



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Autorité de surveillance indépendante
des activités de renseignement

Rapport d'activités 2019

de l'Autorité de surveillance indépendante
des activités de renseignement (AS-Rens)



1. Résumé

L'AS-Rens a planifié 21 inspections pour l'année 2019.¹ Les inspections 19-13 (processus de recrutement, d'encadrement et de sortie), 19-15 (fonctionnement, contenu et utilisation des systèmes d'information GEVER SRC, BURAUT, SiLAN [analyse temporaire]) et 19-16 (classification de l'information) concernaient pour leur part différents services ou systèmes et ont dès lors été subdivisées en deux à trois rapports distincts. Deux des inspections prévues à l'origine, à savoir 19-17 (payage des systèmes d'information RM) et 19-21 (accès à des systèmes d'information de tiers [Confédération, cantons, services étrangers, poursuite pénale]), n'ont pas pu être démarrées en raison de la priorisation d'autres tâches. L'inspection 19-19 (systèmes d'analyse des données du COE) a quant à elle été lancée peu avant la fin décembre, raison pour laquelle le présent rapport d'activités ne contient aucune information à son sujet.

En 2019, l'AS-Rens a commencé par examiner la collaboration du SRC avec les cantons. Elle a contrôlé les services de renseignement cantonaux (SRCant) de Genève, du Jura, de Berne, des Grisons et de Schaffhouse. Les SRCant, qui sont intégrés aux polices cantonales dans presque tous les cantons, sont pour la plupart financés par la Confédération. En 2019, les prestations fournies par ces services cantonaux correspondaient à un volume total de 124 postes à temps plein. L'AS-Rens a développé à cet effet une inspection standard et a émis diverses recommandations, avant tout d'un point de vue organisationnel.

En outre, elle a mené cinq inspections dans le domaine des mesures de recherche soumises à autorisation (MRSA) et des opérations, ainsi que quatre pour ce qui est du traitement des données et de l'archivage.

Eu égard à la population totale de la Suisse, le nombre de personnes concernées par une MRSA est infiniment petit².

L'AS-Rens est d'avis que cet instrument du SRC, des plus invasifs, est utilisé de manière adéquate. Le SRC s'immisçant par ce biais profondément dans les droits fondamentaux des personnes concernées, leur usage tendanciellement prudent est approprié. L'AS-Rens va suivre attentivement l'évolution future dans ce domaine.

Au sein du SRC, l'AS-Rens voit un potentiel d'amélioration avant tout dans le domaine du traitement des données. Le SRC doit pouvoir expliquer de manière transparente quelles informations personnelles sont récoltées et exploitées dans ses banques de données et pourquoi. Des exigences élevées peuvent aussi être posées en termes d'ordonnancement et de discipline en matière de suppression de données, points sur lesquels le SRC peut s'améliorer. Les réflexions nécessaires à cet effet sont complexes, avant tout d'un point de vue technique. Il faut par ailleurs tenir compte du fait que l'on attend des projections de la part d'un service de renseignement. L'un des principes majeurs du renseignement consiste à penser à l'impossible et à en déduire des scénarios plausibles. Or, il est aujourd'hui souvent difficile de savoir ce dont on aura besoin demain pour l'extrapolation de ces scénarios.

Les services examinés sont tenus à la transparence vis-à-vis des autorités de surveillance. Ces dernières peuvent consulter des documents, des processus et des locaux qui non seulement ne sont pas accessibles au public, mais qui sont parfois à dessein protégés du public. Cet accès, ainsi que ce droit de consultation ont été octroyés à l'AS-Rens dans toutes les situations et à tout moment.

L'AS-Rens a émis de nombreuses recommandations sur le plan organisationnel, ainsi que dans le domaine des structures et des processus du SRC. Conformément à l'art. 78, al. 7, de la loi fédérale sur le renseignement (LRens)³, c'est le Département fédéral de la défense, de la protection de la popu-

lation et des sports (DDPS) qui est chargé de la mise en œuvre des recommandations. Il ordonne donc au SRC, au RM et au COE de les appliquer. En règle générale, le département exige que l'organe examiné en tienne compte, même si elles ne sont pas contraignantes. L'AS-Rens a formulé 63 recommandations et 40 suggestions. Toutes les recommandations ont été adoptées. Grâce à la mise en œuvre de ces dernières, les risques existants peuvent être minimisés davantage encore et l'efficacité améliorée, ce qui est une préoccupation centrale de l'AS-Rens du point de vue du renforcement en personnel du SRC.

Les deux secteurs liés au renseignement militaire, soit le COE et le RM, ont des compétences attribuées plus étroitement. Il existe une forme de dépendance des deux services militaires vis-à-vis du SRC. Dans les deux cas, le but est de se positionner vis-à-vis du SRC, de remplir les niches de manière optimale, ainsi que d'utiliser et d'optimiser les synergies existantes.

Outre son activité d'inspection, l'AS-Rens a investi du temps pour porter son regard au-delà du cadre habituel dans le contexte national et international, afin de se perfectionner pour accomplir la mission principale, de procéder au transfert de savoir et de poursuivre le développement de la coopération avec nos partenaires et interlocuteurs.

Le rapport d'activités⁴ a été soumis en consultation auprès du DDPS et de la Délégation des Commissions de gestion (DélCdG) du 13 au 23 janvier 2020. Si les commentaires mentionnaient des erreurs de forme ou de fond dans le présent rapport ou des intérêts à protéger qui empêchaient la publication de certaines parties, ceux-ci ont été pris en compte.



¹ Les plans d'inspections sont publiés sur le site www.ab-nd.admin.ch
² En 2018, 28 personnes étaient concernées, voir le rapport de situation du SRC «La sécurité en Suisse 2018».

³ RS 121

⁴ À l'exclusion des chapitres 3 et 8

2. Table des matières

1. Résumé	2
2. Table des matières	4
3. Note personnelle	5
4. Transparence et confidentialité	6
4.1 Combien de transparence faut-il vis-à-vis du public ?	6
4.2 Demandes LTrans portant sur les rapports d'inspection 18-9 et 18-11	10
5. Activités de surveillance	12
5.1 Plan des inspections	12
5.2 Inspections menées en 2019	13
5.2.1 Stratégie et planification	13
5.2.2 Organisation	14
5.2.3 Collaboration	14
5.2.4 MRSA	17
5.2.5 Opérations	19
5.2.6 Ressources	21
5.2.7 Traitement des données et archivage	23
5.3 Acceptation	28
5.4 Controlling des recommandations et des suggestions	28
6. Regard interne	29
6.1 Révision de la LRens	29
6.2 Formation continue du personnel de l'AS-Rens	29
7. Coordination	31
7.1 Contacts nationaux	31
7.2 Contacts internationaux	31
8. Regard externe	33
9. Chiffres-clés au 31 décembre 2019	36
10. Annexe	37
10.1 Plan des inspections 2019	37
10.2 Liste des abréviations	38

3. Note personnelle



Thomas Fritschi, chef de l'AS-Rens

« Ressortissants suisses arrêtés pour terrorisme à l'étranger, montée de l'extrémisme de droite, collecte frénétique et fichage par le SRC, surveillance systématique, cyberattaques, voyageurs du djihad et terroristes présumés, espions russes, service de renseignement fonctionnant uniquement par beau temps... Voilà autant de termes qui ont fait la une des journaux durant l'année écoulée. Vous en souvenez-vous encore ?

