Stellar Wind
L'anatomie d'un programme de surveillance de masse

Stéphane FOSSE
fosse.fr

16 décembre 2025

Le 11 septembre 2001 a constitué un tournant dans l'histoire de la surveillance électronique aux États-Unis. Dans les semaines qui ont suivi les attentats, l'administration Bush a mis en place un programme secret d'écoutes sans mandat qui allait s'avérer être l'un des systèmes de surveillance domestique les plus vastes jamais déployés par la National Security Agency. Son nom de code : Stellar Wind.

Un programme né dans l'urgence

Stellar Wind a été officiellement autorisé pour la première fois par le président George W. Bush le 4 octobre 2001, moins d'un mois après les attentats. Le programme a été périodiquement réautorisé par des documents présidentiels successifs jusqu'en février 2007, totalisant 43 autorisations présidentielles distinctes sur toute sa durée d'existence.

L'ampleur de ce programme était sans précédent. Selon William Binney, ancien cryptologue de la NSA, Stellar Wind s'appuyait sur un réseau de salles d'écoute sans fenêtres réparties dans tout le pays, connues sous le nom de *switches*, qui permettaient d'accéder aux communications internationales et domestiques. Des opérateurs de télécommunications majeurs comme AT&T et Verizon ont été intégrés dans ce vaste réseau d'écoute.

Les trois paniers de la surveillance

L'information collectée par Stellar Wind se divisait en trois catégories distinctes, souvent désignées par le terme de paniers (*baskets*) :

Panier 1 : Le contenu des communications

Ce premier panier comprenait l'interception du contenu des appels téléphoniques et des courriels. Contrairement aux métadonnées, il s'agissait ici de la substance même des conversations et des messages échangés.

Panier 2 : Les métadonnées téléphoniques

Cette catégorie englobait ce que l'on appelle les informations de type numérotation : les numéros de téléphone d'origine et de destination, la date, l'heure et la durée des appels, mais pas le contenu des conversations elles-mêmes.

Panier 3 : Les métadonnées des courriels

Ce panier concernait les lignes "à", "de", "cc", "bcc" et "envoyé" des courriels, mais excluait la ligne "objet" et le corps du message.

Des citoyens américains dans le viseur

L'un des aspects les plus controversés de Stellar Wind résidait dans le fait qu'il ciblait les communications de citoyens américains sur le territoire américain. Avant le 11 septembre, il était généralement admis que l'espionnage domestique était hors limites pour la CIA et la NSA. Ces agences avaient déjà eu des problèmes par le passé pour avoir surveillé des citoyens américains, et les règles avaient été durcies en conséquence.

L'autorisation présidentielle du 4 octobre 2001 permettait l'acquisition d'une communication lorsqu'il existait des « motifs raisonnables de croire » qu'au moins une partie à cette communication était un groupe engagé dans le terrorisme international ou un agent d'un tel groupe. Le programme autorisait également l'acquisition d'informations d'en-tête, de routage et d'adressage, y compris les données de numérotation téléphonique, mais pas le contenu de la communication, lorsque au moins une partie à la communication se trouvait en dehors des États-Unis ou qu'aucune partie n'était connue pour être citoyen américain.

Cette définition floue des cibles a permis une collecte massive de données concernant des millions d'Américains qui n'avaient aucun lien avec le terrorisme.

Un contournement systématique du cadre légal

L'aspect le plus troublant de Stellar Wind était qu'il contournait délibérément le Foreign Intelligence Surveillance Act, la loi qui encadrait normalement la surveillance électronique à des fins de renseignement depuis les années 1970. Le FISA avait établi une cour spéciale chargée de délivrer rapidement des mandats aux agences de renseignement, mais Stellar Wind ignorait complètement ce processus.

John Yoo, alors avocat au sein de l'Office of Legal Counsel du Département de la Justice, a rédigé plusieurs mémorandums juridiques tentant de justifier cette approche. Son argumentation reposait principalement sur deux piliers : les pouvoirs du président en tant que commandant en chef selon l'Article II de la Constitution, et l'Authorization for Use of Military Force votée par le Congrès après les attentats.

Dans son mémorandum du 2 novembre 2001, Yoo affirmait que lire le FISA comme étant « le moyen statutaire exclusif pour mener une surveillance électronique pour le renseignement étranger » constituerait « une atteinte inconstitutionnelle aux autorités du président selon l'Article II ». Il soutenait que le FISA ne fournissait qu'un « refuge sûr » pour la surveillance électronique et ne pouvait restreindre la capacité du président à mener des recherches sans mandat pour protéger la sécurité nationale.

Cette analyse juridique sera plus tard fortement critiquée par les successeurs de Yoo au sein de l'OLC, notamment Jack Goldsmith et Patrick Philbin, qui la jugeront insuffisamment étayée et omettant des éléments cruciaux comme l'exception de 15 jours prévue par le FISA en cas de déclaration de guerre par le Congrès.

