Upstream Collection : surveillance massive NSA des câbles Internet

Stéphane FOSSE
fosse.fr

9 février 2026

Upstream Collection désigne l'ensemble des opérations par lesquelles la National Security Agency (NSA) des États-Unis intercepte directement les communications Internet sur les câbles de fibres optiques qui constituent l'infrastructure mondiale d'Internet. Contrairement au programme PRISM qui collecte les données auprès des fournisseurs de services comme Google ou Facebook, Upstream intercepte les communications « en vol », au moment où elles transitent physiquement sur les câbles. Depuis septembre 2003, quatre programmes distincts orchestrent cette surveillance : FAIRVIEW (partenariat avec AT&T depuis 1985), BLARNEY (autorité FISA depuis 1978), STORMBREW (Verizon depuis 2001) et OAKSTAR (huit sous-programmes internationaux depuis 2004). Ces programmes sont toujours actifs en 2026.

L'infrastructure d'Internet repose sur un réseau de câbles sous-marins en fibres optiques qui acheminent environ 80 % du trafic mondial. Les États-Unis occupent une position stratégique : une part considérable des communications internationales transite par leur territoire, même lorsque l'émetteur et le destinataire se trouvent tous deux à l'étranger. Cette particularité géographique et technique du réseau mondial explique pourquoi la NSA a développé des capacités d'interception massives sur le sol américain.

L'origine : de la Guerre froide aux attentats du 11 septembre

La surveillance des télécommunications par la NSA ne date pas d'hier. Le programme SHAMROCK, actif de 1945 à 1975, interceptait déjà les télégrammes internationaux. Avec l'avènement d'Internet dans les années 1990, les communications ont migré vers les câbles de fibres optiques. La NSA a alors adapté ses méthodes. Le programme BLARNEY démarre en 1978, la même année que le Foreign Intelligence Surveillance Act (FISA), la loi qui encadre théoriquement la surveillance à des fins de renseignement étranger.

FAIRVIEW, le plus ancien des programmes Upstream modernes, débute en 1985 avec AT&T. À cette époque, le démantèlement du monopole Bell vient de donner naissance à AT&T Communications, qui hérite du réseau longue distance. La NSA établit alors un partenariat que les documents internes qualifieront plus tard de « hautement collaboratif », louant « l'extrême volonté d'aider » de l'opérateur.

Mais c'est le 11 septembre 2001 qui marque l'accélération. Le lendemain des attentats, l'administration Bush lance le Terrorist Surveillance Program, un ensemble de programmes de surveillance sans mandat judiciaire. AT&T commence à transmettre e-mails et appels téléphoniques « en quelques jours », selon un rapport de l'inspecteur général de la NSA. En octobre 2001, les premières interceptions démarrent. STORMBREW, le partenariat avec Verizon, est mis en place la même année. OAKSTAR suivra en 2004 pour la surveillance hors du territoire américain.

La mécanique de l'interception : splitters optiques et salles secrètes

En 2006, Mark Klein, technicien chez AT&T à San Francisco pendant 22 ans, révèle l'existence de la Room 641A. Cette salle secrète de 24 pieds sur 48, située au 611 Folsom Street dans les bureaux centraux d'AT&T, abrite l'équipement d'interception de la NSA. Klein avait été chargé de connecter des circuits transportant les données Internet à des splitters optiques installés juste à l'extérieur de cette salle. Ces splitters, des dispositifs qui divisent un faisceau lumineux en deux sans l'altérer, créent une copie intégrale de tout le trafic circulant sur les câbles d'AT&T. Une copie est acheminée vers la salle 641A, inaccessible sauf à deux techniciens disposant d'une habilitation secret défense de la NSA.

Mark Klein apporte plus d'une centaine de pages de schémas techniques authentifiés à l'Electronic Frontier Foundation (EFF). Ces documents montrent que l'interception ne se limite pas au trafic d'AT&T : grâce aux accords de *peering* (interconnexion) entre opérateurs, les communications des clients d'autres fournisseurs transitant par le réseau AT&T sont également copiées. L'équipement installé dans la salle comprend notamment

un Narus STA 6400, un Semantic Traffic Analyzer fabriqué par une filiale de Boeing, capable de filtrer le trafic Internet à très haut débit.

