Le réseau ECHELON

Stéphane FOSSE
fosse.fr

23 juillet 2025

Résumé

Dans les méandres des relations internationales contemporaines se cache un système d'une puissance sans précédent. Le réseau Echelon, fruit d'une alliance secrète entre pays anglo-saxons, demeure l'un des dispositifs de surveillance les plus élaborés jamais créés. Ce document analyse son fonctionnement, son histoire et ses implications géopolitiques, tout en questionnant les dérives potentielles pour nos libertés individuelles.

Table des matières

1 Aux origines d'une alliance

Peu de systèmes d'espionnage ont suscité autant de controverses qu'Echelon. Ce vaste dispositif d'interception des communications électroniques tire ses racines dans la période trouble de l'après-guerre mondiale. Le 17 mai 1943, alors que le conflit faisait rage, les États-Unis et le Royaume-Uni signèrent discrètement un accord secret pour partager leurs renseignements issus de l'interception des communications. Cette coopération, fructueuse pendant la guerre, fut pérennisée par la signature du traité UKUSA (United Kingdom - United States Communications Intelligence Agreement) le 5 mars 1946.

Cette alliance s'élargit progressivement pour inclure trois autres pays anglo-saxons : le Canada en 1948, puis l'Australie et la Nouvelle-Zélande en 1956. Ces cinq nations, connues aujourd'hui sous l'appellation « Five Eyes » (les cinq yeux), formèrent ainsi le socle d'une collaboration sans précédent dans le domaine du renseignement électronique.

La Guerre froide offrit un contexte idéal pour développer ce réseau. Face à l'Union soviétique et au bloc de l'Est, les pays occidentaux investirent massivement dans des capacités d'interception des communications. L'objectif était alors principalement militaire et stratégique pour permettre d'anticiper les mouvements de l'adversaire, décoder ses messages et surveiller ses activités. C'est au milieu des années 1970 qu'est né ce qui allait devenir le réseau Echelon.

Initialement codé P415 par les entreprises ayant participé à son développement, ce système s'inscrivait dans un programme plus vaste de la NSA baptisé FROSTING, qui comportait deux sous-programmes : TRANSIENT, dédié à l'interception des communications des satellites soviétiques, et ECHELON, consacré à la surveillance des transmissions satellitaires mondiales. Son lancement officiel, quoique secret, date de 1971.

2 L'architecture d'un système global

Echelon s'appuie sur un réseau tentaculaire d'installations réparties stratégiquement à travers le globe. Ce maillage serré permet une couverture quasi totale des communications mondiales, qu'elles transitent par voie satellitaire, hertzienne ou sous-marine.

Au cœur de ce dispositif se trouvent les stations d'écoute terrestres, dont la plus emblématique reste sans doute celle de Menwith Hill, située dans le Yorkshire, au Royaume-Uni. Cette base, facilement reconnaissable à ses nombreux radômes – ces structures sphériques blanches ressemblant à d'énormes balles de golf – abrite des antennes paraboliques ultra-puissantes capables d'intercepter les communications satellitaires. Selon diverses estimations, près de 2 000 personnes y travaillent, dont environ 1 500 Américains, témoignant de l'implication prépondérante des États-Unis dans le dispositif.

D'autres stations similaires complètent ce réseau mondial, comme Yakima aux États-Unis, Waihopai en Nouvelle-Zélande, Pine Gap en Australie, ou encore Buckley AFB au Colorado. Chacune possède des caractéristiques et des missions spécifiques, mais toutes concourent au même objectif de collecter un maximum de données électroniques.

L'interception ne se limite pas aux communications aériennes. Les câbles sous-marins, qui transportent une part considérable des télécommunications mondiales, font également l'objet d'une surveillance attentive. L'opération Ivy Bells, révélée dans les années 1980, illustre parfaitement cette dimension. Pendant plusieurs années, des sous-marins américains posèrent des dispositifs d'enregistrement (les POD) sur des câbles soviétiques au fond de la mer d'Okhotsk, captant ainsi des communications que les Russes croyaient inviolables. L'évolution technologique a nécessité l'adaptation constante des moyens d'interception. À l'ère de la fibre optique, les points de vulnérabilité se situent principalement au niveau des répéteurs, où le signal lumineux est temporairement converti en signal électrique, offrant ainsi une fenêtre d'opportunité pour l'interception.

