# SAC 056

# Avis du SSAC sur les impacts du blocage de contenus par le système de noms de domaine

Avis du comité consultatif

sur la sécurité et la stabilité (SSAC)

de l'ICANN

Le 9 octobre 2012

# Préface

Voici le rapport du Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC).  Le SSAC conseille la communauté et le Conseil d'administration de l'ICANN sur des questions liées à la sécurité et à l'intégrité des systèmes de nommage et d'adressage sur Internet. Ceci inclut des questions opérationnelles (par ex., des questions se rapportant à l'opération correcte et fiable du système de noms racine), des questions administratives (par ex., des questions se rapportant à l'attribution d'adresses et de numéros sur Internet), et des questions d'enregistrement (par ex., des questions se rapportant aux services des registres et des bureaux d'enregistrement). Le SSAC se livre à une évaluation continue des menaces et à une analyse des risques des services de nommage et d'attribution d'adresses Internet pour évaluer les principales menaces à la sécurité et à la stabilité, et conseille la communauté de l'ICANN en conséquence.  Le SSAC n'a pas d'autorité officielle pour réglementer, faire valoir ou se prononcer. Ces fonctions relèvent d'autres services, et l'avis donné ici devrait être évalué selon ses propres mérites.

Les personnes ayant contribué à l'élaboration de ce rapport, les biographies des membres du comité, les déclarations d'intérêt et les objections des membres du comité aux conclusions ou aux recommandations de ce rapport se trouvent à la fin du présent document.

# Table des matières

# 1. Résumé

L'utilisation du blocage par le système de noms de domaine (DNS) pour limiter l'accès à des ressources Internet suscite un intérêt croissant dans les nombreux forums de gouvernance d'Internet.  Plusieurs gouvernements du monde entier, par le biais de lois, de traités, de décisions judiciaires, d'actions d'application de la loi ou d'autres actions ou traités, ont mis en œuvre le blocage par DNS ou envisagent sérieusement de le faire. Cependant, en raison de l'architecture d'Internet, le blocage par nom de domaine peut être aisément contourné par des utilisateurs finaux, si bien qu'il peut s'avérer très peu efficace à long terme et entraîner des conséquences imprévues dans le court terme. De plus, le blocage par DNS peut donner lieu à des conflits avec l'adoption des extensions de sécurité du DNS (DNNSEC) et risque de promouvoir la balcanisation d'Internet, avec une vision « pays par pays » de l'espace de nommage d'Internet.

Ce document se limite à faire état d'une exploration des impacts techniques liés au blocage par DNS, y compris :

- Blocage de domaine par le biais de :
  - Un registre ou un bureau d'enregistrement ;
  - Un serveur faisant autorité ;
  - Dans un résolveur récursif, par le biais de la redirection des requêtes, la non existence d'un nom de domaine, l'envoi d'un code de réponse « refusé » à une requête ou d'autres codes de réponse, ou bien le manque de réponse à une requête.
- Blocage DNS dans des résolveurs récursifs et conflits avec DNSSEC ;
- Conditionnement des utilisateurs finaux pour une plus grande utilisation du cryptage de bout en bout
- Surblocage ;
- Fautes de frappe ;
- Routage du trafic DNS en dehors du pays qui impose le blocage ;
- Impact du changement de résolveurs par les utilisateurs, et
- Difficulté à localiser les réseaux de diffusion de contenus (CDN) si les utilisateurs changent les résolveurs.

Des conséquences non techniques liées à l'atteinte à la liberté d'expression peuvent aussi être signalées, mais il s'agit de questions qui ne seront pas abordées dans le présent document.  La communauté d'Internet, les gouvernements ainsi que les autres acteurs devraient bien comprendre et examiner avec attention toutes les conséquences liées au blocage par DNS, autant du point de vue technique que non technique.

## 2. Introduction

Le présent document se base sur le « SAC050 : Blocage par DNS : Bénéfices versus inconvénients – un rapport consultatif du comité consultatif sur la sécurité et la stabilité », qui peut être intéressant pour les lecteurs de ce document.[1]

En 2011 et 2012, plusieurs gouvernements ont propose ou établi des directives formelles, des lois, des décisions judiciaires ou des actions d'application de la loi liées au blocage par DNS, filtrage de DNS et/ou saisie de noms de domaine.[2] Dans certains cas, ces activités avaient pour but l'élaboration d'une nouvelle législation destinée à contrôler l'utilisation d'Internet, alors que dans d'autres cas, les tribunaux ou les agences d'application de la loi se sont servis du blocage par DNS ou des saisies de nom de domaine comme autant de mécanismes pour bloquer l'accès à certains sites ou à certaines adresses Internet.[3,4,5,6]

Ce document examine les impacts techniques de plusieurs types de blocages par DNS qui ont été mis en œuvre ou proposés. Le présent rapport est destiné à informer la communauté Internet, les décideurs, les fonctionnaires des gouvernements et les autres acteurs sur les implications techniques générales de l'utilisation du blocage par DNS pour contrôler l'accès aux ressources Internet.[7]

## 3. Blocage par DNS : Bénéfices versus inconvénients

Les principales conclusions du SAC050 sont :

---

[1] Voir  « SAC050 : Blocage par DNS : bénéfices versus inconvénients – un rapport consultative du comité consultatif sur la sécurité et la stabilité sur le blocage des domaines de premier niveau dans le système de noms de domaine », Société pour l'attribution des noms de domaines et des numéros sur Internet (ICANN), Comité consultatif sur la sécurité et la stabilité, 14 juin 2011, http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf.

[2] Voir H.R. 3261 « Stop Online Piracy Act » (Loi anti-piratage), Chambre des représentants des États-Unis, 112e Congrès, version en date du 16 décembre 2011 et la loi estonienne concernant le blocage de sites de jeux de hasard illégaux, https://www.riigiteataja.ee/akt/125042012010.

[3] Voir initiative OpenNet, http://opennet.net/youtube-censored-a-recent-history.

[4] Voir http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/.