Cette infrastructure n'est pas unique. Les documents révélés par Edward Snowden en 2013 montrent que FAIRVIEW dispose de neuf stations d'atterrissage de câbles sous-marins sur les côtes Est et Ouest des États-Unis. STORMBREW en compte huit, dont le site de BRECKENRIDGE, une installation de 10 000 pieds carrés certifiée en septembre 2009 et équipée de 15 systèmes TURMOIL offrant 150 gigabits par seconde de capacité de traitement. Le câble Trans-Pacific Express, reliant la côte Ouest américaine à cinq villes asiatiques, dont Shanghai et Tokyo, fait partie des accès STORMBREW.

Les quatre piliers d'Upstream : qui fait quoi

FAIRVIEW reste le programme phare. En septembre 2003, AT&T devient le premier partenaire à activer une nouvelle capacité de collecte que la NSA décrit comme une « présence en direct sur le réseau mondial ». Dès le premier mois, le programme transmet 400 milliards d'enregistrements de métadonnées Internet et achemine plus d'un million d'e-mails par jour vers le système de filtrage par mots-clés au siège de la NSA à Fort Meade, dans le Maryland. En 2011, AT&T fournit 1,1 milliard d'enregistrements d'appels de téléphones portables par jour. Le budget de FAIRVIEW atteint 188,9 millions de dollars en 2013, soit le double de STORMBREW.

BLARNEY fonctionne différemment. Ce n'est pas un partenariat avec un opérateur unique mais un programme-cadre qui regroupe les interceptions réalisées sous l'autorité du FISA original de 1978. Plus de trente compagnies télécoms coopèrent avec BLARNEY. Le programme produit environ 11 000 rapports par an et constitue l'une des sources principales du President's Daily Brief, le document quotidien ultra-confidentiel remis au président des États-Unis. PRISM, le programme d'accès aux serveurs des géants technologiques révélé par Snowden, est en réalité un sous-programme de BLARNEY, identifié par le code SIGAD US-984XN.

STORMBREW complète le dispositif côté Verizon. Avec un budget de 46,06 millions de dollars en 2013, le programme se concentre notamment sur le trafic vers et depuis la Chine. Les huit sites de collecte sous autorité Section 702 FAA portent les codes US-984XA à US-984XH. Le site BRECKENRIDGE a été financé à 100 % par la Comprehensive National Cybersecurity Initiative (CNCI) et visait spécifiquement à surveiller les communications transitant entre les États-Unis et la Chine.

OAKSTAR, avec son budget de 9,41 millions de dollars, orchestre la surveillance hors du territoire américain via huit sous-programmes. MONKEYROCKET cible l'Europe, le Moyen-Orient et l'Asie pour le contre-terrorisme. SHIFTINGSHADOW intercepte les télécommunications en Afghanistan, notamment les opérateurs MTN Afghanistan, Roshan GSM et Afghan Wireless. SILVERZEPHYR (SIGAD US-3273) collecte Internet et téléphonie en Amérique du Sud, Centrale et Latine en partenariat avec une compagnie codée STEELKNIGHT. YACHTSHOP capte les métadonnées Internet mondiales qui alimentent la base de données MARINA de la NSA. ORANGECRUSH, inactif lors des présentations NSA de 2011-2012, devait intercepter le trafic du Moyen-Orient et d'Afghanistan via un partenaire américain (PRIMECANE) et les services de renseignement polonais. Les trois derniers sous-programmes (ORANGEBLOSSOM, BLUEZEPHYR, COBALTFALCON) restent peu documentés.

Le cadre légal : Section 702 et zones grises

Après les révélations du New York Times en décembre 2005 sur le programme de surveillance sans mandat de l'administration Bush, le Congrès légalise rétroactivement ces pratiques. Le Protect America Act de 2007, puis le FISA Amendments Act de 2008, créent la Section 702 qui autorise la surveillance programmatique sans ordonnance individuelle pour chaque cible. La NSA peut cibler toute personne non-américaine située à l'étranger dès lors qu'un « but significatif » de la surveillance est de collecter des « renseignements de sécurité étrangère », une définition d'une ampleur remarquable.

Ce cadre juridique présente plusieurs particularités. La Section 702 distingue deux types de collecte : downstream (PRISM) et upstream (les quatre programmes dont il est question ici). Pour Upstream, la NSA ne demande pas directement les données aux fournisseurs de services. Elle les intercepte sur les câbles. Les opérateurs télécoms effectuent un premier filtrage, sélectionnant le trafic susceptible de contenir des communications étrangères. Puis la NSA applique des « sélecteurs forts » : numéros de téléphone, adresses e-mail, adresses IP de personnes ou organisations ciblées.

