MYSTIC
La NSA enregistre tous les appels d'un pays pendant 30 jours

Stéphane FOSSE
fosse.fr

8 février 2026

MYSTIC est un programme de surveillance déployé par la National Security Agency (NSA) américaine depuis 2009 qui permet l'enregistrement intégral des communications téléphoniques de pays entiers. Le sous-programme SOMALGET stocke chaque appel pendant 30 jours, offrant aux analystes une capacité d'écoute rétroactive inédite. Les Bahamas, l'Afghanistan, le Mexique, le Kenya et les Philippines ont été ciblés.

L'existence de MYSTIC a été révélée en mars 2014 par le Washington Post à partir de documents transmis par Edward Snowden. Deux mois plus tard, The Intercept identifiait les pays surveillés et détaillait les mécanismes techniques. Ce qui frappe dans ce programme, au-delà de son ampleur, c'est sa banalisation de la surveillance totale. Pas de soupçon préalable, pas de ciblage individuel. Juste l'aspiration systématique de 100 millions d'événements d'appel par jour.

Genèse d'un système industriel d'écoute

MYSTIC naît en 2009 au sein de la division Special Source Operations de la NSA, l'entité chargée de nouer des partenariats avec les opérateurs télécoms et les équipementiers. Le contexte est celui de l'après 11 septembre, période où l'intelligence américaine dispose de budgets considérables et d'une latitude juridique étendue sous l'Executive Order 12333, directive présidentielle signée par Ronald Reagan en 1981.

Les documents Snowden décrivent MYSTIC comme un « programme pour systèmes de collecte intégrés installés ouvertement sur les réseaux cibles, principalement pour la collecte et le traitement des réseaux de communications sans fil et mobiles ». La formulation est euphémisante. Dans la pratique, la NSA exploite l'infrastructure d'interception légale que de nombreux pays ont déployée pour leurs propres besoins judiciaires.

Ces systèmes d'interception légale, installés par des contractants privés sur les réseaux télécoms, permettent normalement aux autorités locales de placer des cibles sous écoute après autorisation judiciaire. La NSA détourne cette infrastructure. Elle transforme un outil de police ciblée en dispositif de surveillance généralisée. Un mémo de 2012 l'indique sans ambiguïté : « Les pays hôtes ne sont pas conscients de la collecte SIGINT de la NSA. »

SOMALGET : la machine à remonter le temps

Si MYSTIC collecte les métadonnées téléphoniques, c'est son composant SOMALGET qui franchit le seuil suivant. SOMALGET enregistre le contenu audio de chaque conversation. Pas un échantillon, pas une sélection. Tout. Un manager du programme le compare à « une machine à remonter le temps » permettant de rejouer n'importe quel appel des 30 derniers jours.

La métaphore du magnétoscope numérique revient dans les documents internes. Si l'ensemble des communications d'un pays était un menu de programmes télévisés, MYSTIC serait le guide des chaînes indiquant quoi, quand, où. SOMALGET serait le DVR qui enregistre automatiquement chaque émission sur chaque chaîne et les conserve un mois. Les analystes peuvent ensuite naviguer dans cette archive, écouter ce qui les intéresse, remonter dans le passé pour identifier ce qu'une cible disait avant même d'être identifiée comme cible.

Cette capacité de « récupération rétrospective » (*retrospective retrieval*) via l'outil RETRO modifie radicalement la logique de surveillance. Traditionnellement, on cible d'abord, on écoute ensuite. Avec SOMALGET, on enregistre d'abord, on cible plus tard. Un analyste peut formuler une hypothèse mercredi et vérifier ce qui se disait lundi. La base de données NUCLEON stocke ces milliards de conversations en attente d'exploitation.

Cinq pays dans le viseur, 250 millions de personnes concernées

Les documents Snowden révèlent que dès 2013, MYSTIC opérait dans cinq pays avec des niveaux de surveillance variables. Les Bahamas et l'Afghanistan subissent la collecte intégrale SOMALGET. Le Mexique, le Kenya et les Philippines font l'objet d'une collecte de métadonnées uniquement. Au total, plus de 250 millions de personnes voient leurs communications aspirées.

