أصدرت منظمة ICANN في 22 تشرين الأول لعام 2019 ورقة عمل سلطت الضوء فيها على بعض المعايير المتعلقة بنظام أسماء النطاقات مثل DNS Over TLS (DoT)وDNS Over HTTPS (DOH). بالإضافة لتشفير قناة النقل بين الأجهزة مثل أجهزة الكمبيوتر الخاصة بالمستخدم النهائي والمحللات العودية. بعنوان:

" الآثار المترتبة من تشفير DNS على السياسة المحلية والانترنت"

عند إضافة الخصوصية لـ DNS فهو يمنع إمكانية التنصت بهدف الحصول على معلومات قيمة وكذلك يمنع مسؤولو الشبكة من استخدام DNS كوسيلة لفرض سياسات المحتوى والوصول وغيرها من سياسات التحكم.

لا يحتوي الـ DNS الكلاسيكي على أي تشفير للرسائل المتبادلة بين الأطراف أو أي مصادقة لأطراف الاتصال، فهم يقومون لاحقاً بإضافة التشفير والمصادقة. من أجل ذلك في عام 2016تم وضع معيار DOH (DNS Over Https) حيث تم تصميمه لتشفير حركة مرور DNS للتطبيقات كقناة النقل بين الأجهزة مثل أجهزة الكمبيوتر الخاصة بالمستخدم النهائي والمحللات العودية. وفي عام 2018 تم وضع معيار DOT (DNS Over TLS) ليكون وسيلة نقل بديلة أكثر خصوصية لاستعلامات DNS ولاستجابات أنظمة التشغيل.

يوجد أسباب متنوعة للفلترة كالتقليل من مخاطر التصيد والبرامج الضارة و..... وغيرها إلا أن الفلترة تكون عادة من أجل اعتراض استعلامات الDNS لأسماء النطاقات ذات بالصلة بالمحتوى المشكوك والغير مرغوب به وذلك:

- إما لمنع استجابة الـ DNS لتلك الاستعلامات.
- أو لتحويل الطلبات إلى خوادم غير فعالة أو خوادم لها محتوى مختلف عن المحتوى المطلوب.

بالنسبة لعملية مراقبة حركة مرور DNS تكون مفيدة للعثور على محاولات اختبار المعلومات التي تهدف إلى البقاء داخل الشبكة أو على جهاز كمبيوتر معين ، وأيضاً لاكتشاف البرامج الضارة التي يتم تثبيتها على الرغم من أفضل الجهود التي يبذلها مسؤولو الشبكة ، .....و غيرها.

من خلال استخدام الصناديق الوسيطة التي تقوم بالفلترة أو المراقبة، لا يمكن رؤية استعلامات DNS المشفرة واستجاباتها. حيث أنه ما لم يتم تجهيز صندوق الوسيط وأجهزة الكمبيوتر المرتبطة به للقيام بهذا العمل بحيث يتم تزويده بمفتاح لفك تشفير حركة مرور TLS.

القضايا الأساسية للسياسات المتعلقة بـ DNS المشفر:

هذا فيما يخص السياسة المحلية والانترنت فقط وليس فيما يتعلق بسياسة منظمة الـ ICANN.

1. زيادة خصوصية حركة مرور مستخدمي ال DNS.
2. زيادة ثقة مستخدمي حركة مرور ال DNS.
3. التحايل على فلترة ال DNS من أجل الأمن وذلك من خلال تشفير استعلامات الـ DNS.
4. التحايل على فلترة الـ DNS للسياسة المحلية بحيث يتم استخدام الـ DNS المشفر لتجاوز القيود المفروضة على الوصول إلى الخدمات أو المحتوى على الانترنت.
5. التحايل على فلترة الـ DNS المفروضة من قبل الحكومات: حيث تفرض بعض الحكومات على بعض الجهات فلترة الـ DNS لأنواع معينة من المحتوى ويمكن تخطي هذه المشكلة باستخدام التشفير.
6. عدم إمكانية كشف استخدام محللات الـ DNS المركزية حيث أن تشفير حركة المرور على الانترنت باستخدام DOH يمنع الجدار الناري من معرفة ما إذا كانت حركة المرور تحتوي على استعلام DNS.

الأطراف المهتمة:

1. مطورو المتصفح: أعلن كل من Mozilla Firefox و Google Chrome عن خطط لنشر DoHفي متصفحاتهما.
2. مطورو نظام التشغيل: نظام التشغيل الوحيد الذي أعلن عن نشر DNS المشفر هو نظام تشغيل Googleلنظام الأندرويد .
3. الحكومات: بدأت جلسات التشريعية المتعلقة بـ DOT و DOH في بلدان مختلفة كما هو الحال في برلمان المملكة المتحدة.
4. مسؤولو الشبكة
5. مطورو الـ DNS .

وفي الختام رأي منظمة الـ ICANN:

تهدف المبادئ التالية إلى زيادة المستخدمين الثقة وهي ليست إجبارية:

1. الخصوصية جيدة لأن تشفير الاتصال بين الكمبيوتر والمحلل ممارسة جيدة.
2. فلترة لل DNS تعد مفيدة للحد من مخاطر التصيد، وتوزيع البرامج الضارة، والبريد الواغل، وغيرها من أشكال الاساءة التي تؤثر على أسماء النطاقات.
3. من الضروري أن تحتوي التطبيقات على معلومات كافية وعلى سبيل المثال عن طريق الاستدلال التشغيلي أو تفاعل المستخدم قبل اتخاذ القرارات التي قد تتعارض مع قرارات التحكم بالشبكة.
4. يجب حماية بيانات الـ DNS عبر نشر مصادقة DNSSEC وذلك يتم في المحلل العودي (لحماية البيانات من من المخدمات الموثوقة) وكذلك داخل الكمبيوتر (للحماية من تعديل البيانات داخل ذاكرة التخزين المؤقتة بين المحلل والكمبيوتر).