Si l'un ou l'autre de ces titres vous concerne ou a suscité votre intérêt, il vous sera sans doute plus ou moins resté en mémoire. De mon côté, ce qui me restera à l'esprit, c'est cette intervention d'un journaliste qui, après la conférence de presse consacrée à la publication du rapport d'activités de l'an dernier, a été quelque peu déçu que l'autorité de surveillance n'ait pas pu présenter de véritable scandale du renseignement.

« Le thème de la transparence sert de fil rouge au présent rapport d'activités. »

Thomas Fritschi

Au cours de l'année 2019, nous avons effectué 19 inspections sur place auprès des services de renseignement concernés. Nous avons conduit 127 entrevues avec du personnel et avons eu un libre accès aux banques de données du SRC. Dans l'ensemble nous avons obtenu un aperçu transparent des activités de renseignement. Cette transparence figure partiellement dans le présent rapport d'activités. Ce dernier est un moyen de mieux expliquer les tenants et aboutissants des activités de renseignement, raison pour laquelle le thème de la transparence sert de fil rouge au présent compte rendu.

Cette année, le point de vue externe est assuré par Martin Stoll. Le correspondant de la Sonntagszeitung pour l'administration fédérale est l'initiateur du site loitransparence.ch, qui est exploité par une association indépendante. Le but est d'établir la loi sur la transparence comme un instrument ef-

ficace en Suisse au service des travailleurs des médias. Il expose sa vision des choses en page 31 de ce rapport.

Novembre 2019 a marqué les 30 ans de l'affaire dite des fiches. J'avais 20 ans à l'époque. Le Mur de Berlin venait de tomber, je n'avais encore de loin pas d'adresse électronique et encore moins un smartphone. Du point de vue du renseignement, l'appréciation de la menace a massivement évolué depuis, tout comme l'organisation des services de renseignement et les bases juridiques sur lesquelles ceux-ci s'appuient. Sur le plan technique, nous avons globalement aujourd'hui des possibilités tout autres pour traiter les données. La révolution numérique place notre société devant d'énormes défis. Dans ce contexte, les services de renseignement doivent fournir des informations-clés pour l'identification précoce des dangers, être plus rapides et plus fiables que les médias sans pour autant amasser des informations erronées ou trop nombreuses, ce qui représente une tâche très exigeante.

Nous avons surveillé l'exécution de ces tâches et constaté que de nombreuses activités ont été effectuées correctement, mais que des erreurs ont également été commises. Dans certains cas, trop de données ont été conservées trop longtemps, ou des rapports ont été rédigés de manière non exhaustive. Nous sommes par ailleurs d'avis que des aménagements organisationnels et des processus optimisés permettraient d'améliorer encore l'efficacité des services de renseignement.

À travers notre travail, nous voulons contribuer à éliminer les risques liés aux activités de renseignement ou, à tout le moins, à les minimiser, tout en respectant les droits fondamentaux des personnes vivant en Suisse.

Je vous souhaite une agréable lecture. »

Thomas Fritschi, chef de l'AS-Rens

4. Transparence et confidentialité

Pour l'accomplissement de notre vision « Nous renforçons la confiance », il est extrêmement important que l'AS-Rens rapporte de manière transparente à la cheffe du DDPS, aux services de renseignement et à la population suisse. Ce dernier point constitue un défi particulier, raison pour laquelle nous avons souhaité mettre quelques facteurs en évidence dans le texte suivant.

4.1 Combien de transparence faut-il vis-à-vis du public ?

Pour l'AS-Rens, la transmission d'observations issues des activités de renseignement est un exercice permanent d'équilibre. D'un côté, les principes du renseignement selon lesquels une personne doit par exemple connaître une information uniquement si cela est nécessaire (need to know) exigent un degré élevé de confidentialité et de discrétion. D'un autre côté, transmettre des savoirs à la population sur les activités de renseignement peut renforcer la compréhension de cette dernière à cet égard. Dans tous les cas, la population suisse devient méfiante lorsque des informations lui sont cachées et qu'elle n'est pas en mesure de comprendre l'action étatique, notamment dans le domaine du renseignement.

Les services de renseignement sont tenus de veiller à ce que les acteurs qui menacent la sécurité intérieure de la Suisse ne puissent pas prendre connaissance d'informations sensibles. Les stratégies et les méthodes de protection doivent rester cachées des adversaires. Elles constituent notre première ligne de défense pour la sécurité de la Suisse. Les espions provenant d'autres pays, les terroristes potentiels, les marchands d'armes nucléaires et les extrémistes violents doivent dès lors en apprendre le moins possible sur les activités de renseignement.

Quiconque souhaite être un partenaire crédible au sein de la communauté internationale du renseignement et avoir accès à des informations sensibles et secrètes doit prouver sa

