CH_VB 2003-2615 1377 vom 10. November 2003

Bundesverwaltung, 2003-11-10, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/ch_vb_2003-2615_1377_

FR: CH_VB 2003-2615 1377 du 10 novembre 2003

IT: CH_VB 2003-2615 1377 del 10 novembre 2003

Erwägungen

E. 1

Introduction A l'instar de plusieurs Etats, le Conseil fédéral a décidé en 1997 de développer un projet d'interception des communications par satellite. Ce système, appelé Onyx (anciennement SATOS-3), permet de capter les communications internationales civiles et militaires qui transitent par satellite. Il fournit aux autorités supérieures de la Confédération des informations importantes pour l'appréciation et la prise de décision en matière de politique de sécurité. L'activité d'Onyx est fondée principa- lement sur l'art. 99 de la loi fédérale du 3 février 1995 sur l'armée et l'admini- stration militaire (LAAM; RS 510.10) qui fixe les missions du service de rensei- gnement extérieur de la Confédération. Onyx est entré en service en avril 2000 et fonctionne actuellement de manière expé- rimentale. Il entrera en phase opérationnelle dans le courant l'année 2004 et sera en exploitation complète fin 2005/début 2006. Le système Onyx offre aujourd'hui déjà de nombreuses fonctions et possibilités de collecte d'informations au Service de renseignement stratégique (SRS) du Dépar- tement de la défense, de la protection de la population et des sports (DDPS) qui est son principal utilisateur. Il sert également, dans une moindre mesure, au Service d'analyse et de prévention (SAP) du Département fédéral de justice et police (DFJP). Onyx permet une surveillance de masse des communications. Il facilite et multiplie les capacités des services de renseignement de collecter des informations utiles, par exemple dans la lutte contre la prolifération d'armes de destruction massive (ADM) ou contre le terrorisme international. Le système n'a pas que des avantages. Il peut aussi présenter, s'il n'est pas stricte- ment encadré sur les plans juridique et politique, des risques importants pour les droits fondamentaux, notamment pour le droit à la protection de la sphère privée et au respect du secret des télécommunications. Ce droit est garanti par l'art. 13 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.; RS 101). En droit international, la sphère privée est protégée par l'art. 8 de la Convention euro- péenne des droits de l'homme du 4 novembre 1950 (CEDH; RS 0.101) et par l'art. 17 du Pacte international relatif aux droits civils et politiques du 16 décembre 1966 (Pacte ONU II; RS 0.103.2). Depuis l'affaire des fiches dans les années 90, on sait le Parlement très sensible aux dangers que représentent les mesures étatiques de surveillance pour les droits fon- damentaux. Les interceptions, par leur caractère secret, suscitent des craintes et sou- lèvent des objections légitimes. C'est pourquoi la Délégation des commissions de gestion (DCG) a suivi étroitement la réalisation du projet Onyx dès son début. Il s'agissait en l'occurrence d'examiner si le système respecte, tant par sa structure que dans son exploitation, l'ordre juridi- que suisse ainsi que les droits fondamentaux. La délégation a aussi veillé à ce que les points les plus critiques du projet soient corrigés au fur et à mesure avant que le système n'entre en phase opérationnelle.

1379 Le présent rapport décrit les différents constats faits par la délégation ainsi que les mesures prises par le DDPS et le Conseil fédéral. Il expose aussi l'appréciation générale de la délégation et propose diverses recommandations. Le rapport rend compte de l'état de la situation à fin octobre 2003.

E. 2

Méthode de travail

E. 2.1

Mandat général de la Délégation des commissions de gestion La DCG exerce, sur mandat des Chambres fédérales, la haute surveillance sur les activités de la Confédération dans le domaine de la sécurité de l'Etat et du rensei- gnement (art. 47quinquies, al. 2, LREC; RS 171.11). Par «sécurité de l'Etat», il faut comprendre toutes les activités de la Confédération qui ont un caractère répressif ou préventif et qui concourent à garantir la «sûreté intérieure» de la Suisse. Il s'agit en particulier de la lutte contre le terrorisme, contre les groupes extrémistes ayant recours à la violence, contre le crime organisé, contre l'espionnage et contre la prolifération des ADM. Le terme de «renseignement» recouvre toutes les activités qui permettent à la Confédération de collecter et d'exploiter des informations sur l'étranger et qui visent à garantir la «sûreté extérieure» de la Suisse. La haute surveillance s'exerce principalement sous l'angle des principes de légalité, d'opportunité et d'efficacité. La DCG examine les activités secrètes de la Confédération de manière continue et approfondie afin de repérer à temps les points justifiant une intervention politique. Ce faisant, la DCG accorde une grande importance à la détection précoce des pro- blèmes et contribue à corriger les insuffisances et dysfonctionnements constatés. Pour exercer sa tâche, la DCG dispose, en vertu de la constitution et de la loi, de droits d'information particulièrement étendus. Ni le secret de fonction, ni le secret militaire ne peuvent lui être opposés (art. 169, al. 2, Cst.).

E. 2.2

Définition de l'objet et des limites de l'inspection La réalisation du projet Onyx pose toute une série de questions: Qui écoute-t-on? Dans quels buts? Sur quels domaines? Qui confie les mandats d'exploration et selon quelles procédures? Qui contrôle les interceptions? Qui les archive? Qui a accès aux documents? Qui les utilise? Que fait-on des informations recueillies de manière fortuite? S'agit-il d'une activité exclusivement nationale ou participe-t-elle d'un accord international? etc. Ces questions soulèvent des problèmes importants d'ordre juridique, mais aussi politique. La délégation s'est donnée le mandat suivant: – examiner et commenter le système d'interception Onyx, – décrire les processus d'attribution des mandats d'exploration et de collecte d'informations,

1380 – apprécier l'environnement juridique en la matière, tant sur le plan national qu'international, – situer le projet Onyx dans le contexte international, – évaluer les systèmes de contrôle mis en place, – formuler le cas échéant des recommandations politiques et législatives. La délégation a décidé de concentrer son analyse, dans un premier temps, sur la légalité des interceptions. Lors d'une prochaine inspection, elle examinera égale- ment l'efficacité du système, sa fiabilité ainsi que son rendement. Il convient de relever ici que le système Onyx couvre uniquement les interceptions administratives à des fins de renseignement. Il ne concerne pas les mesures de surveillance téléphonique réalisées dans le cadre de procédures pénales, fédérales et cantonales ou de procédures d'entraide judiciaire internationale en matière pénale. Ces mesures sont réalisées dans un cadre

juridique précis fixé par la loi fédérale du

E. 2.3

Démarche La DCG s'est intéressée à la mise en oeuvre du projet Onyx dès janvier 1999. Entre cette date et jusqu'à fin octobre 2003, elle y a consacré 17 réunions au cours desquelles elle a entendu les personnes1 et services suivants, dont certains à plusieurs reprises: – le chef du DDPS (12.11.99, 14.3.2001, 18.9.2001, 12.11.2001, 19.5.2003); – le rapporteur du chef du DDPS pour les questions spéciales (15.9.2000, 5.7.2002); – le coordinateur des renseignements et/ou son remplaçant (26.3.2001, 12.11.2001, 5.7.2002, 28.1.2003, 19.5.2003); – le chef de l'Etat-major général (15.9.2000, 19.5.2003); – le chef de l'inspectorat du DDPS et un expert (8.2.2002); – des représentants du Groupe d'état-major de l'aide au commandement et en particulier de la Division de la conduite de la guerre électronique (CGE) (26.3.2001, 28/29.5.2001, 12.11.2001, 8.2.2002, 5.7.2002, 28.1.2003, 19.5.2003);

1 Voir la liste des personnes entendues à l'annexe 2.

1381 – le sous-chef d'état-major des renseignements (28.1.1999) et son remplaçant (15.9.2000); – des représentants du SRS (29./30.1.2001, 26.3.2001, 12.11.2001, 8.2.2002, 5.7.2002, 7.10.2002); – des représentants du service de l'Inspectorat et des tâches spéciales du Se- crétariat général du DFJP (28./29.5.2001); – des représentants de l'Office fédéral de la police et du SAP (4.7.2001, 12.11.2001, 22.11.2001, 22.1.2002, 5.7.2002, 19.5.2003); – un représentant du Secrétariat d'Etat à l'économie (commerce mondial, 5.7.2002). La délégation a procédé également à deux visites des infrastructures d'engagement d'Onyx, dont une visite inopinée. A cette occasion, elle a discuté avec les responsa- bles d'un très grand nombre de questions touchant au fonctionnement, à la sécurité, au financement et aux mandats donnés à Onyx ainsi qu'aux relations entre le DDPS et Swisscom. La délégation s'est également rendue au siège du SRS pour y ren- contrer les collaborateurs chargés de l'élaboration des ordres d'exploration. La délégation a eu également plusieurs échanges de correspondance avec le Conseil fédéral, la Délégation du Conseil fédéral pour la sécurité, le chef du DDPS ainsi que la cheffe du DFJP. Les thèmes suivants ont été évoqués dans ces courriers: missions et légalité de l'exploration électronique, contrôle des mandats d'interception, traite- ment et protection des données personnelles, collaboration avec l'étranger, surveil- lance politique des interceptions par le Conseil fédéral et les départements concernés (DDPS, DFJP). La DCG a traité plusieurs rapports, dont un rapport de l'inspectorat du DDPS, daté du 9 mai 2001, consacré à une inspection effectuée auprès de la CGE. Elle a égale- ment examiné un rapport de révision du Contrôle fédéral des finances (CDF) sur le financement du projet, daté du 15 août 2003. La délégation a également interrogé les services du SRS et du Contrôle fédéral des finances sur certains aspects liés à l'utilisation des crédits de financement d'Onyx. La délégation a également pris con- naissance des différentes interventions parlementaires touchant aux interceptions de communications2.

2 98.5085 Question. Espionnage informatique à grande échelle par Echelon, du 15.6.1998 (BO 1998 N 1162); 99.3416 Interpellation. Surveillance électronique mandatée par le Groupe des renseignements, du 31.8.1999 (BO 2000 N 736); 00.3629 Interpellation. Antennes satellite de Loèche, du 28.11.2000 (BO 2001 N 365); 00.5144 Heure des questions. Satos 3. Contrôle du Parlement, du 25 septembre 2000 (BO 2000 N 958); 01.3189 Postulat. Satos 3. Vente par Swisscom du terrain de Loèche, du 23.3.2001 (classé sans

traitement après deux ans); 01.3601 Interpellation. Sécurité des données. Etat des lieux, du 5.10.2001 (BO 2002 N 467); 01.5095 Heure des questions. Système d'interception Echelon, du 18.6.2001 (BO 2001 N 757); 03.1046 Question ordinaire. Espionnage éco- nomique sur le territoire suisse au profit des Etats-Unis, du 8.5.2003 (BO 2003 N 1758).

1382 Dans ses réflexions, la DCG a profité des travaux effectués par d'autres parlements européens. La délégation a notamment étudié différents rapports établis par les par- lements français, européen et belge3 sur les réseaux de surveillance et d'interception électronique. Ces rapports concernent surtout le réseau Echelon qui est un réseau de surveillance mondial des télécommunications conçu et coordonné par l'Agence nationale de sécurité américaine (National Security Agency, NSA). La délégation a également reçu deux rapports sur le système Echelon: le premier a été élaboré par le SAP en février 2000 et le second par les services du coordinateur des renseigne- ments en février 2001. Les travaux de la délégation ont été coordonnés avec ceux de la Commission de la politique de sécurité du Conseil national (CPS-N) qui s'est également intéressée au dispositif Onyx. Aux termes d'un accord conclu entre la délégation et la CPS-N, il a été convenu que la délégation s'occuperait de la surveillance du système Onyx, la CPS-N n'étant pas habilitée à intervenir dans les domaines secrets de la Confédéra- tion4. La délégation a régulièrement informé les Commissions de gestion (CdG) sur l'état d'avancement des travaux. Elle a également publié deux communiqués de presse, le 19 septembre 2000 et le 27 mars 2001, et a décrit ses activités dans les rapports annuels des CdG5. Sur la base des renseignements obtenus lors de ses travaux, la délégation a élaboré un projet de rapport dont elle a transmis les conclusions provisoires au Conseil fédéral le 16 octobre 2003. Ce dernier a pris position dans un avis daté du 29 octobre 2003. Le rapport final tient compte des observations du Conseil fédéral. La délégation a présenté son rapport final aux Commissions de gestion le 21 novem- bre 2003. Les CdG ont décidé à l'unanimité de le publier. La DCG tient à relever ici qu'elle a pu mener ses travaux en toute indépendance et qu'elle n'a subi aucune entrave dans ses activités. Elle a eu accès à toutes les infor- mations nécessaires à sa tâche. La délégation tient ici à remercier tous les services concernés pour leur collaboration positive et constructive.

3 Rapport de la Commission de la défense nationale et des forces armées de l'Assemblée nationale française sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, du 11.10.2000 (rapport d'information de M. Arthur Paecht)(ci-après: rapport français); rapport de la Commission temporaire du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)(2001/2098(INI)), du 11.7.2001 (ci-après: rapport européen); rapport de la Commission chargée du suivi du comité permanent de contrôle des services de renseignements et de sécurité et de la Commission spéciale chargée de l'accompagnement parlementaire du comité permanent de contrôles des services de police du Sénat et de la Chambre des représentants de Belgique consacré à l'existence éventuelle d'un réseau d'interception des communications, nommé «ECHELON», du 25.2.2002 (ci-après: rapport belge). 4 Voir communiqué de presse de la CPS-N, du 10.4.2001. 5 Voir le rapport annuel 2000/2001 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, du 22.5.2001 (FF 2001 5332) ainsi que le rapport annuel 2001/2002 des Commissions de gestion et de la Délégation des Com- missions de gestion des Chambres fédérales, du 17.5.2002 (FF 2002 5521).

