Extrait de

CENTRE D'ÉTUDES D'HISTOIRE
DE LA DÉFENSE

LE RENSEIGNEMENT :
Guerre, Technique et Politique
(XIXe-XXe siècles)

sous la direction de Bertrand Warusfel

LAVAUZELLE
2004

UKUSA : LE DÉVELOPPEMENT DU RENSEIGNEMENT TECHNIQUE ANGLO-SAXON À PARTIR DE LA SECONDE GUERRE MONDIALE

par Bertrand Warusfel

Quatre rapports remis au service d'étude du parlement européen[1] ont déclenché en 1999 une vive controverse autour du mal-nommé « réseau *ÉCHELON* ». Le grand public découvrit alors que les États-Unis et plusieurs pays anglo-saxons entretenaient depuis plus de cinquante ans d'importants moyens d'écoute afin d'intercepter les communications internationales. Le retentissement en fut considérable, comme celui qu'avait déjà provoqué en 1931 la publication de *The American Black Chamber*[2], l'ouvrage de Yardley, l'ancien chef du service de décryptement du département d'État, qui révélait que les États-Unis décryptaient secrètement les messages diplomatiques depuis 1912. Mais entre ces deux scandales, le rapprochement ne s'arrête pas là. On sait aujourd'hui que le système mondial de renseignement électronique anglo-saxon actuellement en service trouve directement ses racines profondes dans les efforts que le gouvernement américain a entrepris dans les années 1930 puis durant la Seconde Guerre mondiale pour développer ses moyens de décryptement et pour coopérer avec le Royaume-Uni dans ce domaine très sensible.

---

[1] Rapports publiés sous le titre commun de « Development of Surveillance Technology and Risk of Abuse of Economic Information », STOA/PE 168.184, octobre 1999 et comprenant quatre volumes rédigés respectivement par Duncan CAMPBELL, Franck LEPRÉVOST, Chris ELLIOTT et Nikos BOGONIKOLOS (disponibles sur le site http ://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-1en.pdf).

[2] Publié ensuite en français, sous le titre *Le cabinet noir américain*, Éd. de la nouvelle revue critique, 1935.

En effet, bien que le secrétaire d'État Stimson ait annoncé en 1929 mettre fin aux activités de décryptement du département d'État[3], le scandale créé par les révélations de Yardley (qui dut quitter les États-Unis) n'empêcha pas l'*US Navy* de poursuivre, de son côté, le travail de sa propre unité de décryptement, l'*OP20G*. De même, l'armée de terre confia en 1930 l'interception et le décryptement des messages étrangers à la nouvelle section cryptographique de l'*US Army's Signal Corps*, le *Signal Intelligence Service* (*SIS*). Le chef de ce nouveau *SIS* William F. Friedman, devint alors la cheville ouvrière du renseignement technique américain et contribua à lui donner une importance accrue[4]. Ce mouvement trouva son aboutissement durant la Seconde Guerre mondiale quand le *SIS* et l'*OP20G* conclurent une alliance avec le renseignement britannique, à ce point indéfectible qu'elle perdure encore aujourd'hui et qu'elle a joué un rôle majeur et méconnu durant toute la guerre froide. Les remous actuels autour du « réseau *ÉCHELON* » trouvent ainsi leur origine dans cette relance du renseignement cryptographique anglo-saxon qui se poursuivit après 1945 par l'accord *UKUSA* et qui donna lieu à l'exploitation d'une des sources de renseignement les plus secrètes de la guerre froide, l'opération *VENONA*.

ULTRA et *MAGIC* : une alliance de guerre

À la veille de l'invasion de la France en 1940, les Britanniques avaient engagé tardivement une coopération en matière d'interception radios et de cryptographie avec les services du SR français et ceux des nations alliés d'Europe centrale, la Pologne et la Tchécoslovaquie[5]. Ce fut ainsi que le Royaume-Uni put accéder, en août 1939, aux premiers résultats obtenus par les Français et les Polonais dans le décryptement de la machine à chiffrer allemande *ENIGMA*[6]. Mais aux lendemains de l'armistice de juin 1940, cette collaboration cessa (sauf en ce qui

[3] En prononçant la fameuse sentence restée célèbre : *Gentlemen do not read other Gentlemen's mail* (« Un gentleman ne lit pas le courrier des autres »).

[4] Pour son témoignage, cf. William F. FRIEDMAN, « *A Brief History of The Signal Intelligence Service* », *in* James P. FINLEY (dir.), *U.S. Army Military Intelligence History : A Sourcebook*, U.S. Army Intelligence Center & Fort Huachuca, Fort Huachuca, Arizona, 1995, p. 152-158.

[5] Cf. notamment, Gilbert BLOCH, « Polish Reconstitution of the German Military - *Enigma* and the First Decryptments of its Messages », *The Journal of Intelligence History*, Volume 1, n° 1, Summer 2001 ; également « *ENIGMA* Before *ULTRA* : Polish Work and French Connection », *Cryptologia*, Volume XI, n° 3, July 1987.

[6] Cf. notamment – en ce qui concerne les témoignages du côté français – Gustave BERTRAND, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Plon, 1973 et Paul PAILLOLE, *Notre agent chez Hitler*, Robert Laffont, 1985.

concerne l'équipe clandestine du commandant Bertrand du SR français qui effectua plus de 4 000 décryptements *ENIGMA* entre juillet 1940 et novembre 1942 depuis la zone libre, en liaison avec Londres[7]) et les Britanniques placés en première ligne face à l'Allemagne dans le cadre de la « bataille d'Angleterre » se tournèrent rapidement vers les États-Unis, quoique ceux-ci soient toujours neutres.

Cette coopération commença officieusement en septembre 1940 lorsque le général Marshall, chef d'État-major américain autorisa le *SIS* américain à coopérer avec ses homologues britanniques (c'est-à-dire la *Goverment Codes and Cypher School-GC&CS*, créée en 1919 et repliée à partir de 1939 au château de Bletchley Park). Cette proposition fut acceptée par Churchill dès que celui-ci connut, en octobre, les résultats significatifs obtenus par les Américains dans le déchiffrement des messages diplomatiques japonais[8]. Un premier accord secret fut donc signé en novembre 1940[9] et dès février 1941, une délégation de cryptologues américains de l'*OP20G* et du *SIS* (qui devait à l'origine être dirigée par Friedmann, lequel ne put l'assurer du fait d'une dépression nerveuse, et qui fut finalement menée par l'un de ses adjoints Abraham Sinkov) apporta à Bletchley Park deux copies des machines à chiffrer *PURPLE* et *RED* qui permettaient de réaliser le décryptement des messages japonais[10]. En retour, les Américains reçurent des informations utiles pour faciliter le décryptement des messages navals allemands[11].

Mais l'entente n'était pas encore totale entre la Grande-Bretagne en guerre et l'Amérique toujours neutre. Aussi, les Britanniques ne donnèrent pas à leurs homologues de copies d'*ENIGMA*. De même, certains travaux semblent indiquer qu'ils n'auraient pas transmis en 1941 au gou-

[7] Cf. G. BERTRAND, *op. cit.*, p. 110-111 et p. 117 ; également Eunan O'HALPIN, « Small States and Big Secrets : Understanding Sigint Cooperation between Unequal Powers during the Second World War », *Intelligence & National Security*, Vol. 17, n° 3, p. 10 (qui – citant des sources britanniques – limite la coopération secrète entre Bletchey Park et Bertrand à la période mars 1941-août 1942).

[8] James BAMFORD, *Puzzle Palace – Inside the National Security Agency, America's most secret intelligence organisation*, Penguin Books, 1982 (nouvelle édition : 1983), p. 394.

[9] *Ibid.*

[10] Cf. notamment Ralph ERSKINE, « Anglo-US Cryptological Co-operation », conférence au 5e colloque annuel de l'*International Intelligence History Study Group*, 18-20 June 1999 (résumé in *International Intelligence History Study Group Newsletter*, Vol. 7, n° 1, Summer 1999, http ://intelligence-history.wiso.uni-erlangen.de/. Également, Nigel WEST, *Venona – The greatest secret of the cold war*, 1999, ed. paperback 2000, p. 2 ; Rusbridger & Nave, *op. cit.*, p. 120-122).

[11] Ralph ERSKINE, « What did the Sinkov Mission receive from Bletchley Park ? », *Cryptologia*, April 2000, Volume XXIV, n° 2, p. 97-109 ; cf. également le témoignage de l'un des membres de la mission Sinkov : Prescott CURRIER, « My 'Purple' Trip to England in 1941 », *Cryptologia*, July 1996, Volume XX, n° 3, p. 193-201.

vernement américain tous les décryptements en leur possession concernant les projets d'attaque japonais, afin de préserver le secret sur le fait qu'ils déchiffraient depuis 1939 le code naval japonais (dénommé JN25), voire pour obliger les États-Unis à basculer dans la guerre et à rejoindre le camp allié[12].