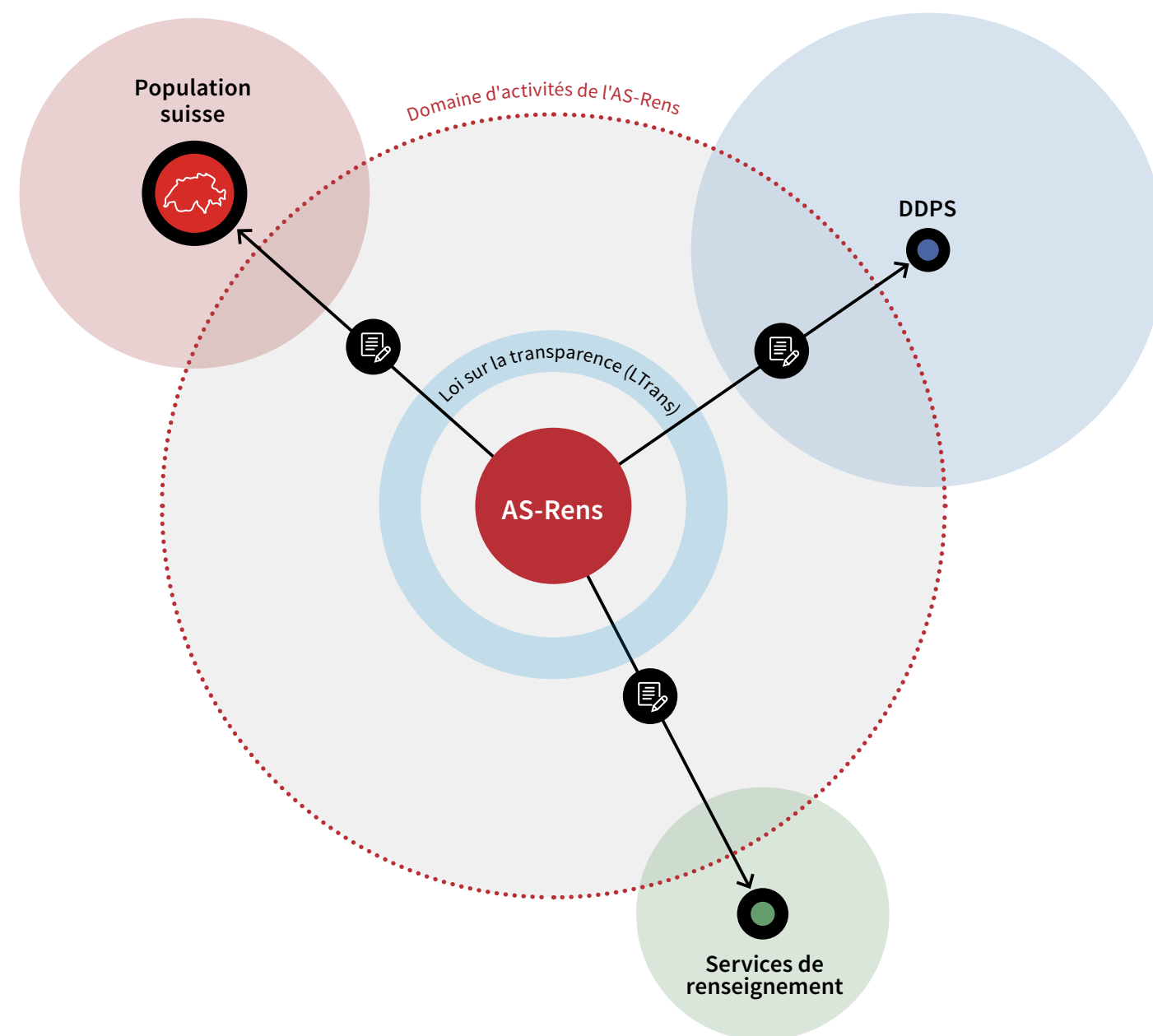
fiabilité et donc cacher au mieux ses sources d'informations et compétences au public. Si de telles informations venaient à faire l'objet d'une couverture médiatique en raison d'une violation des principes du maintien du secret, les services de renseignement concernés risqueraient d'être exclus de tout échange futur d'informations lié à la sécurité entre services partenaires. Une telle situation mettrait elle aussi en péril la sécurité intérieure de la Suisse. Le service autrichien du renseignement intérieur a par exemple vécu de telles expériences au cours de l'année écoulée. Après la confiscation de nombreux supports de données, il a massivement perdu en crédibilité auprès des services de renseignement étrangers et s'efforce depuis lors à se faire réhabiliter⁵.

Les services de renseignement, et plus encore les services secrets, suscitent une grande méfiance ou le rejet auprès d'une partie de la population. De trop nombreux exemples négatifs avec des conséquences douloureuses et catastrophiques pour des ethnies, des opposants politiques ou des minorités expliquent cette attitude. Les activités que ces services mènent dans l'ombre peuvent par conséquent renforcer les préjugés existants.

Le travail d'un service de renseignement consiste principalement à recueillir et à évaluer des informations. Toutefois les dispositions légales doivent être strictement respectées. En Suisse, au cours de l'année écoulée, les gros titres engendrés par la manie de collecter, par le fichage et l'espionnage sup-

⁵ Article paru dans la NZZ du 10 avril 2019 intitulé « Ist Österreichs Geheimdienst noch vertrauenswürdig? »

Des rapports transparents



« Les stratégies et les méthodes de protection doivent rester cachées des adversaires. »

« Des rapports aussi transparents que possible permettent de rendre le champ d'action des services de renseignement plus clair et compréhensible. »

posé de politiciennes et politiciens ont donné une image négative du travail du SRC, rappelant des souvenirs datant de l'affaire des fiches, ainsi que de la surveillance secrète d'une grande partie de la population suisse. En répondant aux demandes d'accès, le SRC contribue de manière importante à la transparence du service vis-à-vis du public. À l'heure actuelle, de nombreux moyens sont investis dans le traitement de ces demandes.

Grâce à son mandat légal d'inspection, l'AS-Rens a un accès détaillé aux activités de renseignement. Les services de renseignement du pays doivent être transparents vis-à-vis de l'AS-Rens. De manière générale, l'AS-Rens a ressenti cette transparence dans son travail quotidien d'inspection. Quant à savoir dans quelle mesure elle peut en informer le public, c'est une autre question. Souvent, il semble que l'un ou l'autre fait relevant d'activités de renseignement pourrait facilement être expliqué à un large public sans pour autant mettre durablement en péril la sécurité du pays. Procéder ainsi permettrait de renforcer la compréhension et, au final, la confiance vis-à-vis des activités de renseignement ainsi que du personnel des services de renseignement en Suisse.

Il est par exemple correct de dire que des noms d'activistes politiques figurent dans les banques de données du SRC. Dans la plupart des cas, ceux-ci émanent toutefois de sources publiques telles que les médias. Il est évident que les prescriptions légales doivent être respectées ici également. Ainsi, des informations sur des activistes politiques ne peuvent être recherchées et traitées qu'à titre exceptionnel, en présence d'indices concrets indiquant que les droits politiques sont utilisés afin de préparer et exécuter des activités relevant du terrorisme, de l'espionnage ou de l'extrémisme violent. Pour l'année écoulée, l'AS-Rens a examiné par sondages le traitement des informations sur des politiciennes et politiciens dans le système de gestion des affaires du SRC et rend compte dans le présent rapport d'activités des constats effectués et des recommandations qui s'y rapportent.⁶

La contribution de l'AS-Rens à la visibilité partielle des activités de renseignement pour le grand public ne passe toutefois pas seulement par les inspections et les rapports qui y sont liés. Les activités de l'AS-Rens sont en effet soumises au champ d'application de la loi du 17 décembre 2004 sur la transparence (LTrans)⁷. La loi vise à promouvoir la transparence quant à la mission, à l'organisation et à l'activité de l'administration, en l'occurrence dans le domaine des services de renseignement. L'AS-Rens en est bien consciente et prend ce mandat légal au sérieux. Elle a en conséquence examiné deux demandes d'accès s'appuyant sur la LTrans et décrit les expériences faites à cet égard dans le présent rapport.⁸

Enfin, la publication du rapport annuel d'activités de l'AS-Rens sert également à la transparence. Conformément aux prescriptions légales, l'AS-Rens rapporte au DDPS. Le rapport est ensuite mis à la disposition du public. Si son contenu doit respecter les directives en matière de prescriptions concernant le maintien du secret, il convient aussi d'informer la population de manière compréhensible sur les activités des services de renseignement. Dans ce cadre, l'AS-Rens peut notamment rapporter les motifs ayant présidé à l'initiation des inspections et les méthodes utilisées à cet effet. De plus, les explications fournies sur les activités de renseignement et les expressions qui y ont cours visent à améliorer la compréhension et les connaissances en la matière.

L'AS-Rens est convaincue que des rapports aussi transparents que possible permettent de rendre le champ d'action des services de renseignement plus clair et compréhensible. Cela induit une certaine charge de travail, car il y a également un intérêt contradictoire à maintenir le secret. Il s'agit donc de peser soigneusement le pour et le contre dans le but de garantir la sécurité de la Suisse.

Un défi particulier pour la préservation de la transparence réside dans le respect des prescriptions de la LTrans. Par conséquent, l'AS-Rens fournit au point suivant des informations sur les premières expériences réalisées à cet égard.