1383

E. 2.4

Maintien du secret La délégation a pour principe d'informer avec le maximum de transparence et de publier les résultats de ses travaux. Pour atteindre cet objectif, la délégation doit parfois renoncer à donner des précisions sur certaines questions qui sont couvertes par le secret. Pour gagner la confiance du Parlement, la délégation doit en dire assez; pour gagner la confiance des services surveillés, elle doit se montrer réservée. La délégation travaille aux frontières de la transparence et du secret et doit veiller à ce que soit rendu à l'une et à l'autre ce qui leur revient. Comme cela a été dit plus haut, la délégation a eu accès à toutes les informations utiles à l'exercice de son mandat de contrôle sur Onyx. Certaines informations sont classifiées et ne peuvent pas être publiées. Dans l'élaboration du présent rapport, la délégation a donc dû faire une pesée d'intérêts entre l'obligation qui lui est faite d'informer le Parlement et l'opinion publique de manière aussi complète que pos- sible et le maintien du secret nécessaire au fonctionnement de certains services de l'Etat. La DCG a décidé de ne pas donner dans son rapport d'indications détaillées sur les capacités, les coûts et les performances du système Onyx. Elle estime en effet que la publication de ces informations ne s'impose pas et qu'elle n'est ni utile, ni néces- saire à la compréhension du sujet. La délégation est aussi d'avis que la divulgation de telles informations pourrait porter atteinte aux relations extérieures de la Suisse et mettre en péril l'application de mesures destinées à protéger la sécurité intérieure et extérieure du pays. Il s'agit aussi, dans certains cas, de protéger la sphère privée de tiers. Pour la délégation, il est important de ne pas confondre confidentialité et loi du silence. En se montrant discrète sur certaines questions, la DCG ne vise pas à cou- vrir des activités critiquables ou des actions illégales, mais à protéger les moyens, les sources et les procédures de collecte d'informations de la Confédération. En se limitant à maintenir secrètes les informations dont la communication pourrait porter atteinte à des intérêts publics ou privés prépondérants, la délégation veut également faire apparaître plus clairement l'importance du secret lorsqu'il est jugé nécessaire. La délégation est consciente que cette restriction n'est pas entièrement satisfaisante, mais c'est à ce prix que le présent rapport peut être publié. 3 Généralités et situation à l'étranger 3.1 Définitions Tous les Etats du monde sont dotés d'agences de renseignement plus ou moins développées dans la collecte et l'analyse d'informations destinées aux organes de décision militaires et politiques. Le renseignement peut poursuivre plusieurs objectifs. A l'origine, il servait essen- tiellement à recueillir des informations de nature militaire ou diplomatique. Par la suite, avec l'accroissement des échanges, l'intérêt s'est élargi à d'autres types d'informations touchant à la sécurité (terrorisme, crime organisé, prolifération, etc.), mais aussi, dans certains cas, à la technologie, aux sciences et au commerce.

1384 Les services de renseignement – la Suisse ne fait pas exception – utilisent plusieurs formes de collecte d'informations qui se complètent mutuellement. Les principales sources d'informations sont6: – l'exploitation des sources ouvertes (open source intelligence, OSINT) telles que les banques de données, les publications scientifiques, la littérature spé- cialisée, Internet, etc.; – la recherche d'informations d'origine humaine (human intelligence, HUMINT) communiquées par des attachés de défense et des agents (infor- mateurs, espions, agents sous couverture, etc.); – l'échange d'informations avec d'autres services partenaires ainsi qu'avec des sources tierces; – l'exploration des signaux ou renseignement électronique (signals intelli- gence, SIGINT). Cette technique permet la

collecte d’informations issues de l’écoute de systèmes de transmission ou de l’interception d’autres émissions électromagnétiques. Le renseignement électronique se décompose en deux grandes catégories: – l’exploration radio ou renseignement électronique discursif (communica- tions intelligence, COMINT); – l’exploration électronique ou renseignement électronique non discursif (elec- tronic intelligence, ELINT). En d’autres termes, le COMINT s’occupe de l’interception, de l’exploitation et de la transmission des émissions radio pouvant être traduites en langage humain (tels le morse ou les communications radio) ou sous forme de graphiques. ELINT concentre sa recherche sur les signaux électroniques ne servant pas aux communications et qui sont émis par les radars et autres systèmes d’armes ainsi que sur l’analyse de leurs paramètres techniques (fréquence, modulation, polarisation, etc.)7. Le système Onyx est une source d’informations de type COMINT. 3.2 Bref aperçu des systèmes d’interception existant dans d’autres pays Plusieurs Etats ont développé ces dernières années des systèmes d’interception des communications. La plupart du temps, ces systèmes sont à vocation opérationnelle militaire. Rares sont en effet les Etats qui disposent de systèmes stratégiques permet- tant l’interception à large échelle de communications militaires, diplomatiques, commerciales ou privées. Selon certaines sources, une trentaine d’Etats posséde- raient une capacité d’interception importante8.

E. 6

Voir la brochure éditée par le DDPS et le DFJP: «Die Nachrichtendienste der Schweiz», 1re édition, 2003, p. 14 ss.

E. 7

Voir la documentation élaborée par l’armée suisse: «Le combat moderne en Europe», documentation 52.15 f, valable dès le 1er juillet 1999, p. 99 ss.

E. 8

Rapport belge, p. 17; rapport de l’Office fédéral de la police, février 2000, p. 1 (non publié).

1385 Aucune donnée précise n’existe en la matière; souvent, on en est réduit à des conjec- tures et il est difficile d’affirmer quoi que ce soit avec certitude. Pour des raisons évidentes, les informations sur ces systèmes sont le plus souvent tenues secrètes par les autorités des pays concernés. Quant aux sources d’informations ouvertes, elles ne sont pas toujours fiables et elles se contredisent parfois. Les faits avérés se confon- dent aussi souvent avec des informations non vérifiées, voire fantaisistes. En l’occurrence, la délégation s’est fondée sur un nombre limité de sources ouvertes, et notamment sur les rapports des parlements français, belge et européen ainsi que sur d’autres sources publiques disponibles9. Elle s’est également appuyée sur un rapport de l’Office fédéral de la police, datant de février 2000, consacré à l’espion- nage économique et à l’interception des communications, ainsi que sur un rapport établi en février 2001 par les services du coordinateur des renseignements. Les Etats-Unis sont le pays qui dispose des capacités les plus développées en ma- tière de renseignement électronique. L’organe central responsable des écoutes est la National Security Agency (NSA) qui emploie près de 40 000 collaborateurs aux Etats-Unis et dans le monde et qui dispose d’un budget annuel de l’ordre de 4 mil- liards de francs. La NSA est la plus grande institution de renseignement aux Etats-Unis devant la CIA (Central Intelligence Agency) et le FBI (Federal Bureau of Investigations). Elle s’appuie sur un réseau planétaire d’interception des communi- cations qui comprend, outre des satellites d’interception, des stations d’écoute des satellites de communication, des réseaux radio terrestres ainsi que des réseaux câblés10. Selon de

nombreuses sources concordantes, la NSA exploiterait également, en collaboration avec la Grande-Bretagne, le Canada, l'Australie et la Nouvelle- Zélande, un réseau multinational d'écoute: le réseau Echelon. Ce système serait en mesure d'intercepter toutes les communications par satellites et de les filtrer grâce à des ordinateurs très puissants, par l'utilisation de mots-clefs prédéfinis ou par des techniques de reconnaissance vocale. Selon certaines sources, Echelon écouterait également les communications qui sont transmises par réseaux câblés terrestres ou

E. 9

Voir Nicky Hager, «Secret Power. New Zealand's Role in the International Spy Network», Craig Potton Publishing, Nelson, Nouvelle-Zélande, 1996. Voir également le rapport établi pour le Bureau d'évaluation des choix scientifiques et technologiques (Science and Technology Options Assessment Panel, STOA) du Parlement européen: Steve Wright, «An appraisal of technologies of political control», Omega Foundation, étude intérimaire, Luxembourg, avril 1997, PE 166.499 ainsi que les cinq rapports consa- crés au «Development of Surveillance Technology and Risk of Abuse of Economic Information», édité par Dick Holdsworth pour le STOA: Peggy Becker, «Data protection and human rights in the European Union and the role of the European Parliament», Luxembourg, octobre 1999, PE.168.184, volume 1/5; Duncan Campbell, «The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition», Luxembourg, octobre 1999, PE 168.184, volume 2/5 (ci-après: rapport Campbell); Franck Leprevost, «Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues», Luxembourg, novembre 1999, PE 168.184, volume 3/5 ; Chris Elliot, «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law», Luxembourg, octobre 1999, PE 168.184, volume 4/5; Nikos Bogolikos, «The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception», Luxembourg, octobre 1999, PE 168.184, volume 5/5.

E. 10

Voir en particulier James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001.

1386 sous-marins ou par faisceaux hertziens. En Grande-Bretagne, c'est le Government Communications Headquarters (GCHQ) qui est officiellement chargé des intercep- tions. Il disposerait de stations d'écoute au Belize, à Gibraltar, à Chypre, à Oman, en Turquie et en Australie. La collaboration entre les Etats-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande serait formalisée dans un accord secret, appelé accord UKUSA. Cet accord aurait été signé à la fin des années 40 par les Etats-Unis et par la Grande- Bretagne, puis élargi au Canada qui aurait conclu un accord bilatéral avec les Etats- Unis (accord CANUSA). L'Australie et la Nouvelle-Zélande auraient été associées plus tard. Selon les sources à disposition, d'autres pays participeraient indirectement au système Echelon en accueillant des stations d'interception sur leur territoire ou en recevant des informations d'Echelon. Il s'agirait notamment de l'Allemagne, de la Corée du Sud, du Japon, de la Norvège, de la Turquie11 et de Chypre. Echelon constituerait le seul système multilatéral d'interception des communications dans le monde. Jusqu'à aujourd'hui, les gouvernements

américain, britannique et canadien n'ont jamais reconnu l'existence de l'accord UKUSA. Le gouvernement néo- zélandais ainsi que le directeur australien du service des interceptions de défense (Defence Signals Directorate [DSD]) ont admis pour leur part l'existence de cet accord. Initialement à vocation militaire, certaines sources ont indiqué qu'Echelon serait de plus en plus souvent utilisé à des fins d'espionnage économique et de veille concur- rentielle afin de promouvoir les intérêts des entreprises américaines et d'accroître leur part de marché. Les Etats-Unis ne nient pas faire de l'espionnage économique, mais celui-ci aurait pour seul but de lutter contre les entreprises qui rompent les embargos internationaux, qui développent des technologies à double usage, civil et militaire, ou qui versent des commissions pour décrocher des contrats12. A ce jour, aucune entreprise n'a encore déposé plainte, en Europe ou aux Etats-Unis, en raison d'éventuels dommages occasionnés par des écoutes électroniques. Echelon pose également une série de problèmes juridiques et politiques au sein de l'Union européenne (UE) du fait de la double appartenance du Royaume-Uni à l'UE et à l'accord UKUSA et des distorsions de concurrence que d'éventuelles écoutes économiques pourrait entraîner. Bien que de nombreux ouvrages et rapports officiels aient été consacrés à Echelon, on dispose de peu d'informations irréfutables sur les objectifs et les capacités réelles du système. Les rapports officiels se réfèrent d'ailleurs très souvent aux mêmes sources d'origine et distillent les mêmes informations. Selon le rapport de l'Assem- blée nationale française, «cette similitude des informations et leur relative indigence à l'analyse peuvent témoigner d'une volonté délibérée d'orienter le débat sur les interceptions des communications, volonté à laquelle la communauté du ren- seignement ne serait pas étrangère»13. D'ailleurs, on peut s'étonner du soudain intérêt de l'opinion publique pour Echelon depuis la fin des années 90, alors que ce système était connu des spécialistes depuis longtemps.

E. 11

Selon la Free Congress Research and Education Foundation qui siège à Washington D.C., cité par Jacques Isnard, «La CIA et la NSA justifient les missions du réseau d'espionnage Echelon», in: Le Monde, 10.3.2000, p. 5.

E. 12

Voir les déclarations faites par l'ancien directeur de la CIA, James Woolsey, au Foreign Press Center de Washington D.C., le 7.3.2000, ainsi que son article «Why we spy on our allies», in: The Wall Street Journal, 17.3.2000, p. A18.

E. 13

Rapport français, p. 25.

1387 Le rapport du Parlement européen constitue vraisemblablement l'analyse la plus détaillée sur les possibilités et les limites du système Echelon. Ce rapport considère que l'existence de ce système mondial d'interception des communications ne fait plus de doute14 et que la NSA collabore avec d'autres services dans le domaine COMINT15. Le rapport précise également que les possibilités du système ne sont pas aussi grandes que supposées. Les conclusions du rapport du Parlement européen sont partagées par le Conseil fédéral16. De leur côté, les rapports français et belge se montrent moins circonspects et consi- dèrent l'existence d'Echelon comme acquise. D'autres pays possèdent des capacités d'espionnage électronique sans qu'aucun ne puisse rivaliser avec les capacités d'interception des Etats-Unis. Selon le rapport du Parlement européen et d'autres sources non officielles17, la France disposerait éga- lement d'un réseau d'écoute global. Ce réseau

aurait été mis en place ces dix derniè- res années par son service de renseignement extérieur, la Direction générale de la sécurité extérieure (DGSE). Il comprendrait notamment des bases d'interception satellitaire en France, mais aussi dans les Emirats arabes unis18, à Kourou (Guyane française) ainsi que sur l'île française de Mayotte (Comores), dans l'Océan indien. Ces deux dernières bases seraient gérées en commun avec le service de renseigne- ment extérieur allemand, le Bundesnachrichtendienst (BND). Grâce à la large cou- verture géographique des stations au sol, la France serait en mesure d'intercepter des communications par satellite partout dans le monde. Selon un rapport officiel de l'Assemblée nationale française, «l'interception des liaisons satellites de télécom- munications reste une priorité (de la DGSE)»19. La France dispose également de satellites espions ainsi que, sur le plan opérationnel, des capacités d'écoute navales et aériennes qui peuvent être engagées sur un théâtre d'opération. Selon le rapport du Parlement européen, la Russie disposerait également, sans qu'il soit possible de le confirmer, d'un système d'interception d'envergure mondiale avec des stations d'écoute au sol à Cuba et au Vietnam20. D'autres Etats de l'Union européenne semblent également posséder des capacités de renseignement électronique, certes plus limitées. C'est le cas du Danemark, de la Finlande, de l'Allemagne, des Pays-Bas, de l'Espagne, de la Suède et de la Grande- Bretagne21. Selon le rapport du Parlement belge qui cite un journaliste, l'Allemagne disposerait d'une base en République populaire de Chine, à Taiwan et – en collabo- ration avec la France – en Guyane française22.

E. 14

Rapport européen, p. 17.

E. 15

Rapport européen, p. 71.

E. 16

Voir la réponse du Conseil fédéral du 15.3.2002 à l'interpellation 01.3601 Sécurité des données. Etat des lieux (BO 2002 N 468).

E. 17

Jacques Isnard, «Le Royaume-Uni au cœur du dispositif en Europe», in: Le Monde, 23.2.2000, p. 2. Voir aussi Vincent Jauvert, «Espionnage, comment la France écoute le monde», in: Le Nouvel Observateur, n° 1900, 5.4.2001, p. 14 ss.

E. 18

Rapport de l'Office fédéral de la police, février 2000, p. 9 (non publié).

E. 19

Rapport fait au nom de la Commission des finances, de l'économie générale et du plan de l'Assemblée nationale sur le projet de loi des finances pour 2003, du 10.10.2002, rapport n° 256, annexe n° 36, Secrétariat général de la défense nationale et renseignement, rap- porteur spécial: Bernard Carayon, p. 11.

E. 20

Rapport européen, p. 13 et p. 85 ss.

E. 21

Rapport européen, annexe IV.

E. 22

Rapport belge, p. 37.

