Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Affaire Crypto AG

Rapport de la Délégation des Commissions de gestion des Chambres fédérales

du 2 novembre 2020

L'essentiel en bref

À partir de l'automne 1993, le Service de renseignement stratégique (SRS) a réussi à obtenir des informations fiables au sujet de la société Crypto AG. Il a ainsi appris que celle-ci appartenait à des services de renseignement étrangers et exportait des appareils «vulnérables», dont le cryptage pouvait être décodé moyennant un minimum d'efforts. Afin de pouvoir décoder lui-même le cryptage de tels appareils, le SRS a commencé à se procurer des informations techniques sur les procédures de cryptage utilisées ainsi que des listes de clients de la société. Plus tard, alors que le SRS avait été transformé en office fédéral civil, il a été possible de garantir un accès fiable à ces connaissances avec l'accord des services de renseignement américains.

Sur le plan juridique, la Délégation des Commissions de gestion (DélCdG) considère qu'il s'agissait d'une collaboration en matière de renseignement telle qu'elle était prévue à l'époque dans la loi sur l'armée et qu'elle l'est aujourd'hui dans la loi fédérale sur le renseignement (LRens). Le fait que le SRS et les services américains agissaient d'un commun accord implique aussi une coresponsabilité des autorités suisses dans les activités de Crypto AG. Juridiquement, il était permis au SRS et à un service étranger d'utiliser, ensemble, une entreprise sise en Suisse afin de rechercher des informations sur l'étranger. Vu la grande portée politique de cette collaboration, la DélCdG est toutefois d'avis qu'il est regrettable que, avant la cheffe actuelle du Département fédéral de la défense, de la protection de la population et des sports (DDPS), aucun de ses prédécesseurs n'ait été informé de cette opération.

En outre, les renseignements que possédait le SRS au sujet de Crypto AG n'auraient pas dû être cachés aux responsables politiques lors de l'affaire Bühler, sur laquelle la Police fédérale (PF) a mené l'enquête au cours des années 1994 et 1995. Comme le chef de l'époque du Département militaire fédéral (DMF) l'a expliqué à la DélCdG, il n'a pas non plus appris la vérité sur Crypto AG par d'autres voies. La délégation n'a pas pu confirmer les allégations selon lesquelles les investigations de la PF auraient été influencées par des responsables politiques. Au contraire, le chef du Département fédéral de justice et police (DFJP) s'est efforcé de faire la lumière sur la question des véritables propriétaires de la société. En fin de compte, la PF a toutefois dû mettre un terme à son enquête sans avoir pu répondre à cette question.

En 1994, la DélCdG a demandé à plusieurs reprises à la PF de l'informer des investigations en cours. Toutefois, à l'instar des supérieurs militaires et politiques du SRS, elle n'a pas eu connaissance des informations recueillies par le service de renseignement extérieur au sujet de Crypto AG. La société n'a pas non plus été mentionnée dans les renseignements fournis par le DDPS à l'organe de haute surveillance lorsque celui-ci s'est spécifiquement penché sur le thème de la cryptologie, en 2007 et en 2009.

Les dossiers opérationnels du SRS et de la PF, que le Service de renseignement de la Confédération (SRC) conservait dans une installation K réaménagée, se sont en particulier avérés très précieux pour l'inspection de la DélCdG. Ces dossiers doivent encore être archivés de manière conforme aux prescriptions. Cependant, étant donné la pratique des services de renseignement en matière d'archivage, rien ne garantit que d'autres documents importants soient encore disponibles. Dans certains cas, la

destruction de tels documents était en partie permise par les dispositions légales alors que dans d'autres, elle a constitué une violation des prescriptions en vigueur. Ainsi, de 2011 à 2014, le SRC détruisait encore des documents découlant d'échanges avec des services partenaires étrangers au lieu de les conserver en interne conformément aux prescriptions. Au cours de l'inspection, il s'est avéré que la destruction de dossiers par le service de renseignement ne constituait pas un moyen éprouvé de protéger les sources et risquait au contraire de mettre d'anciennes sources en danger lorsque les autorités agissent sans connaître leur existence.

Les entreprises et les organisations qui exercent une activité sur le territoire suisse profitent, à l'étranger, de l'image de la Suisse, en sa qualité d'État neutre. Des services étrangers peuvent donc avoir intérêt à effectuer des opérations de renseignement au détriment d'autres États en se cachant derrière une société suisse. Dans certaines conditions, les activités de la société concernée peuvent alors représenter des éléments constitutifs d'espionnage au préjudice des États tiers. D'après le droit en vigueur, une telle opération est toutefois admissible si un service étranger utilise une entreprise suisse en collaboration avec le SRC pour rechercher des renseignements sur l'étranger (cf. art. 34, al. 2, LRens). La DélCdG considère que, lorsqu'une telle opération doit être menée, il convient de procéder préalablement à une évaluation politique des conséquences qu'elle peut avoir pour la Suisse, mais aussi pour les éventuels collaborateurs concernés. Le Conseil fédéral devrait donc clarifier la question de principe de savoir quelle marge de manœuvre il souhaite laisser au DDPS à ce sujet.

L'analyse de l'affaire Crypto AG montre que des entreprises placées sous l'influence de services de renseignement étrangers peuvent produire des appareils utilisant des procédures de cryptage vulnérables. La DélCdG part toutefois du principe que Crypto AG n'a jamais livré d'appareils de cryptage «vulnérables» aux autorités suisses. Il est cependant important aussi que les autorités suisses contrôlent les appareils qu'elles achètent et même exercent une influence sur leur conception. Or, cela n'est possible qu'avec des fournisseurs qui développent et produisent leurs appareils en Suisse. Pour des raisons de sécurité, la Confédération ne doit pas acquérir de solutions de cryptage auprès de fournisseurs étrangers. Depuis le début, le Conseil fédéral n'a pas accordé l'importance requise au fait que les fournisseurs indigènes sont indispensables pour que les autorités suisses puissent disposer de techniques de cryptage sûres. En tant que département responsable de ce domaine, le DDPS n'a pas suffisamment tôt analysé les risques pour la sécurité de l'approvisionnement et adressé son appréciation au Conseil fédéral.

Le fait que le SRS avait accès à des informations concernant la société Crypto AG a été un secret bien gardé au sein de sa direction. Lors de la création du SRC, cette information n'a pas été transmise à son directeur. Lorsque, quelques années plus tard, celui-ci en a été informé, il a toutefois rejeté toute responsabilité à ce sujet.

Ce n'est que sous l'autorité du directeur actuel du SRC qu'un bilan de la situation a été établi, à l'été 2019, ce alors que le directeur n'avait pas été informé de la situation par son prédécesseur et que le SRC n'avait pas encore appris que des médias effectuaient des recherches sur Crypto AG. Le directeur du SRC n'a toutefois pas exploité cet avantage en termes d'informations pour faire procéder à un examen de l'évolution

des relations entre les organisations qui avaient précédé le SRC, les services de renseignement américains et la société Crypto AG. Au lieu d'évaluer le contexte juridique et la portée politique de l'affaire, le SRC s'est contenté de minimiser son importance pour le service actuel.

Même le DDPS, qui avait déjà averti le Conseil fédéral et la DélCdG en novembre 2019, n'a pas réalisé que des mesures s'imposaient au niveau politique. Le groupe de travail interdépartemental que le département avait également mis en place n'a quant à lui pas pu soutenir efficacement les responsables politiques en raison de la rétention d'informations pratiquée par le SRC dans cette affaire qui prenait de l'ampleur.

Dans sa proposition destinée à la séance du Conseil fédéral du 20 décembre 2019, le DDPS a affirmé que les informations alors disponibles étaient insuffisantes pour mener une discussion sur le fond de l'affaire Crypto AG. Cette constatation n'était toutefois plus exacte depuis la découverte de dossiers dans l'installation K, dont le DDPS a fait part au Conseil fédéral. Étant donné que le SRC n'avait pas encore évalué ces dossiers volumineux avant la séance du Conseil fédéral, ce dernier a décidé d'instituer un comité d'experts externe chargé de clarifier les faits, pensant qu'il s'agissait d'une affaire purement historique. Ainsi, dès le départ, le Conseil fédéral n'a pas assumé la conduite stratégique dans le cadre de la gestion de l'affaire Crypto AG.

Lorsque la DélCdG a entamé son inspection, le 13 février 2020, l'ancien juge fédéral Niklaus Oberholzer était déjà en fonction depuis un mois en qualité d'expert externe, sur mandat du Conseil fédéral, sans toutefois avoir obtenu l'accès aux dossiers découverts dans l'installation K. Après que la DélCdG eut demandé tous les documents pertinents du SRC, elle a constaté que l'affaire Crypto AG revêtait bien plus qu'un aspect purement historique et que son importance était des plus actuelles. Par conséquent, le choix du DDPS d'enquêter séparément sur les aspects historique et actuel de l'affaire s'est avéré peu judicieux. Eu égard aux liens étroits entre les différentes enquêtes, la DélCdG a jugé nécessaire de s'entretenir avec la cheffe du DDPS au sujet de la coordination des travaux avant que ceux-ci ne soient poursuivis. Toutefois, lorsque le DDPS a étendu le champ de recherche de l'enquête Oberholzer, ce avant la date à laquelle était prévu l'entretien avec la DélCdG, cette dernière a révoqué, le 21 février 2020, l'autorisation qu'elle avait donnée pour le mandat confié par le Conseil fédéral à M. Oberholzer. Celui-ci s'est ensuite penché, en tant que chargé d'enquête de la DélCdG, sur les aspects de l'affaire Crypto AG liés au renseignement, dont il a rendu compte à la DélCdG dans un rapport secret.

Le 25 février 2020, la DélCdG a discuté de la révocation de l'autorisation avec la cheffe du DDPS. La correspondance qui s'est ensuivie avec le Conseil fédéral a débouché sur une rencontre, le 25 mai 2020, avec la présidente de la Confédération et la cheffe du DDPS. À cette occasion, la DélCdG leur a communiqué les principales informations dont elle disposait concernant faits les plus importants liés au rôle des services de renseignement dans l'affaire Crypto AG. Ces informations ont également été transmises au Conseil fédéral par courrier secret.

Après la séance du Conseil fédéral du 20 décembre 2019, le Département fédéral de l'économie, de la formation et de la recherche (DEFR) a décidé de suspendre les licences générales d'exportation octroyées aux entreprises ayant succédé à

Crypto AG. L'objectif était visiblement d'éviter la publication d'articles de presse défavorables au DEFR. De l'avis de la DélCdG, cette suspension ne se justifiait toutefois pas sur les plans matériel et juridique, pas plus d'ailleurs que la manœuvre dilatoire adoptée par le Secrétariat d'État à l'économie (SECO), avec le soutien du DEFR, à l'encontre des entreprises concernées. Des demandes d'exportation individuelles pouvaient en effet toujours être déposées. Aucune raison légale ne s'opposait non plus à leur attribution, ainsi que le groupe de contrôle des exportations l'a admis à juste titre le 4 mars 2020. Étant donné la position du Département fédéral des affaires étrangères (DFAE), on a cependant décidé, dans le courant du mois de mai 2020, de soumettre toutes les demandes au Conseil fédéral pour décision.

Le 25 février 2020, le SECO a déposé, avec l'appui du DEFR, une plainte pénale auprès du Ministère public de la Confédération (MPC). À la suite de la parution de premiers articles dans les médias, le SECO soupçonnait en effet que Crypto AG n'avait pas respecté, avant 2018, les obligations de déclaration prévues par le droit sur le contrôle des biens en exportant des appareils utilisant une technique de cryptage «vulnérable». Le DEFR a approuvé, sans l'analyser, l'argumentation du SECO selon laquelle il y avait obligation de dénoncer pour des raisons légales. Pour sa part, le MPC a déconseillé de déposer une plainte lorsque le SECO lui a demandé son avis. Ce dernier n'en a pas parlé avec d'autres services fédéraux compétents.

Aux yeux de la DélCdG, la plainte pénale reposait sur une appréciation des faits superficielle et sur une argumentation juridique déficiente. La plainte étant manifestement motivée par des raisons politiques, elle aurait dû être déposée non pas par le SECO, mais par le DEFR.

Le 13 mars 2020, le MPC a demandé au DFJP l'autorisation d'ouvrir une procédure pénale concernant les violations du droit relatif au contrôle des biens dénoncées par le SECO. Trois mois plus tard, le DFJP a soumis la demande d'autorisation du MPC au Conseil fédéral pour décision. Au préalable, il en avait parlé avec la DélCdG, le 25 mai 2020. De son côté, le DEFR a proposé au Conseil fédéral, le 10 juin 2020, d'autoriser toutes les demandes d'exportation en suspens, alors qu'il était coresponsable de la plainte du SECO. Le Conseil fédéral ayant ajourné le traitement du dossier d'une semaine, le DEFR lui a proposé, en avançant exactement les mêmes motifs, de suspendre la décision relative aux demandes jusqu'à la clôture de la procédure du MPC. Le 19 juin 2020, le Conseil fédéral a accepté cette proposition et a délivré au MPC, dans le cadre d'une deuxième décision prise le même jour, l'autorisation demandée par le DFJP.

La DélCdG reconnaît que les décisions du Conseil fédéral concernant la demande d'autorisation du MPC et celles relatives aux demandes individuelles d'exportation des sociétés qui ont succédé à Crypto AG étaient cohérentes. Cependant, en reportant le traitement des demandes sans fixer de délai, le Conseil fédéral pourrait avoir contrevenu au principe de la bonne foi, étant donné que toute entreprise suisse devrait pouvoir s'attendre à ce que ses demandes d'autorisation relatives à des exportations soient approuvées rapidement pour autant qu'aucun motif juridique ne s'y oppose. Le droit relatif au contrôle des biens ne constituait pas non plus le moyen approprié de réagir dans l'affaire Crypto AG, et la plainte pénale n'était visiblement qu'une tentative de se soustraire à sa responsabilité politique en laissant la justice gérer l'affaire

Crypto AG. C'est ainsi que, en dernier ressort, le Conseil fédéral a associé la procédure du MPC à l'enquête que la DélCdG était en train de mener, ce qui était problématique du point de vue de la séparation des pouvoirs.

Table des matières

Rapport

1 Contexte

Lorsque la Délégation des Commissions de gestion (DélCdG) s'est constituée, le 19 décembre 2019, c'est le vice-président sortant, le conseiller national Alfred Heer, qui a repris la présidence. La conseillère aux États Maya Graf, qui avait déjà été membre de la délégation lorsqu'elle était conseillère nationale, a été nommée à la vice-présidence. La conseillère nationale Yvonne Ferri, le conseiller national Stefan Müller-Altermatt et les conseillers aux États Philippe Bauer et Werner Salzmann ont également rejoint la délégation.

Lors de sa première séance, le 20 janvier 2020, la DélCdG a pris acte de la décision du Conseil fédéral de confier à l'ancien juge fédéral Niklaus Oberholzer une étude historique de l'affaire Crypto AG (cf. ch. 6.2). Depuis l'entretien qu'elle avait eu le 25 novembre 2019 avec la cheffe du Département fédéral de la défense, de la protection de la population et des sports (DDPS), la délégation n'avait pas reçu d'autres informations ni d'autres documents de la part du DDPS sur ce dossier (cf. ch. 4.1.4). De plus en plus préoccupé par ce manque d'informations, le président de la délégation a demandé à rencontrer le directeur du Service de renseignement de la Confédération (SRC) au début du mois de février 2020. Ce fut fait le 6 février, mais les renseignements fournis étant insuffisants, le président de la DélCdG a exigé que lui soit remise immédiatement une copie du rapport MINERVA (cf. ch. 2.1.1), auquel visiblement plusieurs journalistes avaient déjà eu accès.

La DélCdG a décidé, le 12 février 2020, de se réunir en séance extraordinaire le jour suivant. Le soir même, le président de la délégation a participé à l'émission «Rundschau». À l'issue de sa séance du 13 février 2020, la délégation a décidé de mener une inspection formelle sur cette affaire et en a informé le Conseil fédéral et le public[1]. Il s'agissait notamment d'enquêter sur les liens existant entre les services de l'administration fédérale et les services de renseignement étrangers impliqués dans cette affaire et de clarifier si et dans quelle mesure le Conseil fédéral avait connaissance de leur lien avec l'entreprise Crypto AG.

Dans le même temps, la délégation a exigé du DDPS la remise d'un grand nombre de documents. En outre, elle s'est procuré auprès de la Chancellerie fédérale (ChF) les extraits des procès-verbaux de toutes les séances au cours desquelles le Conseil fédéral a abordé l'affaire Crypto AG. La délégation a aussi immédiatement procédé à l'audition des employés (anciens et actuels) de la Confédération. Entre le 19 et le 26 février 2020, la DélCdG a auditionné 14 personnes et a eu un entretien avec la cheffe du DDPS.

Jusqu'à la dernière audition qu'elle a menée le 26 août 2020, la DélCdG a entendu en tout 32 employés de la Confédération (anciens et actuels), dont certains plusieurs fois. Parmi les 12 personnes auditionnées qui n'étaient plus au service de la Confédération figuraient deux anciens chefs du département fédéral de la défense, l'un de l'ancien

[1] Inspection de la Délégation des Commissions de gestion sur l'affaire Crypto AG, communiqué de presse de la DélCdG du 13.2.2020.

Département militaire fédéral (DMF) et l'autre du DDPS (*Samuel Schmid* et *Kaspar Villiger*), et un ancien chef du Département fédéral de justice et police (DFJP) (*Arnold Koller*). Tous les anciens directeurs du SRC et du Service de renseignement stratégique (SRS)[2], les derniers chefs de la Police fédérale (PF) et du SRS ont également été entendus.

Après que la DélCdG est revenue sur l'autorisation donnée au Conseil fédéral d'ouvrir une enquête – enquête que ce dernier avait confiée à Niklaus Oberholzer –, la délégation a rencontré M. Oberholzer le 24 février 2020 afin de s'informer des travaux qu'il avait menés jusque-là sur mandat du Conseil fédéral. Elle a convenu avec M. Oberholzer qu'il poursuivrait ses travaux, mais sur mandat de la DélCdG. Lors de l'entretien entre la délégation et la cheffe du DDPS du 25 février 2020, cette dernière a adhéré à l'approche adoptée par la DélCdG.

M. Oberholer a repris officiellement ses investigations en tant que chargé d'enquête de la DélCdG le 2 mars 2020. Il a eu accès à tous les documents que la DélCdG avait reçus, et a reçu, pour information, les procès-verbaux de toutes les auditions menées par la délégation concernant l'affaire en question. Toutefois, la délégation n'a pas jugé nécessaire qu'il participe aux auditions.

Son travail a principalement porté sur l'étude des dossiers opérationnels des organisations qui ont précédé le SRC ainsi que sur l'analyse des évènements pertinents (cf. ch. 2.1.3). Sur cette base, il a procédé à une évaluation des évènements, tels qu'ils se sont succédé depuis la création du SRC.

Le 2 juillet 2020, M. Oberholzer a discuté de son projet de rapport avec la DélCdG; il lui a remis ensuite la version définitive dudit rapport, lequel regroupe l'ensemble des informations disponibles, dont celles que la délégation n'a pas fait figurer dans son rapport d'inspection pour des raisons de confidentialité. Le rapport de M. Oberholzer, d'environ 90 pages, complète le rapport d'inspection de la DélCdG. Il est destiné uniquement à la DélCdG et au Conseil fédéral.

2 Documents ayant servi à l'inspection

2.1 Rappel des faits

2.1.1 Rapport MINERVA

Le rapport «MINERVA – A History» explique comment les services de renseignement américains ont utilisé à leur profit et avec l'accord de son propriétaire suédois l'entreprise Crypto AG, celle-ci fabriquait en Suisse des appareils de cryptage depuis les années 1950. En 1970, Crypto AG – baptisée entre-temps du nom de code MINERVA – est devenue la propriété commune des services de renseignement américains et allemand. Le rapport évoque encore le retrait des Allemands à la fin de l'année 1993 et relate les faits qui se sont produits jusqu'en 1995.

2 En 2001, le Groupe des renseignements de l'armée a été dissous et sa division SRS a été intégrée dans la direction civile du SRS.

Le rapport MINERVA a été rédigé par les services américains après l'année 2000, avec le concours de représentants du service de renseignement allemand. Vers 2005, celui-ci a apparemment reçu une copie du rapport, à laquelle il a ajouté ultérieurement des appréciations complémentaires. Cette version du rapport américain et les documents allemands sont parvenus aux médias, qui ont commencé à en publier des extraits dès la deuxième semaine du mois de février 2020. À ce jour, les médias n'ont toutefois pas rendu publique l'intégralité des près de 100 pages du rapport MINERVA.

La DélCdG a analysé le rapport MINERVA, que le SRC lui avait transmis. Les informations complémentaires fournies par le SRC ne laissent aucun doute sur l'authenticité du document. Les indications qui figurent dans le rapport au sujet des évènements ayant eu lieu en Suisse et au sujet des autorités helvétiques manquent toutefois souvent de précision et contiennent certains détails dont il est établi qu'ils sont erronés. On peut supposer dès lors que les auteurs américains ne connaissaient pas très bien la Suisse et ses institutions. Cependant, la DélCdG part du principe que les rédacteurs du rapport ont relaté en toute bonne foi les évènements qui leur avaient été narrés par les agents de liaison de Crypto AG ou par d'autres personnes, et qu'ils les ont évalués selon leur propre modèle d'interprétation. La DélCdG ne connaît qu'une partie des documents allemands, mais les informations disponibles sur ce point ne présentent de toute façon aucun intérêt direct pour l'inspection de la délégation.

2.1.2 Procès-verbaux des entretiens de conduite du chef du DDPS

Après la transformation du SRS en office fédéral civil, le chef du DDPS a assumé, à partir de 2001, une responsabilité directe en matière de conduite pour ce qui était du renseignement extérieur. Pour les années 2002 à 2008, le DDPS a pu transmettre à la DélCdG les procès-verbaux des entretiens mensuels que le chef du DDPS (*Samuel Schmid*) avait avec le directeur du SRS (*Hans Wegmüller, puis Paul Zinniker*). Ces procès-verbaux étaient dressés par le rapporteur du chef de département compétent en la matière. Dans le procès-verbal du dernier entretien mensuel de 2008, la DélCdG a trouvé une indication selon laquelle le chef du DDPS de l'époque avait encore eu d'autres entretiens avec le directeur du SRS, lesquels n'avaient pas fait l'objet de procès-verbaux, et qu'il voulait conserver ses notes personnelles à ce sujet ailleurs qu'aux Archives fédérales suisses (AFS).

