

Stateroom : le réseau d'espionnage caché dans les ambassades

Stéphane FOSSE

fosse.fr

20 février 2026

Copyright : cette œuvre est libre, vous pouvez la copier, la diffuser et la modifier
selon les termes de la [Licence Art Libre](#)

Résumé

Stateroom est le nom de code d'un programme de collecte de renseignements électromagnétiques (SIGINT) opérant depuis les ambassades et consulats des cinq pays membres de l'alliance Five Eyes : États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande. Révélé en octobre 2013 par l'ancien contractant de la NSA Edward Snowden, ce programme interceptait les communications radio, téléphoniques et Internet à proximité immédiate des centres de décision politiques, économiques et diplomatiques des pays hôtes. Derrière les façades anodines de missions diplomatiques officielles se cachaient des postes d'écoute SIGINT dissimulés dans de fausses structures architecturales — appareils de climatisation factices, pans de murs opaques à la lumière mais transparents aux ondes radio.

1 Le Special Collection Service : une fusion née de la guerre froide

Pour comprendre Stateroom, il faut remonter à 1978. Cette année-là, Bobby Inman, directeur de la NSA, et Barry Kelly, chef de l'Office of SIGINT Operations de la CIA, signent un accord qui donne naissance au Special Collection Service (SCS)[4]. L'idée est simple : mettre fin à la rivalité stérile entre les deux agences qui, depuis des années, se marchent dessus dans les ambassades du monde entier. La CIA sait comment entrer dans un bâtiment ; la NSA sait ce qu'elle cherche une fois à l'intérieur. Le SCS est le mariage de ces deux compétences.

Le SCS hérite d'une longue tradition d'opérations clandestines depuis les ambassades. La CIA menait déjà des écoutes depuis ses missions diplomatiques dans les années 1950 sous le nom de Division D, puis de Staff D. Dès les années 1960, la station de Moscou interceptait les conversations des membres du Politburo sur leurs radiotéléphones de limousine — une opération baptisée « Gamma Guppy » qui prit fin quand les Soviétiques chiffrèrent leurs communications après qu'un article dans la presse eut révélé l'opération. L'histoire du renseignement est ainsi faite : chaque révélation génère une contre-mesure, qui génère une nouvelle technique.

La structure du SCS, dont le siège est à Beltsville dans le Maryland, reflète ce compromis institutionnel : sa direction alterne entre un officier de la CIA et un officier de la NSA. Quatre unités internes structurent ses opérations — le Bureau des opérations de terrain, le Bureau du génie de terrain, le Bureau du soutien aux missions et le Bureau d'installation et de logistique. Les agents déployés utilisent des couvertures de fonctionnaires du département d'État ou de spécialistes des télécommunications diplomatiques[6], ce qui leur confère une immunité diplomatique et l'accès aux zones sécurisées des ambassades.

Un ancien employé de l'agence canadienne Communications Security Establishment, Mike Frost, a décrit dans ses mémoires l'atmosphère du quartier général SCS en 1994 : des fils partout, des gadgets bricolés dans tous les coins, des ordinateurs sur chaque surface, des gens en costume trois pièces côtoyant des ingénieurs en jeans. Une sorte de laboratoire de mad scientists appliqué à l'espionnage.

2 UKUSA, Five Eyes : le cadre juridique fantôme

Stateroom n'est pas une initiative américaine isolée. Il s'inscrit dans l'accord UKUSA, un traité de partage du renseignement électromagnétique signé le 5 mars 1946 entre le Royaume-Uni et les États-Unis, étendu ensuite au Canada (1948), à l'Australie et à la Nouvelle-Zélande (1956)[9]. Ce traité — dont le contenu complet n'a été rendu public qu'en juin 2010 — constitue la charpente juridique de ce qu'on appelle communément les Five Eyes, ou FVEY.

L'accord UKUSA crée un espace de partage SIGINT tellement intégré que, selon d'anciens responsables du renseignement, « le produit national est souvent indiscernable » de celui d'un partenaire. Les cinq agences partenaires — la NSA américaine, le GCHQ britannique, le CSE canadien, l'ASD australienne et le GCSB néo-zélandais — opèrent des installations parfois co-localisées, parfois co-staffées. Leurs classifications comportent

systématiquement la mention « REL TO USA, AUS, CAN, GBR, NZL », ce qui signifie que chaque document est accessible aux cinq partenaires par défaut.

Stateroom est l'expression diplomatique de cette intégration. Chaque pays membre déploie ses propres équipes dans ses propres missions diplomatiques, collecte du SIGINT sur place, puis partage les résultats avec les quatre autres partenaires[11]. Les données collectées par les installations britanniques transitent par la base de RAF Croughton dans le Northamptonshire avant d'être transmises vers un centre de données co-opéré par la CIA et la NSA à College Park, dans le Maryland.