1388 Dans le reste du monde, la Chine, l'Inde, Israël et le Pakistan disposeraient également de capacités SIGINT d'une certaine importance23. 4 Description du système Onyx 4.1 Introduction Onyx est un système COMINT d'interception des communications militaires et civi- les qui transitent par satellites (COMSAT). Il permet de capter les transmissions et transferts de données écrites et vocales (appels téléphoniques, télécopies, télex, courriers électroniques, données informatiques). Ce système complète l'écoute des signaux radio à ondes courtes qui étaient, longtemps durant, la seule forme de ren- seignement électronique utilisée par les autorités suisses. La décision de réaliser Onyx a été prise par le Conseil fédéral le 13 août 1997 sur proposition du DDPS. Le système a pour objectif d'intercepter des communications touchant au terrorisme international, à l'extrémisme violent, au crime organisé, à l'espionnage et à la prolifération ainsi que toutes autres informations concernant la politique de sécurité. Les informations acquises doivent améliorer les possibilités du Conseil fédéral de reconnaître à temps, et indépendamment de l'étranger, des mena- ces et des risques dans le domaine de la politique de sécurité. Le système Onyx ne peut être utilisé que pour des écoutes à l'extérieur des fron- tières. Après une phase de développement, le système Onyx a été mis en service en avril 2000. Depuis avril 2001, le système est en phase pilote d'exploitation. Durant cette phase, l'accent a été mis principalement sur l'interception de communications con- cernant les ADM. Le système entrera en phase opérationnelle dans le courant de l'année 2004 sur les sites de Zimmerwald, d'Heimenschwand et de Loèche. L'exploitation complète est prévue pour fin 2005/début 2006. D'ici là, le nombre d'antennes doit être doublé. Le financement du système Onyx est assuré par le budget ordinaire du matériel d'armement du Groupement de l'armement qui est examiné chaque année par les Commissions des finances et adopté par les Chambres fédérales (rubriques 540.3210.00124 et 540.3220.00125). Le financement des constructions y afférentes a été adopté par l'arrêté fédéral du 9 décembre 1999 concernant l'immobilier militaire 200026 et émarge au budget de l'Etat-major général (rubrique 510.3200.001). Le personnel supplémentaire nécessaire est mis à disposition par l'Etat-major général. La DCG ainsi que la Délégation des finances ont connaissance des coûts d'investis- sements et des frais d'exploitation annuels de l'installation. Ces données ne sont pas exposées ici pour des motifs de confidentialité.

E. 23

Rapport Campbell, p. 1, ch. 7.

E. 24

Rubrique «Etudes de projets, essais et préparatifs d'achats de matériel d'armement»[en allemand: «Projektierung, Erprobung und Beschaffungsvorbereitung von Rüstungsmaterial (PEB)»].

E. 25

Rubrique «Equipement personnel et besoins de renouvellement (BER)»[en allemand: «Ausrüstung und Erneuerungsbedarf (AEB)»].

E. 26

Voir le message du Conseil fédéral sur l'immobilier militaire 2000, du 18.8.1999, FF 1999 7807.

1389 4.2 Bases légales L’exploitation du système Onyx est fondée principalement sur l’art. 99 LAAM. Cet article constitue la base légale des activités de renseignement extérieur de la Confé- dération27: Art. 99 LAAM Service de renseignement 1 Le service de renseignement a pour tâche de rechercher, d’évaluer et de diffuser des informations sur l’étranger importantes en matière de politique de sécurité. 2 Il est habilité à traiter, le cas échéant à l’insu des personnes concernées, des don- nées personnelles, y compris des données sensibles et des profils de la personnalité, à condition et aussi longtemps que ses tâches l’exigent. Il peut, de cas en cas, com- muniquer des données personnelles à l’étranger en dérogation aux dispositions de la protection des données. 2bis Il peut communiquer à l’Office fédéral de la police les informations sur des personnes en Suisse qu’il a obtenues dans l’exercice des activités mentionnées à l’al. 1, et qui peuvent êtres importantes pour la sûreté intérieure ou pour la poursuite pénale. 3 Le Conseil fédéral règle: a. le détail des tâches du service de renseignement, son organisation et la pro- tection des données; b. l’activité du service de renseignement en période de service de promotion de la paix, de service d’appui et de service actif; c. la collaboration du service de renseignement avec les autres services canto- naux et fédéraux ainsi qu’avec les services étrangers; d. les exceptions aux dispositions sur l’enregistrement des fichiers lorsque, à défaut, la recherche des informations serait compromise. 4 La protection des sources doit dans tous les cas être assurée. 5 Le service de renseignement est directement subordonné au chef du Département de la défense, de la protection de la population et des sports. Cet article est complété par l’ordonnance du 4 décembre 2000 sur le renseignement du Département fédéral de la défense, de la protection de la population et des sports (Ordonnance sur le renseignement, Orens; RS 510.291). Cette ordonnance précise notamment que le SRS «gère les activités de renseignement permanentes en rapport avec l’étranger» et qu’il recueille, en collaboration avec d’autres services fédéraux, «les informations importantes pour la sécurité de la Confédération à l’intention des autorités politiques et du commandement militaire» (art. 2, Orens). S’agissant des activités d’Onyx au profit du SAP, elles relèvent de la sûreté inté- rieure et ressortent à la législation sur la protection préventive de l’Etat, en premier lieu à la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la

E. 27

Avec la modification du 4 octobre 2002; l’art. 99, al. 2bis, al. 3, let. b et c, al. 4 et al. 5 entrera en vigueur au 1.1.2004.

1390 sûreté intérieure (LMSI; RS 120). L’art. 14 LMSI décrit de manière exhaustive les informations que le SAP peut rechercher dans l’exercice de son mandat légal: Art. 14 LMSI Recherche d’informations 1 Les organes de sûreté de la Confédération et des cantons recherchent les informa- tions nécessaires à l’exécution des tâches définies par la présente loi. Ils peuvent rechercher ces informations à l’insu de la personne concernée. 2 Des données personnelles peuvent être recueillies par le biais: a. de l’exploitation de sources accessibles au public; b. de demandes de renseignements; c. de la consultation de documents officiels; d. de la réception et de l’exploitation de communications; e. d’enquêtes sur l’identité ou le lieu de séjour de personnes; f. de l’observation de faits, y compris au moyen d’enregistrements d’images et de sons, dans des lieux publics et librement accessibles; g. du relevé des déplacements et des contacts de personnes. 3 Le recours à des mesures de contrainte prévues par la procédure pénale n’est permis que dans le cadre d’une procédure d’enquête de police judiciaire ou d’une instruction préparatoire. Il en va de même de l’observation de faits dans des locaux privés. La LAAM et la LMSI fixent les principes

et les compétences en matière de collecte d'informations par les services de renseignement. Les détails de l'exploration radio sont réglés quant à eux dans l'ordonnance sur la conduite de la guerre électronique (OCGE) que le Conseil fédéral a adoptée le 15 octobre 2003 (RO 2003 3971)28. Cette ordonnance est entrée en vigueur au 1er novembre 2003. La LAAM et l'OCGE règlent également les échanges d'informations lorsque des indications relatives à la sûreté intérieure ou à des activités criminelles en Suisse sont captées de manière fortuite29. Ces informations concernant la Suisse ne sont généralement pas transmises au SRS qui n'a pas le droit de procéder à des activités d'exploration dans le pays. L'art. 99, al. 2bis, LAAM donne la possibilité, pour les agents de la CGE, de transmettre directement les informations concernant la Suisse ou des usagers suisses à l'Office fédéral de la police, qui pourra, à son tour, les transmettre aux autorités pénales compétentes. La collaboration entre le SRS et le SAP est réglée quant à elle dans une directive des chefs du DDPS et du DFJP du 19 mars 1997 et dans une convention entre le SRS et le SAP du 6 février 2003.

E. 28

Voir communiqué de presse du DDPS, du 15.10.2003.

E. 29

L'OCGE parle, en pareil cas, de «produits annexes»; voir art. 5, al. 3, OCGE.

1391 4.3 Cycle du renseignement Onyx est un instrument de collecte d'informations. Son activité s'inscrit dans un cycle dont il constitue une étape30: – La première phase – la phase de planification et conduite – consiste à déter- miner les besoins en renseignements et à en planifier la collecte. Cette tâche est du ressort du SRS et du SAP sur la base des missions générales qui leur sont dévolues par la loi, par ordonnance ou par mandat des autorités politi- ques responsables (Délégation du Conseil fédéral pour la sécurité, chefs du DDPS et du DFJP). – La deuxième phase – la phase de collecte proprement dite – a pour objectif de réunir les informations auprès des sources. Elle peut faire intervenir plu- sieurs acteurs et différents services. Onyx intervient au cours de cette phase en tant qu'instrument de collecte. Les procédures et méthodes de collecte, qu'elles soient électroniques ou humaines, sont généralement les secrets les mieux gardés par les services de renseignement. – La troisième phase – la phase d'exploitation – est la partie du cycle qui consiste à analyser et à interpréter les informations recueillies. C'est au cours de cette phase que l'information devient un renseignement. Cette phase est assurée par les services d'exploitation du SRS et du SAP. – La quatrième et dernière phase s'appelle la phase de diffusion au cours de laquelle les renseignements sont acheminés sous forme de rapports vers les organes demandeurs. Cette phase est soumise à des règles strictes de confi- dentialité afin d'éviter que les destinataires ne viennent à connaître les pro- cédures de collecte de renseignements et puissent en identifier les sources. 4.4 Exploitation Onyx est exploité par la Division de la conduite de la guerre électronique (CGE) qui est un service du Groupe de l'aide au commandement de l'Etat-major général. Le système intercepte les communications transitant par satellites grâce aux liaisons électromagnétiques entre les satellites de communications – généralement en orbite géostationnaire – et les stations au sol31 (voir schéma 1, ci-dessous). Il existe plusieurs sortes de satellites de communications (Intelsat, Inmarsat, Eutel- sat, PanAmSat, Arabsat, Gorizont, etc.) qui offrent à leur clientèle différents types de prestations. A titre d'exemple, le réseau Intelsat propose des services dans le domaine des communications entre réseaux terrestres fixes («fixed satellite servi- ces»). Il dispose actuellement de 24 satellites qui couvrent le continent américain, l'Afrique,

l’Europe, l’Asie ainsi que le Pacifique. Le système Inmarsat, qui couvre les mêmes secteurs qu’Intelsat, offre des prestations satellitaires entre un réseau téléphonique terrestre et des usagers mobiles tels des avions, navires, plates-formes offshore («mobile satellite services»).

E. 30

Voir Jacques Baud, «Encyclopédie du renseignement et des services secrets», Lavauzelle, Paris, 2002, p. 196.

E. 31

Pour plus d’informations sur les aspects techniques de l’interception des communications et sur la technique des communications satellitaires, il est recommandé de lire les chap. 3 et 4 du rapport du Parlement européen, p. 32 ss.

1392 L’interception des communications par Onyx s’opère au moyen d’antennes paraboliques d’un diamètre variant entre 4 et 18 mètres. Toutes les antennes du système Onyx sont situées en territoire suisse. Elles captent les faisceaux d’onde que les satellites de communications renvoient vers la terre («downlinks»). En général, les faisceaux d’onde qui descendent vers la terre ne sont pas focalisés dans une zone géographique précise, mais englobent plusieurs pays («footprint»). Cette zone peut représenter jusqu’à 50 % de la surface terrestre si le signal n’est pas concentré. En Europe, par exemple, les zones d’empreinte d’Intelsat et d’Inmarsat s’étendent généralement à l’ensemble de l’Europe. Il suffit donc de disposer d’une seule station de réception en Suisse pour intercepter les communications par satellite de toute l’Europe. En règle générale, il faut une antenne par satellite que l’on veut intercepter. L’interception ne porte que sur les communications internationales civiles et militai- res. L’interception et l’exploitation de communications civiles ayant lieu en Suisse est prohibée. Le système Onyx fonctionne 24 heures sur 24, 365 jours par année. Schéma 1 Communications par satellite (Schéma explicatif simplifié)

Orbite géostationnaire

satellite

Uplink Downlink

station station

au sol au sol

1393 4.5 Mandats d’exploration La CGE n’effectue des interceptions que sur mandat des services dûment autorisés (ci-après: mandants). Pour l’instant, selon une décision prise par la Délégation du Conseil fédéral pour la sécurité le 10 juin 200232, seuls le SRS et le SAP ont la qualité de mandant à l’égard des interceptions satellitaires. Il est prévu à terme que le chef du DDPS puisse élargir la qualité de mandant à d’autres offices pour autant qu’ils disposent de bases légales suffisantes (par exemple: le Renseignement mili- taire et le Renseignement des Forces aériennes). Il serait également possible, lors d’un service d’assistance de l’armée (par exemple pour assurer la sécurité du World Economic Forum de Davos), de prévoir l’utilisation éventuelle d’interceptions satellitaires. Une telle décision dépendrait du Conseil fédéral et du Parlement. Les principes de collaboration entre la CGE et les mandants sont fixés dans l’OCGE ainsi que dans des accords-cadres passés avec chaque mandant. Les accords-cadres doivent obligatoirement revêtir la forme écrite (art. 3, al. 2, OCGE). Ils fixent éga- lement les responsabilités respectives, les standards de sécurité

à adopter, les proces- sus de gestion et la définition des produits attendus. Actuellement, il existe un accord-cadre entre la CGE et le SRS, datant du 3 octobre 2001, et un accord-cadre entre le Groupe de l'aide au commandement de l'Etat- major général (dont dépend la CGE) et le SAP, daté du 1er avril 1998. Sur la base des accords-cadres, les mandants fixent les mandats d'exploration indi- viduels qui doivent faire l'objet d'une convention de prestations écrite entre le mandant et la CGE (art. 3, al. 3, OCGE). Les conventions de prestations précisent les points forts de l'exploration en fonction de zones géographiques ou de thèmes précis ayant trait à la politique de sécurité de la Suisse. Une convention de presta- tions différente correspond à chaque thème ou à chaque région géographique d'intérêt. Les conventions de prestations contiennent tous les éléments nécessaires à l'exé- cution des mandats et à leur contrôle. Elles comprennent notamment les objets d'exploration recherchés (noms de personnes, d'organisations ou d'entreprises, éléments d'adressage, etc.) ainsi que la liste de mots-clefs (key words) dont le man- dant attend qu'ils apparaissent dans les communications interceptées. Toutes ces informations sont nécessaires pour l'élaboration des systèmes de filtre automatique des communications. Selon les mandats, il peut y avoir entre 5 et plusieurs centaines de mots-clefs. Par exemple, dans le domaine de la lutte contre la prolifération, la liste des mots-clefs compte plus de dix pages, à raison de 25 termes par page. Plus les mots-clefs sont précis, plus pertinentes sont les informations retenues. Des expressions triviales comme «terrorisme», «bombe» ou «anthrax» ne sont pas adé- quates car elles n'apparaissent pratiquement jamais de la sorte dans une communica- tion entre deux usagers. Les listes d'éléments d'adressage ou de mots-clefs ne doivent contenir aucune indication relative à des usagers suisses. Les numéros de téléphones ou de téléco- pieurs comportant, par exemple, l'indicatif international pour la Suisse (0041) sont proscrits à moins qu'il soit techniquement prouvé que l'appareil opère depuis l'étranger. C'est le cas notamment pour certains types de téléphones portables.

E. 32

Chiffre 3.2. du mandat de base du Service de renseignement stratégique, du 10.6.2002 (non publié).