La DélCdG ayant prié le DDPS et les AFS de procéder aux investigations nécessaires, les deux carnets contenant les notes manuscrites du chef du DDPS de l'époque ont été retrouvés à la «Bibliothèque Am Guisanplatz». Manifestement, ces documents avaient été confiés à l'ancien chef de la bibliothèque militaire, mais n'avaient pas ensuite été archivés correctement. La DélCdG veillera à ce que le Secrétariat général du DDPS (SG-DDPS) garantisse la conservation de ces notes et à ce qu'elles soient archivées conformément aux dispositions légales.

Après le changement intervenu à la tête du département début 2009 (*nouveau chef: Ueli Maurer*), le premier entretien mensuel avec le SRS a encore fait l'objet d'un procès-verbal. La suppression du poste de rapporteur compétent pour les services de

renseignement a toutefois eu pour effet de voir le SG-DDPS cesser de consigner les entretiens de conduite mensuels avec le directeur du SRS dans un procès-verbal. En tout état de cause, la DélCdG n'a trouvé aucune mention de Crypto AG dans les procès-verbaux existants des entretiens de conduite que les chefs du DDPS ont eus avec les directeurs du SRS.

Toujours au début de l'année 2009, le Service d'analyse et de prévention (SAP) a été transféré du DFJP au DDPS, puis, au début de l'année 2010, il a fusionné avec le SRS pour former le SRC. Cependant, les entretiens mensuels du chef du DDPS avec le directeur du SRC (*Markus Seiler*) n'ont fait l'objet d'un procès-verbal qu'à partir du début de l'année 2014, tenu par le chef de la Surveillance SR – organe interne au DDPS. Sa participation à ces entretiens mensuels résultait en somme de l'enquête administrative que le professeur Heinrich Koller avait menée, sur mandat du chef du DDPS, à la suite du vol de données au détriment SRC. Cette enquête a été achevée à la fin du mois de mars 2013[3]. Les seuls documents qui existent pour les années antérieures sont les ordres du jour que le directeur du SRC établissait en vue de ses entretiens mensuels avec le chef du DDPS.

La rédaction de procès-verbaux concernant ces entretiens mensuels s'est poursuivie sous l'autorité du chef du DDPS suivant (*Guy Parmelin*). Or, aucun d'eux ne contient le moindre indice selon lequel le directeur du SRC aurait mentionné, d'une façon ou d'une autre, Crypto AG en présence de son chef de département.

2.1.3 Dossiers opérationnels de la PF et du SRS

Afin de savoir ce que les services de renseignement suisses connaissaient de Crypto AG, la DélCdG a dû compulser les dossiers relatifs à la recherche d'informations effectuée par la PF et le SRS. Ceux-ci se rapportaient à des activités qui remontaient jusqu'aux années 1970.

À la suite de l'affaire des fiches, la PF a insisté auprès des AFS pour que l'archivage des documents fasse l'objet d'une distinction entre les pièces faisant foi au tribunal et les autres, et pour que seules les premières nommées soient versées aux AFS. Ainsi que la DélCdG l'a appris au début de l'année 2001, le directeur de l'époque des AFS (*Christoph Graf*) estimait que cette exigence n'était pas admissible juridiquement, mais il ne pouvait pas obliger la PF à lui remettre les dossiers établis à des fins de prévention policière.

L'enquête préliminaire que la PF a effectuée en 1994 sur la base des accusations portées contre Crypto AG par Hans Bühler et les médias s'inscrivait dans la perspective de l'ouverture ultérieure d'une procédure de police judiciaire. Vu que les dossiers concernés avaient été considérés comme des pièces faisant foi au tribunal, ils avaient été versés aux AFS, ce qui a permis de les retrouver assez rapidement.

Par contre, les AFS ne détiennent pas de documents concernant l'enquête que la PF a réalisée dans les années 1970 sur la base des indications données par l'ancien chef de

3 Inspection consécutive à l'arrestation d'une ancienne source du SRC en Allemagne, rapport de la DélCdG du 13.3.2018, ch. 2.3 (FF **2018** 5147 5164).

développement de Crypto AG. Ces dossiers, liés à des investigations menées à des fins de prévention policière, n'ont jamais été versés aux AFS, mais ils ont été conservés à l'interne sous l'appellation «Cas Code» (cf. ch. 3.1.1). Au début de l'année 2010, ils ont été remis au SRC en même temps que les dossiers de l'opération «Rötel» (cf. ch. 3.1.2). Ils ont été retrouvés dans l'ancienne installation protégée (installation K)[4] que le SRS avait transformée afin d'y conserver des documents particulièrement secrets (cf. ch. 2.1.4). C'est dans cette installation K qu'ont été trouvés les dossiers pertinents du SRS au sujet de Crypto AG.

2.1.4 Pratique des services de renseignement en matière d'archivage

La loi fédérale sur l'archivage (LAr)[5] est entrée en vigueur le 1er octobre 1999 et a remplacé le règlement du Conseil fédéral du 15 juillet 1966 pour les archives fédérales. Cette nouvelle loi introduisait une obligation de proposer les documents aux AFS au lieu de l'obligation de verser les documents aux AFS. Le but de l'archivage restait toutefois le même: conserver tous les documents qui présentent une certaine valeur pour la postérité. La LAr ne prévoyait aucune exception. Néanmoins, le Conseil fédéral a commencé à s'écarter de ce principe par voie d'ordonnance et ce au bénéfice des services de renseignement.

L'art. 17, al. 7, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[6], qui est entré en vigueur le 1er juillet 1998, dispose que, dans les relations avec l'étranger, la protection des sources doit dans tous les cas être assurée. Se fondant sur cette disposition, le Conseil fédéral a exempté, en juin 2001, le SAP (qui avait repris les fonctions de la PF) de l'obligation de proposer aux AFS, aux fins d'archivage, les données classifiées émanant des relations directes avec les autorités de sécurité étrangères (art. 21, al. 2, OMSI)[7]. Comme le chef de l'époque du SAP (*Urs von Daeniken*) l'a expliqué à la DélCdG en juillet 2001, son service devait, en règle générale, détruire ces documents au plus tard après cinq ans. En 2008, le SAP a par exemple reçu 8200 communications en provenance de services partenaires et, de son côté, il leur en a fait parvenir 10 900[8].

Les investigations consacrées aux contacts que les services de renseignement suisses avaient eus avec l'Afrique du Sud, menées par la DélCdG entre 1999 et 2003, ont

4 La liste AGFA (Abteilung für Genie und Festung Anlageverzeichnis [division du génie et des fortifications – liste des installations]) de l'Office fédéral du génie et des fortifications, qui n'existe plus, classait les installations et les constructions de l'armée en différentes catégories. Les installations de commandement faisaient partie des catégories «A» ou «F», comme l'installation A-01780 de l'organisation P-26, à Gstaad (cf. rapport annuel 2018 des CdG et de la DélCdG du 28.1.2019, ch. 4.10 [FF **2019** 2689 2774]). Les installations de commandement de la direction civile et militaire étaient souvent désignées aussi par le nom d'installations K (pour Kriegsanlagen).

5 Loi fédérale du 26.6.1998 sur l'archivage (LAr; RS **152.1**).

6 Loi fédérale du 21.3.1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS **120**).

7 Ordonnance du 27.6.2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI; RO **2001** 1829).

8 Rapport d'activité 2008 de fedpol, mai 2009, p. 19.

révélé que le service de renseignement militaire avait détruit systématiquement des documents pendant des années, les soustrayant ainsi à l'archivage[9]. Lorsque la DélCdG a effectué une visite aux AFS, en janvier 2001, elle a constaté que les archives les plus récentes du service de renseignement dataient des années 1940. Comme la DélCdG l'a appris plus tard, le nouveau directeur du SRS avait toutefois décidé, début 2001, qu'aucun autre document ne devrait être détruit sans l'accord des AFS.

Au début de l'année 2004, l'entrée en vigueur de l'art. 99, al. 4, loi sur l'armée (LAAM)[10] a introduit une nouvelle norme relative à la protection des sources. Selon le message du Conseil fédéral, le SRS avait dès lors la compétence de déroger à la LAr[11]. Par la suite, la nouvelle mouture de l'art. 12, al. 2, Ordonnance sur l'organisation des services de renseignements au sein du DDPS (ORens)[12] prévoyait que le SRS ne devait pas proposer d'archiver les documents classifiés émanant des relations directes avec des services étrangers et ceux issus de la recherche opérative, mais que tous ces documents devaient être conservés par les services de renseignement d'entente avec les AFS. Afin de pouvoir conserver ce genre de documents en sûreté durant une longue période, le SRS a fait transformer l'installation K susmentionnée pour en faire son lieu exclusif d'archives internes (cf. ch. 2.1.3).

Alors que la dérogation accordée au SAP a eu pour conséquence de voir tous les documents émanant des relations avec l'étranger être définitivement détruits, la teneur de l'ORens, tout du moins, ne donnait aucune compétence au SRS de détruire des documents importants. Le Conseil fédéral autorisait néanmoins le SRS à tenir ses propres archives, en dehors des AFS. Toutefois, plusieurs questions n'étaient pas réglées au sujet de l'organisation de ces archives ou de la réglementation de leur consultation. Ainsi que la DélCdG a pu le constater en janvier 2011, lors d'un entretien avec le directeur des AFS (*Andreas Kellerhals*), ces dernières et le SRS ne sont jamais parvenus, durant toutes ces années, à se mettre d'accord sur les modalités de la conservation des documents entreposés dans l'installation K susmentionnée. De plus, les AFS n'avaient pas accès à ces documents.

Lorsque les ordonnances concernant le SRC ont été élaborées, en 2009, le directeur désigné du SRC (*Markus Seiler*) a fait harmoniser les dispositions de l'OMSI et de l'ORens relatives aux exceptions en matière d'obligation d'archivage. L'art. 28, al. 2, Ordonnance sur le Service de renseignement de la Confédération (OSRC)[13], qui était nouveau, supprimait l'obligation de proposer aux AFS, aux fins d'archivage, la totalité des données et documents classifiés émanant des relations directes avec les autorités de sécurité étrangères ou de renseignements opérationnels sur l'étranger. Cette disposition s'appliquait rétroactivement aux documents qui n'avaient pas encore été remis. Ainsi, la destruction irrémédiable, que le SAP pratiquait déjà en ce qui concerne

9 Examen des contacts des services de renseignement suisses avec l'Afrique du Sud du temps de l'apartheid, rapport de la DélCdG du 18.8.2003, ch. 4.3.7 (FF **2004** 2101 2130)
10 Loi fédérale du 3.2.1995 sur l'armée et l'administration militaire (Loi sur l'armée, LAAM; RS **510.10**).
11 Message du Conseil fédéral du 24.10.2001 sur la réforme Armée XXI et sur la révision de la législation militaire (FF **2002** 816 835).
12 Ordonnance du 26.9.2003 sur l'organisation des services de renseignements au sein du DDPS (ORens; RO **2003** 4001).
13 Ordonnance du 4.12.2009 sur le Service de renseignement de la Confédération (OSRC; RO **2009** 6937).

les documents émanant des relations avec l'étranger, était dès lors formellement possible aussi pour les documents émanant de renseignements opérationnels sur l'étranger. Cette destruction était toutefois permise seulement au bout de 45 ans de conservation, en tout cas selon la teneur de la disposition.

Pour la DélCdG, ces nouvelles normes dérogatoires prévues par le Conseil fédéral pour le SRC n'étaient pas compatibles avec les nouvelles bases légales régissant le SRC que la délégation avait conçues elle-même dans le cadre du traitement de l'initiative parlementaire Hofmann[14]. Lors de l'entrée en vigueur de la loi fédérale sur le renseignement civil (LFRC)[15], les dispositions sur la protection des sources de la LAAM et de la LMSI ont été abrogées, tout comme, s'agissant de cette dernière, la légitimité reconnue par le Conseil fédéral de détruire des documents émanant des relations avec des services partenaires. Selon l'art. 7 LFRC, seules les personnes qui sont en danger en raison de leurs activités de renseignement sur l'étranger doivent être protégées dans tous les cas. Or, cette disposition n'était pas prévue pour servir à contourner la LAr.

La DélCdG a demandé un avis à l'Office fédéral de la justice (OFJ) et, début 2011, elle a auditionné le directeur des AFS et des représentants du SRC, après quoi elle a décidé de prescrire explicitement dans la loi, à la première occasion, l'archivage complet et sûr de tous les documents du SRC[16]. Cette façon de procéder lui paraissait pertinente parce que, en toute bonne foi, la délégation partait de l'idée que la destruction d'autres documents était exclue à court terme, étant donné le délai de 45 ans.

Les Chambres fédérales ont suivi les propositions de la DélCdG, d'abord en 2013, lors de la révision de la LFRC, puis en 2014, lors de l'examen de la loi fédérale sur le renseignement (LRens)[17]. En 2019, la DélCdG a commencé à contrôler la mise en œuvre de la nouvelle disposition sur l'archivage. À la lecture d'un rapport que le SRC avait rédigé en mai 2019 à l'intention de la DélCdG, celle-ci apprenait pourtant que le SRC avait encore détruit irrémédiablement, entre 2011 et 2014, des documents émanant de services partenaires du SAP. À en croire les explications que le SRC a données en novembre 2019, cette opération avait eu lieu lors du passage à une nouvelle version du Système d'information sécurité intérieure (ISIS)[18].

Par la suite, la DélCdG a prié la cheffe du DDPS (*Viola Amherd*) de vérifier la légalité de la destruction de ces données et de trouver qui en assumait la responsabilité. Selon un rapport complémentaire du SRC du 3 mars 2020, dont la teneur a été confirmée par la cheffe du DDPS lors d'un entretien tenu le 25 mai 2020, le DDPS a jugé que la destruction des documents critiquée par la DélCdG était légale. D'après le directeur du SRC (*Jean-Philippe Gaudin*), cette destruction effectuée avant l'expiration du délai de conservation de 45 ans était fondée sur l'avis de l'OFJ de 2010.

14 Iv. pa. Hofmann «Transfert des tâches des services de renseignement civils à un département» du 13.3.2007 (07.404).
15 Loi fédérale du 3.10.2008 sur le renseignement civil (LFRC; RO **2009** 6565)
16 Rapport annuel 2013 des CdG et de la DélCdG du 31.1.2014, ch. 4.4 (FF **2014** 4831 4903).
17 Loi fédérale du 25.9.2015 sur le renseignement (LRens; RS **121**)
18 Avant 2010, l'abréviation ISIS désignait le «Système de traitement des données relatives à la protection de l'État»; elle signifie aujourd'hui «Système d'information sécurité intérieure».

2.2 Appréciation de la DélCdG

Le public comme le Parlement ont appelé la DélCdG à faire toute la lumière, à travers son inspection, sur les activités des services de renseignement, dont certaines remontaient à plus de 40 ans. La DélCdG tient donc à souligner que le législateur accordait autrefois trop peu d'importance à l'archivage dans le domaine du renseignement. Un archivage fiable dans le domaine du renseignement n'est garanti au niveau de la loi que depuis novembre 2014 – et cela s'est fait notamment grâce aux efforts de la DélCdG.

Il y a lieu de relever aussi que le Conseil fédéral a permis pendant des décennies aux services de renseignement de soustraire à grande échelle des documents importants à l'archivage. En mai 2020 encore, le DDPS justifiait des destructions manifestement illégales de documents très récents du SRC en se référant de manière inexacte à un avis de l'OFJ que la DélCdG avait demandé. Pour la délégation, cette situation est incompréhensible.

Il s'avère rétrospectivement que le Conseil fédéral avait prévu des dérogations à l'obligation d'archivage pour les services de renseignement sans avoir d'idée directrice et sans se soucier des contradictions éventuelles. De toute évidence, ni le SRC, ni le DDPS, ni le Conseil fédéral ne savaient réellement quels documents les services de renseignement avaient archivés, n'avaient pas encore archivés ou avaient détruits au cours de ces dernières décennies. Le directeur actuel du SRC (*Jean-Philippe Gaudin*) était en fonction depuis plus d'un an quand il a appris l'existence de documents entreposés dans une ancienne installation K.

Sur la base de ses investigations, la DélCdG considère que les documents retrouvés éclairent les activités de la PF en relation avec Crypto AG de telle manière que la haute surveillance dispose d'informations suffisantes pour procéder à une appréciation sur le fond. Cependant, la DélCdG ne peut garantir que tous les documents concernant la prévention policière ayant un lien avec Crypto AG aient été conservés et transférés dans l'installation K du SRC. S'il devait s'avérer nécessaire un jour d'enquêter sur les rapports de la PF ou du SAP avec des partenaires étrangers, la DélCdG peut affirmer aujourd'hui déjà que, en raison de la pratique de destruction de documents autorisée par le Conseil fédéral, les dossiers y afférents seraient incomplets.

Pour l'inspection de la DélCdG, c'est une chance que le SRS ait conservé à l'interne des documents importants sur Crypto AG et que ceux-ci aient été retrouvés intacts dans l'installation K. La directive émise en 2001 par le directeur du SRS (*Hans Wegmüller*), commandant de ne plus détruire aucun document, y a probablement contribué. Rien ne garantit toutefois que des documents relatifs à d'autres activités de recherche exercées par le renseignement militaire, les plus anciennes en particulier, existent encore à un niveau de qualité similaire.

Aux yeux de la DélCdG, l'inspection a montré en outre que la destruction de documents n'était pas un moyen efficace de protéger des sources, et qu'elle pouvait même aller à l'encontre de cet objectif. Il y a lieu de tenir compte notamment du fait que le SRC n'est souvent pas le seul à connaître l'existence de ses sources. La source elle-même, éventuellement ses proches ou d'autres services avec lesquels le SRC recherche des informations, peuvent savoir qu'elle agit au service de la Suisse.

Si la source est découverte par un antagoniste sans qu'il y ait faute du service de renseignement suisse, il faut que le SRC connaisse l'existence de cette source, car c'est la seule façon pour lui de continuer à la protéger dans les limites de ses possibilités. S'il n'est pas au courant, le risque est grand de voir sa réaction, celle du DDPS ou celle du Conseil fédéral provoquer une mise en danger supplémentaire de ladite source. La destruction de documents issus de la recherche opérationnelle peut ainsi, suivant la situation, impliquer que le SRC ne pourra pas ou plus remplir son obligation légale de protection des sources au sens de l'art. 35 LRens.

L'inspection de la DélCdG prouve à nouveau l'importance de la conduite politique du service de renseignement. Il faut donc qu'il soit possible de déterminer si les chefs de département assument leur responsabilité directe en matière de conduite et, dans l'affirmative, de quelle manière ils s'y prennent. C'est pourquoi la DélCdG est convaincue qu'il est important que les entretiens de conduite fassent l'objet de procès-verbaux clairs et que ceux-ci soient archivés dans leur intégralité et en toute sécurité.

3 Activités de la Police fédérale

3.1 Rappel des faits

3.1.1 Cas «Code»

En 1977, le chef de la recherche et du développement de Crypto AG s'est adressé à la Police fédérale (PF) par l'intermédiaire de membres du commandement de l'armée qu'il connaissait depuis son service militaire. D'après ses déclarations, l'entreprise appartenait à des organisations allemandes et américaines actives dans la recherche de renseignements et, sur leur ordre, elle intégrait intentionnellement des failles dans les appareils conçus pour l'étranger. Selon les reproches formulés par cette personne, la démarche visait à permettre à des services de renseignement étrangers de décrypter et de lire des communications qui ne leur étaient pas destinées.

Afin de faire toute la lumière sur ces reproches, la PF s'est tournée vers l'Office fédéral des troupes de transmission (OFTRM). Celui-ci a recommandé, en avril 1979, de se procurer un appareil douteux à l'étranger et de l'analyser en vue de procéder à des investigations plus poussées. Le service juridique du Ministère public de la Confédération (MPC) a présenté un examen approfondi des infractions éventuelles en juillet 1979, en particulier dans le domaine du service de renseignement interdit. En août 1979, un entretien entre le procureur général de la Confédération (*Rudolf Gerber*), le chef de la PF (*André Amstein*) et d'autres représentants du MPC a eu pour conclusion qu'il ne pouvait être exclu que Crypto AG soit mêlée à des activités de renseignement et qu'il convenait de suivre la proposition de l'OFTRM. Comme les éclaircissements qui devaient être entrepris par l'OFTRM auprès d'un État étranger approprié prenaient du retard, le chef de la PF a décidé, en mars 1980, d'abandonner l'idée d'une enquête de police judiciaire jusqu'à nouvel avis.

Il a fallu attendre 1982 pour que l'OFTRM ait accès à un appareil crypté provenant d'un État voisin et qui convienne. L'année suivante, l'office a conclu que les reproches selon lesquels des dispositifs avaient été modifiés ne pouvaient ni être prouvés ni être totalement réfutés. Il avait cependant constaté qu'il y avait une divergence

entre le circuit logique et la description figurant dans la documentation de l'utilisateur, et que la thèse de la manipulation ne pouvait par conséquent pas être complètement exclue.

On n'a pas retrouvé de traces écrites de la réaction du MPC ou de la PF à cette dernière remarque de l'OFTRM. En revanche, il apparaît que celui-ci a ensuite davantage concentré son attention sur la sécurité des appareils utilisés en Suisse, de sorte qu'il ne disposait plus d'aucune ressource pour les questions soulevées par la PF en matière de renseignement.

3.1.2 Opération «Rötel»

En 1988, la PF a constaté que des services de renseignement d'États membres du pacte de Varsovie essayaient, par le biais de tiers, d'acquérir des appareils de cryptage auprès de Crypto AG. À la même époque, des informations relatives à des demandes suspectes ainsi que des listes de clients sont parvenues à la PF de la part de Crypto AG. Ce canal de transmission n'a toutefois pas fonctionné longtemps: il s'est éteint après le départ du collaborateur compétent de la PF. Les informations reçues et l'accès aux informations de Crypto AG semblent avoir ensuite été oubliés au sein de la PF.

3.1.3 Affaire Bühler

Au terme d'une incarcération de neuf mois en Iran, l'ingénieur de vente de Crypto AG Hans Bühler est rentré en Suisse, en janvier 1993. Le même mois, il a été interrogé par la PF, notamment au sujet des accusations d'espionnage dont qui l'avaient visé en Iran. Il n'y a pas eu d'investigations plus approfondies à ce moment-là. Au printemps 1993, Crypto AG a résilié le contrat de travail de Hans Bühler. C'est alors que les médias se sont emparés de l'affaire.

Lorsque, en mars 1994, les médias se sont davantage intéressés à l'affaire, la PF elle a informé le SG-DFJP que la presse allait bientôt publier des articles à son sujet et a relancé des investigations. Il s'agissait, d'une part, de la question des services de renseignement étrangers qui détenaient Crypto AG et, d'autre part, du soupçon concernant la manipulation intentionnelle de certains appareils de cryptage.