⁶ Rapport d'inspection 19-15

⁷ RS 152.3

⁸ Page 10

« Un défi particulier réside dans le respect des exigences de la loi sur la transparence. »

4.2 Demandes LTrans portant sur les rapports d'inspection 18-9 et 18-11

Après la conférence de presse portant sur le premier rapport d'activités, deux demandes d'accès selon la LTrans ont été déposées auprès de l'AS-Rens. Cette loi vise à renforcer la transparence sur la mission, l'organisation et l'activité de l'administration et, ainsi, à faire la lumière sur les dossiers classés et archivés. Les demandes, déposées par un quotidien suisse, concernaient les rapports d'inspection 18-9 (aperçu des données COE et vérification des critères de sélection du système⁹) et 18-11 (aperçu des mesures du RM visant à atténuer les risques).

Au stade du projet, la LRens prévoyait que l'ensemble des activités du SRC soient exclues du champ d'application de la LTrans. À l'époque, le Préposé fédéral à la protection des données et à la transparence (PFPDT) s'y est opposé en sa qualité de garant du principe de transparence. Au final, conformément à l'art. 67 LRens, seul le secteur le plus sensible du service de renseignement, à savoir la recherche d'informations, a été exclu de la LTrans.

Le rapport d'inspection 18-9 examine la création, le contrôle ainsi que l'adaptation éventuelle des sélecteurs avec lesquels le COE pilote sa recherche d'informations. D'après l'AS-Rens, l'accès au rapport d'inspection 18-9 a dès lors dû être refusé, conformément à l'art. 67 LRens. Aucune autre mesure n'a été prise à l'encontre de cette décision.

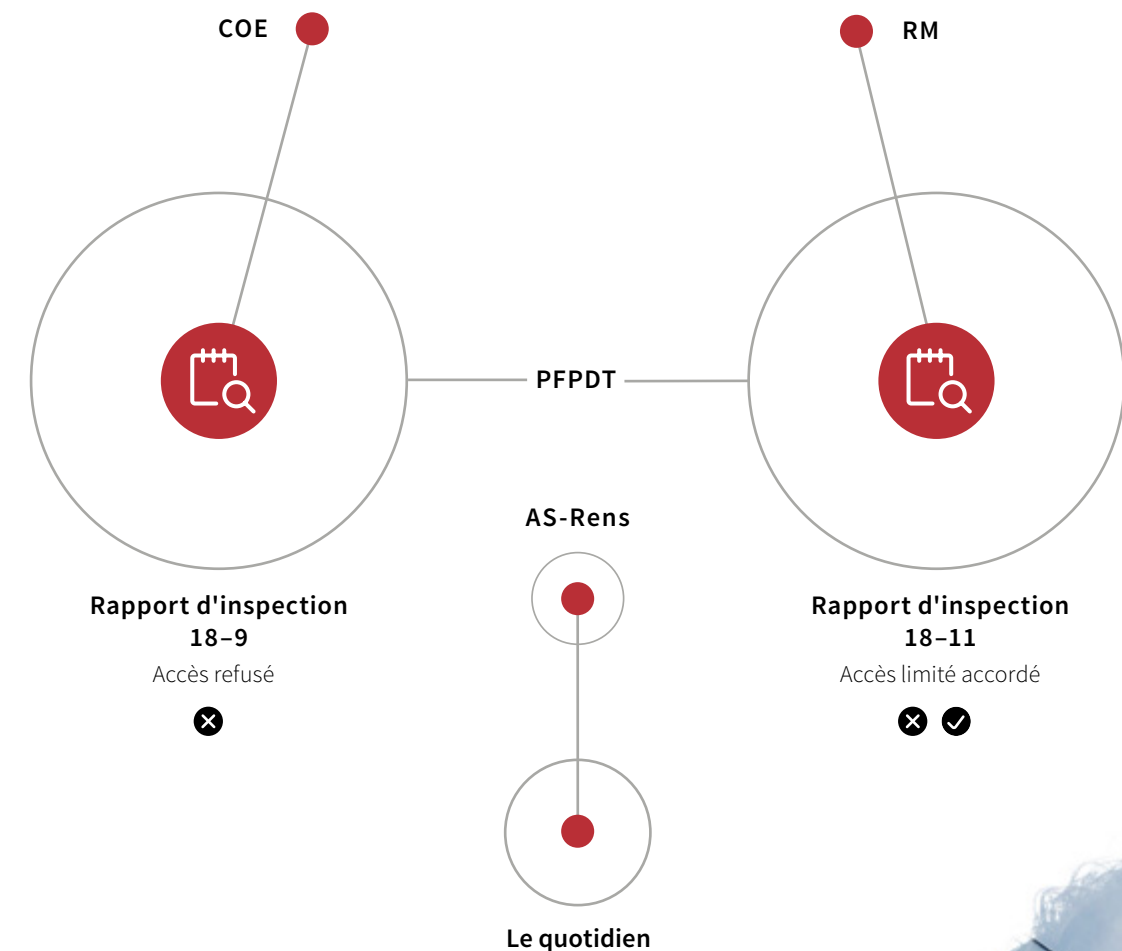
L'AS-Rens a jugé différemment la question de l'accès au rapport d'inspection 18-11. Selon la LTrans, l'accès à des documents officiels peut également être restreint lorsqu'un tel accès met par exemple en péril la sécurité publique. Des informations sur l'organisation, l'activité ou la stratégie d'autorités dotées de tâches de sécurité, en l'occurrence le RM, peuvent faire l'objet d'une telle restriction. De l'avis de l'AS-Rens, tous

les contenus de ce rapport d'inspection ne risquaient toutefois pas de menacer la sécurité publique. Elle a dès lors décidé de donner un accès limité au rapport d'inspection 18-11 et de noircir certains passages et informations qui y figuraient.

Comme le rapport concernait avant tout l'organe surveillé, le RM, l'AS-Rens a prié ce dernier de prendre position. Le RM a pour sa part défendu le point de vue selon lequel l'accès au rapport d'inspection devait être globalement refusé, renvoyant à cet égard à la classification du rapport et arguant que l'exécution du mandat du RM serait considérablement entravée par la publication d'un rapport partiellement noirci. Cette position a été défendue par le commandement de l'armée.

