://mailman.powerdns.com/mailman/listinfo/>.

<sup>29</sup> على سبيل المثال، راجع تعقب المشكلات لـ CoreDNS على الرابط <https://github.com/coredns/coredns/issues> وأيضًا BIND 9 على الرابط <https://gitlab.isc.org/isc-projects/bind9/-/issues/>.

<sup>30</sup> مركز عمليات وتحليلات وأبحاث نظام اسم النطاق. "مقدمة تعريفية حول مركز عمليات وتحليل وأبحاث نظام أسماء النطاقات DNS-OARC" بتاريخ 3 يوليو/تموز 2008. على الرابط <https://www.dns-oarc.net/oarc/info>.

بشكل أسرع وأوسع بالمشكلات التشغيلية، وأخطاء البرامج، وعدم التوافق بين عمليات التنفيذ، وأخطاء المشغل التي تؤثر على أجزاء أخرى من النظام.

### 3.4.2 الاستقرار والدعم طويل الأمد

تعتمد برمجيات FOSS بشكل عام على الصيانة التطوعية، والتي تتم في أغلب الأحيان من قبل شخص واحد. في حالة نظام DNS، يتم إنشاء أربعة حلول مفتوحة المصدر رائدة من قبل أربع منظمات مختلفة (ثلاث مؤسسات غير ربحية وشركة تجارية واحدة) من بلدان ومناطق متعددة في أمريكا الشمالية وأوروبا.<sup>31</sup> وقد بدأت هذه المنظمات الأربع في الأيام الأولى لاعتماد الإنترنت على نطاق واسع، وحققت الاستقرار في مصادر إيراداتها وتنظيمها الداخلي. كل واحدة من هذه المنظمات تقود تطوير برامجها من خلال كتابة كود جديد ومراجعة وتدقيق مساهمات الكود من المجتمعات النشطة المنتشرة في جميع أنحاء العالم. إن الالتزام طويل الأمد من قبل هذه المنظمات الراحية والتحكم الفني المركزي في تغييرات البرمجيات يساعد في التخفيف من المخاوف المتعلقة بالجودة والأمان والموثوقية الشائعة في مشاريع برمجيات FOSS التي تم تطويرها دون ضوابط فنية قوية. إن ثقافة المجتمع الفني لنظام DNS المفتوح المصدر تتطلب من المتسلل بذل جهد مستمر وطويل الأمد لبناء العلاقات والسمعة المطلوبة لدور موثوق به.

### 3.4.3 المرونة التشغيلية من خلال التنوع

إن التوفر العالي المطلوب لخدمات نظام اسم النطاق يعني الحاجة إلى التكرار وتجنب نقاط الفشل الفردية. وبالنسبة للعديد من المشغلين، يتضمن هذا تشغيل عمليات تنفيذ متعددة مستقلة لنظام اسم النطاق في البرامج. ويمكن للمشغلين الذين يستعينون بمصادر خارجية أن يتبعوا استراتيجية تعدد موفري الخدمات على نحو مماثل. ويؤدي هذا إلى خلق طلب جوهري على وجود حلول متعددة، بحيث يمكن لمشغلي الخدمات عالية الموثوقية تشغيل اثنين أو أكثر في آن واحد وتجنب الاعتماد على أي مطور برامج فردي أو التعرض بالكامل للمشاكل في أي منتج واحد. إن توافر برنامج نظام اسم النطاق لبرمجيات FOSS يخفف العوائق أمام المنظمات التي تريد تشغيل البنية التحتية الخاصة بها، مما يوفر طريقة للخروج من تركيز السوق والمركزية.<sup>32</sup>

### 3.4.4 محفز النمو الاقتصادي والابتكار

من المعروف أن برمجيات FOSS هي أحد محفزات النمو.<sup>33,34</sup> وكما رأينا، فإن العديد من المنتجات مفتوحة المصدر متاحة بسهولة ومجانية لأي شخص يحتاج إلى برنامج نظام DNS، في أي مكان في العالم. والمستخدمون المحتملون هم موفرو خدمة الإنترنت، وسجلات أسماء النطاقات وأمناء السجلات، ومستخدمو الإنترنت. قد يتمكن الأفراد والمنظمات غير الربحية

<sup>31</sup> حسب الترتيب الأبجدي: CZNIC، وهي جمعية لموفري خدمات الإنترنت التشيكين ("ISP") تأسست في عام 1998؛ و Internet Systems Consortium, Inc. (أو "ISC")، وهي شركة أمريكية غير ربحية تأسست في عام 1994 خصيصًا لدعم أنظمة وبرامج مفتوحة المصدر للبنية التحتية للإنترنت؛ و NLnet Labs، وهي شركة هولندية غير ربحية تأسست في عام 1999 لتطوير المعايير المفتوحة وبرامج مفتوحة المصدر لنظام اسم النطاق والتوجيه بين النطاقات؛ و PowerDNS، وهي شركة هولندية تأسست في عام 1999 لدعم تطوير برامج نظام اسم النطاق المتخصصة لموفري خدمات الإنترنت.

<sup>32</sup> مارك نوتنغهام "RFC 9518: المركزية واللامركزية ومعايير الإنترنت". طلب الحصول على الملاحظات والتعليقات. فريق عمل هندسة الإنترنت، في 18 ديسمبر/كانون الأول 2023. على الرابط <https://datatracker.ietf.org/doc/rfc9518>.

<sup>33</sup> "يقدّر التحليل نسبة التكلفة إلى الفائدة بأكثر من 1: 4 ويتوقع أن زيادة بنسبة 10% في مساهمات برمجيات المصدر المفتوح من شأنها أن تولد سنويًا ما بين 0.4% إلى 0.6% إضافية من الناتج المحلي الإجمالي فضلاً عن أكثر من 600 شركة ناشئة إضافية في مجال تكنولوجيا المعلومات والاتصالات في الاتحاد الأوروبي. وتكشف دراسات الحالة أنه من خلال شراء برمجيات مفتوحة المصدر بدلاً من البرمجيات الاحتكارية، يمكن للقطاع العام أن يقلل من التكلفة الإجمالية للملكية، ويتجنب الاحتكار من قبل البائعين، وبالتالي زيادة استقلاليته الرقمية." من المفوضية الأوروبية. الإدارة العامة لشبكات الاتصالات والمحتوى والتكنولوجيا. تأثير البرمجيات والعتاد مفتوح المصدر على الاستقلالية التقنية والتنافسية والابتكار في اقتصاد الاتحاد الأوروبي. تقرير دراسة نهائي. لوكسمبورغ: مكتب المنشورات، 2021. <https://data.europa.eu/doi/10.2759/430161>.

<sup>34</sup> ناتاليا لانغبيرد رايت، وفرانك نيغل، وشين غرينشتاين. "Open Source Software and Global Entrepreneurship" (البرمجيات مفتوحة المصدر وريادة الأعمال العالمية). *Research Policy*، 52، رقم 9 (2023): 104846. على الرابط <https://doi.org/10.1016/j.respol.2023.104846>.

والشركات الناشئة والخبراء المعنيين الذين قد لا يتمكنون من تحمل تكلفة تراخيص البرامج الاحتكارية من الحصول على البرامج التي يحتاجون إليها مجانًا. وكما ذكر أحد المشاركين في استطلاع رأي مشغلي نظام اسم النطاق (انظر الملحق ج): "أكبر مخاوف اليوم هو أننا نستخدم العديد من مكونات المصدر المفتوح في أجزاء غير حرجة من مجموعتنا، والتي لا نملك عقود دعم لها، وبالتالي لا نستطيع تحمل تكاليف الترخيص حتى لو كان متاحًا".<sup>35</sup>

إن وجود حلول متعددة لبرنامج FOSS DNS له تأثير إيجابي على التطور التقني والتجاري لاستخدام الإنترنت والبرمجيات والخدمات عبر الإنترنت بشكل عام، سواء كانت مفتوحة المصدر أو احتكارية. وتعتمد العديد من الأنظمة الاحتكارية والخدمات المستضافة بشكل كبير على مكونات مفتوحة المصدر للوظائف الحيوية؛ وتعتمد العديد من المنصات الاحتكارية للخدمات السحابية وعبر الإنترنت على أحد منتجات FOSS DNS كمكون.<sup>36</sup> وفي الوقت نفسه، يعتمد جزء كبير من البنية التحتية لنظام DNS على مكتبات التشفير لبرمجيات FOSS مثل OpenSSL. وعلى نحو مماثل، يشكل Linux، وهو نظام تشغيل مفتوح المصدر، الأساس لجزء كبير من البنية التحتية السحابية، وبيئات الخوادم، وأجهزة إنترنت الأشياء (IoT). ويؤكد هذا الدور التأسيسي على التأثير العميق الذي تتمتع به برمجيات FOSS على الابتكار التكنولوجي. وغالبًا ما تتضمن البرامج الاحتكارية أطر عمل برمجيات FOSS هذه أثناء إنشاء تطبيقات أو ميزات مغلقة المصدر فوقها، مما يخلق علاقة تكافلية بين النموذجين.<sup>37</sup>

### 3.4.5 المساهمة في الاستقلالية الرقمية

بما أن استخدام برمجيات FOSS لا يتطلب عمومًا دفع تراخيص أو تعويضات، فإن حجم رأس المال اللازم لبدء مشاريع رقمية جديدة قد يكون أقل من استخدام البرمجيات الاحتكارية. وعلاوة على ذلك، فإن الحرية في دراسة وتغيير وإعادة توزيع كود (شفرة) البرمجيات، التي توفرها برمجيات FOSS، تمكن من نمو المعرفة والمهارات المحلية، مما يؤدي إلى مشاريع بحثية وتجارية جديدة. ولا تتطلب التخصيصات المحلية أو التطورات الإضافية أي ترخيص أو موافقة من واضعي كود البرمجية الأصليين. لا يمكن لأصحاب حقوق النشر الأجانب حظر أي خدمة تعتمد على برمجيات FOSS، حيث لا يمكن إلغاء تراخيص هذه البرمجيات؛ حتى في حالة النزاعات التجارية والحظر، سيظل الكود متاحًا.

### 3.5 المخاطر الكامنة في نموذج برمجيات FOSS

رغم أن نموذج برمجيات FOSS يوفر نقاط قوة كبيرة، فإن خصائصه الفريدة تشكل أيضًا مجموعة متميزة من المخاطر التي تختلف عن المخاطر التي تشكلها البرمجيات الاحتكارية التقليدية. وهذه ليست عيوبًا في النموذج نفسه، بل هي بالأحرى مقابضات متأصلة يجب فهمها وإدارتها، وخاصة عندما يتم استخدام البرنامج في البنية التحتية الحيوية. إن النموذج الاقتصادي، والطبيعة الموزعة للتطوير، والافتقار إلى العلاقات التعاقدية التقليدية، كلها عوامل لها آثار على الاستدامة طويلة الأمد والأمن التشغيلي. وتتناول الأقسام التالية هذه المخاطر الكامنة بالتفصيل.

<sup>35</sup> اللجنة الاستشارية للأمن والاستقرار، "استطلاع اللجنة الاستشارية للأمن والاستقرار في ICANN حول التأثيرات المتوقعة للتنظيم مفتوح المصدر على البنية التحتية لنظام أسماء النطاقات".

<sup>36</sup> في الوقت الحالي، لا يوجد أي مصدر مستقل يدعم هذا الادعاء. ومع ذلك، واستنادًا إلى التحقيق الذي أجراه المؤلفون بشكل جماعي في هذه الوثيقة، يمكننا أن نؤكد بثقة أن هذه هي الحال. وهناك قضايا تتعلق بالسرية تتعلق بالكشف علنًا عن المنصة التي تستخدم أي خدمة على وجه التحديد، وبالتالي فإن هذا البيان مبرر تمامًا دون توثيق مناسب.

<sup>37</sup> جيف غورميك. "سياسة البرمجيات مفتوحة المصدر في توازن الصناعة". ورقة عمل، تقرير فني، 2024. على الرابط [https://jeffgortmaker.com/files/Open\\_Source\\_Software\\_Policy\\_in\\_Industry\\_Equilibrium.pdf](https://jeffgortmaker.com/files/Open_Source_Software_Policy_in_Industry_Equilibrium.pdf)

### 3.5.1 الاستدامة المالية وإرهاق المسؤولين

أحد التهديدات الرئيسية التي تواجه نظام اسم النطاق هي مشكلة الاستدامة المالية العامة لبرمجيات FOSS. ويفصل النموذج بين التمويل والاستخدام (القسم 3.2.3)، مما يتيح التنبؤ على نطاق واسع، ولكنه يسمح أيضًا بالركوب المجاني،<sup>38</sup> حيث قد يعتمد العالم بأسره على البرامج التي يتم تمويلها من قبل قلة من الناس.<sup>40:39</sup>

وكما أشار تقرير صادر عن مجموعة استشارات تكنولوجيا الإنترنت ذات النطاق العريض (BITAG):

هناك فجوة بين شراء معدات الشبكة من خلال عقود الدعم الباهظة الثمن والفشل في تمويل البرمجيات مفتوحة المصدر التي تعتمد عليها هذه المعدات في كثير من الحالات. وفي كثير من الأحيان، يكون الموظفون الفنيون لدى مشغلي الشبكات على استعداد لدعم التطوير، ولكن هيكلهم المؤسسي لا يسمح لهم بذلك لأن مثل هذه البرامج ليست شيئًا يمكن شراؤه في صندوق مغلف وبعقد دعم. إن رعاية تطوير ميزة ما قد تكون مشكلة، لأن الافتراض التلقائي الذي تتبناه الأقسام القانونية هو أن تطوير البرمجيات يؤدي إلى امتلاك الراعي [حصريًا] للملكية الفكرية، وهو ما يتعارض مع نموذج برمجيات FOSS.<sup>41</sup>

في الوقت الذي يتم فيه صيانة عمليات تنفيذ نظام اسم النطاق مفتوحة المصدر الأربعة الرائدة من قبل المنظمات التي حققت الاستقرار المالي والتنظيمي المستدام، إلا أن هذه المنظمات كلها صغيرة. إن أيًا من هذه المؤسسات قد يتعرض لزعزعة الاستقرار إذا تعرض مصدر تمويلها للتهديد، أو إذا فرضت عليها القواعد التنظيمية أعباءً تتجاوز قدرتها على تحمل التكاليف المرتبطة بذلك. وفي حالة عدم صيانة أحد أنظمة المصدر المفتوح الرائدة أو عدم توفره بالكامل، فقد يكون التأثير على نظام اسم النطاق كبيرًا.