Entre mars et novembre 1994, dans le cadre de son enquête, la PF a interrogé Hans Bühler (une deuxième fois) ainsi que vingt autres personnes, anciens employés, collaborateurs en activité, membres du conseil d'administration ou du comité consultatif de Crypto AG, en qualité de personnes tenues de renseigner. Seules deux d'entre elles ont été en mesure de parler des manipulations présumées des appareils de cryptage, tandis que les autres n'avaient fait qu'entendre des rumeurs à ce sujet et ne pouvaient donc pas fournir de renseignements concrets là-dessus. Ces recherches n'ont pas permis de corroborer les soupçons de manière à justifier l'ouverture d'une enquête de police judiciaire par le MPC. Dans son rapport final du 3 mai 1995, la PF a toutefois relevé que les véritables propriétaires de Crypto AG n'avaient pas pu être identifiés.

Le DFJP a assisté la PF dans ses investigations relatives aux titres de propriété de Crypto AG. L'interrogatoire de deux membres du comité consultatif de l'entreprise n'ayant apporté aucune réponse satisfaisante, le secrétaire général du DFJP (*Armin Walpen*) a prié avec insistance, le 5 mai 1994, le conseiller national Georg Stucky, qui était membre du conseil d'administration de Crypto AG depuis 1992, d'exercer son influence afin de clarifier la question des titres de propriété de cette entreprise.

Après la parution du rapport final de la PF, le chef du DFJP (*Arnold Koller*) a transmis celui-ci au chef de ce qui était alors le DMF (*Kaspar Villiger*) avec une lettre d'accompagnement, datée du 2 juin 1995, dans laquelle il précisait que le rapport pourrait être utile en cas de discussion avec le conseiller national Stucky au sujet des titres de propriété de Crypto AG. La documentation disponible ne permet pas de savoir si une telle discussion a eu lieu. On pourrait penser que non, car le chef du DFJP prévoyait, selon une note de son secrétaire général prise à la fin du mois de juin 1995, de s'entretenir personnellement avec le conseiller national Stucky pour connaître les véritables propriétaires de Crypto AG. Le chef du DFJP a déclaré à la DélCdG qu'il supposait qu'une telle rencontre n'avait pas eu lieu.

Selon les investigations de la DélCdG, menées auprès de la Chancellerie fédérale notamment, rien n'indique que le rapport final de la PF ait été évoqué au Conseil fédéral ou que ses conclusions aient été publiées. En juillet 1997, la PF a fait parvenir une lettre à Crypto AG, à la demande de cette dernière, qui résumait les résultats de l'enquête, finalement stérile.

3.1.4 Informations transmises à l'organe de haute surveillance

La DélCdG s'est renseignée à plusieurs reprises sur le déroulement de l'enquête de la PF relative à l'affaire Bühler. Le 24 mars 1994, le chef de la PF (*Urs von Daeniken*) a assuré aux représentants de la haute surveillance parlementaire que l'autorité compétente éclaircirait la question des véritables propriétaires de Crypto AG. Peu après, la DélCdG a demandé à la PF d'adresser à la délégation un rapport écrit visant à l'informer de l'état de la procédure et des résultats de l'enquête.

Dans une lettre du 27 mai 1994, le chef de la PF informait la DélCdG qu'il n'y avait eu jusque-là aucun soupçon concret d'infraction et que, par conséquent, aucune enquête judiciaire ne serait ouverte. D'après lui, les personnes appelées à donner des renseignements n'avaient pu ou n'avaient voulu donner aucune indication sur l'influence que les services secrets allemands ou américains étaient supposés exercer. Le chef de la PF concluait en déclarant que les soupçons de manipulation des appareils de cryptage n'avaient pas pu être prouvés concrètement. Néanmoins, certains indices donnaient à croire à la PF qu'il existait peut-être deux niveaux de qualité en matière de cryptage. En outre, la réticence de Crypto AG à révéler l'identité de ses propriétaires ne laissait pas d'étonner. Sur ce point, la piste s'arrêtait à une fondation liechtensteinoise, au capital de laquelle on notait une participation allemande.

La DélCdG a pris connaissance du contenu de cette lettre lors de sa séance de la fin du mois de juin 1994. Autant que l'on puisse en déduire rétrospectivement des dossiers concernés, aucune autre information n'a été transmise à la DélCdG et celle-ci n'en a pas demandé d'autre de son côté.

3.2 Appréciation de la DélCdG

En se référant aux investigations menées par la PF dans les années 1970, 1980 et 1990, la DélCdG arrive, au vu des informations dont elle dispose, à la conclusion que celles-ci ont été réalisées correctement et que, partant, elles ne prêtent pas le flanc à la critique. Aucun élément ne permet d'affirmer que les recherches auraient fait l'objet d'obstruction de la part d'instances politiques en Suisse ou auraient été influencées par ces dernières, ou que certains faits n'auraient sciemment pas été étudiés ou ne l'auraient été que superficiellement.

Pour les enquêtes qu'elle a effectuées dans les années 1990 en particulier, la PF a recouru à tous les instruments dont elle disposait à l'époque. La direction du DFJP était informée rapidement et exhaustivement, le chef de département prenant connaissance des investigations sans toutefois intervenir directement dans le déroulement de la procédure. Cependant, ni le chef de la PF *Urs von Daeniken*) ni celui du DFJP (*Arnold Koller*) n'étaient entièrement satisfaits du résultat des recherches. C'est la raison pour laquelle le DFJP a encore tenté, une fois les investigations achevées, de creuser la question des propriétaires de Crypto AG au moyen de différents canaux. La coopération envisagée à ce propos avec le conseiller national Stucky, membre du conseil d'administration de Crypto AG, ne s'est visiblement jamais concrétisée.

Selon le rapport MINERVA, ainsi que d'autres documents que la DélCdG a analysés dans le cadre de son inspection, la direction de Crypto AG a communiqué, au printemps 1994, l'identité des véritables propriétaires de l'entreprise au conseiller national Stucky. On peut supposer que cette information est passée de la direction, dont certains membres étaient dans la confidence, aux documents susmentionnés. Ces personnes savaient aussi quels membres du conseil d'administration les avaient renseignées. L'ancien conseiller national Stucky a toutefois déclaré à la DélCdG, en mai 2020, qu'il ignorait travailler pour une entreprise détenue par les services secrets américains.

Aux termes du rapport MINERVA, le conseiller national Stucky aurait confié au chef du DMF de l'époque (*Kaspar Villiger*) qui étaient les véritables propriétaires de Crypto AG. Cette information et les indications y afférentes qui figurent dans d'autres documents en possession de la DélCdG confirment que la direction de Crypto AG partait du principe que le conseiller national Stucky et le chef du DMF avaient eu cet échange. Quant à savoir si celui-ci a réellement eu lieu, et sous quelle forme, la DélCdG n'est pas parvenue à élucider la question sur la base des documents qu'elle a consultés et des auditions qu'elle a menées. Devant la DélCdG, l'ancien chef du DMF a toutefois indiqué qu'il pensait avoir eu un entretien avec le conseiller national Stucky au sujet de Crypto AG durant la période de l'affaire Bühler. Cependant, il ne se rappelait pas avoir jamais été informé de l'identité des propriétaires de Crypto AG

et de l'opération des services de renseignement mentionnée dans le rapport MINERVA.

4 Activités des services du DMF et du DDPS

4.1 Rappel des faits

4.1.1 Sources d'information du SRS

À partir de l'automne 1993, le SRS[19] a réussi à obtenir des informations fiables au sujet de la société Crypto AG. Il a ainsi appris que celle-ci appartenait aux services de renseignement américains et allemand et, plus tard, que le service allemand avait mis fin à sa participation (cf. ch. 2.1.1). Le SRS a également eu connaissance du fait que la société exportait des appareils «vulnérables», dont le cryptage pouvait être décodé moyennant un minimum d'efforts, contrairement à ce qui était le cas pour les appareils «non vulnérables»

Le SRS s'est fixé comme objectif de pouvoir décoder lui-même systématiquement le cryptage des appareils «vulnérables». À cette fin, il s'est procuré des informations techniques sur les procédures de cryptage utilisées pour les appareils exportés. Ces connaissances ont également pu être utilisées pour détecter d'éventuelles procédures de cryptage «vulnérables» utilisées par les appareils achetés par la Suisse.

À la suite de l'affaire Bellasi[20], le Groupe des renseignements (Grrens) a été dissous et le SRS a été transformé en office fédéral civil début 2001. Sous la direction de son premier directeur (*Hans Wegmüller*), le SRS s'est efforcé de poursuivre la recherche d'informations sur les procédures de cryptage «vulnérables» utilisées par Crypto AG. Cela n'a en fin de compte été possible que parce que les services de renseignement américains étaient d'accord pour que la Suisse obtienne les informations souhaitées pour autant que le volume d'informations transmises soit pertinent.

Afin de pouvoir exploiter les connaissances acquises au sujet des procédures de cryptage «vulnérables» en vue de se procurer des renseignements pertinents sur le plan de la politique de sécurité, le SRS a aussi dû systématiquement obtenir l'accès à des transmissions cryptées. L'exploration radio était alors effectuée par la Base d'aide au commandement de l'armée (BAC) sur mandat du SRS. Après la modernisation des systèmes d'exploration des ondes courtes, les capacités d'exploration des liaisons de satellites de communication ont été développées à partir de l'année 2000[21]. En 2006, l'exploitation complète du système «Onyx» a commencé selon la configuration prévue. Les compétences en matière de décryptage ont alors été implémentées dans les processus d'exploration radio pilotés par le SRS.

19 Pour en savoir plus sur l'intégration du SRS dans l'organisation du département responsable entre 1985 et 2009, voir l'Examen des contacts des services de renseignement suisses avec l'Afrique du Sud du temps de l'apartheid, rapport de la DélCdG du 18.8.2003, ch. 4.3.1 (FF **2004** 2101 2118, 2120 et 2122).

20 Évènements survenus au Groupe des renseignements de l'État-major général («affaire Bellasi»), rapport de la DélCdG du 24.11.1999 (FF **2000** 528).

21 Système d'interception des communications par satellites du DDPS (projet «Onyx»), rapport de la DélCdG du 10.11.2003 (FF **2004** 1377).

4.1.2 Informations fournies aux services hiérarchiquement supérieurs et aux conseillers fédéraux

La recherche d'informations concernant Crypto AG était un secret bien gardé au sein du SRS. Seuls le chef du service (*Fred Schreier*), et, plus tard, ses directeurs (*Hans Wegmüller, puis Paul Zinniker*) ainsi que, selon le moment, un ou deux de ses membres en avaient connaissance. Lorsque que le SRS était subordonné au Grrens, la hiérarchie militaire n'était pas au courant de cette activité.

En 2010, le SRC est né de la fusion du SRS et du SAP. Ce dernier avait été transféré du DFJP au DDPS un an plus tôt à la suite de l'initiative parlementaire Hofmann[22]. Au cours de sa première année de fonction (2010), le directeur du nouveau service (*Markus Seiler*) a été informé de l'existence d'appareils «vulnérables» de Crypto AG et, en tout cas dans les grandes lignes, des relations entre Crypto AG et les services américains. Au cours de sa dernière année à ce poste (2017), on lui a également montré ce qui avait permis au service de renseignement suisse d'exploiter cette procédure de cryptage «vulnérable». On lui a exposé aussi la nécessité pour le SRC d'agir, en lui présentant les options envisageables. Toutefois, le directeur du SRC ne se considérait alors pas comme responsable de cette question et a refusé de prendre possession d'une note d'information à ce sujet. Son adjoint (*Paul Zinniker*), qui avait déjà été informé du temps du SRS, a soutenu la décision de son directeur de ne plus rien entreprendre au sujet de ce dossier.

Les prédécesseurs de l'actuelle cheffe du DDPS n'ont été informés ni par le SRS ni, plus tard, par le SRC du fait que la société Crypto AG était contrôlée par les services de renseignement américains et que le service de renseignement suisse avait connaissance de l'existence des procédures de cryptage «vulnérables» et exploitait ces failles dans le cadre de la recherche d'informations.

4.1.3 Informations fournies à l'actuelle cheffe du DDPS et au Conseil fédéral

Au printemps 2019, le directeur actuel du SRC (*Jean-Philippe Gaudin*) a reçu, pour l'essentiel, les mêmes informations que son prédécesseur deux ans auparavant. Contrairement à ce dernier, il a estimé qu'il était nécessaire de prendre des mesures. Il a alors demandé qu'on lui présente la situation en détail, puis a donné l'ordre, à la mi-juin 2019, de dresser un bilan de la situation.

Vers la fin du mois de juin 2019, le SRC a été informé via des canaux dans les milieux du renseignement que des médias américains et allemands enquêtaient au sujet de Crypto AG et du rôle que la société avait joué dans une opération de recherche d'informations à grande échelle menée par les services de renseignement américains et allemand. Cette évolution fortuite de la situation a provoqué une accélération des investigations ordonnées par le directeur du SRC.

22 Iv. pa. Hofmann «Transfert des tâches des services de renseignement civils à un département» du 13.3.2007 (07.404).

Lors de la séance de direction d'office du 19 août 2019, le directeur du SRC a informé la cheffe du DDPS que la société Crypto AG avait collaboré avec des services de renseignement étrangers. Selon les notes manuscrites disponibles sur cette rencontre, il y a été dit que le service de renseignement suisse avait lui aussi eu la possibilité d'exploiter les faiblesses des procédures de cryptage de la société.

Le bilan de la situation demandé par le directeur du SRC a été achevé à la mi-septembre 2019. L'un des deux exemplaires de ce rapport, qui était considéré comme un document à l'usage exclusif du service, a été remis au directeur du SRC et le second a été remis au chef de la division Aide à la conduite et à l'engagement (NDBU). Ce n'est qu'au début novembre 2019 que d'autres exemplaires ont été établis à l'intention du chef en fonction de la division Recherche (NDBB), qui avait mené les investigations de la PF en 1994, et d'un autre membre de la direction du SRC. Le document contenait toutes les informations pertinentes pour comprendre les relations entretenues entre les services de renseignement du DDPS et les services de renseignement américains ainsi que leurs opérations menées avec Crypto AG. Il contenait également une analyse aussi poussée que possible des conséquences de la scission de la société, qui avait eu lieu l'année précédente. Aucune suite n'a été donnée à ce document au sein du SRC et les informations pertinentes sur le plan politique qu'il contenait n'ont pas été transmises à la cheffe du DDPS.

À la mi-octobre 2019, le SRC est entré en possession du rapport MINERVA (cf. ch. 2.1.1) et son directeur a été informé du contenu du rapport. À partir de fin octobre, les échanges de renseignements entre le SRC, les services américains et d'autres services étrangers impliqués se sont intensifiés. L'objectif était de faire en sorte que tous disposent des mêmes informations et d'anticiper les conséquences de la publication de révélations tirées du rapport MINERVA dans les médias.

À l'occasion de la séance de direction d'office du 31 octobre 2019, le directeur du SRC a de nouveau évoqué l'affaire Crypto AG, informant notamment la cheffe du DDPS que des médias suisses menaient dorénavant aussi l'enquête et que des discussions avaient eu lieu entre le SRC et les services étrangers concernés. À la suite de cela, le DDPS a élaboré une note d'information sur les liens de Crypto AG avec le domaine du renseignement, destinée à la séance du Conseil fédéral du 6 novembre 2019. La note souligne que les services de renseignement suisses n'ont jamais été directement impliqués dans cette opération menée par des services étrangers, mais qu'ils en ont profité indirectement, car ils avaient pu ainsi se procurer les connaissances techniques correspondantes. Ces déclarations ne reflètent toutefois que de manière incomplète les conclusions pertinentes sur le plan politique et la nécessité de prendre des mesures mises en lumière par le bilan de la situation réalisé en septembre 2019, car le SRC n'a porté ce bilan à la connaissance de la cheffe du DDPS que vers la mi-février 2020.

4.1.4 Informations fournies à l'autorité de haute surveillance

Si la DélCdG s'était penchée à plusieurs reprises sur l'enquête de la PF portant sur Crypto AG en 1994, la société elle-même n'avait jamais fait, jusqu'en 2019, l'objet de discussions entre l'autorité de haute surveillance et les services du DMF puis du DDPS. En revanche, la sécurité des outils de communication de la Confédération et l'utilisation de la cryptologie ont été abordées plusieurs fois. Ainsi, en 2007, le directeur du SRS avait informé la DélCdG que le service suisse renforçait sa collaboration en matière de cryptologie avec un partenaire européen et que cela avait des effets positifs sur l'échange de renseignements dans le domaine de l'exploration radio.

En 2007 toujours, la délégation a également demandé à être informée sur l'utilisation de la cryptologie par le DDPS. L'intégration du décryptage dans le processus d'interception des communications lui a alors été expliquée. Il est notamment ressorti d'une fiche d'information que de nombreux fabricants d'appareils de cryptage intégraient intentionnellement des failles dans les appareils destinés à certains clients et que les services de renseignement américains et ceux de certains de leurs alliés étaient à l'origine de cette pratique. La fiche indiquait également que d'autres pays disposant des compétences nécessaires, tels que la Suisse, pouvaient aussi en profiter: pour ceux-ci, il s'agissait principalement d'identifier les portes dérobées en vue du décryptage.

La DélCdG a mené une autre audition sur le thème de la cryptologie en mai 2009 afin d'approfondir ce sujet. Elle n'a pas non plus été informée à cette occasion que des procédures de cryptage d'entreprises sises en Suisse étaient manipulées pour le compte de services de renseignement étrangers et que ces derniers étaient d'accord pour que la Suisse soit informée des failles en question. La discussion a porté sur la question de la sécurité des appareils achetés par la Suisse.

Le 12 novembre 2019, le président de la DélCdG (*Claude Janiak*) a reçu pour la première fois des informations au sujet de l'affaire Crypto AG, oralement, de la part du DDPS. À la suite de cet entretien, le président de la DélCdG a remis le procès-verbal de l'audition menée par la délégation en mai 2009 à la cheffe du DDPS en mains propres. Cela a été fait de cette manière car il semblait que le DDPS avait besoin de toutes les données disponibles pour pouvoir compléter ses maigres connaissances dans cette affaire.

Le 26 novembre 2019, la DélCdG a été officiellement informée de l'affaire en sa qualité d'organe de haute surveillance. Le directeur du SRC lui a indiqué que la Suisse était au courant de l'opération menée par les services secrets américains avec Crypto AG et a souligné que les évènements pertinents avaient encore eu lieu pendant la guerre froide et faisaient donc partie du passé. Il a précisé que la Suisse avait pu profiter de ces connaissances dans le cadre de ses activités de renseignement, mais que le SRC ou les organisations que celui-ci a remplacées n'avaient pas eu de liens avec Crypto AG dans cette affaire. Pour le directeur du SRC, cette affaire était de l'histoire ancienne et il ne fallait pas lui accorder une trop grande importance.

Pour sa part, la cheffe du DDPS a estimé que cette affaire ne risquait pas de nuire à l'image de la Suisse étant donné que la Confédération n'avait pas de participation dans la société Crypto AG et ne lui était aucunement liée. En outre, cette société n'avait

besoin ni de licence ni d'autorisation de la Confédération. Un groupe de travail interdépartemental (GTID) a par ailleurs été mis en place sous la direction du DDPS pour établir les faits dans cette affaire complexe et garantir une politique de communication envers les médias cohérente pour l'ensemble du Conseil fédéral (cf. ch. 6.1.1).

Lors de la séance du 25 novembre 2019, le DDPS s'est engagé à résumer la suite des investigations dans un rapport et à le remettre à la DélCdG. Un tel rapport n'a toutefois jamais été rédigé. De plus, bien que le secrétariat de la délégation l'ait demandé à plusieurs reprises, le SG-DDPS n'a pas été en mesure de lui fournir une copie de la note d'information que le DDPS avait élaborée pour la séance du Conseil fédéral du 6 novembre 2019. La transmission du document n'a eu lieu qu'une fois l'inspection de la DélCdG ouverte.

4.2 Appréciation de la DélCdG

4.2.1 Légalité de la recherche d'informations (avant 2002)

Lorsque le SRS a commencé à se procurer des informations au sujet des appareils de cryptage «vulnérables» de la société Crypto AG, à l'automne 1993, il n'existait pas encore de base légale spécifique pour le service de renseignement extérieur de l'armée. Le Conseil fédéral avait toutefois déjà proposé de mettre en place de telles dispositions dans son message[23] du 8 septembre 1993 sur la nouvelle loi sur l'armée. Il comptait ainsi notamment mettre en œuvre les interventions de la commission d'enquête parlementaire DMF (CEP DMF)[24].

Dans la nouvelle loi sur l'armée, qui est entrée en vigueur le 19 juin 1995, la mission du SRS était décrite de manière très vague: «rechercher [...] des informations sur l'étranger importantes en matière de politique de sécurité» (art. 99, al. 1, LAAM).

D'après le message sur la LAAM, on entendait par là des «informations concernant les menaces de l'extérieur, qui pourraient entraîner l'engagement de l'armée ou d'une partie de celle-ci». Au cours des années suivantes, la notion de politique en matière de sécurité a été de plus en plus étendue au-delà de la défense nationale militaire. Cela s'est notamment reflété dans la transformation du SRS en office fédéral civil en 2001. En revanche, les bases légales régissant les activités de renseignement civil extérieur n'ont été transférées de la LAAM à la LFRC que neuf ans plus tard.

Toujours selon le message sur la LAAM, seules des informations qui ne pouvaient pas être acquises par des sources accessibles à tous ou ne pouvaient l'être à temps, devaient faire l'objet de la recherche de renseignements militaires. Cela signifie que le SRS pouvait avoir activement recours à des moyens relevant du renseignement, qu'il s'agisse de sources humaines ou de moyens techniques tels que l'exploration radio ou le décryptage.

23 Message du 8.9.1993 relatif à la loi fédérale sur l'armée et l'administration militaire et à l'arrêté fédéral sur l'organisation de l'armée (FF **1993**, vol. IV 1).

24 Iv. pa. Bureau CN «Évènements survenus au DMF. Commissions parlementaires d'enquête» du 13.3.1990 (90.022).

De l'avis de la DélCdG, la LAAM prévoyait que la recherche d'informations sur les États qui avaient acquis des appareils «vulnérables» de Crypto AG, d'une part, et l'acquisition de connaissances sur les procédures de cryptage utilisées par ces appareils, d'autre part, étaient compatibles avec la mission du SRS, dans la mesure où celui-ci devait décrypter les transmissions d'autorités étrangères, en particulier dans le domaine des forces armées et des services de sécurité.