[5] Voir http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6] Voir http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

[7] Pour une description du DNS, voir http://queue.acm.org/detail.cfm?id=1242499

> « Le filtrage de noms de domaine ou le filtrage basé sur les adresses du protocole Internet (IP) (pour empêcher l'accès à, par exemple, des contenus Web capables d'infecter les ordinateurs avec des virus ou considérés inappropriées dans le cadre des ressources d'un employeur) peuvent être vus par certaines organisations comme une extension naturelle des anciennes politiques qui empêchaient les gens de ces organisations d'engager des frais téléphoniques.
> …
> Indépendamment du mécanisme utilisé, les organisations qui mettent en œuvre le blocage devraient appliquer les principes ci-dessous :
>
> 1. L'organisation impose une politique à un réseau et à ses usagers, sur lesquels elle exerce un contrôle administratif (c'est à dire, elle est le gestionnaire d'un domaine politique)
> 2. L'organisation détermine que la politique est avantageuse pour ses intérêts et pour les intérêts de ses usagers.
> 3. L'organisation met en œuvre la politique moyennant une technique considérée comme étant la moins perturbatrice pour ses opérations de réseau et ses utilisateurs, à moins que les régulations n'établissent l'application de certaines techniques spécifiques.
> 4. L'organisation mène des actions concertées pour ne pas porter préjudice aux réseaux ou aux utilisateurs extérieurs au domaine concerné par la politique, comme conséquence de la mise en œuvre de cette dernière.
>
> Lorsque ces principes ne sont pas appliqués, le blocage par DNS risque d'entraîner des dommages collatéraux ou des conséquences imprévues, pour lesquels les solutions disponibles sont limitées, voire inexistantes»

Pour élargir les conclusions du SAC050, la correcte prise en compte de la stabilité générale d'Internet exige que toute politique ou action de blocage par DNS soit entièrement informée aux parties concernées, y compris aux utilisateurs finaux, aux fournisseurs de service et aux concepteurs d'applications. À défaut d'une telle information, le blocage par DNS entraînera des activités de dépannage inutiles ainsi que des réponses adaptatives, voire même des activités imprévues de contournement par les opérateurs de réseau et les utilisateurs finaux. De telles informations doivent inclure les motivations, les effets attendus ainsi que les effets collatéraux prévus. À défaut d'une telle transparence, le blocage par DNS risque d'être considéré comme une coupure ou une attaque malveillante et peut donner lieu à des réponses de la part des utilisateurs finaux, des gestionnaires de réseau, des fournisseurs de service, etc., visant à atténuer les préjudices.

Ces erreurs potentielles de diagnostic et la recherche inévitable de moyens de contournement peuvent entraîner des dommages collatéraux ou des conséquences

imprévues.  Une évaluation publique indépendante a été demandée dans le rapport du Haut-commissariat des Nations Unies aux droits de l'homme sur la promotion et la protection du droit à la liberté d'opinion et d'expression, où il est établi :

> « 31. […] Troisièmement, même lorsqu'une justification est avancée, les mesures de blocage constituent un moyen inutile ou disproportionné pour atteindre le but prétendu, dans la mesure où souvent elles ne sont pas suffisamment ciblées et empêchent l'accès à un large éventail de contenus au delà de ceux qui avaient été considérés illégaux. Finalement, le contenu est souvent bloqué sans l'intervention ou la possibilité de révision par un organe judiciaire ou indépendant. » [8]

Le reste du présent document est une exploration sur les types de blocage par DNS et leurs impacts.

## 4. Blocage de contenus dans le contexte de l'architecture Internet

Un des principes fondamentaux de l'architecture Internet repose sur son abstraction de « bout en bout », qui minimise le besoin d'intelligence au cœur du réseau (le nœud) mais accueille l'intelligence à ses extrémités (les hôtes individuels).  Cette architecture a donné lieu à des innovations profondes et nombreuses, qui permettent, par exemple, qu'un développeur d'un côté du réseau déploie une nouvelle application dans un hôte et qu'un utilisateur à l'autre bout du réseau en installe le client correspondant pour ainsi permettre de nouvelles formes de communication, sans qu'il y ait besoin d'aucune permission spéciale ou aucun contrôle dans aucune autre partie du réseau.

Le blocage de contenus par le système de noms de domaine a parfois été mis en œuvre au niveau du « cœur » d'Internet et parfois au niveau de ses « extrémités » . Les connexions entre un fournisseur d'accès, ses sources de trafic et ses puits de trafic sont appelées « extrémités ». Les connexions à l'intérieur ou entre les opérateurs sont appelées « nœud ». Des exemples de blocage au niveau des extrémités incluent les listes noires dans les navigateurs Web ainsi que le filtrage du trafic IP au bout d'une connexion.  Si le même blocage appliqué sur les extrémités se faisait au niveau du cœur du réseau, les utilisateurs finaux affectés pourraient contourner le blocage en changeant de fournisseur de DNS ou en utilisant des réseaux privés virtuels (VPN), des proxy ou des modules complémentaires (plug-in). Le type de blocage appliqué sur les extrémités ne sera efficace que si des filtres basés sur des politiques sont présents dans tous les

[8] Frank La Rue, « **Rapport sur le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression »** A.HRC.17.27., http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

chemins entre les utilisateurs finaux affectés et tous les réseaux avec lesquels ils pourraient échanger des paquets. Parmi des exemples de ce type de topologies, on retrouve les pare-feu nationaux et les pare-feu d'entreprise.

