LA VÉRITÉ SUR LE DARK WEB

Conçu pour protéger les dissidents politiques, il dissimule aussi des activités illicites

Aditi Kumar et Eric Rosenbach

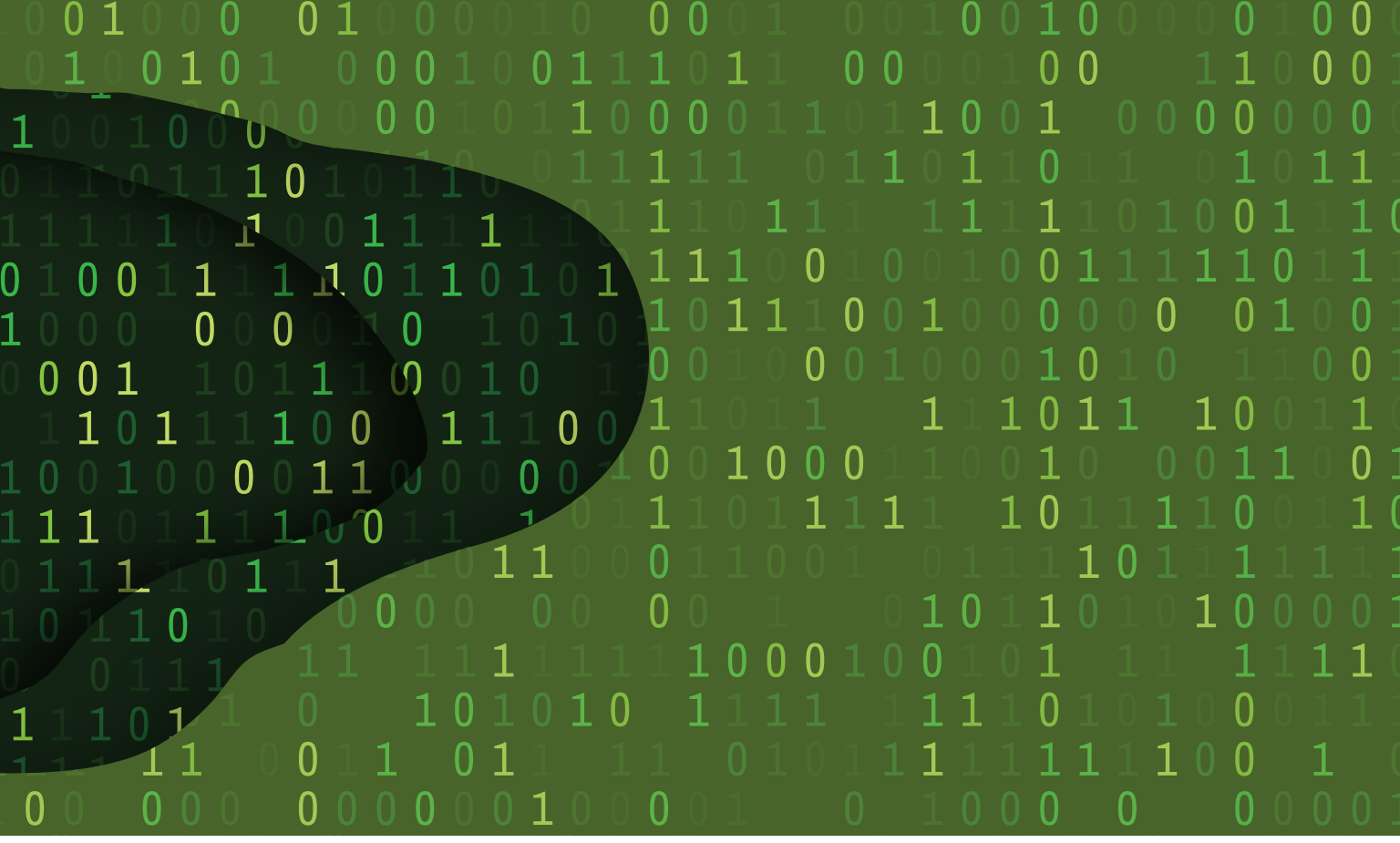
À la fin des années 90, deux organismes de recherche du ministère américain de la Défense ont piloté une initiative visant à élaborer un réseau anonyme et chiffré qui protègerait les communications sensibles des espions du pays. Les utilisateurs ordinaires d'Internet n'auraient pas connaissance de ce réseau secret et ne pourraient pas y avoir accès. Bien que l'objectif de clandestinité envisagé initialement ne se soit pas pleinement concrétisé, certains chercheurs ont vu dans ce projet une autre possibilité intéressante : le lancement d'un système non lucratif, axé sur l'anonymat, à destination des militants des droits humains et de la protection de la vie privée.