Ce cadre a un avantage opérationnel non négligeable. La Convention de Vienne sur les relations diplomatiques de 1961 interdit aux autorités du pays hôte de fouiller les locaux diplomatiques, d'y pénétrer sans autorisation ou d'inspecter leur équipement. Une ambassade est, juridiquement, le territoire de l'État accréditaire. C'est cette inviolabilité que Stateroom exploite : personne ne peut légalement vérifier ce qui se passe derrière les panneaux du toit de l'ambassade américaine de Berlin ou de celle de Paris.

3 La technique : des panneaux diélectriques et des greniers sans fenêtres

Comment cache-t-on une station d'interception SIGINT dans un bâtiment diplomatique au cœur d'une capitale ? La réponse tient dans un matériau particulier : les panneaux diélectriques. Un diélectrique est, par définition, un isolant électrique qui laisse passer les champs électromagnétiques. Contrairement au béton armé ou à l'aluminium qui atténuent ou bloquent les signaux radio, les panneaux en plastique ou en fibres de verre les laissent traverser sans perte significative.

Le journaliste d'investigation britannique Duncan Campbell, mandaté par Der Spiegel pour analyser techniquement l'ambassade américaine de Berlin après les révélations Snowden, a identifié la signature visible de ces installations[1]. Sur le toit de l'ambassade berlinoise, située sur la Pariserplatz à quelques dizaines de mètres du Reichstag, plusieurs zones présentent des panneaux de couleur légèrement différente des maçonneries environnantes, positionnés aux angles sud-ouest, nord-ouest et nord-est de la structure. Ces « fenêtres radio » sont imperméables à la lumière mais transparentes aux ondes électromagnétiques. Derrière elles se trouvent les antennes et équipements d'interception, protégés des regards sans être protégés des signaux qu'ils cherchent à capter.

Le document SCS classifié décrit Stateroom comme déployant des « équipements de surveillance dissimulés à l'intérieur de caractéristiques architecturales factices » et dans des « hangars d'entretien de toits »[2]. L'objectif est de capter l'ensemble du spectre des communications civiles et gouvernementales à courte portée : téléphonie mobile GSM, GPRS, 3G et CDMA, liaisons radio des services gouvernementaux et de police, et potentiellement tout trafic Wi-Fi ou point-to-point en clair. La note NSA issue du programme SIDtoday publiée par The Intercept décrit des équipements couvrant la plage de fréquences allant de 20 MHz à 1 GHz, ce qui englobe la quasi-totalité des communications terrestres civiles et gouvernementales de l'époque[8].

Les locaux des opérateurs SCS occupent quant à eux des étages sans fenêtres — les Sensitive Compartmented Information Facilities (SCIF) — qui empêchent les signaux parasites de l'équipement lui-même de fuir vers l'extérieur et de trahir la présence des installations. L'analyse du cas italien par Greenwald et Maurizi révèle que les sites SCS de Rome et de Milan figuraient comme actifs dans un document de 2010, et qu'un examen du toit de l'ambassade américaine via Veneto permettait d'identifier sans ambiguïté la présence d'une structure SIGINT[7].

4 Octobre 2013 : les révélations et leurs effets diplomatiques

L'existence de Stateroom est révélée en octobre 2013 dans la vague des publications issues des documents Snowden[3]. Der Spiegel publie le premier article identifiant l'ambassade américaine à Berlin comme un centre d'espionnage SCS[10]. La même semaine, le Süddeutsche Zeitung et le Guardian révèlent que la chancelière Angela Merkel a été mise sur écoute depuis 2002 à partir de cette même ambassade — son numéro de téléphone figurant dans la base cible du SCS sous l'intitulé « GE Chancellor Merkel ». L'opération a duré plus de dix ans.

Le 23 novembre 2013, le quotidien néerlandais NRC Handelsblad publie une présentation NSA classifiée Top Secret révélant la liste des villes où des sites SCS sont opérationnels dans les missions diplomatiques américaines[5]. Le document, issu d'une présentation de management de 2012 intitulée « Driver 1 : Worldwide SIGINT/Defense Cryptologic Platform », liste 88 emplacements au total, dont 46 sont volontairement caviardés à la demande de Snowden lui-même. Les villes confirmées incluent Athènes, Bangkok, Berlin, Brasilia, Budapest, Francfort, Genève, Lagos, Milan, New Delhi, Paris, Prague, Vienne et Zagreb pour les seuls sites SCS américains.

Les partenaires Five Eyes déploient leurs propres installations selon le même principe. L'Australie opère des postes d'écoute depuis ses ambassades à Bangkok, Pékin, Dili, Hanoï, Jakarta, Kuala Lumpur et Port Moresby. En mars 2015, il est révélé que la Nouvelle-Zélande maintient un site d'interception codé « Caprica » au

Haut-Commissariat néo-zélandais à Honiara, capitale des Îles Salomon — explicitement modélisé sur les postes Stateroom américains. Le GCHQ britannique fait de même dans ses propres ambassades, dont les données remontent vers la base de RAF Croughton.

