Annexe 15

Extrait de « Julian Assange - Google contre WikiLeaks » - p86 (une discussion qui se déroule le 23 juin 2011)
Edition Ring, 2018

JA > Julian Assange, rédacteur en chef et fondateur de WikiLeaks.

ES > Eric Schmidt, président exécutif de Google, coauteur de The New Digital Age, membre du Council of Advisors on Science and Technology du président Obama, membre du Council on Foreign Relations.

.../...

JA : Oui, rendre public le matériau de source primaire. C'est ce que j'entends par publier.

ES : Donc la première étape a consisté à faire cela convenablement ?

JA : Il était clair que publier partout dans le monde était un problème, du fait de la censure ou de l'auto-censure.

ES : Pardonnez-moi, mais est-ce que vous pensez à la peur de représailles par les gouvernements ? Ou à autre chose ?

JA : A l'autocensure principalement. Je dirais même que la forme de censure la plus conséquente, historiquement, a été la censure économique, lorsqu'il n'est tout simplement pas rentable de publier quelque chose parce qu'il n'y a pas de marché pour cela. Je vois la censure comme une pyramide. Au sommet de la pyramide, il y a les meurtres de journalistes et d'éditeurs. En-dessous, les attaques juridiques contre les journalistes et les éditeurs. Une attaque juridique n'est qu'un recours retardé à la coercition, qui n'entraîne pas nécessairement le meurtre, mais l'incarcération ou la saisie de biens.

Dites-vous que le volume de la pyramide augmente considérablement à mesure que vous descendez, ce qui veut dire que le nombre d'actes de censure augmente aussi à mesure que l'on descend.

Il y a très peu de gens qui sont assassinés, il y a peu d'attaques juridiques publiques contre des particuliers et des sociétés, mais au niveau du dessous, il y a une énorme autocensure. En partie parce que les gens ne veulent pas se retrouver aux étages supérieurs de la pyramide - ils ne veulent pas subir d'attaques légales et de la coercition, ils ne veulent pas être tués. Cela décourage les gens d'adopter certains comportements. Il y a ensuite d'autres formes d'autocensure motivées par la crainte de manquer une affaire ou une promotion. Celles-ci sont d'autant plus significatives qu'elles sont les plus basses de la pyramide. Au bas de l'échelle - le plus grand volume - se trouvent toutes les personnes qui ne savent pas lire, qui n'ont pas accès à l'imprimerie, aux communications rapides ou sont dans des lieux où il n'est pas rentable de fournir de tels services[1].

Nous avons décidé de nous attaquer aux deux plus hauts étages de la pyramide : les menaces de violence et les menaces de violence retardées du système judiciaire. C'est ce qu'il y a de plus difficile et de plus facile à la fois. Facile, parce que la démarcation entre censure et non censure est claire, et parce que les volumes sont relativement faibles, malgré l'importance potentiellement élevée par évènement.

Au départ, WikiLeaks n'avait que peu d'amis. Même si j'avais bien sûr quelques contacts politiques du fait d'autres activités, nous n'avions pas d'alliés politiques de poids ni d'audience mondiale s'intéressant à nous. On a alors décidé qu'il nous fallait un système de publication dont la seule défense serait l'anonymat. Pas de défenses financières. Pas de défenses juridiques. Pas de défenses politiques. Ses défenses étaient purement techniques.

Cela impliquait un système *distributed at its front*[2], avec de nombreux noms de domaine, et une capacité à rapidement passer de l'un à l'autre[3], un système de mise en cache[4], et, à l'arrière, un tunnel à travers le réseau Tor conduisant à des serveurs cachés[5].

..../...

(1) Pour une représentation visuelle de la pyramide de la censure, voir Marienna Pope-Weidemann, « Cypherpunks: Freedom and the Future of the Internet" (review), *Counterfire*, 13 septembre 2013, archive.today/Oyczc.

Pour davantage sur cette idée, voir Julian Assange avec Jacob Appelbaum, Andy Müller-Maguhn, et Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet* (OR Books, 2012), pp. 123-124.

