Sécurité informatique au Service de renseignement de la Confédération

Rapport du 30 août 2013 de la Délégation des Commissions de gestion des Chambres fédérales (résumé)

Avis du Conseil fédéral

du 30 octobre 2013

Table des matières

Rapport

1 Introduction

1.1 Contexte

Le Service de renseignement de la Confédération (SRC) existe sous sa forme actuelle depuis le 1er janvier 2010. Auparavant, les tâches qu'il assume étaient partagées entre le Service d'analyse et de prévention (SAP ; rattaché au Département fédéral de justice et police (DFJP) jusqu'à la fin 2008) et le Service de renseignement stratégique (SRS ; au DDPS). Les bases légales sur lesquelles s'appuie le SRC sont notamment la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC ; RS 121) et la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI ; RS 120). Ces bases légales doivent être remplacées par une nouvelle loi sur les services de renseignement qui se trouvait en phase de consultation jusqu'au 30 juin 2013.

1.2 Ressources et synergies

Arrêté du Conseil fédéral du 25 mars 2009

Le 25 mars 2009, le Conseil fédéral a chargé le DDPS de prendre les mesures nécessaires en vue de la fusion, au 1er janvier 2010, du SAP et du SRS en un seul office, au sens de la LFRC. Les obligations relatives à cette mise en œuvre sont énumérées dans une note de discussion correspondante :

1. mise en œuvre dans un délai approprié ;
2. mise en œuvre dans le cadre des lois en vigueur ;
3. mise en œuvre sans ressources supplémentaires ;
4. transparence et contrôles sont des tâches permanentes.

Le point 3 précise que la solution recherchée doit être réalisée sans ressources supplémentaires.

Initiative parlementaire Hofmann

L'initiative parlementaire Hofmann du 13 mars 2007 (07.404 : Transfert des tâches des services de renseignement civils à un département) avait déjà pour objectif l'amélioration des résultats en matière de renseignement :

« L'initiative vise uniquement à optimiser l'exploitation des données recueillies dans le cadre des activités de renseignement. Le regroupement des missions du SAP et du SRS au sein d'un même département permettra par la même occasion de créer des synergies et de garantir que les ressources limitées seront utilisées au mieux. »

En conséquence, l'avis du Conseil fédéral du 23 avril 2008 relatif au rapport de la Commission de gestion du Conseil des Etat du 29 février 2008 met aussi l'accent sur une utilisation optimale des ressources à disposition (FF 2008 3630s).

Les différentes interventions et discussions qui ont conduit à la création du SRC montrent que les attentes portaient en premier lieu sur des prestations supplémentaires du nouveau service dans son domaine d'activité principal.

Situation initiale du SAP et du SRS avant la fusion

La réunion de deux unités organisationnelles permet généralement de réaliser des effets de synergie en supprimant les chevauchements. La situation initiale du SAP et du SRS en la matière était toutefois fondamentalement différente.

Les fonctions transversales et d'assistance (informatique, services, communication, service du personnel, sécurité, droit et autres fonctions de support spécifiques à l'acquisition du renseignement) dont disposaient le SAP et le SRS étaient très réduites, lorsqu'elles existaient. Le SAP avait recours aux centres de service départementaux du DFJP pour la quasi-totalité des prestations dont il avait besoin et ne disposait pas de fonctions d'assistance propres. Le SRS, quant à lui, ne disposait que partiellement des fonctions d'assistance nécessaires et avait largement recours aux prestations de support du SG DDPS. Le SRC devait, après la fusion, assurer lui-même les fonctions d'assistance dont il avait besoin et en n'ayant recours qu'aux ressources existantes. Cela a par contre entraîné un certain allègement financier au niveau du département.

Le SRC dans la mise en œuvre du réexamen des tâches

Dans son rapport sur la mise en œuvre du réexamen des tâches, le Conseil fédéral a fixé, le 14 avril 2010, des étapes pour la réalisation de 25 mesures à long terme auxquelles les départements devaient donner suite. Ces étapes ont été actualisées le 1er septembre 2010 lors de l'adoption du message relatif au programme de consolidation pour les années 2012 et 2013. La mesure no 13 concernait l'exploitation des synergies dans le domaine des services civils de renseignement. A ce propos, le Conseil fédéral devait se prononcer en 2011 sur l'ampleur et l'utilisation des synergies : [Cette fusion] doit permettre de nouvelles synergies qui restent à quantifier de manière définitive et qui doivent être favorables au budget de la Confédération.