C'est ainsi qu'est né le réseau Tor, acronyme de « *The Onion Router* » (le routeur oignon), en référence aux nombreuses couches de chiffrement protégeant les informations qui y transitent. Tor se situe en marge d'Internet et constitue la technologie sous-jacente du « *dark web* » (le web obscur), un ensemble de sites cachés inaccessibles aux navigateurs classiques et non indexés par les moteurs de recherche comme Google. Le navigateur Tor, téléchargeable gratuitement, est le seul outil nécessaire pour déverrouiller cette partie cachée du web où le respect de la vie privée est le maître mot. Cependant, l'anonymat complet a de sombres conséquences.

En vérité, outre l'anonymat et la protection extrêmes que le dark web oppose à la surveillance des gouvernements autoritaires, il facilite le développement d'un marché clandestin que d'ingénieux criminels utilisent pour échanger des drogues, des identités volées, des contenus relatifs à des abus pédosexuels et d'autres produits et services illicites. Puisque les cryptomonnaies intraçables y représentent le principal moyen de paiement, il est nécessaire que les forces de l'ordre, les institutions financières et organismes de réglementation du monde entier coopèrent étroitement afin de resserrer l'étau autour de ces activités néfastes.

Les zones grises

Aujourd'hui, le réseau Tor compte plus de 65 000 URL uniques se terminant par .onion. Une étude réalisée en 2018 par la société de sécurité informatique Hyperion Gray a répertorié environ 10 % de ces sites et constaté que la plupart d'entre eux ont pour fonction de faciliter la communication, par des forums, des salons de discussion et des hébergeurs de fichiers et d'images, et le commerce sur des places de marché. Ces rôles fonctionnels, en particulier ceux liés à la communication, permettent de nombreux usages considérés comme légaux et légitimes dans les sociétés libres. En outre, une étude de 2016 de la société de recherche Terbium Labs,



pour laquelle 400 sites en .onion ont été sélectionnés au hasard et analysés, indique que plus de la moitié de tous les domaines du dark web sont en fait légaux.

Pour les habitants de pays où des régimes oppressifs bloquent l'accès à des pans entiers d'Internet ou répriment les dissensions politiques, le dark web est une bouée de secours qui leur donne accès à l'information et les protège de la persécution. Dans des sociétés plus libres, il peut constituer un outil essentiel d'alerte et de communication qui préserve les citoyens de représailles ou d'un jugement sur leur lieu de travail ou dans leur communauté. Il peut aussi simplement garantir le respect de la vie privée et de l'anonymat à ceux qui se méfient de la manière dont les entreprises et les États suivent, utilisent voire monétisent leurs données. De nos jours, de nombreuses organisations disposent d'un site Web caché sur Tor, y compris presque tous les grands journaux, Facebook et même la CIA, l'agence de renseignements américaine. En effet, avoir un site Web sur Tor montre un attachement, parfois symbolique, au respect de la vie privée. Le New York Times et la CIA, par exemple, espèrent encourager la communication avec des informateurs spontanés susceptibles de leur fournir des renseignements sensibles.

Le revers de la médaille est que ce respect de la vie privée et cet anonymat, qui protègent des tyrans et des publicités ciblées, font également du *dark web* un terreau fertile pour la criminalité. Les activités illicites qu'on y retrouve le plus sont notamment le trafic d'armes, le trafic de drogues et le partage de contenus relatifs à des pratiques d'exploitation, souvent d'enfants — pornographie ou images de violences et autres types d'abus. Certains sites Web soutiennent le discours de néonazis, de suprémacistes blancs et d'autres groupes extrémistes.

Pour les habitants de pays où des régimes oppressifs bloquent l'accès à des pans entiers d'Internet ou répriment les dissensions politiques, le dark web est une bouée de secours.