Une fois l'Amérique officiellement en guerre après Pearl Harbour, la situation évolua et les réticences disparurent assez rapidement. En avril 1942, un officier de la *GC&CS*, le colonel John Tiltman visita l'*OP-20-G* et son voyage permit d'organiser une coordination plus étroite en matière de renseignement naval[13]. Elle fut institutionnalisée par un accord du 1er octobre 1942 (conclu à *Washington* entre Travis pour la *GC&CS* et le capitaine Joseph Wenger de l'*US Navy*[14]), ce qui permit aux Américains et aux Britanniques non seulement d'échanger les informations décryptées concernant les opérations navales en Atlantique, mais aussi de se répartir les tâches de décryptement[15]. Le texte de l'accord est clair sur ce point :

> « The British will withdraw from active work in the Pacific Area and leave to the US the general direction and control of the combined effort against the Japanese. They plan to maintain a research unit at GC&CS so as not to lose touch with the Japanese problem. They have acceded to us desires with regard to work on the German submarine and naval problem but, in effect, will be the coordinating head in the Atlantic theatre as the US will be in the Pacific. »

[12] C'est la thèse centrale de l'ouvrage écrit à partir des souvenirs du cryptologue australien Eric Nave qui travailla à Hong Kong et à Singapour pour le compte de la *GC &CS* durant la guerre : James RUSBRIDGER & Eric NAVE, *Betrayal of Pearl Harbor – How Churchill Lured Roosevelt into World War II*, Simon & Schuster, New York, 1991, traduction française : *Trahison à Pearl Harbour – Comment Churchill a entraîné Roosevelt dans la Seconde Guerre mondiale*, Pygmalion/Gerard Watelet, 1992.

[13] Cf. J.N. WENGER, H.T. ENGSTROM, and R.I. MEADER, « History of the Bombe Project », *OP-20-G* Memorandum dated 30 May 1944, 2 (*NARA* Record Group 457, File #4584.) – cité.

[14] Cf. Bradley F. SMITH, *The Ultra-Magic Deals and the Most Secret Special Relationship, 1940-1946*, Presidio Press, 1992, reed. paperback, Presidio, 1994, p. 126-129. Le texte de cet accord (dont le titre exact est *Memorandum for OP-20 : Collaboration of U.S. and British radio intelligence organizations on Japanese and German projects*, 1 October 1942) a été publié et mis en ligne par le Mariners Museum de Newport (http ://www.mariner.org).

[15] Cf. Ralph ERSKINE, « The Holden Agreement on Naval Sigint : The First BRUSA? » *Intelligence and National Security*, Volume 14, n° 2, Summer 1999, p. 187-197. Alors de R. ERSKINE semble considérer dans l'article précité que cet accord naval (qu'il nomme *Holden Agreement*, du nom de l'officier de la *Royal Navy* qui le contresigna pour le compte de la marine britannique) a été le véritable fondement des relations privilégiées anglo-américaines en matière de renseignement technique, Bradley SMITH considère pour sa part qu'il ne s'agissait encore que d'un accord restreint et précurseur (B. SMITH, *op. cit.*, p. 129), ce qui le distinguerait de l'accord *BRUSA* ultérieur de 1943 (cf. *infra*) qui aurait revêtu au contraire, un caractère totalement innovant (*op. cit.*, p. 157).

Cette coopération anglo-américaine eut tout de suite une grande importance pour permettre la lutte anti-sous-marine et la protection des convois alliés durant la bataille de l'Atlantique[16].

Cet accord fut ensuite élargi à l'ensemble des informations militaires recueillies par les moyens de décryptement par un accord global dénommé *BRUSA* (*Britain-USA*), signé le 17 mai 1943[17] à l'occasion d'un nouveau séjour d'une délégation américaine (qui comprenait cette fois Friedman lui-même). Dès lors, les Américains surent tout concernant *ENIGMA*[18] et les techniques de décryptement mises au point à Bletchley Park (y compris les machines à casser les clés, dites *Bomba*[19]) et leurs forces armées eurent accès aux décryptements *ENIGMA* réalisés par les Britanniques (et diffusés sous le code *Ultra*). De leur côté, les Britanniques eurent également accès aux décryptements *MAGIC* des messages japonais.

[16] Cf. Commander Jerry C. RUSSELL, « Ultra and the Campaign against the U-Boats in World War II », US Army War College, 20 may 1980 (consultable sur le site www.history.acusd.edu) ; également, Stephen BUDIANSKY, « German vs. Allied Codebreakers in the Battle of the Atlantic », *International Journal of Naval History*, Volume 1, n° 1, April 2002. Ce décryptement des communications navales allemandes fut largement coordonné par le mathématicien britannique Alan Turing, que la *GCCS* avait recruté à *Blechtley Park* à partir de 1939 et qui fut ensuite l'un des concepteurs des machines informatiques contemporaines (cf. notamment sa biographie : Andrew HODGES, *Alan Turing ou l'énigme de l'intelligence, traduction française* : Payot, 1988, en particulier son chapitre IV). Inversement, la coopération anglo-canado-américaine en matière de chiffrement des communications navales (notamment celles relatives aux convois qui traversaient l'Atlantique) fut relativement longue à se mettre en place, ce qui permit aux services allemands de décrypter de nombreux messages alliés (cf. Ralph ERSKINE, « The Admiralty and Cipher Machines During the Second World War : Not So Stupid after All », *The Journal of Intelligence History*, Volume 2, n° 2, Winter 2002).

[17] Cf. J. RICHELSON, *The U.S. Intelligence Community*, Westview Press, 4e ed., 1999, p. 292 ; R. ERSKINE, *op. cit.* ; Bamford, *op. cit.*, p. 397 ; également, « The BRUSA Agreement of May 17 1943 » *Cryptologia*, Vol 21, n° 1, 1997, p. 30-38.

[18] J. BAMFORD, *op. cit.*, p. 396.

[19] R. ERSKINE, *op. cit.* Dès l'accord de 1942 sur le renseignement naval, les Britanniques avaient partagé avec les Américains les caractéristiques de la *Bomba* – mises au point par Turing à partir des prototypes polonais – afin que ceux-ci puissent en fabriquer pour leurs propres opérations de décryptement. Alan Turing fut envoyé à *Washington* en décembre 1942 pour conseiller les Américains sur la mise au point de leurs propres *Bomba* et en contrepartie de cette assistance, *Bletchley Park* conserva la coordination des décryptements réalisés des deux côtés de l'Atlantique (cf. A. HODGES, *op. cit.*, p. 206 et 212-213). Le rapport de sa visite à l'usine NCR de *Dayton* – où se construisaient les « Bombes » navales américaines – a été publié : A. TURING, « Visit to National Cash Register Corporation of Dayton, Ohio », *Cryptologia*, Volume 25, n° 1, janvier 2001, p. 1-7.

Cette coopération se traduisit notamment par l'affectation à Bletchley Park, à partir d'août 1943, d'un contingent de militaires américains du *Signal Corps*, qui étaient commandés par le capitaine Bundy[20]. L'effectif de ce détachement augmenta progressivement pour atteindre une soixantaine de personnes en 1944, répartis principalement entre trois affectations : les décryptements *ENIGMA* de la *Wehrmacht* et de la *Luftwaffe* (confiés à la « hutte 6 »), la traduction et l'interprétation de ces décryptements (confiées à la « hutte 3 »), l'analyse des trafics radios (assurée par la section dite *Sixta*) et le décryptement des machines allemandes dites *Fish* (machines à chiffrer automatiques de type téléscripteur – et non plus manuelle comme *ENIGMA* – utilisées par le haut commandement allemand à partir de 1941 et utilisant le code Baudot, différent du morse)[21].

Quant aux dominions britanniques (en particulier, le Canada, l'Australie et la Nouvelle-Zélande), leur contribution fut également requise pour permettre de bénéficier de stations d'écoute placées sur leur sol. Au Canada, notamment, fut créé en 1941 un bureau de renseignement électromagnétique appelé « sous-section de l'examen » qui travailla durant toute la guerre à intercepter des messages provenant tout à la fois d'Allemagne, d'Italie, d'Amérique du Sud, d'Asie ou d'Union soviétique, et les partagea avec les Britanniques et les Américains[22]. En mars 1944, une conférence interalliée réunit d'ailleurs à Arlington les services britanniques et américains avec les unités d'interception canadiennes et australiennes[23]. Et pour organiser cette coopération, les deux responsables britanniques du renseignement cryptographique (Travis et Hinsley) arrivèrent en avril 1945 à *Washington* tandis que l'amiral Rushbrooke se rendait, pour sa part, au Canada[24].

[20] Cf. son témoignage : William P. BUNDY, « From the Depths to the Heights », *Cryptologia*, Volume VI, n° 1, January 1982, p. 65-74.

[21] Pour une synthèse d'époque sur l'activité de ce contingent, dénommé en 1944 le *6813th Signals Security Detachment*, cf. le rapport déclassifié : *Technical History of 6813th Signals Security Detachment*, 20 October 1945 (accessible sur le site www.codesandciphers.org.uk). Cf. également deux témoignages d'officiers américains affectés à Bletchley : Telford TAYLOR, « Anglo-American signals intelligence co-operation », *in* F. H. HINSLEY & A. STRIPP, *Codebreakers - The inside Story of Bletchley Park*, Oxford University Press, 1993, reed. Oxford Paperbacks, 1994, p. 71-73 ; Robert M. SLUSSER, « An american at *Bletchley Park* », *ibid.*, p. 74-76.