Dans un rapport confidentiel du 27 mai 2011 au Conseil fédéral, le DDPS a montré que la création du SRC par la fusion du SAP et du SRS avait permis de générer des synergies et des économies à l'interne. Toutefois, de nouvelles tâches étaient apparues, que le SRC ne pouvait financer qu'avec les économies ainsi réalisées. En fin de compte, l'opération n'engendrait donc aucune économie pour la Confédération. En revanche, l'amélioration souhaitée des prestations en matière de renseignement était réalisée.

En acceptant ce rapport le 10 juin 2011, le Conseil fédéral a dégagé le SRC du réexamen des tâches.

L'informatique du SRC, nécessaire au maintien de l'exploitation, a constitué, dès le moment de la fusion, un poste dont l'importance n'a cessé de croître, tant au niveau des applications que de l'infrastructure. Afin de garantir cette exploitation, des fournisseurs et des collaborateurs externes ont dû être engagés de manière ponctuelle. Le rapport mentionné plus haut montrait également au Conseil fédéral comment les synergies mises en place depuis 2010 étaient utilisées pour créer diverses fonctions transversales.

1.3 Réalisation des objectifs du Conseil fédéral

Le Conseil fédéral a accompagné étroitement les débuts du SRC avec des objectifs annuels et l'établissement de rapports.

2010 : mise en place des bases organisationnelles

La mise en place du SRC a pu être réalisée dans l'ensemble en 2010. Le modèle de processus du SRC, le paysage des processus et les processus pilotes prévus pour la mise sur pied d'un système de gestion des affaires ont été définis et documentés. Les processus normatifs ont été documentés et mis en œuvre selon la planification. En 2010, le Conseil fédéral a également pris des décisions concernant la suite de la procédure relative à la législation du SRC. Le 27 octobre 2010, il a approuvé le message complémentaire relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (« LMSI II réduite »). Le 24 août 2010, le chef du DDPS a approuvé la proposition de projet et le concept d'une nouvelle loi sur les services de renseignement, suite au mandat donné le 27 novembre 2009 par le Conseil fédéral.

2011 : définition des thèmes prioritaires et assurance qualité

En 2011, l'accent était mis sur la hiérarchisation des domaines thématiques du nouveau mandat central du SRC, sur l'adaptation des bases légales et sur la mise en œuvre des recommandations de la Délégation des Commissions de gestion (DélCdG) concernant l'assurance qualité du système d'information « Sécurité intérieure » (ISIS). Les thèmes ont été fixés au début de 2011 dans le nouveau mandat de base donné par le Conseil fédéral, la mise en œuvre des mesures et la diminution des affaires en suspens concernant ISIS se sont déroulées selon la planification et une esquisse d'acte normatif a été établie pour la loi sur les services de renseignement.

2012 : fin de la mise en œuvre des mesures du rapport ISIS de la DélCdG – cyberstratégie

Les mesures nécessaires à l'application de la LMSI II (adaptation des ordonnances, directives et prescriptions administratives) ont pu être réalisées et sont entrées en vigueur le 16 juillet 2012. Les mesures recommandées par le rapport ISIS de la DélCdG ont pu être intégralement mises en œuvre. Le SRC a également contribué de façon substantielle à la réalisation de la stratégie nationale de protection de la Suisse contre les cyberrisques, qui a été approuvée par le Conseil fédéral le 27 juin 2012.

2013 : message pour la nouvelle loi sur les services de renseignement

L'activité législative a de nouveau été au premier plan en 2013 avec l'adoption du message relatif à la nouvelle loi sur les services de renseignement (consultation jusqu'à fin juin 2013) et l'adoption du message relatif à la révision partielle de la loi fédérale sur le renseignement civil (LFRC). Le Conseil fédéral a réalisé un dernier objectif par sa décision du 14 août 2013 qui doit permettre au SRC de continuer à exploiter des informations essentielles en matière de politique de sécurité concernant l'étranger, disponibles dans la base de données ISAS, également au-delà du mois de juin 2015 si la nouvelle loi sur les services de renseignement devait ne pas encore être entrée en vigueur.

1.4 Règlement des affaires en suspens

Le SRC a, dès le départ, également dû s'occuper de diverses affaires en suspens laissées par les organisations qui l'ont précédé.

Révision de la LMSI

Après près d'une décennie de travail, le vote final des parlementaires du 23 décembre 2011 a permis de mettre positivement un terme à la révision de la LMSI (« LMSI II réduite »), pour laquelle le Conseil fédéral avait approuvé un message complémentaire le 27 octobre 2010.