Comme effet collatéral de cette architecture, les efforts pour bloquer le trafic, que ce soit par DNS (tels qu'example.com) ou par adresse IP (telle que 192.0.2.117), à tout point du réseau autre que les extrémités, peuvent être contournés, par exemple, moyennant l'utilisation d'un réseau privé virtuel (VPN).[9] Les VPN ou d'autres méthodes similaires sont facilement disponibles et faciles à adopter y compris par des utilisateurs peu expérimentés. Même dans les cas où un contrôle total, administratif et opérationnel, des réseaux d'accès à internet est possible (comme ceux chez un fournisseur d'accès Internet ou dans certains points d'échange Internet[10]), les utilisateurs finaux seront tout de même capables d'accéder aux contenus interdits.[11]

La caractéristique commune des filtrages les plus efficaces repose sur le fait que l'utilisateur final et son opérateur de réseau se mettent explicitement ou implicitement d'accord sur ce qui sera filtré et sur la façon dont le filtrage de contenus sera mis en place. Dans ces cas, l'utilisateur final voit le blocage par DNS comme un service avantageux.

## 5. Types de blocage par DNS observés ou proposés

Plusieurs méthodes de blocage par DNS ont été proposées ou mises en œuvre au cours des dernières années. Certaines méthodes posent des difficultés techniques plus importantes que d'autres. En voici une liste non exhaustive :

1. **Saisie de domaine par un registre ou un bureau d'enregistrement** : Cette méthode élimine des données DNS de leur source par le biais d'un registre DNS ou d'un bureau d'enregistrement agissant en qualité d'agent du registre. Un registre est l'entité responsable de la création d'une base de donnés faisant autorité qui contient les données du DNS, y compris celles concernant les domaines à bloquer. Un exemple de cette méthode serait le démontage (*take-down*) d'un nom de domaine mis en place par un registre ou un bureau d'enregistrement suite à un ordre de démontage envoyé par un gouvernement, qu'ils sont légalement tenus d'exécuter. La réponse d'un registre ou d'un bureau d'enregistrement à un tel ordre de démontage dépend des éléments spécifiques de l'ordre. Le nom de domaine peut : soit être retiré de la zone (option connue sur le nom de « mise en attente de domaine » quand les données d'enregistrement du domaine concerné sont gardées), ce qui empêche les utilisateurs finaux de

[9] Voir http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html ou http://vpn-account.com/bypassblockedsites.html.

[10] Voir http://en.wikipedia.org/wiki/Internet_exchange_point.

[11] Voir http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter.

résoudre un nom de domaine associé à un site spécifique ; soit être mis en correspondance avec un nom de serveur différent qui redirigera donc les utilisateurs vers une page Web affichant des informations supplémentaires, y compris l'avis de l'agence d'application de la loi faisant état du démontage. Dans la situation de « mise en attente du domaine », une fois que le paramètre TTL (time to live –durée de vie) de l'entrée DNS du nom de domaine arrive à expiration -normalement au bout de quelques heures ou de quelques jours- le domaine devient globalement irrésoluble. Cela veut dire que lorsqu'un utilisateur tape ce nom de domaine, il obtiendra une réponse du type « le domaine n'existe pas ». Si les noms de domaine corrects sont saisis, il n'y a pas d'implications techniques négatives directes propres à la méthode de « mise en attente de domaine ». Parmi les implications techniques négatives indirectes on retrouve des failles dans les services à distance, si d'autres domaines dépendent du domaine soumis à cette « mise en attente » pour leur service de noms, leur service de courrier électronique, ou leur service Web. Autant dans la méthode de « mise en attente du domaine » que dans celle de changement de nom du serveur, le bureau d'enregistrement ou le registre doivent mettre à jour ou supprimer toute donnée DNSSEC concernant le domaine ciblé. Autrement, les applications chargées de vérifier la conformité DNSSEC risquent d'identifier des données non valides en réponse à des requêtes DNS et d'empêcher ainsi toute communication, y compris celle destinée à expliquer aux utilisateurs pourquoi le domaine n'est plus disponible.

2. **Blocage de domaine dans un serveur faisant autorité** : Ce type de blocage, mis en œuvre par l'opérateur des serveurs de noms faisant autorité du domaine concerné, contourne le registre et probablement le bureau d'enregistrement, et cible directement le mécanisme grâce auquel le nom de domaine est disponible sur Internet. Une fois qu'un registrant a obtenu un nom de domaine et l'a correctement configuré, le registre produit les données DNS et publie ces informations dans un ensemble de « serveurs faisant autorité ». Très souvent, le bureau d'enregistrement opère avec ces serveurs faisant autorité, mais il ne s'agit pas d'une obligation, comme ce ne l'est pas non plus le fait que tous les serveurs faisant autorité soient opérés par la même entité. Indépendamment de qui opère les serveurs faisant autorité, ceux-ci sont un mécanisme de publication et de ce fait, un point où le blocage par DNS peut être mis en place. Un exemple de ce type de blocage serait le démontage d'un nom de domaine par l'opérateur du serveur DNS faisant autorité du nom de domaine ciblé, suite à un ordre envoyé par un gouvernement. . L'opérateur en question devrait donc supprimer ou modifier leur copie des fichiers DNS faisant autorité pour le domaine concerné. Supposant que l'ordre de démontage ait été envoyé à tous les opérateurs de serveurs faisant autorité pour le domaine et que tous les opérateurs l'aient mis en place, le domaine deviendrait immédiatement peu fiable de manière globale et éventuellement irrésoluble une fois que le TTL de l'enregistrement DNS

du domaine arrivera à expiration. Outre le fait que différentes entités mettent en œuvre le blocage, cette méthode diffère du blocage basé sur le registre / bureau d'enregistrement, en ceci qu'elle peut entraîner des difficultés par rapport aux DNSSEC , car l'opérateur du serveur faisant autorité risque de ne pas être capable de préserver les signatures DNSSEC lorsque le contenu du domaine de registre est modifié.