En complément des stations terrestres et des dispositifs sous-marins, des satellites de surveillance viennent parachever l'architecture d'Echelon. Ces engins, placés sur des orbites hautement elliptiques, sont équipés d'imposantes antennes paraboliques (certaines atteignant jusqu'à 100 mètres de diamètre) capables de capter les signaux qui, normalement, se disperseraient dans l'espace.

3 Le fonctionnement : de l'interception à l'analyse

La puissance d'Echelon réside dans sa méthodologie d'interception et de traitement des données. Son principe de fonctionnement peut se résumer en trois étapes essentielles : collecte massive, filtrage automatisé et analyse humaine.

La première phase consiste à intercepter le plus grand volume possible de communications électroniques. Contrairement à une idée reçue, Echelon ne cible pas uniquement des individus ou des organisations spécifiques, mais procède à une collecte indiscriminée de données. Tout ce qui transite par satellite, ondes radio, câbles téléphoniques ou internet est susceptible d'être capturé.

Ces données brutes, d'un volume colossal, sont ensuite filtrées par des systèmes informatiques surpuissants, principalement situés au siège de la NSA à Fort George G. Meade, dans le Maryland. Ces ordinateurs recherchent, dans le flux continu des communications, certains mots-clés ou expressions prédéfinis – un système appelé « dictionnaire » dans le jargon du renseignement. Quand une communication contient ces termes sensibles, elle est automatiquement signalée pour analyse.

Vient alors la troisième étape : l'analyse humaine. Des spécialistes examinent les communications suspectes et déterminent leur pertinence. Si l'information est jugée valable, elle peut être partagée entre les membres de l'alliance selon des protocoles stricts. Chaque pays membre dispose de droits d'accès spécifiques, avec les États-Unis occupant une position privilégiée dans cette hiérarchie informationnelle.

Cette chaîne de traitement permet au réseau de trier efficacement parmi des millions de communications quotidiennes. Un exemple révélateur : un ancien agent canadien du CSE (équivalent canadien de la NSA) a rapporté qu'une simple conversation téléphonique où une mère mentionnait que son fils avait « vraiment fait un bide » lors d'une pièce de théâtre scolaire avait été signalée, le mot « bide » (*bombed* en anglais) ayant déclenché une alerte terroriste.

4 Stratégie et géopolitique : les visages changeants d'Echelon

La fin de la Guerre froide aurait pu marquer le crépuscule d'Echelon. La menace soviétique s'étant dissipée, sa raison d'être initiale semblait caduque. Pourtant, loin de disparaître, le réseau s'est réinventé, trouvant de nouvelles justifications à son existence et élargissant son champ d'action.

La lutte contre le terrorisme s'est rapidement imposée comme une priorité, particulièrement après les attentats du 11 septembre 2001. Les autorités américaines ont souligné l'importance cruciale d'Echelon pour prévenir de futures attaques, légitimant ainsi la poursuite et même l'intensification des activités de surveillance.

Parallèlement, le réseau s'est tourné vers des cibles économiques et diplomatiques. Les négociations commerciales internationales, les innovations technologiques des pays concurrents, les stratégies industrielles étrangères – tout est devenu potentiellement intéressant pour les analystes d'Echelon.

Cette réorientation a provoqué de vives tensions au sein même des alliances occidentales. Des révélations sur des cas d'espionnage économique visant des entreprises européennes ont suscité l'indignation. L'Allemagne, en particulier, s'est montrée préoccupée après la découverte que la NSA avait espionné des sociétés comme Enercon, un fabricant d'éoliennes. Selon plusieurs sources, les informations interceptées auraient été transmises à Kenetech, un concurrent américain, permettant à ce dernier d'obtenir un brevet similaire et d'interdire l'accès au marché américain à Enercon.

Le cas d'Airbus reste emblématique. En 1994, des communications entre l'avionneur européen et la compagnie Saudi Arabian Airlines auraient été interceptées et transmises à Boeing et McDonnell Douglas. Ces derniers obtinrent finalement le contrat de 6 milliards de dollars qui semblait initialement promis à Airbus. Bien que la preuve formelle de l'implication d'Echelon soit difficile à établir, ces coïncidences troublantes ont alimenté la méfiance européenne.

Face à ces soupçons, la position américaine est restée ambivalente. James Woolsey, ancien directeur de la CIA, admit que les États-Unis espionnaient effectivement des entreprises européennes, mais affirma que c'était principalement pour détecter les pratiques de corruption, et non pour voler des secrets commerciaux. Cette justification n'a guère convaincu les partenaires européens.