En 2011, une décision de la Foreign Intelligence Surveillance Court (FISC) révèle qu'Upstream collecte environ 9 % des 250 millions de communications Internet que la NSA acquiert chaque année sous Section 702. Cela représente 13,25 millions de communications pour le premier semestre 2011. Le pourcentage peut sembler modeste mais la cour souligne que cette collecte est particulièrement précieuse car elle capture des types spécifiques de renseignements étrangers. Elle ajoute une précision embarrassante : il est techniquement impossible pour la NSA d'exclure les communications purement domestiques de cette collecte massive.

Jusqu'en 2017, Upstream pratiquait la collecte « *about* » (au sujet de). Contrairement à la collecte « *to/from* » (vers/depuis) qui cible les communications envoyées ou reçues par un sélecteur, la collecte « *about* » scannait le contenu de toutes les communications pour y trouver une simple mention du sélecteur. Concrètement, chaque e-mail transitant sur les câbles était ouvert et analysé. En avril 2017, après des critiques du FISC sur la collecte abusive de dizaines de milliers de communications purement domestiques, la NSA suspend volontairement cette pratique. La loi de réautorisation de 2018 permet théoriquement sa reprise mais exige une notification préalable au Congrès. À ce jour, la collecte « *about* » n'aurait pas repris.

Les quatre autorités légales qui régissent Upstream créent des zones grises. Executive Order 12333 autorise la collecte hors des États-Unis (OAKSTAR principalement). FISA traditionnel (Title I) impose des ordonnances individuelles du FISC. Section 702 FAA permet le ciblage programmatique. Mais la quatrième autorité, Transit Authority, reste mystérieuse. Elle s'applique quand les deux extrémités d'une communication sont étrangères mais que celle-ci transite par les États-Unis. Sa base légale n'a jamais été clarifiée publiquement : directive présidentielle secrète ou autorisation de la FISC ? FAIRVIEW et SILVERZEPHYR opèrent notamment sous cette autorité.

Dimension internationale : GCHQ et les Five Eyes

La NSA ne travaille pas seule. Le Government Communications Headquarters (GCHQ) britannique mène des opérations similaires avec le programme TEMPORA, qui tapait plus de 200 câbles sous-marins dès 2011. Le GCHQ conserve les métadonnées pendant 30 jours et le contenu pendant 3 jours dans des *buffers* géants. En mai 2012, 300 analystes du GCHQ et 250 de la NSA triaient conjointement les données de TEMPORA, soit un volume de 21 pétaoctets par jour.

INCENSER, un sous-programme de TEMPORA (SIGAD DS-300), illustre la coopération transatlantique. Basé à Bude en Cornouailles, il collecte les données du câble FLAG Atlantic 1 qui relie l'Amérique du Nord au Royaume-Uni et à la France. Le partenaire corporatif, Cable & Wireless (racheté par Vodafone en 2012), porte le nom de code GERONTIC. Les données transitent via le système TICKETWINDOW qui les partage avec les partenaires des Five Eyes (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande). Au Moyen-Orient, la base secrète de Seeb à Oman (OPC-1) permet au GCHQ d'accéder à neuf câbles sous-marins traversant le détroit d'Ormuz.

Volume et portée : qui est surveillé ?

Évaluer le nombre exact de personnes espionnées relève de l'impossible. La NSA surveillait 89 138 cibles en 2013, 92 707 en 2014, 94 368 en 2015. Mais ces chiffres ne comptabilisent que les cibles principales sous Section 702. Pour chaque cible, au moins un Américain voit ses communications collectées « incidemment ». Le chiffre réel pourrait atteindre plusieurs millions selon une opinion de la FISC de 2015 qui évoque des « quantités substantielles » de communications d'Américains.

Les Single Communications Transactions (SCT) et Multi-Communication Transactions (MCT) compliquent le tableau. Un SCT correspond à une communication simple, comme la visite d'une page web. Un MCT regroupe plusieurs communications distinctes dans une seule transaction. L'exemple donné par l'Office of the Director of National Intelligence : ouvrir sa boîte mail affiche les en-têtes et extraits des 15 ou 25 derniers messages. Une seule transaction, des dizaines de communications collectées si l'une d'elles est « *to* », « *from* » ou « *about* » le sélecteur.

La géographie du réseau Internet aggrave la collecte incidente. Une communication entre deux Français peut très bien transiter par les États-Unis si c'est le chemin le moins coûteux pour les opérateurs. Les protocoles de routage BGP optimisent les coûts, pas la géographie. Résultat : des communications purement européennes, africaines ou asiatiques se retrouvent copiées sur le sol américain simplement parce qu'elles ont emprunté un câble trans-atlantique.