Affaires en suspens concernant le traitement de données dans ISIS

Immédiatement après la création du SRC, il a été jugé urgent d'agir pour combler le retard constaté relatif à l'assurance qualité dans le traitement des données ISIS. La DélCdG a publié le 21 juin 2010 un rapport d'inspection à ce sujet. Dans sa prise de position du 20 octobre 2010, le Conseil fédéral a approuvé sur le fond toutes les recommandations. Le SRC a lancé toutes les mesures nécessaires pour que la situation puisse être réglée aussi rapidement que possible. Dans son rapport de gestion 2012, le Conseil fédéral a pu constater que les données mentionnées dans le rapport de la DélCdG et qui devaient faire l'objet d'un examen général en profondeur, avaient été entièrement mises à jour au 5 décembre 2012. Lors des contrôles des saisies et de l'examen général, le préposé à la protection des données externe mandaté par le DDPS, l'ancien conseiller aux Etats Hansruedi Stadler, a confirmé que les affaires en suspens avaient été entièrement réglées.

1.5 Défis à relever par le SRC en raison de la situation

Depuis 2010, le SRC s'est trouvé face à plusieurs défis influencés par l'évolution de la situation à l'intérieur du pays et à l'étranger.

Déplacement des priorités relatives à l'acquisition et à l'évaluation d'information

Bien que la Suisse ne soit pas une cible déclarée prioritaire par les mouvements d'inspiration djihadiste, plusieurs citoyens suisses ont, durant ces trois dernières années, été les victimes d'enlèvements politiques ou terroristes. Suite aux violents bouleversements politiques dans les pays arabes et d'Afrique du Nord, une hausse du nombre de déplacements de voyageurs pour motifs djihadistes a pu être constatée non seulement en Europe, mais aussi en Suisse.

Ces trois dernières années, la Suisse a davantage été concernée par les efforts intensifs de certains pays pour acquérir, en contournant les dispositions légales, des biens à double usage dans le but de de pouvoir développer et fabriquer des armes de destruction massive et leurs vecteurs ; cette tendance s'est accentuée avec le développement de la situation au Moyen-Orient.

La prévention et la défense contre des attaques visant des structures informatiques critiques ont aussi gagné en importance. On a constaté une recrudescence des investigations menées par des services de renseignement étrangers au sujet d'opposants à leur régime se trouvant en Suisse ainsi qu'une augmentation de la recherche illégale d'informations sur la place économique, financière, industrielle et scientifique suisse, avec une tendance notable au recours à des attaques informatiques.

Adaptation des capacités

Le Conseil fédéral prend note du fait que le SRC a pris diverses mesures pour relever ces nouveaux défis déterminés par l'évolution des événements :

– Depuis 2010, le SRC, en collaboration avec les cantons, poursuit son programme PROPHYLAX de prévention et de sensibilisation aux menaces de la prolifération-

on et de l'espionnage économique auprès des entreprises, des centres de recherche et des institutions de formation potentiellement concernés. Plus de 1800 entreprises et une centaine de centres de recherche en Suisse et dans la Principauté du Liechtenstein sont intéressées par ce programme. La millième entreprise a été contactée à la fin du mois de septembre 2013.

– Depuis 2011, le SRC, en collaboration avec la Police judiciaire fédérale, réalise un monitorage du djihadisme. Dans sa décision du 10 juin 2010, le Conseil fédéral, s'appuyant sur la mise en œuvre de la motion 07.3751 Büchler, a chargé le SRC d'observer les sites Internet djihadistes.
– En 2012, le SRC a pour la première fois préparé un aperçu national de la situation de l'extrémisme violent actuel avec des moyens électroniques, permettant ainsi d'avoir les bases pour une appréciation de la situation mise à jour de manière continue. Après l'introduction des bases légales correspondantes dans la LMSI, c'est ainsi une demande de longue date des cantons qui a pu être réalisée.
– En 2012, le SRC et l'unité de renseignement de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI ont participé à l'élaboration par le DDPS d'une stratégie nationale de protection de la Suisse contre les cyberrisques. Le Conseil fédéral a approuvé le document correspondant le 27 juin 2012. Ceci a permis de satisfaire plusieurs interventions parlementaires.
– Le 1er mai 2013, le Conseil fédéral a approuvé la répartition des tâches, des compétences et des responsabilités entre les services concernés du DFAE, du DFJP et du DDPS lors de la recherche de solution en cas d'enlèvement. Dans ce cadre, la tâche du SRC est d'assurer le suivi continu de la situation, son évaluation et sa présentation ainsi que de fournir des prestations opérationnelles.