ينطبق هذا بشكل خاص على الأدوات الأساسية التي تتطلب صيانة مستمرة ولكنها منفصلة عن العمليات التجارية الأساسية لمستخدميها. وإن عمليات تنفيذ نظام اسم النطاق مفتوحة المصدر الأربعة الأكثر شيوعًا مدعومة من قبل فرق تطوير لا يزيد عدد أفرادها على اثني عشر مهندسًا أو نحو ذلك، لذا فإن إضافة متطلبات المشروع التي قد تستهلك ما يعادلها من الموظفين بدوام كامل، على سبيل المثال، ستكون عبئًا كبيرًا.

ويتم تمويل مشرفي الصيانة مدفوعي الأجر بعدة طرق، بعضها قد يكون غير متوقع. بالإضافة إلى قبول التبرعات وتقديم الدعم الفني الخاص، تقدم بعض المشاريع للداعمين الماليين إمكانية الوصول المبكر إلى إصلاحات الأخطاء، والدعم للفروع التي

<sup>38</sup> جاستين باباس جونسون. "مقالات في نظرية الاقتصاد المصغر". مقالة مطولة، معهد ماساتشوستس للتكنولوجيا 1999. على الرابط <http://hdl.handle.net/1721.1/9518>

<sup>39</sup> جون كريستوف، وأليكساندر باند، وأونريج فيليب، وجيف أوزبورن. اللجنة: لجنة نظام الدعم التشغيلي للنظم الجوهرية. مجموعة مشغلي شبكات أميركا الشمالية - NANOG رقم 84، في 2022. <https://www.youtube.com/watch?v=vWiW-3jMw7w>

<sup>40</sup> على سبيل المثال، يسلط أحد التقارير الضوء على عدم التوازن بين استخدام برامج التوجيه الأساسية والمساهمات المالية في تطويرها: "نحن نوضح أهمية هذا الخلل بين التمويل والاستخدام... من خلال مثالين. من بين ما يقدر بنحو 2000 عملية تثبيت لبرنامج Routinator RP و1400 شبكة تستخدم برنامج Krill delegated CA، فإن أقل من عشرة منها تمول تطويرها. إن غالبية المشغلين يعتمدون على استقرار البرمجيات واستمرار وجودها وتطويرها في المستقبل، لكنهم لا يساهمون في تحقيق هذه الغاية." مجموعة العمل الفنية في مجموعة الاستشارات الفنية للنطاق العريض (BITAG)، "أمن البنية التحتية لتوجيه الإنترنت"، في 2 نوفمبر/تشرين الثاني 2022، 26، على الرابط [https://www.bitag.org/documents/BITAG\\_Routing\\_Security.pdf](https://www.bitag.org/documents/BITAG_Routing_Security.pdf)

<sup>41</sup> مجموعة العمل الفنية في مجموعة الاستشارات الفنية للنطاق العريض BITAG، "أمن البنية التحتية لتوجيه الإنترنت"، 26.

انتهت صلاحيتها، وتطوير الميزات ذات الأولوية، والوصول إلى الحزم المترجمة مسبقاً وخدمات الأمان الإضافية.<sup>42,43,44,45</sup> ويجب على الجهات التنظيمية أن تكون حذرة حتى لا تحظر عن غير قصد أيًا من هذه الطرق المحتملة لمسؤولي برمجيات FOSS لتمويل عملياتهم.

يعد استخدام برمجيات FOSS لنظام اسم النطاق DNS أمرًا استثنائيًا في سياق وجود منظمات تعمل على مدى طويل لتخصيص مسؤولين عن تشغيل البرمجية. وبالنسبة لاستمرار وجودهم، فإن الخطر يكمن في الاستدامة المالية. ولكن في الحالة العامة، فإن الخطر تحفيزي. يتم صيانة الغالبية العظمى من برمجيات FOSS من قبل فرد واحد، في وقت فراغه.<sup>46</sup> وتتضمن أمثلة برامج نظام اسم النطاق Dnsmasq، برامج نظام اسم النطاق المضمنة في أغلب الأحيان في أجهزة التوجيه الصغيرة غير المكلفة المستخدمة في المنازل والشركات الصغيرة. ويتم صيانتها في الغالب من قبل متطوع واحد بدون أجر في الغالب.<sup>47</sup> وبالمثل، يتم صيانة العديد من مكتبات البرامج الناضجة لبرمجة نظام اسم النطاق على نحو فعال وذلك من قبل فرد واحد في وقت فراغه.<sup>48</sup> يتم دعم تنفيذ نظام اسم النطاق الشهير الآخر، CoreDNS ومكتبة Go DNS الأساسية، على التوالي من خلال جهود المجتمع ومسؤول متطوع (خبير) واحد. وتؤكد هذه الأمثلة على سمة مميزة لمنظومة البرمجيات: إذ يمكن لمنظمة صغيرة أو مطور واحد أن يلعب دورًا حاسمًا في كتابة البرمجيات للبنية التحتية الرقمية العالمية، مع انفصالها تمامًا عن رأس المال أو النفقات التشغيلية لتشغيلها. وبالنسبة لهؤلاء المسؤولين المتطوعين الذين يعملون منفردين، ما لم يتم تمويل هذا العمل باعتباره وظيفتهم الأساسية بدوام كامل، فإن الخطر لا يتمثل في الاستدامة المالية، بل في تحميل المتطوعين عبء العمل المتواصل. ويتعين على الجهات التنظيمية أن تكون حذرة في فرض أعباء إضافية تتجاوز قدرة واستعداد المسؤولين لاستثمار وقتهم الفائض في صيانة ما تشكل في الأساس مشاريع هواة. لقد كان هذا مجالاً فعالاً للدراسة، ومن الأفضل لصناع السياسات أن يأخذوا بعين الاعتبار التوصيات التي قدمها الدارسين للموضوع.<sup>49</sup>

<sup>42</sup> على سبيل المثال، يقدم اتحاد أنظمة الإنترنت خدمة الإخطار المبكر بالثغرات الأمنية. انظر Internet Systems Consortium، "إشعار الاختراق المبكر (EVN)"، على الرابط <https://www.isc.org/evn>.

<sup>43</sup> توفر NLnet Labs، من خلال شركتها التابعة Open NetLabs، خدمات التدريب والاستشارات والدعم الفني وتطوير البرامج. انظر NLnet Labs، "خدمات Netlabs المفتوحة- مكتب استشارات"، <https://nlnetlabs.nl/services/consultancy/>.

<sup>44</sup> توفر PowerDNS مجموعة متنوعة من الخدمات والمنتجات بما في ذلك PowerDNS Protect، وهي خدمة أمان تتضمن قوائم حظر وقائية. راجع "PowerDNS Protect"، على الرابط <https://www.powerdns.com/powerdns-protect>.

<sup>45</sup> للحصول على نظرة عامة على مجموعة متنوعة من أنواع نماذج المنظمات مفتوحة المصدر، راجع "Open Source Archetypes: A"، Open Tech Strategies، Mozilla Corporation، بتاريخ 28 أكتوبر/تشرين الأول 2019، على الرابط [https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS\\_OS\\_Archetypes\\_report\\_ext\\_scr.pdf](https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf).

<sup>46</sup> جوش بريسرز. "Open Source Is One Person". مؤسسة Open Source Security، بتاريخ 28 أغسطس/آب 2025. <https://opensourcesecurity.io/2025/08-oss-one-person/>

<sup>47</sup> "Dnsmasq - خدمات الشبكة للشبكات الصغيرة"، <https://thekelleys.org.uk/dnsmasq/doc.html>.

<sup>48</sup> تتضمن الأمثلة `Net::DNS` للغة البرمجة Perl و `miekg/dns`، وهي مكتبة من نوع Go DNS مستخدمة في Kubernetes و Docker وهيئة شهادة Let's Encrypt. ويمكن العثور على المزيد من الأمثلة للمكتبات في الجدول 7.

<sup>49</sup> Eghbal, Nadia. "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure". Ford Foundation بتاريخ 14 يوليو/تموز 2016. على الرابط <https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure>.

### 3.5.2 مخاطر سلسلة التوريد الناجمة عن التبعيات المشتركة

يعتمد قدر كبير من البرمجيات الحساسة، بما في ذلك برمجيات FOSS والبرامج التجارية، على نفس مكونات برمجية FOSS. وقد يؤثر خطأ فني خطير في مكتبة تشفير برمجيات FOSS الشهيرة<sup>50</sup> على جميع عمليات تنفيذ نظام اسم النطاق.<sup>51</sup> هناك أيضًا مكونات أخرى أقل ظهوراً ويتم إعادة استخدامها بشكل شائع. وهذا ضعف كبير محتمل، ليس فقط في نظام اسم النطاق DNS، وليس فقط في برمجيات FOSS، ولكن بالنسبة للبرمجيات بشكل عام.<sup>52</sup> وتنطبق مخاطر الاستدامة التي ناقشناها أعلاه في القسم 3.5.1 على هذه المكونات المشتركة أيضًا، مما يؤدي إلى تفاقم التهديد.

يتفاقم هذا الخطر بسبب حقيقة أن المساهمين في برمجيات FOSS ذوي النوايا الخبيثة قد يتمكنون من دمج أكواد البرمجيات الخبيثة في مشاريع مفتوحة المصدر أو مكوناتها دون اكتشافها. ويمكن إدخالها من خلال العبث بمستودعات الحزم أو كمساهمات في المشاريع. إن اليقظة خلال فحص ومراقبة تبعيات أكواد البرمجيات أمر ضروري لمنع دمج أكواد البرمجيات الضارة في مشاريع البرمجيات.

### 3.5.3 تأتي برمجيات FOSS المجانية بدون أي ضمان أو ضمان للدعم

تُعد البرمجيات المتاحة مجانًا خيارًا جذابًا نظرًا لأنها تُقدم دون أي تكلفة، وعادةً ما تكون دون بذل أي جهد فيما بعد تنزيل الحزمة نفسها. ولكن نظرًا لأنه لا يأتي مع أي ضمان أو وعد بالدعم، فإن استخدامه ينطوي أيضًا على مخاطر. فتلقائيًا، لا يوجد عقد آخر غير اتفاقية ترخيص المصدر المفتوح بين موفر منتج برمجيات FOSS والمستخدم.<sup>53</sup> وما لم يقيم المستخدم بإجراء ترتيبات الصيانة الخاصة به مع المسؤول أو الآخرين، فلن يكون لديه أي ضمان للصيانة الفعالة أو الدعم.

إذا كان المنتج يعاني من ثغرات أمنية، سواء تم إدخالها عن طريق الخطأ كما هو الحال في خطأ<sup>54</sup> OpenSSL Heartbleed، أو بشكل خبيث كما هو الحال في الباب الخلفي<sup>55</sup> xz Utils، فلا أحد ملزم بتوفير التصحيحات. ففي الوقت الذي يمكن فيه لأي شخص، بما في ذلك المستخدم، ومن الناحية الفنية أخذ نسخة من الكود المصدر وتصحيح المشكلة يدويًا، فإن مثل هذا "التفريع" يتطلب خبرة كبيرة في هندسة البرمجيات وموارد تشغيلية، بحيث لا يكون لدى المستخدم في معظم الحالات أي سيطرة فعالة على توفر الإصلاحات. وتعتبر هذه المشكلة خطيرة بشكل خاص في الحزم التي يتم استخدامها على نطاق واسع، مثل OpenSSL وxz، بحيث لا توجد بدائل متاحة بسهولة. إن مخاطر ما يشار له بمصطلح الزراعة الأحادية في هذا السياق ليست معزولة عن المصدر المفتوح، ولكن قد يكون هذا هو السبب وراء تطبيق هذه المخاطر العامة على برمجيات FOSS.

<sup>50</sup> يعد OpenSSL مثالًا أساسيًا لمكتبة تشفير يتم الاعتماد عليها على نطاق واسع. ولتوضيح حجم هذا الاعتماد، ففي وقت ظهور ثغرة "Heartbleed" في OpenSSL، كان يُعتقد أن 17% من خوادم الويب على الإنترنت المعتمدة من قبل سلطات موثوقة معرضة للهجوم. "Half a Netcraft"، *Netcraft News*، "Million Widely Trusted Websites Vulnerable to Heartbleed Bug"، بتاريخ 8 أبريل 2014، على الرابط <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>

<sup>51</sup> كما هو الحال مع برنامج نظام DNS، فإن تطوير برامج التشفير هو عمل متخصص. وعلى الرغم من وجود بعض تقنيات التشفير لبرمجيات FOSS منذ فترة طويلة، إلا أن التنوع والجودة يمثلان مشكلة.