Le cas des Bahamas illustre le cynisme du programme. Cette nation des Caraïbes de 400 000 habitants ne menace nullement la sécurité américaine. Le Département d'État lui-même la qualifie de « démocratie stable partageant les principes démocratiques, les libertés personnelles et l'État de droit avec les États-Unis ». Pourtant, SOMALGET y est déployé. Les documents internes l'admettent : les Bahamas servent de « banc d'essai pour les déploiements système, capacités et améliorations ». Un cobaye pratique. Population réduite, flux gérable, conditions idéales pour tester de nouvelles fonctionnalités avant déploiement ailleurs.

L'Afghanistan s'inscrit dans une logique différente. WikiLeaks révèle en mai 2014 qu'il s'agit du deuxième pays sous surveillance totale, celui que The Intercept avait choisi de ne pas nommer « en réponse à des préoccupations spécifiques et crédibles que cela pourrait conduire à une violence accrue ». James Clapper, directeur du renseignement national, confirmera plus tard que la divulgation du nom avait conduit le gouvernement afghan à fermer immédiatement un programme de renseignement qu'il qualifie de « source unique la plus importante de protection des forces et d'alerte pour nos gens en Afghanistan ».

Pour le Mexique, les Philippines et le Kenya, la collecte se limite officiellement aux métadonnées. Ces données révèlent qui appelle qui, quand, d'où, pour combien de temps (un peu ce que fait WhatsApp finalement). Elles permettent de cartographier les réseaux sociaux, identifier les déplacements, déduire les relations. L'opération philippine s'appuie sur un « actif DSD dans un site de fournisseur philippin » – le DSD étant le service de renseignement électromagnétique australien. Au Kenya et au Mexique, c'est la CIA qui « sponsorise » les opérations selon la terminologie des documents.

L'exploitation du système DEA

Comment la NSA accède-t-elle techniquement aux réseaux télécoms de pays souverains ? Les documents suggèrent que l'agence détourne l'infrastructure mise en place par la Drug Enforcement Administration (DEA) pour ses opérations antidrogue. Un mémo indique que les données SOMALGET sont acquises sous couvert d'« interceptions légales » effectuées via des « accès DEA ».

Le mécanisme est ingénieux. Quand les agents antidrogue américains veulent placer sur écoute le téléphone d'un trafiquant présumé dans un pays étranger, ils contactent leurs homologues locaux qui déploient l'interception via les équipements d'interception légale installés sur le réseau télécom. Ces équipements sont fournis et maintenus par des contractants privés. La NSA utilise apparemment l'accès créé par ces contractants pour aspirer discrètement l'ensemble du trafic téléphonique du pays.

Finn Selander, ancien agent spécial de la DEA, l'exprime crûment : « La DEA est en fait l'une des plus grandes opérations d'espionnage qui existent. Notre mandat n'est pas seulement la drogue. Nous collectons du renseignement. » Les pays accueillent la DEA parce qu'ils ne la perçoivent pas vraiment comme une organisation d'espionnage. Erreur. Un mémo NSA de 2004 titre « DEA : l'autre combattant » et vante « la relation d'échange d'information bilatérale vibrante » entre les deux agences.

Aux Bahamas, la NSA intercepte les données GSM transmises via l'« interface A », composant central des réseaux mobiles qui transfère les communications entre les antennes relais et le cœur du réseau. Toucher cette portion du réseau mobile d'un pays donne accès à un flux pratiquement ininterrompu de communications. Cela requiert aussi une puissance technique considérable. Un ancien ingénieur télécom consulté par The Intercept observe : « Je ne pense vraiment pas que ce serait votre équipement d'interception légale ordinaire. » L'équipement standard plafonne à 1000 interceptions simultanées. La NSA enregistre des dizaines de millions d'appels.