3. **Blocage de domaine dans un résolveur récursif** : Les résolveurs récursifs sont un lieu souvent choisi pour exécuter le blocage par DNS, grâce à l'existence d'un certain nombre d'outils (autant commerciaux que libres) qui facilitent la mise en œuvre du blocage.[12] Cependant, en raison de l'architecture du DNS, les blocages dans des résolveurs récursifs comptent parmi les plus facilement contournés. Les résolveurs récursifs, normalement opérés par le fournisseur d'accès internet de l'utilisateur final, récupèrent les données DNS des serveurs faisant autorité à partir de requêtes envoyées par les utilisateurs finaux. Lorsqu'un utilisateur final souhaite se connecter à un site Web ou à un autre service, le résolveur récursif desservant cet utilisateur final traduit le nom de domaine de ce site ou de ce service en adresses IP. Le blocage par DNS à travers des résolveurs récursifs vise à filtrer, éditer ou bloquer cette traduction. Cela peut se faire de plusieurs manières :

   a. **Par redirection** : dans cette modalité de blocage dans le résolveur récursif, la réponse du serveur faisant autorité est modifiée afin d'y substituer les valeurs spécifiées dans la politique de blocage par DNS. Par exemple, au lieu de renvoyer l'adresse IP du serveur Web incriminé, le résolveur récursif renvoie l'adresse IP d'un serveur de remédiation qui affiche un message indiquant que le site est bloqué.[13]

      Cette forme de blocage nécessite un serveur de remédiation pour supporter les protocoles et les services supportés par les serveurs cible d'origine, pour lesquels l'affichage d'une bannière de redirection est techniquement possible. C'est à dire que si l'objectif du blocage est d'utiliser le protocole de transfert de fichiers (FTP) pour fournir des contenus, le serveur vers lequel l'utilisateur est redirigé doit aussi utiliser le protocole FTP pour pouvoir afficher la bannière.[14] En raison de la façon dont travaillent certains

[12] Voir http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ et http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/.

[13] Voir http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf.

[14] Voir « **Protocole de transfert de fichiers »** sur http://en.wikipedia.org/wiki/File_Transfer_Protocol.

protocoles, ce type de redirection peut ne pas être faisable dans tous les cas.[15] Cependant, pour les protocoles le plus communément utilisés, tels que le protocole de transfert hypertexte (HTTP, le principal protocole de la toile mondiale –world wide web), ce type de redirection est faisable.

b. **Par un code de réponse de nom de domaine inexistant (NXDOMAIN)** : Tout comme pour la redirection, cette modalité de blocage modifie la réponse du serveur faisant autorité ; cependant, au lieu de renvoyer l'adresse IP d'un autre serveur, la réponse est modifiée pour indiquer que le domaine demandé n'existe pas.

c. **Par un code de réponse de refus de requête** : Le protocole DNS a un code de réponse, REFUSÉ, qui vise à indiquer qu'un domaine ne peut pas être résolu pour des raisons administratives. Le blocage par DNS peut être mis en œuvre en changeant la réponse du serveur faisant autorité par une réponse REFUSÉ pour les domaines bloqués.

   Une interprétation parfaitement valable et raisonnable de la spécification du protocole DNS consiste à dire que le code de réponse REFUSÉ indique que le serveur de noms ne devrait pas du tout être interrogé, ce qui entraîne l'élimination de ce résolveur récursif de la liste de serveurs de noms par le système d'exploitation. La réponse REFUSÉ est donc interprétée comme un problème de contrôle d'accès pour le client et pour tous les noms de domaines demandés par ce client, plutôt que comme un refus à répondre pour un nom de domaine en particulier. Avec un nombre suffisant de requêtes d'utilisateurs finaux, ce type de blocage pourrait entraîner la suppression de tous les serveurs de noms utilisés par l'utilisateur final, après quoi l'ordinateur de l'utilisateur final devient incapable (ou réticent) de chercher des noms. Ainsi, les résolveurs renvoyant une réponse REFUSÉ pour un domaine bloqué, risquent d'entraîner des dommages collatéraux inacceptables.

d. **Par d'autres codes de réponse :** D'autres codes de réponse spécifiés dans le protocole DNS peuvent être utilisés pour indiquer qu'un domaine ne peut pas être résolu, généralement en indiquant qu'un certain type d'erreur s'est produite. Parmi ces codes de

[15] Voir « Redirection dans les domaines COM et NET (9 juillet 2004) », Comité consultatif de l'ICANN sur la sécurité et la stabilité, sur http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf.

réponse on retrouve « défaillance du serveur » (SERVFAIL), « non mis en œuvre » (NOTIMPL) et « erreur de format » (FORMERR).

Tout comme pour REFUSÉ, le blocage par ces codes de réponse peut avoir comme conséquence que le système d'exploitation déclare que le résolveur récursif est non opérationnel et le supprime de la liste de serveurs de nom récursifs interrogés par le système d'exploitation. C'est pourquoi aucune de ces réponses de substitution n'est adéquate pour le blocage par DNS.

e. **Par non réponse à la requête** : Finalement, le résolveur récursif pourrait être configuré pour ignorer les requêtes concernant le domaine demandé. Cela entraînerait pour les applications essayant de se connecter au site bloqué la multiplication des tentatives de résolution par le biais de multiples itérations de la requête.

   Tout comme pour le code REFUSÉ et les autres codes de réponse d'erreur, le système d'exploitation peut éliminer le résolveur récursif de sa liste de serveurs de noms interrogés pour la recherche de tout nom de domaine (et pas seulement le nom de domaine bloqué).  Cependant, contrairement au blocage par les codes de réponse décrits ci-dessus, le blocage par non réponse implique pour l'utilisateur final une plus mauvaise expérience, dans la mesure où l'application doit attendre que toutes les requêtes s'achèvent.  Cela peut encourager les utilisateurs à basculer vers un autre résolveur récursif et à utiliser des serveurs non couverts par l'ordre de démontage ou la politique de blocage souhaitée.

La reconfiguration des résolveurs récursifs dépend du système d'exploitation, mais un petit nombre de clics sur l'interface graphique d'utilisateur dans les « préférences du système » suffisent pour le faire. Dans les systèmes d'exploitation courants, ainsi que dans d'autres dispositifs intelligents, un grand nombre de logiciels applicatifs gérant les systèmes d'exploitation permettent aussi de réussir cette reconfiguration en un clic.  Dans presque tous les cas, cette reconfiguration est à la portée de tous, y compris les utilisateurs les moins expérimentés.

