Programme Muscular : L'espionnage de masse des géants du cloud

Stéphane FOSSE
fosse.fr

19 janvier 2026

Le programme Muscular (nom de code DS-200B) constitue l'une des opérations de surveillance les plus sophistiquées et controversées révélées par Edward Snowden. Cette collaboration secrète entre la NSA américaine et le GCHQ britannique a permis l'interception massive de données circulant entre les centres de données de Google et Yahoo !, collectant 181 millions d'enregistrements en seulement 30 jours sans le consentement de ces entreprises [1]. Les révélations d'octobre 2013 ont déclenché une transformation fondamentale de la sécurité informatique mondiale et redéfini les relations entre les géants technologiques et les gouvernements.

Naissance d'un programme d'espionnage moderne

Le programme Muscular voit le jour en 2009, dans le contexte post-11 septembre d'expansion massive des capacités de surveillance occidentale. Créé comme une collaboration directe entre la NSA et le GCHQ, il s'inscrit dans le programme-parapluie WINDSTOP, exploitant les partenariats avec les « parties tierces de confiance » de l'alliance Five Eyes (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande) [2].

L'innovation stratégique du programme résidait dans son approche technique : plutôt que de demander l'accès aux données via des procédures judiciaires, Muscular interceptait directement les communications circulant entre les centres de données des entreprises technologiques. Cette méthode « backdoor » permettait une collecte bien plus massive – deux fois supérieure aux volumes de PRISM – tout en échappant aux contraintes légales américaines [3].

Le nom de code DS-200B désignait le point d'accès technique situé au Royaume-Uni, où le GCHQ opérait physiquement le programme avant de transférer quotidiennement des millions d'enregistrements vers Fort Meade, le siège de la NSA dans le Maryland. Cette architecture transnationale était volontairement conçue pour contourner les protections légales nationales, exploitant les différences juridiques entre les pays alliés.

L'ingénierie de l'interception : méthodes techniques révolutionnaires

L'aspect le plus impressionnant du programme Muscular résidait dans sa sophistication technique. Les agences de renseignement exploitaient une vulnérabilité fondamentale de l'architecture cloud de l'époque : l'absence de chiffrement des liaisons entre centres de données.

La technologie des *splitters* optiques constituait l'outil principal d'interception. Ces dispositifs, installés sur les câbles à fibre optique reliant les centres de données Google et Yahoo !, divisaient le signal lumineux en deux flux : l'un continuait vers sa destination normale, l'autre était dévié vers l'équipement de surveillance. Cette méthode d'interception passive était pratiquement indétectable, n'introduisant qu'une légère atténuation du signal [4].

Les équipements Glimmerglass, utilisant la technologie MEMS (Micro-Electro-Mechanical Systems) avec 210 micro-miroirs dorés de 1 mm de diamètre, permettaient un contrôle à distance sophistiqué du routage des signaux optiques. Le logiciel CyberSweep analysait automatiquement le trafic Gmail, Yahoo ! Mail, Facebook et Twitter, extrayant les informations « exploitables » en temps réel.

Les points d'interception géographiques étaient stratégiquement positionnés. Le centre de Bude en Cornouailles, développé avec un financement NSA de 25 millions de dollars en 2009, pouvait traiter 201 liens Internet à 10 Gbps chacun. Des installations similaires existaient à Seeb (Oman) sur 9 câbles sous-marins, et aux États-Unis dans la célèbre Room 641A de San Francisco, équipée d'analyseurs sémantiques de trafic Narus STA 6400 [5].

Le programme exploitait particulièrement les formats propriétaires des entreprises. Pour Yahoo !, l'interception du format NArchive – contenant des comptes email complets avec des années de messages – prouvait l'accès aux systèmes internes les plus sensibles. Les documents NSA montraient fièrement des schémas où le chiffrement était « ajouté et retiré » aux points de terminaison, accompagnés du célèbre smiley face dessiné à la main.

Documents Snowden : l'anatomie d'une révélation historique

L'exposition publique du programme Muscular a eu lieu le 30 octobre 2013. Barton Gellman du Washington Post et son collègue Ashkan Soltani publient l'article révélateur basé sur des documents internes NSA d'une précision technique stupéfiante [1].

Le document le plus iconique reste la présentation PowerPoint « Google Cloud Exploitation » montrant l'intersection entre « Internet Public » et « Google Cloud », avec la note manuscrite sarcastique « encryption added and removed here ! :-) ». Cette image cristallisera la colère publique et les réactions corporatives, un ingénieur Google déclarant publiquement : « *Fuck these guys.* J'ai passé les dix dernières années de ma vie à essayer de garder les utilisateurs de Google en sécurité ».