Collaboration ciblée avec les partenaires en Suisse et à l'étranger

Durant ces trois premières années, le SRC a établi et développé de manière ciblée sa collaboration avec des partenaires en Suisse et à l'étranger.

En Suisse, il s'agit principalement des cantons et, au niveau fédéral, des organes représentés au sein du groupe Sécurité. La collaboration avec les cantons a été renforcée par de nouveaux programmes de formation, les demandes d'assurance qualité ainsi que par une nouvelle réglementation de la surveillance des organes cantonaux chargés de la protection de l'Etat.

Dans le cadre de la collaboration avec les services étrangers, le SRC s'est concentré sur les partenaires qui accomplissent des tâches au sens de la LMSI et/ou de la LFRC. La politique du SRC à l'égard des services partenaires est soumise annuellement à l'approbation du Conseil fédéral.

2 Mesures prises par le Conseil fédéral après l'incident

2.1 Vérifications et rapports du chef du DDPS

Le 22 avril 2013, le DDPS a soumis au Conseil fédéral un rapport présentant les événements entourant la fuite de données déjouée et les mesures déjà prises ou encore à prendre après l'incident. Ce document constate que les données du SRC n'ont jamais été en mains non autorisées. Cependant, sans les mesures fermes et rapides qui ont été prises à l'intérieur et à l'extérieur de l'administration, des

données du SRC auraient pu être remises à des tiers, en Suisse ou à l'étranger, ou être publiées.

Le rapport relate également que, suite à ces événements, la direction du DDPS et celle du SRC ont pris les décisions qui s'imposaient. Plusieurs services et groupes d'experts internes et externes à l'administration ont été chargés d'analyser la situation et de mettre en évidence les mesures à prendre. Le SRC a déjà identifié et introduit quelque 40 mesures relevant de ses domaines de compétence. Elles concernent des aspects techniques et organisationnels ainsi que des restrictions de consultation et d'accès.

Après la prise de connaissance par le Conseil fédéral, le rapport du DDPS a été transmis à la DélCdG et publié le 30 avril 2013 par le DDPS.

2.2 Renforcement des effectifs dans les domaines de l'informatique et de la sécurité

Parallèlement à l'élaboration du rapport mentionné ci-dessus, le DDPS a proposé au Conseil fédéral, le 26 avril 2013, de renforcer les effectifs dans les domaines de l'informatique et de la sécurité du SRC.

Par arrêté du 1er mai 2013, le Conseil fédéral a pris connaissance du fait que l'augmentation nécessaire et significative de la sécurité et de la sécurité informatique entraînera la création de huit postes de travail supplémentaires au sein du SRC à partir de 2014 et de trois autres postes de travail à partir de 2015. A l'occasion de son appréciation globale des ressources humaines en 2013, le Conseil fédéral a décidé, par arrêté du 26 juin 2013, d'allouer huit postes dès 2014 sur la base de la proposition du DDPS. Au cours du 1er semestre 2013 déjà, le DDPS a autorisé le SRC à financer immédiatement ces huit postes en puisant dans la réserve du département.

Ces postes supplémentaires permettent de fournir, dans une très large mesure avec des collaborateurs internes, des prestations critiques pour la sécurité et de réaliser des projets de migration qui se sont accumulés. Des capacités manquantes au niveau de la sécurité informatique et de la sécurité d'exploitation ont pu être comblées et des postes redondants ont pu être créés. Le principe des quatre yeux est assuré tout particulièrement lors d'activités spécialement critiques, et ce durant des plages horaires élargies.

2.3 Mesures d'information et de formation à prendre par le DFF en faveur des cadres de l'administration fédérale

Suite à ce vol de données, le Conseil fédéral a chargé le Département fédéral des finances (DFF), en date du 15 mars 2013, de prendre des mesures afin d'informer et de former les cadres de l'administration fédérale aux questions de sécurité de l'information. D'autres améliorations concernant la sécurité suivront avec la nouvelle loi sur la sécurité des informations (LSI) qui est en cours d'élaboration sous la conduite du DDPS. Il est actuellement planifié de mettre en consultation le projet de LSI en janvier 2014.