<sup>52</sup> للحصول على مثال على إحدى المحاولات لجعل التبعيات المشتركة مرئية، راجع "Census III of Free and Open Source Software"، دار *The Linux Foundation*، ديسمبر/كانون الأول 2024: على الرابط <https://www.linuxfoundation.org/research/census-iii>

<sup>53</sup> إن وجود علاقات تعاقدية بين المسؤولين والمشغلين هو مفهوم خاطئ شائع، الذي تم تناوله في القسم 3.2.2.

<sup>54</sup> "Heartbleed Bug"، على الرابط <https://heartbleed.com/>

<sup>55</sup> دان غودين. "What We Know about the xz Utils Backdoor That Almost Infected the World". *Ars Technica*. أبريل/نيسان 2024. على الرابط <https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/>

إن انخفاض اهتمام المجتمع بتوفير الصيانة لبرمجيات FOSS قد يبدو بمثابة حافز لدخول المنظمات التي تقدم الصيانة بموجب عقد. ومع ذلك، فإن التغييرات التي تطرأ على قاعدة أكواد البرمجيات من قبل هذه المنظمات الداعمة عادة ما يتم إرسالها مرة أخرى إلى مشروع برمجيات FOSS لتقليل العبء المتمثل في الحفاظ على قاعدة أكواد برمجيات منفصلة. وهذا بدوره يسمح للأخريين بالاستفادة من هذه الصيانة دون أن يدفعوا لأنفسهم. ويؤدي هذا إلى مشكلة الراكب المجاني: عندما يستخدم موفر الخدمة برمجيات FOSS ولكنه لا يساهم في صيانتها، فقد يفعل ذلك بتكلفة أقل من المنافس الذي يفعل ذلك، مما يقلل من قيمته.<sup>56</sup>

يمكن التخفيف من مشكلة عدم وجود ضمان أو دعم جوهري. يمكن للمشغلين تدريب الخبراء الموجودين في فريق العمل والاحتفاظ بهم، وتمويل أو توظيف المسؤولين،<sup>57</sup> أو الدخول في عقود دعم للحصول على إمكانية الوصول إلى الخبرة من المسؤولين أو المساهمين الخبراء.<sup>58</sup> ويوضح تقرير BITAG المذكور في القسم 3.5.1 العقبات التنظيمية التي تمنع المشغلين من القيام بذلك.

#### 3.5.4 المخاطر التشغيلية في النشر

إن الطبيعة الموزعة لبرمجيات FOSS تخلق تحديات تشغيلية تتعلق بأصالة البرمجيات، وتحديثها، ونقص المشغلين المهرة.

##### *التحقق من أصالة البرامج*

يتم توزيع برمجيات FOSS بحرية عبر الإنترنت، وبالتالي قد تكون عرضة للاختطاف أو الاستبدال بكواد مزيف. وبسبب هذه المخاطرة، يتم توقيع برمجيات FOSS بشكل روتيني من قبل المسؤول، باستخدام طرق تشفير قوية. ويمكن للمستخدم التحقق من هذه التوقيعات للتأكد من سلامة البرنامج. ويتم توقيع جميع عمليات التنفيذ لنظام اسم النطاق للبرمجيات المجانية مفتوحة المصدر FOSS DNS الأكثر شيوعاً المستخدمة في البنية التحتية للإنترنت. ومع ذلك، لا يجوز للمستخدمين التحقق من هذه التوقيعات، أو الحصول على البرمجيات عبر وسطاء لا يتحققون من سلامة البرنامج أو يحافظون على سلامتها بأي طريقة أخرى.

##### *نقص المعلومات حول عمليات النشر وسرعة التصحيحات*

هناك اهتمام شديد من قبل الباحثين في مجال البحث عن الثغرات الأمنية في برمجية FOSS DNS وسجل رصين من الحقائق المستحصل عليها وعن طرق الإبلاغ عنها. يتبع كل بائعي برمجيات نظام DNS الرواد أفضل الممارسات المقبولة عموماً للتعامل مع الثغرات الأمنية في البرمجية وإصلاحها والكشف عنها. ومع ذلك، لا يوجد مصدر موثوق للمعلومات حول ما إذا كان المستخدمون يقومون بتحديث برامجهم إلى الإصدارات الحالية المحسنة، وبأي سرعة يقومون بذلك.

في مجال برمجيات FOSS بشكل عام، هناك بيانات محدودة للعمل بها لتقييم هذا الخطر. إن حقيقة أن مستهلكي البرمجيات يحصلون عليها في كثير من الأحيان من خلال جهة أخرى – وهو جهة تصنيع أنظمة التشغيل، أو أحد المتحمسين لبرمجيات FOSS والذي ربما قام بنسخ البرنامج وإعادة توزيعه – تجعل تتبع نشر التحديثات أكثر صعوبة. ويمكن معالجة هذا الخطر من خلال وضع لوائح تتطلب من المشغلين تقديم نوع ما من الإبلاغ المركزي حول أي برنامج يعتبر بالغ الأهمية لعمليات الإنتاج الخاصة بهم.

<sup>56</sup> على سبيل المثال، أشارت إحدى جمعيات الأعمال الألمانية لمطوري برمجيات FOSS إلى هذه المسألة باعتبارها مشكلة في المشتريات العامة لبرمجيات FOSS. انظر مجموعة عمل المشتريات في Open Source Business Alliance، بعنوان "Selection Criteria for the Sustainable Procurement of Open Source Software"، لـ Open Source Business Alliance، بتاريخ 11 فبراير/شباط 2025، على الرابط <https://osb-alliance.de/publikationen/veroeffentlichungen/selection-criteria-for-the-sustainable-procurement-of-open-source-software>.

<sup>57</sup> فيليبو فالسوردا. بعنوان "I'm Now a Full-Time Professional Open Source Maintainer"، بتاريخ 2 فبراير/شباط 2023. على الرابط <https://words.filippo.io/full-time-maintainer/>.

<sup>58</sup> تتوفر عقود الدعم للعديد من أنظمة برمجيات FOSS المذكورة في هذا التقرير.

#### الاستعانة بمصادر خارجية ونقص المهارات

إن تعقيد التشغيل الصحيح لبرمجيات FOSS يشكل مشكلة، وذلك بسبب وجود نقص في المشغلين المهرة في بعض المناطق في العالم. ويؤدي هذا الجمع بين الأهمية والتعقيد إلى دفع بعض صناع القرار إلى الاستعانة بخدمات سحابية، وهو ما قد يضعف التنوع والطبيعة الموزعة للنظام، مما قد يقلل من المرونة والأمان. على سبيل المثال، إذا اختار الجميع في منطقة ما موفر خدمة بريد إلكتروني مستضاف شائعاً لأن ذلك أسهل من بناء وتشغيل وصيانة خوادم البريد الإلكتروني الخاصة بهم، فإن توفر البريد الإلكتروني داخل المنطقة بأكملها يتحدد من خلال استقرار موفر بريد إلكتروني واحد.

هناك أيضاً تحول جيلي في المؤسسات وموفري الخدمات الأصغر حجماً، حيث أصبح الموظفون في بداية حياتهم المهنية يعتمدون على الخدمات السحابية وأصبحوا أقل دراية بتشغيل خدمات الشبكة الخاصة بهم. وتقوم العديد من المنظمات بإدارة فعاليات تدريبية للمشغلين (APNIC و NSRC و PCH) لتطوير مهارات نظام اسم النطاق وإدارة الشبكات الأخرى. وتحاول مشاريع برمجيات FOSS معالجة هذه المشكلة باستخدام حزم مجمعة مسبقاً وميزات سهلة الاستخدام، ولكن لا يزال من الصعب التنافس مع البدائل التي تقدمها البرمجيات كخدمة.

## 4 انتشار برمجيات FOSS في البنية التحتية لنظام DNS وتسجيل أسماء النطاقات

تلعب برمجيات FOSS دوراً حاسماً ومهمناً في العمليات الفنية لأسماء النطاقات وأنظمة التسجيل على الإنترنت. وفي الأجزاء الأكثر أهمية من هذه البنية التحتية، تعد برمجيات FOSS هي القاعدة، بينما تشكل البرمجيات الاحتكارية الاستثناء. ويؤكد البحث الذي أجراه هذا التقرير أن البنية التحتية العالمية والموزعة لنظام اسم النطاق تعتمد على برمجيات FOSS. وعلى الأقل تسعة من أصل 12 مشغلاً لنظام خادم الجذر على الإنترنت يستخدمون عمليات التنفيذ لنظام اسم النطاق للبرمجيات المجانية مفتوحة المصدر FOSS DNS. وعلى نحو مماثل، يستخدم تسعة من أكبر 10 موفري خدمات نطاقات المستوى الأعلى برمجيات FOSS. وفي مجال تسجيل أسماء النطاقات، في حين أن العديد من الأنظمة الكبيرة هي أنظمة احتكارية، إلا أنها مبنية بشكل كبير على مكونات برمجيات FOSS، كما أن كبار موفري خدمات ضمان البيانات للسجلات وأمناء السجلات قائمون أيضاً على برمجيات FOSS. وتوضح الأقسام التالية بالتفصيل مدى انتشار برمجيات FOSS في كل مكون من مكونات هذه البنية التحتية الحيوية. والمنهجية موصوفة في الملحق ب.

### 4.1 برمجيات FOSS في البنية التحتية لتسجيل أسماء النطاقات

تشير البنية التحتية للتسجيل إلى الأنظمة التي تسهل تسجيل أسماء النطاقات الفردية، والتي تجعل أسماء النطاقات المسجلة متاحة في نظام اسم النطاق العام. ورغم عدم توفر بيانات واضحة عن المدى الكامل لاستخدام برمجيات FOSS، فإن الأدلة تشير إلى اعتماد كبير على هذه البرمجيات، سواء كنظم كاملة أو كمكونات أساسية.

ويحافظ عدد من مشغلي السجلات على البنية الأساسية للتسجيل والتي تعتمد بالكامل على برمجيات FOSS (الجدول 1). على سبيل المثال، من المعروف أن منصة سجل FRED تُستخدم من قبل ما لا يقل عن 12 سجلاً لنطاقات ccTLD، وتُستخدم منصة Nomulus من قبل العديد من سجلات gTLD.

## الجدول 1: أنظمة برمجيات FOSS المستخدمة في عمليات التسجيل

نظام البرمجيات	رخصة مفتوحة المصدر	مستخدم من قبل
<a href="#">FRED</a>	<a href="#">GPLv3</a>	يتم استخدام FRED (على الأقل) من قبل نطاقات ccTLD الخاصة بألبانيا وأنغولا والأرجنتين والبوسنة والهرسك وكوستاريكا وجمهورية التشيك وليسوتو وماكاو وملاوي ومقدونيا الشمالية وباراغواي وتنزانيا.
<a href="#">Internet ee domain registry</a>	<a href="#">MIT</a>	نطاق ccTLD لإستونيا (.ee).
<a href="#">Namingo</a>	<a href="#">MIT</a>	Namingo مصمم لبرنامج نطاقات gTLD الجديدة التابع لمؤسسة ICANN لعام 2026: الجولة القادمة.
<a href="#">Nomulus</a>	<a href="#">Apache 2.0</a>	سجلات gTLD الخاصة بـ Google، بما في ذلك .app، وما إلى ذلك.

## الجدول 2: أنظمة السجلات المبنية على مكونات برمجيات FOSS

نظام التسجيل/خدمة الواجهة الخلفية	أمثلة على مكونات مفتوحة المصدر قيد الاستخدام	السجل قيد الاستخدام من قبل
<a href="#">Afnic</a>	خادم ويب، قاعدة بيانات	20 نطاق TLD، بما في ذلك .fr
<a href="#">CIRA / SIDN / Hello Registry</a>	قاعدة بيانات، خادم ويب، خادم تطبيقات، إبلاغ، واجهة أمامية	6 نطاقات ccTLD، و6 نطاقات gTLD، بما في ذلك .ie و .ca
<a href="#">CoCCA</a>	خادم ويب، خادم تطبيقات، قاعدة بيانات	56 نطاق ccTLD
<a href="#">CORE Association</a>	خادم ويب، قاعدة بيانات، مكتبات جافا	1 نطاق ccTLD، و21 نطاق gTLD
<a href="#">GoDaddy Registry</a>	قاعدة بيانات، خوادم تطبيقات، إبلاغ، مراقبة، تسجيل، اختبار، واجهة أمامية، نظام اسم النطاق	أكثر من 200 نطاق TLD
<a href="#">Identity Digital</a>	قاعدة بيانات	250 نطاقًا من نوع gTLD و ccTLD بما في ذلك نطاقات المستوى الأعلى لرموز البلدان .pr و .me و .au
<a href="#">Nominet</a>	قاعدة بيانات، خادم تطبيقات، تحليل، تسجيل، اختبار، واجهة أمامية، خادم أسماء	أكثر من 85 نطاق TLD، بما في ذلك .uk
<a href="#">TANGO Registry Services</a>	خادم ويب، قاعدة بيانات، مكتبات جافا	8 نطاقات gTLD
<a href="#">Tu cows Registry</a>	قاعدة بيانات، برنامج نظام اسم النطاق وأدوات الملحقات، خوادم ويب وبريد إلكتروني، طوابير رسائل، تنسيق البنية التحتية والافتراض، نظام تشغيل	222 نطاق "TLD"، بما في ذلك SLD المُدارة ك نطاقات TLD، بما في ذلك .my و .com.my
<a href="#">Verisign<sup>59</sup></a>	(لم يتم توفير أي شيء)	نطاقات .com و .net و .edu ونطاقات TLD أخرى

<sup>59</sup> قدمت Verisign البيان التالي لهذا التقرير: تستخدم Verisign منصة احتكارية لحل نظام اسم النطاق تسمى نظام البحث والتحليل المتقدم للمعاملات (ATLAS). وتستخدم Verisign أيضًا بنية أساسية مخصصة للتسجيل والحل المبني على الغرض باستخدام مجموعة متنوعة ومنسقة من مكونات البرامج التجارية والمفتوحة المصدر للتكرار.