1394 Il appartient aux mandants de s'assurer de la légalité et de la proportionnalité des mandats d'exploration confiés à la CGE (art. 14 OCGE). Une autorité de contrôle indépendante (ACI), composée de représentants de différents départements, surveille les mandats d'exploration (art. 15 OCGE). L'ACI contrôle chaque mandat ainsi que l'adjonction des nouveaux objets d'exploration aux mandats existants. Elle examine également la manière avec laquelle les informations sont recueillies, transmises et traitées auprès du mandant (art. 15, al. 2, OCGE). L'ACI peut, si nécessaire, deman- der au département du mandant de suspendre des ordres d'exploration qui ne satis- font pas ou plus aux principes de la légalité et de la proportionnalité. Sur le plan théorique, il serait possible de définir un nombre illimité de conventions de prestations. Sur le plan technique, les possibilités sont limitées. Il faut donc fixer des priorités dans la recherche des informations. Ces priorités sont fixées par les mandants. Il existe actuellement une trentaine de mandats de prestations entre le SRS et le CGE et un mandat de prestations entre le SAP et le Groupe de l'aide au commandement de l'Etat-major général. Ces mandats concernent la lutte contre la prolifération, le contre-espionnage, la criminalité organisée et la lutte contre le terrorisme ainsi que la situation dans le Golfe. La délégation connaît l'ensemble des accords-cadres passés entre le SRS et la CGE d'une part et entre le SAP et la CGE d'autre part. Elle a accès également à l'ensemble des conventions de prestations. 4.6

Collecte d’informations Sur la base des conventions de prestations, la CGE effectue la collecte des informa- tions émanant de systèmes de télécommunication à l’étranger. Pour ce faire, Onyx doit d’abord accéder et identifier le canal de transmission. Il s’agit durant cette phase de ne retenir que les communications potentiellement intéressantes et d’éliminer tout ce qui relève du domaine public, telles les émissions de radio ou de télévision transitant par satellites. La deuxième étape consiste à analyser automatiquement le contenu déchiffrable de la communication afin de le filtrer automatiquement. Le filtrage s’effectue à l’aide de systèmes d’intelligence artificielle. Ces systèmes comparent le contenu du message avec les éléments d’adressage et les mots-clefs prédéfinis (voir schéma 2, ci-dessous). Les messages qui ne répondent à aucun de ces critères sont automatiquement éliminés.

1395 Schéma 2 Exemple d’interception d’une communication par télécopie entre deux usagers à l’étranger

Etat A TELECOPIE A: Mme K.

Ministère de la défense

Etat B

No de télécopie : WW XX YY ZZ De: Monsieur Z.

Import-Export Ltd

Etat A Concerne: acquisition de fusées pyrotechniques

Madame, Pour faire suite à notre discussion… Etat B

Commentaire du schéma 2: Si le numéro d’appel du destinataire de la télécopie (dans l’exemple: «WW XX YY ZZ») est contenu dans une convention de prestations, Onyx peut intercepter toutes les télécopies envoyées à Mme K. au Ministère de la défense de l’Etat B, à condition toutefois que la communication transite par satellite. Si le nombre de communica- tions est important, il est possible de fixer dans la convention de prestations des mots-clefs destinés à filtrer davantage les informations (par exemple: «fusées pyro-techniques»). La procédure de filtrage est relativement simple si les messages sont transmis sous forme textuelle, comme c’est le cas pour le courrier électronique ou les télex. Elle est rendue beaucoup plus complexe si le système doit lire des retranscriptions im- primées ou manuscrites, ce qui nécessite une opération de reconnaissance optique des caractères, ou s’il doit utiliser un système de reconnaissance de la parole dans le cas de communications verbales. Les systèmes automatiques de reconnaissance verbale sont encore peu fiables, notamment si les voix des interlocuteurs ne sont pas connues ou s’ils parlent de manière peu distincte. Une des autres limites fondamentales à l’exploitation provient du fait que le filtrage automatique doit pouvoir fonctionner sur des communications dans une multitude d’alphabètes et de langues aux prononciations variées. Le tri doit également s’effec-

1396 tuer en temps réel afin d’éviter la surcharge des unités de stockage de l’information et de permettre que l’information parvienne rapidement à son destinataire. Il ressort de ce qui précède que la surveillance exploratoire et généralisée des com- munications par satellites n’est possible que sur une petite partie du trafic. Il est utile d’illustrer cela à partir des statistiques d’interception (voir encadré, ci-dessous). Ces chiffres montrent que les informations réellement intéressantes sont noyées dans un océan d’insignifiances et que les «perles» qui remontent jusqu’au plus haut niveau de l’Etat sont extrêmement rares. Statistiques d’interception Possibilités d’interception du BND allemand : Sur les quelque 10

millions de communications internationales effectuées chaque jour au départ et à destination de l'Allemagne, 800 000 environ transitent par satellites (8 pour cent). Moins de 10 pour cent d'entre elles (75 000 communications) sont filtrées par un appareil de recherche33. Il semblerait que sur ces communications, seules 700 présente- raient des informations pertinentes pour la sécurité du pays et que 15 d'entre elles pourraient faire l'objet d'un examen approfondi34. Le rapport est donc de 15 sur 10 millions (0,00015 pour cent). Autre exemple: La NSA américaine capterait un million de conversations satelli- tes par demi-heure. Sur ce million de communications, 6500 seraient retenues par sondage, 1000 correspondraient aux critères prédéfinis, 10 seraient choisies par les analystes, un seul rapport étant finalement produit sur cette base35. La proportion est ici de 1 sur 1 million, soit 0,0001 pour cent. Les informations brutes (raw intelligence) qui ont traversé les différents filtres sont triées manuellement par un opérateur de la CGE et rassemblées en fonction de différents critères. Elles sont ensuite transmises, munies d'un commentaire de l'opé- rateur ou d'une courte traduction, au mandant respectif. Aucune information n'est transmise au mandant sans qu'elle ait été examinée au préalable par un collaborateur de la CGE (contrôle). Les informations reçues sont communiquées aux services d'exploitation du SRS ou du SAP. Ces derniers les analysent, les traduisent et les interprètent pour établir des rapports ou des synthèses (finished intelligence). Le SRS ou le SAP ne transmettent aucune information brute provenant de l'explo- ration électronique à d'autres services, sauf dans des cas exceptionnels. En revanche, il est fréquent que les rapports d'analyse des services de renseignement suisses soient remis, sans indication des sources, à d'autres organes de la Confédération et des cantons ou à des services de renseignement ou de sécurité à l'étranger, confor-

E. 33

Déclarations faites par le coordinateur allemand des services de renseignement devant la commission temporaire du Parlement européen, le 21.11.2000 (voir le rapport européen, p. 38).

E. 34

Jochen Bittner, «Bedingt abhörbereit. Der BND hat zu viele elektronische Quellen und zu wenige kundige Auswerter», in: Die Zeit, Nr. 40, 27.9.2001, p. 2.

E. 35

Déclaration faite par l'amiral William O. Studeman, ancien directeur de la NSA (1988–1992), cité par James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001, p. 411 et note p. 671.

 ment aux procédures prévues dans les lois et ordonnances correspondantes36. La liste des pays avec lesquels les services de renseignement suisses sont autorisés à échanger des informations est définie par le Conseil fédéral. La DCG en a également connaissance et effectue des contrôles ponctuels réguliers. Les informations brutes obtenues par le système Onyx sont des informations qui relèvent uniquement du renseignement. Elles ne peuvent pas, en l'état actuel du droit, être utilisées comme preuves dans une procédure pénale. Les mandants sont responsables de traiter et d'archiver les données qui leur sont transmises conformément aux dispositions légales. La CGE n'archive aucune don- née personnelle et détruit les fichiers informatiques au fur et à mesure. Elle ne conserve que les données de liaison issues de l'activité d'exploration et servant à identifier les objets d'interception (art. 6, al. 2, OCGE). Les données de liaison contiennent des informations portant sur les

circonstances de la communication, mais pas sur son contenu (annexe de l'OCGE, ch. 3). Onyx travaille actuellement à près de 92 % pour le SRS (y compris les résultats transmis au Renseignement des Forces aériennes) et à raison de 8 % environ pour le SAP. Outre ces deux services, il n'existe pas d'autres bénéficiaires de prestations. 4.7 Conditions posées à la collecte d'informations Plusieurs conditions cumulatives sont posées à la récolte d'informations par Onyx. Ces conditions figurent dans l'OCGE ainsi que dans les accords-cadres. Ces conditions sont les suivantes: – Seuls les services désignés par le chef du DDPS peuvent donner des mandats d'exploration à Onyx (art. 2, al. 3, OCGE). – La collecte d'informations n'est autorisée que sur la base de mandats d'exploration écrits (art. 3, al. 3, OCGE). Sans mandat, pas de recherche. – Les mandats délivrés servent uniquement à obtenir des informations tou- chant à la politique de sécurité (art. 2, al. 2, OCGE). Onyx n'est donc pas au- torisé à faire de la surveillance économique, technologique ou scientifique, à moins que cela ne serve la sécurité de la Suisse. – Les mandats d'exploration ne peuvent porter que sur des objets d'explo- ration à l'étranger – ou considérés comme tels – et ne peuvent pas avoir pour cible des usagers suisses (art. 5, al. 1, OCGE). La CGE est ainsi autorisée à intercepter les communications entre deux usagers à l'étranger, ainsi que les communications entre un usager à l'étranger et un usager en Suisse, pour au- tant que l'usager à l'étranger constitue l'objet d'exploration. Il est en revan- che interdit d'utiliser Onyx à des fins relevant de la sûreté intérieure. C'est pourquoi l'interception de conversations entre deux usagers en Suisse, quel- que soit leur nationalité, est prohibée (voir tableau 1, ci-dessous). L'OCGE

E. 36

Voir, pour le SRS, l'art. 6, al. 2, Orens. Voir, pour le SAP, l'art. 17 LMSI, l'art. 6, al. 1, de l'ordonnance sur les mesures visant au maintien de la sûreté intérieure (OMSI), du 27.6.2001 (RS 120.2), et le ch. 26 des directives du Département fédéral de justice et police sur la mise en application de la protection de l'Etat, du 9.9.1992 (FF 1992 VI 150).

1398 procède donc essentiellement d'une logique territoriale et ne dépend pas de la nationalité des usagers. – La CGE n'a en principe pas le droit de transmettre au SRS des informations se rapportant à des usagers suisses qui ont été récoltées de manière non intentionnelle (art. 5, al. 2, OCGE). Si ces informations fortuites – l'ordon- nance parle de «produits annexes» (art. 5, al. 3, OCGE) – sont nécessaires à l'exécution du mandat du SRS, les données relatives aux usagers en Suisse doivent être supprimées en tout ou partie. Il en va de même des usagers à l'étranger clairement identifiés comme étant suisses. Les détails sont réglés dans un document annexé à l'accord-cadre entre le SRS et la CGE du 3 octobre 2001, connu sous le nom d'«annexe 4»37. L'annexe 4 prévoit no- tamment que les informations transmises au SRS en pareil cas doivent faire l'objet d'un procès-verbal établi par le SRS et la CGE. Ces procès-verbaux peuvent être soumis à des contrôles, notamment par la DCG. – Les produits annexes relatifs à des usagers suisses et qui présentent un intérêt pour la sécurité intérieure peuvent être communiquées directement au SAP, conformément à l'art. 99, al. 2bis, LAAM. Ces informations peuvent être transmises intégralement avec les indications nécessaires concernant les usagers suisses. Tableau 1 Interceptions autorisées ou prohibées, suivant le territoire

Emplacement de la cible de l'exploration

En Suisse A l'étranger

En Suisse Interception prohibée Interception autorisée

Emplacement de l’autre usager A l’étranger Interception prohibée Interception autorisée

E. 37

Beilage 4: Richtlinien zur Verarbeitung von Erfassungsresultaten mit Bezug zu H-Personen bzw -Firmen, Produktedefinition SAT, Anhang B1 zur Rahmenvereinbarung zwischen dem Strategischen Nachrichtendienst und der COMINT Organisation betreffend ND Führung, vom 3.10.2001 (seulement en allemand, non publié). Selon cette annexe sont considérés comme usagers suisses (a) tous les citoyens suisses, (b) tous les étrangers ayant leur domicile permanent en Suisse, (c) toutes les personnes morales enregistrées en Suisse (y compris les aéronefs et les navires sous pavillon suisse) et (d) tous les groupe- ments et associations non enregistrés et qui sont composés majoritairement de membres répondant aux critères fixés sous lettres (a) à (c).

1399 5 Constats de la délégation et appréciation 5.1 Légalité des interceptions effectuées par Onyx 5.1.1 Légalité des mandats d’interception en matière de sécurité extérieure La délégation est d’avis que la base légale qui fonde les mandats d’interception du SRS est suffisante. En effet, l’art. 99 LAAM ainsi que l’Orens donnent explicite- ment la compétence au SRS de recueillir activement des informations sur l’étranger. La loi précise que les activités de collecte d’informations sont limitées aux questions touchant à la politique de sécurité de la Suisse et donc aux menaces provenant de l’extérieur38. La collecte et l’exploitation d’informations relatives à la Suisse et l’interception de communications entre des usagers en Suisse sont interdites. L’interdiction d’effectuer des interceptions de communications d’usagers en Suisse se déduit d’ailleurs du code pénal. Ce dernier réprime les infractions effectuées en Suisse contre le domaine privé ainsi que la violation du secret des télécommunica- tions. Seules sont considérées comme non punissables les mesures officielles de surveillance, approuvées par un juge, qui visent à poursuivre ou prévenir les crimes et délits d’une certaine gravité39. Les interceptions de la CGE n’entrent pas dans cette catégorie et sont donc punissables si elles portent délibérément sur des usagers en Suisse. Si la délégation juge suffisant le dispositif législatif actuel concernant les mesures d’interception ordonnées par le SRS, elle estime toutefois qu’il devrait être clarifié et rendu plus précis au niveau de la loi. Force est en effet de constater que le libellé de l’art. 99 LAAM est particulièrement hermétique s’agissant des interceptions de communications, notamment si on le compare aux dispositions extrêmement claires et précises existant en matière de sûreté intérieure (LMSI) ou de surveillance téléphonique dans le domaine pénal (LSCPT). La délégation doute en effet que les personnes qui ne sont pas spécialisées dans les questions de renseignement soient conscientes des activités d’interception qui sont déployées sur la base de l’art. 99 LAAM. D’ailleurs, le message de 1993 relatif à la LAAM ne les mentionne pas. Le message à l’appui de la révision de la législation militaire de 200140 ne donne pas davantage d’informations. La délégation est d’avis que l’existence d’interceptions de communications devrait être mentionnée plus clairement dans la LAAM. Celle-ci devrait indiquer explicite- ment que les interceptions ne peuvent porter que sur des communications à l’étran- ger et faire référence aux dispositions du code pénal qui répriment l’interception de communications d’usagers en Suisse.

E. 38

Voir sur ce point le message du Conseil fédéral relatif à la loi fédérale sur l’armée et l’admnistration militaire et à l’arrêté fédéral sur l’organisation de l’armée, du 8.9.1993 (FF

1993 IV 105).

E. 39

Voir les art. 179bis à 179novies, notamment l'art. 179octies, et l'art. 321ter du code pénal, du 21.12.1937 (CP; RS 311.0). Voir aussi les art. 43, 44 et 50 de la loi fédérale sur les télécommunications, du 30.4.1997 (LTC; RS 784.10). Selon la LSCPT qui règle la surveillance téléphonique en matière pénale, les conversations ne peuvent être écoutées que s'il existe des soupçons fondés de délit grave, uniquement pour une certaine catégorie de délits, et sur décision d'un juge dont la décision doit être confirmée par une instance judiciaire supérieure. Voir aussi l'annexe 1.