[22] Cf. « Historique du Centre de la sécurité des télécommunications », in *Rapport 1996-1997 du Commissaire au CST*, Canada.

[23] J. BAMFORD, *op. cit.*, p. 398.

[24] Cf. Christopher ANDREW, *For the President's Eyes Only : Secret Intelligence and the American Presidency from Washington to Bush* (1re ed. : Harper&Collins, 1995), Paperback ed. : Perennial, 1996, note 18, p. 569.

C'est donc très naturellement que le retournement de la situation internationale à la fin de la Seconde Guerre mondiale et les débuts de la guerre froide conduisirent les membres anglo-saxons de cette alliance de guerre (à laquelle n'avaient été invités ni les services français – pour cause d'occupation – ni ceux d'Union soviétique) à intensifier leur coopération technique secrète, pour lutter contre le nouveau danger communiste qui apparaissait en Europe et en Asie[25].

Un mémorandum rédigé à l'attention du Président Truman le 12 septembre 1945 par Stimson, Forrestal et Acheson est très clair sur ce point :

> *In view of the disturbed conditions of the world and the necessity of keeping informed of technical developments and possible hostile intentions of foreign nations, [...] it is recommended that you authorize continuation of collaboration between the United States and the United Kingdom in the field of communications intelligence*[26].

Le président Truman suivit cette recommandation immédiatement et autorisa les responsables militaires américains à « continuer la collaboration de l'Armée et de la *Navy* avec les Britanniques dans le domaine du renseignement technique [communication intelligence] et à étendre, modifier ou restreindre cette collaboration dans le meilleur intérêt des États-Unis[27] ».

Ayant pris l'habitude – devant la menace des puissances de l'Axe – de partager étroitement les moyens et les informations issus des interceptions radios et des décryptements, les Américains et leurs alliés de l'empire britannique allaient donc être conduits à poursuivre et étendre leur collaboration dans le nouveau contexte stratégique de la guerre froide.

VENONA scelle la nouvelle coopération anti-soviétique

Cette reconduction de l'alliance anglo-saxonne en matière d'interception et de décryptement parut d'autant plus nécessaire que c'est dans ce domaine que se joua le premier acte de la guerre secrète entre l'Est

[25] Selon le rapport officiel canadien précité, la décision canadienne de continuer après-guerre à faire intercepter les communications par ce qui allait devenir le centre de la sécurité des télécommunications, aurait été « influencée par les demandes de maintien de l'aide à la collecte de renseignements faites par les États-Unis et la Grande-Bretagne, et par les révélations du transfuge soviétique Igor Gouzenko touchant les activités de renseignement menées par l'URSS au Canada et aux États-Unis » (rapport 1996-1997, *op. cit.*).

[26] Cité *in* Christopher ANDREW, *op. cit.*, p. 161.

[27] H. Truman le 12 septembre 1945, cité par Ch. ANDREW, *op. cit.*, p. 162.

et l'Ouest. Dès 1943, en effet, quelques cryptologues américains avaient commencé à étudier les messages soviétiques interceptés depuis 1939 par les compagnies de télégraphie américaines et les stations d'écoute radio du *SIS* (devenu *Signal Security Agency* en juin 1943).

Il semble que cette première analyse des câbles soviétiques aurait été décidée pour vérifier si une éventuelle négociation de paix séparée n'était pas engagée entre les Soviétiques et les nazis[28]. Mais l'orientation évolua rapidement vers la recherche d'informations relatives aux activités d'espionnage de l'Union soviétique en Occident.

Ce travail de bénédictin commença à porter ses fruits en 1946 lorsque – à partir de différents éléments recueillis en Allemagne à la fin de la guerre par les missions américano-britanniques *TICOM*[29] ainsi que d'un livre de codes soviétiques retrouvé en Finlande en 1944 – un remarquable cryptologue, Meredith Gardner put commencer à décrypter certains des codes utilisés par les services de renseignement soviétiques (*NKVD* et *GRU*). C'est ainsi qu'en novembre 1946, Gardner réussit à décrypter un message du 2 décembre 1944 révélant que les Soviétiques avaient connaissance du projet atomique *Manhattan* et du nom de plusieurs physiciens impliqués[30].

Dès cette époque, le décryptement des messages soviétiques interceptés durant la guerre devint une priorité en matière de contre-espionnage et les Américains décidèrent d'associer à ce vaste programme (connu d'abord sous le nom de *Jade* puis *Bride* puis enfin dénommé *VENONA*) leurs alliés anglo-saxons de la guerre. Le cryptologue Cecil Philips, puis Gardner lui-même, vinrent en Angleterre en 1945 et 1946 pour informer leurs homologues du nouveau *GCHQ* (*Government Communication Headquarters*, qui venait de remplacer la *GC&CS*) et

[28] Cf. John Earl HAYNES and Harvey KLEHR, *Venona : Decoding Soviet Espionage in America,* Yale University Press, 1999, chapitre 1er ; également James BAMFORD, *Body of secrets – How America's NSA and Britain's GCHQ Eavesdrop on the World*, Century, 2001, Paperback ed. : Arrows Books, 2002, p. 20.

[29] Les équipes *TICOM*, dont la base de départ était située à Bletchley, furent envoyées en Allemagne à la suite des forces alliées en 1944-1945 pour collecter et rapatrier toutes les informations et matériels cryptographiques utilisés par les Allemands (cf. notamment J. BAMFORD, *Body of Secrets, op. cit.* ; également, Nigel WEST, *Venona – The greatest secret of the Cold War*, HarperCollins, Londres, 1999). Comme dans les autres opérations de renseignement scientifique et technique menées en Allemagne, l'un de leurs objectifs majeurs était d'éviter que des compétences ou des données sensibles ne soient récupérées par l'armée soviétique lors de sa progression au cœur de l'Allemagne. À cela s'ajoutait l'intérêt de découvrir des messages soviétiques déjà déchiffrés par les Allemands, voire de pouvoir continuer à utiliser contre les codes soviétiques les spécialistes et les machines allemandes (ce qui fut fait dans certains cas).

[30] Cf. notamment N. WEST, *op. cit.*, p. 21. Le décryptement de ce message (tel qu'il fut définitivement terminé en 1952) est accessible sur le site de la *NSA*.

requérir l'assistance de ce service qui bénéficiait de l'inestimable expérience de Bletchley Park.

Cette expérience ne venait pas seulement de l'exceptionnel travail réalisé contre l'Allemagne. Elle résultait aussi de ce que, dès avant la guerre, la *GC&CS* avait déjà réalisé des interceptions et des décryptements sur les communications soviétiques.

On commence à connaître, en effet, l'importance (jusqu'alors sous-estimée) du travail d'interception et de décryptement mené par les Britanniques après la fin de la Première Guerre mondiale, en particulier en direction de la nouvelle menace incarnée par la naissance de l'URSS[31]. La notice historique officielle établie par les archives nationales britanniques, en 2003, concernant le *GCHQ* et ses prédécesseurs, affirme d'ailleurs nettement que « durant l'entre-deux-guerres, le travail de renseignement de la *GC&CS* était dirigé à l'encontre de l'URSS et de la menace que constituait la subversion et l'espionnage communiste[32] ». Les interceptions et les décryptements réalisés étaient notamment des messages diplomatiques[33] (qui purent être décryptés jusqu'en 1927, date à laquelle les Soviétiques optèrent pour l'utilisation du système très sûr du *one-time-pad*) ou des échanges radio à destination des militants des partis communistes étrangers[34]. Et si ces activités – menées souvent avec l'aide de pays limitrophes comme la Finlande[35] – furent arrêtées ou ralenties en 1941 lors de l'entrée en guerre de l'URSS, elles furent ensuite reprises rapidement, puisque les Britanniques recommencèrent à intercepter les communications soviétiques à destination des cellules

[31] Cf. Victor MADEIRA, « Because I Don't Trust Him, We are Friends : Signals Intelligence and the Reluctant Anglo-Soviet Embrace, 1917–24 », *Intelligence & National Security*, Vol. 19, n° 1, Spring 2004, p. 29-51.

[32] *Government Communications Headquarters and its predecessors*, Operational Selection Policy OSP 28, 2003, p. 3.

[33] Sur la présence de messages diplomatiques soviétiques décryptés parmi les archives du GC&CS entre 1919 et 1926, cf. Bradley F. SMITH, « New Intelligence Releases : A British Side to the Story », *in* David ALVAREZ (ed.) *Allied and Axis Signals Intelligence in World War II*, Frank Cass, 1999.

[34] Les interceptions du trafic à destination des partis-frères furent dénommées *Mask* et ont été déclassifiées par le *GCHQ* en octobre 1997 (cf. « Communist Party chief's secretary worked for *MI5* », *The Times*, 10 octobre 1997). Sur l'ensemble du travail des Britanniques à l'égard des Soviétiques jusqu'en 1941, cf. Craig Graham McKay, « British SIGINT and the Bear, 1919-1941- Some discoveries in the GC&CS archive », *KKrVAHT*, n° 2, 1997 (accessible sur le site suédois : www.kkrva.se/sve/kkrvaht/972/british_sigint.shtml) ; mention également dans l'historiographie officielle du programme *Venona* : Robert L. BENSON, « The Venona Story », *NSA*, Center for Cryptographic History, p. 5.