Il convient toutefois de relever que Crypto AG développait et produisait ses appareils en Suisse et les exportait depuis ce même pays. La recherche d'informations sur la société n'était donc admissible que dans la mesure où ces informations serviraient ultérieurement à obtenir des renseignements sur les pays étrangers grâce au décryptage de transmissions étrangères. Le SRS devait par contre éviter de rechercher d'autres informations sur les activités de la société ou de ses employés, ce qui n'a pas toujours été le cas.

Selon le message susmentionné, la LAAM prévoyait un cloisonnement strict entre le SRS et le service de contre-espionnage et de renseignement civil (à l'époque la PF). En ce qui concernait l'activité à l'intérieur, celle-ci devait être limitée au contre-espionnage au sein du SRS lui-même. Si, au cours de son activité, le service de renseignements avait eu connaissance d'agissements délictueux, il aurait dû faire intervenir les autorités chargées de la répression pénale.

Au vu des connaissances dont le SRS disposait au sujet de l'utilisation de procédures de cryptage «vulnérables» par les appareils de Crypto AG, il était clair pour lui que les services américains se servaient de cette faille pour rechercher des informations sur d'autres États. S'il n'était pas du ressort du SRS de rechercher des informations en vue de prouver que des services de renseignement menaient des activités illégales, il aurait dû transmettre ses découvertes au contre-espionnage et aux autorités de poursuite pénale, en particulier lorsque la PF a lancé une enquête dans ce domaine. Or, il ne l'a pas fait et a au contraire déclaré à la PF qu'il ne disposait pas d'indices laissant penser que des services de renseignement étrangers se cachaient derrière la société Crypto AG.

Le SRS a ainsi décidé d'accorder une plus grande importance à sa recherche d'informations et au maintien des bonnes relations avec les services de renseignement américains qu'aux intérêts de la poursuite pénale. La DélCdG estime que le SRS n'était pas habilité à procéder de la sorte et qu'une pesée des intérêts aurait clairement dû avoir lieu au niveau politique.

4.2.2 Légalité de la collaboration avec les services de renseignement américains (après 2002)

La DélCdG estime que, à partir du moment où les services américains ont donné leur accord au partage de connaissances techniques sur les appareils «vulnérables» de Crypto AG avec leur service partenaire suisse, le SRS ne pouvait plus considérer cette opération comme une recherche d'informations secrète, mais devait admettre qu'il s'agissait bien d'une collaboration entre le service suisse et un service de renseignement étranger.

Conformément à la teneur de l'époque de l'art. 99, al. 3, let. c, LAAM, le Conseil fédéral devait régler la collaboration du SRS avec les services étrangers. Comme il ne l'a pas fait, la collaboration entre le SRS et les services partenaires était laissée à l'appréciation du service lui-même ou devait être approuvée par le chef de département[25]. À la suite de sa première inspection relative aux relations entre le service de renseignement suisse et l'Afrique du Sud, la DélCdG a recommandé que la compétence de décider de la prise de contacts réguliers avec l'étranger, de l'entretien de tels contacts et du contrôle y afférent revienne au Conseil fédéral[26].

Lorsque, début 2001, le SRS a été transféré dans un office fédéral civil, le Conseil fédéral a procédé à une révision totale de l'ORen[27], qui datait de 1995. Conformément à la nouvelle teneur de l'ordonnance, devenue l'ORens[28] (art. 6), le Conseil fédéral devait approuver l'entretien de contacts réguliers avec l'étranger.

L'approbation du Conseil fédéral en matière de collaboration couvrait une large palette d'activités de renseignement: celles-ci allaient de l'échange de données aux entretiens entre experts en passant par la gestion commune de sources ou la conduite d'opérations conjointes pour obtenir des renseignements. On peut considérer que le transfert de connaissances concernant les procédures de cryptage «vulnérables» utilisées par les appareils de Crypto AG était aussi concerné. Le service de renseignement américain qui a donné son accord pour la transmission d'informations relatives aux appareils de cryptage de Crypto AG figurait dès le début sur la liste des contacts étrangers approuvés par le Conseil fédéral.

Comme cela a été expliqué au ch. 4.1.1, l'accès systématique du SRS aux informations concernant les procédures de cryptage de Crypto AG n'a été possible que parce que les services américains y avaient consenti. La DélCdG considère donc que le canal d'information fondé sur cet accord constituait une collaboration en matière de renseignements au sens de l'art. 99, al. 3, let. c, LAAM. L'élément décisif pour l'appréciation de la délégation est l'existence avérée de cette collaboration, qui était connue de la direction du SRS. Aux yeux de la DélCdG, les circonstances concrètes de l'avènement de cette collaboration ne sont pas déterminantes, pas plus que la façon dont elle s'est déroulée dans les faits. Il convient de relever par ailleurs que l'art. 99, al. 3, let. c, LAAM était la seule disposition légale sur laquelle le SRS pouvait s'appuyer pour accéder à ces informations. Cette disposition de la loi sur l'armée est restée en vigueur lors de la création du SRC et a ensuite été intégrée dans la LRens (cf. ch. 5.1).

Du point de vue de la DélCdG, la position défendue par les responsables du SRS, selon lesquels il n'y avait aucune collaboration de ce genre entre le SRS et les services américains, est incompréhensible et, sur le plan juridique, inexacte. Cette position est également problématique parce qu'elle a servi de prétexte à la direction du SRS pour ne pas informer l'organe chargé de la surveillance directe.

25 Rapport annuel 2001/2002 des CdG et de la DélCdG du 17.5.2002, ch. 9.1 (FF **2002** 5521 5552).
26 Le rôle des Services de renseignements suisses dans le cadre des relations entre la Suisse et l'Afrique du Sud, rapport de la DélCdG du 12.11.1999 (FF **2000** 505 512).
27 Ordonnance du 4.12.1995 sur le renseignement (ORen; RO **1995** 5298).
28 Ordonnance du 4.12.2000 sur le renseignement du DDPS (ORens; RO **2001** 124).

Comme la DélCdG l'a appris de la bouche du directeur actuel du SRC (*Jean-Philippe Gaudin*), les services américains partaient du principe que, au sein du service de renseignement suisse, les responsables successifs seraient informés de la collaboration. Il est évident que les services américains étaient conscients de l'utilité de leur entente avec le service suisse pour garantir le bon déroulement de leur opération. De l'avis de la DélCdG, le fait que le SRS et les services américains agissaient d'un commun accord implique aussi une coresponsabilité des autorités suisses dans les activités de Crypto AG.

4.2.3 Opportunité et efficacité de la recherche d'informations

La DélCdG arrive à la conclusion que les informations que la Suisse a pu obtenir grâce à ses connaissances au sujet des procédures de cryptage «vulnérables» utilisées par les appareils de Crypto AG se sont avérées, au fil des ans, profitables en termes de renseignement pour la Suisse.

Ces connaissances ont pu être directement utilisées pour décrypter des communications en provenance des États étrangers. Ce savoir-faire a aussi constitué une précieuse base pour les échanges d'expériences et de données avec des services de renseignement étrangers, ce qui a permis d'améliorer encore les capacités de la Suisse en matière de décryptage et de renforcer sa position dans le milieu du renseignement.

La DélCdG connaît plusieurs cas concrets où ces capacités de décryptage ont donné des résultats dont les autorités suisses et l'armée ont pu retirer des avantages considérables. Il convient de relever toutefois que les procédures de cryptage et les possibilités d'accéder aux communications pertinentes changeaient constamment, raison pour laquelle le savoir-faire acquis pouvait rapidement perdre de son efficacité.

Pour la sécurité de la Suisse, il est nécessaire que les appareils de cryptage achetés à l'intention de ses propres autorités soient sûrs. La capacité de contrôler la sûreté des appareils et celle d'exploiter leurs faiblesses sont indissociablement liées. Ainsi que l'a montré l'inspection menée par la DélCdG, la Suisse est parvenue à identifier les points faibles de différents types d'appareils et à éliminer elle-même les défauts en question. La délégation a aussi pu constater à quel point il était important de bien connaître les fournisseurs établis dans son pays et de pouvoir influer sur la qualité de leurs produits. Les informations que le service de renseignement a pu obtenir ont grandement contribué à ce que ce soit le cas.

4.2.4 Opportunité de la surveillance et de la conduite exercées par le DMF et le DDPS

Avant sa transformation en office fédéral civil, le SRS faisait partie du Grrens, qui était lui-même subordonné au chef de l'État-major général. La recherche d'informations sur Crypto AG a eu lieu sans que le commandement militaire le sache. Cette situation soulève dès lors la question du fonctionnement interne du Grrens, laquelle

n'a pas été approfondie par la DélCdG dans le cadre de l'inspection faisant l'objet du présent rapport.

Le chef du DMF de l'époque (*Kaspar Villiger*) n'était pas directement impliqué dans la conduite du SRS militaire. Ainsi que le confirme une note d'information de mars 1994 établie par le SRS sur l'affaire Bühler, il avait été laissé dans l'ignorance au sujet des véritables propriétaires de Crypto AG, alors que le chef du SRS (*Fred Schreier*) les connaissait déjà à ce moment-là. Toutefois, le chef du DMF était suffisamment préoccupé par les accusations portées contre l'entreprise pour se renseigner auprès des spécialistes compétents des troupes de transmissions à propos de la sécurité des appareils de cryptage de l'armée.

En tant qu'office fédéral civil, le SRS était placé sous la conduite politique du DDPS, et même directement subordonné au chef de département à partir de 2004, en vertu de l'art. 99, al. 5, LAAM. L'inspection menée par la DélCdG ne laisse pas supposer que le directeur du SRS (*Hans Wegmüller*) aurait informé son chef de département (*Samuel Schmid*) des relations existant entre les services de renseignement américains et Crypto AG ou des informations auxquelles avait accès le SRS. Si l'on se fonde sur l'appréciation juridique émanant de la DélCdG, selon laquelle le SRS civil a en fin de compte collaboré avec les services américains, le chef du DDPS aurait pourtant dû impérativement être mis au courant.

Comme la DélCdG l'a appris à la lecture des notes manuscrites du chef du DDPS datant des années 2002 à 2008 (cf. ch. 2.1.2), la sécurité des appareils de cryptage de la Confédération a fait l'objet de plusieurs discussions entre le directeur du SRS et le chef du DDPS. Quand il a été avéré qu'un fabricant suisse (autre que Crypto AG) avait livré des appareils peu fiables à la Confédération et à deux grandes entreprises, le DDPS a pris les mesures qui s'imposaient afin de combler les failles. Le chef du DDPS était d'ailleurs informé régulièrement du déroulement de l'affaire par le SRS.

Le SRC et sa nouvelle direction sont devenus opérationnels en 2010. Du point de vue de la DélCdG, le premier directeur du SRC (*Markus Seiler*) n'a intentionnellement pas assumé sa responsabilité lorsque des indices évidents concernant Crypto AG lui ont été soumis en 2017 et qu'il a refusé de prendre possession de ces informations sous forme écrite. Par son attitude, il a notamment empêché que la direction politique du département ne puisse se pencher sur les aspects de la question qui la concernaient. Rétrospectivement, l'omission du premier directeur du SRC paraît d'autant plus grave que le SRC aurait encore pu, à cette époque, préparer sans urgence les décisions de conduite nécessaires et les appliquer d'entente avec la direction du département, voire avec le Conseil fédéral. Lorsque le SRC a dû faire face au problème, deux ans plus tard, les circonstances étaient beaucoup plus difficiles en raison de la pression médiatique.

La DélCdG ne dispose pas d'informations lui indiquant que le premier directeur du SRC a été informé de l'étendue du problème concernant Crypto AG par son adjoint (*Paul Zinniker*). Celui-ci avait été directeur du SRS et, au sein de ce dernier, il avait été personnellement impliqué dans la genèse de l'affaire Crypto AG (cf. ch. 4.1.2). Lorsque son supérieur hiérarchique est devenu le secrétaire général du Département fédéral des affaires étrangères (DFAE), il a dirigé le SRC par intérim, de décembre 2017 à juillet 2018. À la passation de pouvoir au directeur actuel du SRC

(*Jean-Philippe Gaudin*), le cas de Crypto AG n'a pas été évoqué. Du point de vue de la DélCdG, le directeur du SRC aurait toutefois dû être informé en détail par son adjoint au plus tard à l'été 2019, quand les des médias ont commencé à s'intéresser à Crypto AG (cf. ch. 4.1.3).

Dans ces circonstances, les anciens chefs du DMF et du DDPS n'ont pas pu assumer leur responsabilité en matière de conduite. Selon la DélCdG, il aurait pourtant été essentiel qu'ils soient en mesure de le faire car la situation ne relevait pas de la seule appréciation des personnes directement responsables au sein du service de renseignement.

4.2.5 Opportunité de la façon de procéder du SRC et des informations fournies à la cheffe du DDPS

Au printemps 2019, le directeur actuel du SRC a reçu à peu près les mêmes informations que son prédécesseur en 2017. Il en a profité pour faire dresser un bilan de la situation concernant Crypto AG. Ce bilan devait aussi mettre en lumière la nécessité pour le SRC de prendre des mesures. De plus, le directeur du SRC a attiré en temps utile l'attention de la cheffe du DDPS sur l'intérêt que les médias allaient bientôt porter à Crypto AG.

Néanmoins, la DélCdG regrette que la direction du SRC n'ait pas été en mesure, après avoir reçu ledit bilan sous forme écrite, de déterminer correctement le rôle de son propre service en qualité d'organe ayant succédé au SRS et d'en tirer les conséquences politiques. En particulier, le directeur du SRC aurait dû veiller à ce que, au sein de son service, toutes les informations disponibles soient rapidement rassemblées et soumises à une analyse approfondie. Il aurait dû confier cette mission à une personne compétente, dotée de l'expérience requise.

À cause du fait que le nouveau directeur du SRC n'avait pas été informé de la situation par le directeur par intérim, puis adjoint (cf. ch. 4.2.4), et de l'évaluation incomplète et insatisfaisante de la situation réalisée pour cette raison, les efforts du service et du DDPS ont surtout consisté, dès l'automne 2019, à anticiper les questions et les articles des médias et à élaborer une stratégie de communication appropriée à cet égard. L'analyse du rôle du SRC et des organes qui l'avaient précédé n'a été effectuée qu'à la suite des indications qui avaient été transmises au fur et à mesure aux membres dirigeants du service, auxquelles aucun caractère d'urgence n'avait été accordé.

Au lieu d'approfondir la nature des relations que le service de renseignement suisse entretenait avec Crypto AG et les services américains, le directeur du SRC s'est contenté de relativiser leur importance pour le SRC et pour libérer le service actuel de toute responsabilité. Cette volonté de protéger son propre service et la cheffe du département sont la cause des insuffisances de l'appréciation de la situation qui s'en est suivie à l'égard du département et de la DélCdG.

Le SG-DDPS n'a pas non plus discerné la portée de la problématique, nonobstant le fait qu'il comptait un poste de conseiller en renseignement auprès de la cheffe de département.

En outre, le DDPS a manqué l'occasion de se pencher de manière approfondie sur les questions stratégiques qui se posaient en relation avec l'affaire Crypto AG, concernant la compétence de la Suisse en matière de cryptologie aussi bien dans le domaine du renseignement que dans celui de l'armée ou celui de l'industrie. Le commandement de l'armée n'a pas été consulté, alors que la sécurité des réseaux de l'armée et le succès de projets importants étaient directement concernés.

5 Questions générales pour l'avenir

5.1 Opérations relevant du renseignement effectuées avec la collaboration d'entreprises suisses

La Suisse n'est membre d'aucune alliance militaire et est tenue de respecter le principe de neutralité armée. Étant donné son indépendance politique et les bonnes relations qu'elle entretient aux échelons bilatéral et multilatéral, les autres États n'ont guère de raisons de supposer que la Suisse représente une menace pour eux. Les entreprises et les organisations qui exercent une activité sur le territoire suisse profitent, à l'étranger, de l'image de neutralité du pays. Les services de renseignement étrangers peuvent donc voir un intérêt à se cacher derrière des entreprises suisses pour effectuer des opérations au préjudice d'un État tiers.

Pour les activités de ce type faisant partie des éléments constitutifs d'espionnage (art. 272 à 274 et art. 301 CP)[29], il incombe au contre-espionnage de s'y opposer, c'est-à-dire au SRC et aux autorités de poursuite pénale, qui assument ce rôle dans le cadre de leurs attributions respectives. Si leurs démarches aboutissent à une procédure pénale, c'est le DFJP ou le Conseil fédéral qui décide en dernier ressort de la poursuite judiciaire des personnes responsables.

On peut également imaginer qu'un service de renseignement étranger cherche à collaborer avec le SRC en vue d'exploiter les avantages de la Suisse dans une opération de renseignement et qu'il soit disposé, en échange, à faire profiter le SRC des résultats de l'opération. Comme l'art. 12, al. 1, let. c, LRens autorise le SRC à participer à des activités communes visant à rechercher des informations, à les évaluer et à apprécier la menace, une telle collaboration est tout à fait licite («*Joint Operation*»). Aux termes de l'art. 34 LRens, le SRC peut en outre confier des mandats à des services étrangers et à des particuliers pour la recherche d'informations, que ce soit en Suisse ou à l'étranger.

L'art. 36, al. 1, LRens dispose que le SRC peut collecter secrètement des informations sur des évènements se produisant à l'étranger. La loi est muette pour ce qui est des modalités applicables, mais l'art. 36, al. 3, LRens impose au SRC de veiller à ce que les risques pris lors de la recherche d'informations ne soient pas disproportionnés par rapport au but. Le bénéfice apporté par les informations doit ainsi être proportionnel aux risques opérationnels et politiques d'une opération et aux atteintes aux droits fondamentaux des personnes concernées.

29 Code pénal suisse du 21.12.1937 (CP; RS **311.0**).

La recherche d'informations par le SRC doit être axée sur les menaces actuelles en matière de politique de sécurité. Dans la mission de base confiée au SRC, le Conseil fédéral détermine les États qui constituent des objectifs de recherche prioritaires. En approuvant les contacts étrangers, le Conseil fédéral définit les services de renseignement étrangers avec lesquels il estime qu'il est politiquement opportun de coopérer. Le service de renseignement est donc un instrument que le Conseil fédéral peut solliciter en fonction des menaces et de l'opportunité politique. Une égalité de traitement sans réserve d'États étrangers dans le domaine du renseignement n'est pas prévue et irait d'ailleurs à l'encontre de la proportionnalité exigée par la loi.

Conformément au droit en vigueur, il est donc permis au SRC et à un service étranger d'utiliser, ensemble, une entreprise sise en Suisse afin de rechercher des informations sur l'étranger (cf. art. 34, al. 2, LRens). En cas de participation du SRC à une telle opération, les activités du service de renseignement étranger ne font pas partie des éléments constitutifs d'espionnage.

Si une entreprise suisse devait être partie prenante dans une collaboration du SRC avec un service partenaire, il serait absolument nécessaire, selon la DélCdG, que les conséquences politiques possibles soient analysées au préalable par les autorités politiques. Il y aurait en particulier lieu d'examiner spécialement les conséquences pour la place économique suisse et pour les personnes éventuellement touchées au sein de ladite entreprise. Il s'agirait de prendre aussi en considération les effets de cette collaboration sur la politique extérieure de la Suisse en général et sur les relations bilatérales concernées en particulier.

Aux yeux de la DélCdG, il faut par conséquent que le Conseil fédéral étudie les possibilités que la LRens offre au SRC. Le Conseil fédéral doit notamment établir quelle marge de manœuvre politique il est prêt à octroyer au DDPS et dans quelles circonstances il souhaite recevoir des informations ou décider de telles opérations.

5.2 Une cryptographie sûre en Suisse

La possibilité de disposer d'outils de cryptographie sûrs est une condition sine qua non pour assurer la sécurité des infrastructures de communication et d'information suisses. Ainsi, garantir la sûreté du cryptage au niveau de la transmission des données est indispensable dans le cadre des deux projets du DDPS, «Réseau de conduite Suisse» et «Télécommunications de l'armée». Sans cela, l'investissement d'environ 2,2 milliards de francs qu'ils représentent est remis en question. De même, le DFAE et le SRC doivent disposer de liaisons sécurisées pour leurs communications.

L'un des principaux enseignements découlant de l'inspection de la DélCdG est que les fournisseurs de technologie de cryptage sont des cibles de choix dans le cadre des tentatives d'infiltration de services de renseignement étrangers. L'histoire de Crypto AG montre que les entreprises suisses peuvent elles aussi, sous l'influence de services de renseignement étrangers, produire des appareils pour lesquels les procédures de cryptage sont «vulnérables». Dans le même temps, il ressort de cette inspection que les autorités suisses ont quand même pu garantir la sûreté de leurs propres appareils.

Comme la DélCdG a pu s'en assurer, toutes les vérifications effectuées ont confirmé que Crypto AG n'a jamais livré aux autorités suisses d'appareils dont les procédures de cryptage étaient «vulnérables», contrairement à une autre société qui a vendu de tels outils à l'administration fédérale, y compris aux services de renseignement (cf. ch. 4.2.4). Il est donc impératif que la Confédération dispose de compétences suffisantes dans le domaine de la cryptologie, car seules ces compétences permettront de contrôler la sûreté des appareils, voire d'influer sur leur conception. Cela exige d'avoir la capacité et les connaissances nécessaires pour déchiffrer des cryptages étrangers, une faculté incontournable si l'on veut instaurer une collaboration entre les services de renseignements, telle que décrite au ch. 5.1.

Enfin, la Confédération ne peut influer de manière satisfaisante sur la sûreté des appareils de cryptage afin qu'ils répondent à ses exigences et à ses besoins que si ces derniers sont conçus et produits en Suisse et si le fournisseur est clairement en mains suisses. Par contre, la Confédération n'a pratiquement aucune possibilité d'influer sur la fiabilité des fournisseurs étrangers. Par conséquent, la DélCdG considère que la Confédération ne pourra compter sur des outils de cryptage fiables que si ces derniers sont produits à l'intérieur du pays par une industrie spécialisée dans le chiffrement sise en Suisse.

Au cours de ses investigations, la DélCdG a pu constater que ni le Conseil fédéral ni en particulier le Département fédéral de l'économie, de la formation et de la recherche (DEFR) n'avaient pas pris conscience de l'importance du fait que la fiabilité des techniques de cryptage ne peut être assurée qu'en coopération avec des fournisseurs indigènes. Même au sein du DDPS, qui avait encore indiqué au Conseil fédéral, le 6 novembre 2019, que les articles de presse qui devaient être publiés sur l'affaire Crypto AG mettaient en danger l'existence même des entreprises appelées à succéder à cette dernière, cette thématique n'était pas considérée comme prioritaire.