Concernant la revente de données sur le dark web, aucun élément des documents Snowden ou des rapports officiels ne l'évoque. La NSA collecte pour le renseignement, pas pour un commerce illégal. Cela ne signifie pas que les données soient totalement sécurisées. En 2013, Snowden lui-même a exfiltré des milliers de documents classifiés. D'autres fuites sont possibles. Mais le modèle économique d'Upstream n'est pas celui du vol et de la revente : c'est celui de la surveillance étatique massive.

État actuel et perspectives

En 2026, Upstream Collection demeure actif. La Section 702 a été réautorisée en 2018 avec quelques modifications : obligation de développer des procédures spécifiques pour les requêtes concernant des personnes

américaines, interdiction conditionnelle de la collecte « *about* ». En avril 2024, le Reforming Intelligence and Securing America Act (RISAA) prolonge une nouvelle fois l'autorisation jusqu'en 2030, malgré les critiques d'organisations de défense des droits civiques comme l'EFF et l'ACLU.

Les budgets donnent une indication de l'ampleur. En 2013, les quatre programmes Upstream totalisaient environ 310 millions de dollars. Les Special Source Operations (SSO), la division de la NSA responsable de ces programmes, représentent plus de 80 % de l'information collectée par l'agence selon un document interne.

Mark Klein est décédé en mars 2025 à l'âge de 79 ans. Les deux procès qu'il avait contribué à lancer avec l'EFF, Hepting v. AT&T et Jewel v. NSA, ont été rejetés. Le premier après que le Congrès ait accordé l'immunité rétroactive aux opérateurs télécoms en 2008. Le second pour défaut de standing : les plaignants ne pouvaient pas prouver qu'ils avaient personnellement subi un préjudice par la surveillance, puisque la NSA refuse de confirmer ou d'infirmer qui est surveillé.

Upstream Collection pose une question fondamentale : peut-on considérer Internet comme un réseau de communication privé ? La réponse technique est non. Toute communication transitant par un câble accessible à la NSA ou au GCHQ peut être copiée, analysée, stockée. Le chiffrement de bout en bout (*end-to-end encryption*) protège le contenu mais pas les métadonnées : qui parle à qui, quand, d'où, combien de temps. Ces métadonnées suffisent souvent à reconstruire des informations sensibles.

Les solutions existent mais restent partielles. Utiliser Tor pour anonymiser le trafic, privilégier les VPN qui ne conservent pas de logs, chiffrer systématiquement les communications avec des protocoles vérifiés, éviter les services hébergés aux États-Unis pour les données sensibles. Mais tant que l'infrastructure physique d'Internet repose sur des câbles contrôlés par quelques nations et quelques opérateurs, la surveillance de masse restera techniquement possible. La question n'est pas technique, elle est politique.

Références

[1] Julia Angwin et al. A Trail of Evidence Leading to AT&T's Partnership with the NSA. In : *ProPublica* (15 août 2015).

[2] Julia Angwin et al. NSA Spying Relies on AT&T's 'Extreme Willingness to Help'. In : *ProPublica & The New York Times* (15 août 2015).

[3] Electronic Frontier Foundation. Foreign Intelligence Information, PRISM, and Upstream Collection.

[4] Electronic Frontier Foundation. In Memoriam: Mark Klein, AT&T Whistleblower Who Revealed NSA Mass Spying. 12 mars 2025.

[5] Electrospaces.net. FAIRVIEW: Collecting foreign intelligence inside the US. Août 2015.

[6] Electrospaces.net. Slides about NSA's Upstream collection. Jan. 2014.

[7] David Lyon. Surveillance, Snowden and Big Data: Capacities, consequences, critique. In : *Big Data & Society* (2014).

[8] National Security Archive. NSA PRISM and Upstream Briefing Slides. documents Edward Snowden. George Washington University.

[9] PBS Frontline. Interviews - Mark Klein | Spying On The Home Front. 9 jan. 2007.

[10] Privacy and Civil Liberties Oversight Board. Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. 2 juill. 2014.

[11] Privacy and Civil Liberties Oversight Board. Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. 2023.

[12] Robin Simcox. Surveillance After Snowden: Effective Espionage in an Age of Transparency. Henry Jackson Society, juin 2015.

[13] The Ohio State University. The NSA, AT&T, and the Secrets of Room 641A. In : *I/S: A Journal of Law and Policy for the Information Society* 3.3 (2007).