[35] Cf. notamment C.G. MCKAY, « Anglo-Finnish SIGINT Cooperation, 1940-1941 », *Journal of Intelligence History*, Vol. 3, n° 1 (Summer 2003).

du *Komintern* installées dans l'Europe occupée et en Chine à partir de 1943[36].

Les Canadiens furent également impliqués car ils venaient de bénéficier, en septembre 1945, de la première défection d'un chiffreur soviétique, Igor Gouzenko. Et à la même période, en octobre 1945, les Britanniques demandèrent aux Canadiens leur accord pour négocier en leur nom avec les États-Unis l'extension des échanges en matière d'interceptions[37]. De même, les Australiens furent mis au courant en 1948 par les Britanniques des activités soviétiques sur leur sol, que révélaient les premiers décryptements des échanges radios entre Canberra et Moscou[38]. Et à partir de 1947, les cryptologues britanniques et américains furent intégrés dans des équipes mixtes, tant à *Arlington Hall* (siège de l'*ASA* à Washington) qu'au siège du *GCHQ*[39].

Le travail engagé en 1943 sur les messages soviétiques aurait ainsi pu se poursuivre sur toutes les nouvelles interceptions de messages radios de l'URSS, mais cela fut rendu impossible par un changement brutal des procédures de chiffrement soviétiques le vendredi 29 octobre 1948. Ce jour-là – désormais connu dans l'histoire du renseignement américain comme le *Black Friday*, les Soviétiques revinrent à un usage strict des systèmes – quasi-inviolables – du *one-time pad* et les Anglo-saxons perdirent pour longtemps toute possibilité de décryptement efficace de leurs messages radios et télex[40]. Dès lors, le programme *VENONA* fut limité aux seuls messages interceptés avant cette date fatale et devint alors un programme purement rétrospectif. Cela changea aussi son utilisation : dès lors qu'il n'était plus possible d'espérer intercepter des données actuelles sur les activités et la politique soviétiques, *VENONA* ne fut plus considéré comme une source de renseignement extérieur, mais seulement comme un moyen unique de contre-espionnage, puisque les messages *VENONA* en cours de traitement devaient

[36] Ce programme d'interception reçut le nom de code *ISCOT* (ou *ISCOTT*), cf. Richard J. ALDRICH, *The Hidden Hand – Britain, America and Cold War Secret Intelligence*, John Murray, London, 2001, Paperbak edition : Overlook Press, 2002, p. 237 (qui indique que les décryptements *Ultra* fournirent également de précieuses informations sur le résultat des interceptions que la *Luftwaffe* effectuait avec succès contre les Soviétiques sur le front de l'Est). J. BAMFORD indique pour sa part que de 1943 à 1947, les interceptions britanniques portaient en particulier sur les échanges entre Moscou et Mao (J. BAMFORD, *Body of Secrets*, *op. cit.*, p. 27).

[37] Cf. Christopher ANDREW, « The Making of the Anglo-American SIGINT Alliance », *in* Win Hayden PEAKE and Samuel HALPERIN (dir.) *In the Name of Intelligence : Essays in Honor of Walter Pforzheimer*, Washington, NIBC Press, 1994, p. 105.

[38] Cf. Frank CAIN, « Venona in Australia and its Long-term Ramifications », *Journal of Contemporary History*, Volume 35, n° 2, Avril 2000.

[39] Cf. N. WEST, *op. cit.*, p. 27.

[40] Cf. notamment R. ALDRICH, *op. cit.*, p. 250.

permettre *a posteriori* d'identifier des sources et des agents soviétiques déjà actifs durant la guerre et dont une partie d'entre eux étaient susceptibles d'avoir continué de travailler pour le *KGB* ou le *GRU* après la fin du conflit. Cela explique pourquoi des spécialistes du contre-espionnage anglo-saxon, comme James Angleton (chef du contre-espionnage de la *CIA*) ou Peter Wright du *MI5* furent des utilisateurs et des défenseurs forcenés de *VENONA*, alors que rapidement certains s'interrogèrent dans les services respectifs sur l'utilité de continuer à long terme un travail aussi important et de moins en moins directement lié à l'actualité[41].

Ainsi *VENONA*, première grande opération de contre-espionnage de la guerre froide dont l'exploitation devait être à l'origine de la plupart des affaires de « taupe » de l'après-guerre (Burgess, MacLean, Fuchs, Rosenberg, Philby[42],...) fut en quelque sorte le berceau initiatique de cette nouvelle alliance anglo-saxonne du renseignement technique. Et elle se poursuivit tout au long des décennies de la guerre froide (puisque le décryptement ne fut définitivement arrêté qu'en octobre 1980[43]).

Mais d'emblée, l'accord qui s'établit entre les différentes agences (l'*Army Security Agency* – future *NSA*, le *GCHQ*, le *DSD* australien et le *CBNRC* canadien – futur *CST*) fut extrêmement étroit et très exclusif. C'est ainsi, par exemple, que le *GCHQ* fut informé de *VENONA* avant même le *FBI* américain (qui n'y fut associé qu'en 1947) tandis que la *CIA* n'en connut l'existence qu'en 1952[44], soit plus de quatre ans après qu'ait été conclu l'accord *UKUSA*.

Si, en effet, les alliés de la guerre mondiale ont continué à coopérer ensemble pour exploiter rétrospectivement les résultats de *VENONA* (c'est-à-dire, tirer profit dans leur lutte contre les services soviétiques, des informations issues des messages soviétiques échangés durant la guerre), ils avaient décidé de poursuivre à l'avenir de manière permanente leur coopération s'agissant des interceptions et des décryptements.

[41] N. WEST évoque ces débats internes, N. WEST, *op. cit.*, p. 36.

[42] Sur l'importance et les suites du programme *Venona*, cf. dans le même volume, l'article de Gildas LE VOGUER, « La "déclassification" des archives *Venona* par la *National Security Agency* », p. 279.

[43] Ce travail de près de quarante ans justifie certainement que *Venona* soit cité comme « un exemple de la persévérance dont il faut faire montre dans le domaine du *SIGINT* », ainsi que l'a déclaré l'actuel directeur de la *NSA*, le Général Michael V. Hayden (conférence devant la *Kennedy Political Union* à l'*American University*, le 17 février 2000, traduction par les services du parlement européen, CM\434208FR, PE 300.136, février 2002).

[44] Le *FBI* a notamment déclassifié le mémorandum établi par ce service après la réunion du 23 mai 1952 et qui reprend *« the results of the conference held between the Central Intelligence Agency and the Armed Forces Security Agency regarding the material, as obtained through liaison with AFSA »* (document accessible sur le site du *FBI*).

Mais désormais cette reconduction de l'alliance anglo-américaine (que l'on allait connaître plus tard sous le nom de *UK-USA*, en souvenir du premier accord *BR-USA*) allait se faire sous le contrôle et la direction des Américains.

Et le même secret qui enveloppa durant plus de trente ans les décryptements alliés de la guerre ainsi que le programme *VENONA*, fut aussi strictement appliqué à l'existence et au contenu de cette nouvelle organisation transnationale du renseignement technique.

UKUSA, un dispositif d'interception intégré sous contrôle américain

Le premier secret sur l'accord *UKUSA* concerne non seulement son contenu exact mais également les circonstances précises de sa conclusion.

D'après les deux spécialistes que sont James Bamford et le professeur Christopher Andrew, qui s'appuient sur des témoignages de première main recueillis auprès de responsables britanniques et américains, la première étape aurait été conclue à Londres en mars 1946[45]. Il ne s'agissait sans doute encore que de la reconduction de l'accord *BRUSA*, pour laquelle les Britanniques avaient obtenu des Canadiens de pouvoir signer l'arrangement en leur nom à *Washington*[46]. Mais l'accord définitif ne fut établi et signé qu'en 1948[47]. Ou plutôt, peut-on considérer, comme l'indique Richard Aldrich, que c'est à cette date que « l'ensemble complexe d'accords, de courriers et de *memoranda* auquel on se réfère souvent sous le nom de traité *UKUSA* » fut complété[48].

[45] Cf. J. BAMFORD, *Body of Secrets op. cit.*, p. 394 (qui donne la date précise du 5 mars 1946) ; Ch. ANDREW, *op. cit.*, p. 163. La date de 1946 avait déjà été mentionnée par R. Clark, qui – bien que ne mentionnant pas l'accord *UKUSA* – indiquait qu'un officier de liaison américain était venu à Londres en 1946 pour confirmer le maintien des échanges cryptographiques (Ronald CLARK, *The Man Who Broke Purple*, Boston, Little Brown, 1977, p. 208).