L'alliance des services proposés sur le dark web et des cryptomonnaies fait craindre une explosion de la criminalité. Il y a dix ans, un expert inconnu du chiffrement, spécialisé dans le décodage de mots de passe et se faisant appeler Satoshi Nakamoto, a mis au point la première monnaie et le premier réseau de paiement du monde qui ne soient pas contrôlés par un État : le Bitcoin. Moyen d'échange peu répandu utilisé à l'origine par la communauté technologique, le Bitcoin a émergé en 2011 comme la monnaie par excellence des trafiquants de drogue effectuant des transactions sur un site du dark web appelé Silk Road. Ces cinq dernières années, l'association d'un réseau chiffré inaccessible au plus grand nombre et d'une monnaie d'échange pratiquement intraçable pour les services répressifs a vu naître un marché, certes de petite taille mais important, pour des vendeurs illicites de marchandises illégales.

ILLUSTRATION : ISTOCK/TETIANA LAZUNOVA

De nombreuses menaces, parmi les plus dangereuses pour notre société, opèrent aujourd'hui dans l'ombre du réseau Tor et méritent donc l'attention d'enquêteurs internationaux.

Sur près de 200 noms de domaines classés comme illégaux par Terbium Labs, plus de 75 % sont des places de marché. La plupart sont alimentées par le Bitcoin et d'autres cryptomonnaies comme le Monero. Les produits les plus populaires sont les drogues récréatives et les médicaments, suivis de documents volés ou falsifiés tels que des pièces d'identité, des cartes de crédit et des identifiants bancaires. Certains sites proposent des services de piratage et de cybercriminalité, y compris des logiciels malveillants, des attaques par déni de service distribué et du piratage à la demande. Nombreux sont ceux qui proposent plusieurs de ces services et d'autres produits, notamment de la pornographie et des marchandises de contrefaçon.

Même si la gravité et la croissance rapide des transactions illicites sur le dark web ont de quoi préoccuper les États et les institutions financières mondiales, la part totale du commerce mondial effectué sur le dark web est minuscule, une fois rapportée au commerce illicite dans le monde. Un récent rapport de Chainalysis, société à la pointe dans l'analyse des cryptopaiements, montre que les transactions en Bitcoin sur le dark web sont passées d'environ 250 millions de dollars en 2012 à 872 millions en 2018. Cette société estime que les échanges de Bitcoin sur le dark web dépasseront le milliard de dollars en 2019. Si cela se vérifie, il s'agirait d'un niveau record de transactions illicites dans ce domaine. Ce même rapport indique également que la proportion de transactions en Bitcoin liées à des échanges illicites a diminué de 6 % depuis 2012 et représente maintenant moins d'un pourcent de l'ensemble des activités en Bitcoin. Dans un contexte encore plus vaste, les Nations Unies estiment que la quantité d'argent blanchi dans le monde en un an équivaut à 2 % à 5 % du PIB mondial, soit entre 1 600 et 4 000 milliards de dollars.

Même si le volume économique total des activités illicites sur le dark web reste relativement faible, de nombreuses menaces, parmi les plus dangereuses pour notre société, opèrent dans l'ombre du réseau Tor et méritent donc l'attention des législateurs, institutions financières et forces de l'ordre internationales.

Combattre l'ombre

La protection des dissidents politiques, des défenseurs de la vie privée et des lanceurs d'alerte ne devrait pas se faire au prix d'un pouvoir accru pour les bourreaux d'enfants, les trafiquants d'armes et les barons de la drogue. C'est là que réside le défi pour les législateurs et les services répressifs : élaborer des approches trouvant le juste équilibre entre la protection des principes de liberté dans une époque de contrôle de l'information, d'une part, et le repérage et l'élimination des activités les plus insidieuses du dark web, d'autre part. Ces dernières années, la communauté internationale a réalisé des progrès notables pour relever ces défis, en améliorant le partage de renseignements, en affinant les capacités techniques des forces de l'ordre pour fermer de grandes places de marché illicites, et en réglementant les transactions en cryptomonnaies.