D'après les investigations de la DélCdG, le chef de l'armée (CdA) comme le SG-DDPS ont abordé, en février 2020, les conséquences éventuelles que pourrait avoir pour l'armée une perte de son fournisseur d'instruments de cryptage. Néanmoins, il apparaît qu'aucune stratégie visant à trouver d'autres options que les appareils fournis par les entreprises qui ont succédé à Crypto AG n'a été définie. De même, la cheffe du DDPS et le CdA n'ont jamais discuté des mesures à prendre pour garantir que l'armée dispose d'instruments de cryptage sûrs si ses fournisseurs actuels devaient cesser leur activité.

Le 19 juin 2020, le Conseil fédéral a donné son autorisation au MPC pour ouvrir une procédure pénale concernant les exportations antérieures de Crypto AG et a décidé de geler l'approbation des demandes d'exportation déposées par Crypto International AG et TCG Legacy AG jusqu'à ce que cette procédure pénale soit close (cf. ch. 8.4). Peu avant la décision du Conseil fédéral, le DDPS avait relevé la dépendance de la Suisse vis-à-vis des sociétés qui ont succédé à Crypto AG, notamment de CyOne Security AG, mais n'avait pas été en mesure, comme le montre la proposition du DFJP du 17 juin 2020, d'évaluer les conséquences pour l'armée d'une éventuelle faillite de Crypto International AG, qui était violemment touchée par le gel illimité des exportations. Ce n'est qu'en septembre 2020 que le DDPS a entrepris des investigations sérieuses pour clarifier la question. Les informations transmises par le CdA à la DélCdG sur les investigations en cours auprès des entreprises concernées etaient insuffisantes.

La DélCdG estime que le Conseil fédéral n'a pas suffisamment pris en compte l'intérêt fondamental pour la Suisse de disposer d'instruments de cryptographie fiables dans sa décision du 19 juin 2020. Mais il faut dire que le DDPS n'avait pas mené une étude approfondie ni déterminé de manière convaincante les risques auxquels s'exposait la Confédération, et notamment l'armée.

La DélCdG considère qu'il ne lui revient pas de procéder, dans le cadre de son inspection, aux clarifications et aux études de risques qui auraient dû être menées par l'exécutif. Elle ne peut pas non plus présumer de l'issue de la procédure pénale, ni des procédures de recours que les entreprises concernées ont engagé contre les décisions de refus des autorisations d'exportation émises par le Conseil fédéral. Par conséquent, la délégation s'abstiendra de juger dans quelle mesure les décisions du Conseil fédéral ont durablement remis en question l'accès de la Suisse à des instruments de cryptographie sûrs.

6 Mesures prises par le DDPS et le Conseil fédéral

6.1 Décision du Conseil fédéral du 20.12.2019

6.1.1 Institution et travaux du groupe de travail interdépartemental

Le 7 novembre 2019, lors d'une séance réunissant la cheffe du DDPS (*Viola Amherd*), le vice-chancelier de la Confédération, le secrétaire général du DDPS, la secrétaire générale du DFJP et des représentants du SRC, décision a été prise d'instituer un groupe de travail interdépartemental (GTID) en rapport avec Crypto AG. À ce moment-là, les informations étaient floues et plusieurs départements avaient reçu des demandes fondées sur la loi sur la transparence (LTrans)[30] et la LAr. Le GTID était chargé de rassembler les informations disponibles et d'en établir une synthèse qui permettrait de décider notamment de la marche à suivre. Les faits concernant l'entreprise Crypto AG devaient être examinés de manière approfondie. Le GTID a siégé une première fois le 18 novembre 2019, sous la direction du secrétaire général du DDPS. La ChF y avait été conviée, car on partait de l'idée que le Conseil fédéral dans son ensemble était aussi directement concerné et que la ChF devait coordonner les informations. Différentes auditions menées dans le cadre de l'inspection ont révélé que la tâche confiée au GTID n'avait pas été interprétée uniformément par tous ses membres, ce qui tendrait à démontrer qu'elle n'avait pas été formulée assez clairement.

Lors de cette première séance, le GTID (composé des secrétaires généraux du DDPS et du DFJP, du vice-chancelier de la Confédération, du chef de la division NDBU, d'un représentant de l'OFJ et d'autres représentants du DDPS) a décidé de traiter l'affaire en deux étapes successives. D'une part, il fallait procéder à une étude historique. D'autre part, le GTID entendait dresser un état des lieux des développements les plus récents. La priorité devait toutefois consister à élaborer d'abord une chronologie, afin

30 Loi fédérale du 17.12.2004 sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans; RS **152.3**).

de pouvoir, dans un deuxième temps, répondre à des questions concrètes et préparer une stratégie et la communication. Le GTID a en outre décidé que, à partir de sa deuxième séance, il accueillerait également un représentant du DFAE et un autre du MPC. Dans la note relative à la première séance du GTID, on peut lire que la DélCdG aurait été informée en 2009, par le DDPS, de certains aspects de l'affaire Crypto AG. Or, cette affirmation ne correspond pas au contenu du procès-verbal que le président de la DélCdG a fait parvenir à la cheffe du DDPS à la suite de leur rencontre du 12 novembre 2019 (cf. ch. 4.1.4).

Quatre autres séances du GTID ont eu lieu (les 29 novembre et 9 décembre 2019 et les 10 février et 2 mars 2020). À partir de la troisième séance, plusieurs représentants du SG-DEFR et des AFS étaient également présents. Il semble que deux aspects en particulier ont retenu l'attention du GTID: les demandes de consultation en vertu de la LTrans et l'élaboration de la chronologie par le SRC. Celui-ci a présenté une première chronologie au GTID lors de la séance du 9 décembre 2019. Le document a cependant été renvoyé au SRC pour remaniement, car il était nébuleux et incomplet – il y manquait par exemple les informations concernant les 20 dernières années.

En fin de compte, le GTID a renoncé à dresser lui-même un état des lieux détaillé, vu les travaux commencés le 16 janvier 2020 par Niklaus Oberholzer (cf. ch. 6.2). La DélCdG constate, au vu de ses connaissances actuelles, que les résultats du bilan effectué à l'automne 2019 à la demande du directeur du SRC n'ont pas été pris en considération dans les travaux du GTID. D'après les explications fournies par la cheffe du DDPS, le chef NDBU a été prié, lors des quatre premières séances du GTID, de dire s'il existait d'autres documents ou informations, mais il a toujours répondu par la négative. Seules de rares personnes connaissaient la teneur du bilan qui avait été établi, et le chef NDBU en faisait partie. En fait, le SRC ne voulait pas évoquer la collaboration qu'il entretenait avec les services de renseignement américains au sujet de Crypto AG au sein du GTID et il a donc fait en sorte que celui-ci n'approfondisse pas cette question dans le cadre de ses travaux. C'est ainsi que les dossiers découverts dans l'installation K n'ont pas non plus été mentionnés. Selon les dires de la cheffe du DDPS, si elle avait connu à cette époque le bilan de la situation réalisé à l'automne 2019, il aurait été possible de s'abstenir d'instituer un GTID et le mandat confié à M. Oberholzer aurait été d'une autre nature. Le GTID a décidé de ne pas se dissoudre et de continuer à siéger en fonction des besoins. Le 15 janvier 2020, le Conseil fédéral a décidé que le GTID devrait soutenir, à titre consultatif, le comité de recherche désigné autour de M. Oberholzer.

Globalement, il convient de relever que, pour remplir les tâches précitées, le GTID s'est en premier lieu occupé de traiter des questions formelles et de renseigner les médias. Dans le contexte de l'intervention de la DélCdG et après la révélation du bilan réalisé par le SRC, le GTID n'assumait plus qu'une fonction de coordination et ses travaux ne pouvaient servir de base de décision au Conseil fédéral que dans une mesure restreinte.

6.1.2 Découverte de dossiers dans l'installation K

Le 12 novembre 2019, le SRC a reçu des premiers renseignements, encore vagues, sur l'existence probable d'autres documents concernant Crypto AG. Il s'est écoulé ensuite près d'un mois – jusqu'au 10 décembre 2019 – avant que ces informations ne soient vérifiées. Le jour suivant, huit boîtes remplies de dossiers liés à Crypto AG ont été découvertes dans un lieu extérieur aux AFS (l'installation K, cf. ch. 2.1.4). Le directeur du SRC a été mis au courant le 12 décembre 2019 de cette découverte et de premiers éléments d'information. À la question de savoir pourquoi le SRC avait attendu près d'un mois pour se pencher effectivement sur les indices qu'il avait reçus, le directeur du SRC a répondu qu'il ne s'agissait pas d'une urgence.

Cette réponse agace la DélCdG étant donné que la clôture du bilan établi à l'automne 2019 (cf. ch. 4.1.4) avait été anticipée afin de donner au directeur du SRC un avantage en matière d'information dans la perspective d'éventuels articles de presse. De l'avis de la DélCdG, le fait que le SRC n'a pas agi plus rapidement à propos des dossiers découverts dans l'installation K, sous prétexte qu'il n'y voyait aucune urgence, montre que les responsables au sein du SRC n'avaient pas mesuré l'ampleur et la portée de l'affaire.

Divers éléments confirment le point de vue de la DélCdG: les dossiers découverts dans l'installation K n'ont été que sommairement parcourus, ils n'ont pas été répertoriés de façon exhaustive et n'ont fait l'objet d'aucune évaluation. Le 17 février 2020, lorsque la DélCdG a demandé un répertoire du contenu de ces documents, le SRC n'a pu lui livrer que des mots clés, qu'un collaborateur avait notés de son propre chef et qui ne se rapportaient qu'à certaines boîtes.

Le 16 décembre 2019, le directeur du SRC a rapporté oralement à la cheffe du DDPS que des documents avaient été trouvés dans une installation K. Après quoi, le Conseil fédéral s'est penché une deuxième fois sur l'affaire Crypto AG, à sa séance du 20 décembre 2019.

6.1.3 Bases de la décision du Conseil fédéral du 20.12.2019

La proposition que le DDPS a adressée au Conseil fédéral en vue de la séance du 20 décembre 2019 précisait que les informations connues étaient insuffisantes pour qu'un débat de fond puisse être tenu au Conseil fédéral. Aujourd'hui, à la lumière des constatations faites par la DélCdG, il apparaît que cette affirmation était juste, non pas parce qu'on ne disposait pas de toutes les informations nécessaires, mais parce que celles-ci n'avaient pas été consultées ou traitées de manière adéquate et avec la célérité requise par le SRC. En outre, le DDPS n'a pas informé correctement le Conseil fédéral, sinon il n'aurait pas déclaré, dans sa proposition, qu'il n'existait presque pas de documents officiels, ou qu'ils étaient introuvables, et que le SRC n'avait accès qu'à relativement peu de documents. À ce moment-là, le SRC connaissait déjà l'existence des dossiers découverts dans l'installation K, même s'il ne les avait pas encore étudiés en détail; certains mots clés relatifs au contenu de ces documents avaient été retrans-

crits et étaient alors disponibles. Concernant lesdits dossiers, on avait seulement indiqué à la cheffe du DDPS qu'un ancien membre du Conseil fédéral était probablement au courant des différents événements.

D'après les données disponibles à ce jour, on peut conclure que le bilan réalisé à l'automne 2019 contenait toutes les informations importantes permettant de comprendre la portée et les conséquences de l'affaire Crypto AG. Ces informations n'ont toutefois pas été communiquées de façon satisfaisante au Conseil fédéral en vue de ses séances des 6 novembre 2019 et 20 décembre 2019, ce qui explique pourquoi le gouvernement en savait si peu (cf. ch. 4.1.3). On a argué que les sources ayant servi à établir ce bilan étaient très minces et que celui-ci aurait encore dû être complété de façon substantielle, mais cela n'a jamais été fait.

Comme il l'a été mentionné au ch. 4.1.3, le SRC a reçu le rapport MINERVA en octobre 2019, en même temps que d'autres documents. Le 21 novembre 2019, le vice-chancelier de la Confédération et deux représentants du SG-DDPS ont consulté ces pièces durant une heure. Compte tenu du volume de la documentation, il convient de relever qu'une heure était loin de suffire à une étude sérieuse de celle-ci. Les représentants de la ChF et du SG-DDPS, qui sont aussi membres du GTID, avaient été chargés de cette mission par ce dernier. À la deuxième séance du GTID, on a simplement annoncé que les documents avaient été examinés et qu'ils devraient jouer un rôle important dans l'élaboration de la chronologie. En l'état actuel des connaissances, les informations issues de ces documents n'ont toutefois pas été prises en considération lorsque le Conseil fédéral a pris sa décision, le 20 décembre 2019.

En raison des informations lacunaires transmises par le SRC au GTID et de l'ignorance qui en a résulté (cf. ch. 6.1.1), le GTID a jugé nécessaire, le 9 décembre 2019, de soumettre trois propositions de marche à suivre au Conseil fédéral, dont l'une consistait à recourir à des personnes extérieures afin de procéder à de plus amples investigations. C'est ainsi que, suivant une recommandation du DDPS, le Conseil fédéral a décidé, le 20 décembre 2019, de confier à un comité de recherche le mandat de traiter l'affaire Crypto AG et qu'il a chargé le DDPS de lui soumettre, avant sa séance du 15 janvier 2020, une candidature pour la direction de ce comité. De plus le département devait aussi informer le Conseil fédéral jusqu'à fin février 2020 de la procédure ultérieure. En résumé, le Conseil fédéral a été mal aiguillé.

On peut déduire de la communication adoptée lors de cette séance que le Conseil fédéral partait du principe qu'il s'agissait simplement d'un travail de recherche historique.

6.2 Nomination du chargé d'enquête

Le 23 décembre 2019, un premier entretien s'est déroulé au SG-DDPS, au cours duquel la possibilité a été évoquée de nommer l'ancien juge fédéral Niklaus Oberholzer à la tête du comité de recherche. Une discussion initiale avec l'intéressé a eu lieu le 8 janvier 2020, lors de laquelle celui-ci s'est déclaré prêt à diriger le comité de recherche.

À sa séance du 15 janvier 2020, le Conseil fédéral a décidé, sur la proposition du DDPS, de nommer Niklaus Oberholzer chef du comité de recherche. Aux termes de la décision en question, le mandat de ce comité était le suivant: procéder à un examen complet des faits concernant l'entreprise Crypto AG depuis 1945 jusqu'à sa scission en février 2018.

Il s'agissait notamment de clarifier le rôle tenu par l'administration fédérale et par les autorités politiques. Selon la proposition du DDPS, les questions de la légalité et de l'opportunité des activités de renseignement relevaient de la compétence des autorités ordinaires de surveillance (AS-Rens et DélCdG). Le mandat prévoyait en outre qu'un rapport soit présenté au Conseil fédéral à la fin du mois de juin 2020 au plus tard. Étant donné l'urgence de la mission et le nombre important de documents à consulter, M. Oberholzer s'est vu adjoindre plusieurs juristes d'un cabinet d'avocats renommé, mais il n'a pas sollicité leur assistance. Il est entré en fonction le 16 janvier 2020.

Pour la DélCdG, le fait que le mandat d'enquête portait jusqu'à février 2018 montre que la possibilité de trouver des liens avec l'actualité n'a pas été envisagée. Par ailleurs, ce mandat se fondait sur des connaissances lacunaires du GTID.

Lorsque Niklaus Oberholzer a entamé l'exécution de son mandat, le 16 janvier 2020, il n'avait reçu du DDPS que la chronologie incomplète que le SRC avait établie à l'intention du GTID (cf. ch. 6.1.1). Il ne disposait pas du rapport MINERVA et ignorait l'existence des dossiers découverts dans l'installation K. C'est par l'intermédiaire des médias qu'il a pris connaissance pour la première fois d'éléments relatifs au rapport MINERVA. Le 15 février 2020, M. Oberholzer a rédigé une note à l'intention de la cheffe du DDPS (*Viola Amherd*) en réaction au débat médiatique concernant le fait que certains conseillers fédéraux avaient eu connaissance de l'affaire. Comme il ignorait l'existence des documents découverts dans l'installation K, il a conclu que cela ne pouvait être prouvé à partir des documents en sa possession. Le jour suivant, la presse dominicale se faisait l'écho des dossiers découverts dans l'installation K, lesquels prouvaient, d'après les journalistes, que le chef du DMF d'alors (*Kaspar Villiger*) devait être au courant.

À cause de l'approche du DDPS, il était impossible que l'enquête Oberholzer fournisse rapidement des informations dignes de foi et utiles à de futures décisions politiques. La tâche prioritaire du comité de recherche était de clarifier les évènements historiques et non de soutenir le Conseil fédéral dans la gestion de l'affaire Crypto AG. Certes, le Conseil fédéral avait prévu la possibilité de préciser encore le mandat d'enquête après une première consultation des documents disponibles, mais cela restait irréalisable tant que le DDPS – en raison du manque d'échange d'informations en son sein – ne donnait pas accès aux documents qui se trouvaient en sa possession.

6.3 Rôle de la Délégation pour la sécurité

Lors de la séance de la Délégation pour la sécurité (Délséc) du 18 février 2020, la cheffe du DDPS (*Viola Amherd*) a fait savoir qu'elle informerait le Conseil fédéral le lendemain des premiers résultats intermédiaires de l'enquête Oberholzer. Le Conseil

fédéral a ensuite reçu la note que M. Oberholzer avait rédigée à l'intention de la cheffe du DDPS le 15 février 2020 sans connaître les documents les plus importants.

Par la suite, l'affaire Crypto AG n'a plus été abordée au sein de la Délséc. Par exemple, cette dernière n'a pas profité de sa séance du 5 mai 2020 pour discuter de la demande d'autorisation déposée par le MPC le 13 mars 2020 auprès du DFJP (cf. ch. 8.4.3). Le DFAE n'a pas non plus abordé les difficultés diplomatiques qui se profilaient avec les pays amis concernés par la suspension des livraisons par les entreprises ayant succédé à Crypto AG.

La séance prévue de la Délséc du 20 août 2020 a été annulée faute de thèmes urgents à traiter, alors qu'à ce moment-là tous les membres du Conseil fédéral avaient reçu une demande de réexamen de la part de Crypto International AG concernant la suspension de ses licences d'exportation (cf. ch. 8.5). Même la question de savoir si une faillite de Crypto International AG pourrait compromettre la disponibilité d'une cryptographie sûre pour l'armée (cf. ch. 5.2) n'était manifestement pas un sujet devant être traité par la Délséc aux yeux du DDPS, qui assure la présidence permanente de la délégation. Il convient toutefois de relever que, depuis la réforme[31] des instruments de conduite de la politique de sécurité, en octobre 2011, le CdA et l'armée ne font plus partie du cercle fixe des participants de la Délséc. En revanche, la directrice de l'Office fédéral de la police (fedpol) et le directeur du SRC y prennent toujours part, de même que, en principe, les secrétaires généraux des trois départements concernés.

7 Prise en main par la DélCdG

7.1 Autorisation au sens de l'art. 154*a* LParl

Le 13 février 2020, la DélCdG a décidé, dans le cadre d'une séance extraordinaire, d'ouvrir une procédure d'inspection. Le Conseil fédéral en a été informé par lettre le 14 février 2020.

L'art. 154*a*, al. 1, de la loi sur l'Assemblée fédérale (LParl)[32] dispose qu'une enquête disciplinaire ou administrative de la Confédération ne peut être engagée ou poursuivie qu'avec l'autorisation de la DélCdG, si elle concerne des affaires ou des personnes qui sont visées par une enquête de cette même délégation.

Dans sa lettre du 14 février 2020, la DélCdG informait le Conseil fédéral qu'elle lui donnait l'autorisation, au sens de l'art. 154*a* LParl, de poursuivre l'enquête Oberholzer. Par la même occasion, elle lui demandait de faire en sorte que M. Oberholzer ait accès sans restriction à toutes les pièces des archives et elle lui annonçait vouloir coordonner étroitement sa propre enquête avec la sienne. En outre, elle indiquait au Conseil fédéral qu'elle faisait valoir sa priorité s'agissant de l'audition de personnes travaillant ou ayant travaillé pour la Confédération.

31 Directives du Conseil Fédéral du 24.8.2011 sur l'organisation de la conduite de la politique de sécurité du Conseil fédéral (FF **2011** 6305).
32 Loi du 13.12.2002 sur l'Assemblée fédérale (loi sur le Parlement, LParl; RS **171.10**).

La demande de la DélCdG visant à ce que Niklaus Oberholzer ait intégralement accès aux archives était motivée par les restrictions découlant de la décision du Conseil fédéral du 15 janvier 2020. Selon la proposition du DDPS du 13 janvier 2020, le comité de recherche devait disposer des mêmes droits de consultation des données personnelles que toute autre personne en faisant la demande, au sens de l'art. 11 LAr. Ainsi, chaque demande de consultation de données personnelles devait être examinée par l'organe fédéral compétent. Cela signifiait en somme que la consultation de certains documents aurait pu être refusée à M. Oberholzer en présence d'intérêts de protection prépondérants. Or, cet état de fait était en contradiction avec l'objectif avoué d'éclaircir absolument tous les aspects historiques de l'affaire Crypto AG.

La DélCdG a, à l'époque estimé que le comité de recherche devait disposer des mêmes droits de consultation que les services qui ont versé des documents, au sens de l'art. 14 LAr. Or, Niklaus Oberholzer était mandaté par le Conseil fédéral, auquel les offices compétents étaient subordonnés et la consultation de données personnelles archivées n'était permise, selon l'art. 14 LAr, que dans certains cas bien définis, par exemple lorsqu'elles sont utilisées comme moyens de preuve. Ce but étant établi dans l'enquête Oberholzer, la DélCdG ne voyait aucun motif légal pour que les services qui avaient versé des documents aux AFS puissent restreindre l'accès à ces derniers. Lors de l'entretien qu'elle a eu avec la DélCdG le 25 février 2020, la cheffe du DDPS (*Viola Amherd*) a pourtant considéré qu'il était nécessaire, légalement, que la procédure de consultation visée à l'art. 11 LAr soit également appliquée à M. Oberholzer.

7.2 Transmission des documents

7.2.1 Rétention de documents au détriment de la DélCdG

Dans un courriel du 12 février 2020, le SG-DDPS a été prié de remettre, rapidement et sans restriction, à la DélCdG tous les documents nécessaires. La DélCdG avait adressé cette demande au titre de ses droits étendus à l'information, étant entendu que les délégations des commissions de surveillance ont accès à toutes les informations dont elles ont besoin pour exercer leurs attributions (art. 154, al. 1, LParl). De plus, ces délégations ont le droit de demander que leur soient remis les procès-verbaux des séances du Conseil fédéral et les documents qui sont classés secrets (art. 154, al. 2, LParl).