على النقيض من ذلك، غالبًا ما تستخدم السجلات الأكبر ووحدات السجلات الخلفية أنظمة احتكارية. ومع ذلك، لا يتم بناء هذه الأنظمة عادةً من الصفر؛ بل إنها غالبًا ما تكون مبنية على ملحقات وتكاملات احتكارية ومخصصة للمكونات – مثل قواعد البيانات وخوادم الويب – والتي هي في الغالب من برمجيات FOSS (الجدول 2).

وينطبق هذا الاعتماد على برمجيات FOSS أيضًا على خدمات ضمان البيانات، التي تخزن نسخًا آمنة من بيانات تسجيل النطاق. لقد قامت أكبر ثلاث جهات مقدمة لهذه الخدمات لكل من السجلات وأمناء السجلات ببناء أنظمتها على الأقل جزئيًا على مكونات برمجيات FOSS (الجدول 3).

الجدول 3: برمجية FOSS في وكلاء ضمان البيانات

وكيل ضمان البيانات	للسجلات	لأمناء السجلات	تدمج برمجيات FOSS في الوظائف الرئيسية؟
<a href="#">Beilong Zedata (Beijing) Data Technology Co., Ltd</a>	✓	✓	لا
<a href="#">China Internet Network Information Center (CNNIC)</a>	✓	✓	لا
<a href="#">China Organizational Name Administration Center (CONAC)</a>	✓	✓	لا
<a href="#">DENIC Services GmbH &amp; Co. KG</a>	✓	✓	نعم جزئيًا
<a href="#">Escrow4All</a>	✓		نعم
<a href="#">Joint Stock Company Internet Exchange "MSK-IX"</a>	✓	✓	غير معروف
<a href="#">NCC Group</a>	✓		نعم جزئيًا
<a href="#">مركز تايوان لمعلومات الشبكة (TWNIC)</a>	✓		لا

لم يتم قياس أو مسح البنية التحتية لأمين السجل لهذا التقرير. ونعقد أنه من المحتمل أن يستخدم أمناء السجلات بانتظام ملحقات وتكاملات احتكارية ومخصصة للمكونات التي هي في الغالب من نوع برمجيات FOSS. على سبيل المثال، يستخدم بعض أمناء السجلات برنامج خادم الويب nginx أو Apache لتشغيل بوابات الويب الخاصة بهم للمسجلين. كما وأنهم يستخدمون حلول برمجيات FOSS لمراقبة البرامج، وتحليل البيانات، وإدارة أكواد البرمجيات، والاحتياجات الأخرى.

## 4.2 برمجيات FOSS في البنية التحتية لنشر نظام DNS (الخوادم الرسمية)

إن الدليل على هيمنة برمجيات FOSS يكون أكثر وضوحًا في البنية التحتية التي تنشر معلومات النطاق. في أعلى مستويات التسلسل الهرمي لنظام اسم النطاق DNS – الجذر ونطاقات TLD – تكون برمجيات FOSS موجودة في كل مكان تقريبًا.

نظام خادم الجذر هو المستوى الأعلى في التسلسل الهرمي لنظام اسم النطاق. ومن بين المنظمات المستقلة البالغة 12 التي تدير خوادم الجذر، هناك على الأقل تسع منظمات تستخدم عمليات تنفيذ نظام FOSS DNS حصريًا للإجابة على الاستعلامات (الجدول 4).

الجدول 4: استخدام برمجيات FOSS في نظام خادم الجذر

المصدر المقترح <sup>60</sup>	البرمجيات	معرف خادم الجذر
جزئيًا <sup>61</sup>	ATLAS (احتكاري) NSD	A, J
نعم <sup>63,62</sup>	Knot BIND9	B
نعم	BIND9	C
نعم	NSD	D
جزئيًا <sup>65</sup>	غير معروف (برمجيات FOSS)، داخلي (احتكاري) <sup>64</sup>	E
جزئيًا	BIND9، داخلي (احتكاري) <sup>66</sup>	F
نعم	BIND9	G
نعم	NSD	H
نعم <sup>67</sup>	سري	I
نعم	BIND9 Knot NSD	K
نعم	Knot NSD	L
نعم <sup>68</sup>	BIND9	M

<sup>60</sup> ويليم توروب وآخرون، "تقرير دراسة تنفيذ RSSAC028" (تقرير، NLnet Labs and Stichting Internet Domeinregistratie Nederland (SIDN)، بتاريخ 27 سبتمبر/أيلول، 2023)، 15، على الرابط <https://www.icann.org/en/system/files/files/rssac028-implementation-study-report-27sep23-en.pdf>.

<sup>61</sup> من بيان Verisign حول توقعات خدمة RSSAC001v2 لخوادم الجذر، "تستخدم Verisign قاعدتين مختلفتين من قواعد أكواد البرمجيات لخدمة جذر نظام اسم النطاق: (1) منصة حل ATLAS الحاصلة على براءة اختراع والاحتكارية، و(2) البرنامج المفتوح المصدر NLnet Labs Name Server Daemon (NSD). قد يكون أحد التنفيذيين أو الآخر أو كلاهما قيد الاستخدام في أي وقت محدد،" <https://a.root-servers.org/aroot-rssac001v2-expectations.pdf>.

<sup>62</sup> "خادم ملف الجذر لنظام أسماء النطاقات الخاص بـ USC/ISI"، على الرابط <https://b.root-servers.org/>.

<sup>63</sup> "RSSAC023v2: History of the Root Server System". اللجنة الاستشارية لنظام خادم الجذر (RSSAC) في ICANN، بتاريخ 17 يونيو/حزيران 2020. على الرابط <https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf>.

<sup>64</sup> Grant, Dani. "Delivering Dot." The Cloudflare Blog <sup>64</sup> بتاريخ 10 سبتمبر/أيلول 2017. على الرابط <https://blog.cloudflare.com/f-root/>.

<sup>65</sup> رالف بيسكوف. "E-Root Instance in San Francisco Servfails:?"، بتاريخ 19 يونيو/حزيران 2025. على الرابط <https://lists.dns-oarc.net/pipermail/dns-operations/2025-June/022899.html>.

<sup>66</sup> Grant, "Delivering Dot".  
<sup>67</sup> تمت المشاركة بإذن من Netnod في المراسلة مع SSAC بتاريخ 13 ديسمبر/كانون الأول 2024.

<sup>68</sup> "M-Root DNS Server"، على الرابط <https://m.root-servers.org/>.

عند النظر إلى كل من نطاقات ccTLD ونطاقات gTLD مجتمعة، نجد أن تسعة من أفضل 10 مشغلين يقدمون خدمات موثوقة لسجلات نطاقات TLD يستخدمون برمجيات FOSS للقيام بذلك.<sup>69</sup>

تحت الجذر ونطاقات TLD، يتم تشغيل خوادم الأسماء المعتمدة من قبل مجموعة واسعة من الكيانات، بما في ذلك الأفراد والمؤسسات والجامعات والحكومات. ورغم عدم توفر بيانات شاملة لهذه المجموعة المتنوعة بأكملها، فمن المعروف أن العديد من أنظمة برمجيات FOSS المستخدمة في الجذر ونطاقات TLD هي أيضاً الخيارات الأكثر شيوعاً لهؤلاء المشغلين. والعديد من المنظمات التي تقدم نظام اسم النطاق الثانوي هي نفسها التي تقدم خدمات نظام اسم النطاق المعتمدة لنطاقات TLD. يوضح الجدول 5 والجدول 6 أنظمة برمجيات FOSS والمنتجات التجارية المناسبة لعمليات تنفيذ نظام اسم النطاق المعتمدة.

غالباً ما يتم دمج خوادم الأسماء المعتمدة مع أنظمة التزويد لتسهيل تحديث معلومات المنطقة بسهولة وتنفيذ التفويض والضوابط المناسبة لصيانة هذه السجلات. بعض أنظمة التزويد الأكثر شعبية هي برمجيات FOSS.<sup>70</sup>

يتم استضافة جزء كبير من المحتوى الأكثر شعبية على الإنترنت في عدد قليل من شبكات المحتوى الكبيرة، مثل YouTube من Google، والذي يستخدم نظام اسم نطاق احتكاري. في الوقت الذي يستخدم فيه عدد من المشغلين الكبار للخدمات المعتمدة للمستويات الثانية والأدنى في التسلسل الهرمي برمجيات FOSS (على سبيل المثال، أولئك الذين يخدمون أيضاً مناطق الجذر أو TLD)، إلا أنه لا تتوفر بيانات عامة كافية لإجراء مسح والخروج بإحصاءات موثوقة فيما يتعلق باستخدامهم لبرمجيات FOSS.<sup>71</sup> انظر الجداول أدناه لمزيد من المعلومات. وهذه فجوة ملحوظة في المعلومات المتاحة لنا، لأن أربعة من مقدمي الخدمة الكبار للغاية قد يكونون مسؤولين عن أكثر من نصف الاستعلامات عن الأسماء المعتمدة المرئية على الإنترنت.<sup>72</sup>

### 4.3 برمجيات FOSS في البنية التحتية لاسترجاع نظام DNS (المُحلِّلات)

لا يقتصر انتشار برمجيات FOSS على نشر بيانات نظام اسم النطاق؛ بل إنه مهم بنفس القدر في البنية التحتية التي تسترد تلك المعلومات: المنظومة المتنوعة لمُحلِّلات نظام اسم النطاق DNS. وتتمتع برمجيات FOSS بحضور كبير في جميع أنحاء منظومة المُحلِّلات، بدءاً من الشبكات المحلية وحتى منصات السحابات العالمية.

ويتم تقديم الخدمة لمعظم المستخدمين من خلال مُحلِّلات محلية يتم تشغيلها من قبل موفري خدمة الإنترنت أو الشركات أو المؤسسات التعليمية. وقد قدرت الأبحاث أن النسبة الإجمالية للمستخدمين الذين تخدمهم المُحلِّلات السحابية أقل من 20% على مستوى العالم. أما نسبة 80% المتبقية من المستخدمين فيستخدمون نوعاً ما من المُحلِّل المحلي.<sup>73</sup> ويمكن استخدام العديد من أنظمة برمجيات FOSS الأكثر شيوعاً للوظائف المعتمدة والمُحلِّلات (الجدول 5).

<sup>69</sup> أفضل المشغلين حسب عدد النطاقات TLD التي يتم تقديم الخدمات لها. انظر الملحق ب لوصف المنهجية المستخدمة.  
<sup>70</sup> تتضمن الأنظمة الشائعة VinylDNS على الرابط (<https://www.vinyldns.io/>) الذي يتم صيانته من قبل Comcast، و OctoDNS، الذي يتم صيانته من قبل Amazon و DNS Control. Oracle هو نظام تكوين شائع آخر، يدير نظام اسم النطاق عبر كل من الأنظمة المستضافة ذاتياً والخدمات السحابية بما في ذلك Cloudflare وخدمة Route53 من Amazon و Gandi، وهو أمين سجل لنظام اسم النطاق وموفر استضافة.

<sup>71</sup> إن قياسات اعتماد برمجيات FOSS بشكل موثوق تشكل مشكلة صعبة. يقدم دانيال ستينبيرغ عدة أسباب تجعل هذا هو الحال في المدونة "What We Can't Measure"، على الرابط <https://daniel.haxx.se/blog/2025/06/05/what-we-cant-measure/> (مدونة)، 5 يونيو/حزيران 2025، على الرابط

<sup>72</sup> جيوف هوستن. "Looking at Centrality in the DNS". APNIC Blog (مدونة)، بتاريخ 22 نوفمبر/تشرين الثاني 2022. على الرابط <https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/>

<sup>73</sup> هوستن، بعنوان "Looking at Centrality in the DNS".

### الجدول 5: أنظمة برمجيات FOSS الشائعة الاستخدام لتطبيقات خادم نظام DNS

نظام البرمجيات	رخصة مفتوحة المصدر	التطبيق – مثال للمستخدمين
<a href="#">BIND9</a>	MPL 2.0	رسمي، مُحلّلات – CIRA و NIC.BR، Visionary Broadband
<a href="#">CoreDNS</a>	Apache 2.0	Kubernetes، رسمي – Meta
<a href="#">dnsmist</a>	GPL 2.0	موازنة حمل نظام اسم النطاق
<a href="#">Dnsmasq</a>	GPL 2 or 3	مُحلّلات بشكل أساسي – شائعة في الأنظمة المضمنة، مثل OpenWRT، والبوابات الرئيسية.
<a href="#">Knot DNS</a>	GPL 3.0	رسمي – TLD .cz
<a href="#">Knot Resolver</a>	GPL 3.0	مُحلّل – DNS4EU
<a href="#">NSD</a>	BSD 3-Clause	رسمي – Rcode Zero
<a href="#">PowerDNS</a>	GPL 2.0	رسمي – Rakuten
<a href="#">PowerDNS Recursor</a>	GPL 2.0	مُحلّل – British Telecom
<a href="#">Unbound</a>	BSD 3-Clause	مُحلّل – Quad9، و Let's Encrypt
<a href="#">YADIFA</a>	BSD 3-Clause	رسمي – TLD .eu

وفي الوقت الذي توجد فيه العديد من المنتجات التجارية المخصصة لهذا السوق، إلا أن معظمها يشتمل على حل واحد أو أكثر من حلول برمجيات FOSS باعتبارها المكون الأساسي لنظام اسم النطاق في عروضها (الجدول 6).