Les documents révèlent l'ampleur opérationnelle du programme :

— 181 280 466 nouveaux enregistrements collectés en 30 jours (décembre 2012-janvier 2013)

— Transfert quotidien de millions d'enregistrements vers Fort Meade

— Stockage tampon de 3 à 5 jours chez GCHQ pour traitement initial

— Capacités de traitement dépassant parfois les systèmes, causant des saturations lors des migrations techniques de Yahoo !

L'email GCHQ-NSA du 24 novembre 2009 mentionnant explicitement Muscular prouve l'ancienneté de la collaboration, tandis que les rapports d'activité NSA de mars 2013 documentent méticuleusement les volumes et types de données collectées. Ces documents constituent une archive unique des capacités de surveillance moderne, validée par des experts techniques qui ont confirmé l'authenticité des formats de données internes jamais vus publiquement.

De l'indignation à la transformation

La révélation du programme Muscular a provoqué des réactions corporatives sans précédent, marquant une rupture définitive dans les relations entre l'industrie technologique et les agences de renseignement.

Google réagit avec une indignation publique rare. David Drummond, Chief Legal Officer, déclare l'entreprise « indignée par les longueurs auxquelles le gouvernement semble être allé pour intercepter les données de nos réseaux de fibres privées » [6]. La réaction la plus symbolique vient de l'ingénieur Brandon Downey, qui compare sur Google+ la découverte du programme à « rentrer de la guerre contre Sauron, détruire l'Anneau Unique, pour découvrir que la NSA est sur le porche du Comté en train de couper l'Arbre de la Fête ».

Yahoo !, ayant précédemment mené une bataille juridique secrète contre PRISM en 2007-2008, nie catégoriquement avoir donné accès volontaire à ses systèmes [7]. La société avait été contrainte de participer à PRISM sous peine d'amendes de 250 000 dollars par jour, rendant la découverte de l'accès non-autorisé via Muscular particulièrement amère.

Microsoft adopte une approche plus diplomatique mais tout aussi significative, annonçant en décembre 2013 des plans de chiffrement renforcé tout en utilisant l'expression « menace persistante avancée » – terminologie habituellement réservée aux hackers parrainés par des États hostiles, interprétée comme une comparaison directe de la NSA aux cybercriminels chinois.

La transformation technique de l'industrie s'avère immédiate et radicale. En novembre 2013, soit trois semaines après les révélations, Google et Yahoo ! annoncent simultanément l'accélération du déploiement du chiffrement entre leurs centres de données [8]. Cette course au chiffrement, qualifiée par un responsable Google de « course aux armements » contre les agences gouvernementales, transforme fondamentalement l'architecture de sécurité d'Internet.

L'impact économique se révèle considérable : le marché du chiffrement, évalué à 13,4 milliards de dollars en 2022, atteint une projection de 38,5 milliards de dollars en 2030, avec une croissance de 16,3% par an directement attribuable aux réformes post-Snowden. Les entreprises européennes exploitent la défiance envers les services cloud américains pour développer des alternatives « souveraines », forçant les géants américains à investir massivement dans la localisation des données et les certifications de sécurité.

Architecture juridique : entre vides légaux et réformes incomplètes

Le programme Muscular illustre parfaitement les zones grises juridiques exploitées par les agences de renseignement modernes. Contrairement au programme PRISM qui opérait sous mandats FISA, Muscular fonctionnait exclusivement sous l'autorité de l'Executive Order 12333 de 1981, évitant toute supervision judiciaire [9].

Cette base légale permettait la surveillance à l'étranger sans contrôle, le point d'accès DS-200B étant stratégiquement situé au Royaume-Uni pour échapper aux protections du 4^{e} Amendement américain. Le

GCHQ opérait techniquement le programme sous l'Intelligence Services Act 1994 britannique, partageant automatiquement les données avec la NSA via les accords secrets UKUSA de 1946.

L'alliance Five Eyes fournissait le cadre institutionnel permettant ce contournement des lois nationales [10]. Chaque pays exploitait les capacités techniques de ses partenaires pour surveiller ses propres citoyens par procuration, une pratique que le Rapporteur Spécial des Nations Unies qualifiera plus tard d'illégale.

Les révélations Snowden déclenchent des réformes législatives significatives mais incomplètes. L'USA Freedom Act de 2015 met fin à la collecte de masse des métadonnées téléphoniques sous la Section 215, introduit un « avocat spécial » à la Cour FISA, et exige des mandats individualisés [11]. Cependant, ces réformes ne touchent pas la surveillance sous Executive Order 12333, laissant des programmes comme Muscular techniquement toujours possibles.