Tel qu'il a été mentionné ci-dessus, le blocage par des résolveurs récursifs est le moyen le plus utilisé à l'heure actuelle pour bloquer le DNS ; cependant, les utilisateurs finaux peuvent contourner ce type de blocage en utilisant un résolveur récursif qui ne mette pas en place le blocage, par exemple, un résolveur « libre » qui accepte des requêtes d'adresses IP

provenant de n'importe quelle source[16] ou bien en utilisant leurs propres résolveurs récursifs.

De plus, étant donné que le blocage par DNS basé sur les résolveurs récursifs réécrit ou modifie les réponses DNS reçues de la part des serveurs faisant autorité, il brise le modèle de chaîne de confiance utilisé par DNSSEC et donne lieu à des erreurs DNSSEC. Ces erreurs peuvent amener un utilisateur final à conclure que le résolveur récursif du DNS a un problème ou est attaqué. Cette conclusion serait crédible, car avec DNSSEC, les réponses DNS réécrites en vertu d'un mandat gouvernemental sont techniquement impossibles à distinguer de celles que l'on peut observer dans un empoisonnement de cache malveillant.

## 6. Comparaison entre le blocage par DNS basé sur le registre ou le serveur faisant autorité et le blocage basé sur un résolveur récursif

Certains pays, tels que le Royaume Uni, agissant contre des noms de domaine dans le TLD .uk[17] , ou les États-Unis agissant contre des noms dans le domaine de premier niveau (TLD) .com [18] , ont saisi des domaines gérés par des registres opérant à l'intérieur de leurs frontières. Dans certains cas, le nom de domaine a été placé en attente dans le registre ; dans d'autres cas, les entrées DNS ont été modifiées pour diriger le trafic vers des sites Web contrôlés par le gouvernement.

Supposant que les noms de domaine bloqués sont peu nombreux et que la création de nouveaux domaines visant le même public et le même but n'est pas sans importance ni sans coût, les saisies de nom de domaine peuvent s'avérer efficaces pour bloquer des contenus Internet.  Étant donné que les actions dans un TLD sont mises en place au niveau du point de publication, tous les résolveurs récursifs DNS au niveau global vont supprimer les noms bloqués dans une période de temps assez courte, spécifiquement pendant le délai TTL au bout duquel les entrées DNS seront bloquées.

Lorsque les domaines sont saisis au niveau du registre, DNSSEC[19] continue de fonctionner comme prévu, car cette action est une modification du contenu DNS à sa source et de ce fait, en supposant que les signatures DNSSEC sont recréées de

[16] Parmi les résolveurs « libres » les plus populaires on retrouve OpenDNS (http://www.opendns.com/) et Google Public DNS (https://developers.google.com/speed/public-dns/).

[17] Voir http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/.

[18] Voir http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0.

[19] Voir http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

façon appropriée, la chaîne de confiance DNSSEC n'est pas brisée.

Cependant, si le registre fournissant les noms devant être bloqués est localisé dans une juridiction légale différente, la coopération entre des agences d'application de la loi ou entre des fonctionnaires gouvernementaux dans les différentes juridictions peut s'avérer nécessaire. Cela peut poser des problèmes dans des cas où les lois de l'autre pays sont incompatibles, ou bien lorsque les organisations d'application de la loi n'ont pas signé des traités d'assistance légale mutuelle explicite, des accords de partenariat, de coopération ou de coordination à travers, par exemple, l'Interpol. C'est pourquoi le démontage au niveau du registre reste le moyen le plus pratique dans une seule juridiction légale, même si des améliorations dans la coordination et la coopération entre des agences d'application de la loi ont pu récemment être constatées. Par exemple, la coopération peut se mettre en place grâce à la participation des services d'application de la loi dans le cadre du processus multipartite de l'ICANN, et grâce à la création de groupes de travail spéciaux au sein des organisations, comme c'est le cas du Centre européen de lutte contre la cybercriminalité (E3C) dans Europol.[20]

Le blocage par DNS au niveau du serveur faisant autorité exige à chaque opérateur des serveurs faisant autorité d'introduire des changements dans la zone qu'il reçoit du registre, sans autorisation dudit registre. Lorsque les serveurs faisant autorité sont opérés par plusieurs organisations, cela peut poser des difficultés. Il suffit qu'un ou plusieurs opérateurs des serveurs faisant autorité ne réussissent pas à refléter le même changement dans la même version de la zone, pour que des résultats incohérents soient renvoyés pour la même requête, en fonction du résolveur interrogé, du serveur faisant foi interrogé par les résolveurs, l'endroit où les requêtes ont été faites, etc. De plus, à moins que l'opérateur du serveur faisant autorité s'avère être le détenteur de la zone de signature de clé (ZSK), les modifications introduites dans la zone par l'opérateur du serveur faisant autorité ne seraient pas signées, ce qui entraînerait l'échec des vérifications de la chaîne de confiance DNSSEC pour les résolveurs chargés de la validation. Par conséquent, cette forme de blocage a tendance à ne pas être pratique.

L'utilisation du blocage par DNS basé sur des résolveurs récursifs évite ces difficultés juridictionnelles, puisque les ordres de démontage sont adressés aux fournisseurs d'accès Internet ou à d'autres opérateurs de résolveurs dans la même juridiction légale de l'organisme demandant le démontage. En contrepartie, puisque de nombreux opérateurs de réseau dans le monde entier opèrent des résolveurs récursifs, il est impossible d'assurer une couverture complète sans un filtrage coordonné et universel du chemin de données et sans la manipulation des données utiles.  En plus, ceci empêcherait une correcte validation DNSSEC de

[20] Voir https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

bout en bout au niveau des applications, comme on le verra dans la prochaine section.  Or, au moins une étude a démontré qu'en raison d'un phénomène dit « filtrage amont » (*upstream filtering*), les actions mises en place par un fournisseur d'accès à Internet (FAI) d'un pays pour filtrer ou bloquer des contenus peuvent entraîner le blocage de contenus dans un autre pays en vertu d'arrangements de routage entre FAI.[21] Les conséquences imprévues de ce type d'influence gouvernementale extraterritoriale peuvent se traduire par une augmentation des coûts opérationnels et une diminution de la stabilité pour tous les opérateurs et les utilisateurs d'Internet.