E. 40

Message du Conseil fédéral sur la réforme Armée XXI et sur la révision de la législation militaire, du 24.10.2001 (FF 2002 835).

1400 Il y a d'ailleurs, pour la délégation, un paradoxe à constater que les mesures de surveillance des communications effectuées par les autorités suisses sur leur terri- toire sont encadrées par un régime légal très strict, impliquant des contrôles judiciai- res et des voies de recours, alors que les interceptions à l'étranger disposent – la DCG ne saurait dire à dessein – d'un cadre réglementaire plutôt vague. Ainsi, les personnes à l'étranger ne bénéficient d'aucune protection juridique en droit suisse contre les interceptions dont elles pourraient faire l'objet par les autorités de la Confédération. En demandant que les interceptions de communications soient inscrites expressé- ment dans la LAAM, la DCG poursuit un objectif de transparence. Cette exigence se justifie moins sur le plan interne, puisque que l'interception d'usagers en Suisse est interdite, qu'à l'égard du droit international, et en particulier de la CEDH41. L'art. 8 CEDH n'autorise les atteintes à la vie privée que lorsqu'il s'agit de préserver la sécurité nationale et pour autant que plusieurs conditions soient remplies (existence et accessibilité de la base légale, proportionnalité, etc.). Dans plusieurs arrêts, la Cour européenne des droits de l'homme de Strasbourg a indiqué que les lois régle- mentant les écoutes administratives ou judiciaires devaient être accessibles au public et rédigées de façon suffisamment précise et détaillée pour que les citoyens puissent y répondre par un comportement adéquat42. Dans cet ordre d'idée, la délégation salue l'initiative prise récemment par le Conseil fédéral de fixer précisément dans l'OCGE les tâches et compétences en matière d'interception de communications. Cette démarche contribue à rendre la législation en la matière plus transparente et va dans le sens préconisé par la délégation. Malgré cette première mesure, la délégation reste de l'avis que l'existence d'interceptions de communications devrait être mentionnée plus clairement dans la LAAM. Celle-ci devrait indiquer explicitement que les interceptions ne peuvent porter que sur des communications à l'étranger et faire référence aux dispositions du code pénal qui répriment l'interception de communications d'usagers en Suisse.

E. 41

Selon plusieurs auteurs, la CEDH est l'instrument le plus efficace au plan international en matière de protection de la vie privée.

E. 42

Voir l'arrêt de la Cour européenne des droits de l'homme dans l'affaire Kruslin c. France, du 24.4.1990 (§ 33): «Les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance.

Partant, elles doivent se fonder sur une ‹loi› d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner.». Voir aussi les arrêts Malone c. Royaume-Uni du 2.8.1984 (§ 67), Huvig c. France du 24.4.1990 (§ 29) et Amann c. Suisse du 16.2.2000 (§ 58). Pour l'instant, la jurisprudence de la Cour a porté sur des me- sures de surveillance téléphonique, judiciaires ou administratives, réalisées par des autori- tés à l'encontre de citoyens soumis à leur juridiction. A la connaissance de la DCG, la Cour n'a pas encore eu à se prononcer sur des interceptions effectuées par un membre si- gnataire de la CEDH sur le territoire d'un autre pays.

1401 Recommandation n° 1 La Délégation des commissions de gestion recommande au Conseil fédéral d'examiner l'opportunité d'introduire dans la LAAM une référence explicite aux interceptions de communications à l'étranger. Celle-ci devrait indiquer égale- ment que les écoutes ne peuvent porter que sur des communications à l'étranger et faire mention des dispositions du code pénal réprimant l'interception de com- munications d'usagers en Suisse. Recommandation n° 2 La Délégation des commissions de gestion recommande au Conseil fédéral d'examiner la conformité à la CEDH de la législation relative aux activités d'interceptions de communications à l'étranger et, au besoin, de lui apporter les adaptations nécessaires. 5.1.2 Légalité des mandats d'interception en matière de sécurité intérieure L'art. 14 LMSI règle de manière détaillée et exhaustive les moyens que les autorités de protection de l'Etat sont habilitées à utiliser en matière de recherche d'informa- tions. La loi précise que les informations peuvent être récoltées par le biais: – de l'exploitation de sources accessibles au public; – de demandes de renseignements; – de la consultation de documents officiels; – de la réception et de l'exploitation de communications; – d'enquêtes sur l'identité ou le lieu de séjour de personnes; – de l'observation de faits, y compris au moyen d'enregistrements d'images et de sons, dans des lieux publics et librement accessibles; – du relevé des déplacements et des contacts de personnes. Si la loi précise que les recherches d'informations peuvent se dérouler à l'insu de la personne concernée (art. 14, al. 1, LMSI), la loi ne prévoit pas que le SAP puisse intercepter ou donner mandat d'intercepter des communications privées à l'étranger. La loi interdit par ailleurs que les autorités de protection de l'Etat utilisent des mesu- res de contraintes (art. 14, al. 3, LMSI). Or, il ne fait aucun doute, pour la déléga- tion, qu'une interception de communications emporte la contrainte dès lors qu'elle est constitutive d'une ingérence dans le droit au respect de la vie privée. Ce genre d'ingérence est interdit au SAP en droit interne et rien n'indique que le législateur ait été disposé à l'autoriser au-delà des frontières. Les interceptions réalisées à l'étranger sur mandat du SAP ne sauraient se déduire non plus de la «clause générale de police» qui permet au Conseil fédéral d'ordonner des mesures de sécurité en s'appuyant directement sur la Constitution fédérale. De

1402 telles mesures ne peuvent être prises que par le Gouvernement et seulement s'il existe un «danger sérieux, direct et imminent» (art. 36, al. 1, Cst.) ou des «troubles existants ou imminents menaçant gravement l'ordre public, la sécurité extérieure ou la sécurité intérieure» (art. 185, al. 3, Cst.). Les mandats donnés par le SAP à la CGE ne répondent pas à une telle définition. Pour la délégation, les activités déployées par Onyx sur mandat du SAP ne reposent pas, actuellement, sur une base légale formelle suffisamment solide. Cette apprécia- tion est d'ailleurs partagée par l'Office fédéral de la justice dans un avis de droit du mois d'avril 2003 demandé par l'Etat-major général. Dans une lettre du 23 mai 2003, la délégation a exposé à la cheffe du DFJP les problèmes légaux que posent les mandats

d’exploration du SAP. Dans sa prise de position du 23 juin 2003, la cheffe du DFJP a admis les faiblesses actuelles de la base légale et a estimé que la situation juridique devait être corrigée. La cheffe du DFJP a indiqué qu’elle allait procéder en deux temps: dans une première phase, le DFJP a prévu de proposer une révision partielle de l’OMSI avec l’OCGE; dans un second temps, le département présentera une modification de la loi dans le cadre de la deuxième révision de la LMSI. Dans sa lettre à la délégation, la cheffe du DFJP a insisté pour que le SAP puisse continuer à donner des mandats d’exploration à Onyx. Elle a relevé également que les informations fournies par le système, contrai- rement aux surveillances téléphoniques effectuées dans les procédures pénales, ne pouvaient pas être utilisées dans un procès et qu’elles servaient uniquement à des fins de renseignement. Lors de sa séance du 15 octobre 2003, le Conseil fédéral a décidé de corriger partiel- lement le problème dans le sens préconisé par la cheffe du DFJP. En adoptant l’OCGE, le Conseil fédéral a décidé une modification de l’OMSI de manière à donner au SAP une compétence expresse l’autorisant à donner des mandats d’explo- ration à l’étranger (art. 9bis, OMSI). Parallèlement à cela, le Conseil fédéral a décidé l’institution de l’ACI qui veillera à contrôler la légalité et la proportionnalité des mandats d’interception du SAP. La délégation estime que la modification de l’OMSI est un net progrès par rapport à la situation qui prévalait jusqu’alors. Elle représente une solution provisoire politi- quement acceptable pour la DCG et jugée juridiquement défendable par l’Office fédéral de la justice. La création de l’ACI constitue également une mesure permet- tant de compenser le déficit de légalité actuel. Il reste que le vide juridique n’est pas encore comblé totalement. En effet, si l’on peut comprendre qu’il puisse être judicieux de réglementer une matière d’abord par une ordonnance, puis par une loi au sens formel, on ne saurait oublier les conditions posées par la constitution fédérale. Cette dernière exige en effet que toute restriction grave à un droit fondamental, en l’occurrence le respect de la sphère privé, doit être prévue au moins par une loi au sens formel (art. 36 Cst.). Dans le cas présent, le Conseil fédéral a préféré, pour des raisons tout à fait compréhensibles, inverser la hiérarchie des normes préjugeant une solution qui incombe au législateur. Il est vrai que les mandats du SAP sont peu nombreux par rapport à ceux du SRS. Quantitativement, ils ne représentent que 8 % des informations interceptées par Onyx. Sur le plan qualitatif et politique, ils ont une portée nettement supérieure.

1403 La délégation estime qu’il appartient au Parlement de donner rapidement une base légale formelle aux mandats d’interception du SAP, et ce avant l’entrée en phase d’exploitation complète du système Onyx à fin 2005/début 2006. En formulant cette exigence, la délégation veut donner aux mandats d’interception du SAP une base formelle qui soit au même niveau normatif que celle qui est valable pour le SRS. La délégation veut également éviter que la phase d’expérimentation – dans un cadre législatif très lâche – ne crée une situation que le législateur ne pourra plus modifier par la suite et ne constitue un précédent à d’autres mesures plus contraignantes dans le domaine de la protection préventive de l’Etat. Recommandation n° 3 La Délégation des commissions de gestion recommande au Conseil fédéral de présenter, dans son deuxième projet de révision de la LMSI, une disposition lé- gale qui règle les mandats d’interception que le SAP effectue ou mandate en matière de sûreté intérieure. Le Parlement devra être saisi du projet avant la phase d’exploitation complète d’Onyx. Cela étant, la délégation tient à relever qu’elle n’a découvert aucune élément laissant penser que le vide juridique actuel ait permis au SAP de récolter des informations à d’autres fins que celles prévues par la législation. 5.1.3 Légalité des transferts d’informations du CGE au SAP en matière de sûreté intérieure L’art. 99, al.

2bis, LAAM règle clairement les compétences lorsque des informations fortuites43, émanant de l'exploration radio à l'étranger, concernent la Suisse et des usagers suisses. Il est trop tôt aujourd'hui pour porter une appréciation sur cette nouvelle disposition qui n'entrera en vigueur qu'au début de l'année 2004. La délégation veillera à suivre étroitement les échanges d'informations qui auront lieu sur la base de cette disposi- tion. Elle s'assurera notamment à ce que ne soient remises à l'OFP que les informa- tions potentiellement significatives pour la sûreté intérieure ou la poursuite pénale. Elle demandera aussi aux autorités en question de régler par écrit les procédures et de tenir un contrôle précis de la nature et du contenu des informations transmises. Une telle procédure est d'ailleurs prévue à l'art. 5, al. 3, OCGE. Pour l'instant, le nombre d'informations présentant un lien avec des usagers suisses est très faible, soit 0,5 %, pour les mandats donnés par le SRS. Cela signifie que sur mille informations captées par Onyx sur mandat sur SRS, cinq comportaient des informations relatives à la Suisse. Pour la délégation, il s'agit d'un très bon résultat. Pour le SAP, ce taux s'élève à 15 %, ce qui est logique vu son mandat légal.

E. 43

L'OCGE parle, en pareil cas, de «produits annexes», art. 5, al. 3, OCGE.

1404 5.1.4 La compatibilité des interceptions en regard du droit international Les interceptions de communications à l'étranger soulèvent des questions fondamen- tales de droit international général, au regard des principes de territorialité, et de droit international des droits de l'homme en raison des atteintes à la sphère privée. Pour la DCG, les interceptions effectuées par Onyx sur les communications à l'étranger sont problématiques à plus d'un titre. Elles portent en effet sur des usagers qui se trouvent à l'étranger, c'est-à-dire sur le territoire d'un autre Etat. Or, les principes inhérents à la souveraineté territoriale s'opposent à ce qu'un Etat déploie des activités sur le territoire d'un autre Etat en dehors du consentement de ce der- nier. En droit suisse, cette protection est conférée par le code pénal, et notamment par l'art. 271 CP qui prohibe, sur le territoire suisse, les actes exécutés sans droit pour un Etat étranger. Sont considérés comme tels les actes qui, par leur nature ou leur but, ont un caractère officiel44. La question qui se pose est de savoir si une écoute technique à l'étranger constitue une intrusion – et donc une violation du principe de territorialité – ou s'il faut consi- dérer qu'elle s'effectue à partir de la Suisse et qu'elle ne s'accompagne pas d'une violation physique sur le territoire de l'autre Etat. Une troisième solution serait de dire que l'interception a lieu dans l'espace extra-atmosphérique où sont situés les satellites de communication. Il n'y aurait en l'état pas de violation du principe de territorialité étant donné que l'espace extra-atmosphérique appartient au domaine public international45 et qu'il échappe de ce fait aux règles de territorialité. Quelque soit la réponse donnée à ces problèmes de territorialité, force est d'admettre que les écoutes portent atteinte à la vie privée. Elles constituent en effet des ingéren- ces unilatérales d'un Etat dans la vie privée de personnes qui se trouvent sur le territoire d'un autre Etat qui leur accorde sa protection. En droit suisse, cette protec- tion est garantie par la Constitution fédérale (art. 13 Cst.), par le code pénal (notam- ment les art. 179bis à 179septies CP) ainsi que par la législation sur la protection des données. Sur le plan du droit international public, le droit au respect de la vie privée et familiale est inscrit dans de nombreuses conventions comme la Déclaration uni- verselle des droits de l'homme (art. 12), le Pacte ONU II (art. 17) ou la CEDH (art. 8). Il serait donc concevable – théoriquement du moins et abstraction faite que les preuves seraient difficiles à réunir – qu'un Etat ou un particulier saisisse les

juridictions internationales (Cour européenne des droits de l'homme, Comité des droits de l'homme de l'ONU, Cour internationale de justice) pour violation du respect de la vie privée par les autorités suisses46. Pour la délégation, les interceptions réalisées par le système Onyx sur les communi- cations à l'étranger présentent des problèmes juridiques délicats au regard du droit international. De fait, ces problèmes sont inhérents à l'activité de tout service de renseignement et à son caractère clandestin. Ils ne sont pas propres à la Suisse; tous

E. 44
ATF 114 IV 130.

E. 45
Traité du 27.1.1967 sur les principes régissant les activités des Etats en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la lune et les autres corps célestes, RS 0.790.

E. 46
Voir Dimitri Yernault, «De la fiction à la réalité: le programme d'espionnage électronique global ‹Echelon› et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'homme», in: Revue belge de droit international, vol. XXXIII, 2001/1, Editions Bruylant, Bruxelles, p. 137 ss.