5 Les ambassades : des avant-postes discrets

Au-delà des grandes installations connues, le réseau Echelon s'appuie sur des points d'écoute plus discrets, notamment au sein des ambassades américaines à travers le monde. Ces représentations diplomatiques offrent une couverture idéale pour des activités de surveillance, bénéficiant de l'immunité diplomatique et d'emplacements souvent stratégiques au cœur des capitales.

L'équipement d'interception arrive généralement dans les ambassades par valise diplomatique, échappant ainsi aux contrôles douaniers. Dans certains cas, comme à l'ambassade américaine à Paris, les installations d'espionnage peuvent occuper un étage entier, généralement le dernier, dépourvu de fenêtres. Ces systèmes sophistiqués permettent d'intercepter une grande variété de communications dans un large périmètre : celles d'autres ambassades, du parlement, du gouvernement, ainsi que celles des entreprises et des particuliers.

Les antennes de grande taille sont soigneusement dissimulées pour ne pas éveiller les soupçons. L'immunité diplomatique rend pratiquement impossible toute tentative de contrôle de la part du pays hôte, même en cas de soupçons avérés d'activités d'espionnage.

6 L'Europe face à Echelon : enquêtes et réactions

Les révélations sur l'existence et l'ampleur du réseau Echelon ont suscité de vives réactions au sein des institutions européennes. Cette prise de conscience a conduit à plusieurs initiatives visant à enquêter sur le système et à évaluer ses implications.

En 1998, le Parlement européen commanda une première étude au Scientific and Technological Options Assessment, intitulée « Une évaluation des technologies de contrôle politique ». Ce rapport mit en lumière l'existence d'Echelon, suscitant une onde de choc parmi les parlementaires européens. Suite à ce rapport initial, le Parlement demanda une série d'études complémentaires, dont un rapport détaillé rédigé par le journaliste britannique Duncan Campbell en 1999. Ce document fournit des informations plus précises sur le fonctionnement d'Echelon et ses implications pour l'Europe.

En réponse à ces révélations, le Parlement européen créa en juillet 2000 une commission temporaire sur le système d'interception Echelon. Cette commission, composée de 36 membres, avait pour mission d'enquêter sur l'existence d'Echelon et ses implications pour les citoyens et les entreprises de l'Union européenne. Le rapport final, publié en 2001, confirmait l'existence d'Echelon et soulignait les risques qu'il représentait pour la vie privée et les intérêts économiques européens. Il recommandait notamment le développement de technologies de chiffrement européennes et appelait à une meilleure protection des citoyens contre la surveillance électronique.

En France, la commission de la défense nationale soumit à l'Assemblée nationale, le 11 octobre 2000, un rapport sur les systèmes d'interception des télécommunications, abordant spécifiquement la question d'Echelon et proposant des mesures de protection.

Malgré ces initiatives, les efforts des institutions européennes se sont heurtés à plusieurs obstacles. Les États-Unis ont refusé de coopérer aux enquêtes, et la position ambiguë du Royaume-Uni, à la fois membre de l'Union européenne (jusqu'en 2020) et partenaire clé d'Echelon, a compliqué les discussions.

7 Les défis technologiques d'une surveillance globale

Malgré sa puissance, Echelon fait face à des défis technologiques croissants qui limitent son efficacité. L'évolution des moyens de communication a rendu l'interception plus complexe, obligeant le réseau à s'adapter constamment.

L'avènement de la fibre optique constitue un problème majeur. Contrairement aux câbles traditionnels, la fibre optique transporte l'information sous forme de lumière, rendant l'interception passive beaucoup plus difficile. De plus, sa capacité de transmission gigantesque génère un volume de données que même les supercalculateurs de la NSA peinent à traiter efficacement.

La démocratisation des techniques de chiffrement pose un autre problème. Des solutions comme le chiffrement de bout en bout, désormais intégrées à de nombreuses applications grand public, compliquent considérablement l'exploitation des données interceptées. Face à l'émergence de la cryptographie post-quantique, qui promet un niveau de sécurité encore supérieur, les capacités futures d'Echelon sont remises en question.

Pour surmonter ces obstacles, la NSA investit massivement dans de nouvelles technologies d'interception et d'analyse, ainsi que dans des supercalculateurs toujours plus puissants. Elle cherche également à contourner les mesures de sécurité en exploitant les failles des systèmes ou en tentant d'imposer des *backdoors* dans les produits de sécurité informatique.