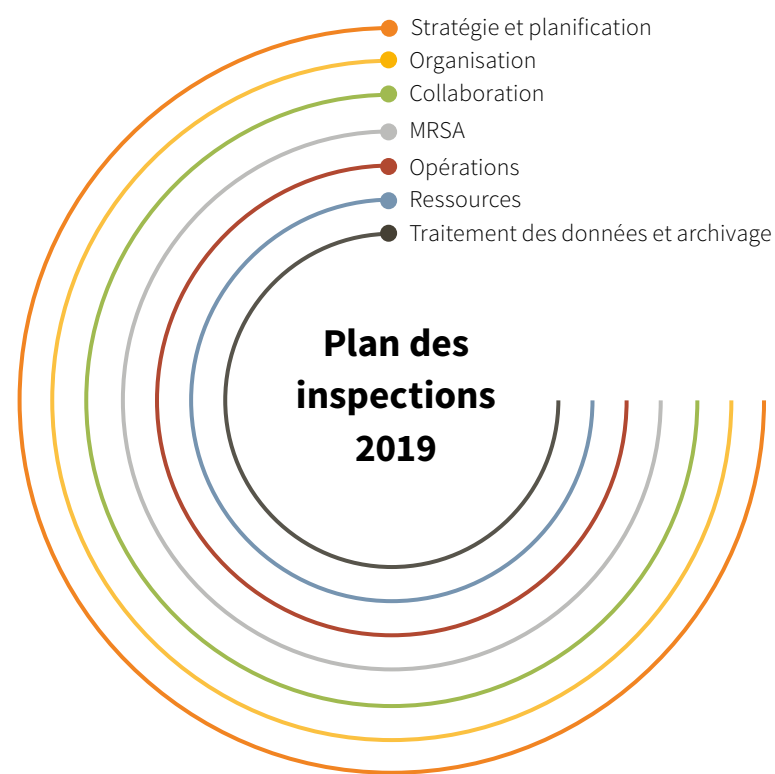
L'AS-Rens y a vu une question de principe et a souhaité clarifier juridiquement les différents points de vue. Elle a donc refusé l'accès au rapport d'inspection 18-11, suivant en cela l'argumentation du RM. Le quotidien s'est opposé à cette décision en déposant une demande de médiation auprès du PFPDT. Cette procédure vise si possible à trouver une entente entre les parties, en l'occurrence l'AS-Rens et le RM d'un côté et le quotidien en question de l'autre. Lors des négociations devant le PFPDT, les parties se sont ensuite entendues pour octroyer un accès à une grande partie du rapport.

Le résultat de la procédure en médiation conforte l'AS-Rens dans sa position consistant à susciter la confiance et la compréhension à chaque fois que cela est possible et autorisé.



⁹ Rapport d'activités 2018, p. 16

5. Activités de surveillance



5.1 Plan des inspections

Chaque année, l'AS-Rens établit un plan des inspections fondé sur les risques, afin de planifier l'exécution de ses tâches. À cette fin, elle évalue les thèmes d'inspection figurant dans son répertoire selon leur probabilité de réalisation et les impacts des risques en question. Le plan des inspections 2019 englobait des inspections dans chacun des secteurs ci-dessous :

- Stratégie et planification
- Organisation
- Collaboration
- Mesures de recherche soumises à autorisation (MRSA)
- Opérations
- Ressources
- Traitement des données et archivage

Le plan des inspections 2019 a été préparé entre les mois de septembre et de décembre 2018. Durant ce laps de temps, le chef du DDPS de l'époque, ainsi que les autorités surveillées ont pu prendre position sur le projet. Le plan définitif a aussi été transmis pour information à d'autres organes de surveillance actifs dans le secteur du renseignement.

« Avec quatre opérations et 170 mesures de recherche soumises à autorisation, la lutte contre l'espionnage s'affiche comme l'une des principales activités du SRC. »

5.2 Inspections menées en 2019

Au total, 21 inspections et le contrôle des recommandations 19-22 étaient planifiés pour 2019. Un partage des inspections 19-13, 19-15 et 19-16 en deux ou trois parties a conduit à l'établissement de sept rapports au total. Les inspections 19-17 (paysage des systèmes d'information RM) et 19-21 (accès à des systèmes d'information de tiers [Confédération, cantons, services étrangers, poursuite pénale]) n'ont pas pu être démarrées, et ce, pour diverses raisons relevant notamment de la priorisation permanente des travaux à effectuer. Ces inspections sont reportées et seront intégrées à de futurs plans d'inspections. L'inspection 19-19 (systèmes d'analyse des données du COE) a été lancée peu avant la fin du mois de décembre 2019, raison pour laquelle aucune information n'est donnée à son sujet dans le présent rapport. L'année 2019 a également marqué le début des inspections dans les cantons. L'AS-Rens a examiné la collaboration entre le SRC et cinq services de renseignement cantonaux (SRCant).

L'AS-Rens a aussi procédé à des clarifications internes, sans devoir consulter les autorités surveillées. Les inspections menées en 2019 sont détaillées aux points suivants selon leurs différents secteurs d'application.

→ Service de renseignement prohibé

Par « service de renseignement prohibé », aussi désigné par la notion d'espionnage, on entend la totalité des actions de recherche d'informations protégées ou secrètes menées au profit d'un État étranger ou d'une entreprise étrangère. À l'inverse, le contre-espionnage d'un pays a comme mission de détecter ces activités, ainsi que d'empêcher au mieux d'autres activités d'espionnage.

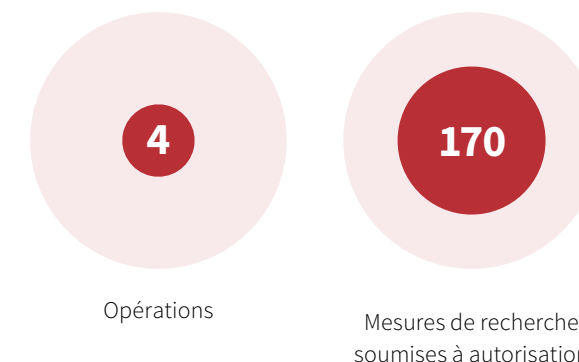
5.2.1 Stratégie et planification

19-1 Stratégie de défense contre l'espionnage

Le rapport du SRC 2019 sur la sécurité de la Suisse montre que notre pays est confronté à une activité d'espionnage toujours aussi agressive de la part de certains États. Avec quatre opérations et 170 MRSA, la lutte contre l'espionnage s'y affiche comme l'une des activités principales du SRC. Une raison suffisante aux yeux de l'AS-Rens pour se préoccuper des réflexions stratégiques dans le domaine de la lutte contre l'espionnage, ainsi que des mesures qui en découlent.

Il en ressort que le SRC considère l'exploration des menaces issues des activités de renseignement prohibées en Suisse comme l'une de ses tâches principales. Lors de l'exécution de mesures visant à véritablement prévenir des activités relevant du renseignement prohibé, le SRC dépend fortement des décideurs politiques. Pour de telles questions stratégiques, il se concentre donc avant tout sur la collaboration avec d'autres autorités ainsi que sur des aspects méthodologiques et organisationnels. L'AS-Rens a estimé que les mesures déjà prises étaient pertinentes et a recommandé de consolider la formulation d'autres aspects stratégiques.

Contre-espionnage 2019



5.2.2 Organisation

19-2 Gestion de l'information en matière de renseignement entre l'attaché de défense (AD) et le SRC

L'AS-Rens s'est intéressée à la gestion et à la coordination des sources d'information sises à l'étranger. Le SRC porte la responsabilité de la recherche d'informations issues du renseignement à travers le réseau de capteurs que sont les attachés de défense. La collaboration selon l'art. 11 al. 2 LRens entre l'armée et le SRC n'est pas concrétisée davantage. Le pilotage des attachés de défense entre les différentes organisations est en partie documenté. La conduite adéquate des missions de renseignement des attachés par le SRC revêt une importance décisive et doit être renforcée, afin d'être encore plus efficace. La plus-value créée par les attachés de défense sur le plan du renseignement doit être consolidée.