1405 les pays qui entretiennent des services de renseignement sont confrontés à la même situation. Certains auteurs estiment que l'espionnage en temps de paix serait contraire au droit international car il implique par définition une violation de la souveraineté territo- riale. D'autres estiment que les activités de renseignement à l'étranger ne sont pas interdites en droit international, mais qu'elles participent tout au plus des actes inamicaux entre Etats qui ne sont pas considérés comme des actes juridiques47. Cette situation peut sembler paradoxale. Alors que tous les pays répriment généra- lement l'espionnage dans leur législation interne (c'est le cas en Suisse des art. 271 à 274 et 301 CP), la question de la légalité de l'espionnage en temps de paix n'est pas tranchée en droit international, que ce soit sur le plan conventionnel ou sur le plan coutumier. Ce constat vaut également pour les interceptions de communications: s'il existe, dans la plupart des Etats, des législations encadrant étroitement les intercep- tions des communications sur leur territoire, aucun régime international ne semble prohiber les interceptions extraterritoriales. Autrement dit, le respect par un Etat de la vie privée des individus s'arrête souvent aux frontières nationales qui sont aussi les limites extrêmes à partir desquelles les impératifs de la sécurité l'emportent sur les libertés publiques. Cette situation qui fait abstraction des libertés fondamentales des personnes situées à l'étranger au profit de la sécurité nationale est compréhensible dans une logique de souveraineté territoriale stricte. Elle apparaît néanmoins difficile à mettre en œuvre dans le do- maine de la surveillance des télécommunications puisque l'Etat chargé de la surveil- lance, la personne surveillée et le processus d'interception ne se déroulent pas sur le même territoire et qu'il est difficile dans ces conditions de déterminer la législation applicable. Pour la délégation, la question de la compatibilité au regard du droit international des interceptions réalisées par la Suisse sur les communications à l'étranger ne peut pas être résolue par des mesures normatives ou conventionnelles, faute de quoi il faut renoncer à avoir un service de renseignement extérieur. Ce problème nécessite une approche politique qui doit être déterminée au cas par cas en fonction des situa- tions qui pourraient se présenter. 5.2 Systèmes de contrôle Pour la

délégation, l'existence d'une base légale réglant les interceptions est une condition nécessaire, mais pas encore suffisante, pour garantir un fonctionnement d'Onyx qui soit conforme aux droits fondamentaux. En effet, l'expérience montre que les activités secrètes sont susceptibles, plus que toutes autres, de conduire à des abus car elles échappent largement aux contrôles traditionnels des contre-pouvoirs, tels la justice ou les médias. C'est pourquoi, dès le début du projet, la délégation a exigé du Conseil fédéral la mise en place d'un système de contrôle destiné à parer à des abus éventuels.

E. 47

Voir Fabien Lafouasse, «L'espionnage en droit international», in: Annuaire français de droit international, XLVII, 2001, CNRS Editions, Paris, p. 64 ss. et les très nombreuses références.

1406 La délégation est intervenue auprès du chef du DDPS et de la Délégation du Conseil fédéral pour la sécurité au printemps 2001 afin de leur demander d'établir un concept de contrôle48. En automne 2001, le chef du DDPS a présenté à la délégation un premier concept de contrôle établi par les services du coordinateur des rensei- gnements. Ce concept a été développé par la suite sur la base des expériences ré- unies. Il devra encore être précisé au fur et à mesure de la mise en exploitation du système. Le système de contrôle actuel fixe toute une série de processus, de documents et des méthodes permettant de surveiller l'exploitation d'Onyx depuis l'établissement des mandats d'exploration jusqu'à l'exploitation des résultats. Il s'inspire de modèles étrangers qui ont fait leur preuve49. Le système de contrôle est composé de trois échelons institutionnels distincts: – Le premier échelon comprend les mandants, en l'occurrence le SRS et le SAP, et les exploitants du système Onyx. Les mandants sont responsables de définir les ordres d'exploration et d'en assurer la légalité et la proportionna- lité. Des procédures détaillées ont été fixées pour le cheminement des infor- mations entre la CGE, le SRS et le SAP. Elles règlent, par exemple, le com- portement à adopter lors d'interceptions fortuites d'informations sur des usagers suisses. Ces informations doivent être masquées ou leur contenu être modifié avant d'être remises au SRS. La CGE, le SRS et le SAP se ren- contrent régulièrement lors de séances afin de discuter des résultats et des problèmes rencontrés dans l'exécution des mandats d'exploration. – Le deuxième échelon de contrôle est constitué par l'autorité de contrôle in- dépendante (ACI). Cette instance de contrôle a une nature interdépartemen- tale. Elle a été créé par le Conseil fédéral le 15 octobre 2003 sur proposition du DDPS. Ses membres sont nommés par la Délégation du Conseil fédéral pour la sécurité sur proposition du chef du DDPS (art. 18, al. 3, OCGE). Le DDPS n'est pas représenté majoritairement dans la commission et n'occupe pas la présidence (art. 18, al. 1, OCGE). L'ACI veille à la légalité et à la proportionnalité des ordres d'exploration en tenant compte des priorités in- hérentes aux besoins des autorités politiques en matière de renseignement (art. 15, al. 1, OCGE). L'ACI peut faire des recommandations écrites au mandant et à la CGE (art. 15, al. 3, let. a, OCGE). Elle peut aussi demander au département du mandant de suspendre des ordres d'exploration qui ne satisfont pas aux principes de légalité et de proportionnalité (art. 15, al. 3, let. b, OCGE). L'ACI doit rendre compte de son activité une fois par année à l'attention de la Délégation du Conseil fédéral pour la sécurité (art. 15, al. 4, OCGE).

L'ACI a été instituée par le Conseil fédéral pour permettre un contrôle des ordres d'exploration qui soit indépendant des mandants. L'autorité de contrôle n'est pas encore opérationnelle; elle devrait entrer en fonction d'ici au début de l'année 2004.

E. 48

Voir en particulier le communiqué de presse de la DCG du 27.3.2001.

E. 49

Voir, par exemple, les directives américaines: «United States Signals Intelligence Directive 18 (USSID 18) – Limitations and Procedures in Signals Intelligence Operations of the United States Sigint System», National Security Agency, du 27.7.1993. Pour plus d'informations, voir James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001, p. 442–449.

1407 – Le troisième échelon est composé des organes directeurs du DDPS et du Conseil fédéral. Il comprend le chef de l'état-major général en tant que supé- rieur hiérarchique de la CGE et de la direction de projet Onyx ainsi que le chef du DDPS en tant que responsable politique du département. Le chef du DDPS exerce une surveillance générale sur Onyx grâce à un système de rap- ports trimestriels mis en place durant l'année 2002. Les rapports à l'intention du chef du DDPS, du chef de l'état-major général et du sous-chef d'état- major de l'aide au commandement indiquent l'état d'avancement du projet Onyx ainsi que les problèmes qui nécessitent une décision. Le chef du DDPS peut également charger son rapporteur pour les questions spéciales ou l'Inspectorat du DDPS afin de réaliser des contrôles ponctuels. Finalement, le chef du DDPS désigne les mandants autorisés (art. 2, al. 3, OCGE) et est informé des propositions et des décisions de suspension d'ordres d'exploration (art. 16, al. 3, OCGE). Par ce biais, il peut également exercer sa surveil- lance sur l'exploitation du système. – La Délégation du Conseil fédéral pour la sécurité est informée chaque année par le chef du DDPS sur les activités de l'ACI (art. 15, al. 4, OCGE). Elle nomme également les membres de l'ACI pour quatre ans (art. 18, al. 3, OCGE). Ces deux compétences lui donnent un droit de regard indirect sur l'utilisation d'Onyx. La délégation est d'avis que le système de contrôle existant permet d'encadrer judicieusement les activités d'Onyx et de limiter les risques d'abus. A l'échelon stratégique, les compétences et les responsabilités entre les autorités politiques et les organes d'exécution sont clairement fixées. A l'échelon opérationnel, il existe une nette séparation des rôles entre les services qui ordonnent les interceptions (SRS, SAP), ceux qui les exécutent (CGE) et ceux qui les contrôlent (ACI). Cette réparti- tion des rôles offre, de l'avis de la délégation, une garantie supplémentaire contre toute atteinte illégale à la vie privée des citoyens. Le système de contrôle mis en place constitue également un cadre adéquat sur lequel la DCG pourra s'appuyer utilement dans l'exercice de son mandat de haute surveil- lance. Le contrôle de la délégation s'effectue d'ailleurs à tous les échelons et à toutes les étapes du processus d'interception depuis la fixation des accords-cadres jusqu'au niveau des produits en passant par les conventions de prestations et les critères pour le filtrage des messages (éléments d'adressage, mots-clefs). Il est encore trop tôt pour porter une appréciation sur le travail de l'ACI. Pour la délégation, cet organe représente un élément-clef du dispositif de contrôle. En effet, il reviendra à cette autorité d'apprécier la proportionnalité des ordres d'exploration et d'opérer ainsi la délicate pesée des intérêts entre les impératifs de sécurité qui fondent la mission des services de renseignement et la protection de la vie privée des personnes à l'étranger dont les communications sont interceptées. Pour la déléga- tion, il est indispensable que l'ACI puisse disposer non seulement d'une autonomie de droit, mais également d'une autorité de fait pour asseoir sa crédibilité dans la pratique. Dans ce contexte, le choix des personnes sera déterminant. La délégation suivra de près la mise en place et le travail de l'ACI. Elle veillera également à ce que le concept de contrôle – axé

aujourd'hui principalement sur des questions de légalité – soit élargi à terme à des contrôles d'efficacité et de qualité.

1408 5.3 Utilité et limites du système Onyx Onyx constitue un investissement particulièrement important du point de vue finan- cier. Aussi la délégation a-t-elle cherché à se faire une idée de la contribution appor- tée par le système par rapport à d'autres formes de collecte d'informations. Evaluer la valeur des informations livrées par Onyx est un exercice complexe. On sait en effet qu'un renseignement de qualité s'obtient rarement sur la base d'une seule source, mais qu'il est le résultat d'un faisceau d'informations multiples. Une information interceptée par Onyx n'a pas de valeur particulière par elle-même. Il faut pouvoir lui assigner une place dans un contexte déjà constitué que cette infor- mation modifie ou renforce sans nécessairement le bouleverser. Le travail d'analyse qui donne une valeur ajoutée à l'information est le résultat de l'interprétation et du recoupement de plusieurs informations provenant de différentes sources. L'évaluation de l'efficacité du système est également rendue difficile par le fait que le système n'est pas encore pleinement opérationnel et que la période prise en consi- dération est relativement courte. Les remarques qui suivent constituent donc un constat à un moment donné. Depuis son entrée en service en avril 2000, Onyx a livré des milliers d'informations, en particulier dans le domaine de la lutte contre la prolifération. Ces données ont été analysées par le SRS et certains résultats ont été mis à disposition des services du Secrétariat d'Etat à l'économie chargés du contrôle des exportations. Actuellement, Onyx représente une source importante d'informations du SRS dans le domaine de la prolifération. De l'avis des services de renseignement et des personnes actives dans le domaine de la lutte contre la prolifération, les informations livrées par Onyx sont utiles. Elles permettent aux services responsables de disposer d'informations de première main et d'être moins dépendants des services de renseignement étrangers. Grâce à Onyx, les services peuvent également, dans certains cas, vérifier la fiabilité des renseigne- ments provenant d'autres sources, les compléter, les préciser, voire les corriger. Les informations recueillies grâce à Onyx constituent également une «monnaie d'échange» utile dans les relations avec des services homologues à l'étranger. Ces échanges s'effectuent en effet sur la base d'un donnant-donnant (principe du «do ut des»). Les services suisses ne peuvent espérer recevoir des informations de leurs partenaires qu'en apportant en contrepartie des informations intéressantes. Les informations recueillies par Onyx constituent donc aussi un instrument permettant d'ouvrir les portes d'autres services de renseignement et d'asseoir la crédibilité des services de renseignement suisses à l'étranger. La délégation a reçu un rapport détaillé comportant plusieurs dizaines d'exemples réels d'informations captées grâce à Onyx. La délégation a pu ainsi se faire une idée précise du type d'informations interceptées et de l'utilisation qui en est faite par les services des renseignement. La délégation a aussi été informée en détail sur plusieurs cas où Onyx a livré au SRS des informations inédites sur différents événements intervenus au Proche et au Moyen-Orient, en Transcaucasie et dans le sous-continent indien. Les cas exposés concernaient pour la plupart des questions liées au transfert illégal de technologies ou de biens à double-usage, au terrorisme international ou au commerce d'armes international.

1409 Grâce à Onyx, le SAP a pu notamment identifier un certain nombre d'entreprises actives dans le domaine des biens à double usage. Ces entreprises n'étaient pas connues auparavant des autorités de contrôle et disposaient d'adresses fictives. En l'état actuel des informations, il semble que les informations livrées par Onyx présentent une importante

valeur ajoutée et que le système a permis d'accroître les capacités des services de renseignement. Ce constat ne doit toutefois pas faire perdre de vue qu'Onyx présente aussi des limites et qu'il est soumis à plusieurs contraintes. Une des limites les plus importantes est due au fait que la grande majorité des com- munications entre pays industrialisés ne transite pas par satellite, mais utilise des infrastructures filaires terrestres ou sous-marines qui ne peuvent pas être intercep- tées. Le développement des câbles à fibres optiques à forte capacité de transmission concentre le trafic des communications sur ceux-ci au détriment des satellites. Selon l'avis de certains ingénieurs, seulement 1 % du trafic téléphonique international transiterait par satellite, principalement pour assurer la connexion vis-à-vis de pays ne possédant pas de bonnes infrastructures filaires terrestres50. Dans les régions à forte densité de communications, seule une très faible part des communications s'effectue par satellite. Malgré ces vastes possibilités, Onyx ne peut être utilisé avec succès que pour l'interception d'une petite partie des communications internationa- les. En revanche, Onyx peut s'avérer utile pour suivre des développements dans des pays momentanément en crise sans infrastructures de communications terrestres. La deuxième limite est représentée par la croissance exponentielle du volume des communications. Cette dernière rend impossible l'interception de tous les messages, et a fortiori leur stockage et leur analyse. Comme il n'est pas possible d'accroître les capacités d'analyse au même rythme que l'accroissement du volume des communi- cations, la part relative des communications qui pourra être interceptée et analysée ira en décroissant. Ce problème va s'accentuer avec la mise en exploitation complète du système. La troisième limite est donnée par l'utilisation toujours plus fréquente par les usa- gers de communications cryptées, ce qui complique et ralentit l'interception et l'analyse. Or, en matière de renseignement, il est essentiel que les informations parviennent rapidement aux autorités chargées de la prise de décision. Une bonne information qui parvient trop tard à son destinataire ne présente en effet aucun intérêt. La quatrième contrainte est représentée par le cadre budgétaire. L'interception de communications fait appel à des technologies extrêmement coûteuses par rapport à d'autres méthodes de collecte d'informations. Cela nécessite donc des investisse- ments importants et réguliers, ne serait-ce que pour adapter les systèmes aux évolu- tions techniques nécessaires. La DCG constate que les coûts de développement d'Onyx ont déjà été multipliés par trois entre 1997 et 2003. La croissance des coûts a été la plus marquée au début du projet, entre 1997 et 2000. Tous ces éléments posent de sérieux défis aux services concernés.