Malgré ces efforts, la course entre les technologies de communication et les capacités d'interception reste serrée. L'efficacité future d'Echelon dépendra largement de sa capacité à surmonter ces obstacles technologiques, dans un contexte où la protection de la vie privée devient une préoccupation majeure.

8 Les dérives constatées : au-delà de la sécurité nationale

Au fil des années, plusieurs dérives et atteintes à la vie privée ont été constatées dans l'utilisation d'Echelon, dépassant largement le cadre de la sécurité nationale initialement invoqué.

Des organisations non gouvernementales comme Amnesty International et Greenpeace ont fait l'objet d'écoutes par le système. Des personnalités comme la princesse Diana et Mère Teresa auraient également été surveillées, notamment en raison de leur engagement contre les mines antipersonnel – un sujet sensible pour certains intérêts industriels et militaires.

Au niveau politique, des cas d'écoutes internes ont été rapportés. L'un des plus notoires concerne Margaret Thatcher, qui aurait utilisé Echelon pour surveiller deux ministres de son propre gouvernement. Pour éviter toute trace et nier son implication, elle aurait fait appel aux services canadiens du CSE plutôt qu'aux services britanniques du GCHQ, illustrant ainsi comment l'alliance des Five Eyes peut être utilisée pour contourner les restrictions légales nationales.

Plus largement, le système procède à une interception massive de communications privées, analysant de manière routinière des millions d'appels téléphoniques, fax et emails sans mandat ni contrôle judiciaire. Cette surveillance exploratoire généralisée, basée sur des mots-clés plutôt que sur des cibles spécifiques, signifie que potentiellement toute personne peut être écoutée.

Cette situation soulève de graves questions sur le respect de la vie privée et des libertés individuelles. Le fonctionnement d'Echelon semble violer les lois sur la protection des données personnelles en vigueur dans de nombreux pays. De plus, l'absence de contrôle démocratique sur les activités du réseau, qui échappent largement à la supervision des parlements et des citoyens, ouvre la porte à des abus potentiels.

9 Évolution récente : de l'ombre aux projecteurs

La révélation la plus spectaculaire concernant Echelon et, plus largement, les activités de surveillance des Five Eyes, a eu lieu en 2013 lorsqu'Edward Snowden, ancien employé de la NSA, a divulgué des milliers de documents classifiés. Ces documents ont confirmé non seulement l'existence d'Echelon mais aussi son évolution vers des systèmes encore plus intrusifs comme PRISM ou XKeyscore.

Ces révélations ont mis en lumière l'extension considérable des activités de surveillance après le 11 septembre 2001, au nom de la lutte contre le terrorisme. Elles ont aussi démontré comment les Five Eyes contournaient mutuellement leurs propres législations nationales. Pour éviter les restrictions légales sur la surveillance de leurs propres citoyens, chaque pays membre surveillait les citoyens des pays partenaires et partageait ensuite ces informations.

Par ailleurs, un rapport du journal norvégien Dagbladet a révélé en 2013 le rôle d'un site norvégien dans les écoutes de la NSA. La station située à Ringerike aurait été utilisée pour collecter les métadonnées relatives à 33,2 millions d'appels téléphoniques passés en Norvège sur une période de moins d'un mois.

Cette publicité accrue a conduit à des débats internationaux sur la balance entre sécurité nationale et respect de la vie privée. En réponse aux critiques, certains pays ont adopté des législations plus restrictives concernant la surveillance de masse, comme le USA Freedom Act aux États-Unis, qui limite partiellement les pouvoirs de la NSA. Toutefois, l'efficacité réelle de ces mesures reste sujette à caution, et les Five Eyes continuent d'étendre leurs capacités de surveillance en mettant l'accent sur la surveillance d'Internet.

FIGURE 1 – Radômes rigides du Centre des Opérations de Cryptologie à Misawa (Japon) – Photo dans le domaine public

10 L'élargissement des alliances de surveillance

Au-delà des Five Eyes historiques, d'autres alliances de surveillance ont émergé ces dernières années, élargissant le cercle des pays collaborant dans le domaine du renseignement électronique. Les « Nine Eyes » incluent les cinq membres originaux plus le Danemark, la France, les Pays-Bas et la Norvège. Les « Fourteen Eyes », formellement connus sous le nom d'SIGINT Seniors Europe, ajoutent l'Allemagne, la Belgique, l'Italie, l'Espagne et la Suède. Ces extensions témoignent d'une volonté d'intégrer davantage de pays dans l'échange de renseignements, tout en maintenant une hiérarchie claire où les Five Eyes originaux conservent un statut privilégié.