Lors des rencontres qui ont eu lieu avant l'ouverture de l'inspection de la DélCdG entre la délégation ou son président et la cheffe du DDPS (*Viola Amherd*) ou le directeur du SRC (*Jean-Philippe Gaudin*), il n'a jamais été question de l'existence d'autres documents que le rapport MINERVA. On a ainsi laissé croire à la DélCdG qu'il n'y avait presque aucune documentation sur l'affaire Crypto AG, alors qu'il a été prouvé par la suite que ce n'était pas le cas. Au moment de la première discussion à ce propos entre la DélCdG, la cheffe du DDPS et le directeur du SRC, le 25 novembre 2019, le bilan réalisé par le SRC à l'automne 2019 était déjà disponible. Quant à la découverte des dossiers dans l'installation K, elle n'a pas non plus été signalée à la DélCdG.

Étant donné que la DélCdG avait prié la cheffe du DDPS, à la séance du 25 novembre 2019, de lui communiquer les résultats des investigations menées sur l'affaire, la délégation est pour le moins déconcertée par le fait qu'on ne l'a pas informée de l'existence des différents documents précités.

À la demande expresse du président de la DélCdG, cette dernière a reçu une copie du rapport MINERVA le 10 février 2020, suivie, le 13 février 2020, d'une copie de la note d'information secrète rédigée par le DDPS à l'intention du Conseil fédéral au début du mois de novembre 2019 (cf. ch. 4.1.3). S'agissant du bilan réalisé par le SRC à l'automne 2019, il a été transmis à la DélCdG le 17 février 2020 seulement. La cheffe du DDPS n'a été mise au courant de l'existence de ce bilan que le jour d'après.

Par ailleurs, il convient de faire remarquer que les droits à l'information de la DélCdG portent aussi sur les notes et les documents qui sont rédigés à l'intention d'un chef de département, d'un directeur ou d'un chef d'office pour un usage interne uniquement.

7.2.2 Octroi de l'autorisation de consulter les documents

Dans une lettre datée du 14 février 2020, la DélCdG a demandé au Conseil fédéral de donner à M. Oberholzer un accès intégral aux archives. Cette demande était motivée, d'une part, par le souhait de la délégation de donner à M. Oberholzer la possibilité d'examiner l'affaire de manière complète et en ayant connaissance de tous les documents et, d'autre part, par l'interprétation, erronée selon la DélCdG, que fait le DDPS de la LAr dans ce contexte (cf. ch. 7.2.1).

Le 17 février 2020, la DélCdG a pour la première fois eu connaissance du bilan réalisé par le SRC à l'automne 2019. L'après-midi du 18 février et en début de matinée du 19 février 2020, les membres de la délégation ont analysé le bilan et ont constaté l'importance du contenu de ce document.

Le président de la délégation a alors immédiatement demandé à la cheffe du DDPS que le bilan ne soit mis à la disposition ni de M. Oberholzer ni du procureur général de la Confédération (*Michael Lauber*) et qu'aucune action irréversible ne soit entreprise en matière de transmission de documents. Le DDPS n'a toutefois pas suivi cette consigne et a laissé M. Oberholzer consulter ce document dans les locaux du SRC le même jour, visiblement sur ordre de la cheffe du département. Le procureur général de la Confédération a lui aussi pu parcourir différentes parties du document le 20 février 2020. D'après les déclarations du DDPS, ni M. Oberholzer ni le procureur général n'en ont toutefois reçu une copie.

7.2.3 Appréciation de la portée des faits

Après la parution d'articles dans les médias, à la mi-février 2020, les personnes responsables au sein du SRC et du DDPS ont continué de partir du principe que l'affaire Crypto AG concernait des faits remontant loin dans le passé et n'ayant aucun lien direct avec le présent. Il s'agissait selon eux simplement de faire un travail de recherche historique afin de faire autant que possible la transparence sur l'affaire. Cette

vision des évènements ressort de divers documents ainsi que des déclarations des différents acteurs.

Le 18 février 2020, le SG-DDPS a eu connaissance du bilan établi par le SRC à l'automne 2019. Le jour suivant, il a permis à M. Oberholzer de consulter les documents concernés, et le surlendemain, le procureur général de la Confédération a également pu en consulter certaines parties. Sur la base de ces informations, le MPC était censé confirmer au DDPS si les activités de Crypto AG étaient constitutives du délit d'espionnage, ce qu'il n'a pas pu faire. Cela montre que le SG-DDPS n'était pas en mesure d'apprécier par lui-même les résultats du bilan du SRC. Il n'a en particulier pas compris le rôle du service de renseignement suisse dans l'affaire Crypto AG ni saisi la portée juridique de la collaboration avec les services américains (cf. ch. 4.2.2 et 5.1).

Les modalités et la durée de la collaboration entre les services de renseignement suisses et américains ressortaient en effet clairement du bilan de la situation, et cette collaboration impliquait en somme aussi une coresponsabilité des autorités suisses dans les activités de Crypto AG. Alors que cette opération des services de renseignement pouvait en principe s'appuyer sur le droit en vigueur, le fait qu'elle se déroulait sans l'approbation des responsables politiques commandait d'informer en urgence le Conseil fédéral. La portée politique de cette opération concernait potentiellement la politique extérieure et la politique économique, mais elle touchait aussi la sécurité personnelle de collaborateurs de l'entreprise sans qu'ils en aient conscience. Face à de tels défis, le Gouvernement suisse est resté paralysé aussi longtemps qu'il n'a pas eu une connaissance exacte des activités de son propre service de renseignement.

À la lumière des demandes d'information reçues de la part de la DélCdG après l'ouverture de son inspection, le DDPS a réalisé, le 18 février 2020, à quel point le SRC n'avait pas suffisamment informé les responsables politiques. Le département a notamment commencé à se rendre compte que l'affaire Crypto AG ne pouvait plus être considérée comme un fait purement historique, mais il n'a pas compris que l'appréciation de la situation actuelle ne pouvait pas être dissociée de la perspective historique. Ainsi, le DDPS a décidé, le 18 février 2020 déjà, de demander à l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) de mener une inspection visant à déterminer si la pratique actuelle en matière de renseignement dans les domaines des interceptions de communications et de décryptage était légale, inspection qui serait menée en parallèle à l'enquête Oberholzer. Ce faisant, le DDPS n'a toutefois pas pris en compte le fait que la légalité de ces activités ne pouvait pas être analysée sans procéder à un examen approfondi des documents découverts dans l'installation K (cf. ch. 4.2.2).

Quant à la DélCdG, les documents dont elle a pris connaissance l'ont poussée à réévaluer l'affaire Crypto AG dans son ensemble. Au vu des nouvelles informations dont elle disposait, la délégation a estimé qu'il était indispensable de démêler les liens étroits et problématiques qui existaient entre les deux enquêtes menées par l'exécutif et sa propre inspection, et qui pourraient en fin de compte perturber son travail. C'est pourquoi elle a jugé opportun que les informations qui venaient d'être révélées ne soient, dans un premier temps, pas transmises à d'autres services (en l'occurrence aux responsables de l'enquête Oberholzer et de celle du MPC) tant que la suite des opérations ne serait pas clairement définie. La DélCdG a également estimé que les autorités de poursuite pénale n'auraient pas dû être impliquées tant que le DDPS n'avait pas

saisi la portée des nouvelles informations. C'est la raison pour laquelle elle a prié le DDPS de renoncer à entreprendre des actions irréversibles en matière de transmission de documents jusqu'à ce qu'elle ait pu s'entretenir avec la cheffe du département.

7.3 Retrait de l'autorisation au sens de l'art. 154*a* LParl

Lorsque, le 18 février 2020, la DélCdG a pris connaissance du bilan de la situation établi par le SRC, elle a soudainement réalisé que le traitement de cette affaire ne se limitait aucunement à un travail de mémoire et que certains éléments avaient non seulement des répercussions dans le présent, mais aussi un caractère potentiellement explosif et une portée majeure.

Dans une lettre datée du 21 février 2020, la délégation a informé le Conseil fédéral qu'elle révoquait l'autorisation donnée pour l'enquête menée par M. Oberholzer sur mandat du gouvernement[33]. Il s'est avéré que la concomitance de plusieurs enquêtes nuirait à l'établissement rapide et sans accroc des faits. D'une part, il était devenu clair pour la délégation que ni le SRC ni le DDPS n'avaient alors reconnu l'ampleur et la portée des faits, si bien que la DélCdG s'est unanimement vue dans l'obligation de reprendre la conduite des investigations et de révoquer l'autorisation du 14 février 2020. D'autre part, la cheffe du DDPS (*Viola Amherd*) avait proposé à l'AS-Rens, dans une lettre datée du 18 février 2020, de se pencher sur la légalité des activités cryptanalytiques menées par le DDPS pour le compte du SRC. Étant donné que cet aspect faisait l'objet d'une enquête de la DélCdG, la cheffe du DDPS aurait, conformément à l'art. 154*a*, al. 1, LParl, dû demander une autorisation à la délégation, ce qu'elle n'a pas fait. Afin de pouvoir examiner les faits rapidement et efficacement, la délégation a donc décidé de révoquer l'autorisation permettant à l'exécutif de poursuivre son enquête. Dans le même temps, elle a indiqué au Conseil fédéral qu'elle s'opposait à l'enquête de l'AS-Rens demandée par le DDPS.

L'art. 154*a*, al. 2, LParl prévoit que la DélCdG statue sur l'autorisation après audition du Conseil fédéral. Le Conseil fédéral a ainsi fait valoir qu'il n'avait pas été auditionné avant la révocation de l'autorisation, ce qui était en contradiction avec la disposition susmentionnée. Or, lorsque, le 19 février 2020, le président de la DélCdG avait communiqué à la cheffe du DDPS qu'il ne fallait pas permettre à M. Oberholzer ni au procureur général de la Confédération de consulter le bilan de la situation du SRC, il avait proposé à la cheffe du DDPS de l'auditionner avant la séance du Conseil fédéral. Celle-ci avait rejeté cette proposition, suggérant que la rencontre pourrait plutôt avoir lieu le 25 février 2020. La DélCdG considère qu'avec cette proposition faite à la cheffe du DDPS de l'auditionner, les conditions de l'art. 154*a*, al. 2, LParl ont été remplies. La délégation ne pouvait pas attendre que la séance du 25 février 2020 soit passée pour révoquer l'autorisation, car il fallait agir en urgence pour couper court à la diffusion des informations sensibles.

33 Crypto AG: la Délégation des Commissions de gestion reprend la conduite de l'enquête, communiqué de presse de la DélCdG du 26.2.2020.

L'obligation d'auditionner le Conseil fédéral a été introduite à l'art. 154*a* LParl parce qu'il y a des cas où le gouvernement doit pouvoir avoir le droit de mener ou de poursuivre des enquêtes disciplinaires ou administratives[34]. Il n'existe visiblement pas de tel motif en l'occurrence. À l'époque, le Conseil fédéral avait proposé d'inscrire directement dans la loi des exceptions plus étendues. Ainsi, il souhaitait que l'autorisation soit en règle générale délivrée en présence de raisons pertinentes, parmi lesquelles il citait notamment la nécessité de se faire le plus rapidement possible une opinion sur l'affaire considérée et de remédier sans attendre aux insuffisances supposées[35]. L'Assemblée fédérale avait alors renoncé à ce que les raisons soient explicitement inscrites dans la loi, étant parvenue à la conclusion qu'une audition pouvait tout à fait être justifiée. La DélCdG relève en outre que, dans sa réponse du 5 mars 2020 portant sur la révocation de l'autorisation, le Conseil fédéral n'a avancé aucune raison justifiant le maintien de l'autorisation. Au vu de la portée de l'affaire, que le Conseil fédéral n'avait alors pas encore saisie, et de l'urgence qui régnait, l'autorisation devait être révoquée sans attendre.

7.4 Désignation d'un chargé d'enquête par la DélCdG

Dans sa lettre du 21 février 2020 au Conseil fédéral, par laquelle elle lui signifiait qu'elle révoquait l'autorisation, la DélCdG a également informé le gouvernement qu'elle souhaitait que M. Oberholzer poursuive son enquête, mais sur mandat de la délégation. L'objectif était de veiller à ce que les travaux puissent continuer sans interruption.

La DélCdG a ainsi fait usage de son droit de faire appel à un chargé d'enquête conformément à l'art. 166, al. 2, en relation avec l'art. 155, al. 6, LParl. Elle a en effet la possibilité de confier à un chargé d'enquête le soin d'administrer les preuves. Conformément au renvoi figurant à l'art. 155, al. 6, LParl, le droit de faire appel à un chargé d'enquête revient non seulement aux CEP, mais aussi à la DélCdG. En effet, l'alinéa en question prévoit explicitement que, pour les délégations des commissions de surveillance, la procédure et les droits des personnes concernées sont régis par les art. 166 à 171 LParl. Par conséquent, les CEP et la DélCdG disposent des mêmes droits et compétences.

7.5 Activité de l'AS-Rens et responsabilité du DDPS en matière de surveillance

Le 12 novembre 2019, la cheffe du DDPS (*Viola Amherd*) a informé successivement le président de la DélCdG (cf. ch 4.1.4), pour la première fois, et le chef de l'AS-Rens au sujet de l'affaire Crypto AG. À ce moment-là, la cheffe du DDPS et les services

34 Cf. le débat qui s'est tenu au Conseil des États: BO **2004** E 409.
35 Procédures de la Délégation des Commissions de gestion et enquêtes disciplinaires ou administratives de la Confédération menées parallèlement et sur un même objet, avis du Conseil fédéral du 31.3.2004 sur le rapport de la Commission de gestion du Conseil des Etats du 21.11.2003 (FF **2004** 1355 1359).

directement concernés du département avaient aussi reçu la planification des inspections 2020 de l'AS-Rens pour prise de position. Ni le DDPS, ni l'AS-Rens n'ont alors considéré comme nécessaire d'intégrer certains aspects de l'affaire Crypto AG au nouveau programme des inspections de l'autorité de surveillance.

Trois mois plus tard, la DélCdG a décidé d'ouvrir son inspection, à la suite de quoi le chef de l'AS-Rens a informé la délégation du fait qu'il était disposé à soutenir les travaux de cette dernière dans la mesure de ses possibilités. En outre, l'AS-Rens a indiqué qu'elle allait prendre en considération les éventuelles révélations des médias dans deux de ses inspections en cours, mais qu'elle ne prévoyait pas de mener elle-même d'investigations au sujet de l'affaire Crypto AG.

La DélCdG a salué les efforts de l'AS-Rens en matière de coordination et l'a remerciée du soutien offert dans une lettre datée du 24 février 2020. Par la suite, l'AS-Rens a entrepris, avec l'accord de la délégation, d'examiner l'installation K ainsi que d'autres locaux du SRC où sont entreposés des documents, et ce, dans le cadre d'un contrôle inopiné. Son rapport d'inspection, qui a été finalisé en juillet 2020, a confirmé l'impression de la DélCdG selon laquelle il n'existait aucun inventaire fiable de ces documents.

Dans son rapport d'inspection, l'AS-Rens a renoncé à émettre des recommandations, ce que la DélCdG a jugé opportun au vu de sa propre inspection en cours, car cela permettait dès le départ d'éviter toute contradiction avec les futures recommandations de la haute surveillance parlementaire.

Par contre, la délégation a jugé problématique la proposition du DDPS du 18 février 2020, visant à ce que l'AS-Rens examine immédiatement la légalité des activités cryptanalytiques menées par le DDPS pour le compte du SRC. La cheffe du DDPS n'a émis cette proposition qu'après la médiatisation de l'affaire Crypto AG et l'ouverture de l'inspection de la DélCdG, et alors que les besoins en matière de coordination entre la délégation et l'AS-Rens avaient déjà été clarifiés. Le DDPS n'avait donc pas utilisé tout le temps qu'il avait eu à disposition depuis novembre 2019 pour assumer de manière autonome ou avec le soutien de l'AS-Rens son rôle de surveillance concernant l'exploitation de capacités cryptanalytiques par le SRC. C'est pourtant le DDPS et non l'AS-Rens qui porte la responsabilité de la légalité des activités de renseignement.

Lors d'une affaire liée au renseignement d'une telle portée politique, la DélCdG estime que la direction du DDPS est tenue de se procurer de manière autonome les informations nécessaires à ce qu'elle puisse assumer son rôle politique de conduite des affaires. La direction doit pouvoir réaliser cette tâche elle-même et ne peut pas la déléguer à un organe de contrôle indépendant, non soumis à des directives, tel que l'AS-Rens.

7.6 Informations intermédiaires fournies à la présidente de la Confédération

Dans une lettre datée du 10 mars 2020, la DélCdG a proposé à la présidente de la Confédération (*Simonetta Sommaruga*) de se réunir pour un entretien. Cette proposition était fondée sur deux raisons: d'une part, la délégation voulait lui présenter une nouvelle fois de manière détaillée les raisons de la révocation de l'autorisation afin d'éviter que ses relations avec le Conseil fédéral ne pâtissent de cette mesure et, d'autre part, elle doutait du fait que le Conseil fédéral eût alors saisi la portée et le caractère explosif de cette affaire. La présidente de la Confédération ayant répondu positivement à la proposition, la délégation s'est entretenue avec elle ainsi qu'avec la cheffe du DDPS (*Viola Amherd*) le 25 mai 2020. C'est dans ce cadre que la présidente de la Confédération a été informée des principaux résultats des recherches de la DélCdG. La délégation lui a également présenté, à l'intention du Conseil fédéral, les défis qui allaient selon elle se poser. L'un de ces défis résidait dans le traitement de la demande d'autorisation déposée par le MPC auprès du DFJP, concernant la plainte pénale du Secrétariat d'Etat à l'économie (SECO) (cf. chap. 8).

8 Suspension des licences d'exportation par le DEFR et le Conseil fédéral et plainte pénale du SECO

8.1 Rappel des faits

Le 3 décembre 2019, le SECO a délivré à la société TCG Legacy AG, l'une des entreprises ayant succédé à Crypto AG, une licence générale d'exportation.

Le 16 décembre 2019, la secrétaire générale du DEFR et le collaborateur personnel du chef du DEFR se sont entretenus de l'affaire Crypto AG avec le chef de la division NDBU. Il est ressorti de cette discussion que la Suisse n'aurait pas avantage à ce que soit divulguée l'information selon laquelle l'entreprise avait obtenu une licence d'exportation juste avant que l'affaire n'éclate dans les médias. Selon le chef de la division NDBU, l'unique objectif poursuivi alors était de gagner du temps. Le 19 décembre 2019 au soir, le chef du DEFR (*Guy Parmelin*) a informé la cheffe du DDPS (*Viola Amherd*), en présence des deux secrétaires généraux, de l'intention de suspendre la licence générale d'exportation.

Le 20 décembre 2019, à la suite d'une injonction de la direction du DEFR, le SECO a suspendu jusqu'à nouvel ordre la licence générale d'exportation ainsi que les licences délivrées à Crypto International AG, une autre entreprise ayant succédé à Crypto AG. La note de la séance du GTID du 10 février 2020 indiquait que le SECO continuerait néanmoins de traiter les demandes individuelles d'exportation.

Le 25 février 2020, le SECO a déposé une plainte pénale contre inconnu auprès du MPC, fondée sur l'art. 18 de la loi sur le contrôle des biens (LCB)[36] et de l'art. 10 de

[36] Loi fédérale du 13.12.1996 sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (loi sur le contrôle des biens, LCB; RS **946.202**).

l'ordonnance sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (OSIC)[37]. La plainte en question avait été préalablement approuvée par la secrétaire d'État du SECO et son dépôt était soutenu par le SG-DEFR.

Le 2 mars 2020, le président et la secrétaire de la DélCdG ont été informés par le procureur général de la Confédération du dépôt de la plainte pénale. Le groupe chargé du contrôle des exportations s'est réuni deux jours plus tard, soit le 4 mars 2020. Les personnes en présence sont parvenues à la conclusion que les demandes individuelles d'exportation devaient être soumises à la décision du Conseil fédéral. Outre le SECO, sont représentés au sein de ce groupe de contrôle (art. 27, al. 3, OCB) le DFAE, le DDPS et le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), pour ce qui est des départements. Le SRC est entendu au sujet des demandes.

Le 6 mars 2020, la Police judiciaire fédérale (PJF) a saisi près de 400 appareils des sociétés Crypto International AG et TCG Legacy AG, tout en en laissant la majeure partie dans les entrepôts de Crypto International AG. Le procès-verbal de la perquisition a été adressé à la société le 9 mai 2020.

À la demande du SECO, le délégué fédéral à la cybersécurité a organisé, le 10 mars 2020, un échange de vues consacré aux possibilités de manipulation et aux éléments prouvant celles-ci.

Le 13 mars 2020, le MPC a adressé au DFJP une demande d'autorisation au sens de l'art. 66 de la loi sur l'organisation des autorités pénales (LOAP)[38].

Jusqu'au 18 mai 2020, Crypto International AG et TCG Legacy AG ont déposé en tout quinze demandes individuelles visant à exporter des appareils et des modules de cryptage. Aussi bien les représentants du DDPS que ceux du DETEC au sein du groupe de contrôle des exportations se sont déclarés favorables, en mai 2020, à l'autorisation de l'ensemble des demandes individuelles d'exportation. Les représentants du DFAE, par contre, souhaitaient approuver uniquement les demandes de TCG Legacy AG et soumettre à la décision du Conseil fédéral les demandes de Crypto International AG.

Le 25 mai 2020, la DélCdG s'est entretenue, le matin, avec la présidente de la Confédération et la cheffe du DDPS et, l'après-midi, avec la cheffe du DFJP (*Karin Keller-Sutter*). La délégation a été informée du traitement de la demande d'autorisation du MPC au sein du DFJP.

En vue de la séance du Conseil fédéral du 12 juin 2020, le DEFR a formulé une proposition visant à autoriser les quinze demandes individuelles d'exportation soumises par Crypto International AG et TCG Legacy AG. Dans le cadre de la procédure de corapport, proposition a été faite de reporter l'examen de l'objet. La question de l'opportunité d'attendre la conclusion des investigations de la DélCdG et du MPC avant de prendre une décision a également été soulevée.

37 Ordonnance du 13.5.2015 sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (OSIC; RS **946.202.3**).

38 Loi fédérale du 19.3.2010 sur l'organisation des autorités pénales de la Confédération (loi sur l'organisation des autorités pénales, LOAP, RS **173.71**).

Le 19 juin 2020, le Conseil fédéral a décidé, en se fondant sur une proposition modifiée du DEFR, de suspendre sa décision concernant les quinze demandes individuelles d'exportation émanant des sociétés ayant succédé à Crypto AG, en attendant la fin des investigations du MPC. Il a simultanément autorisé l'ouverture d'une poursuite pénale contre inconnu.

Le 3 juillet 2020, le SECO a décidé que l'examen des demandes individuelles d'exportation émanant de TCG Legacy AG serait suspendu jusqu'à la fin des investigations du MPC. Lors de sa séance du 26 août 2020, le Conseil fédéral a rejeté une demande de réexamen des demandes d'octroi de licences individuelles d'exportation formulée par Crypto International AG.