في السحابة، تعمل منصات الحوسبة الضخمة مثل Microsoft Azure و Google Cloud و Amazon AWS على تشغيل بنية أساسية كبيرة للمُحلّل لدعم خدماتها. ويعتمد ما لا يقل عن أربعة من أكبر شركات تطوير البرمجيات على برمجيات FOSS لحل مشاكل نظام اسم النطاق،<sup>74</sup> في حين قامت شركات أخرى ببناء حلول احتكارية تعتمد على مكتبات نظام اسم النطاق للبرمجيات الحرة والمفتوحة المصدر (الجدول 7).

أخيراً، يقوم بعض المستخدمين النهائيين بتكوين أنظمتهم لتجاوز المُحلّل الذي يوفره مشغل الشبكة لديهم واستخدام مُحلّلات عامة مفتوحة بدلاً من ذلك. وفي الوقت الذي تستخدم فيها اثنتان من أكثر الخدمات العامة شيوعاً (Google 8.8.8.8 و Cloudflare 1.1.1.1) برامج احتكارية، إلا أن مُحلّلات عامة رئيسية أخرى، مثل Quad9 (9.9.9.9) و DNS4EU، تكون مبنية على برمجيات FOSS. المزيد من التفاصيل متاحة في الملحق ب.

<sup>74</sup> غامضة من حيث التصميم بناءً على السرية.

### الجدول 6: أمثلة على خدمات نظام DNS التجارية التي تتضمن برمجيات FOSS

الشركة المصنعة	المنتج	التطبيق	يتضمن برمجيات FOSS
Akamai	Edge DNS	مُحلِّل سحابي هجين وخدمة معتمدة	لا
Bluecat Networks	Integrity, Micetro	رسمي، مُحلِّل	نعم
Cynga Labs	VitalQIP, DiamondIP	رسمي، مُحلِّل	نعم
EfficientIP	SolidServer DDI	رسمي، مُحلِّل، جهاز وسحابة	نعم
F5	BIG-IP DNS	مُحلِّل	نعم
IBM	NS1 Connect	خدمة معتمدة تعتمد على السحابة	غير معروف
InfoBlox	Universal DDI & NIOS DDI	رسمي، مُحلِّل، جهاز وسحابة	نعم
Knipp	IronDNS	رسمي	جزئي
Microsoft	Windows Server DNS	رسمي، مُحلِّل، يستخدم في شبكات المؤسسات، يتكامل مع Active Directory	لا
	Azure DNS	خدمة مُحلِّل سحابي	نعم
Netgate	pfSense	مُحلِّل	نعم
Oracle	OCI DNS	خدمة سحابية معتمدة	نعم
TCPWave	DDI Management	جهاز معتمد	نعم

### الجدول 7: مكتبات برمجيات FOSS المستخدمة في تطبيقات البنية التحتية لنظام DNS

نظام البرمجيات	لغة البرمجة	التطبيق - مثال للمستخدمين
<a href="#">c-ares</a>	C	libcurl, curl, NodeJS
<a href="#">dnsjava</a>	Java	(احتكاري) واجهات سجل خلفية
<a href="#">dnspython</a>	Python	Mailman, Samba, Ansible
<a href="#">domain</a>	Rust	Cascade
<a href="#">miekg/dns</a>	Go	Let's Encrypt, CoreDNS, Docker
<a href="#">ldns</a>	C	خادم الاسم dnstap و Zonemaster (احتكاري)
<a href="#">libunbound</a>	C	Open vSwitch, libreswan, opendkim
<a href="#">Net::DNS</a>	Perl	Spamassassin, Mail::DMARC, Mail::DKIM, Mail::SPF

## 5 حالات معاصرة في ضوابط برمجيات FOSS

يتناول هذا القسم العديد من الحالات المعاصرة من الولايات المتحدة والمملكة المتحدة والاتحاد الأوروبي التي توضح كيف يقوم صناع السياسات بتكييف لوائح الأمن السيبراني مع الحقائق الفريدة لمنظومة برمجيات FOSS. ويقدم الجدول 8 ملخصاً رفيع المستوى لهذه الوسائل التي تُنتهج، التي تظهر نمطاً لإعفاء المسؤولين المتطوعين من المسؤولية المباشرة مع التركيز على مسؤوليات الكيانات التجارية التي تدمج أو تنشر برمجيات FOSS. ويتم بعد ذلك استكشاف كل حالة بالتفصيل.

## الجدول 8: ملخص للمناهج التنظيمية المعاصرة لبرمجيات FOSS

القسم	التركيز الرئيسي	مثال على الضوابط	معالجة برمجيات FOSS
5.1	توزيع المسؤولية	استراتيجية الأمن السيبراني الأمريكية لعام 2023، قانون المملكة المتحدة لعام 2025	إعفاء المسؤولين من المسؤولية، التركيز على الكيانات التجارية
5.2	تحفيز التعاون	قانون المرونة السيبرانية في الاتحاد الأوروبي	إدخال دور "المشرف" الاختياري لتحفيز الدعم
5.3	تجنب الافتراضات الاحتكارية	قانون تنفيذ نظام المعلومات الوطنية 2 للاتحاد الأوروبي	لا توجد عقود = لا يوجد مورد مباشر، تشجيع الدعم
5.4	تجنب الأنظمة المتضاربة	توجيه الاتحاد الأوروبي بشأن نظام المعلومات الوطنية 2	تجنب التداخلات للعناصر العالمية مثل خوادم الجذر

### 5.1 توزيع المسؤولية على أصحاب المصلحة الأكثر قدرة على العمل

سعت استراتيجية الأمن السيبراني الوطنية الأمريكية لعام 2023<sup>75</sup> إلى تحويل المسؤولية عن المنتجات والخدمات البرمجيات غير الآمنة (الهدف الاستراتيجي 3.3). وقد صاغت رؤية رفيعة المستوى حيث "يجب أن تتمتع الشركات التي تصنع البرمجيات بالحرية في الابتكار، ولكن يجب أيضًا تحميلها المسؤولية عندما تفشل في الوفاء بواجب التعهد بالرعاية الذي تدين به للمستهلكين أو الشركات أو موفري البنية التحتية الحيوية." ومنذ البداية، ركزت الاستراتيجية على مسؤولي برمجيات FOSS من أجل معالجة أكثر دقة: "يجب أن تقع المسؤولية على عاتق أصحاب المصلحة الأكثر قدرة على اتخاذ الإجراءات اللازمة لمنع النتائج السيئة، وليس على المستخدمين النهائيين الذين يتحملون في كثير من الأحيان عواقب البرامج غير الآمنة، ولا على مطور المصدر المفتوح لمكون مدمج في منتج تجاري."

وعلى نحو مماثل، يهدف قانون ممارسات أمن البرمجيات الطوعي في المملكة المتحدة لعام 2025<sup>76</sup> إلى "دعم بائعي البرمجيات وعملاتهم في تقليل احتمالية وتأثير هجمات سلسلة توريد البرمجيات وغيرها من حوادث مرونة البرمجيات." وينطبق الأمر نفسه على بائعي البرامج التجارية: "بالنسبة للبرمجيات مفتوحة المصدر، لا يتحمل المطور/المسؤول أي التزام رسمي تجاه سلسلة التوريد المستمرة أو تجاه الصيانة المستمرة وأمان الكود الخاص به. ويجب على المستخدمين النهائيين أو المطورين الاحتكاريين الذين يستخدمون الكود المفتوح المصدر في برامجهم إدارة أي مخاطر مرتبطة بالكود المفتوح المصدر."

### 5.2 تحفيز التعاون بين الصناعات المختلفة في مجال الصيانة المستدامة

تهدف هيئة تنظيم الاتصالات<sup>77</sup> في الاتحاد الأوروبي إلى معالجة "المستوى المنخفض للأمن السيبراني للمنتجات ذات العناصر الرقمية، والذي يعكس في الثغرات الأمنية الواسعة النطاق وعدم كفاية وعدم تناسق تحديثات الأمان لمعالجتها." وفي الوقت الذي يتم فيه إعفاء مسؤولي البرمجيات مفتوحة المصدر من المسؤولية بشكل مماثل، إلا أن ذلك يحفز التعاون بين الصناعات المختلفة بشأن الصيانة المستدامة للبرمجيات الحرة والمفتوحة المصدر من خلال تقديم فاعل قانوني جديد ("المشرف على البرمجيات المفتوحة المصدر") "يقدم الدعم على أساس مستدام للتطوير" ويضمن "جدوى تلك المنتجات." يُعد المشرفون بمثابة دور اختياري، ولكنه غير منتشر على نطاق واسع حتى الآن، للمنظمات التي يمكن لمسؤولي برمجيات FOSS اختيار

<sup>75</sup> الرئيس الأمريكي. "استراتيجية الأمن السيبراني الوطني". واشنطن العاصمة: البيت الأبيض، 1 مارس/آذار 2023. على الرابط <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

<sup>76</sup> "مدونة ممارسات أمن البرمجيات".

<sup>77</sup> قانون (الاتحاد الأوروبي) 2847/2024 البرلمان الأوروبي ومجلسه بتاريخ 23 أكتوبر/تشرين الأول 2024 بخصوص اشتراطات الأمن السيبراني الأفقي للمنتجات ذات العناصر الرقمية وتعديلات القانون (الاتحاد الأوروبي) رقم 2013/168 وأيضًا (الاتحاد الأوروبي) 1020/2019 والتوجيه (الاتحاد الأوروبي) 1828/2020 (قانون المرونة السيبرانية الأوروبي)، 2024 الجريدة الرسمية 1 (L 2024/2847)، <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

الارتباط بهم كوسيلة لتوجيه الموارد من الشركات المصنعة أو مشغلي البنية التحتية الأساسية المعتمدة على برمجيات FOSS. وفي الوقت الذي تكون فيه كمية برمجيات FOSS التي تدعمها حاليًا منظمة شبيهة بالمشرف صغيرة حاليًا، إلا أن هيئة تنظيم الاتصالات تعمل على زيادة هذه الممارسة في المستقبل، ومن المرجح أن ينطبق ذلك على بعض المنظمات التي تقوم بصيانة برامج نظام اسم النطاق. إن الابتكار التنظيمي الأخير هو الخيار المستقبلي المتمثل في "الشهادات الأمنية الطوعية"، والذي يسمح بالتعاون بين الصناعات المختلفة في جهود العناية الواجبة.

### 5.3 تجنب متطلبات أمن سلسلة التوريد بافتراض وجود برامج احتكارية

يهدف توجيه الاتحاد الأوروبي بشأن أنظمة الشبكات والمعلومات 2 إلى "التخفيف من التهديدات التي تواجه أنظمة الشبكات والمعلومات المستخدمة لتوفير الخدمات الأساسية في القطاعات الرئيسية".<sup>78</sup> وينظم هذا التوجيه البنية التحتية الرقمية باعتبارها "قطاعًا ذا أهمية عالية"، ويكلف الإدارة بمسؤولية الأمن السيبراني ويفرض "تدابير إدارة المخاطر"، المفصلة في قانون تنفيذي.<sup>79</sup> وتشمل هذه "أمن سلسلة التوريد، بما في ذلك الجوانب المتعلقة بالأمن فيما يتعلق بالعلاقات بين كل كيان ومورديه المباشرين أو موفري الخدمات." والملحق الذي يوضح هذه المتطلبات مستمد من الضوابط الواردة في ISO/IEC 27002:2022، وعلى عكس واقع برمجيات FOSS (انظر القسم 3.2.2) فإنه يفترض سلسلة من الالتزامات التعاقدية حتى مطور البرنامج.

في إرشاداتها التنفيذية الفنية للكيانات الخاضعة للتنظيم،<sup>80</sup> توضح وكالة الأمن السيبراني التابعة للاتحاد الأوروبي، ENISA، مفهوم "المورد المباشر وموفر الخدمة" فيما يتعلق ببرمجيات FOSS: "في حالة برمجيات (FOSS) FOSS، لا يمكن اعتبار المجتمعات والمشاريع التي تقوم بتطوير وصيانة وتوزيع البرمجيات بشكل مفتوح موردين أو موفري خدمات مباشرين حيث لا توجد علاقة تعاقدية بين الكيان المعني ومشروع المصدر المفتوح، باستثناء الالتزام بترخيص حقوق الطبع والنشر الموحد، أو حيث تكون العلاقة التعاقدية مع مشرف برمجيات المصدر المفتوح." وبدلاً من ذلك، توصي "بالفكر في دعم المجتمعات التي تعمل على تطوير وصيانة برمجيات FOSS والاستثمار في علاقة مفيدة للطرفين معها. وعندما يكون ذلك فعالاً، فقد يتضمن ذلك إقامة علاقات مع المشرف على برمجيات المصدر المفتوح ذات الصلة والتي [توفر] الدعم على أساس مستدام لتطوير هذه المنتجات وتضمن استمراريتها".

أجرى تقرير صدر عام 2025 بتكليف من وزارة العلوم والابتكار والتكنولوجيا في المملكة المتحدة استطلاعاً لممارسات الصناعة فيما يتعلق بالبرمجيات مفتوحة المصدر ومخاطر سلسلة التوريد.<sup>81</sup> ومن بين أمور أخرى، يوصي التقرير المنظمات "بإنشاء سياسة داخلية للبرمجيات مفتوحة المصدر لإدارة اعتماد مكوناتها" و"تعزيز المشاركة النشطة مع مجتمع البرمجيات المفتوحة المصدر [...] لضمان مكونات مفتوحة المصدر عالية الجودة ومنظومة مستدامة للبرمجيات المفتوحة المصدر." وعلى النقيض من ذلك، فإن تنظيم أمن سلسلة التوريد غير المصمم خصيصاً لبرمجيات FOSS من شأنه أن يفرض متطلبات تعاقدية على المشغلين لطلب التحقق من خلفية مسؤولي برمجيات FOSS باعتبارهم "موردين"، حتى لو لم يتم شراء البرمجيات المفتوحة المصدر. قد يؤدي هذا التنظيم غير المدروس إلى دفع مواهب برمجيات FOSS إلى التخلي عن مشاريعها، مما يترك المشاريع مع عدد أقل أو أقل من المسؤولين ذوي الكفاءة، مما يتسبب في تدهور الجودة. وهذا يتعارض مع التأثير المقصود من تنظيم أمن سلسلة التوريد.