5.2.3 Collaboration

Les SRCant sont les organes désignés par chaque canton pour collaborer avec le SRC en vue de l'exécution de la LRens. Que ce soit de leur propre initiative ou sur ordre du SRC, ils recherchent et traitent des informations sur le terrorisme,

l'espionnage, la prolifération, les infrastructures critiques et l'extrémisme violent. Ils sont, pour ainsi dire, les yeux et les oreilles du SRC à l'échelon cantonal. Ces capteurs, qui sont intégrés dans les organes cantonaux de police, sont essentiellement financés par la Confédération. Les moyens financiers sont octroyés sur la base d'une clé de répartition, qui est ré-examinée tous les trois ans. En 2019, les prestations cantonales correspondaient à environ 124 postes à plein temps.

La compétence de surveillance de l'AS-Rens englobe aussi bien les activités du SRC que celles des services cantonaux. Lors de la planification des inspections, l'examen de la légalité, de l'adéquation et de l'efficacité de la collaboration entre ces acteurs était une évidence pour l'AS-Rens. Fin 2018, cette dernière s'est ainsi fixé comme but de procéder à une inspection des 26 SRCant dans les cinq prochaines années. Elle a développé à cet effet un protocole d'inspection standardisé portant sur l'organisation, l'exploitation, la légalité, le traitement des données, la sécurité et l'utilisation des ressources, une manière de procéder permettant également une comparaison entre les cantons. Outre l'examen des documents pertinents, les inspections englobent aussi un sondage annuel effectué auprès du personnel du SRC, au cours duquel leur collaboration avec les services cantonaux contrôlés est examinée. L'AS-Rens rend ensuite visite aux cantons concernés pour une discussion approfondie, à laquelle les autorités can-

→ Attachés de défense

Les AD constituent un réseau de contacts résistant aux crises et indépendant de toute alliance, qui répond aux besoins de la politique suisse en matière de sécurité ainsi que de l'armée. Ils utilisent ce réseau et le développent pour qu'il devienne un instrument efficace et axé sur les prestations.

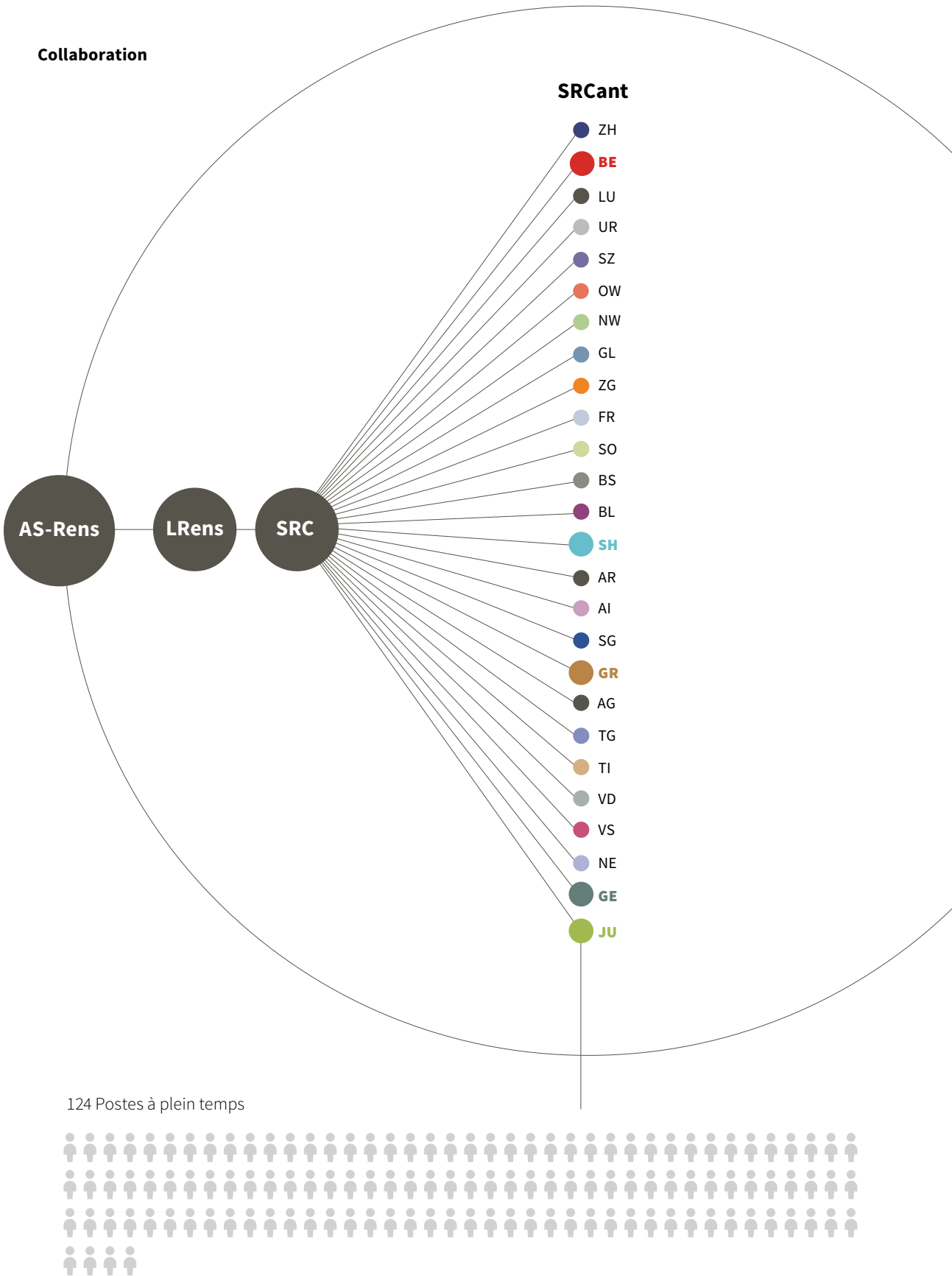
Le 12 août 2019, le réseau des AD suisses englobait 19 accréditations principales et 39 accréditations secondaires¹⁰, dont trois étaient inactives en raison de conflits en cours (Yémen, Syrie et Libye). Ce dispositif est régulièrement révisé.

Les tâches des AD ont été définies par le Conseil fédéral conformément au cadre donné par la Convention de Vienne.

Les AD font partie de l'Armée suisse. Ils reçoivent des missions formulées par différents acteurs et transmises de manière centralisée par le SRC. La conduite des AD est assurée par la division Relations internationales de la Défense (RI D) de l'État-major de l'armée. Le pilotage sur le plan du renseignement est quant à lui assuré par le SRC.

Les AD reçoivent une formation spéciale de six mois dispensée par l'armée, le SRC et d'autres autorités telles que le Secrétariat d'État aux migrations (SEM) ou le Département fédéral des affaires étrangères (DFAE).

¹⁰ <https://www.vtg.admin.ch/fr/actualite/themes/internationale-beziehungen/einsatz.html>, vu le 27 décembre 2019.



tonales de surveillance sont invitées également. Des séances additionnelles peuvent avoir lieu en cas de besoin.