8.2 Bases légales

En l'espèce, plusieurs questions se posent en ce qui concerne le droit relatif au contrôle des biens. Le cadre légal applicable aux mesures prises par la Confédération à l'égard des sociétés ayant succédé à Crypto AG est précisément la législation relative au contrôle des biens. Selon l'art. 2, al. 2, LCB, le Conseil fédéral détermine les biens qui relèvent de la LCB. Le gouvernement a précisé quels étaient les biens concernés en édictant l'Ordonnance sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (OCB)[39], notamment.

La liste des biens dont l'exportation est soumise à autorisation figure dans les différentes annexes de l'OCB. L'annexe 2, partie 2, mentionne les systèmes et procédures de cryptage[40] ainsi que les systèmes, équipements et composants destinés à mettre en échec, à affaiblir ou à contourner la sécurité de l'information, qui ont été conçus ou modifiés pour effectuer des fonctions cryptanalytiques[41].

Par ailleurs, pour éviter que des systèmes de surveillance exportés par la Suisse ne soient utilisés par leurs destinataires étrangers à des fins d'oppression politique, le Conseil fédéral a soumis les exportations de ce type à une procédure contraignante d'autorisation individuelle. C'est la raison pour laquelle il a édicté, en 2015, une ordonnance en ce sens, à savoir l'OSIC. Selon l'annexe de l'ordonnance, sont également concernés par cette dernière les appareils à fonctions cryptanalytiques.

39 Ordonnance du 3.6.2016 sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (ordonnance sur le contrôle des biens, OCB; RS **946.202.1**).
40 Annexe 2, partie 2, OCB, numéro de contrôle à l'exportation (NCE) 5A002.
41 Annexe 2, partie 2, OCB, NCE 5A004.

8.3 Suspension des licences générales d'exportation par le DEFR

8.3.1 Légalité de la suspension

Deux types de licence sont prévus dans le cadre de la LCB: la licence individuelle et la licence générale d'exportation. Selon les art. 12 et 13 de l'OCB, le SECO peut délivrer une licence générale ordinaire ou une licence générale extraordinaire d'exportation si les différentes conditions fixées dans la LCB et l'OCB sont remplies.

En tout, le SECO a délivré cinq licences générales d'exportation – aussi bien des licences ordinaires que des licences extraordinaires – aux sociétés ayant succédé à Crypto AG. Il a notamment octroyé, le 4 décembre 2019, une licence générale ordinaire d'exportation pour l'Allemagne. Le 16 décembre 2019, le SECO a eu, pour la première fois, connaissance de l'affaire Crypto AG. Les premiers éléments attestant d'efforts visant à suspendre les licences générales d'exportation des trois entreprises datent du 16 décembre 2019, jour où le chef de la division NDBU a informé le SG-DEFR de la situation. Le 20 décembre 2019, les licences générales d'exportation ont été suspendues par le SECO. La décision en question a été prise par le chef du DEFR (*Guy Parmelin*), dont le collaborateur personnel a donné les instructions nécessaires aux personnes du SECO chargées de mettre en œuvre la décision. Dans le cadre de ces instructions, il a été précisé explicitement que la décision ne devait pas être motivée plus avant auprès des entreprises concernées et qu'il fallait revenir à la pratique des autorisations individuelles d'exportation. Le SECO a appliqué cette décision, la communication se faisant au moyen de la plate-forme électronique ELIC[42]. Pour quatre des cinq licences générales d'exportation, il est indiqué explicitement que les licences du SECO ont été retirées et qu'elles sont suspendues jusqu'à nouvel ordre. S'agissant de la demande de TCG Legacy AG, il manque la notion de retrait. Conformément aux instructions du SG-DEFR, la décision n'est motivée pour aucune des demandes. À la société TCG Legacy AG, qui s'enquerrait du motif de la suspension de la licence, le SECO a répondu que la licence générale ordinaire d'exportation était soumise à une nouvelle évaluation. Crypto International AG et TCG Legacy AG partaient du principe qu'une décision et les motifs de la décision leur seraient notifiés par courrier postal, ce qui n'a toutefois pas été le cas.

Le droit en vigueur, qu'il s'agisse de la LCB ou de l'OCB, ne prévoit pas la possibilité de suspendre une licence. Le SECO avait attiré l'attention du SG-DEFR sur ce point, mais la suspension a malgré tout été maintenue. Dans ce contexte, la suspension doit être traitée comme un retrait au sens de l'art. 7 LCB, qui dispose que le permis est retiré si, depuis son octroi, les circonstances ont changé de sorte que les conditions du refus, mentionnées à l'art. 6, sont remplies (art. 7, al. 1, LCB). Le permis peut également être retiré si les conditions et les charges dont il est assorti ne sont pas observées (art. 7, al. 2, LCB).

42 E-licensing, système d'autorisation électronique.

8.3.2 Appréciation de la DélCdG

D'après les explications du SECO, les licences générales d'exportation ont été retirées sur la base de l'art. 7, al. 2, LCB en relation avec l'art. 5, al. 2, OCB. La DélCdG considère que ces bases légales ne sont en réalité qu'un prétexte, qui, pour plusieurs raisons, ne résiste pas à une analyse factuelle et juridique:

- Premièrement, la DélCdG dispose de documents dont il ressort qu'il n'existait aucun motif reposant sur l'art. 7 LCB et que l'on a plutôt tenté fébrilement de retarder la procédure en recourant à des manœuvres bureaucratiques, afin de gagner du temps et de fabriquer de toutes pièces une raison expliquant le retrait des licences. Ces efforts ont débouché sur l'établissement d'un lien entre l'art. 7, al. 2, LCB et l'art. 5, al. 2, OCB.
- Deuxièmement, le fait de s'appuyer sur l'art. 5, al. 2, OCB n'est pas convainquant, étant donné qu'au moins une licence générale d'exportation a encore été délivrée le 3 décembre 2019. L'entreprise concernée satisfaisait aux conditions requises 17 jours seulement avant le retrait de la licence: ce fait corrobore lui aussi la conclusion de la DélCdG selon laquelle on est bien en présence d'une raison fallacieuse, construite a posteriori. Si tel n'était pas le cas, la licence n'aurait pas pu être délivrée le 3 décembre 2019.
- Troisièmement, en ce qui concerne les demandes individuelles d'exportation que le Conseil fédéral n'a pas approuvées et pour lesquelles il a reporté sa décision le 19 juin 2020, le DEFR est arrivé à la conclusion qu'une licence devait en réalité être délivrée. Si la condition fixée à l'art. 5, al. 2, OCB n'avait véritablement pas été remplie, le SECO aurait dû se prononcer lui aussi en faveur du rejet des demandes. Or, il ne l'a pas fait.

Le SECO voulait en outre éviter de devoir rendre une décision susceptible de recours. Il fait par ailleurs valoir que les entreprises concernées auraient pu exiger une telle décision, mais qu'elles ont omis de le faire. Même si, du point de vue juridique, on ne peut faire aucun reproche au SECO à cet égard, ces affirmations viennent corroborer le tableau brossé jusqu'ici: tant Crypto International AG que TCG Legacy AG ont affirmé qu'elles partaient du principe que la décision ou les motifs du retrait de la licence leur seraient signifiés par courrier postal. La DélCdG relève à cet égard que le principe de la bonne foi, tel qu'il est garanti par la Constitution[43] (art. 9 Cst.), a été mis à rude épreuve.

De plus, la DélCdG s'étonne de ce que le chef du DEFR, selon ses propres dires, n'ait donné le mandat de clarifier la situation juridique qu'après le 20 décembre 2019, soit après le retrait des licences générales d'exportation. La question du retrait des licences n'a pas non plus été soumise au groupe chargé du contrôle des exportations.

La DélCdG constate que le retrait des licences générales d'exportation, opéré par le SECO le 20 décembre 2019 sur ordre du chef du DEFR, ne reposait sur aucune base légale et n'était donc pas licite. Il constitue une violation du principe de la légalité visé à l'art. 5 Cst. et de l'interdiction de l'arbitraire visée à l'art. 9 Cst.

43 Constitution fédérale de la Confédération suisse du 18.4.1999 (Cst.; RS **101**).

La DélCdG estime cependant qu'il ne faut adresser aucun reproche aux personnes responsables au sein du SECO, car celles-ci se sont retrouvées dans la situation délicate de devoir exécuter et motiver la décision du chef du DEFR. La responsabilité de la procédure doit être attribuée uniquement au chef du DEFR et au SG-DEFR.

8.4 Plainte pénale du SECO

Le 25 février 2020, le SECO a déposé une plainte pénale contre inconnu auprès du MPC. Dans sa plainte, le SECO indique que les appareils de cryptage exportés – et par conséquent soumis au contrôle suisse à l'exportation – jusqu'en 2018 pourraient avoir été manipulés et que le droit relatif au contrôle à l'exportation pourrait ainsi avoir été violé. Il signale en particulier une possible infraction à l'art. 14, al. 1, let. c, LCB et à l'art. 9, al. 1, let. a, OSIC.

8.4.1 Décisions prises au sein du DEFR

À la suite de la suspension par le DEFR des licences générales d'exportation, le SECO soupçonnait les activités de Crypto AG d'être punissables. De premiers éléments de preuve étayant cette appréciation ont été produits le 12 février 2020. À ce moment-là, le chef du secteur Contrôle à l'exportation/Produits industriels (BWIP) a indiqué que la possible violation du droit relatif au contrôle à l'exportation devait immédiatement être portée à la connaissance du MPC. L'interprétation juridique nécessaire à cet égard a été effectuée par le chef du BWIP lui-même. La prise de contact avec le MPC a été saluée tant par les supérieurs directs au sein du SECO que par le SG-DEFR. Le jour même, un entretien avec le MPC a été sollicité.

Parallèlement, le SG-DEFR a prié le chef du BWIP de déterminer au plus vite si le SECO devait déposer une plainte pénale. Le 17 février 2020, ce dernier a informé le SG-DEFR que, selon lui du moins, il y avait en l'occurrence une violation présumée de la LCB (art. 14, al. 1, let. c).

Le 21 février 2020, une rencontre a eu lieu entre les représentants du SECO et ceux du MPC. Une note du SECO indique que, sur la base des informations disponibles à l'époque, le MPC n'avait identifié aucune violation du droit relatif au contrôle à l'exportation. Le MPC soupçonnait que les appareils de cryptage en cause présentaient un cryptage «vulnérable» sans fonction cryptanalytique. Dans ce cas, les requérants n'auraient pas fourni d'indications erronées ou incorrectes. Dans l'ensemble, le MPC estimait qu'une plainte formelle du SECO ne s'imposait pas. Une plainte donnait toutefois l'occasion au MPC de prendre des mesures de précaution pour saisir les appareils de cryptage proposés à l'exportation. Lors de son audition par la DélCdG, le procureur général de la Confédération (*Michael Lauber*) a confirmé que le MPC avait déconseillé au SECO de déposer une plainte. Il était d'avis que le dépôt d'une plainte avait pour but de faire passer «la patate chaude» du DEFR au MPC. L'opportunité de déposer une plainte pénale dépendait également, selon le MPC, du résultat du traitement politique de l'affaire Crypto AG, en particulier par la DélCdG.

À la suite de sa rencontre avec le MPC, le SECO s'est entretenu avec le SG-DEFR. Il ressort de cet échange que la décision de déposer une plainte pénale a été prise par le SECO, et non par le SG-DEFR, bien que celui-ci ait aussi souhaité le dépôt d'une plainte. Le projet de plainte a été soumis à la secrétaire d'État, qui a soutenu la plainte mais n'a pas souhaité la cosigner. Le chef du DEFR (*Guy Parmelin*) a plus tard fait valoir devant la DélCdG que la situation juridique était claire et que le SECO n'avait eu d'autre choix que de déposer une plainte. Selon lui, que le SECO agisse ou non, on risquait dans tous les cas de reprocher son comportement au secrétariat. Le 25 février 2020, la plainte a été officiellement déposée.

8.4.2 Évaluation de la plainte par la DélCdG

Conformément à ce qu'il indique dans sa plainte, le SECO soupçonnait Crypto AG d'avoir exporté, jusqu'en 2018, des appareils manipulés, c'est-à-dire pour lesquels des procédures de cryptage «vulnérables» étaient utilisées. Ces soupçons se fondaient, selon le SECO, sur des révélations faites à l'époque dans les médias concernant l'affaire Crypto AG.

Partant de l'existence présumée d'une procédure de cryptage «vulnérable», le SECO en a déduit que les appareils servaient non seulement au cryptage, mais aussi à la cryptanalyse[44]. Ils permettraient ainsi d'analyser des procédures de cryptage et, à l'aide des résultats de cette analyse, de décrypter des informations cryptées au moyen desdites procédures.

Toutefois, le SECO n'a pas tenu compte du fait que le destinataire d'un appareil présentant un cryptage «vulnérable», qui est contrôlé dans le cadre du contrôle à l'exportation, ne peut en tirer aucun profit sur le plan de la cryptanalyse. En effet, il a crypté lui-même les informations et n'a donc pas besoin de les décrypter pour les connaître. Des procédures de cryptage «vulnérables» peuvent par contre permettre plus facilement à des tiers de percer le cryptage des appareils exportés de Suisse.

Outre les soupçons exprimés, la plainte du SECO ne contenait aucune indication concrète sur les «faiblesses» des procédures de cryptage utilisées ni sur les fonctions cryptanalytiques présumées. De même, elle ne mentionnait aucune information concrète des médias qui prouverait l'existence de telles fonctions.

Les médias avaient toutefois révélé à l'époque que l'existence de procédures de cryptage «vulnérables» avait été cachée aux destinataires des appareils. Par conséquent, ces derniers ne pouvaient en aucun cas avoir connaissance des fonctions cryptanalytiques présumées par le SECO.

Selon les informations tirées du rapport MINERVA que les médias ont publiées, les services de renseignement américains avaient eux-mêmes développé les procédures de cryptage «vulnérables» des appareils de Crypto AG et les avaient conçues de

44 Cf. NCE 5A004 de la liste des biens à double usage à l'annexe 2, partie 2.

manière à pouvoir percer le cryptage en temps utile à l'aide de ces connaissances préalables et moyennant des ressources informatiques suffisantes[45]. Les services américains et leurs partenaires disposaient ainsi depuis le début des capacités cryptanalytiques nécessaires pour ce faire. L'exportation de telles fonctionnalités, développées à l'étranger, au moyen d'un appareil de Crypto AG, fabriqué en Suisse, était ainsi impossible.

Manifestement, le SECO et le DEFR ont fondé la plainte pénale sur les informations publiées par les médias, sans avoir analysé ni compris celles-ci. Ils n'ont en outre fait appel à aucun autre service de l'administration pour vérifier la plausibilité des soupçons avant de déposer la plainte. Le SECO n'a ainsi pas fait preuve, au moment de l'examen des faits, de la diligence requise eu égard en particulier aux lourdes conséquences de sa plainte. Il apparaît en outre que le SECO s'est contenté d'une appréciation juridique générale, sans avoir jamais évalué la plausibilité de celle-ci; le fait qu'il n'ait pris contact avec le délégué de la Confédération à la cybersécurité qu'après avoir déposé sa plainte ne fait que confirmer ce constat.

Le SECO a par ailleurs supposé que les exportations de Crypto AG étaient soumises au régime du permis au sens de l'OSIC. Cependant, cela ne serait plausible que si les États auxquels étaient destinés les appareils de Crypto AG pouvaient aussi utiliser les procédures de cryptage «vulnérables» pour surveiller les activités numériques de leurs habitants. Or, la vulnérabilité du cryptage n'a compromis que le cryptage des autorités des États répressifs qui ont utilisé ces appareils, pas celui de leurs habitants. Dès lors, l'hypothèse selon laquelle les appareils de cryptage de Crypto AG pourraient être soumis aux dispositions de l'OSIC ne peut, dans les faits, en aucun cas être retenue, et on ne peut donc pas en déduire que l'entreprise a violé les obligations de déclaration prévues par l'ordonnance.

De même, les arguments présentés par le SECO pour appuyer ses soupçons de violations de la LCB, qui prévoit que l'exportation de biens dotés de fonctions cryptanalytiques est soumise au régime du permis, ne sont guère convaincants. Étant donné que Crypto AG n'avait pas déclaré de telles fonctions dans ses demandes d'exportation, le SECO la soupçonnait de s'être rendue coupable de n'avoir pas fourni des informations complètes.

Il convient de relever ici que seules les procédures utilisant un cryptage «fort» sont soumises au contrôle à l'exportation[46]. L'hypothèse abstraite du SECO selon laquelle un cryptage «vulnérable» implique nécessairement des fonctions cryptanalytiques revient à dire que de la même caractéristique d'un appareil – à savoir le cryptage «vulnérable» – découle à la fois l'obligation d'obtenir une autorisation, en raison de l'existence de fonctions cryptanalytiques, et l'exemption d'une telle obligation, car le

45 Cf. The intelligence coup of the century. In: Washington Post, 11.2.2020: la National Security Agency (NSA) n'a pas installé de simples «portes dérobées» et n'a pas programmé secrètement les appareils de manière à ce que ceux-ci livrent leur clé de cryptage. La NSA devait en outre continuer d'intercepter les communications d'autres États. (...) Toutefois, la manipulation des algorithmes de Crypto (AG) a facilité le processus de décryptage en ce que certaines tâches qui prendraient normalement des mois ont pu être exécutées en quelques secondes [trad.].

46 La liste des biens à double usage, qui figure à l'annexe 2, partie 2, OCB, définit, sous le NCE 5A002, les types de procédures de cryptage et la longueur minimale des clés utilisées qui sont soumises au régime du permis.

cryptage est «vulnérable». En conséquence, des prescriptions contradictoires s'appliqueraient à l'exportation d'un appareil présentant la double caractéristique présumée par le SECO. L'erreur ne pouvant pas se trouver dans le droit relatif au contrôle à l'exportation, l'hypothèse abstraite du SECO selon laquelle des appareils pour lesquels des procédures de cryptage «vulnérables» ont été appliquées doivent être dotés de fonctions cryptanalytiques est nécessairement erronée à la lumière du droit relatif au contrôle à l'exportation.

8.4.3 Demande d'autorisation du MPC et entretien de la DélCdG avec la présidente de la Confédération et la cheffe du DFJP

L'art. 66, al. 1, LOAP (infractions politiques) prévoit que la poursuite des infractions pénales est soumise à l'autorisation du Conseil fédéral et que celui-ci peut la refuser si les intérêts du pays l'exigent.

Dans sa demande d'autorisation du 13 mars 2020, le MPC indique qu'il existe un soupçon suffisant laissant présumer un délit ou un crime selon l'art. 14 LCB et l'art. 9 OSIC. Le MPC fait valoir que l'application de l'art. 66 LOAP n'est pas clairement réglée et que cet article ne se limite pas au titre 13 du code pénal. Parvenant à la conclusion que les diverses conditions étaient remplies dans le cas de la plainte pénale déposée par le SECO, le MPC a soumis au Conseil fédéral la décision concernant l'autorisation d'ouvrir une poursuite pénale. Il n'est pas nécessaire d'exposer ici les raisons ayant motivé cette décision.

Dans la demande d'autorisation adressée au Conseil fédéral, le MPC a indiqué qu'il n'était pas urgent d'accorder une autorisation et qu'il était peu judicieux de le faire avant que la DélCdG ait pu se pencher sur la question sous l'angle politique.

Le 25 mai 2020, la DélCdG a mené un entretien – notamment en raison de la demande d'autorisation du MPC – avec la présidente de la Confédération (*Simonetta Sommaruga*) et la cheffe du DFJP (*Karin Keller-Sutter*), à laquelle la demande d'autorisation avait été adressée. Comme cela a été exposé au chap. 7.5, la DélCdG ne savait pas à l'époque si le Conseil fédéral avait véritablement conscience du caractère sensible et de la portée de la question. En raison notamment de la demande d'autorisation adressée par le MPC au DFJP, la délégation tenait à communiquer à la présidente de la Confédération et à la cheffe du DFJP les dernières informations dont elle disposait, afin que le Conseil fédéral puisse examiner la demande d'autorisation sur cette base. En outre, la cheffe du DFJP a sollicité un entretien avec la DélCdG afin d'évaluer s'il s'agissait en l'occurrence d'un cas d'une importance particulière nécessitant qu'il soit soumis à la décision du Conseil fédéral. La cheffe du DDPS a relevé que, selon une pratique constante, une autorisation n'était refusée que dans de rares cas et uniquement pour des motifs institutionnels impératifs.

Par lettre du 28 mai 2020, la DélCdG a informé l'ensemble du Conseil fédéral des principaux résultats intermédiaires de ses investigations et attiré son attention sur les risques que présentait à ses yeux la plainte pénale du SECO pour la sécurité de la Suisse. Elle a toutefois clairement souligné que la décision relative à la demande

d'autorisation du MPC était une question politique à laquelle seul le Conseil fédéral pouvait répondre.

Lors de sa séance du 19 juin 2020, le Conseil fédéral a pris la décision d'autoriser le MPC à ouvrir une procédure pénale. Les principales conclusions de la DélCdG ont été reprises dans la proposition soumise par le DFJP au Conseil fédéral.

8.5 Demandes individuelles d'exportation des entreprises ayant succédé à Crypto AG

De la décision du DEFR du 20 décembre 2019 de retirer les licences générales d'exportation a découlé celle d'évaluer d'éventuelles futures demandes dans le cadre d'une procédure d'autorisation individuelle. Jusqu'au 10 juin 2020, treize demandes d'exportation de Crypto International AG et deux demandes de TCG Legacy AG ont été déposées.

Le 4 mars 2020, le groupe chargé du contrôle des exportations s'est réuni en vertu de l'art. 27, al. 3, OCB, afin de délibérer au sujet des diverses demandes d'exportation. Il a décidé de soumettre les demandes concernées au Conseil fédéral pour décision, conformément à l'art. 47, al. 4, de la loi sur l'organisation du gouvernement et de l'administration (LOGA)[47]. Le groupe de contrôle est toutefois parvenu à la conclusion qu'il n'existait aucun motif légal justifiant de ne pas délivrer de licence d'exportation. En mai 2020, le DETEC et le DDPS se sont prononcés en faveur de l'octroi des licences d'exportation. Le DFAE souhaitait pour sa part approuver les demandes de TCG Legacy AG et soumettre celles de Crypto International AG au Conseil fédéral pour décision.