<sup>78</sup> توجيه (الاتحاد الأوروبي) 2555/2022 البرلمان الأوروبي ومجلسه في 14 ديسمبر/كانون الأول 2022 بخصوص تدابير من أجل مستوى عام ومرتفع من الأمن السيبراني في جميع أنحاء الاتحاد (مبادرة أمن معلومات الشبكة NIS)، 2022 الجريدة الرسمية. 80 (L 333)، على الرابط <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.

<sup>79</sup> اللائحة التنفيذية للمفوضية (الاتحاد الأوروبي) 2690/2024 الصادرة في 22 أكتوبر/تشرين الأول 2024 التي تضع القواعد الخاصة بتنفيذ وتطبيق القانون (الاتحاد الأوروبي) 2847/2024 للاتحاد الأوروبي ومجلسه، 2024 الجريدة الرسمية 1 (L 2024/2690)، على الرابط [https://eur-lex.europa.eu/eli/reg\\_impl/2024/2690/oj](https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj).

<sup>80</sup> وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) الإرشادات التنفيذية الفنية لتوجيه أمن الشبكات والمعلومات NIS2 (تقرير، مكتب منشورات الاتحاد الأوروبي 2025)، على الرابط <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance>.

<sup>81</sup> "أفضل ممارسات البرمجيات مفتوحة المصدر".

## 5.4 تجنب الأنظمة الإقليمية المتضاربة لمجتمعات برمجيات FOSS العالمية

إن الضوابط المباشرة لتطوير البرمجيات واستخدامها في البنية التحتية الحيوية ليست ممارسة واسعة الانتشار. ونظرًا لأن برمجيات FOSS تسمح بالتطوير التعاوني العالمي (القسم 3.2.1)، فيجب على الأنظمة التنظيمية المستقبلية تجنب إنشاء متطلبات متداخلة ومتضاربة بشكل متبادل، والتي يتم تمييزها حسب الموقع المادي للمسؤولين الفرديين.

لقد حرص توجيه الاتحاد الأوروبي بشأن نظام المعلومات الوطنية<sup>82</sup> المذكور أعلاه على تجنب موقف مماثل من الأنظمة المتداخلة مع متطلباتها لموفري خدمات نظام اسم النطاق من خلال استبعاد خوادم أسماء الجذر من نطاقها التنظيمي، وبالتالي تجنب موقف حيث يكون مشغلو خوادم أسماء الجذر عرضة لأنظمة إقليمية متداخلة ومتضاربة في بعض الأحيان.<sup>83</sup>

## 6 النتائج الرئيسية

يقوم هذا القسم بدمج التحليل الأساسي للتقرير في سلسلة من النتائج التي تشكل أساس الأدلة للمبادئ التوجيهية القابلة للتنفيذ التي تليها.

**النتيجة 1: برمجيات FOSS هي الأساس للبنية التحتية الحيوية لنظام DNS.** بينما يسعى صناع السياسات والهيئات التنظيمية في جميع أنحاء العالم إلى تأمين سلسلة توريد البرمجيات، فمن الأهمية بمكان أن تستند جهودهم إلى فهم واضح لكيفية بناء وصيانة أهم أنظمة الإنترنت. وتشير الأبحاث الخاصة بهذا التقرير إلى أن البنية التحتية العالمية لنظام اسم النطاق اليوم تعتمد بشكل كبير على برمجيات FOSS. في الأجزاء الأكثر أهمية من هذه البنية التحتية، تعد برمجيات FOSS هي القاعدة، بينما تشكل البرمجيات الاحتكارية الاستثناء. ويشمل ذلك نظام خادم الجذر، حيث يستخدم تسعة على الأقل من بين 12 مشغلاً عمليات تنفيذ نظام اسم النطاق للبرمجيات الحرة والمفتوحة المصدر حصريًا، ونطاقات TLD، حيث يستخدم تسعة من بين أكبر 10 موفري الخدمات برمجيات FOSS.

**النتيجة 2: نموذج تطوير برمجيات FOSS يختلف بشكل أساسي عن البرمجيات الاحتكارية.** في الوقت الذي يتم إنشاء البرمجيات الاحتكارية عادةً داخليًا من قبل منظمة واحدة، إلا أن نموذج برمجيات FOSS مفتوح وموزع. وإنه مبني على أربع حريات أساسية تمنحها تراخيصه: حرية الاستخدام والدراسة والمشاركة وتغيير البرنامج. ويعمل هذا الإطار على تعزيز منظومة فريدة من نوعه من المسؤولين والمساهمين والمشغلين الذين لا يقتصرون بشكل عام على العلاقات التعاقدية التي تحدد سلسلة التوريد التجارية التقليدية.

**النتيجة 3: لا تعتبر برمجيات FOSS بطبيعتها أكثر أو أقل أمانًا من البرمجيات الاحتكارية؛ إذ يعتمد الأمان على العملية والصيانة، وليس على وضوح الكود المصدر.** لا بد من فهم التداعيات الأمنية لهذا النموذج المفتوح في سياق نقاش مستمر منذ عقود من الزمن دون إجابة واضحة. وكما لخص باحث هندسة الأمن روس أندرسون، فإن رؤية الكود المصدر بالنسبة للأنظمة الكبيرة والمعقدة تساعد المهاجمين والمدافعين على حد سواء. وعلى المدى الطويل، سواء كان النظام مفتوحًا أو مغلقًا، فإن هذا لا يحدث فرقًا كبيرًا فيما يتعلق بأمنه. إن إخفاء الكود المصدر لا يوفر أمانًا إضافيًا؛ بل ينشأ أمان النظام من جودة عمليات التطوير والمراجعة والصيانة.

**النتيجة 4: تتمتع منظومة برمجيات FOSS لنظام اسم النطاق بنقاط قوة فريدة تعمل على تعزيز الاستقرار والمرونة.** رغم أن الانفتاح في حد ذاته قد يكون محايدًا، فإن العملية التعاونية التي يتيحها فعالة بشكل خاص في بناء البنية الأساسية الحيوية للإنترنت وصيانتها. إن الشفافية المتأصلة في برمجيات FOSS تسمح لمجتمع عالمي من المطورين والباحثين والمشغلين بدراسة الكود المصدر ومعالجة الثغرات الأمنية بشكل جماعي، وهي الممارسة التي غالبًا ما تؤدي إلى تصحيح أسرع من

<sup>82</sup> توجيه أمن الشبكات والمعلومات NIS2.

<sup>83</sup> يمكن العثور على ملخص للحجج التي قدمها بيرت هوبرت في مقال بعنوان "Dear EU: Please Don't Ruin the Root"، بتاريخ 10 مايو/أيار 2021، على الرابط <https://berthub.eu/articles/posts/dont-ruin-the-root/>.

الأنظمة الاحتكارية. ويؤدي هذا إلى نقاط قوة متأصلة، بما في ذلك تعزيز الأمن التعاوني، والمرونة التشغيلية من خلال تنوع البرامج، والاستقرار الملحوظ الذي توفره الدعم الطويل الأجل من المنظمات غير الربحية والتجارية المخصصة.

**النتيجة 5: إن نموذج برمجيات FOSS ينطوي على مخاطر متأصلة تتطلب اتباع نهج سياسة مصمم خصيصًا، وليس نهجًا واحدًا يناسب الجميع.** إن نفس الخصائص التي توفر نقاط القوة هذه تقدم في الوقت نفسه مجموعة متميزة من المخاطر التي تتطلب نهج سياسة مصمم خصيصًا. وبما أن نموذج تطوير برمجيات FOSS يفصل التمويل عن الاستخدام، فإن المشاريع قد تواجه تحديات تتعلق بالاستدامة المالية وإرهاق المسؤولين، حيث قد تعتمد البنية التحتية الحيوية على الجهود التطوعية غير الممولة لعدد قليل من الأفراد. علاوة على ذلك، فإن إعادة استخدام مكونات برمجيات FOSS على نطاق واسع يخلق خطر التبعيات المشتركة، حيث يمكن أن يؤدي وجود ثغرة أمنية في مكتبة واحدة إلى تأثير متتالي على مستوى منظومة بأكملها. ولا يمكن حل هذه المشكلات من خلال اللوائح المصممة لسوق البرمجيات التجارية والاحتكارية.

**النتيجة 6: إن فرض المسؤولية القانونية والمالية الجديدة على تطوير وتوزيع برمجيات FOSS لا بد وأن يتم بعناية لتجنب تسميم البيئة التي أدت إلى تطوير هذا العنصر الأساسي من البنية التحتية للإنترنت.** إن عدم وجود كيان قانوني واحد مسؤول أو سلسلة تعاقدية تقليدية في مشاريع برمجيات FOSS يجعل من غير العملي والمحفوف بالمخاطر تطبيق أطر المسؤولية التقليدية. يعتمد نموذج تطوير برمجيات FOSS على المتطوعين الأفراد والمنظمات الصغيرة ذات التمويل البسيط. إن فرض أعباء تنظيمية ثقيلة على هؤلاء المسؤولين قد يثبط مشاركتهم، مما قد يؤدي إلى خنق الابتكار ويؤدي إلى التخلي عن البرامج التي تعتبر حيوية للبنية التحتية الحيوية للإنترنت.

**النتيجة 7: تعتبر برمجيات FOSS مهمة لتمكين موفري الخدمات الجدد من دخول سوق خدمات الإنترنت وتقديم فرصًا لصناع القرار لتشجيع تطوير الخدمات المحلية وتقليل الاعتماد على موفري الخدمات السحابية الأجانب.** بالإضافة إلى دورها التقني، تعمل برمجيات FOSS على تمكين النمو الاقتصادي والاستقلالية الرقمية والمنافسة في السوق. ويعمل نموذج تطوير برمجيات FOSS على خفض تكلفة دخول السوق للشركات الجديدة من خلال إلغاء رسوم ترخيص البرمجيات. وتعمل هذه الإمكانية على تعزيز الابتكار والمهارات المحلية، مما يمنح صناع السياسات وسيلة قوية لإنشاء منظومة رقمية أكثر تنوعًا ويمكن أن يساعد في تقليل الاعتماد على الخدمات السحابية الأجنبية.

## 7 مبادئ توجيهية قابلة للتنفيذ لصانعي السياسات

يستند هذا القسم إلى نتائج التقرير لتقديم مبادئ توجيهية مباشرة وقابلة للتنفيذ لصانعي السياسات. والهدف هو تمكين تطوير التنظيم الفعال وغير الضار الذي يعزز، بدلاً من تقويض، منظومة برمجيات FOSS التي تعد ضرورية للتشغيل الآمن والمستقر للإنترنت.

**المبدأ التوجيهي 1: الاعتراف بالدور الحاسم لبرمجيات FOSS.** يؤكد هذا التقرير حقيقة أن البنية التحتية العالمية لنظام DNS تعتمد على برمجيات FOSS. في الأجزاء الأكثر أهمية من هذه البنية التحتية، تعد برمجيات FOSS هي القاعدة، بينما تشكل البرمجيات الاحتكارية الاستثناء. ولذلك، يتعين على صانعي السياسات أن يعترفوا صراحة في أي تشريع أو لائحة ذات صلة بأن برمجيات FOSS تدعم البنية الأساسية الحيوية للإنترنت وأن استخدامها يشكل قوة يجب الحفاظ عليها. وينبغي أن يشكل هذا الاعتراف أساساً للتنظيم بدءاً من مرحلة التصميم الأولية لمنع الضرر غير المقصود للمنظومة.

**المبدأ التوجيهي 2: التشاور مع مجتمع برمجيات FOSS.** نموذج تطوير برمجيات FOSS هو نموذج مفتوح وموزع ويختلف بشكل أساسي عن نموذج تطوير البرمجيات الاحتكارية. إنه منظومة من المسؤولين والمساهمين والمشغلين الذين لا يلتزمون عمومًا بالعلاقات التعاقدية التي تحدد سلسلة التوريد التجارية التقليدية. ومن الضروري إشراك جميع قطاعات منظومة برمجيات FOSS – بما في ذلك الشركات والمنظمات غير الربحية والمسؤولين الأفراد والمؤسسات المجتمعية – طوال عملية وضع السياسات. ويضمن هذا أن تكون اللوائح مستنيرة بحقائقها التشغيلية ويمنع الضرر غير المقصود لمنظومة برمجيات FOSS، وبالتالي البنية التحتية الحيوية للإنترنت.