E. 50

Voir le rapport complémentaire du comité permanent de contrôle des services de renseignement sur la manière dont les services belges de renseignemnt réagissent face à l'éventualité d'un réseau «Echelon» d'interceptions de communications, in: «Rapport complémentaire d'activités 1999», Bruxelles, 2000, p. 30.

1410 Pour éviter que le système ne se transforme, faute d'anticipation, en un échec technologique, la délégation invite le DDPS à dresser un tableau complet des risques technologiques et financiers qui menacent la réalisation du projet et des mesures à prendre le cas échéant. Recommandation n° 4 La Délégation des commissions de gestion invite le DDPS à dresser un tableau complet des risques technologiques et financiers qui menacent la réalisation du projet Onyx et des mesures à prendre le cas échéant. De manière plus générale, la délégation est d'avis que les services de renseignement doivent veiller à ne pas s'appuyer uniquement sur le renseignement électronique au détriment d'autres sources

d’informations. En effet, l’efficacité d’un service de renseignement dépend pour beaucoup de la complémentarité de ses sources d’informations. C’est pourquoi, au niveau des efforts et investissements, il convient d’assurer une évolution cohérente et équilibrée des différentes formes de collecte d’informations (COMINT, OSINT, HUMINT, collaboration avec services partenaires) et des capa- cités d’exploitation. Recommandation n° 5 La Délégation des commissions de gestion invite le Conseil fédéral à présenter, pour les services de renseignement, une stratégie sur cinq ans qui expose les efforts et investissements matériels et humains que le DDPS et le DFJP envisa- gent de faire dans le domaine des sources d’informations (OSINT, HUMINT, COMINT, collaboration avec services partenaires) et de leur exploitation. 5.4 Information du Parlement et de l’opinion publique Pour des raisons de confidentialité évidentes, le DDPS s’est toujours montré discret vis-à-vis du Parlement et du public sur le projet Onyx. Alors que le Conseil fédéral a pris la décision de réaliser Onyx en août 1997, les premières informations sur Onyx ont été communiquées à la DCG le 12 janvier 1999 dans une lettre adressée par le sous-chef d’état-major du Groupe des renseignements au président de la délégation. La DCG a reçu ensuite des informations complémen- taires lors d’une séance organisée le 28 janvier 1999 qui faisait d’ailleurs suite à différents articles publiés dans la presse. Après avoir informé la DCG, le DDPS a diffusé, le 1er février 1999, un communiqué de presse officiel dans lequel il présentait brièvement le projet. Le projet a égale- ment été exposé dans des circulaires qui ont été distribuées dans les communes directement concernées par le projet.

1411 Au Parlement, le projet Onyx a été abordé pour la première fois lors de l’examen du message sur l’immobilier 2000 durant la session d’hiver 1999. Ce message proposait aux Chambres différents travaux de transformation de bâtiments dans le cadre du projet Onyx51. Lors des débats consacrés au message sur l’immobilier militaire, puis lors de l’examen du budget 2000 qui a suivi quelques jours plus tard, plusieurs questions ont été posées concernant les buts et les principes de fonctionnement du système52. Onyx a également été discuté au Parlement, une année plus tard, lors de la vente à Verestar des stations satellitaires de Swisscom en octobre 2000. Le sujet a également été traité dans diverses interventions parlementaires. Ces quelques discussions mises à part, le projet Onyx n’a jamais fait l’objet d’une discussion politique au Parlement quant à son opportunité et à son financement. Les investissements, étalés sur plusieurs années, ont été réalisés en recourant à diverses rubriques budgétaires sans que le Parlement ait jamais reçu une vue d’ensemble des coûts totaux du projet. Des chiffres ont certes été avancés par des parlementaires53 et par les médias, mais ils n’ont jamais été confirmés par le DDPS. Ce manque de transparence financière a d’ailleurs été critiqué par le Contrôle fédéral des finances (CDF) dans un rapport de révision54 daté du 15 août 2003, dont la DCG a reçu un exemplaire. Sur la base de ce rapport, la Délégation des finances a demandé des compléments d’information au DDPS après avoir constaté que les coûts du projet allaient vraisemblablement être multipliés par trois. La DCG juge également problématique le fait qu’elle ait été informée du projet Onyx plus de 16 mois après que le Conseil fédéral ait décidé sa réalisation. La délégation est d’avis que ce projet aurait dû lui être communiqué sans délais. Finalement, la délégation estime que l’information du Parlement et du public sur Onyx n’est pas suffisante. Malgré un concept d’information détaillé55, l’information s’effectue le plus souvent au gré des circonstances et en réaction à des événements particuliers ou à la publication d’informations par les médias. La délégation est d’avis que l’ensemble du Parlement et l’opinion publique ont le droit d’être mieux renseignés sur les buts du projet Onyx pour lequel des moyens importants ont été alloués. C’est pourquoi la

délégation invite le DDPS à développer une politique d'informa- tion active sur les tenants et les aboutissants du projet Onyx. Il s'agit de montrer la valeur ajoutée que représente Onyx pour les autorités politiques responsables et d'exposer clairement sa légitimité démocratique. Le présent rapport est un premier pas dans ce sens.

51 Voir ch. 212 du message du Conseil fédéral du 18.8.1999 sur l'immobilier militaire (FF 1999 7821). 52 BO 1999 E 1015, BO 1999 N 2460 et BO 1999 N 2508. 53 BO 1999 N 2530. 54 Bericht an den Rüstungs- und Generalstabschef über die Prüfung des Projektes elektroni- sche Aufklärungssystem für Satellitenverbindungen (SATOS/ONYX), vom 11.8.2003, p. 1 (n'existe qu'en langue allemande, non publié). 55 Concept d'information du chef de l'Etat-major général «EA von Satellitenverbindungen», du 22.1.1999 (n'existe qu'en langue allemande, non publié).

1412 Recommandation n° 6 La Délégation des commissions de gestion invite le DDPS à mettre en place une politique d'information ouverte et régulière sur les activités déployées par le système Onyx. 5.5 La vente des antennes de Swisscom à l'opérateur Verestar Lors de sa visite à Zimmerwald le 15 septembre 2000, la délégation a été informée par le chef de l'état-major général que l'entreprise Swisscom avait l'intention de céder à un opérateur étranger certaines installations et bâtiments qui touchaient à la défense générale de la Confédération. Cela concernait tout le secteur radiodiffusion (secteur «broadcasting») de Swisscom ainsi que les stations terriennes de communi- cation par satellite de Loèche qui jouxtaient les installations Onyx de la CGE. Le chef de l'état-major général avait indiqué à la délégation qu'il avait eu connaissance de la décision de Swisscom par hasard et que le DDPS n'avait pas été impliqué dans le projet de vente. Le même jour, la délégation est intervenue auprès du Conseil fédéral en lui faisant part de son extrême préoccupation. Elle a invité ce dernier à prendre sans délais toutes les mesures utiles visant à défendre les intérêts légitimes de la Confédération vis-à-vis du conseil d'administration et de la direction générale de Swisscom. Quelques jours plus tard, la question a également été débattue au sein de la Commis- sion de gestion du Conseil des Etats et des Commissions de la politique de sécurité du Conseil national et du Conseil des Etats. Elle a également fait l'objet de différen- tes interventions parlementaires56 et de discussions aux conseils57. Pour la délégation, seule la vente des stations au sol de Loèche posait problème puisque les antennes du système Onyx étaient situées sur un terrain dont Swisscom était propriétaire. De plus, le DDPS avait conclu, en date du 20 mars 2000, un contrat de dix ans avec Swisscom qui prévoyait que l'entreprise assurerait l'alimen- tation en eau et en électricité des installations Onyx ainsi que différents travaux d'entretien au profit de l'Etat-major général. Avec la vente des installations de Swisscom à l'opérateur américain Verestar, il a fallu renégocier le contrat et scinder les installations à usage commercial de celles exploitées par le DDPS.

56 00.5180 Heure des questions. Question. Swisscom. Vente d'émetteurs, du 2.10.2000 (BO 2000 N 1055); 00.5181 Heure des questions. Question. Swisscom/DDPS. Vente d'immeubles, du 2.10.2000 (BO 2000 N 1056); 00.5184 Heure des questions. Question. Swisscom. Vente des activités de radiodiffusion, du 2.10.2000 (BO 2000 N 1056); 00.3518 Interpellation. Swisscom. Vente du Broadcasting service, du 4.10.2000 (BO 2000 E 799); 00.5202 Heure des questions. Question. Sort du secteur Broadcasting Services de Swisscom, du 4.12.2000 (BO 2000 N 1348). 57 Voir notamment les débats au Conseil des Etats, du 30.11.2000 (BO 2000 E 799).

1413 Une solution a été trouvée entre le DDPS et Swisscom. Cette solution a nécessité un redécoupage du terrain de Loèche et une cession de plusieurs parcelles à la Confé- dération. L'acte de vente a été établi à Loèche le 15 novembre 2000 et le registre foncier modifié, en conséquence, le 3 janvier 2001 – avec effet au 1er janvier 2001 – lors de la conclusion de la transaction et de la remise des installations à Verestar. A l'heure actuelle, toutes les composantes classifiées du système Onyx sont inté- grées dans des installations du DDPS et il n'existe aucune interface entre ces instal- lations et les installations exploitées par Verestar. Le seul lien existant encore entre les deux sites concerne l'alimentation en électricité et en eau. Une alimentation indépendante des installations Onyx en eau et en électricité est actuellement à l'étude. La vente par Swisscom de ses installations à Verestar a provoqué un retard de 9 mois dans la réalisation du projet Onyx. Sinon, le système n'a pas été affecté par la vente de la station d'émission. La délégation constate avec satisfaction que, malgré les problèmes rencontrés au début de l'opération, le DDPS est parvenu à préserver les intérêts et la sécurité du système Onyx. 5.6 Participation supposée du système Onyx à un réseau d'interception international Ces dernières années, plusieurs rapports officiels et certains médias ont relevé que le système Onyx ferait partie d'un réseau d'interception multinational. Cette hypothèse a été avancée, par exemple, par le rapport de l'Assemblée nationale française d'octobre 2000. Dans ce document, il est indiqué que le réseau Echelon aurait inclus dans son système «(…) la Suisse qui envisage l'installation sur son territoire de stations de réception (…)»58. Le rapport précise également, citant un député, que le système « Echelon (…) a tissé une ‹toile d'araignée› planétaire avec des emprises (…) en Suisse»59. En ce qui concerne le Parlement européen, son rapport du 11 juillet 2001 évoque les propos de Duncan Campbell, un des journalistes les plus connus en matière d'interceptions de communications. Selon lui, les «capacités d'interception de plu- sieurs pays européens (se seraient) nettement accrues au cours des dernières années – notamment en Suisse, au Danemark et en France. On observe d'ailleurs un renfor- cement de la coopération bilatérale et multilatérale dans le domaine du renseigne- ment»60. Quant au rapport du Parlement belge, datant du 25 février 2002, il indique, invo- quant certaines sources, que la Suisse collaborerait avec les Etats-Unis et le Royaume-Uni dans la mise en place de son système d'interception61. Le rapport précise également que l'Allemagne et la France ne participeraient pas à l'opération.

58 Rapport français, p. 25. 59 Rapport français, p. 66. 60 Rapport européen, p. 74. 61 Rapport belge, p. 37.

1414 A l'analyse, il apparaît que la plupart des informations véhiculées par les rapports des parlements français, européen et belge trouvent leur origine dans des propos de Duncan Campbell qui ont été déformés. En effet, Duncan Campbell n'a jamais affirmé qu'il existait une collaboration entre la Suisse et Echelon, ni déclaré qu'il pouvait en apporter la preuve. Duncan Campbell relève seulement que la collabora- tion entre Etats est courante en matière d'exploration électronique62 et que la Suisse n'échappe certainement pas à la règle. Dans un article publié dans la presse britanni- que, il souligne également que les capacités réunies du Danemark et de la Suisse seraient en mesure d'apporter à Echelon davantage d'informations que celles livrées par les capacités réunies du Canada, de l'Australie et la Nouvelle-Zélande63, sans affirmer toutefois qu'une telle collaboration existe ou ait existé. Les supputations quant à une possible participation d'Onyx au réseau Echelon se sont ravivées à l'automne 2000, lors de la vente par Swisscom de ses stations ter- riennes de communication par satellite à l'opérateur américain Verestar (voir ch. 5.5, ci-dessus). La

société Verestar est une filiale de l'un des principaux exploitants et concepteurs de services de radiodiffusion en Amérique du Nord. Verestar dispose d'une vaste clientèle dont le Département d'Etat américain et le Département de la défense américain. Pour certains observateurs, l'acquisition des antennes de Swiss- com par Verestar ainsi que leur proximité par rapport aux antennes du système Onyx étaient autant d'indices laissant supposer une collaboration entre les Etats-Unis et la Suisse, voire une participation d'Onyx au réseau Echelon. Certains parlementaires se sont d'ailleurs inquiétés de cette situation et des conséquences qu'une telle collabo- ration pourrait présenter pour la neutralité suisse64. La délégation ne peut confirmer aucune des suppositions faisant état d'une intégra- tion d'Onyx dans un réseau international d'écoute comme Echelon. En effet, tout au long de ses travaux, la délégation n'a trouvé aucun élément attestant une possible intégration du système Onyx dans un quelconque réseau d'interception international. D'ailleurs, s'agissant plus particulièrement d'Echelon, il est difficile d'imaginer quels avantages ce réseau pourrait tirer d'une collaboration avec la Suisse. En effet, Echelon disposerait déjà en Europe d'une couverture d'antennes suffisantes. Pour la Suisse, une telle collaboration serait d'ailleurs incompatible avec sa politique de neutralité. En l'état actuel des informations, la délégation est en mesure d'affirmer que le système Onyx est un instrument à caractère strictement national qui s'appuie uni- quement sur des infrastructures situées sur territoire suisse. Onyx fonctionne de manière autonome et ne dispose pas d'interfaces techniques avec un autre système étranger. Il n'existe pas non plus, à la connaissance de la DGC, d'accord de collabo-

62 Echelon mis à part, cette assertion de Duncan Campbell est démentie par d'autres sources: «Force est de constater qu'il n'existe pour l'heure aucune véritable coopération technique dans (le) domaine (de l'exploration électronique), chaque Etat considérant que la maîtrise de la situation électromagnétique sur une zone ressortit à sa souveraineté», in: «Renseignement européen: les nouveaux défis – réponse au rapport annuel du Conseil», Assemblée de l'Union de l'Europe occidentale, 48e session, document A/1775, Paris, 4.6.2002, p. 19. 63 Duncan Campbell, «Fight over Euro-intelligence plans», in: The Guardian, 6.8.2001. 64 00.3629 Interpellation. Antennes satellite de Loèche, du 28.11.2000 (BO 2001 N 365); 01.3189 Postulat. Satos 3. Vente par Swisscom du terrain de Loèche, du 23.3.2001 (classé sans traitement après deux ans); 03.1046 Question ordinaire. Espionnage économique sur le territoire suisse au profit des Etats-Unis, du 8.5.2003 (BO 2003 N 1758).