Le Conseil fédéral reconnaît ainsi la nécessité d'agir conformément aux recommandations de la DélCdG et prend notamment des mesures relatives à la sécurité informatique et à la gestion des risques. Avec ses arrêtés concernant l'augmentation des

ressources dans les domaines de l'informatique et de la sécurité, il a aussi entrepris les démarches nécessaires pour renforcer la sécurité du SRC.

3 A propos des recommandations de la DélCdG

Le Conseil fédéral répond aux différents recommandations comme suit :

Recommandation 1

La DélCdG recommande au Conseil fédéral de charger le DDPS de mener une analyse approfondie et précise sur les effectifs dont le SRC a besoin pour pouvoir exécuter les missions supplémentaires prévues par la nouvelle loi sur le Service de renseignement.

Dans son message concernant la nouvelle loi sur les services de renseignement, le Conseil fédéral démontrera les effets en matière de finances et de ressources humaines induits par chacune des mesures prévues. Les carences dans la sécurité informatique constatées après le vol de données doivent être comblées par les mesures décidées le 1er mai 2013. Même après l'adoption de la nouvelle loi sur les services de renseignement, le SRC disposera de ressources très limitées, en comparaison internationale, et devra fixer des priorités.

Recommandation 2

La DélCdG recommande au Conseil fédéral de s'assurer que le DDPS lui rende compte, d'ici juin 2014, de l'état de la gestion des risques au sein du SRC et précise dans quelle mesure le SRC met en œuvre de manière adéquate les directives du Conseil fédéral en la matière.

Le Conseil fédéral suit cette recommandation et sa mise en œuvre est déjà en cours. Le 9 janvier 2013, le chef du DDPS a chargé la Surveillance des services de renseignement d'évaluer en permanence la poursuite de la mise en place de la gestion des risques au sein du SRC et les mesures qui en découlent. Le Conseil fédéral pourra ainsi s'assurer que le SRC met en œuvre ces directives de manière adéquate.

Recommandation 3

La DélCdG demande au Conseil fédéral de veiller à ce que le délégué à la sécurité informatique du département (DSID DDPS) contrôle, d'ici à la fin de l'année 2014, si toutes les applications et tous les systèmes du SRC ont été dotés d'un concept de sécurité valable contenant une analyse des risques fondée et complète. Un plan de mesures contraignant sera établi pour la correction des carences éventuelles.

Le Conseil fédéral partage l'avis de la DélCdG que les applications et systèmes du SRC doivent être dotés d'un concept de sécurité valable contenant une analyse des risques fondée et complète. Un inventaire exhaustif des objets protégés a été établi. Sur cette base, un plan de mesures pour chacun des objets protégés sera maintenant élaboré par le SRC en accord avec le DSID DDPS. Le Conseil fédéral suit donc cette recommandation.

Recommandation 4

La DélCdG demande au Conseil fédéral de charger le DDPS d'examiner, d'ici à la fin de l'année 2013, si les dispositions de l'art. 7, al. 1, OSI-SRC relatives au cryp-

tage du SiLAN peuvent être mises en œuvre de manière que la charge de travail exigée soit proportionnée aux gains pour la sécurité informatique. Selon le résultat de cet examen, cette disposition devra soit être appliquée dans les meilleurs délais soit être immédiatement abrogée.

Le Conseil fédéral fait sienne cette recommandation relative au cryptage du SiLAN. La déclaration contenue dans l'art. 7, al. 1, OSI-SRC, relative au cryptage du SiLAN repose sur une méprise d'ordre législatif commise par inadvertance lors de l'élaboration de l'ordonnance. Après le vol de données, le SRC a toutefois retenu le cryptage du SiLAN comme consituant une mesure souhaitable en vue de renforcer la sécurité informatique. Lors de la planification de sa mise en œuvre, il s'est avéré que les avantages procurés par le cryptage n'étaient ni proportionnés aux coûts ni aux risques causés à la sécurité informatique, parce qu'un cryptage intégral aurait requis des efforts techniques considérables entraînant des frais en conséquence. Cette mesure a alors été rejetée. En août et septembre 2013, le SRC a procédé à la consultation des offices relative à la modification planifiée de l'OSI-SRC. Le SiLAN est maintenant décrit correctement comme une plateforme autonome et protégée sur laquelle les transmissions de messages sont partiellement cryptées. Les progrès techniques à venir pourraient permettre d'envisager la réalisation d'un cryptage intégral.