Le Japon [1] a manifesté son intérêt pour devenir le « sixième œil » de l'alliance, comme l'indiquait en 2020 son ministre de la Défense, Taro Kono. Cette extension potentielle reflète les préoccupations croissantes concernant l'influence chinoise dans la région Asie-Pacifique et illustre la dimension géopolitique persistante de ces alliances de renseignement.

Certains pays, bien que n'étant pas formellement membres de ces alliances, entretiennent des relations privilégiées avec le réseau. L'Allemagne, par exemple, abrite sur son sol la station d'écoute de Bad Aibling, gérée par la NSA, illustrant cette collaboration complexe même avec des pays qui, officiellement, ont parfois critiqué les pratiques américaines de surveillance.

11 Echelon aujourd'hui : persistance et adaptation

Malgré les controverses et les évolutions technologiques, le réseau Echelon semble toujours opérationnel aujourd'hui, comme en témoignent les images récentes des installations de Menwith Hill encore visibles sur Google Maps et Street View en mai 20242. Plusieurs facteurs expliquent cette pérennité remarquable.

D'abord, son efficacité dans la lutte antiterroriste reste reconnue par les services de renseignement. Même si les détails opérationnels demeurent secrets, les autorités continuent d'affirmer que le système a permis de déjouer plusieurs attentats.

Ensuite, les avantages stratégiques et économiques qu'il procure aux pays membres sont considérables. Au-delà de la sécurité nationale, l'accès privilégié à certaines informations sensibles confère un avantage significatif dans les négociations internationales et les marchés concurrentiels.

Par ailleurs, les États non-membres se trouvent dans une position délicate pour s'y opposer concrètement. Critiquer ouvertement le système pourrait entraîner des répercussions diplomatiques ou économiques que peu de nations sont prêtes à risquer.

Enfin, et c'est peut-être le point le plus important, l'évolution technologique constante du réseau lui permet de s'adapter aux nouveaux moyens de communication. Les investissements massifs dans la recherche et développement maintiennent Echelon à la pointe de la technologie de surveillance, malgré les défis mentionnés précédemment.

L'existence d'Echelon a néanmoins eu des conséquences importantes sur la sécurité des communications. De nombreux pays et entreprises ont été poussés à développer leurs propres systèmes de protection et de

FIGURE 2 – Base de Menwith Hill, Yorkshire, Royaume-Uni – Photo Google Street View – Mai 2024

chiffrement. Cette course à la sécurité informatique a stimulé l'innovation dans le domaine de la cryptographie et de la protection des données, illustrant parfaitement l'éternel jeu du chat et de la souris entre surveillance et protection de la vie privée.

12 Conclusion

Le réseau Echelon représente l'une des entreprises de surveillance les plus ambitieuses de l'histoire. Né dans le contexte de la Guerre froide, il a su évoluer et s'adapter aux bouleversements géopolitiques et technologiques, conservant sa pertinence dans un monde radicalement différent de celui qui l'a vu naître.

Son existence soulève des questions fondamentales sur l'équilibre entre sécurité nationale et libertés individuelles. Si la lutte contre le terrorisme et les menaces extérieures justifie une certaine forme de surveillance, l'absence de contrôle démocratique et la possibilité d'abus restent des préoccupations majeures.

Les révélations sur l'espionnage économique et politique ont également mis en lumière les tensions inhérentes à un système où la frontière entre protection des intérêts nationaux et avantage concurrentiel déloyal devient de plus en plus floue.

À l'ère numérique, où nos vies se déroulent de plus en plus en ligne, la question de la surveillance électronique prend une dimension encore plus critique. Le réseau Echelon nous rappelle que, dans l'ombre de nos communications quotidiennes, des yeux et des oreilles sont peut-être à l'affût, captant et analysant nos échanges les plus privés.

Face à cette réalité, la vigilance citoyenne et le débat démocratique sur les limites acceptables de la surveillance apparaissent plus nécessaires que jamais. Car si la sécurité est un droit fondamental, la liberté et la vie privée le sont tout autant.