1415 ration avec un autre État en matière d'interception des communications par satelli- tes, ni d'échanges automatisés de données brutes avec l'étranger. Affirmer qu'Onyx est indépendant de tout système étranger sur le plan technique ne revient pas à dire qu'il ne profite pas, pour son développement ou son exploitation, d'informations provenant de l'étranger. Comme cela a été dit plus haut, les services de renseignement et la CGE entretiennent des contacts bilatéraux réguliers avec leurs homologues étrangers. Les échanges d'informations s'effectuent au cas par cas et peuvent porter sur des données techniques (bandes de fréquence, canaux de transmission, analyse du trafic, etc.) ou des éléments d'adressage tels des numéros d'appel. Ces informations permettent souvent de mieux définir les cibles de l'explo- ration et de faciliter la collecte d'informations. Ces contacts ainsi que les pays avec lesquels ils ont lieu sont soumis à l'autorisation du Conseil fédéral65. La délégation en a également connaissance et effectue des contrôles ponctuels réguliers. La délégation connaît également les pays de provenance des différents systèmes qui composent Onyx. 6 Conclusions La Délégation des commissions de gestion constate

que: 1. Plusieurs Etats ont développé ces dernières années des systèmes d'inter- ception des communications. 2. Le système Onyx permet de capter les communications internationales civi- les et militaires qui transitent par satellites. Il est exploité par la Division de la conduite de la guerre électronique (CGE) qui est une division de l'Etat- major général. 3. Le système est entré en service en avril 2000 et fonctionne actuellement de manière expérimentale. Il entrera en phase opérationnelle dans le courant l'année 2004 et sera en exploitation complète fin 2005/début 2006. 4. Le système collecte des informations touchant uniquement à la politique de sécurité de la Suisse et ne fait pas de surveillance économique, technologi- que ou scientifique. 5. Le système procède à des interceptions de communications uniquement à l'extérieur des frontières. 6. Le système respecte les droits fondamentaux et les libertés des personnes en Suisse puisque les interceptions de communications entre des usagers situés en Suisse sont prohibées. 7. Le système est utilisé uniquement dans le domaine du renseignement. Les informations recueillies ne peuvent pas, en l'état actuel du droit, être utili- sées comme preuves dans une procédure pénale. 8. Les interceptions ordonnées par le Service de renseignement stratégique (SRS) dans le domaine de la sûreté extérieure de la Suisse reposent sur une base légale formelle jugée suffisante.

65 Voir l'art. 6, al. 2, Orens, et l'art. 26, al. 2, LMSI.

1416 9. Les interceptions ordonnées par le Service d'analyse et de prévention (SAP) dans le domaine de la sûreté intérieure de la Suisse reposent sur une base lé- gale formelle qui n'est pas suffisamment solide. 10. Les transferts d'informations entre la CGE, le SRS et le SAP reposent sur des bases légales et des conventions clairement établies. 11. Les interceptions effectuées par Onyx sur les communications à l'étranger présentent des problèmes juridiques délicats au regard du droit international, tant sous l'angle du principe de territorialité que sous celui du respect à la vie privée et du secret des communications. 12. Il existe un système de contrôle adéquat permettant à tous les échelons responsables, opérationnels et politiques, de surveiller les activités d'inter- ception et de limiter les risques d'abus. 13. Il existe une volonté politique manifeste du chef du DDPS et de la Déléga- tion du Conseil fédéral pour la sécurité de donner un cadre juridique et poli- tique précis aux activités d'interception. 14. Les mandats d'interception sont contrôlés sous l'angle de la légalité et de la proportionnalité par une autorité interdépartementale: l'autorité indépen- dante de contrôle (ACI). 15. Il existe une séparation claire des rôles entre les services qui ordonnent les interceptions (SRS, SAP), ceux qui les exécutent (CGE) et ceux qui les contrôlent (ACI). 16. Les informations interceptées par Onyx présentent, pour les services concer- nés, une valeur ajoutée importante. Ces informations permettent d'augmen- ter les capacités des services de renseignement et d'asseoir leur crédibilité à l'étranger. 17. Le système est soumis à des contraintes techniques et financières qui sont susceptibles à terme d'en limiter les potentialités. 18. La politique d'information du DDPS envers le Parlement et le public sur les activités déployées par Onyx est jugée comme étant particulièrement rete- nue. 19. Le système Onyx est un instrument à caractère strictement national s'ap- puyant uniquement sur des infrastructures situées en territoire suisse. Il n'existe aucun élément attestant une possible intégration du système Onyx dans un quelconque réseau d'interception international. Au vu de ce qui précède, la Délégation des commissions de gestion : 1. recommande au Conseil fédéral d'examiner l'opportunité d'introduire dans la LAAM une référence explicite aux interceptions de communications à l'étranger. Celle-ci devrait indiquer également que les écoutes ne peuvent porter que sur des communications à l'étranger et faire mention des disposi- tions du code pénal réprimant l'interception de

communications d’usagers en Suisse; 2. recommande au Conseil fédéral d’examiner la conformité à la CEDH de la législation relative aux activités d’interception des communications à l’étranger et, au besoin, de lui apporter les adaptations nécessaires;

1417 3. recommande au Conseil fédéral de présenter, dans son deuxième projet de révision de la LMSI, une disposition légale qui règle les mandats d’inter- ception que le SAP effectue ou mandate en matière de sûreté intérieure. Le Parlement devra être saisi du projet avant la phase d’exploitation complète d’Onyx; 4. invite le DDPS à dresser un tableau complet des risques technologiques et financiers qui menacent la réalisation du projet Onyx et des mesures à pren- dre le cas échéant; 5. invite le Conseil fédéral à présenter, pour les services de renseignement, une stratégie sur cinq ans qui expose les efforts et investissements matériels et humains que le DDPS et le DFJP envisagent de faire dans le domaine des sources d’informations (OSINT, HUMINT, COMINT, collaboration avec services partenaires) et de leur exploitation; 6. invite le DDPS à mettre en place une politique d’information ouverte et ré- gulière sur les activités déployées par le système Onyx. 7 Suite des travaux La Délégation des commissions de gestion prie le Conseil fédéral de prendre posi- tion sur le présent rapport et sur les recommandations qu’il contient d’ici à la fin mars 2004. 10 novembre 2003 Au nom de la Délégation des commissions de gestion

Le président: Alexander Tschäppät, conseiller national Le secrétaire: Philippe Schwab Les Commissions de gestion ont pris acte du présent rapport le 21 novembre 2003 et en ont approuvé la publication. 21 novembre 2003 Au nom des Commissions de gestion

Le président de la Commission de gestion du Conseil des Etats: Michel Béguelin, député au Conseil des Etats La présidente de la Commission de gestion du Conseil national: Brigitta M. Gadient, conseillère nationale

1418 Abréviations ACI Autorité de contrôle indépendante ADM Armes de destruction massive ATF Arrêt du Tribunal fédéral BND Bundesnachrichtendienst (service de renseignement extérieur allemand) CDF Contrôle fédéral des finances CdG Commissions de gestion des Chambres fédérales CEDH Convention de sauvegarde des droits de l’homme et des libertés fondamentales (Convention européenne des droits de l’homme), du 4 novembre 1950) (ratifiée par la Suisse avec effet au 28 novembre 1974) CGE Division de la conduite de la guerre électronique CIA Central Intelligence Agency (service de renseignement extérieur des Etats-Unis) COMINT Communications intelligence (exploration radio) COMSAT Communications par satellites CP Code pénal suisse, du 21 décembre 1937 CPS-N Commission de la politique de sécurité du Conseil national Cst. Constitution fédérale de la Confédération suisse, du 18 avril 1999 DCG Délégation des commissions de gestion des Chambres fédérales DDPS Département fédéral de la défense, de la protection de la population et des sports DFE Département fédéral de l’économie DFJP Département fédéral de justice et police DGSE Direction générale de la sécurité extérieure (service de renseigne- ment extérieur français) DSD Defense Signals Directorate (agence australienne d’interception des communications) ELINT Electronic intelligence (exploration électronique) FBI Federal Bureau of Investigations (service de renseignement intérieur des Etats-Unis) GCHQ Government Communications Headquarters (agence britannique d’interception des communications) HUMINT Human intelligence (renseignement humain) LAAM Loi fédérale sur l’armée et l’administration militaire, du 3 février 1995 LMSI Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, du 21 mars 1997 LREC Loi fédérale sur la procédure de l’Assemblée fédérale, ainsi que la forme, la publication et l’entrée en vigueur des actes législatifs (loi sur les

rapports entre les conseils), du 23 mars 1962

1419 LSCPT Loi fédérale sur la surveillance de la correspondance par poste et télécommunication, du 6 octobre 2000 LTC Loi fédérale sur les télécommunications, du 30 avril 1997 NSA National Security Agency (agence américaine d'interception des communications) OCGE Ordonnance sur la conduite de la guerre électronique, du 15 octobre 2003 OMSI Ordonnance sur les mesures visant au maintien de la sûreté intérieure, du 27 juin 2001 Onyx Système suisse d'interception des communications par satellites Orens Ordonnance sur le renseignement du Département fédéral de la défense, de la protection de la population et des sports (Ordonnance sur le renseignement), du 4 décembre 2000 OSINT Open source intelligence Pacte ONU II Pacte international relatif aux droits civils et politiques, du 16 décembre 1966 (ratifié par la Suisse avec effet au 18 septembre 1992) SAP Service d'analyse et de prévention SATOS-3 Ancienne dénomination du projet Onyx SIGINT Signals intelligence (exploration des signaux) SRS Service de renseignement stratégique STOA Science and Technology Options Assessment Panel (Bureau d'évaluation des choix scientifiques et technologiques, service de la Direction générale des études du Parlement européen) UE Union européenne

1420 Annexe 1 Interceptions des télécommunications par les autorités suisses

Bases légales Finalité des interceptions et restrictions Autorités habilitées à donner des ordres d'interception Autorités de surveillance Voies de recours Interceptions de communications en Suisse

En matière pénale (procédure pénale fédérale ou cantonale ou lors de l'exécution d'une demande d'entraide pénale internationale) LSCPT, OSCPT Art. 3 LSCPT – Existence de graves soupçons – Gravité de l'acte justifiant la surveil- lance – Les autres mesures d'instruction sont restées sans succès ou n'auraient aucune chance d'aboutir – Liste exhaustive des actes punissables permettant d'effectuer une sur- veillance Art. 6 LSCPT – Procureur général de la Confédération – Juges d'instruction fédéraux ou militai- res – Autorités compéten- tes en vertu du droit cantonal – Directeur de l'OFJ (dans les cas d'extradition) – Autorités fédérales ou cantonales qui traitent les deman- des d'entraide judi- ciaire Art. 7 LSCPT – Président de la Chambre d'accusation du Tri- bunal fédéral, si l'ordre d'interception émane d'une autori- té civile de la Confédération – Président du Tribu- nal militaire de cas- sation, s'il émane d'un juge d'instruction mili- taire – Autorité judiciaire désignée par le can- ton, s'il émane d'une autorité can- tonale Art. 10 LSCPT En général, communication de l'interception aux personnes surveillées à l'issue de la surveil- lance et possibilité d'interjeter recours contre la mesure

En matière de renseignement Prohibée (Art. 179octies CP), à l'exception des mesures qui pourraient être prises par le Conseil fédéral en vertu de la clause générale de police (art. 36, al. 1, et art. 185, al. 3, Cst.)

1421

Bases légales Finalité des interceptions et restrictions Autorités habilitées à donner des ordres d'interception Autorités de surveillance Voies de recours Interceptions des communications à l'étranger

En matière pénale Prohibée (souveraineté territoriale pour des actes à caractère officiel et pour les mesures de contrainte)

En matière de renseignement Art. 99 LAAM et OCGE – Uniquement pour obtenir des informa- tions utiles à la poli- tique de sécurité (art. 2, al. 2, OCGE) – L'exploration ne peut pas avoir pour cible des usagers suisses (art. 5, al.1, OCGE) Les services expressé- ment autorisés par le chef du DDPS (art. 2, al. 3 OCGE) – Autorité administra- tive indépendante de contrôle (ACI, art. 15 OCGE) – Chef du DDPS (art. 2, al. 3, art. 15, al. 4, art. 15. al.3 let b, art. 16, al. 3, OCGE) – Autres chefs de départements (art 15, al. 3, let. b) – Délégation du Conseil fédéral pour la sécurité (art. 15, al. 4, art. 18, al. 3, OCGE) – Conseil fédéral – Délégation des Commissions de gestion Non-prévues en droit interne (éventuelle- ment en droit con- ventionnel au titre de l'art. 8 CEDH ou de l'art. 17 du pacte ONU II)

1422 Annexe 2 Liste des personnes entendues (fonction exercée au moment des auditions) Borchert, Heiko Expert de l'inspectorat du DDPS, DDPS Bühler, Jürg S. Remplaçant du chef du Service d'analyse et de prévention, Office fédéral de la police, DFJP Ebert, Edwin Divisionnaire, sous-chef d'état-major de l'aide au commandement, Etat-major général, DDPS Graf, Urs Directeur suppléant du Service de renseignement stratégi- que, DDPS Hofmeister, Albert Chef de l'inspectorat du DDPS, DDPS Keckeis, Christophe Commandant de corps, chef de l'Etat-major général (depuis le 1er janvier 2003), DDPS Keller, Martin (†) Chef de l'Inspectorat et projets du DFJP, DFJP Kreiliger, Ivo Remplaçant du coordinateur des renseignements, Bureau d'appréciation de la situation et de détection précoce Leuthold, Christian Division de la conduite de la guerre électronique, Groupe de l'aide au commandement, Etat-major général, DDPS Nydegger, Kurt Chef de la division de la conduite de la guerre électronique, Groupe de l'aide au commandement, Etat-major général, DDPS Ogi, Adolf Conseiller fédéral, chef du DDPS Regli, Peter Divisionnaire, sous-chef d'état-major des renseignements, Etat-major général, DDPS Rüdin, Jacques Rapporteur du chef du DDPS pour les questions spéciales, DDPS Scherrer, Hans-Ulrich Commandant de corps, chef de l'Etat-major général (jus- qu'au 31 décembre 2002), DDPS Schmid, Samuel Conseiller fédéral, chef du DDPS Stuber, Peter Rapporteur du chef du DDPS pour les questions spéciales, DDPS Von Daeniken, Urs Chef du Service d'analyse et de prévention, Office fédéral de la police, DFJP Von Orelli, Martin Divisionnaire, sous-chef d'état-major des renseignements (en remplacement), Etat-major général, DDPS Wegmüller, Hans Directeur du Service de renseignement stratégique, DDPS Werz, Bernard Remplaçant du chef de l'Inspectorat et des tâches spéciales, DFJP Wyss, Othmar Remplaçant du chef du domaine «commerce mondial», Secrétariat d'Etat à l'économie, DFE La DCG a également entendu trois collaborateurs du SRS dont elle a décidé de ne pas communiquer les identités.