Le Privacy and Civil Liberties Oversight Board, dans son rapport 2014, conclut que le programme Section 215 « manque de fondement légal viable » et que la collecte de masse n'a « pas contribué de manière unique » à la prévention terroriste [12]. Ses recommandations pour réformer EO 12333 sont largement ignorées par l'administration Obama puis Trump.

En Europe, la Cour Européenne des Droits de l'Homme rend en 2021 un arrêt historique condamnant le régime britannique de surveillance massive pour violation des articles 8 (vie privée) et 10 (liberté d'expression) de la Convention [13]. La Cour affirme qu'un « système de surveillance secrète peut détruire la démocratie sous prétexte de la défendre », exigeant une autorisation indépendante obligatoire.

Coopération NSA-GCHQ : anatomie d'une alliance secrète

La collaboration NSA-GCHQ dans le programme Muscular révèle l'intégration opérationnelle des agences de renseignement anglo-saxonnes. Cette coopération dépasse le simple partage d'informations pour atteindre une véritable fusion des capacités techniques et des infrastructures de surveillance.

Le GCHQ opérait comme maître d'œuvre technique du programme, exploitant sa position géographique privilégiée aux points d'atterrissage des câbles sous-marins européens. Le centre de Bude en Cornouailles, financé conjointement par la NSA pour 25 millions de dollars, traitait le trafic de 201 liens Internet à 10 Gbps chacun, soit une capacité théorique de plus de 2 térabits par seconde.

Cette architecture transnationale permettait un contournement sophistiqué des contraintes légales. La NSA ne pouvait pas intercepter directement les communications de Google et Yahoo ! depuis le territoire américain sans mandats FISA, mais pouvait recevoir ces mêmes données via le GCHQ sous prétexte de coopération internationale. Réciproquement, le GCHQ accédait aux capacités d'analyse avancées de la NSA, notamment le système TURMOIL de traitement de données et XKEYSCORE d'analyse en temps réel.

Les accords de partage techniques révélés montrent une intégration opérationnelle totale : personnel échangé, bases partagées, budgets communs, et même systèmes informatiques interconnectés. Les coûts du programme étaient répartis selon les capacités : le GCHQ fournissait l'infrastructure d'interception physique, la NSA apportait les capacités de stockage et d'analyse massive à Fort Meade.

Cette coopération s'étendait aux opérateurs de télécommunications via des partenariats secrets obligatoires. BT (nom de code REMEDY), Vodafone/Cable & Wireless (GERONTIC), et Level 3 Communications (LITTLE) fournissaient l'accès physique aux câbles contre paiements secrets et sous contrainte légale. Le GCHQ versait des millions de livres annuels à ces « intercept partners » tout en leur imposant des ordres de silence juridiquement contraignants.

Impact transformationnel sur la cybersécurité mondiale

Les révélations du programme Muscular ont déclenché une révolution de la sécurité informatique dont les effets se prolongent encore aujourd'hui. Cette transformation dépasse largement les réactions immédiates des entreprises ciblées pour restructurer fondamentalement l'architecture de sécurité d'Internet.

L'adoption massive du chiffrement constitue l'effet le plus visible. En novembre 2013, Google accélère le déploiement du chiffrement entre ses centres de données, une mesure qui était prévue pour 2020 [14]. Yahoo ! suit immédiatement avec des annonces similaires, tandis que Microsoft généralise le chiffrement à tous ses services cloud (Outlook, Office 365, OneDrive). Cette course au chiffrement transforme en quelques mois ce qui était prévu sur une décennie.

L'initiative « Encrypt All The Things » de l'industrie technologique généralise l'adoption du HTTPS sur le web. Le pourcentage de sites web utilisant le chiffrement SSL/TLS passe de 30% en 2013 à plus de 95% aujourd'hui, une transformation directement attribuable aux révélations Snowden. Google modifie même son algorithme de recherche pour favoriser les sites chiffrés, accélérant cette transition.

Les architectures « Zero Trust » émergent comme nouveau paradigme de sécurité. Le principe de « ne jamais faire confiance, toujours vérifier » remplace les modèles traditionnels de périmètre de sécurité, assumant que

toute communication peut être interceptée. Cette approche, initialement développée par Google après Muscular, devient le standard industriel pour les entreprises et administrations, même si dans les faits elle reste complexe à mettre en œuvre.

L'impact sur l'industrie de la cybersécurité s'avère considérable. Le marché global de la cybersécurité croît de 16,3% par an, atteignant 345 milliards de dollars en 2024. Les investissements en R&D sécuritaire explosent, financés par la prise de conscience que les gouvernements alliés constituent des menaces aussi sophistiquées que les États hostiles.