Références

[1] N. HAGER, Secret Power : New Zealand's Role in the International Spy Network. Nelson, New Zealand : Craig Potton Publishing, 1996.

[2] D. CAMPBELL, « Somebody's listening, » *New Statesman*, t. 4, n° 12, p. 10-12, 1988.

[3] S. WRIGHT, « An appraisal of technologies of political control, » European Parliament, Scientific et Technological Options Assessment, 1998.

[4] D. CAMPBELL, « Interception capabilities 2000, » European Parliament, Scientific et Technological Options Assessment, 2001.

[5] P. R. KEEFE, Chatter : Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping. New York : Random House, 2006.

[6] M. FROST et M. GRATTON, Spyworld : Inside the Canadian and American Intelligence Establishments. Doubleday Canada, 1994.

[7] C. DELESSE, « Du réseau ECHELON à la « révolution des affaires de renseignement » aux États-Unis, » *Annuaire français de relations internationales*, t. 5, p. 645-655, 2004.

[8] TEMPORARY COMMITTEE ON THE ECHELON INTERCEPTION SYSTEM, « Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), » European Parliament, Session Document, 2001.

[9] L. Poitras, G. Greenwald et E. MacAskill, « NSA whistleblower Edward Snowden : 'I don't want to live in a society that does these sort of things', » *The Guardian*, 9 juin 2013.

[10] P. Rivière, « Le système Echelon, » *Le Monde diplomatique*, juill. 1999.

[11] R. J. Woolsey, « Why We Spy on Our Allies, » *The Wall Street Journal*, 17 mars 2000.

[12] Atlas Report, « The Real History of the ECHELON Program : The "5 Eyes" Global Espionage Alliance, » *Atlas Report*, 25 juill. 2024.

[13] J.-M. Dinant et Y. Poullet, « Le réseau Echelon. Existe-t-il ? Que peut-il faire ? Peut-on et doit-on s'en protéger ? » *Droit de l'informatique et des télécoms*, p. 10-22, 2000.

[14] Commission de la défense nationale et des forces armées, « Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, » Assemblée Nationale, 2623, 11 oct. 2000.

[15] L. Matney, Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life, TechCrunch, 3 août 2015.

[16] M. Bera, Remembering ECHELON: The First International Mass Surveillance Program, IDN-InDepthNews, 20 avr. 2022.

[17] J. Carter, What You Should Know About the "Five Eyes" Intelligence Community, Providence, 18 mai 2017.

[18] E. MacAskill, J. Borger, N. Hopkins, N. Davies et J. Ball, « GCHQ taps fibre-optic cables for secret access to world's communications, » *The Guardian*, 21 juin 2013.

[19] Windpower Monthly, « Trans Atlantic espionage claimed by German wind company, » *Windpower Monthly*, mai 1999.

[20] S. Vingoe, Inside the Global Signals Intelligence Apparatus: An Overview of the Five Eyes Alliance, NATO Association of Canada, 2015.

[21] FO Airbus Groupe, AIRBUS ciblé par des cyberattaques, un espionnage industriel piloté depuis la Chine? FO Airbus Groupe, 26 sept. 2019.

[22] CyberInsider, Five Eyes, Nine Eyes, 14 Eyes (What to Avoid in 2025), CyberInsider, 2024.

[23] Privacy Journal, What are the Five Eyes, Nine Eyes, & 14 Eyes in 2025? Privacy Journal, 24 oct. 2024.

[24] VPNMentor, What Are the 5/9/14 Eyes Countries? Surveillance in 2025, VPNMentor, 2024.

[25] D. Fouquereau, Echelon : un réseau d'espionnage planétaire, Eurêka, 2000.

[26] Postman Patel, Enercon v Echelon - how comercial espionage actually works at the nation state level, UK TOP SECRET Postman Patel, mai 2008.

[27] P. Germano, Echelon [P415], Blog de Patrick Germano, juill. 2007.

[28] A. Dinan, One of the Oldest Conspiracies Proven True: Project Echelon, Gaia, 2023.

[29] List23, 5 Eyes, 9 Eyes, and 14 Eyes: A Surveillance Primer, List23 : Latest U.S. & World News, 15 août 2022.

[30] TechTarget, What is the Five Eyes Alliance? TechTarget, 2024.

[31] Techno-Science.net, Echelon : définition et explications, Techno-Science.net, 2020.

[32] R. Gallagher, The Powerful Global Spy Alliance You Never Knew Existed, The Intercept, mars 2018.