La révélation et ses conséquences

Le programme est resté secret jusqu'en décembre 2005, lorsque le New York Times a publié un article révélant que « le président Bush a secrètement autorisé la National Security Agency à espionner les Américains et d'autres personnes à l'intérieur des États-Unis pour rechercher des preuves d'activité terroriste sans les mandats approuvés par les tribunaux normalement requis pour l'espionnage domestique ».

L'article précisait que le Times avait retenu la publication de cette information pendant plus d'un an à la demande de l'administration, qui soutenait que sa divulgation pourrait compromettre des enquêtes en cours et alerter des terroristes potentiels qu'ils pourraient être surveillés. Cette décision de publier n'a été prise qu'après des mois de délibérations internes agonisantes.

La révélation a provoqué une onde de choc politique. Le cas est inhabituel en ce que la pression pour ne pas publier est allée jusqu'au plus haut niveau du gouvernement : le président des États-Unis avait personnellement convoqué l'éditeur et le rédacteur en chef du New York Times au Bureau ovale pour faire un dernier plaidoyer contre la publication.

Une crise constitutionnelle au sein même du Département de la Justice

En 2003 et début 2004, plusieurs hauts responsables du Département de la Justice ont commencé à remettre en question la légalité du programme. Jack Goldsmith, devenu chef de l'OLC, et Patrick Philbin ont découvert que l'analyse juridique de Yoo présentait de graves lacunes. Ils ont notamment constaté que Yoo n'avait jamais abordé la disposition du FISA concernant expressément la surveillance électronique après une déclaration formelle de guerre, et qu'il avait omis toute analyse de la jurisprudence Youngstown Steel Seizure Case, une décision cruciale de la Cour suprême sur la répartition des pouvoirs gouvernementaux entre l'exécutif et le législatif en temps de guerre.

Cette réévaluation juridique a conduit à une confrontation dramatique en mars 2004. Le procureur général John Ashcroft était hospitalisé, et James Comey, procureur général adjoint, exerçait ses fonctions. Lorsque l'administration Bush a tenté d'obtenir la recertification du programme malgré les objections juridiques, Comey et d'autres hauts responsables du Département de la Justice, ainsi que le directeur du FBI Robert Mueller, ont menacé de démissionner.

La crise a culminé avec la célèbre « visite à l'hôpital » du 10 mars 2004, lorsque le conseiller juridique de la Maison Blanche Alberto Gonzales et le chef de cabinet Andrew Card se sont rendus au chevet d'Ashcroft pour tenter d'obtenir sa signature sur une nouvelle autorisation. Ashcroft, bien que gravement malade, a refusé, déclarant qu'il n'était « pas le procureur général » à ce moment-là.

Face à cette révolte sans précédent au sein de son administration, le président Bush a finalement accepté de modifier le programme le 19 mars 2004 pour répondre aux préoccupations juridiques soulevées.

L'exploitation des données et son impact sur les enquêtes du FBI

La NSA transmettait régulièrement au FBI des tuyaux (*tips*) issus de Stellar Wind pour investigation. Ces pistes prenaient la forme d'informations sur des numéros de téléphone ou des adresses électroniques potentiellement liés à des activités terroristes.

Cependant, l'efficacité réelle de ces informations s'est révélée extrêmement décevante. Une enquête menée en 2006 par des responsables du FBI sur les pistes issues des données téléphoniques et de courriels a révélé des résultats troublants. La grande majorité des pistes transmises par la NSA se sont avérées sans valeur, conduisant rarement à des enquêtes significatives sur le terrorisme et n'ayant contribué à aucune arrestation majeure pour terrorisme.

Le FBI recevait des centaines, voire des milliers de pistes qu'il devait investiguer, mobilisant des ressources considérables pour des résultats minimes. Cette situation a créé des tensions entre les agences et soulevé des questions sur le rapport coût-bénéfice d'un tel programme de surveillance massive.

La transition vers une autorité FISA

Après la crise de 2004 et face aux préoccupations juridiques croissantes, l'administration Bush a progressivement cherché à placer les activités de Stellar Wind sous l'autorité du FISA, tout en maintenant certaines capacités de surveillance étendues.

En 2004, le Département de la Justice a commencé à demander des ordonnances de la Cour FISA pour couvrir certaines activités qui avaient été menées dans le cadre de Stellar Wind. La collecte de métadonnées de courriels a été placée sous autorité FISA en utilisant des ordonnances de type *pen register/trap and trace* à partir du milieu de 2004. La collecte de métadonnées téléphoniques a suivi en 2006 en utilisant la Section 215 du Patriot Act.

Cependant, cette transition n'a pas mis fin à la surveillance de masse. Elle a simplement changé son cadre juridique, et des programmes similaires ont continué sous d'autres formes, comme l'a révélé Edward Snowden en 2013 avec l'affaire PRISM.