19-3 Inspection SRCant GE

La collaboration entre le service de renseignement cantonal de Genève (SRCant GE) et le SRC a été partiellement conforme au droit. S'agissant du traitement des données, certains aspects ont dû être rendus conformes à la LRens par le canton de Genève, en partie en collaboration avec le SRC. Un potentiel d'amélioration a été identifié en termes d'efficacité et d'adéquation, notamment dans les domaines de la coopération opérationnelle, de l'utilisation des ressources et de l'utilisation des moyens techniques.

19-4 Inspection SRCant JU

L'inspection a permis de constater que la collaboration entre le service de renseignement cantonal du Jura (SRCant JU) et le SRC a été conforme au droit.

Après que l'AS-Rens ait constaté que le service de renseignement cantonal n'avait que peu recherché des informations de sa propre initiative au cours des dernières années, elle a rappelé à ses responsables que cela faisait partie de leurs obligations. L'examen de l'adéquation et de l'efficacité de la collaboration a par ailleurs indiqué que la politique de feedback du SRC était insuffisante. L'AS-Rens a donc recommandé au SRC de donner au moins une fois par an un feedback aux services de renseignement cantonaux sur des thèmes tels que l'initiative propre, la qualité de l'exécution de leur mission ou encore leur potentiel d'amélioration. Afin de sécuriser ses propres informations, l'AS-Rens a exigé du SRC qu'il informe dans le détail les autorités cantonales de surveillance sur la procédure à suivre en cas de consultation de données issues des services de renseignement au sens de l'art. 11 de l'ordonnance du 16 août 2017 sur le renseignement (ORens)¹¹.

19-5 Inspection SRCant GR

En vue du présent rapport, l'AS-Rens a examiné la collaboration du SRC avec le service de renseignement du canton des Grisons (SRCant GR). À cette fin, elle a mené plusieurs entrevues avec les collaborateurs compétents du SRC. Elle a par ailleurs effectué une visite du SRCant GR le 2 juillet 2019. Au moment de l'inspection, la collaboration entre le SRCant GR et le SRC était conforme à la loi, adéquate et en partie efficace. L'AS-Rens a eu l'impression que la collaboration entre les deux organisations était établie et fonctionnait bien, hormis le déséquilibre entre les prestations du SRCant GR et l'indemnisation forfaitaire versée par la Confédération à cet effet.

Les cantons sont indemnisés pour les prestations qu'ils fournissent au profit du SRC. Le crédit mis à disposition du SRC à cet effet est déterminant, et sa hauteur est définie dans le budget. La répartition des moyens s'effectue selon une clé de répartition, qui tient compte de la charge de travail que cela représente pour les cantons. En raison du déséquilibre susmentionné, l'AS-Rens a recommandé que le SRC et le SRCant GR examinent ensemble la situation au niveau des missions et des rapports à fournir, ainsi qu'au niveau de l'indemnisation forfaitaire versée par la Confédération. Si les missions, les rapports ou les prestations du SRCant GR devaient ne pas concorder avec l'indemnisation, il s'agirait soit d'augmenter les prestations opérationnelles du SRCant GR au profit du SRC, soit de diminuer l'indemnisation forfaitaire versée par la Confédération. Dans un même ordre d'idée, l'AS-Rens a également recommandé que le SRCant GR examine avec le SRC la question de savoir sous quelles conditions une implication future et durable du premier au Forum économique mondial (WEF) serait possible. Cette rencontre annuelle entre cheffes et chefs de gouvernement, ainsi que responsables économiques à Davos peut en effet donner la possibilité à des délégations étrangères de mener des opérations d'espionnage.

Le SRC consacre d'importants efforts à la promotion de la collaboration avec les SRCant, par exemple à travers des cours de formation réguliers, la mise à disposition de moyens techniques et des conseils. Le SRCant GR a fait appel à ce soutien

et a tiré profit de ces échanges. Les deux parties ont par ailleurs estimé que la culture du feedback pouvait être améliorée. L'AS-Rens va suivre l'évolution de la situation à cet égard.

19-6 Inspection SRCant SH

Comme pour toutes les inspections effectuées en 2019 auprès des SRCant, l'AS-Rens a mis l'accent sur la collaboration avec le SRC lors de son inspection menée auprès du service de renseignement cantonal de Schaffhouse (SRCant SH). Elle s'est rendue sur place le 11 avril 2019, procédant le jour même aux entrevues avec les personnes impliquées à l'échelle cantonale.

Sur la base des informations récoltées, il a été constaté que la collaboration entre le SRCant SH et le SRC a été conforme au droit, adéquate et efficace. Les deux parties ont mis l'accent sur la gestion commune des tâches relevant du renseignement, ainsi que sur le positionnement du SRCant comme capteur important en la matière. Le SRCant SH a accepté le rapport d'inspection de l'AS-Rens. Les recommandations et suggestions émises par l'AS-Rens, comme par exemple la mise en place au sein de l'environnement informatique cantonal d'un contrôle traçable des suppressions de données inhérentes aux informations issues du renseignement selon la LRens, ont déjà été suivies par le SRCant SH ou seront mises en œuvre.

19-7 Inspection SRCant BE

L'AS-Rens a mené une inspection dans les locaux du service de renseignement cantonal bernois (SRCant BE) en date du 11 mars 2019. Elle a également discuté avec le secrétaire général adjoint de la Direction de la police et des affaires militaires, chargé de la surveillance cantonale de ce service. L'AS-Rens a constaté qu'il manquait, au sein de l'environnement informatique cantonal, un système de contrôle traçable de la suppression des données inhérentes aux informations issues du renseignement selon la LRens. Elle a donc recommandé à la direction du SRCant BE de prendre les mesures nécessaires pour veiller à ce que les informations issues du renseignement provisoirement enregistrées auprès du canton en vue de leur

importation dans le système d'information du SRC soient supprimées de l'environnement de travail cantonal 60 jours après leur dépôt. Ces nettoyages ont dû être documentés.

S'agissant de la coopération entre le SRC et le SRCant BE, l'AS-Rens n'a constaté aucune irrégularité. Elle a eu l'impression que la collaboration entre les deux services était bien établie et qu'elle fonctionnait bien, certainement aussi grâce à la proximité géographique.

5.2.4 MRSA

➔ Mesures de recherche soumises à autorisation (MRSA)

Les MRSA englobent la surveillance du trafic postal et des télécommunications, l'engagement d'appareils de localisation et de surveillance dans des endroits non publics, l'intrusion dans des systèmes informatiques et des réseaux, ainsi que la fouille de locaux, de véhicules ou de conteurs. Toutes ces mesures donnent au SRC de meilleures possibilités pour identifier précocement les éventuels dangers pesant sur la Suisse et sa population. Les MRSA ne peuvent être ordonnées que si la sûreté intérieure ou extérieure de la Suisse est concrètement menacée, par du terrorisme, des activités d'espionnage, la prolifération d'armes de destruction massive et de leurs vecteurs ou une attaque dirigée contre des infrastructures critiques, ou quand leur utilisation, fondée sur une décision du Conseil fédéral, vise à sauvegarder des intérêts nationaux importants. L'extrémisme violent en est exclu.