General Dynamics et l'industrialisation

Le géant de la défense General Dynamics détient un contrat de 51 millions de dollars sur huit ans pour traiter « toutes les données MYSTIC et les données d'autres accès NSA » dans une installation à Annapolis Junction, Maryland, à quelques kilomètres du siège de la NSA. Les logs d'activité SOMALGET font référence à un technicien travaillant dans une « installation de traitement SOMALGET » dont le nom correspond à celui d'un utilisateur LinkedIn indiquant General Dynamics comme employeur.

Cette sous-traitance illustre l'industrialisation de la surveillance de masse. On est loin de l'agent isolé écoutant une conversation suspecte au casque. MYSTIC traite plus de 100 millions d'événements d'appel par jour. Cela demande des datacenters, des *pipelines* de données, des systèmes de stockage massifs, des équipes d'ingénieurs pour maintenir l'infrastructure. Un memo de 2012 rapporte qu'en première année d'opération, le programme

« avait depuis longtemps atteint le point où il collectait et envoyait bien plus que la bande passante ne pouvait traiter ». Réponse de la NSA : expansion du stockage cloud et création d'un « nouveau dépôt de données de mission gigantesque ».

Une justification douteuse

Officiellement, SOMALGET aux Bahamas vise à localiser « les trafiquants internationaux de narcotiques et les passeurs d'étrangers présentant un intérêt particulier ». Une présentation interne NSA de 2013 se félicite d'avoir utilisé SOMALGET pour localiser un individu qui « organisait des expéditions de marijuana du Mexique vers les États-Unis » via le service postal américain.

L'écart entre la puissance déployée et les résultats affichés interroge. On bâtit une infrastructure capable d'enregistrer chaque conversation d'un pays pour coincer un dealer qui poste de l'herbe ? Les documents ne reflètent aucune attention particulière aux blanchisseurs d'argent et institutions financières puissantes – dont de nombreuses banques occidentales – qui alimentent le marché noir de la drogue aux Bahamas. Près de 5 millions d'Américains visitent les Bahamas chaque année. Leurs conversations sont aspirées au passage.

Michael German, ancien agent FBI devenu chercheur au Brennan Center for Justice, pointe la myopie stratégique : « C'est surprenant, la courte vue du gouvernement. Qu'ils n'aient pas pu voir comment exploiter un mécanisme légal à un tel degré que vous pourriez perdre cet accès justifiable – c'est là que la communauté du renseignement agit d'une manière qui nuit à ses intérêts à long terme, et clairement aux intérêts de sécurité nationale à long terme des États-Unis. »

Executive Order 12333 : une autorité sans limites ?

MYSTIC opère sous l'autorité de l'Executive Order 12333, directive présidentielle émise par Ronald Reagan en décembre 1981. Cet ordre exécutif établit un cadre général pour les activités de renseignement américaines et définit les rôles de chaque agence. Il autorise la collecte d'« informations de renseignement étranger », notion définie de manière extrêmement large comme toute information « concernant les capacités, intentions et activités de puissances étrangères, organisations ou personnes ».

Le cadre juridique de l'EO 12333 contraste avec celui du Foreign Intelligence Surveillance Act (FISA) qui régit la surveillance sur le territoire américain. FISA impose une supervision judiciaire via la Foreign Intelligence Surveillance Court. L'EO 12333, opérant hors du territoire américain, échappe à tout contrôle judiciaire. Aucun juge ne valide les programmes. Aucune cour ne révise les pratiques. La supervision congressionnelle reste limitée.

Cette absence d'oversight judiciaire pose problème même pour des opérations ciblant des étrangers à l'étranger, car les communications des Américains sont inévitablement collectées. Un Américain en vacances aux Bahamas voit ses appels enregistrés. Un Américain qui téléphone à un correspondant au Kenya voit sa conversation aspirée. Un rapport du Brennan Center for Justice estime que « les communications et données de millions, ou de centaines de millions, d'Américains » sont collectées sous l'autorité de l'EO 12333.