[46] Le commissaire canadien qui contrôle le *CST* reconnaît officiellement qu'*UKUSA* s'est créé sur la base de la reconduction des accords antérieurs conclus durant la Seconde Guerre mondiale, lorsqu'il indique que « le Canada profite d'arrangements de longue date » avec ses alliés anglo-saxons et que ces arrangements « ont été officialisés après la Deuxième Guerre mondiale et maintenus durant la guerre froide » (commissaire du centre de la sécurité des télécommunications – Rapport Annuel 2000-2001, p. 4).

[47] Ch. ANDREW réfute – en se basant sur le témoignage de Louis Tordella, futur directeur adjoint de la *NSA*, qui était présent – la date souvent évoquée de 1947 (Ch. ANDREW, *op. cit.*, p. 571, note 58). R. Aldrich fixe également à 1948 la finalisation des différents échanges. De même, M. Aid & C. Wiebes retiennent le mois de juin 1948 (Matthew AID & Cees WIEBES, *Intelligence & National Security*, Vol. 16, n° 1, Spring 2004, p. 314).

[48] R. ALDRICH, *op. cit.*, p. 245.

Dans l'intervalle, il semble que la Grande-Bretagne – dont le nouveau gouvernement travailliste avait pris quelques distances avec les États-Unis – avait cherché un moment à constituer une organisation *SIGINT* autonome au sein du nouveau *Commonwealth* et qui aurait rassemblé le Royaume-Uni et ses anciens dominions[49]. Une conférence secrète réunissant les services *SIGINT* des différents dominions se serait d'ailleurs tenue sous la présidence de Travis à Londres durant l'hiver 1946-1947[50]. La reconduction l'année suivante des accords anglo-américains antérieurs signifia donc l'abandon par la Grande-Bretagne de cette velléité transitoire d'indépendance.

Politiquement et géographiquement, cet accord de 1948 constituait un élargissement important de l'accord antérieur entre les Britanniques et les Américains. Il était notamment étendu aux services techniques de trois anciens dominions britanniques (Canada[51], Australie puis la Nouvelle-Zélande) dont les positions géographiques devenaient très utiles pour surveiller l'URSS et la Chine.

Techniquement, *UKUSA* n'a pas été non plus un simple accord de coopération technique et d'échanges d'information comme il en existe entre de nombreux services de renseignement. Chacun des partenaires a dû s'engager, en effet, à travailler directement au profit de toute la communauté *UKUSA* et une stricte répartition des tâches a été instaurée à l'échelle mondiale, puisque chacun des cinq pays d'origine a pris en charge d'intercepter le trafic radio et les communications (téléphoniques, télégraphiques – et aujourd'hui informatiques) qui pouvaient transiter par sa zone géographique.

C'est donc, depuis l'origine, une organisation intégrée qui a été mise en place, et non une simple bourse d'échanges entre alliés. Mais, bien que ses textes fondateurs n'aient jamais été rendus publics, on croit savoir qu'*UKUSA* a toujours été un dispositif asymétrique placé sous le

[49] Martin RUDNER, *Canada's Communications Security Establishment : From Cold War to Globalisation*, Occasional Paper, n° 22, Centre for Security and Defence Studies, Carleton University, 2000, Ottawa, p. 16.

[50] R. ALDRICH, *op. cit.*, p. 246. M. Rudner, quant à lui, fait même état d'un accord *Commonwealth Sigint Organization* (*CSO*) qui aurait été signé en 1947 mais dont les objectifs auraient été considérés comme trop ambitieux (Martin RUDNER, « Canada's Communications Security Establishment from Cold War to Globalization », *Intelligence & National Security*, Vol. 16, n° 1).

[51] L'accord bilatéral entre les États-Unis et le Canada qui organise la participation directe à l'alliance *UKUSA* est parfois dénommé *CANUSA* et aurait été conclu sur la base d'un mémorandum en date du 7 juin 1948 (cité par M. AID & C. WIEBES, *op. cit.*, note 7, p. 330) puis confirmé par un échange de lettres entre les services de sécurité respectifs (le *CRC* et l'*US Communications Intelligence Board*) le 29 juin 1949. J. Richelson indique pour sa part une autre date, celle du 15 septembre 1950 (Jeffrey T. RICHELSON, *op. cit.*, p. 273).

contrôle des États-Unis. Selon, en effet, la terminologie utilisée dans les échanges de lettres qui constituèrent l'accord d'origine (et connue indirectement par des documents officiels émanant des gouvernements concernés), les Américains et les Britanniques constituent à eux seuls la première partie (*First Party*) de l'accord[52]. Les autres alliés anglo-saxons n'en sont que les « secondes parties », tandis que les autres États alliés qui ont conclu, depuis lors, de simples accords d'échanges et de coopération avec les membres d'*UKUSA*, ils ont été tous dénommés *Third parties*. Parmi ces membres du troisième cercle, on compte notamment différents pays membres de l'OTAN, comme la Norvège (qui aurait signé le 10 décembre 1954 un accord bilatéral *NORUSA* avec la *NSA*[53]) et très vraisemblablement le Danemark[54], mais aussi la RFA, l'Italie, la Grèce et la Turquie[55]. Mais des accords similaires auraient aussi été conclus dans les années 1960 avec d'autres alliés en Asie, comme la Thaïlande, la Corée du Sud, Taïwan, les Philippines ou le Japon[56].

Or, cette hiérarchie à plusieurs niveaux a une double signification. Elle marque, d'une part, le fait qu'il s'agit bien de l'extension d'un accord bilatéral entre le Royaume-Uni et les États-Unis qui s'est élargi mais dont la polarité par rapport à la période de la Seconde Guerre mondiale s'est inversée : là où les Britanniques – avec Bletchley Park – dominaient, ce sont désormais les Américains – surtout à partir du remplacement de l'*ASA* par la *National Security Agency* (*NSA*) en 1952 – qui mènent le jeu. Les Britanniques demeurent le partenaire privilégié des Américains (pouvant à l'occasion les suppléer temporairement[57]) mais ils ne sont plus que les auxiliaires de la *NSA*. D'autre part, cette classification a introduit des modalités opérationnelles inégalitaires : là où les *thirds parties* ne peuvent qu'échanger des données ou apporter des facilités sans partager les résultats, les cinq membres fondateurs d'*UKUSA* travaillent ensemble et accèdent directement aux interceptions des différentes stations des *second parties*, tandis que, seule, la *NSA* décide uni-

[52] Matthew AID & Cees WIEBES, *op. cit.*, p. 315 ; également, M RUDNER, *op. cit.*, p 574.

[53] Alf R. JACOBSEN, « Scandinavia, *Sigint* and the Cold War », *Intelligence & National Security*, Vol. 16, n° 1, Spring 2004, p. 227.

[54] *Ibid.*, p. 228-229.

[55] Matthew AID & Cees WIEBES, *op. cit.*, p. 316.

[56] *Ibid.*

[57] Dans le rapport annuel de l'*Intelligence and Security Committee* du Parlement britannique pour 1999-2000, il est indiqué concernant le *GCHQ* : « *The quality of intelligence gathered clearly reflects the value of the close cooperation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCH* ».

latéralement d'autoriser les autres membres à accéder à ses propres données de renseignement technique[58].

Cette intégration inégalitaire s'est d'ailleurs traduite par le fait que seuls les Américains ont pu installer directement leurs stations et leurs équipes sur le territoire de leurs partenaires. Ce fut le cas, en particulier, de Menwith Hill (créée en 1956 dans le Yorkshire et où fut installée en 1974 la première grande antenne satellitaire) et de Chicksand au Royaume-Uni, de Bad Aibling (base militaire installée en Allemagne depuis 1947 et confiée à la *NSA* en 1971), de Karamursel en Turquie, de la station satellitaire de Pine Gap en Australie (ouverte par la *CIA* en 1968) ou encore de la station de Misawa (créée au Japon dès l'après-guerre). Inversement, il semble qu'aucune *second parties* n'a eu l'autorisation d'implanter directement ses matériels dans un site de la *NSA* et qu'en particulier, les Américains refusèrent même aux Britanniques d'envisager le rapatriement du centre britannique de Hong Kong sur la base américaine de Guam.

Les révélations progressives

Jusqu'aux débuts des années 1970, cet accord *UKUSA* et les différentes pratiques de décryptement (comme *VENONA*) restèrent, malgré leur importance et leur coût, totalement secrets, du moins pour les opinions publiques. De même, il semble que – tout comme le président Roosevelt s'était vu priver à certaines périodes de l'accès aux décryptements *MAGIC* durant la guerre du Pacifique[59] – le président Truman ne fut jamais réellement mis au courant de l'existence du programme *VENONA*, du fait de la réticence des responsables de l'*AFSA* et du *FBI* en 1949-1950[60].

Mais ce ne fut pas longtemps le cas pour les Soviétiques, principale cible de cette alliance anglo-saxonne, et qui en eurent rapidement vent.

[58] Un mémorandum du président Eisenhower en 1953 aurait notamment prescrit que « les informations secrètes ne sont communiquées aux alliés que si elles profitent à Washington » (..... 86 ?).