La lutte contre les activités les plus néfastes du dark web suppose une amélioration du partage de renseignements entre les forces de l'ordre et les institutions financières. La nature mondiale de ce réseau rend nécessaire la coopération internationale. En 2018 et 2019, Interpol et l'Union européenne ont associé des forces de l'ordre de 19 pays afin d'identifier 247 cibles de grande importance, et partagé le type de renseignements opérationnels nécessaires à la répression. Les résultats sont prometteurs : rien que cette année, ces efforts concertés ont permis à des

membres du groupe de procéder à des arrestations et de fermer 50 sites illicites du dark web, notamment deux des plus grands marchés de stupéfiants, à savoir Wall Street Market et Valhalla.

La progression des transactions illégales sur le dark web a également poussé de nombreux États, partout dans le monde, à perturber les activités criminelles en améliorant les capacités des forces de l'ordre nationales. Aux États-Unis par exemple, le Federal Bureau of Investigation (FBI) aurait mené des opérations lui permettant de lever l'anonymat de serveurs Tor. Il y parvient en mettant en place des nœuds dans le réseau par lesquels il peut accéder à l'identité et à la localisation de certaines pages Web Tor illégales. La première action notable du FBI a été la fermeture du site Web « Silk Road 2.0 », qui était la plus importante place de marché illicite du dark web en 2014. L'enquête a révélé que, en deux ans et demi d'exploitation, ce site avait été utilisé par plusieurs milliers de trafiquants de drogue et autres vendeurs clandestins pour distribuer des centaines de kilos de drogues illégales et d'autres marchandises et services prohibés à plus de 100 000 acheteurs. Le site servait à blanchir des millions de dollars issus de ces transactions illicites. Au total, il a généré des ventes pour plus de 9,5 millions de Bitcoin, évalués à l'époque à environ 1,2 milliard de dollars. AlphaBay et Hansa, deux des plus gros successeurs de Silk Road, ont été fermés en 2017.

Les capacités répressives sur le dark web continuent de croître. Ainsi, les Pays-Bas ont récemment mené une opération de prise de contrôle d'un grand site de vente du dark web, qu'ils ont exploité anonymement pendant un mois, avant d'utiliser les renseignements collectés pour démanteler des dizaines d'autres sites de vente de ce réseau secret.

Adopter de nouvelles réglementations

En plus des opérations de démantèlement, les États et les institutions internationales cherchent à réglementer directement les cryptomonnaies qui alimentent les marchés du dark web. En juin 2019, par exemple, le Groupe d'action financière a publié une recommandation tendant à ce que les entreprises qui traitent des transferts de cryptomonnaies identifient à la fois l'expéditeur et le destinataire des transferts de fonds. Cette recommandation suit celle du sommet du G-20 de 2018, dans laquelle les dirigeants demandent aux organismes de réglementation internationaux d'examiner les mesures à prendre en matière de crypto-actifs, en particulier concernant la connaissance de la clientèle, la lutte contre le blanchiment de capitaux et le financement du terrorisme. L'écosystème des nouvelles entreprises proposant des places boursières, des portefeuilles et d'autres mécanismes de paiement en cryptomonnaies est loin de disposer de l'infrastructure nécessaire à l'adoption de normes semblables à celles du secteur financier, mais les organes de contrôle doivent commencer à poser les bases d'une amélioration de la surveillance. Le lancement imminent de la Libra, la cryptomonnaie de Facebook, ne fait que renforcer l'urgence de la question puisque les barrières à l'adoption d'actifs virtuels seront moindres pour les utilisateurs de ce réseau, qui seront bientôt plus de deux milliards.

Un équilibre délicat

Les régimes autoritaires vont poursuivre leurs efforts pour bloquer l'accès au dark web et à la menace qu'il constitue pour leur légitimité en permettant aux dissidents et aux activistes de s'organiser. Face à ce risque, les sociétés civiles libres auront naturellement tendance à défendre le statut non surveillé et non réglementé de Tor pour protéger la liberté d'expression et le respect de la vie privée. La réalité du dark web est bien plus complexe : les organes de contrôle et les services répressifs devront adopter une approche nuancée pour empêcher les activités considérées comme illégales et immorales dans des sociétés libres, tout en protégeant l'intérêt bien réel d'un réseau anonyme. FD

ADITI KUMAR est le directeur du Belfer Center for Science and International Affairs à la John F. Kennedy School of Government de l'université Harvard. **ERIC ROSENBACH** est codirecteur du Belfer Center et a précédemment occupé le poste d'adjoint du secrétaire à la défense américain pour la sécurité mondiale.