## 7. Blocage par DNS dans des résolveurs récursifs et conflits avec le DNSSEC

Comme cela a été discuté dans les sections précédentes, la mise en œuvre des DNSSEC peut avoir un impact important sur les activités de blocage par DNS. Les DNSSEC sont un ensemble d'améliorations au protocole DNS conçues pour répondre aux problèmes d'authenticité des données du DNS. Même si les applications autorisées par DNSSEC ne sont pas encore largement utilisées, le besoin de telles applications est un moteur clé du développement et du déploiement des DNSSEC. Le déploiement de bout en bout des DNSSEC est nécessaire pour permettre une authentification cryptographique dans les applications actuelles et futures qui sont sensibles en termes de sécurité et restent essentielles pour sauvegarder la confiance du public en l'Internet global.

Un blocage efficace par DNS au moyen des résolveurs récursif entre en conflit avec l'objectif et le fonctionnement des DNSSEC. En effet, les améliorations DNSSEC ont été conçues pour identifier exactement ce type de changements que le blocage tente d'introduire, même si le terme « blocage » implique que le changement en lui même est introduit conformément à la législation et/ou à d'autres règles acceptées par les parties concernées. Les changements produits par le blocage ne peuvent pas être différenciés des changements que DNSSEC doit identifier, tels que l'introduction par des criminels de fausses réponses DNS afin que le trafic soit redirigé vers de faux services. Les modifications introduites dans les données signées DNSSEC ont la même apparence que les tentatives malveillantes d'empoisonnement du DNS, car aucun trait ou signe des DNSSEC ne permet au récepteur de se rendre compte que la réponse reçue a été signée par une autorité autre que le détenteur du domaine. Cela est vrai pour des domaines dont le but est tout simplement de voiler un site Web et aussi pour des redirections de domaine dont le but est d'afficher une notification du gouvernement communiquant l'interception/démontage du site Web. Dans les deux cas, lorsque le résolveur d'un utilisateur final validera les réponses signées DNSSEC, il sera capable de voir qu'une manipulation a eu lieu, mais n'en connaîtra pas les causes. Suite à la détection de ce type d'altération, le résolveur

[21] Voir https://citizenlab.org/2012/07/routing-gone-wild/.

de l'utilisateur final peut utiliser des contournements, tels qu'ignorer le résolveur récursif local en résolvant de façon itérative toute la chaîne de confiance depuis la racine jusqu'aux serveurs faisant autorité.

Le blocage par DNS au niveau du résolveur récursif peut être mis en œuvre comme solution temporaire de dépannage. Plus spécifiquement, si on bloquait ou on filtrait le DNS uniquement quand le détenteur de nom de domaine ou l'utilisateur final n'utiliseraient pas DNSSEC, les données modifiées seraient donc toujours acceptées par les résolveurs des utilisateurs finaux et utilisées par des applications telles que les navigateurs Web. Or, pour un détenteur de domaine qui ne voudrait pas que son nom de domaine soit bloqué, le contournement consisterait à signer les données DNS, alors que le contournement pour les utilisateurs finaux qui ne voudraient pas que leurs contenus soient bloqués consisterait à permettre les DNSSEC dans leurs résolveurs basiques.[22] D'où la caractérisation de « solution de dépannage temporaire ».

S'il est souvent considéré que la validation DNSSEC peut ou doit se faire uniquement « dans le réseau », cette idée ignore pourtant les besoins des applications qui tiennent compte des DNSSEC. Les mécanismes DNSSEC peuvent être utilisés « dans le réseau » afin de protéger le cache DNS des données empoisonnées. Pendant les premières années du déploiement DNSSEC c'était d'ailleurs le seul usage que l'industrie en faisait. Cependant, la vision à long terme des DNSSEC vise à créer une toute nouvelle classe d'applications d'utilisateurs finaux qui tiendraient en compte les DNSSEC, à l'aide de technologies telles que  la « DNS-based Authentication of Named Entities » (DANE), une initiative en cours de l'IETF (groupe de travail chargé de développer et de promouvoir les standards Internet).[23] Le groupe de travail DANE travaille actuellement à la standardisation d'un mécanisme grâce auquel l'identité d'un serveur Web sécurisé et la sécurité de la connexion entre un navigateur et ce site web sécurisé est améliorée à l'aide des DNSSEC plutôt qu'à travers l'ancien réseau d'autorité de certification X.509, qui pose de plus en plus de problèmes.[24]

Dans le cadre des efforts mis en place pour utiliser les DNSSEC comme l'infrastructure générale sur laquelle des applications sécurisées seront

---

[22] Les résolveurs basiques (*stub resolvers*) sont des résolveurs DNS comportant des fonctions minimales, qui utilisent des requêtes récursives pour décharger la plupart du travail de résolution de DNS vers un serveur de noms récursif.  Presque tous les dispositifs Internet contiennent un résolveur basique, et presque tous les accès à des réseaux fournissent un serveur de noms récursif à leurs clients.  Voir http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers.

[23] Voir https://datatracker.ietf.org/wg/dane/charter/.

[24] Parmi des exemples des difficultés récentes rencontrées avec X.509 on retrouve la mise en danger de Diginotar (voir http://en.wikipedia.org/wiki/DigiNotar) et les multiples difficultés des autorités d'enregistrement de Comodo (voir http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/).

construites, on peut supposer que le blocage par DNS dans les résolveurs récursifs aura un impact négatif sur le déploiement des DNSSEC, ou bien deviendra inefficace une fois que les DNSSEC seront plus largement déployés. L'économie mondiale peut avoir de deux choses, l'une : soit yn système de nommage Internet sûr et par conséquent des applications Internet sécurisées, soit un système efficace de blocage par DNS Internet – mais non pas les deux.