[59] Cf. James RUSBRIDGER & Eric NAVE, *Betrayal of Pearl Harbor - How Churchill Lured Roosevelt into WWII*, Simon & Schuster, New York, 1991, traduction française : *Trahison à Pearl Harbour - Comment Churchill a entraîné Roosevelt dans la Seconde Guerre mondiale*, Pygmalion/Gerard Watelet, 1992, p. 131 & 195.

[60] Cf. notamment, Gildas LE VOGUER, « Transparence et secret aux États-Unis : la publication du projet *venona* », *Sources*, printemps 2001, p. 121 (qui y voit un symptôme d'une « culture du secret » dans les États-Unis d'après-guerre) ; également Michael WARNER, « Did Truman Know about Venona ? », *Center for the Study of Intelligence Bulletin*, Summer 2000, n° 11 (cet historien officiel de la *CIA*, n'exclut pas – pour sa part – que la Maison Blanche ait pu, à l'époque, être partiellement mise au courant).

On sait, en effet aujourd'hui que, déjà, durant la guerre, le *NKVD* avait déjà été informé des décryptements réalisés à Bletchley Park par l'intermédiaire de plusieurs de ses agents britanniques, dont John Cairncross (l'un des « cinq de Cambridge » avec Burgess, MacLean, Philby et Blunt, qui fut affecté à Bletchley en 1943) et Leo Long (qui travaillait à la section *MI14* du *War Office*, laquelle était destinataire des décryptements *ENIGMA*)[61].

Mais ce n'est qu'en 1962 que cette évidence fut clairement établie, lorsque le programme *VENONA* lui-même permit le décryptement d'un message soviétique de mai 1941 prouvant que les Soviétiques recevaient depuis Londres des informations militaires provenant de Bletchley (en l'occurrence des informations sur les gares ferroviaires en Ukraine que les Allemands envisageaient d'utiliser lors de leur invasion de l'URSS[62]). Mais bien que les messages soviétiques décryptés faisaient référence à un troisième agent placé au sein de la *GC&CS* et identifié sous le nom de code « Baron », les recherches sont toujours restées vaines pour identifier cette autre source soviétique qui aurait violé le secret d'*Ultra* et des performances de cryptanalyse britanniques[63].

De la même façon, Moscou apprit rapidement le lancement du programme *VENONA* grâce à la trahison de l'un des linguistes de l'*ASA*, William Weisband qui y travailla au contact des équipes *VENONA* et de M. Gardner entre 1944 et 1948. Ensuite l'arrivée de Kim Philby comme représentant du *MI6* britannique à Washington, en 1949, leur offrit à nouveau un poste d'observation idéal pour suivre les progrès des décryptements et des opérations de contre-espionnage qui en découlaient. Ainsi renseigné sur l'efficacité croissante des Américains et de leurs alliés en matière de renseignement technique et de cryptographie, les services de renseignement soviétiques n'eurent de cesse de recruter des taupes et des transfuges dans les rangs des services de renseignement technique anglo-saxons. Cela réussit à plusieurs reprises comme le prouva le spectaculaire passage à l'Est de deux employés de la *NSA*, Martin et Mitchell, en 1960. En juillet 1963, la *NSA* dut faire face au suicide de l'un des sous-officiers, Dunlap, qui avait été découvert en train de vendre des documents aux Soviétiques[64]. Puis au milieu des années 1970, fut découverte la trahison de deux américains, Boyce et Lee, qui avaient accès aux documents classifiés de l'industriel TRW en charge des

[61] Cf. N. WEST, *op. cit.*, p. 37.
[62] *Ibid.*
[63] Cf. notamment, Michael SMITH, « *Enigma* of KGB's Third Man at *Bletchley Park* », *Electronic Telegraph*, 26 June 1997.
[64] Cf. David WISE & Thomas B. ROSS, *The Invisible Government*, trad. française : *Le gouvernement secret des USA*, Fayard, 1965, p. 232-233.

nouveaux projets de satellites-espions de la *CIA* (Rhyolite et Argus). Enfin, les Britanniques arrêtèrent en 1982 l'un des linguistes du *GCHQ*, Geoffrey Prime, qui travaillait pour le *KGB* depuis 1968. C'est d'ailleurs à l'occasion des enquêtes menées à la suite de cette trahison que le gouvernement de Sa Majesté fut – enfin – obligé de révéler officiellement l'existence et les missions du *GCHQ*[65].

Nettement moins bien informé que les services soviétiques, le public occidental attendit pour sa part plusieurs décennies, avant de connaître véritablement l'importance de l'implication des nations anglo-saxonnes dans le renseignement technique et le décryptement durant la Seconde Guerre mondiale et depuis lors. En 1964, David Wise et Thomas Ross mentionnèrent, parmi les premiers, que la *NSA* utilisait 2 000 stations d'interception autour du globe et que : « si la *NSA* lisait les communications les plus secrètes de plus de quarante nations, dont certaines très amies, elle partageait avec elles certains de ses secrets grâce notamment aux rapports qui existaient entre son bureau de liaison avec le Royaume-Uni (*UKLO*) et son homologue anglais, le *GCHQ*[66] ». Mais cette notation succincte passa largement inaperçue. C'est ensuite la publication, en 1973, des souvenirs du général Bertrand, ancien directeur général adjoint du SDECE et responsable de la section cryptographique du SR français au début de la Seconde Guerre mondiale, qui fit connaître au monde l'existence des décryptements *ENIGMA*[67], dont l'histoire fut immédiatement complétée – côté britannique – par l'ouvrage du colonel Winterbotham, officier du *MI6* en charge de la sécurité de la diffusion des données *Ultra* durant la guerre.

Parallèlement, aux États-Unis, les dernières années de la guerre du Vietnam et les remous de l'affaire *Watergate* favorisèrent également les révélations. En août 1972, un ancien analyste de la *NSA* camouflé sous le pseudonyme de Winslow Peck (de son véritable nom, Perry Fellwock) révéla dans le magazine contestataire *Ramparts* l'existence de l'accord *UKUSA* et indiqua notamment que ces capacités d'écoute et de décryptement n'étaient pas uniquement tournées vers les pays socialistes mais aussi utilisées pour suivre les communications d'autres pays occidentaux[68]. Dans cet entretien, le soi-disant W. Peck se montra, pour la première fois, relativement précis sur la nature et la portée des relations

[65] Plus récemment, le *GCHQ* a admis en 2002 que deux autres Britanniques avaient été identifiés comme ayant espionné le projet *VENONA* pour le compte de l'URSS (cf. Lord Chancellor's Advisory Council on Public Records, 7 févier 2002).
[66] D. WISE & Th. B. ROSS, *op. cit.*, p. 232.
[67] Gustave BERTRAND, *op. cit.*
[68] « US Electronic Espionnage : A Memoir », *Remparts*, Vol. 11, n° 2, août 1972, p. 35-50 (reproduit sur : http://jya.com/nsa-elint.htm).

existant entre les États-Unis et ses alliés les plus proches en matière de renseignement technique :

> « [...] The SIGINT community was defined by a TOP SECRET treaty signed in 1947. It was called the UKUSA treaty. The National Security Agency signed for the US and became what's called First Party to the Treaty. Great Britain's GCHQ signed for them, the CBNRC for Canada, and DSD for Australia, New Zealand. They're all called Second parties. In addition, several countries have signed on – ranging from West Germany to Japan – over the years as Third parties. Among the First and Second Parties there is supposed to be a general agreement not to restrict data. Of course it doesn't work out this way in practice. The Third party countries receive absolutely no material from us, while we get anything they have, although generally it's of pretty low quality. We also worked with so-called neutrals who weren't parties to the UKUSA treaty. They'd sell us everything they could collect over radar on their Russian border. »

Il révéla également le nom de plusieurs des sites en Europe sur lesquels avaient été installées des stations d'écoute travaillant pour la *NSA* et ses partenaires (comme Karamursel, Darmstadt en Allemagne, Chicksands au Royaume-Uni, Brindisi en Italie, mais aussi Trabisonde et en Crète).

En 1975, fut aussi révélé devant le congrès et dans la presse que la *NSA* et la *CIA* avaient poursuivi après-guerre la collecte systématique des messages télégraphiques internationaux en provenance ou à destination des États-Unis dans le cadre d'un programme dénommé *Shamrock*[69]. À la même période, de l'autre côté de l'Atlantique, le journaliste écossais Duncan Campbell, ayant rencontré à Londres le pseudo-Winslow Peck, rédigea un premier article en juin 1976 qui décrivait les activités d'interception du *GCHQ* britannique et ses liens avec les Américains[70].

S'agissant de *VENONA*, la première mention (indirecte et sans en fournir le nom) en a été faite, en 1980, dans l'ouvrage du journaliste

[69] Horrock NICHOLAS, « National Security Agency Reported Eavesdropping on Most Private Cables, » The *New York Times*, 8 August 1975, p. 1. Le détail des révélations effectuées devant la Commission Church se trouve dans le 3e volume de son rapport : *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities*, US Senate, 1976, Book III, p. 765-776.

