



# CHRONIQUES DES NOUVELLES CONFLICTUALITÉS



@David Arrowsmith/Unsplash

## Salt Typhoon : le retour des préoccupations sur le chiffrement

Par Fanny Tan

*La campagne d'espionnage massive des télécommunications par Salt Typhoon suscite de vives réactions à Washington. Face à la persistance de la menace, les autorités recommandent désormais l'usage de messageries chiffrées de bout en bout auprès de la population américaine. Si cette prise de position semble représenter une volte-face surprenante, elle illustre plutôt la volonté continue des autorités américaines de garder sa population à l'œil, au détriment de la sécurité nationale.*

Qualifiée de « pire piratage des télécommunications de l'histoire du pays » par l'ex-président de la Commission spéciale sur le renseignement du Sénat [Mark Warner](#), la campagne d'espionnage [révélée](#) à la fin du mois de septembre a semé la panique au gouvernement américain. Menée par Salt Typhoon, un groupe de menace persistante avancée (APT) [affilié](#) au ministère chinois de la Sécurité nationale, l'opération choque par son ampleur : jamais n'a-t-on rapporté une campagne d'espionnage aussi large visant des fournisseurs d'accès à Internet aux États-Unis. En infiltrant les systèmes d'au moins [neuf compagnies](#) de télécommunications depuis [2022](#), Salt Typhoon a pu géolocaliser et récolter les métadonnées de millions d'individus, en plus d'espionner le contenu des communications d'un plus petit nombre (à peu près 150), dont de hauts fonctionnaires américains et d'autres individus de haut profil, comme Donald Trump et JD Vance.

L'ampleur de l'attaque et la présence potentiellement continue des espions dans les systèmes informatiques ont conduit le FBI et l'agence de cyberdéfense américaine CISA à [recommander](#), auprès de la population américaine, l'utilisation de messageries chiffrées de bout en bout, comme Signal ou WhatsApp. Cette technique de chiffrement assure la confidentialité des communications en n'octroyant les clés de déchiffrement qu'à l'émetteur et au récepteur du message, rendant celui-ci [indéchiffrable](#) aux yeux de toute tierce partie, y compris du propriétaire des serveurs par lesquels transitent les messages.

### Une prise de position qui surprend

La prise de position des autorités américaines étonne. En effet, celles-ci ont toujours été hostiles vis-à-vis de l'accès généralisé à cette méthode de chiffrement qui les [empêcherait](#) d'enquêter sur des crimes graves, comme l'exploitation sexuelle de

mineurs ou les actes terroristes. Pourtant, la CISA et le FBI se défendent d'avoir fait volte-face, affirmant plutôt avoir toujours [appuyé](#) l'usage de telles méthodes... à condition de pouvoir conserver un accès privilégié leur permettant de déchiffrer les messages soi-disant confidentiels.

C'est dans cette conception d'un chiffrement « géré de [manière responsable](#) » que le bât blesse. Pour les défenseurs du chiffrement de bout en bout, exiger des compagnies technologiques qu'elles fournissent aux autorités un accès privilégié aux communications transitant dans de tels systèmes (via l'octroi de clés de déchiffrement ou encore, par l'implantation de portes dérobées) compromet l'intégrité du système lui-même en ouvrant la porte à l'infiltration d'acteurs malveillants. Au lendemain de la tuerie de masse de San Bernardino en 2015, le [patron](#) d'Apple avait notoirement [refusé](#) de se plier aux injonctions du FBI, qui lui demandait d'aider à déchiffrer le contenu de l'iPhone de l'un des perpétrateurs. Le PDG d'Apple avait alors déclaré que « les portes dérobées sont pour tout le monde : les bons, comme les méchants ». C'est d'ailleurs cet exact scénario qui s'est déroulé lors de la campagne d'espionnage de Salt Typhoon, où celui-ci aurait vraisemblablement réussi à infiltrer les systèmes [d'écoute téléphonique](#) mis en place par la justice américaine.

### Un débat qui persiste

Le débat opposant les défenseurs de la vie privée aux autorités américaines ne date pas d'hier. Pour [Andrew Crocker](#), directeur du département des litiges en matière de surveillance à l'Electronic Frontier Foundation (EFF), ces dernières ressassent les mêmes arguments « illogiques » depuis plus de 30 ans. C'est effectivement sous la présidence de Clinton en 1994 qu'a été mise en place la *Communications Assistance for Law Enforcement Act* (connue sous le nom de loi CALEA), qui aurait

originellement permis l'implantation des points d'accès [exploités](#) par Salt Typhoon. Dix ans plus tard, la loi a été modifiée de sorte à [élargir](#) considérablement sa portée pour inclure la possibilité de surveiller l'ensemble du trafic VoIP (*Voice over Internet Protocol*) et celui d'Internet à large bande. Pour l'experte en chiffrement [Susan Landau](#), l'espionnage massif des télécommunications par Salt Typhoon a bel et bien confirmé les inquiétudes de la communauté pro-chiffrement : la loi CALEA représente « une catastrophe pour la sécurité nationale qui ne demandait qu'à se produire ».