**المبدأ التوجيهي 3: الاستفادة من الحالات المعاصرة في تنظيم برمجيات FOSS.** كما هو مفصل في القسم 5، فقد بدأت الجهود التنظيمية الأخيرة بالفعل في التعامل مع الخصائص الفريدة لبرمجيات FOSS مع مواصلة تعزيز الأهداف الأساسية للسياسات. وتوفر هذه الحالات إطارًا قيمًا لوضع سياسات جديدة تتناسب مع الخصائص الفريدة لمنظومة برمجيات FOSS. ويتطلب تطبيق هذه الدروس تصميم سياسات وأنظمة من شأنها:

- توزيع المسؤولية على أصحاب المصلحة الأكثر قدرة على العمل. ويقع واجب الرعاية على عاتق الكيانات التي تنتشر البرامج في المنتجات التجارية أو البنية التحتية الحيوية، وليس على عاتق مطوري برمجيات FOSS المتطوعين الذين يقومون بإنشاء المكونات.
- تحفيز التعاون بين الصناعات المختلفة في مجال الصيانة المستدامة. يمكن ضمان جدوى منتجات برمجيات FOSS الهامة من خلال دعم النماذج القانونية المبتكرة، مثل "مشرف البرمجيات مفتوحة المصدر"، الذي يوجه الموارد من الصناعة.
- تجنب متطلبات أمن سلسلة التوريد التي تفترض نموذجًا للبرمجيات الاحتكارية. ويجب تذكر أنه في برمجيات FOSS، لا توجد غالبًا علاقة تعاقدية مباشرة بين المسؤول والمشغل خارج ترخيص المصدر المفتوح نفسه.
- تجنب إنشاء أنظمة إقليمية متضاربة لمجتمعات برمجيات FOSS العالمية. وينبغي تجنب الالتزامات المتداخلة والمتناقضة لمشاريع برمجيات FOSS العالمية في اللوائح لمنع تجزئة التطوير وتقويض الأمن.

**المبدأ التوجيهي 4: تحفيز استدامة برمجيات FOSS.** يفصل نموذج برمجيات FOSS التمويل عن الاستخدام، وهو ما من المعروف أنه يؤدي إلى تحديات الاستدامة المالية وإرهاق المسؤولين. وقد تعتمد البنية التحتية الحيوية على منظمات صغيرة أو جهود تطوعية غير مرضية من قبل عدد قليل من الأفراد. ولتخفيف هذه المخاطر، يُحث صناعات السياسات على وضع سياسات تفضيلية مرضية لتشجيع مساهمات القطاعين العام والخاص في مشاريع برمجيات FOSS المهمة كشكل من أشكال الاستثمار لأجل منفعة عامة مشتركة.

**المبدأ التوجيهي 5: معالجة المخاطر النظامية بشكل جماعي.** يؤدي إعادة استخدام مكونات برمجيات FOSS على نطاق واسع إلى نشوء خطر التبعيات المشتركة، حيث يمكن أن يكون للثغرة الأمنية في مكتبة واحدة تأثير متتالي على مستوى المنظومة في كل من برمجيات FOSS ومنتجات البرمجيات الاحتكارية. وبما أن هذا يشكل خطرًا منهجيًا متأصلًا في كافة عمليات تطوير البرمجيات الحديثة، فينبغي للسياسة أن تعزز وتمول الحلول التعاونية على مستوى المنظومة، مثل تحسين أدوات الأمن والبحث المستقل، بدلًا من وضع العبء الكامل على المسؤولين المتطوعين الأفراد.

## 8 الإقرارات والإفصاح عن المصالح والانسحابات

لتحقيق الشفافية، توفر هذه الأقسام للقارئ معلومات حول جوانب عملية اللجنة الاستشارية للأمن والاستقرار SSAC. يسرد قسم الشكر والعرفان أعضاء SSAC والخبراء الخارجيين وموظفي ICANN الذين شاركوا في وضع هذه الوثيقة أو ساهموا فيها بشكل مباشر أو قدموا المراجعات. ويشير قسم الإفصاح عن المصالح إلى السير الذاتية لجميع أعضاء SSAC، التي تكشف عن أي مصالح قد تمثل تضاربًا – حقيقيًا أو ظاهريًا أو محتملاً – مع مشاركة أي من الأعضاء في إعداد هذا التقرير. ويحدد قسم الانسحابات الأفراد الذين انسحبوا من مناقشة الموضوع الذي يتناوله هذا التقرير. باستثناء الأعضاء المدرجين في قسم الانسحابات، حظيت هذه الوثيقة بموافقة بالتوافق في الآراء من قبل جميع أعضاء SSAC.

### 8.1 الشكر والعرفان

ترغب اللجنة بتوجيه الشكر إلى أعضاء SSAC والضيوف المدعوين وموظفي ICANN على وقتهم ومساهماتهم ومراجعتهم في إصدار هذا التقرير.

#### أعضاء SSAC

جو أبلي  
مارتن أيرتسن (رئيس مشارك لفريق العمل)  
غونام أكيواتي

نظام اسم النطاق يعمل باستخدام البرمجيات المجانية المفتوحة المصدر (FOSS)

تيم أبريل  
نبيل بن عمار  
كي سي كلافي  
هادية المنياوي  
أوندرج فيليب (عضو SSAC حتى 31 ديسمبر/كانون الأول 2024)  
جيمس غالفين  
روبرت غويرا  
روس هوسلي  
ماتياس هادوبيك  
جيف هيوستن  
ليال جيران  
ميريك كاو (عضو SSAC حتى 31 ديسمبر/كانون الأول 2024)  
أندريه كوليسنيكوف  
وارن "إيس" كوماري  
باري ليا (رئيس مشارك لفريق العمل)  
جون ليفين  
روس ماندي  
رام موهان  
مات توماس  
بيتر توماسن  
تارا والين  
سوزان وولف  
جيانكانغ ياو

#### الضيوف المدعوون

فيتوريا بيرتولا  
ميريك كاو (ضيف مدعو من 01 يناير/كانون الثاني 2025)  
فيكي ريسك  
رافاييل سوميسي

#### موظفو ICANN

جون إيمري (محرر)  
دانييل غلوك  
غوستافو لوزانو إيبارا  
مايكل باكيت  
كارلوس ريبس  
دانييل رودفورد (محررة، مؤلفة مشاركة)  
كاثي شنيث  
ستيف شينغ (موظف دعم SSAC حتى 30 نوفمبر/تشرين الثاني 2024)

## 8.2 الإفصاح عن المصلحة

تتوفر معلومات السيرة الذاتية لأعضاء SSAC والإفصاح عن المصلحة في وقت نشر التقرير على:  
<https://www.icann.org/en/ssac/members/archive/16-05-2025>

## 8.3 الانسحابات

لم يكن هناك أي انسحابات.

## الملحق أ: المصطلحات والمختصرات

### 1. أ. مسرد المصطلحات

- الخادم الرسمي:** خادم يحتفظ بسجلات نظام اسم النطاق الرسمية النهائية لاسم نطاق معين. وهو يوفر الإجابات النهائية لاستعلامات نظام اسم النطاق لهذا النطاق.
- المساهم:** فرد أو منظمة تقدم تحسينات لمشروع برمجيات FOSS، مثل إرسال أكواد البرمجيات أو الوثائق أو تقارير الأخطاء.
- ضمان البيانات:** تخزين نسخة من بيانات تسجيل النطاق لدى جهة خارجية معتمدة من ICANN لحفظها بأمان.
- اسم النطاق:** اسم فريد يمكن قراءته من قِبل الإنسان (على سبيل المثال، icann.org) يحدد عنواناً محدداً على الإنترنت ويشكل أساس عناوين URL.
- نظام اسم النطاق (DNS):** النظام العالمي اللامركزي الذي يعمل بمثابة "دفتر عناوين الإنترنت"، حيث يقوم بترجمة أسماء النطاقات التي يمكن قراءتها من قِبل الإنسان إلى عناوين IP العددية اللازمة لتحديد موقع الخدمات والأجهزة الحاسوبية.
- بروتوكول التزويد المرن (EPP):** بروتوكول فني موحد يستخدم لأتمتة المعاملات بين أمناء السجلات لأسماء النطاقات والسجلات، مثل التسجيلات والتجديدات وعمليات النقل.
- المشروع الفرعي:** مشروع برمجي جديد منفصل يتم البدء به عن طريق أخذ نسخة من الكود المصدر من مشروع موجود لبرمجيات FOSS.
- البرمجيات المجانية مفتوحة المصدر (FOSS):** برنامج مرخص بطريقة تمنح المستخدمين أربع حريات أساسية: الاستخدام والدراسة والمشاركة وتعديل البرنامج. وهذا يحدد نموذج التطوير التعاوني، وليس فقط البرمجيات المجانية.
- عنوان بروتوكول الإنترنت (IP):** تسمية عددية فريدة يتم تعيينها لكل جهاز متصل بشبكة كمبيوتر تستخدم بروتوكول الإنترنت للاتصال.
- اسم النطاق المدول (IDN):** عبارة عن اسم نطاق فيه تسمية واحدة أو أكثر تحتوي على أحرف غير أحرف ASCII أو الأرقام أو الواصلات.
- المسؤول:** الفرد أو المجموعة المسؤولة عن التوجيه العام ومراقبة الجودة لمشروع برمجيات FOSS. ولديه السلطة لقبول أو رفض المساهمات في النسخة الرسمية للبرنامج.
- المشغل:** فرد أو منظمة تقوم بنشر واستخدام البرامج لتشغيل خدمة ما. وفي سياق نظام اسم النطاق DNS، المشغل هو كيان يقوم بتشغيل مكونات البنية التحتية لنظام اسم النطاق، مثل الخوادم أو المُحَلِّلات الرسمية.
- النشر (في نظام DNS):** العملية الفنية المتمثلة في جعل سجلات نظام اسم النطاق DNS الخاصة بالنطاق متاحة على خوادم رسمية حتى يتمكن الآخرون على الإنترنت من إيجاد اسم النطاق.
- المُحَلِّل التكراري (أو المُحَلِّل):** خادم يتم تشغيله غالباً من قبل موفر خدمة الإنترنت (ISP)، والذي يعمل نيابةً عن جهاز المستخدم للعثور على عنوان IP الصحيح لاسم النطاق المطلوب.
- التسجيل (في نظام DNS):** العملية الإدارية المتمثلة في حجز اسم نطاق فريد من خلال إضافته إلى قاعدة البيانات الرئيسية المعتمدة (السجل) لنطاق مستوى أعلى محدد.

نظام اسم النطاق يعمل باستخدام البرمجيات المجانية المفتوحة المصدر (FOSS)

**المسجل:** الفرد أو المنظمة التي تسجل وتحمل حقوق اسم نطاق معين.

**أمين المسجل:** منظمة تتعامل مع الجمهور وتعمل كموزع لأسماء النطاقات، وتدير حجز النطاقات نيابةً عن المسجلين.

**المسجل:** قاعدة البيانات الرئيسية المعتمدة لجميع أسماء النطاقات المسجلة ضمن نطاق المستوى الأعلى المحدد (على سبيل المثال، سجل .org). والمنظمة التي تقوم بصيانة قاعدة البيانات هذه هي مشغل المسجل.

**نظام خادم الجذر (RSS):** مجموعة الخوادم الموجودة في أعلى مستوى من التسلسل الهرمي لنظام اسم النطاق والتي تكون مسؤولة عن توجيه الاستعلامات إلى خوادم نطاق المستوى الأعلى الصحيحة.

**نطاق المستوى الأعلى (TLD):** الجزء من اسم النطاق الموجود على يمين النقطة الأخيرة، مثل .com، أو .org، أو .uk..

**المحدد الموحد لمصدر المعلومات (URL):** العنوان الكامل المستخدم للعثور على مورد محدد على الإنترنت، والذي يتضمن عادةً بروتوكولاً (على سبيل المثال https)، واسم النطاق، ومساراً محدداً (على سبيل المثال <https://www.icann.org/resources>).

## 2. أ. الاختصارات المستخدمة في هذا التقرير

ccTLD: نطاق المستوى الأعلى لرمز البلد

DNS: نظام اسم النطاق

EPP: بروتوكول التزويد المرن

FOSS: برمجيات FOSS

gTLD: نطاق المستوى الأعلى العام

IP: بروتوكول الإنترنت

ISP: موفر خدمة الإنترنت

RSS: نظام خادم الجذر

SSAC: اللجنة الاستشارية للأمن والاستقرار

TLD: نطاق المستوى الأعلى

URL: المحدد الموحد لمصدر المعلومات

IDN: اسم النطاق المدوّل

## الملحق ب: منهجية البحث في انتشار برمجيات FOSS ونتائجها

يقدم هذا الملحق ملخصاً كاملاً ومستقلاً للبحث الأصلي للتقرير. ويتضمن التقرير تفاصيل المنهجية المستخدمة للحصول على النتائج بشأن انتشار البرمجيات المجانية مفتوحة المصدر (FOSS) والنتائج نفسها، والتي تم تقديمها في القسم 4 من هذا التقرير.

### ب.1 النهج العام والتحديات

يعد تحديد البرامج التي يستخدمها مشغلو البرامج في هذا العالم بشكل مؤكد أمرًا صعبًا. في الوقت الذي فيه تم إدخال سجلات معينة لنظام اسم النطاق (DNS) (على سبيل المثال، version.bind و authors.bind و id.server) لمساعدة المستخدمين النهائيين على تحديد إصدار خادم نظام اسم النطاق الذي يتواصلون معه، إلا أن هذه السجلات لا يتم اعتمادها على نطاق واسع بسبب المخاطر الأمنية المحتملة والحاجة إلى التكوين المنفرد يدويًا. وقد تم استكشاف طرق أخرى في الأدبيات، بما في ذلك التحليل السلبي والقياسات الفاعلة. ومع ذلك، فإن هذه الأساليب غالبًا ما تكون محدودة النطاق – فبعضها لا يستطيع سوى تحديد البنية الأساسية المتكررة – وتواجه تحديات تتعلق بإمكانية التوسع.

ولهذه الأسباب، يركز النهج المتبع في هذا التقرير على تقييم مشغلي نظام DNS الكبار حسب حصتهم في السوق، حيث يمكن تأكيد الاستخدام الكبير للبرمجيات المفتوحة المصدر بشكل مباشر.