[70] Duncan CAMPBELL et Mark HOSENBALL, « The Eavesdroppers », *Time Out*, Juin 1976. La publication de cet article donna lieu à un procès à l'encontre de ses auteurs pour divulgation d'informations classifiées, qui défraya la chronique sur le nom de l'affaire ABC (sur certains aspects du procès, cf. B. WARUSFEL, *Contre-espionnage et protection du secret – Histoire, droit et organisation de la sécurité nationale en France*, Éditions Lavauzelle, 2000, p. 342).

David Martin consacré au contre-espionnage américain[71], mais elle fut reprise et développée en 1987 dans l'ouvrage de mémoires non autorisé de Peter Wright, ancien cadre supérieur du *MI5*[72].

Plus généralement, une étape importante fut franchie avec, en 1982, le livre de James Bamford – *The Puzzle Palace* – entièrement consacré à la *NSA*[73]. Cet ouvrage ne se contentait pas d'indiquer l'existence de la coopération entre agences *UKUSA*, il expliquait également que la *NSA* et ses alliés venaient d'engager un programme d'informatisation et d'interconnexion mondiale des moyens d'interception afin de pouvoir traiter plus vite les volumes de données collectées, notamment par la détection automatique de mots-clés[74]. Ce programme alors identifié sous le nom de code de *Plateform* par Bamford devait se révéler être – une fois mis en œuvre – le fameux programme *ÉCHELON* (dont le nom fut mentionné pour la première fois dans un autre article de Duncan Campbell en 1988[75]).

S'il fallut attendre encore juillet 1995 pour que la *NSA* et les autres services de renseignement américains reconnaissent officiellement l'existence de *VENONA* et décident la déclassification des déchiffrements, on peut donc considérer qu'à la chute du mur de Berlin, les principales révélations concernant l'histoire secrète de la coopération anglo-saxonne en matière de renseignement électromagnétique avaient été déjà rendues publiques. Mais c'est pourtant près de dix années plus tard que l'opinion publique mondiale s'empara du sujet en focalisant d'ailleurs son attention sur le soi-disant « réseau *ÉCHELON* », qui n'est en fait que l'ensemble des stations d'interception travaillant dans le cadre d'*UKUSA*.

ÉCHELON : une polémique emblématique de l'après-guerre froide

En demandant notamment au journaliste Duncan Campbell de rédiger, en 1999, un rapport sur l'état des techniques de renseignement électronique, le service d'études du parlement européen, le *STOA* permit de faire connaître à l'opinion publique et aux autorités européennes l'état des connaissances accumulées depuis une dizaine d'années par une poignée de chercheurs et de journalistes qui s'étaient intéressés – depuis

[71] cf. D. MARTIN, *op. cit.*, p. 64-70.

[72] P. WRIGHT, tr. française, p. 117.

[73] James BAMFORD, *Puzzle Palace...*, *op. cit.*, p. 397.

[74] *Ibid.*, p. 418.

[75] « They've got it taped », *New Stateman*, 12 août 1988, p. 10-12 (http ://jya.com/echelon-dc.htm).

les premières révélations de Winslow Peck – à la pratique du renseignement électronique anglo-saxon.

Le rapport Campbell fut rendu public en avril 1999[76]. Il était accompagné de trois autres rapports consacrés aux aspects cryptographiques, juridiques et économiques du sujet[77]. L'effet indirect de ces documents fut d'obliger plusieurs gouvernements membres d'*UKUSA* à reconnaître semi-officiellement l'appartenance de leurs pays à cet accord. Ce fut le cas, en particulier, en Australie où, en mars 1999, le directeur du service de renseignement électronique australien (*DSD*) en personne reconnut finalement, lors d'une émission télévisée, que son service « coopère avec des services de renseignement électronique homologues étrangers dans le cadre des relations *UKUSA*[78] ». Dans ce pays, pourtant signataire de l'accord *UKUSA* dès l'origine, le secret avait été effectivement bien gardé (à tel point qu'il semble qu'aucun premier ministre australien n'avait été informé de l'accord avant 1973). De même, ce n'était que trois ans auparavant (en 1996) que la *NSA* américaine avait accepté de déclassifier et de rendre public les documents *VENONA* relatifs à l'espionnage soviétique à Canberra durant la dernière guerre[79].

Les débats furent également vifs au Canada et en Nouvelle-Zélande, deux autres membres d'*UKUSA*. Au Canada, le rapport Campbell avait été précédé par un ouvrage publié en 1995 par un ancien membre du renseignement électronique canadien, Mike Frost, qui révélait notamment comment le Canada participait à l'alliance *UKUSA* et comment les ambassades canadiennes dans des pays étrangers servaient de stations d'écoute[80]. Aujourd'hui, les autorités canadiennes reconnaissent quasi-officiellement (bien qu'à demi-mots) l'existence des accords

[76] Duncan CAMPBELL, *The state of art in communications intelligence (Comint) of automated processing for inteligence purposes of intercepting broadband multi-language leased or common carrier system, and its applicability to comint targeting and selection, including speech recognition* (Stoa PE 168.184/part4/4 avril 1999).

[77] Franck LEPRÉVOST, *Chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie* (Stoa PE168.184/part 3/4 : avril 1999) ; Dr. Chris ELLIOT, *The legality of the interception of electronic communications : a concise survey of principal legal issues and instruments under international, european and national law* (Stoa PE 168.184/part2/4 : avril 1999) ; Nikos BOGOLIKOS (dir.), *The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception* (Stoa PE 168.184/int.st/part1/4 : mai 1999).

[78] Martin Brady, Director of DSD, 16 March 1999. Broadcast on the Sunday Programme, Channel 9 TV (Australia), 11 April 1999.

[79] Cf. Frank CAIN, « Venona in Australia and its Long-term Ramifications », *Journal of Contemporary History*, Vol. 35, n° 2, 2000, p. 231-248.

[80] Mike FROST and Michel GRATON, *Spyworld : How CSE Spies on Canadians and the World*, Seal/McClelland-Bantam, Toronto, 1995.

UKUSA[81]. En Nouvelle-Zélande, ce fut l'ouvrage de Nick Hager, *Secret Power* publié en 1996 qui avait lancé le débat[82]. Il étudiait de façon détaillée des activités de renseignement électronique du service néo-zélandais, le *GCSB* (le *Government Communications Security Bureau*, dont il révélait notamment que l'un des principaux directeurs avait été entre 1984 et 1987 un officier américain de la *NSA*) et décrivait l'intégration dans le réseau d'interception piloté par la *NSA* des deux stations d'écoute néo-zélandaises de *Tangimoana* (spécialisée dans les interceptions radio) et de *Waihopai* (spécialisée dans les interceptions des satellites *Intelsat* au-dessus du Pacifique). Et dans son introduction, l'ancien premier ministre néo-zélandais David Lange reconnaissait que, quand il avait pris la décision de créer la station de Waihopai (ouverte en 1989), il n'avait pas été informé par ses propres services de sécurité du fait qu'elle serait reliée au réseau mondial de la *NSA*[83].

De son côté, au Royaume-Uni, le gouvernement adopta une politique de *no comment* classique : répondant à un député des communes, en 1996, à propos des activités de la *NSA* à la base de Menwith Hill, le représentant du gouvernement répondit : « *Il n'entre pas dans la politique du gouvernement de commenter les opérations détaillées menées à Menwith Hill. En tout cas, aucune activité considérée comme hostile aux intérêts britanniques n'est, ou ne serait, permise dans cette station*[84]. » Et après la publication des rapports de *STOA*, le *Foreign Office* britannique se contenta d'indiquer en février 2000 que les services de renseignement britanniques travaillaient exclusivement dans le cadre de la loi et que celle-ci n'autorisait les interceptions que pour la protection de la sécurité nationale ou dans les intérêts de la « sécurité économique » britannique et excluait toute collecte massive et non discriminée d'informations[85]. Quant au gouvernement allemand – bien que son pays soit un partenaire de second rang d'*UKUSA* – il est resté très évasif face aux questions du *Bundestag* sur ce sujet, se contentant d'indiquer « qu'il avait pris

[81] Ainsi, le rapport annuel du commissaire du centre de la sécurité des télécommunications pour 2000-2001, indique : « Le Canada profite d'arrangements de longue date conclus entre le CST et ses homologues des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande. Ces arrangements, qui ont été officialisés après la Deuxième Guerre mondiale et maintenus durant la guerre froide, permettent l'échange de renseignements électromagnétiques, de technologies et d'information au sujet de sources et de techniques d'intérêt commun. »

[82] Nicky HAGER, *Secret Power*, Craig Potton Publishing, 1996.

[83] We even went the length of building a satellite station at Waihopai. But it was not until I read this book that I had any idea that we had been committed to an international integrated electronic network (David Lange in N. HAGER, *op. cit.*, p. 9).

[84] Chambre des Communes, 3 juin 1996, réponse à Lord Jenkins of Putney.

[85] Guardian Unlimited, 24 février 2000.

connaissance des rapports du Parlement européen mais qu'il ne disposait pas d'informations sur l'état actuel de la coopération entre membres du pacte *UKUSA* ou sur les risques qu'*ÉCHELON* pourrait représenter pour la vie privée des citoyens ou la compétitivité de l'économie allemande[86] ».