Recommandation 5

La DélCdG recommande au Conseil fédéral de réviser l'OCSP de sorte que les collaborateurs externes soient soumis au même degré de contrôle de sécurité que les employés de la Confédération qui exercent la même activité qu'eux. Le service de la Confédération qui est le destinataire final des prestations fournies par les entreprises externes doit être responsable du respect, par ces entreprises et par leurs collaborateurs, des prescriptions applicables.

L'OCSP en vigueur prévoit d'ores et déjà que les collaborateurs externes (tiers) soient soumis aux mêmes exigences en matière de degré de CSP que les employés de la Confédération qui exercent la même activité qu'eux. En fonction des accès planifiés pour eux, les tiers peuvent ainsi être soumis tant à un contrôle de sécurité de base (art. 10, al. 2, OCSP), qu'à un contrôle de sécurité élargi (art. 11, al. 2, OCSP), voire à un contrôle de sécurité élargi avec audition (art. 12, al. 1, OCSP). Il ne s'agit pas d'une lacune juridique mais de l'application des dispositions en vigueur.

L'art. 14, al. 1, let. c, OCSP retient que, pour les tiers prenant part à des projets classifiés à partir de l'échelon CONFIDENTIEL, le CSP est déclenché par l'autorité qui confie le mandat et les entreprises bénéficiant d'une déclaration de sécurité valable dans le cadre de la procédure de maintien du secret. Tout service confiant un mandat classifié à partir de l'échelon CONFIDENTIEL est donc compétente pour la mise en œuvre du CSP du bon degré.

Selon les art. 144 ss de la loi fédérale sur les systèmes d'information de l'armée (LSIA ; RS 510.91), les organes compétents, conformément à l'art. 14, al. 1, OCSP, pour l'ouverture de la procédure de CSP sont en outre reliés (art. 148, al. 1, let. d, LSIA) au Système d'information sur le contrôle de sécurité relatif aux personnes (SICSP) du service spécialisé (CSP DDPS). Conformément à l'art. 148, al. 1, let. d, LSIA, les services fédéraux responsables des tâches relatives à la sécurité dans le cadre des CSP sont pour la plupart reliés au système ou peuvent y avoir accès sur

demande. Les services reliés peuvent accéder en ligne au système pour vérifier si des tiers doivent subir un contrôle de sécurité relatif aux personnes et, dans l'affirmative, quel est le degré de contrôle à effectuer ainsi que pour contrôler si le CSP est encore valable. Les services ont ainsi la vue d'ensemble nécessaire et peuvent, le cas échéant, introduire un nouveau CSP.

Le Conseil fédéral maintient que des bases juridiques claires existent concernant les CSP de tiers et que les responsabilités en la matière ne doivent en principe pas être davantage clarifiées. Les départements et la Chancellerie fédérale sensibiliseront cependant davantage leurs services compétents à ce propos.

Recommandation 6

La DélCdG recommande au Conseil fédéral de présenter, dans son message relatif à la loi sur la sécurité de l'information (LSI), une explication détaillée des rôles imputables aux contrôles de sécurité relatifs aux personnes et à la conduite du personnel dans le domaine de la sécurité de l'information et de les différencier clairement. Parallèlement, il faudrait établir un rapport séparé comportant une estimation des effectifs que la Confédération doit affecter à la réalisation des contrôles de sécurité, d'une part, et une description de la contribution que la Confédération entend ainsi apporter à la sécurité de l'information, d'autre part.

Le Conseil fédéral est d'accord de présenter en détail, dans son message relatif à la LSI, les rôles imputables aux contrôles de sécurité relatifs aux personnes et à la conduite du personnel dans le domaine de la sécurité de l'information ainsi que de les différencier clairement.

Les effectifs que la Confédération affecte aux CSP dépendent directement des contrôles de sécurité relatifs aux personnes requis et effectués par les services spécialisés sur mandat de la Confédération. Les effectifs nécessaires aujourd'hui peuvent donc différer des besoins futurs sur la base de la LSI. Dans le cadre du message, le Conseil fédéral exposera le besoin en ressources.

Recommandation 7

La DélCdG recommande au chef du DDPS de veiller à ce que le SRC déplace la cellule de sécurité dans son organigramme afin qu'elle ne soit plus subordonnée à la division SRCA. Parallèlement, il y a lieu de repenser la répartition des tâches relatives à la gestion des risques à l'échelle du service.