Au niveau géopolitique, les révélations alimentent les initiatives de « souveraineté numérique » européenne et asiatique. L'UE développe le RGPD partiellement en réaction à la surveillance américaine, tandis que la Chine et la Russie renforcent leurs « murailles numériques » nationales. Ces fragmentations du cyberespace, directement issues des révélations Snowden, restructurent durablement l'Internet global.

Réformes et persistance des vulnérabilités

Douze ans après les révélations Snowden, le bilan des réformes reste contrasté et incomplet. Si certaines pratiques ont effectivement changé, les capacités de surveillance de masse demeurent largement intactes, simplement déplacées vers des cadres juridiques moins visibles.

L'USA Freedom Act de 2015 constitue la réforme la plus visible, mettant fin à la collecte de masse des métadonnées téléphoniques sous la Section 215 du Patriot Act. Cependant, cette réforme ne touche pas l'Executive Order 12333, sous lequel opérait Muscular. La NSA continue de collecter « 5 milliards d'enregistrements téléphoniques par jour » via cette autorité, sans supervision judiciaire effective.

Les accords Five Eyes demeurent largement non-réformés. Les arrangements détaillés restent classifiés, et aucun cadre légal public ne régit les échanges d'intelligence entre alliés. Cette opacité permet la poursuite du contournement des protections légales nationales via la coopération internationale, le mécanisme fondamental exploité par Muscular.

La supervision parlementaire reste structurellement inadéquate. La Cour FISA maintient un taux d'approbation supérieur à 99% des demandes gouvernementales, malgré l'introduction de « l'avocat spécial » en 2015. Le Privacy and Civil Liberties Oversight Board, créé pour surveiller les programmes de surveillance, opère avec des ressources limitées et des pouvoirs consultatifs seulement.

Plus préoccupant encore, les capacités techniques révélées par Muscular ont été étendues et perfectionnées. Les agences de renseignement exploitent désormais l'intelligence artificielle pour l'analyse massive de données, développent des capacités quantiques pour casser le chiffrement futur, et exploitent l'Internet des Objets pour de nouvelles formes de surveillance. Le Programme Upstream de la NSA, qui intercepte les communications sur les « backbone » Internet, continue d'opérer avec des capacités élargies.

L'émergence de nouveaux acteurs complique encore le paysage. La Chine, la Russie, et d'autres puissances développent leurs propres programmes Muscular, exploitant les vulnérabilités révélées par Snowden tout en évitant les contraintes juridiques occidentales. Cette prolifération des capacités de surveillance étatique transforme la cybersécurité en véritable course aux armements technologique.

L'héritage durable d'une révélation historique

Le programme Muscular restera dans l'histoire comme le révélateur d'une époque charnière entre l'Internet naïf des débuts et le cyberespace militarisé contemporain. Cette opération de surveillance, par sa sophistication technique et son audace juridique, a cristallisé les tensions fondamentales entre sécurité nationale, innovation technologique et droits individuels qui définissent notre époque numérique.

L'impact transformationnel sur l'industrie technologique s'avère irréversible. Le chiffrement, jadis domaine réservé aux experts en sécurité, est devenu ubiquitaire. Les architectures « Zero Trust », nées de la méfiance envers la surveillance gouvernementale, constituent désormais le standard de sécurité pour les entreprises mondiales. Cette militarisation défensive de l'Internet civil, directement causée par les révélations Snowden, restructure fondamentalement l'économie numérique.

Paradoxalement, le programme Muscular a également démontré les limites de la surveillance de masse. Malgré la collecte de 181 millions d'enregistrements mensuels, aucune preuve n'a émergé d'une contribution unique à la prévention terroriste. Cette disproportion entre capacités techniques et résultats opérationnels alimente encore aujourd'hui les débats sur l'efficacité réelle de la surveillance massive.

L'héritage juridique reste problématique. Si les réformes post-Snowden ont introduit des garde-fous importants, les mécanismes fondamentaux exploités par Muscular – Executive Order 12333, accords Five Eyes, surveillance étrangère sans mandat – demeurent largement intacts. Cette persistance des « zones grises » légales garantit que des programmes similaires restent techniquement possibles, simplement mieux dissimulés.

Sur le plan géopolitique, Muscular a accéléré la fragmentation de l'Internet global. Les initiatives de souveraineté numérique, nées de la méfiance envers la surveillance américaine, fragmentent le cyberespace en blocs régionaux de plus en plus étanches. Cette balkanisation, contraire à la vision originelle d'un Internet universel, constitue peut-être l'effet le plus durable des révélations de 2013.