Les réactions diplomatiques sont vives, mais courtes. Angela Merkel appelle Barack Obama pour exiger des explications et qualifie l’espionnage entre alliés d’inacceptable. Le ministre des Affaires étrangères allemand Guido Westerwelle convoque l’ambassadeur américain, puis convoque également l’ambassadeur britannique. L’Indonésie proteste officiellement. L’Italie se retrouve dans la situation embarrassante d’avoir son Premier ministre, Enrico Letta, qui avait déclaré quelques semaines plus tôt qu’il n’avait « aucune indication que la sécurité des communications du gouvernement et des ambassades italiens ait été compromise » — avant que les documents Snowden ne révèlent deux opérations distinctes contre l’ambassade italienne à Washington : « Bruneau » et « Hemlock »[7].

5 Ce que Stateroom révèle d’une architecture de surveillance

Vu depuis la perspective d’un architecte de systèmes, Stateroom est remarquablement bien conçu. Le programme résout un problème de collecte SIGINT que l’interception passive à distance ne peut pas résoudre : la proximité. Les communications entre dirigeants politiques, entre ambassades étrangères, entre état-major et ministères, entre services d’un même gouvernement, sont souvent à très courte portée, parfois sur des réseaux locaux ou des liaisons point-à-point qu’aucun satellite ou station d’interception distante ne peut capter efficacement.

Stateroom résout ce problème de la seule façon possible : en plaçant le récepteur le plus près physiquement de la source. Une ambassade américaine à 350 mètres de l’Élysée ou à quelques dizaines de mètres du Bundestag est le point de collecte optimal. Ni un satellite, ni une station côtière, ni un câble sous-marin ne peuvent faire ce que fait un récepteur de 20 MHz à 1 GHz installé dans un grenier sans fenêtres avec vue sur le quartier gouvernemental.

Le programme illustre aussi une tension structurelle propre aux architectures de surveillance : la tension entre légitimité et efficacité. Stateroom n’est pas un programme de surveillance de masse au sens de PRISM ou de Tempora. C’est, fondamentalement, un programme de ciblage précis — des cibles spécifiques, des emplacements précis, des fréquences identifiées. Mais son déploiement à grande échelle dans près de 100 missions diplomatiques américaines, combiné aux réseaux parallèles australien, britannique, canadien et néo-zélandais, en fait un réseau mondial de collecte dont la couverture agrégée touche la quasi-totalité des capitales significatives du monde.

La Convention de Vienne de 1961, sur laquelle repose toute la diplomatie moderne, n’a pas été conçue pour ce scénario. Elle protège les locaux diplomatiques de toute intrusion extérieure, ce qui — par un paradoxe juridique intéressant — protège aussi les équipements d’écoute installés à l’intérieur. L’immunité diplomatique, outil de la réciprocité internationale et du dialogue entre États, est devenue l’armure légale d’une infrastructure de surveillance à l’échelle planétaire.

Nicky Hager, journaliste néo-zélandais qui avait révélé en 1999 l’existence du réseau ECHELON, a confirmé en 2013 que de telles opérations existent depuis « un bon moment ». C’est là que réside le point le plus instructif de l’affaire Stateroom : pas la révélation de l’existence d’un programme secret, mais la confirmation que ces pratiques sont si ancrées dans les routines du renseignement allié qu’elles constituent depuis des décennies une infrastructure invisible, parfaitement intégrée dans le paysage urbain des capitales mondiales — et que personne, jusqu’à Snowden, n’avait eu les moyens de le documenter publiquement.

Références

- [1] Duncan CAMPBELL. [How embassy eavesdropping works](#). Consulté en 2026.
- [2] Duncan CAMPBELL. [Special Collection Service slides](#). Consulté en 2026.
- [3] CONTRIBUTEURS WIKIPÉDIA. [Révélations d’Edward Snowden](#). Consulté en 2026. 2026.
- [4] CONTRIBUTEURS WIKIPÉDIA. [Special Collection Service](#). Consulté en 2026. 2026.
- [5] ELECTROSPACES.NET. [NSA’s global interception network](#). Déc. 2013.
- [6] George ENGLEHART. [Special Collection Service: America’s Mission Impossible Force](#). Juill. 2025.
- [7] Glenn GREENWALD et Stefania MAURIZI. [Revealed: How the NSA Targets Italy](#). In : *L’Espresso* (déc. 2013).
- [8] NSA. [SCS and Executive Protection](#). Document NSA classifié Top Secret du 18 août 2004, publié par The Intercept le 5 février 2018. Août 2004.
- [9] Carly NYST et Anna CROWE. [Unmasking the Five Eyes’ global surveillance practices](#). Rapp. tech. Privacy International / Global Information Society Watch, 2014.

- [10] Laura POITRAS, Marcel ROSENBACH et Holger STARK. [Embassy Espionage: NSA's Secret Spy Hub in Berlin](#). In : *Der Spiegel* (oct. 2013).
- [11] WIKIPEDIA CONTRIBUTORS. [Stateroom \(surveillance program\)](#). Consulté en 2026. 2026.