Mark Jaycox, dans son étude académique de 88 pages pour le Harvard National Security Journal, décrit l'EO 12333 comme « une directive des années 1980 qui établit un cadre politique global pour les pouvoirs d'espionnage de la branche exécutive » caractérisé par des « standards de ciblage permissifs » permettant « la collecte substantielle de communications d'Américains contenant peu ou pas de valeur de renseignement étranger ».

Statut actuel : opérationnel mais opaque

Les révélations Snowden concernent des documents datant de 2013. Qu'en est-il aujourd'hui ? Aucune source ouverte ne confirme formellement l'arrêt de MYSTIC. La NSA n'a jamais commenté publiquement l'existence du programme. Les documents budgétaires classifiés de 2013 évoquaient déjà des plans d'expansion vers d'autres pays. Un officiel NSA écrivait qu'il y a « peu de raisons » pour que SOMALGET ne puisse être étendu à davantage de pays pourvu que l'agence fournisse « une ingénierie, coordination et *hardware* adéquats ».

Le contexte technique a évolué. Les réseaux 3G et 4G mentionnés dans les documents de 2013 comme nécessitant des ajustements sont aujourd'hui matures. La 5G introduit de nouvelles architectures que la NSA a probablement dû adapter. Les capacités de stockage ont continué d'augmenter. La fenêtre de 30 jours pourrait techniquement être étendue, bien qu'aucun document ne le confirme.

Sur le plan juridique, la directive présidentielle PPD-28 émise par Barack Obama en janvier 2014 en réponse aux révélations Snowden impose officiellement de « nouvelles limites » à la collecte en masse de renseignement électromagnétique. Dans la pratique, ces limitations restent permissives. La directive liste cinq conditions générales autorisant la collecte en masse : menaces de puissances étrangères, terrorisme, armes de destruction massive,

cybersécurité, et « menaces criminelles transnationales incluant la finance illicite et l'évasion de sanctions ». MYSTIC entre confortablement dans ces catégories.

L'absence de protection des données personnelles

Aucune donnée volée n'a été revendue sur le dark web. Pas de fuite massive vers des cybercriminels. MYSTIC n'est pas un ransomware, c'est un appareil d'État. Les données restent dans les systèmes NSA. Mais cette distinction apporte peu de réconfort.

Les enregistrements SOMALGET contiennent des conversations privées entre membres de familles, échanges professionnels confidentiels, consultations médicales par téléphone, entretiens thérapeutiques. Des secrets d'affaires sont révélés. Des sources journalistiques sont exposées. Des avocats discutent de stratégies avec leurs clients. Tout est enregistré, indexé, accessible aux analystes autorisés.

Les procédures de minimisation censées protéger les communications des « personnes américaines » s'appliquent après collecte. Une fois les conversations enregistrées, des analystes décident quoi conserver, quoi diffuser, quoi partager avec d'autres agences. Ces décisions sont internes, sans supervision externe. Le système repose sur l'auto-régulation de l'agence même qui a intérêt à maximiser l'exploitation des données.

Parallèles avec la construction parallèle

Un document Snowden mentionne que la Special Operations Division de la DEA a utilisé des informations classifiées obtenues par la NSA pour lancer des enquêtes criminelles, puis créé de faux narratifs pour dissimuler l'origine de l'information devant les tribunaux. Cette pratique, révélée par Reuters en 2013 et appelée « construction parallèle » (parallel construction), pose un problème constitutionnel majeur.

Si une enquête commence par une information MYSTIC mais que cette origine est cachée au juge et à la défense, comment l'accusé peut-il contester la légalité de la collecte initiale ? La « construction parallèle » transforme une surveillance potentiellement illégale en preuve apparemment légale. C'est une corruption du processus judiciaire, un contournement des protections constitutionnelles par le mensonge procédural.