Un héritage controversé

Le programme Stellar Wind soulève des questions fondamentales sur l'équilibre entre sécurité nationale et libertés civiles dans une démocratie. Plusieurs points méritent une réflexion approfondie :

La rupture du contrat de confiance

L'existence de Stellar Wind a révélé que l'administration américaine avait franchi une ligne rouge en surveillant systématiquement ses propres citoyens sans mandat judiciaire. Cette rupture du lien de confiance entre le gouvernement et le peuple a eu des répercussions durables.

L'efficacité discutable

Les résultats concrets du programme en termes de prévention d'attaques terroristes restent extrêmement limités. L'administration Bush a souvent cité l'affaire d'Iyman Faris, qui avait l'intention de faire tomber le pont de Brooklyn avec des chalumeaux, comme exemple de succès. Cet exemple a été largement considéré comme peu convaincant, y compris par l'éditeur du New York Times, Arthur Sulzberger Jr., qui a trouvé l'idée risible.

Le précédent juridique dangereux

L'analyse juridique élaborée pour justifier Stellar Wind a établi un précédent inquiétant selon lequel le président pourrait contourner les lois votées par le Congrès au nom de la sécurité nationale. Cette théorie des pouvoirs présidentiels quasi illimités en temps de guerre a été fortement contestée.

L'évolution législative

En réponse aux révélations sur Stellar Wind, le Congrès a adopté le FISA Amendments Act de 2008, qui a largement légalisé a posteriori les pratiques mises en place par le programme. Certains critiques ont comparé cette loi à « déclarer un cambriolage légal après que les cambrioleurs ont été attrapés ».

Conclusion

Stellar Wind représente un chapitre sombre de l'histoire de la surveillance aux États-Unis. Né dans le contexte traumatique du 11 septembre, ce programme a illustré comment la peur peut conduire un gouvernement démocratique à outrepasser les limites constitutionnelles qu'il s'était fixées.

Au-delà de ses aspects techniques, Stellar Wind pose une question éthique fondamentale : dans quelle mesure une société démocratique peut-elle sacrifier les libertés individuelles de ses citoyens au nom de leur sécurité collective ? La réponse apportée par l'administration Bush – une surveillance massive et secrète sans contrôle judiciaire – s'est révélée à la fois constitutionnellement contestable et opérationnellement peu efficace.

Le legs de Stellar Wind continue de se faire sentir aujourd'hui. Les programmes de surveillance révélés par Edward Snowden en 2013, comme PRISM et Xkeyscore, s'inscrivent dans la continuité directe des pratiques initiées par Stellar Wind. Ils démontrent que, malgré les controverses et les réformes législatives, l'appétit des agences de renseignement pour la surveillance de masse n'a pas faibli.

Comme l'a déclaré Ben Bradlee, ancien rédacteur en chef du Washington Post : « J'ai fini par réaliser que le mystère, le secret et tout ça ne restent pas importants très longtemps. C'est bien d'avoir un scoop, mais quelques semaines plus tard, ça n'a plus vraiment d'importance. Et trop souvent, c'était juste des réputations qu'ils essayaient de protéger, pas empêcher que des gens se fassent tuer. »

Cette observation résonne particulièrement dans le cas de Stellar Wind : un programme secret massif qui a violé les droits de millions d'Américains, largement inefficace dans ses objectifs déclarés, et dont la révélation n'a finalement pas compromis la sécurité nationale comme l'administration l'avait prédit.

Références

[1] James Bamford. The NSA Is Building the Country's Biggest Spy Center (Watch What You Say). In : *Wired Magazine* (15 mars 2012).

[2] Glenn Greenwald. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books, 2014.

[3] H. D. S. Greenway et Leora Falk. Anatomy of a Secret. Discussion Paper Series D-73. Avec l'assistance de Leora Falk. Joan Shorenstein Center on the Press, Politics et Public Policy, juin 2012.

[4] Eric Lichtblau. Bush's Law: The Remaking of American Justice. Pantheon Books, 2008.

[5] James Risen et Eric Lichtblau. Bush Lets U.S. Spy on Callers Without Courts. In : *The New York Times* (16 déc. 2005).

[6] Charlie Savage. Takeover: The Return of the Imperial Presidency and the Subversion of American Democracy. Little, Brown et Company, 2007.

[7] Olivier Tesquet. PRISM : le programme de surveillance électronique de trop ? In : *Télérama* (10 juin 2013).

[8] U.S. Department of Justice, Office of the Inspector General. A Review of the Department of Justice's Involvement with the President's Surveillance Program (U). Report 2009-0013-A. 10 juill. 2009.

[9] John Yoo. War by Other Means: An Insider's Account of the War on Terror. Atlantic Monthly Press, 2006.