Le 10 mars 2020, le SECO et le délégué fédéral à la cybersécurité se sont réunis pour un entretien. Cette prise de contact faisait suite à un mandat du SECO visant à déterminer qui pourrait soutenir ce dernier pour l'analyse, lors de futures demandes d'exportation, d'appareils de cryptage ayant éventuellement subi des manipulations. Le délégué a répondu aux questions du SECO le 30 mars 2020 au moyen d'une note d'information. Il a estimé qu'un examen des appareils était certes possible, mais qu'il prendrait un temps considérable et ne fournirait guère d'indications fiables. Il a précisé que sans recourir à l'expertise des cryptologues de l'armée, un examen technique n'était pas réaliste. Cependant, le SG-DDPS a refusé une collaboration en la matière. Dans ce contexte, le délégué a proposé de renoncer à un examen des appareils avant l'exportation. Du point de vue de la DélCdG, il convient de relever qu'il s'agit là des premiers efforts déployés par le SECO, après la décision de retrait des licences générales d'exportation et après le dépôt de sa plainte pénale, en vue d'acquérir l'expertise nécessaire à l'évaluation des demandes.

Dans la première proposition qu'il a soumise au Conseil fédéral, le 10 juin 2020, le DEFR a demandé que toutes les demandes soient autorisées. Il ressort de cette proposition que le groupe de contrôle avait estimé qu'il n'y avait aucun motif légal suscep-

47 Loi du 21.3.1997 sur l'organisation du gouvernement et de l'administration (LOGA; RS **172.010**).

tible de justifier le refus de l'exportation. Puis, le DEFR a opéré un surprenant changement de cap en soumettant une proposition remaniée au Conseil fédéral dans laquelle il a demandé que ce dernier suspende sa décision concernant les demandes d'exportation jusqu'à ce que le MPC ait clos son enquête. La DélCdG ne s'explique pas ce changement de cap, puisque ni l'évaluation du délégué fédéral à la cybersécurité ni celle du groupe de contrôle n'avaient changé. Elle trouve la seule explication plausible dans la procédure de corapport, lors de laquelle un département s'était dit favorable à ce que le Conseil fédéral ne statue sur les demandes d'exportation que lorsque les enquêtes du MPC et de la DélCdG seraient achevées. Le Conseil fédéral a accepté la demande en question lors de sa séance du 19 juin 2020. Le DEFR a en outre invoqué à l'appui de sa proposition qu'il n'était pas impossible que les demandes individuelles d'exportation en suspens portent aussi sur des appareils issus des stocks de l'ancienne société Crypto AG. C'est une autre raison pour laquelle la décision initiale du DEFR d'approuver les demandes est surprenante. Les arguments avancés pour justifier la proposition soumise au Conseil fédéral n'ont d'ailleurs pas été adaptés, bien que cette dernière ait été fondamentalement remaniée.

La DélCdG ignore si les demandes concernaient également des appareils saisis par le MPC ou si le DEFR a clarifié cet aspect.

Le 7 août 2020, Crypto International AG a présenté une demande de réexamen de sa demande d'octroi de licences d'exportation. Le Conseil fédéral a rejeté cette demande de réexamen à sa séance du 26 août 2020.

8.6 Plainte pénale et report du traitement des demandes individuelles d'exportation: évaluation par la DélCdG

La DélCdG ne comprend pas l'approche suivie par le Conseil fédéral, le DEFR et le SECO s'agissant des demandes individuelles d'exportation des sociétés Crypto International AG et TCG Legacy AG. D'une part, il faut souligner ici qu'il s'est écoulé un très long délai entre le dépôt des demandes et la décision du Conseil fédéral du 19 juin 2020 ou le moment où la proposition a été soumise au Conseil fédéral pour qu'il statue sur cette question. Il convient de le mentionner en particulier parce que le groupe de contrôle avait déjà estimé, le 4 mars 2020, qu'il n'existait aucun motif légal s'opposant à une exportation. D'autre part, et précisément dans ce contexte, la DélCdG critique les décisions prises par le Conseil fédéral respectivement le 19 juin 2020 et le 26 août 2020 de suspendre la décision relative aux demandes jusqu'à la clôture de la procédure du MPC. Même si dans ce cas, comme l'affirme le Conseil fédéral, aucun délai légal ne s'applique au traitement d'une demande, l'approche suivie par le Conseil fédéral est susceptible de contrevenir au principe de la bonne foi puisque, en principe, toute entreprise suisse est en droit d'attendre un traitement rapide de ses demandes d'autorisation d'exportation, à moins que des motifs juridiques s'y opposent.

Il n'est pas acceptable que le SECO applique les décisions du Conseil fédéral du 19 juin 2020 et du 26 août 2020, lesquelles se rapportaient à des demandes d'exportation spécifiques, désormais également à d'autres demandes individuelles d'exportation.

S'agissant de la plainte pénale, la DélCdG s'étonne du fait qu'une plainte pénale soit déposée pour des motifs politiques par un office fédéral ou un secrétariat d'État et que le dépôt d'une telle plainte ne relève pas de la compétence de l'autorité politique suprême (chef du département concerné ou Conseil fédéral), d'autant plus si la plainte en question est justifiée par des motifs politiques. La DélCdG tient notamment à souligner que le SECO n'a eu connaissance que de fragments des faits et qu'il s'est avant tout fondé sur les informations relayées par les médias pour se forger une opinion. Aux yeux de la DélCdG, cet état de fait a aussi conduit le SECO à soumettre, à tort, l'exportation d'appareils de cryptage au régime du permis selon l'OSIC. Cette façon de procéder a empêché une évaluation adéquate de la portée des faits. Eu égard à ce qui précède, le dépôt d'une plainte pénale par le SECO pour des motifs politiques est plus que problématique.

En fin de compte, la procédure de contrôle des biens a été utilisée par le département compétent pour faire face à la pression politique qui a découlé du débat public sur l'affaire Crypto AG. La législation sur le contrôle des biens n'était cependant pas le bon moyen pour donner une réponse politique à une affaire relevant du renseignement, comme l'affaire Crypto AG. Avec la plainte pénale du SECO, le DEFR en premier lieu, mais également le Conseil fédéral se sont soustraits à leur responsabilité de conduite politique.

8.7 Conséquences pour l'inspection de la DélCdG

L'approche suivie par le SECO et le DEFR a également eu d'importantes conséquences sur les actions du Conseil fédéral et le travail de la DélCdG. Dans la demande d'autorisation qu'il avait adressée au DFJP, le MPC avait déjà évoqué un lien possible entre la procédure pénale et les résultats de l'inspection de la DélCdG. Ainsi, lorsque le Conseil fédéral a décidé qu'il ne se prononcerait pas sur l'autorisation des demandes d'exportation des sociétés ayant succédé à Crypto AG avant la clôture de la procédure du MPC, il a accepté de ne pas pouvoir prendre non plus de décision à ce sujet avant que la DélCdG ait terminé ses travaux.

Lorsque la DélCdG a réalisé que les décisions du Conseil fédéral du 19 juin 2020 entraîneraient un report, d'une durée indéterminée, de la décision finale sur les demandes d'exportation des sociétés ayant succédé à Crypto AG, elle a été contrainte d'étendre son inspection à ce nouvel aspect de l'affaire Crypto AG. Les décisions du Conseil fédéral ont donc occasionné un surcroît de travail pour l'inspection de la DélCdG, qui a lui-même entraîné un retard dans les travaux du MPC. Enfin, le Conseil fédéral a fait dépendre son traitement des demandes d'exportation en suspens de l'inspection de la haute surveillance parlementaire, ce qui est problématique du point de vue de la séparation des pouvoirs.

Du point de vue de la DélCdG, il convient également de préciser qu'elle a informé le Conseil fédéral par écrit, le 28 mai 2020, de tous les faits essentiels concernant les

liens entre Crypto AG, les services de renseignement américains et le service de renseignement suisse. Depuis le 26 février 2020, chaque membre du Conseil fédéral était en outre en possession d'une copie du bilan interne de la situation effectué par le SRC à la mi-septembre 2019 (cf. ch. 4.1.3). Le 19 juin 2020, le Conseil fédéral disposait donc de toutes les informations nécessaires pour évaluer lui-même tous les aspects pertinents de l'affaire Crypto AG. Ainsi, il aurait pu se doter des bases décisionnelles nécessaires afin de prendre une décision finale concernant les deux objets (demande d'autorisation et demandes d'exportation) qui étaient en suspens à la suite de la réaction non concertée du chef du DEFR (*Guy Parmelin*) dans l'affaire Crypto AG. Il n'y avait pas de raison d'attendre la clôture de la procédure pénale du MPC ni celle de l'inspection de la DélCdG.

Dans sa réponse aux diverses interventions parlementaires déposées durant la session de printemps, le Conseil fédéral a expliqué qu'il attendrait le rapport de la DélCdG après que cette dernière avait retiré, le 21 février 2020, son autorisation relative à l'enquête confiée par le Conseil fédéral à M. Oberholzer.[48] Par ailleurs, le Conseil fédéral a souligné qu'il ne prendrait pas de décisions susceptibles de nuire à l'inspection de la DélCdG ou d'en préjuger. En déposant une plainte pénale le 25 février 2020, le SECO avait déjà agi en contradiction avec cette ligne de conduite définie par le Conseil fédéral, avant que cette dernière soit communiquée aux Chambres fédérales. C'est pourquoi, sans pour autant remettre en question l'indépendance de la justice, la DélCdG considère que les plaintes pénales émanant de l'exécutif devraient, à l'avenir, être coordonnées si elles risquent de nuire à une inspection décidée par la délégation.

9 Recommandations

Recommandation 1: La cheffe du DDPS et son secrétariat général se dotent des instruments nécessaires pour être à même, d'une part, de se procurer immédiatement et de manière autonome les informations dont ils ont besoin si une affaire liée au renseignement survient et, d'autre part, de veiller à ce que la conduite politique du SRC et la capacité d'action du Conseil fédéral soient assurées. Tant que cela n'est pas garanti, les mandats confiés à l'AS-Rens ou à des chargés d'enquête externes ne doivent pas être considérés comme opportuns.

Recommandation 2: Le DDPS fait appel à la Délséc de manière ciblée pour garantir l'échange d'informations au sujet de dossiers dans le domaine du renseignement et ainsi renforcer la capacité de conduite du Conseil fédéral lors d'affaires liées au renseignement. La Délséc ou une délégation ad hoc du Conseil fédéral doit en particulier intervenir lorsque le DDPS ne souhaite ou ne peut pas communiquer des informations secrètes au sein d'organes de l'administration.

Recommandation 3: Le DDPS s'assure que le CdA participe en général aux séances de la Délséc en qualité de représentant de l'administration. Si la préparation des dossiers de la Délséc l'exige, le CdA participe aussi aux séances du Groupe Sécurité.

48 Par ex. interpellation urgente du groupe socialiste «Affaire Cryptoleaks. Le Conseil fédéral doit agir au lieu de temporiser» (20.3034).

Recommandation 4: Si une collaboration en matière de renseignement entre le SRC et un service étranger implique une entreprise suisse, le DDPS en informe le Conseil fédéral. Le Conseil fédéral fixe les critères selon lesquels il statuera lui-même sur une telle collaboration.

Recommandation 5: La Confédération ne fait pas l'acquisition de solutions de cryptage auprès de fournisseurs étrangers. Les fournisseurs indigènes doivent garantir à la Confédération qu'ils ont le contrôle des aspects liés à la sécurité du développement et de la production.

Recommandation 6: Le DDPS veille à ce que l'armée conserve suffisamment de compétences spécialisées en matière de cryptologie pour pouvoir évaluer la sécurité des solutions de cryptage acquises par la Confédération. Il fait en sorte que les synergies entre les compétences en matière de cryptographie et de cryptanalyse soient exploitées de manière optimale.

Recommandation 7: Le DDPS veille à ce que les capacités en cryptanalyse restent adaptées aux besoins existant dans le domaine de l'interception des communications, dont les possibilités ont été étendues à l'exploration du réseau câblé dans la LRens.

Recommandation 8: Le DDPS règle comment la documentation de l'échelon le plus élevé de la direction se rapportant à son activité directe de conduite et de surveillance dans les affaires liées au renseignement doit être archivée de manière sûre et légale. En outre, le SG-DDPS assure l'archivage de la documentation personnelle des anciens chefs du département et rend des comptes à la DélCdG.

Recommandation 9: La DélCdG considère qu'il est nécessaire que le SRC puisse, en cas de besoin, accéder rapidement aux connaissances disponibles au sujet des activités de renseignement passées. À cette fin, le SRC établit une vue d'ensemble des opérations et des sources au sujet desquelles il existe encore des dossiers, ce en parallèle à l'archivage des documents issus de la recherche opérationnelle et des échanges menés entre les organisations qui l'ont précédé et des services étrangers.

Recommandation 10: La DélCdG invite le Conseil fédéral à révoquer l'autorisation qu'il a donnée pour la procédure pénale que le MPC a lancée sur la base de la plainte pénale déposée par le SECO. Ensuite, le DEFR devra fournir aux entreprises qui ont succédé à Crypto AG les autorisations d'exportation demandées pour lesquelles aucun motif juridique clair ne justifie un rejet.

Recommandation 11: Les notes d'information secrètes concernant des affaires liées au renseignement ou ayant un rapport avec des affaires en cours d'examen par la DélCdG, et dont le Conseil fédéral a pris connaissance, sont communiquées au fur et à mesure à la DélCdG. Le Conseil fédéral soumet à la délégation une proposition concernant la procédure à suivre.

Recommandation 12: La DélCdG doit préalablement être consultée au sujet des plaintes pénales de la Confédération portant sur des affaires ou des personnes qui font l'objet d'une enquête menée par la délégation. À cette fin, le département compétent ou la ChF demande un avis écrit à l'autorité de poursuite pénale concernée.

10 Suite de la procédure

La DélCdG invite le Conseil fédéral à prendre position sur le présent rapport et les recommandations qu'il contient d'ici au 1er juin 2021. Le MPC est invité à se prononcer sur la recommandation 2 d'ici au 1er juin 2021 également.

Le 2 novembre 2020

Pour la Délégation des Commissions de gestion

Le président: Alfred Heer
La secrétaire: Beatrice Meli Andres

Les Commissions de gestion des Chambres fédérales ont pris acte du présent rapport et approuvé sa publication.

Le 10 novembre 2020

Pour les Commissions de gestion

Le président de la Commission de gestion
du Conseil national:
Erich von Siebenthal, conseiller national

La présidente de la Commission de gestion
du Conseil des États:
Maya Graf, conseillère aux États

La secrétaire: Beatrice Meli Andres

Abréviations

AFS	Archives fédérales suisses
AGFA	Abteilung für Genie und Festung Anlageverzeichnis (fr.: Division du génie et des fortifications – liste des installations)
AS-Rens	Autorité de surveillance indépendante des activités de renseignement
BAC	Base d'aide au commandement de l'armée
BO	Bulletin Officiel de l'Assemblée fédérale
BWIP	Bewilligungsressort für Industrieprodukte (fr.: secteur Contrôle à l'exportation / Produits industriels du SECO)
CdA	Chef de l'armée
CdG	Commissions de gestion
CEP	Commission d'enquête parlementaire
ChF	Chancellerie fédérale
CP	Code pénal suisse du 21.12.1937 (RS *311.0*)
Cst.	Constitution fédérale de la Confédération suisse du 18.4.1999 (RS *101*)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DélCdG	Délégation des Commissions de gestion
Délséc	Délégation pour la sécurité
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
DMF	Département militaire fédéral
ELIC	E-Licensing (système d'autorisation électronique)
fedpol	Office fédéral de la police
FF	Feuille fédérale
Grrens	Groupe des renseignements
GTID	Groupe de travail interdépartemental
Installation K	Installation protégée
ISIS	«Système de traitement des données relatives à la protection de l'État» resp. «Système d'information sécurité intérieure»
Iv. pa.	initiative parlementaire
LAAM	Loi fédérale du 3.2.1995 sur l'armée et l'administration militaire (Loi sur l'armée; RS *510.10*)
LAr	Loi fédérale du 26.6.1998 sur l'archivage (RS *152.1*)

LCB	Loi fédérale du 13.12.1996 sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (Loi sur le contrôle des biens; RS *946.202*)
LFRC	Loi fédérale du 3.10.2008 sur le renseignement civil, abrogée le 1.9.2017 (RO *2009* 6565)
LMSI	Loi fédérale du 21.3.1997 instituant des mesures visant au maintien de la sûreté intérieure (RS *120*)
LOAP	Loi fédérale du 19.3.2010 sur l'organisation des autorités pénales de la Confédération (Loi sur l'organisation des autorités pénales; RS *173.71*)
LOGA	Loi du 21.3.1997 sur l'organisation du gouvernement et de l'administration (RS *172.010*)
LParl	Loi du 13.12.2002 sur l'Assemblée fédérale (Loi sur le Parlement; RS *171.10*)
LRens	Loi fédérale du 25.9.2015 sur le renseignement (RS *121*)
LTrans	Loi fédérale du 17.12.2004 sur le principe de la transparence dans l'administration (Loi sur la transparence; RS *152.3*)
MPC	Ministère public de la Confédération
NCE	numéro de contrôle à l'exportation
NDBB	Abteilung Beschaffung des NDB (fr.: Division Recherche du SRC)
NDBU	Abteilung Unterstützung des NDB (fr.: Division Aide à la conduite et à l'engagement du SRC)
OCB	Ordonnance du 3.6.2016 sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (Ordonnance sur le contrôle des biens; RS *946.202.1*)
OFJ	Office fédéral de la justice
OFTRM	Office fédéral des troupes de transmission
OMSI	Ordonnance du 27.6.2001 sur les mesures visant au maintien de la sûreté intérieure, abrogée le 1.1.2010 (RO *2001* 1829)
ORen/ORens	Ordonnance du 4.12.1995 sur le renseignement, abrogée le 1.1.2001, citée dans les versions du 4.12.1995 (RO *1995* 5298), du 4.12.2000 (RO *2001* 124) et – sous le nouveau titre – Ordonnance du 26.9.2003 sur l'organisation des services de renseignements au sein du DDPS (ORens; RO *2003* 4001)
OSIC	Ordonnance du 13.5.2015 sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (RS 9*46.202.3*)
OSRC	Ordonnance du 4.12.2009 sur le Service de renseignement de la Confédération (RO *2009* 6937)
PF	Police fédérale
PJF	Police judiciaire fédérale
RO	Recueil officiel du droit fédéral
RS	Recueil systématique du droit fédéral

SAP	Service d'analyse et de prévention
SECO	Secrétariat d'Etat à l'économie
SG	Secrétariat général
SRC	Service de renseignement de la Confédération
SRS	Service de renseignement stratégique

Annexe 1

Liste des personnes auditionnées

Entre le 19 février et le 26 août 2020, la DélCdG a mené des auditions ou des entretiens avec les représentants de la Confédération (anciens et actuels) suivants:

Amherd, Viola	Conseillère fédérale, cheffe du DDPS (depuis 2019)
Boehler, Jürgen	Chef Contrôles à l'exportation/Produits industriels, SECO, DEFR
Brossard, Jean-Claude	Chef Aide à la conduite et à l'engagement, SRC, DDPS
Bühler, Jürg	Vice-directeur et chef Recherche par intérim, SRC, DDPS, auparavant deuxième adjoint du chef de la PF (à partir de 1993), chef Recherche, SAP (à partir de 2001), chef Coordination / Situation, SRC (à partir de 2010), chef Analyse, SRC (à partir de 2015)
Eckmann, Nils	Procureur fédéral assistant, division Protection de l'État / Organisations criminelles, MPC
Eder, Toni	Secrétaire général du DDPS
Gaudin, Jean-Philippe	Directeur du SRC, DDPS (depuis 2018)
Haefelin, Rainer	Ancien chef Sécurité de l'information et cryptologie (de 2005 à 2018), BAC, DDPS
Keller-Sutter, Karin	Conseillère fédérale, cheffe du DFJP (depuis 2019)
Koller, Arnold	Ancien conseiller fédéral, chef du DMF (de 1987 à 1989) et du DFJP (de 1989 à 1999)
Lauber, Michael	Procureur général de la Confédération (de 2012 à 2020)
Leuthold, Christian	Chef du Centre des opérations électroniques, BAC, DDPS
Maurer, Ueli	Conseiller fédéral, chef du DFF (depuis 2016), auparavant chef du DDPS (de 2009 à 2015)
Nydegger, Kurt	Ancien chef BAC (de 2003 à 2010)
Nyffeler, Peter	Ancien chef Cryptologie et cryptage (de 1982 à 2004), OFTRM/Groupe de l'aide au commandement/BAC
Oberholzer, Niklaus	Ancien juge fédéral, responsable du comité de recherche du Conseil fédéral, chargé d'enquête de la DélCdG
Parmelin, Guy	Conseiller fédéral, chef du DEFR (depuis 2019), auparavant chef du DDPS (de 2016 à 2018)

Regli, Peter	Ancien sous-chef d'état-major du renseignement (de 1991 à 2000), auparavant sous-chef d'état-major adjoint du renseignement (de 1989 à 1991) et chef Renseignement aérien et antiaérien (de 1981 à 1988)
Schmid, Samuel	Ancien conseiller fédéral, chef du DDPS (de 2001 à 2008)
Schöttli, Thomas	Vice-directeur et chef Coordination/Situation, SRC, DDPS
Schreier, Fred	Ancien chef SRS (de 1990 à 1999), auparavant chef Analyse (de 1978 à 1989), Groupe renseignements et sécurité
Seiler, Markus	Secrétaire général du DFAE (depuis 2017), auparavant directeur du SRC, DDPS (de 2010 à 2017), et secrétaire général du DDPS (de 2004 à 2009)
Sommaruga, Simonetta	Présidente de la Confédération, cheffe du DETEC (depuis 2019), auparavant cheffe du DFJP (de 2010 à 2018)
Süssli, Thomas	Chef de l'armée (depuis 2020), auparavant chef BAC (de 2018 à 2019)
Villiger, Kaspar	Ancien conseiller fédéral, chef du DMF (de 1989 à 1995) et du DFF (de 1996 à 2003)
von Daeniken, Urs	Ancien chef SAP (de 2001 à 2008), auparavant chef de la PF (de 1990 à 2000)
Walter, René	Chef Sécurité de l'information et cryptologie (depuis 2018), BAC, DDPS
Wegmüller, Hans	Ancien directeur SRS (de 2001 à 2008), auparavant chef Recherche (de 1987 à 1993) au sein du Groupe des renseignements
Wüger, Daniel	Secrétaire général adjoint, DFJP
X	Personne actuellement au service du DDPS
Y	Personne anciennement au service du DDPS
Zinniker, Paul	Ancien directeur adjoint SRC et chef Recherche SRC (de 2010 à 2019), auparavant directeur SRC par intérim (de 2017 à 2018), directeur SRS (de 2008 à 2009) et chef Recherche SRS (à partir de 1996)