Réactions et débats

L'American Civil Liberties Union (ACLU) critique fermement le programme. Son technologue principal, Christopher Soghoian, déclare à The Intercept : « Les systèmes d'interception légale créent des vulnérabilités dans les réseaux, forçant les opérateurs à les affaiblir. Les gouvernements hôtes devraient vraiment réfléchir à deux fois avant d'accepter l'un de ces chevaux de Troie. »

Kurt Opsahl, avocat à l'Electronic Frontier Foundation, rappelle que « un citoyen américain a des droits constitutionnels du Quatrième Amendement où qu'il soit ». Les révélations montrent pourtant que « des programmes vastes et généralisés que la NSA et d'autres agences gouvernementales mènent à l'étranger aspirent les communications des Américains ».

Le gouvernement des Bahamas, informé de l'espionnage, n'a émis aucun commentaire officiel. Le bureau du commissaire à la protection des données bahamen déclare « n'avoir pas été au courant de la question que vous soulevez ». Le silence officiel cache probablement l'embarras d'un pays qui découvre que son allié espionnait sa population entière.

Un précédent dangereux

MYSTIC établit un précédent. Si les États-Unis peuvent enregistrer l'intégralité des communications d'un pays allié sans son consentement, qu'est-ce qui empêche d'autres puissances de faire de même ? La Chine, la Russie, Israël disposent de capacités techniques comparables. Le marché des équipements d'interception légale est mondial. Les mêmes vulnérabilités existent partout.

La sécurité collective des communications repose sur une confiance minimale. Les nations acceptent d'installer des équipements d'interception pour leur propre sécurité judiciaire en supposant que ces outils ne seront pas détournés. MYSTIC trahit cette confiance. Chaque pays qui découvre l'ampleur de la surveillance américaine révise ses hypothèses. Certains se tournent vers des équipementiers chinois comme Huawei, créant de nouvelles dépendances et de nouveaux risques.

Michael German conclut : « C'est presque comme s'ils avaient cette mentalité – si on peut, on le fera. Il n'y a pas d'analyse des risques à long terme, pas d'analyse de si ça vaut vraiment l'effort, pas d'analyse de si on ne pourrait pas prendre ces ressources et les mettre sur de vraies menaces pour faire plus de bien. »

MYSTIC révèle une logique bureaucratique de la surveillance : l'expansion technologique précède la réflexion politique. Les capacités créent leurs propres justifications. L'infrastructure une fois construite demande à être utilisée. Et une fois les limites repoussées, difficile de revenir en arrière.

Références

[1] Julian Assange. WikiLeaks statement on the mass recording of Afghan telephone calls by the NSA. WikiLeaks, mai 2014.

[2] David Burnham. The Silent Power of The N.S.A. In : *The New York Times Magazine* (27 mars 1983).

[3] Ryan Devereaux, Glenn Greenwald et Laura Poitras. The NSA Is Recording Every Cell Phone Call in the Bahamas. The Intercept, 19 mai 2014.

[4] Executive Order 12333: United States Intelligence Activities. Executive Order. Federal Register, 4 déc. 1981.

[5] Barton Gellman et Ashkan Soltani. NSA surveillance program reaches 'into the past' to retrieve, replay phone calls. The Washington Post, 18 mars 2014.

[6] Mark M. Jaycox. No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333. In : *Harvard National Security Journal* 12 (2021).

[7] Presidential Policy Directive 28: Signals Intelligence Activities. Presidential Policy Directive. The White House, 17 jan. 2014.

[8] Privacy and Civil Liberties Oversight Board. Report on Executive Order 12333. PCLOB, 2021.

[9] Bruce Schneier. MYSTIC: The NSA's Telephone Call Collection Program. Mars 2014.

[10] Christopher Soghoian. Interviews published in The Intercept and The Washington Post. Diverses interviews publiées. ACLU, 2014.

[11] Amos Toh, Faiza Patel et Elizabeth Goitein. Overseas Surveillance in an Interconnected World. Brennan Center for Justice, mars 2016.