(2) « Distributed at its front » est un terme technique. Le *front* d'un site est la partie visible lorsqu'on le parcours avec son navigateur. Sur la plupart des sites d'informations, le *front* et la partie invisible du site ont le même emplacement physique. Ce qui les rend plus faciles à censurer. WikiLeaks s'est construit pour échapper à la censure ; il utilise donc un modèle différent, où l'*arrière* des sites est secret et caché, et où le *front* est répliqué sur de nombreux ordinateurs. Ainsi, si un ordinateur hébergeant le *front* est attaqué, il demeurera des répliques du site, le rendant toujours accessible au public. De plus, l'*arrière* demeure secret et de nouveaux fronts peuvent être créés à volonté.

(3) Un nom de domaine est le nom d'un site Internet lisible par un humain, comme wikileaks.org ou whitehouse.gov. Tous les terminaux connectés à Internet se voient assigner une adresse numérique, plus connue sous le nom d'adresse IP. Tous les sites Internet sont hébergés sur des ordinateurs, et on peut y accéder par leur adresse IP. Par exemple, 195.35.109.44 est une adresse IP de WikiLeaks. Les adresses IP sont difficiles à retenir. Pour résoudre ce problème, le DNS (Domain Name System) fut inventé : il relie les « noms de domaine » à des adresses IP. Contrairement aux adresses IP, automatiquement attribuées à chaque fois que vous connectez un terminal au réseau, vous pouvez posséder un nom de domaine de votre choix en l'enregistrant auprès d'un registrar pour une somme modique. Tous les noms de domaine sont inscrits dans un annuaire global - comme un annuaire téléphonique - liant chaque nom de domaine à l'adresse IP réelle d'un site. Quand « wikileaks.org » est tapé dans un navigateur, ce dernier fait d'abord un « lookup » - il contacte un serveur DNS, qui dispose d'une copie de l'annuaire global, puis y cherche le nom de domaine « wikileaks.org » pour trouver l'IP correspondant. Il charge ensuite le site de cette IP. Lorsqu'un nom de domaine est traduit avec succès en adresse IP, on dit qu'il est « resolved ». Une attaque DNS est une tentative de couper un site Internet en interférant avec le répertoire qui lie le nom de domaine à l'adresse IP, de sorte qu'il ne puisse être *resolved*. Mais tout comme il existe différents annuaires téléphoniques, il existe de nombreux serveurs DNS différents. S'il est possible de rapidement changer de serveur DNS, il est possible de parer une attaque DNS et maintenir l'accès au site.

(4) Un système de mise en cache, est un système rapide qui ne contient initialement aucune information, mais qui est connecté à un système lent qui en contient. Lorsqu'on demande des informations au cache, il relaie d'abord la demande au système lent, transmet la réponse et en conserve une copie. Lorsque le cache est à nouveau sollicité, il transmet rapidement la copie qu'il a faite précédemment. WikiLeaks utilise de nombreuses technologies de localisation et de cryptage qui peuvent ralentir le chemin vers le « back end », où le contenu est généré. Dans ce contexte, un système de mise en cache vise à accélérer globalement un système, pour en améliorer l'utilisation par l'accélération des demandes répétées, c'est-à-dire la majorité des demandes.

(5) Un serveur caché, est un serveur qui n'est pas accessible par l'Internet ordinaire. WikiLeaks utilisait un logiciel personnalisé pour cacher certains de ses sites d'une manière à les rendre inaccessibles à la plupart des internautes. Le « back end » de WikiLeaks, c'est-à-dire le logiciel qui produit le site de WikiLeaks, demeurait caché. Du « back end » caché, le contenu a été poussé vers les nœuds frontaux par « tunneling » à travers le réseau Tor, c'est-à-dire en utilisant le réseau Tor, anonymisant et crypté, pour pousser le contenu vers les serveurs où les gens pourraient le lire. Le concept est similaire à celui du « service caché » de Tor.

Voir le site Tor Project : archive.today/tmQ5y.