Le Conseil fédéral suit partiellement cette recommandation. La vérification des questions organisationnelles effectuée par le DDPS avec le SRC est placée dans un contexte plus vaste et prend en considération la gestion des risques, l'assurance qualité ainsi que le respect des instructions, directives et règles de conduite (Compliance). La subordination de la cellule de sécurité sera aussi examinée à cette occasion.

Recommandation 8

La DélCdG recommande au DDPS de permettre au SRC de pourvoir les postes d'informaticiens dès 2013, en puisant dans la réserve de personnel du département, et ce même si le Conseil fédéral n'a approuvé ces postes qu'à partir de 2014.

Le DDPS a autorisé le financement de huit postes au sein du SRC au cours du 1er semestre 2013 déjà, afin d'augmenter la sécurité informatique. Entre-temps, la majorité de ces postes a pu être pourvue. Cependant, l'aménagement de la sécurité informatique et le recrutement d'experts en TIC dans les conditions cadres appliquées par la Confédération prendra un certain temps. Au vu de la situation actuelle, les huit postes au SRC pourront être pourvus le 1er janvier 2014.

Recommandation 9

La DélCdG recommande au Conseil fédéral d'élaborer des propositions visant à améliorer le processus de contrôle de l'état de la sécurité informatique au sein de la Confédération. Ces mesures devront permettre au Conseil fédéral d'identifier les risques liés à la sécurité informatique suffisamment tôt, d'adopter les mesures requises pour réduire ces risques et de suivre leur mise en œuvre dans le cadre d'un processus institutionnalisé.

Le Conseil fédéral est prêt à faire sienne cette recommandation et à développer notamment le processus de contrôle de l'état de la sécurité informatique au sein de l'administration fédérale centrale.

Les directives, la mise en œuvre et le controlling seront différenciés dans le domaine de la sécurité informatique de l'administration fédérale.

En vertu de l'ordonnance sur l'informatique dans l'administration fédérale (OIAF, RS 172.010.58), l'Unité de pilotage informatique de la Confédération (UPIC) élabore des directives qui sont approuvées par le Conseil fédéral ou par l'UPIC en ce qui concerne les détails. Ces directives sont fondées sur une analyse actualisée en permanence de la menace et des besoins de protection généraux. La mise en œuvre des directives relève de la compétence des départements et des unités administratives concernés (responsabilité hiérarchique, art. 9, al. 1, et 10, al. 2, OIAF). La hiérarchie est également chargée du contrôle interne de la mise en œuvre alors que le Contrôle fédéral des finances, en tant qu'organe de révision TIC, s'assure que la hiérarchie assume ses responsabilités dans ce domaine (art. 28 OIAF).

Afin de soutenir le Conseil fédéral qui doit assumer la responsabilité générale de l'engagement des TIC au sein de l'administration fédérale (art. 14 OIAF), l'UPIC lui remet un rapport annuel (controlling) fondé sur les déclarations spontanées des départements et propose, au besoin, des améliorations (art. 11 OIAF). Le Conseil fédéral est prêt à développer ce processus et les vérifications effectuées par la CDF, une combinaison que la CdG estime également judicieuse dans son rapport. Il met ainsi en œuvre la recommandation de la CdG.

Recommandation 10

La DélCdG recommande au Conseil fédéral de constituer un groupe de travail interdépartemental placé sous la conduite de l'Office fédéral du personnel (OFPER), dont la mission consistera à élaborer des conditions d'embauche particulières permettant d'améliorer la capacité de réaction des organes de conduite du personnel face aux risques d'attaques internes. Pour obtenir l'adhésion nécessaire du personnel visé, il convient notamment d'envisager des mesures de compensation de nature financière ou autre. Le Conseil fédéral est invité à donner son avis sur les conclusions du groupe de travail d'ici fin 2014.

Le droit du personnel en vigueur prévoit d'ores et déjà la possibillité de suspendre un collaborateur. Cette mesure peut être prise tant pendant que les rapports de travail n'ont pas été résiliés (art. 103 OPers, RS 172.220.111.3) qu'après la résiliation de tels rapports (art. 103a OPers). Dans son rapport, la CdG souhaite étendre notamment la possibilité de parvenir rapidement à une suspension, alors que les rapports de travail n'ont pas été résiliés. L'art. 103, al. 1, OPers fixe les conditions ci-après pour une supension pendant les rapports de travail :

1 Si l'exécution correcte des tâches est compromise, l'autorité compétente en vertu de l'art. 2 peut immédiatement, à titre préventif, prononcer la suspension de l'employé ou lui attribuer une autre fonction:

a. lorsque des événements graves susceptibles de justifier une mesure pénale ou une mesure disciplinaire sont constatés ou soupçonnés,

b. lorsque l'existence d'irrégularités répétées est établie, ou

c. lorsqu'une procédure en cours est entravée.