# 8. Autres implications du blocage par DNS

Le filtrage et le blocage par DNS peuvent avoir des implications potentielles au-delà de celles évoquées dans les sections précédentes. Parmi celles-ci, il convient de signaler le surblocage et le contournement/évitement grâce au routage du trafic DNS en dehors des points où le blocage est appliqué.

## 8.1 Surblocage

En supposant que des techniques de blocage par DNS seront utilisées, il existe un risque lié à des erreurs qui peuvent se produire sur la liste d'entités à bloquer. Cela est indépendant du fait que le blocage se fasse à partir des noms de domaine ou d'autres identifiants tels que les adresses IP ou les localisateurs uniformes de ressources (URL). C'est pourquoi le processus utilisé pour vérifier les points à ajouter dans une liste donnée soit être sûr, fiable et permettre des contrôles approfondis. Les listes utilisées dans les exemples de blocage décrits dans le présent rapport proviennent de différentes sources : entités privées, agences d'application de la loi prêtant leur coopération, tribunaux ou corps législatifs. Le SSAC ne se prononce pas sur la question de savoir quel est le meilleur processus mais recommande plusieurs mécanismes pour promouvoir la stabilité technique : des règles claires sur ce qui peut être bloqué et un processus bien défini de révision et de prise de décisions.

De plus, il est important de reconnaître que si le blocage est appliqué à un nom de domaine tel qu'*example.com*, le blocage par le système de noms de domaine bloquera non seulement la possibilité de chercher le nom de domaine pour accéder aux contenus de l'URL bloqué  *http://example.com/bad-content.html*, mais aussi tous les autres URL utilisant le même nom de domaine; par exemple, *http://abc.example.com/* or *http://example.com/good-content.html*.  Le blocage par DNS bloquera aussi la recherche du nom de domaine pour tous les autres services - courrier électronique, gestion de réseau, transfert de fichiers, etc.- qui utilisent le même domaine, ainsi que pour les domaines enfants d'*example.com* (par exemple, *sous-domaine.example.com*).[25]

[25] Voir http://gigaom.com/europe/orange-censors-all-blogs/, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/, and http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

Finalement, dans les filtrages, que ce soit dans le DNS ou ailleurs, il est fondamental d'éviter des erreurs dans la création des cibles à bloquer. Par exemple, une faute de frappe lors de la saisie de données pourrait bloquer fatalement le nom de domaine ciblé mais aussi bloquer accidentellement d'autres domaines non liés à celui-ci. Les noms de domaines internationalisés (IDN) peuvent poser des risques spéciaux car deux IDN pouvant apparaître comme étant identiques peuvent cependant être différents à l'intérieur du DNS.

## 8.2 Routage du trafic DNS en dehors du pays qui impose le blocage

L'action du gouvernement qui conduit au blocage d'un domaine peut encourager les utilisateurs finaux à prendre des mesures pour que leur trafic DNS soit routé à travers des serveurs de noms situés à l'extérieur du pays concerné, par exemple, en utilisant des réseaux privés virtuels (VPN) ou des résolveurs récursifs spécifiques au lieu de ceux opérés par le fournisseur d'accès. Ce routage « off shore » des requêtes de nom de domaine peut transférer l'observabilité et le contrôle du DNS vers d'autres pays, entravant ainsi les activités de lutte contre la cybercriminalité du pays mettant en œuvre le blocage et/ou encourageant les activités de cybercriminalité d'entités extérieures au pays en question.  Outre l'augmentation de la latence qui peut y être associée, ce routage extérieur du trafic DNS peut aussi avoir un impact sur la performance d'Internet dans la nation mettant en place le blocage, car plusieurs réseaux de diffusion de contenus prennent des décisions sur quel type d'information renvoyer à des requêtes DNS basées sur l'adresse IP source du résolveur formulant la requête.  L'utilisation de serveurs non locaux peut entraîner un trafic inattendu traversant les liens internationaux.

Le changement vers un autre serveur de noms, qu'il fasse partie du DNS commun coordonné par l'ICANN ou d'un système alternatif, peut se faire en reconfigurant directement un ordinateur, tâche qui est de nos jours facilitée par l'existence d'interfaces graphiques conviviales d'utilisateurs dans la plupart des systèmes informatiques. Même si les individus ne possèdent pas les connaissances nécessaires pour modifier la configuration DNS de leurs ordinateurs (ou réseaux), des scripts et des applications sur mesure destinées à automatiser la modification du DNS ont été publiées et peuvent être téléchargées.  Le plug-in MAFIAAFire en est un exemple. Il a été publié peu après la mise en place de l'initiative « Opération dans nos sites »  des Services de l'immigration et des Douanes du gouvernement américain.[26]

[26] Voir https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ et http://en.wikipedia.org/wiki/MAFIAAFire_Redirector.

### 8.2.1 Impacts du changement de résolveurs par les utilisateurs

Le DNS permet aux fournisseurs d'accès Internet d'avoir un état de situation important et précis de la structure du trafic ainsi que des menaces qui pèsent sur la sécurité de leurs réseaux. Cette information permet aux FAI d'identifier toute augmentation ou changement du trafic et d'obtenir ainsi des informations qui serviront de base à leurs décisions commerciales. Plus important encore, la surveillance des données DNS contribue à améliorer la sécurité du réseau, dans la mesure où elle permet aux FAI de diagnostiquer des attaques de « refus de service » ainsi que d'identifier des hôtes infectés, des domaines fragilisés et des utilisateurs vulnérables.

Le recours de plus en plus fréquent des utilisateurs aux serveurs DNS autres que ceux fournis par leurs FAI entraînera pour ces derniers une diminution de leur capacité à gérer les menaces en matière de sécurité et à assurer l'efficacité des opérations du réseau. La réduction de l'utilisation par les usagers des services DNS d'une entreprise, d'un opérateur de réseau local ou d'un FAI se traduira par un plus grand nombre d'ordinateurs fragilisés qui ne seront ni identifiés ni corrigés.  De plus, les attributs de configuration Internet devant être évalués lorsqu'un client appelle un centre d'assistance de l'opérateur seront beaucoup plus importants, ce qui entraînera une augmentation des coûts et de la complexité du débogage.