Mais les réactions des pays européens qui ne sont ni membres ni partenaires de l'alliance *UKUSA* furent elles aussi embarrassées. Ainsi, en Belgique, un premier rapport d'août 1999 établi par le comité parlementaire de contrôle des services de renseignement (le « Comité R ») a conclu que « les services de renseignements belges n'ont pas la possibilité technique de constater eux-mêmes l'existence du système *ÉCHELON*. Leur connaissance du sujet résulte de la consultation de sources ouvertes » et que si « la sûreté de l'État [le service de sécurité et de contre-espionnage] n'a pas été en mesure de confirmer l'existence de pratiques d'interception de télécommunications », le service général de renseignement et de sécurité (SGR, service de renseignement extérieur) « considère quant à lui l'existence d'un système d'interception de type *ÉCHELON* comme un fait acquis ». Ce n'est que dans un second rapport rédigé en février 2002 par une commission mixte issue des deux chambres du parlement[87] que fut officiellement admise l'existence d'un « système d'interception global, à l'échelle mondiale, qui intercepte les communications par satellite (*COMINT*) », et qui « s'inscrit dans le cadre de la collaboration en matière de *SIGINT* qui unit les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande après la Deuxième Guerre mondiale (pacte *UKUSA*) ». Mais le rapport souligne également que « plusieurs pays membres de l'union européenne disposent de systèmes d'interception globaux similaires, même s'ils n'ont pas tous une capacité comparable à celle d'*ÉCHELON* », tandis qu'il reconnaît que « la Belgique ne dispose pas d'un système équivalent et ne collabore pas à un système d'écoute mis au point par un ou plusieurs pays alliés ». Par ailleurs, ce rapport conclut que si « ces systèmes d'interception globaux servent entre autres à la lutte contre le terrorisme international et contre la criminalité internationale », ils peuvent aussi servir « à des fins d'espionnage économique » et que « ces systèmes, qui travaillent à l'insu des pays qui en sont la cible, constituent indiscutablement des atteintes à la souveraineté de l'État et qu'à ce titre, ils sont contraires au

[86] Cité in : Assemblée nationale, rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, par M. Arthur Paecht, document n° 2623, 11 octobre 2000.

[87] Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé « Échelon », rapport du sénat (n° 2-754/1) et de la chambre des représentants de Belgique (1660/001) – Session 2001-2002, 25 février 2002.

droit international et, plus particulièrement entre États membres de l'union européenne, au droit communautaire ».

Ces réactions belges (en provenance d'un pays, par ailleurs membre de l'OTAN) sont révélatrices de plusieurs caractéristiques de ce dossier très sensible du renseignement électronique contemporain. D'une part, l'alliance *UKUSA* est un pacte ultra-secret dont la réalité profonde n'est accessible qu'à ses membres fondateurs et dont sont tenus à l'écart certains autres alliés politiques ou militaires. D'autre part, depuis la fin du conflit Est-Ouest, les soupçons de détournement de ces moyens à des fins de renseignement économique sont permanents. Enfin, les réactions des différents pays européens sont d'autant plus embarrassées que d'autres États développent leurs propres moyens d'interception électronique et satellitaire. C'est paradoxalement le cas de l'Allemagne qui – tout en accueillant sur son sol des bases *UKUSA* et en assumant son statut de *third party*, a entrepris de participer avec la France à l'exploitation de plusieurs stations d'interception communes (notamment celles de Kourou en Guyane et de Mayotte, mises en œuvre par la DGSE et le *BND* allemand). Mais c'est surtout le cas de la France, qui en dehors d'*UKUSA* (même si des échanges *TOTEM* doivent se produire bilatéralement entre services) a développé fortement les moyens de la direction technique de la Direction générale de la sécurité extérieure (DGSE) afin de disposer (grâce notamment à des implantations outre-mer) d'un ensemble de stations d'interception lui donnant une capacité réelle et globale, bien que très inférieure à celle de l'alliance *UKUSA*[88]. Cet état de fait a été admis par le rapport de l'assemblée nationale française, qui tout en reconnaissant l'existence de ces moyens, indiquait qu'ils « sont géographiquement orientés et limités et ne peuvent en aucune façon être comparés au réseau *ÉCHELON*. On ne saurait donc parler de *Frenchelon*[89] ». Mais ce même rapport ajoutait également que, parmi les raisons qui peuvent expliquer la « position réticente » de certains services de renseignement sur le dossier *ÉCHELON*, on peut noter « l'existence d'écoutes réalisées par les ser-

[88] « Le renseignement par moyens techniques. Cette technique est désormais maîtrisée par certains pays dont la France. L'entrée dans une ère informationnelle rend obligatoire de tels outils, notamment depuis l'accroissement des communications transitant dans l'atmosphère. Faisceaux satellites, téléphonie mobile : bien qu'invisibles, ces signaux électromagnétiques circulant dans l'espace peuvent être interceptés. » (« L'art du renseignement : analyse et combinaison de moyens », *Armées d'aujourd'hui*, n° 276, décembre 2002-janvier 2003). Cf. également l'article de Vincent JAUVERT, *Nouvel Observateur*, 5 avril 2001 (qui donne la liste officieuse des principales stations d'interception françaises).

[89] Assemblée nationale, *Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale*, par M. Arthur Paecht, document n° 2623, 11 octobre 2000, p. 38.

vices nationaux de certains États, même si celles-ci n'ont ni la vocation ni l'ampleur du système *ÉCHELON*[90] ».

Toutes ces ambiguïtés se retrouvent dans les recommandations contenues dans le rapport du 11 février 2001 présenté au parlement européen par Gerhard Schmid. D'un côté, il est demandé aux autorités britanniques de « faire la lumière sur leur rôle dans l'alliance *UKUSA*, étant donné que sont établies l'existence d'un système de type *Échelon* et son utilisation aux fins de collecte de renseignements économiques », mais il se contente de proposer, par ailleurs, que les États membres et le gouvernement américain soient « invités à nouer un dialogue franc sur la collecte de renseignements économiques ». Et, par ailleurs, « les États membres sont invités à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du parlement européen, du conseil et de la commission[91] ».

Pris entre les exigences de sécurité nationale et internationale (notamment depuis les attentats du 11 septembre 2001) et les inquiétudes concernant le détournement possible des moyens d'interception à des fins politiques ou économiques, les Européens sont plus particulièrement mal à l'aise sur le sujet, dès lors que certains d'entre eux (comme la France et l'Allemagne) développent leurs moyens autonomes et que – surtout – le Royaume-Uni continue de jouer un rôle central et mal connu dans le système *UKUSA* lui-même. Ce que l'on sait aujourd'hui de l'histoire d'*UKUSA* et des décryptements *VENONA* montre bien, en effet, que le Royaume-Uni est plus qu'un simple partenaire technique de cette alliance secrète et qu'il en constitue à la fois le berceau historique ancien et un pilier actuel majeur (notamment au travers de son agence spécialisée, le *GCHQ* qui travaille de manière fort intégrée avec la *NSA* dans tous ces domaines, et qui a reconnu officiellement avoir la paternité cachée de la cryptologie à clé publique, l'une des découvertes cryptologiques les plus fondamentales du XX[e] siècle[92]). Et dès lors que, dans le

[90] *Ibid.*, p. 36.

[91] Parlement européen, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques* [*système d'interception ÉCHELON*, 2001/2098(INI), recommandations n° 16, 15 et 12].

[92] Cette révélation faite dans l'ouvrage de Simon Singh (*Histoire des codes secrets*, traduction française, Lattès, 1999) a été officiellement confirmée (bien qu'elle soit parfois discutée par ailleurs) par la déclassification par le *GCHQ* de plusieurs documents internes rédigés à la fin des années 1960 par le mathématicien britannique du *GCHQ* Ellis (accessibles sur le site www.gchq.gov.uk).

monde dérégulé de l'après-guerre froide, l'union européenne veut s'imaginer comme un contrepoids politique et économique à la superpuissance américaine, il est évident que la clarification du rôle britannique dans la gestion d'un tel instrument de savoir et de pouvoir ne sera pas sans conséquence politique.

Que l'on regarde donc l'un ou l'autre des aspects de la coopération *UK-USA* en matière de renseignement technique, on débouche sur des enjeux politiques et stratégiques majeurs. S'agissant de *VENONA*, on s'aperçoit aujourd'hui que ce travail rétrospectif (puisque mené sur des messages contemporains de la Seconde Guerre mondiale) est sans doute d'une réelle importance pour la compréhension de certains dossiers les plus importants de la guerre froide. Mais lorsque l'on s'intéresse aux interceptions dans le cadre du programme *ÉCHELON*, se posent de nouvelles questions, notamment sur la conciliation entre la nécessaire coopération politique et militaire contre certaines menaces (terrorisme, prolifération,...) et l'exacerbation de la concurrence géo-économique. *UKUSA* doit donc rester un sujet d'intérêt et d'étude pour les historiens, non seulement pour ce qu'il révèle des mutations du renseignement depuis soixante ans mais aussi parce que cet accord secret est fortement lié à l'histoire politique et militaire du dernier siècle et de celui qui commence.