Recommandation 11

La DélCdG demande au chef du DDPS de veiller au respect inconditionnel des droits à l'information garantis à la Surveillance SR par la loi (art. 8 LFRC, en relation avec l'art. 26, al. 1, LMSI) et de l'ordonnance (art. 33, al. 1, OSRC). Le SRC ne peut limiter ces droits à l'information ni de son propre chef, ni d'entente avec le chef du département.

La question des compétences et des prestations de la Surveillance des services de renseignement (Surveillance SR), un organe interne au DDPS, a été abordée en 2012 déjà. L'élaboration de nouvelle loi sur les services de renseignement (LSRe) et le vol des données survenu au Service de renseignement de la Confédération ont amené le chef du DDPS à charger un expert externe d'examiner les conditions d'un contrôle efficace du SRC et l'efficacité de la Surveillance SR, mise en place début 2009. Le professeur Heinrich Koller, ancien directeur de l'Office fédéral de la justice, s'est vu confier cette tâche. Son étude a notamment permis de clarifier l'appréciation de l'efficacité de la Surveillance SR dans sa forme d'organisation actuelle et la question de savoir si la Surveillance SR dispose des moyens et des droits nécessaires.

Les droits et obligations de la Surveillance SR, notamment son vaste droit d'être informé, ont été définis aux art. 31 à 34 de l'ordonnance du Conseil fédéral sur le Service de renseignement de la Confédération (OSRC ; RS 121.1) et précisés, à l'interne du département, dans les Directives du chef du DDPS concernant la Surveillance des services de renseignement du 20 janvier 2011. Le personnel du SRC est ainsi tenu de dire toute la vérité à la Surveillance des services de renseignement et de lui donner des informations intégrales. Dans son rapport final livré fin mars 2013, le professeur Koller a également recommandé d'accroître l'importance accordée à la Surveillance SR à l'interne du département, de faciliter l'accès direct au chef du DDPS et d'ancrer, formellement dans une loi, l'indépendance de la Surveillance SR dans l'accomplissement de ses tâches.

Afin de mettre en œuvre ces recommandations, le chef du DDPS a décidé, fin avril 2013, de renforcer la Surveillance SR en adoptant un vaste catalogue de mesures. La plus importante d'entre elles prévoit d'inscrire formellement, dans la nouvelle loi sur les services de renseignement, l'indépendance de la Surveillance SR dans

l'accomplissement de ses missions. Son art. 66 est complété comme suit : « Elle [la Surveillance SR] exécute ses tâches de contrôle sans aucune instruction. » Il est déterminant pour le Conseil fédéral que la Surveillance SR puisse remplir son rôle-clé de manière indépendante et efficace puisqu'elle doit examiner la légalité, l'opportunité et l'efficacité des activités des services de renseignement. Dans cet esprit, le Conseil fédéral fait sienne cette recommandation.

4 Conclusions

S'il ne reconnaissait pas également les prestations d'ensemble du SRC, un rapport concernant des carences manifestes dans l'un des domaines partiels du SRC contredirait la perception réelle qu'ont du SRC ses donneurs d'ouvrage et ses bénéficiaires de prestations. Le Conseil fédéral relève que les partenaires étrangers font plus confiance au SRC depuis la fusion.

Un service de renseignement doit toujours estimer les risques politiques, juridiques, humains ou techniques qu'il encourt. Après la fusion des services de renseignement national et international, initiée par les organes de surveillance parlementaires, le nouveau service est parvenu, de l'avis du Conseil fédéral, à assurer, sans pertes de savoir ou graves problèmes de personnel, la légalité de ses activités, à établir une culture d'entreprise commune à tous les collaborateurs et à poursuivre la fourniture de prestations de haute qualité.

Le fait que dans le cas d'espèce, la réaction est tardive, voire qu'elle intervient trop tard de l'avis de la DélCdG, doit permettre de tirer des enseignements pour le SRC et l'administration fédérale. L'affaire examinée dans ce rapport a valeur d'exemple pour montrer les difficultés rencontrées lorsqu'il faut reconnaître à temps et résoudre efficacement des conflits d'objectifs entre les obligations de l'employeur, les droits de l'employé et les intérêts liés à la sécurité de l'Etat et au maintien du secret.