Les difficultés évoquées ci-dessus représenteront des défis que devront relever les gouvernements des nations où sont localisés les FAI. Ces gouvernements risquent de perdre leur capacité à obtenir des renseignements par le biais d'accords de partage de données avec les opérateurs de réseau et les opérateurs de services Internet, ainsi que d'obtenir des informations qui pourraient constituer des preuves importantes dans le cadre d'investigations en matière d'application de la loi. Par exemple, le gouvernement des États-Unis pourrait ne pas disposer de suffisamment de preuves concernant les structures de commande et de contrôle d'un réseau zombie et des caches empoisonnés pour mettre en place une opération comme celle dite « Ghost click », une importante intervention qui a servi à démanteler des serveurs responsables de la propagation du logiciel malveillant DNSChanger.[27]

Les difficultés en matière d'application de la loi seront particulièrement graves lorsqu'un utilisateur choisit un serveur DNS dans un autre pays. La capacité des mécanismes juridiques à résoudre un problème est d'autant moins importante que les serveurs ne relèvent pas de la juridiction de l'agence d'application de la loi donnée concernée.

### 8.2.2 Difficulté à localiser les CDN suite à un changement de résolveur

[27] Voir http://www.fbi.gov/news/stories/2011/november/malware_110911.

### par les utilisateurs

Le routage du trafic DNS destiné à contourner une topologie de réseau -par exemple, à travers des serveurs DNS situés à l'extérieur d'un pays donné-, affectera aussi négativement la performance du réseau (dans la nation, par propagation ajoutée et délai aller-retour total) et augmentera les coûts des FAI. Par exemple, si les utilisateurs changent de résolveur pour éviter le blocage, la localisation CDN peut ne pas fonctionner et l'utilisateur final sera redirigé vers les contenus à partir de nœuds CDN hébergés dans des serveurs localisés à l'étranger, plutôt que à partir de ceux localisés dans le réseau d'accès de l'utilisateur, avec des liens d'interconnexion directs.

Les CDN localisent généralement la diffusion de contenus en distribuant le même contenu à des serveurs d'un ample éventail de réseaux mondiaux.  Cette localisation réduit la charge de travail de tout serveur unique et minimise la consommation et la congestion de ressources du réseau en diffusant des contenus à partir de serveurs qui se trouvent le plus près possible de l'utilisateur. Plusieurs CDN déduisent la localisation d'un utilisateur sur la base de l'adresse IP de leur résolveur DNS, ce qui veut dire que les utilisateurs ayant changé leur résolveur pour un résolveur situé dans un autre pays, seront considérés par le CDN comme se trouvant à l'étranger. Il en résultera un impact négatif sur la performance et la stabilité des utilisateurs de ces CDN, ainsi qu'un accroissement pour les FAI des coûts de transport du trafic associé.

## 9. Conclusions et lecture recommandées

Si le blocage de contenus par DNS est devenu plus fréquent, autant comme sujet d'étude que comme pratique, il comporte cependant un certain nombre de problèmes techniques.  Le blocage au niveau du registre DNS (directement ou à travers un bureau d'enregistrement) comporte le moindre nombre d'implications techniques. Il peut travailler avec DNSSEC mais se heurte à des problèmes juridictionnels, et peut entraîner une balcanisation de l'espace de noms d'Internet à long terme.  Le blocage au niveau des serveurs faisant autorité pose des problèmes juridictionnels similaires mais ne peut pas travailler avec DNSSEC lorsque les opérateurs des serveurs faisant autorité n'ont pas la capacité de signer correctement la zone contenant le(s) nom(s) à bloquer.  Finalement, le blocage au niveau de résolveur, s'il est aujourd'hui assez banalisé, il n'en reste pas moins problématique vis-à-vis des DNSSEC et, dans le pire des cas, pourrait empêcher le déploiement des DNSSEC.

Les gouvernements et autres devraient examiner ces questions et bien comprendre leurs implications techniques lorsqu'ils développent des politiques reposant sur le blocage ou le filtrage de contenus par le DNS.

Lectures recommandées pour savoir plus à ce sujet :

- *Shutdowns, Suspensions, Seizures, Oh My!*, D. Piscitello, http://securityskeptic.typepad.com/the-security-

skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html.

- *Preventing Access or Removing Content – Laser Scalpel or Saw?*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html.
- *A Chainsaw is a Poor Choice for Surgery and for Blocking Content*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html.
- *Alignment of Interests in DNS Blocking*, P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/.

# 10. Remerciements, déclarations d'intention, objections et rétractations

Ces sections mettent à disposition du lecteur des informations concernant trois aspects de notre processus. La section des remerciements contient la liste des membres ayant contribué à l'élaboration de ce document. La section des biographies et des déclarations d'intérêt contient les biographies des membres du comité ainsi que tout conflit d'intérêts réel, apparent ou potentiel susceptible d'avoir un impact sur le contenu de ce document. La section des objections et des rétractations offre la possibilité aux membres individuels de manifester leur désaccord avec le contenu de ce document ou avec son processus d'élaboration.

## 10.1 Remerciements

Le comité tient à remercier les membres du SSAC ci-dessous ainsi que toutes les personnes ayant contribué à l'élaboration de ce rapport pour leur temps, leurs contributions et leurs révisions.

Alain Aina
Jaap Akkerhuis
Don Blumenthal
KC Claffy
David Conrad
Patrik Fältström
James Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Paul Vixie

## 10.2 Déclarations d'intérêt

Les informations biographiques des membres du SSAC et les déclarations d'intérêt sont disponibles sur : http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

## 10.3 Objections et rétractations

Il n'y a pas eu d'objections ou de rétractations.