### ب.2 البنية التحتية لتسجيل اسم النطاق

#### ب.2.1 المنهجية

لتقييم استخدام برمجيات FOSS في البنية التحتية للتسجيل، قامت اللجنة الاستشارية للأمن والاستقرار (SSAC) باستطلاع آراء السجلات الكبيرة وموفري خدمات السجل الخلفية. ولتقييم استخدام برمجيات FOSS في خدمات ضمان البيانات، تم إجراء مسح على وكلاء ضمان البيانات (DEA) المعتمدين من ICANN المدرجين على موقع ICANN الإلكتروني، مع التركيز على البرامج المستخدمة لمكونات الخدمة الرئيسية (نقل البيانات، والتحقق من التوقيع، والتحقق من الإيداع والتفاعل مع واجهة برمجة إعداد تقارير التسجيل (RRI)).

#### ب.2.2 النتائج

تشير البنية التحتية للتسجيل إلى الأنظمة التي تسهل تسجيل أسماء النطاقات الفردية وتجعلها متاحة في نظام DNS العام. ورغم عدم توفر بيانات واضحة عن المدى الكامل لاستخدام برمجيات FOSS، فإن الأدلة تشير إلى اعتماد كبير على هذه البرمجيات، سواء كنظم كاملة أو كمكونات أساسية.

ويحافظ عدد من مشغلي السجلات، وخاصة في مجال نطاق المستوى الأعلى لرمز البلد (ccTLD)، على البنية الأساسية للتسجيل التي تعتمد بالكامل على برمجيات FOSS (الجدول 1، الجدول 2). ومن المعروف أن منصة السجل FRED، على سبيل المثال، تُستخدم من قبل ما لا يقل عن 12 سجلًا لنطاقات ccTLD، وتُستخدم منصة Nomulus للعديد من نطاقات المستوى الأعلى العامة (gTLD).

على النقيض من ذلك، غالبًا ما تستخدم أكبر السجلات وموفري خدمات الواجهة الخلفية للسجلات أنظمة احتكارية. ومع ذلك، لا يتم بناء هذه الأنظمة عادةً من الصفر؛ بل هي عبارة عن ملحقات وتكاملات احتكارية ومخصصة للمكونات، مثل قواعد البيانات وخوادم الويب، والتي هي في الغالب من برمجيات FOSS.

ويمتد هذا الاعتماد على برمجيات FOSS إلى خدمات ضمان البيانات (الجدول 3)، والتي تخزن بشكل آمن نسخًا من بيانات تسجيل النطاق. لقد قام أكبر موفري هذه الخدمات لكل من السجلات وأمناء السجلات ببناء أنظمتهم على الأقل جزئيًا على مكونات برمجيات FOSS.

### ب.3 البنية التحتية لنظام DNS

#### ب.3.1 المنهجية

**تحليل الخادم الرسمي:** للتحقق من استخدام برمجيات FOSS في البنية التحتية لنطاق المستوى الأعلى، تم استخدام الإجراء التالي:

1. تم جلب منطقة الجذر من IANA وتم تعيين نطاقات المستوى الأعلى إلى عناوين بروتوكول الإنترنت (IP) لخوادم الأسماء الخاصة بها.
2. تم إجراء تحليل منفصل على نطاقات ccTLD من خلال النظر في كل من نطاقات المستوى الأعلى المكونة من حرفين ومكافئاتها من A-Label الترميز بمنظومة الأسكي (Punycode) (للتعامل مع نطاقات ccTLD بأسماء النطاقات المدولة ((IDN)).
3. تم استخدام مكتبة Python ip2asn لربط عناوين IP هذه بأرقام النظام المستقل (ASN) وأسماء ASN (المشغلين) الخاصة بها.
4. تم حساب حصة السوق على أنها عدد نطاقات TLD التي يستضيفها مشغل معين مقسومًا على العدد الإجمالي لنطاقات TLD (مع العلم أنه يمكن استضافة TLD من قبل مشغلين متعددين في وقت واحد).
5. تم تحديد أفضل 25 مشغلًا وتم التحقق يدويًا من استخدامهم لبرنامج خادم الأسماء الرسمي المفتوح المصدر.

**تحليل المُحلَّل:** لا توجد استطلاعات موثوقة لقاعدة المُحلَّلات المثبتة بأكملها. بالنسبة لهذا التقرير، ركز التحليل على تعداد المشغلين الرئيسيين وأنواع النشر (على سبيل المثال، المحلي، والسحابي، والعام) واستطلاع ما إذا كانوا يستخدمون برامج حرة ومفتوحة المصدر أو برامج احتكارية بناءً على البيانات العامة والمعرفة المباشرة.

#### ب.3.2 النتائج

**الخواص الرسمية:** إن الدليل على هيمنة برمجيات FOSS يكون أكثر وضوحًا في البنية التحتية التي تنشر معلومات النطاق. في أعلى مستويات التسلسل الهرمي لنظام اسم النطاق – الجذر ونطاقات TLD – تكون برمجيات FOSS موجودة في كل مكان تقريبًا. ويقع نظام خادم الجذر (RSS) في قمة نظام اسم النطاق. ومن بين المنظمات المستقلة البالغة 12 التي تدير خوادم الجذر، هناك على الأقل تسع منظمات تستخدم عمليات تنفيذ نظام اسم النطاق للبرمجيات الحرة والمفتوحة المصدر حصريًا للإجابة على الاستعلامات (الجدول 4).

يستمر هذا النمط في المستوى التالي من التسلسل الهرمي مع خوادم أسماء نطاقات TLD (الجدول 5). توصلت الأبحاث التي أجريت لهذا التقرير إلى أن تسعة من أكبر 10 مشغلين يقدمون خدمة نظام اسم النطاق المعتمدة لسجلات TLD يستخدمون برمجيات FOSS للقيام بذلك. علاوة على ذلك، يستخدم 20 من بين أفضل 25 مشغلًا يقدمون هذه الخدمة لنطاقات ccTLD برامج لنظام اسم النطاق للبرمجيات الحرة والمفتوحة المصدر، ويخدمون بشكل جماعي 234 نطاق ccTLD فريدًا.

**المُحلَّلات:** لا يقتصر انتشار برمجيات FOSS على نشر بيانات نظام اسم النطاق؛ بل إنه مهم بنفس القدر في البنية التحتية التي تسترد تلك المعلومات: المنظومة المتنوعة لمُحلَّلات نظام اسم النطاق.

## نظام اسم النطاق يعمل باستخدام البرمجيات المجانية المفتوحة المصدر (FOSS)

يتم تقديم الخدمة لمعظم المستخدمين من خلال مُحلّلات محلية يديرها موفرو خدمة الإنترنت (ISP) أو الشركات أو المؤسسات التعليمية. وفي الوقت الذي توجد فيه العديد من المنتجات التجارية المخصصة لهذا السوق، فإن معظمها يشتمل على حل واحد أو أكثر من حلول برمجيات FOSS باعتبارها المكون الأساسي لنظام اسم النطاق في عروضها.

وفي السحابة، تعمل منصات الحوسبة الضخمة مثل Amazon Web Services و Google Cloud و Microsoft Azure على تشغيل بنية أساسية كبيرة للمُحلّلات لدعم خدماتها. ويعتمد ما لا يقل عن أربعة من أكبر شركات تطوير البرمجيات على برمجيات FOSS لحل مشاكل نظام اسم النطاق، في حين قامت شركات أخرى ببناء حلول احتكارية تعتمد على مكتبات نظام اسم النطاق للبرمجيات الحرة والمفتوحة المصدر.

## الملحق ج: استطلاع لوجهات نظر مشغلي نظام اسم DNS بشأن برمجيات FOSS وضوابط البرمجيات

أجرت اللجنة الاستشارية للأمن والاستقرار (SSAC) استطلاعًا غير رسمي عبر الإنترنت حول التأثيرات المتوقعة لتنظيم المصدر المفتوح على البنية التحتية لنظام اسم النطاق (DNS) لجمع المدخلات لهذا التقرير. وتم استخدام أداة EUSurvey لحماية خصوصية المشاركين وإخفاء هويتهم.<sup>84</sup> وتم طلب الردود من المجتمع الفني لنظام اسم النطاق على عدد من قوائم البريد الإلكتروني، بما في ذلك؛ قوائم البريد الفني والقانوني لمجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR)، ومجموعات عمل نظام اسم النطاق والمصدر المفتوح التابعة لمركز تنسيق الشبكات الأوروبية لبروتوكول الإنترنت (RIPE NCC)، وقوائم البريد للمستخدمين لعدة أنظمة برمجيات لنظام اسم النطاق مفتوحة المصدر. وقد تم تقديم الاستطلاع أيضًا في اجتماع مركز عمليات وتحليلات وأبحاث نظام اسم النطاق (DNS-OARC) في شهر فبراير/شباط.

كان الهدف الرئيسي من الاستطلاع هو اكتشاف ما إذا كان المشغلون الفنيون في نظام اسم النطاق على دراية بالمبادرات التنظيمية، وسؤالهم عن التأثيرات التي يتوقعون أن تترتب على تنظيم برمجيات (FOSS) FOSS. تم فتح الاستطلاع في شهر فبراير/شباط 2025. وكان هناك 98 استجابة تعطي مقطعًا عرضيًا للأدوار في البنية التحتية لنظام اسم النطاق DNS.

سألنا المشاركين أولاً عن مشاركتهم في نظام اسم النطاق. وأفاد 96 من أصل 98 من المشاركين بالمشاركة في البنية التحتية لنظام اسم النطاق، وأفاد 64 من المشاركين أيضًا بالمشاركة في البنية التحتية لتسجيل اسم النطاق. وأدرج أربعة وعشرون من المشاركين "مطور/بائع برامج" كأحد أدوارهم، لكن لم يُجب أي منهم كمطور برامج فقط. (لم نسأل ما إذا كان برنامجهم مفتوح المصدر أم مغلق المصدر.)

كان المشاركون من مستخدمي المصادر المفتوحة، وكانوا على دراية تامة بالضوابط. وأفاد جميع المشاركين تقريبًا باستخدام المصدر المفتوح (93%). وأفاد حوالي ثلث المشاركين (33%) أيضًا أنهم يستخدمون برامج احتكارية. ويقدم ثلاثون بالمائة من المشاركين أيضًا المشورة للآخرين بشأن تنفيذ وتشغيل برمجيات FOSS. تمتعت هذه المجموعة بمستوى عالٍ من الوعي بالمبادرات التنظيمية الحالية. ولقد قدمنا قائمة بالمبادرات التنظيمية وسألنا "ما هي المبادرات التنظيمية التي أنت على علم بها؟ (ضع علامة على كل ما تعرفه)." وأشار سبعة وسبعون من المشاركين (أي ما يعادل 77%) إلى أنهم على علم بواحدة أو أكثر من هذه المبادرات. وكان قانون المرونة السيبرانية في الاتحاد الأوروبي وقانون الأمن السيبراني NIS2 مألوفين لدى أكثر من 40% من المشاركين. وأشار ثلاثون بالمائة من المشاركين أيضًا إلى أنهم على دراية بواحدة أو أكثر من مبادرات الحكومة الأمريكية، بما في ذلك الأوامر التنفيذية 14028 و 14144، أو برنامج شهادة تطوير البرمجيات الآمنة، أو علامة CyberTrust لأجهزة إنترنت الأشياء (IoT). وشملت اللوائح الأخرى التي ذكرها المشاركون قانون أمن البنية التحتية الحيوية الأسترالي (SOCI)، والقانون العام لحماية البيانات (GDPR)، ومعياري أمان بيانات صناعة بطاقات الدفع (PCI DSS)، وتراخيص برنامج إدارة المخاطر والتصاريح الفيدرالي الأمريكي والكندي (FedRAMP).

ولقد سألنا "ما هي المخاوف المحددة التي لديك بشأن تأثير تنظيم البرمجيات على مؤسستك؟" مع توفير خيارات إيجابية وسلبية. وتمكن جميع المشاركين من الإجابة على هذا السؤال، بما في ذلك أولئك الذين لم يشيروا إلى إلمامهم بأي من اللوائح المحددة التي ذكرناها.

- رأى 72% من المشاركين أنه من المحتمل بشكل معقول أن يتم التخلي عن بعض مشاريع المصدر المفتوح، أو تصبح غير متاحة
- يعتقد 66% أن الامتثال سيؤدي إلى زيادة تكلفة البرامج بالنسبة لهم
- أعرب 49% عن قلقهم من أن بعض مشاريع المصدر المفتوح التي يعتمدون عليها قد تتحول إلى الترخيص الاحتكاري
- يعتقد 29% أن الضوابط سوف تمنع مؤسستهم من نشر البرامج كمصدر مفتوح

<sup>84</sup> "على الرابط "EUSurvey – About" <https://ec.europa.eu/eusurvey/home/about>

- توقع 21% أن أمن المصادر المفتوحة التي يستخدمونها سوف يتحسن
- توقع 7% أن الضوابط سوف تخفف من عبء تقييم أمن وجودة البرامج على مؤسساتهم.

وعلى الرغم من أننا طلبنا بشكل خاص تعليقات من المشاركين حول التأثيرات والفرص الإيجابية، وذلك في محاولة لإيجاد موقف متوازن، وكان معظم المشاركين متشائمين.

### ج.1 التعليقات المفتوحة (مخاوف محددة)

دعا الاستطلاع إلى تقديم تعليقات مفتوحة حول مخاوف محددة بشأن تأثير تنظيم البرمجيات، فضلاً عن الاستفسار عن الفرص أو التأثيرات الإيجابية المتوقعة.

وكانت المخاوف الأكثر شيوعاً هي:

- زيادة تكاليف الامتثال
- نشر البرامج بشكل أبطأ
- التخلي المحتمل عن بعض مشاريع المصدر المفتوح بسبب الأعباء التنظيمية
- زيادة التعقيد في الامتثال القانوني لمستخدمي برامج المصدر المفتوح