Le programme Muscular illustre parfaitement la tension irréductible entre les capacités techniques modernes et les cadres démocratiques traditionnels. La possibilité technique de surveiller massivement les communications mondiales existe et persistera. La question n'est plus de savoir si de tels programmes sont possibles, mais comment les sociétés démocratiques peuvent maintenir un contrôle effectif sur des capacités qui, par nature, opèrent dans l'ombre et transcendent les frontières nationales.

L'enjeu contemporain ne réside plus dans la révélation de programmes secrets – les capacités sont désormais connues – mais dans l'invention de nouveaux mécanismes démocratiques adaptés à l'ère de la surveillance algorithmique. Le programme Muscular, par les transformations qu'il a déclenchées, demeure ainsi une référence fondamentale pour comprendre les défis de gouvernance du XXI^{e} siècle numérique.

Références

[1] B. Gellman et A. Soltani, NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post, oct. 2013.

[2] B. Gellman, PRISM already gave the NSA access to tech giants. Here's why it wanted more, The Washington Post, oct. 2013.

[3] A. Soltani et B. Gellman, How we know the NSA had access to internal Google and Yahoo cloud data, The Washington Post, nov. 2013.

[4] B. Schneier, NSA Eavesdropping on Google and Yahoo Networks, Schneier on Security, oct. 2013.

[5] D. Campbell, GCHQ's Middle East cable tap centre revealed, DuncanCampbell.org, 2013.

[6] NPR Staff, Report: NSA Has Broken Into Google And Yahoo Data Centers, NPR, oct. 2013.

[7] CBS News, Yahoo waged court fight with U.S. government over surveillance, CBS News, sept. 2014.

[8] B. Gellman et A. Soltani, NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post, oct. 2013.

[9] Electronic Frontier Foundation, A Primer on Executive Order 12333: The Mass Surveillance Starlet, Electronic Frontier Foundation, juin 2014.

[10] Privacy International, Five Eyes, Privacy International, 2023.

[11] P. Williams, Barack Obama Signs 'USA Freedom Act' to Reform NSA Surveillance, NBC News, juin 2015.

[12] American Civil Liberties Union, What's Next for Surveillance Reform After the USA Freedom Act, American Civil Liberties Union, juin 2015.

[13] Amnesty International, UK: Europe's top court rules UK mass surveillance regime violated human rights, Amnesty International, mai 2021.

[14] Harvard Journal of Law & Technology, Google Encrypts Its Network to Counteract NSA Surveillance, Harvard Journal of Law & Technology, 2014.

[15] R. Gallagher, NSA MUSCULAR program: Spying on Google and Yahoo, Slate, oct. 2013.

[16] T. Simonite, NSA Takes Huge Amounts of Data from Google and Yahoo, MIT Technology Review, oct. 2013.

[17] PBS NewsHour, NSA 'taking full advantage' of spying laws to tap into Yahoo, Google traffic, PBS, oct. 2013.

[18] E. Perez et S. Prokupecz, NSA chief addresses report that agency taps into Google, Yahoo data links, CNN, oct. 2013.

[19] Brennan Center for Justice, Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page, Brennan Center for Justice, 2023.

[20] American Civil Liberties Union, New NSA Documents Shine More Light into Black Box of Executive Order 12333, American Civil Liberties Union, nov. 2016.

[21] J. N. Tye, Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans, The Washington Post, juill. 2014.

[22] Yale Law School, Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements, Yale Law School, 2016.

[23] Global Information Society Watch, Unmasking the Five Eyes' global surveillance practices, Global Information Society Watch, 2016.

[24] E. Nakashima, Congressional action on NSA is a milestone in the post-9/11 world, The Washington Post, juin 2015.

[25] R. Speed, 10 years after Snowden's first leak, what have we learned? The Register, juin 2023.

[26] A. Deeks, The Snowden Effect, Six Years On, Just Security, juin 2019.

[27] S. Spaulding et C. Inglis, Why dismantling the PCLOB and CSRB threatens privacy and national security, Brookings Institution, jan. 2025.

[28] Electronic Frontier Foundation, The Privacy and Civil Liberties Oversight Board Signals It Will investigate NSA Surveillance, Facial Recognition, and Terror Watchlists, Electronic Frontier Foundation, juill. 2019.

[29] C. Nyst, The UN privacy report: Five Eyes remains, openDemocracy, sept. 2022.

[30] P. Judge, Report: Google doubles down on inter-data center encryption, Data Center Dynamics, nov. 2013.