Si les autorités américaines continuent de défendre bec et ongles le chiffrement « géré de manière responsable » pour empêcher les criminels d'échapper à leur surveillance, leurs arguments peinent à convaincre. Les défenseurs du chiffrement soulignent que les autorités n'ont pas réellement besoin de la coopération des compagnies technologiques pour accéder aux contenus chiffrés de leurs utilisateurs, comme en témoigne [l'issue du litige](#) de 2016 avec Apple. En outre, on rappelle que les compagnies technologiques, dont plusieurs ont effectué un virage [pro-chiffrement](#) dans les dernières années, collaborent déjà abondamment avec la police. Elles sont d'ailleurs tenues légalement [responsables](#) de signaler aux autorités certains types de contenus nuisibles sous peine d'amende, ce qui devrait, en principe, minimiser la nécessité de vulnérabiliser les systèmes chiffrés de bout en bout par l'implantation d'accès extraordinaires. Finalement, l'efficacité de la gestion « responsable » du chiffrement de bout en bout a été remise en question par l'ancien avocat général du FBI, [Jim Baker](#), qui a admis en 2019 que le chiffrement n'a jamais représenté un réel obstacle aux enquêtes sur les actes terroristes aux États-Unis.

En bref, pour les défenseurs de la vie privée, la persistance des autorités américaines ne témoigne pas d'un besoin réel de protection, mais plutôt

d'un désir de contrôle toujours plus puissant face à la prolifération d'outils destinés à protéger la vie privée sur Internet, qui ont d'ailleurs connu un essor important à la suite des révélations [d'Edward Snowden](#) en 2013.

### Existe-t-il des alternatives?

Si le débat perdure, certains critiquent sa [vision binaire](#) qui oppose le « respect absolu de la vie privée » à « l'accès illimité aux données ». Un tel portrait ne rend pas justice aux multiples possibilités que possèdent déjà les agences de sécurité étatiques pour intercepter et déchiffrer les communications lors d'enquêtes, comme le piratage légal ou la divulgation forcée. Pour les analystes, bien que ces instruments légaux soient plus sécuritaires que ceux continuellement préconisés par les agences de sécurité américaines, ils doivent toutefois être utilisés raisonnablement et être [documentés](#) pour permettre un examen par le public et éviter qu'ils se transforment en outils de surveillance de masse.

D'autres alternatives ne nécessitant pas l'octroi d'un accès extraordinaire sur les données chiffrées en transit sont également explorées, notamment via le [Invest in Child Safety Act](#) et le [Technology in Criminal Justice Act](#). Ces projets de loi, s'attaquant respectivement à la pédopornographie et à la difficulté de collecter et d'utiliser les données acquises légalement, deux enjeux mis de l'avant par les autorités pour justifier la nécessité d'affaiblir le chiffrement, proposent des investissements financiers plus importants dans la lutte contre le cybercrime. De telles mesures pourraient aider les forces de l'ordre à accomplir plus efficacement leur travail sans compromettre la sécurité des systèmes informatiques des infrastructures critiques, comme les télécommunications.

## Le contexte canadien

Sans grand étonnement, les forces de l'ordre canadiennes reprennent elles aussi le narratif porté par les autorités américaines (et plus largement, du Groupe des cinq) qui [exigent](#), face à un monde virtuel de plus en plus « sombre », des options techniques leur permettant de déchiffrer les communications confidentielles en transit. Le ministère de la sécurité publique canadien [critique](#) le chiffrement, qu'il décrit comme « une mesure qui nuit de façon considérable à la capacité des organismes d'exécution de la loi et de sécurité nationale de mener des enquêtes dans le cyberspace ».

Si le ministère réitère l'importance de « mener des consultations rigoureuses auprès de la population », des groupes de défense des libertés civiles déplorent sa position, en rappelant qu'en plus d'affaiblir fondamentalement la sécurité des systèmes visés, la vulnérabilisation du chiffrement met à mal plusieurs [droits](#) garantis par la Charte canadienne des droits et libertés, comme la liberté d'expression, de religion, ou encore, de pensée.

Bien que le piratage de Salt Typhoon n'ait pas modifié la perception des forces de l'ordre sur les dangers de l'affaiblissement du chiffrement, le choc causé par cet incident apportera certainement un nouvel élan aux arguments de la communauté pro-chiffrement et pourrait inciter à explorer des solutions alternatives au-delà d'un débat binaire.

**Fanny Tan** est chercheure à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : <https://dandurand.uqam.ca>.