Conditions supplémentaires du recours à ces mesures, la menace doit s'avérer suffisamment grave et la recherche d'informations par d'autres moyens de renseignement doit être restée vaine jusqu'alors, sans chance d'aboutir, ou rendue excessivement difficile. Les MRSA doivent être approuvées par le Tribunal administratif fédéral (TAF) et avalisées par la cheffe du DDPS, après consultation préalable de ses homologues du DFAE et du Département fédéral de justice et police (DFJP). À cette fin, les instances d'approbation ont accès à toutes les informations utiles.

Dans certains cas, plusieurs MRSA peuvent s'avérer nécessaires. S'agissant du nombre de MRSA, nous renvoyons au rapport annuel sur la sécurité du SRC.

¹¹ RS 121.1

19-8 Adéquation et efficacité des MRSA

L'inspection effectuée a permis de constater que le SRC utilisait les MRSA de manière relativement adéquate et efficace. Le cadre juridique pour la mise en œuvre de ces mesures était connu, et les résultats qui en ont découlé répondaient aux attentes. Dans la plupart des cas, l'accent mis par le SRC sur certaines personnes-cibles a ainsi permis soit de confirmer les soupçons, soit d'exclure ces personnes de ces mesures. L'utilisation des ressources (personnel, technique) nécessaires à la mise en œuvre de ces mesures pourrait quant à elle être améliorée. S'agissant des traductions, il faudrait par ailleurs développer une pratique globale en lieu et place d'une solution au cas par cas.

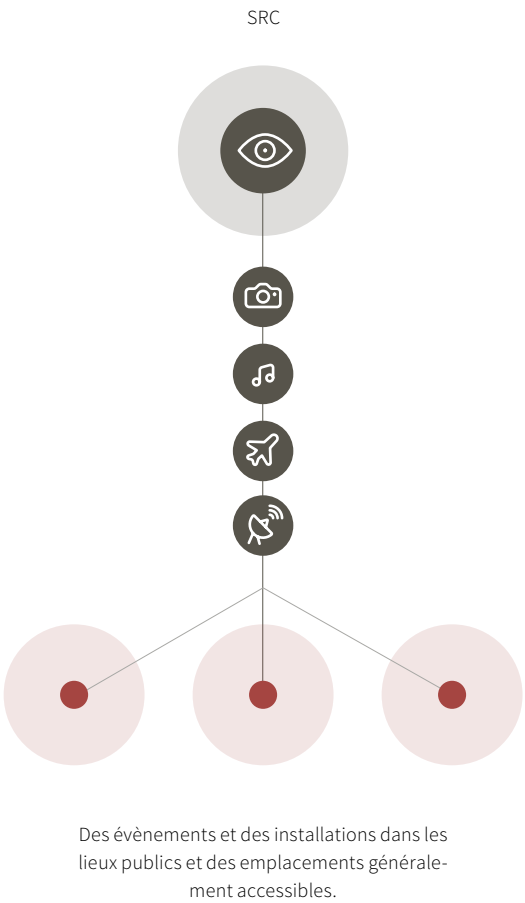
Enfin, la loi opère une distinction entre les MRSA et les mesures de recherche qui peuvent être prises sans approbation préalable. Ces dernières sont considérées comme moins invasives par le législateur. L'observation de personnes dans les lieux publics et librement accessibles en fait partie. L'AS-Rens a dès lors recommandé au SRC d'être mieux en mesure, dès début 2020, de procéder à des observations en fonction des besoins, la hiérarchie des mesures de recherche prévues dans la loi pouvant ainsi être respectée. Cette date correspond au changement prévu dans la structure organisationnelle et dans la répartition des tâches pour l'observation.

19-9 Mise en œuvre des MRSA

L'inspection 19-9 a servi à examiner si le SRC mettait en œuvre les mesures de recherche conformément aux décisions du TAF et respectait les conditions éventuellement imposées. Quelque 35 autorisations, concernant différents types de mesures de recherche, ont été examinées dans ce cadre quant à la légalité de leur mise en œuvre. L'AS-Rens a de plus vérifié si les conditions éventuellement imposées ont été respectées. Elle a constaté lors des inspections que le SRC mettait globalement en œuvre les MRSA de manière correcte et respectait les conditions ad hoc tout en prenant au sérieux le cadre juridique existant. Une vue d'ensemble efficace et effective des MRSA permettrait toutefois de faciliter le pilotage et le contrôle, ainsi que d'établir des rapports de manière plus

→ Observation

Une observation est une recherche d'informations non soumise à autorisation, à travers laquelle le SRC observe des événements et des installations dans les lieux publics et des emplacements généralement accessibles. Des prises de vue et de son peuvent y être effectuées. L'utilisation d'avions et de satellites est expressément autorisée à cet effet. La sphère privée protégée doit toutefois être respectée dans tous les cas.



efficace. L'AS-Rens a donc recommandé d'améliorer les capacités se rapportant à l'utilisation, à l'administration et au contrôle des moyens techniques nécessaires à l'exécution des MRSA.

5.2.5 Opérations

19-10 Opérations

Les opérations de renseignement sont pour le SRC un élément central de la recherche d'informations. Elles vont au-delà du cadre de travail habituel pour ce qui est de leur importance, de leur étendue, des moyens requis ou du maintien du secret. Le rôle central qu'elles jouent au sein du processus de recherche d'informations n'est toutefois pas sans risques :

- Les ressources disponibles pour la recherche d'informations sont-elles effectivement utilisées pour répondre à des menaces majeures pesant sur la sûreté intérieure et extérieure de la Suisse ?
- Les dispositions légales sont-elles respectées ?
- Les procédures adoptées par le SRC dans le cadre d'opérations de renseignement sont-elles objectivement les plus appropriées pour atteindre le but fixé sur le plan du renseignement ?
- Dans quelle mesure le résultat obtenu dans le cadre d'une opération correspond-il à l'objectif visé du point de vue de l'étendue et de la qualité ?

Pour répondre à ces questions, le domaine des opérations du SRC est inspecté au moins une fois par an par l'AS-Rens.

→ Opérations

Dans l'univers du renseignement, la notion d'opération couvre la recherche d'informations au moyen de processus connexes dépassant le cadre habituel des activités de recherche du point de vue de l'importance, de l'étendue, des moyens requis ou du maintien du secret. Une opération de renseignement est limitée dans le temps. Elle doit par ailleurs être formellement initiée puis clôturée.

Dans le cadre d'une opération de renseignement, il est possible de prendre à la fois des mesures non soumises à autorisation (p. ex. des observations dans des lieux publics et librement accessibles) et des MRSA (p. ex. la surveillance du trafic postal et des télécommunications). Si le SRC souhaite exécuter des MRSA, il ne peut le faire que dans le cadre d'une opération de renseignement.

Sur la base de critères choisis et pondérés, l'AS-Rens a établi une matrice de décision et a choisi au final huit opérations de renseignement, dont quatre clôturées, à des fins d'examen approfondi. Les inspections effectuées ont permis de constater que les opérations examinées avaient globalement été exécutées conformément au droit, ainsi qu'avec adéquation et efficacité. Elles étaient clairement définies, limitées dans le temps et documentées séparément.

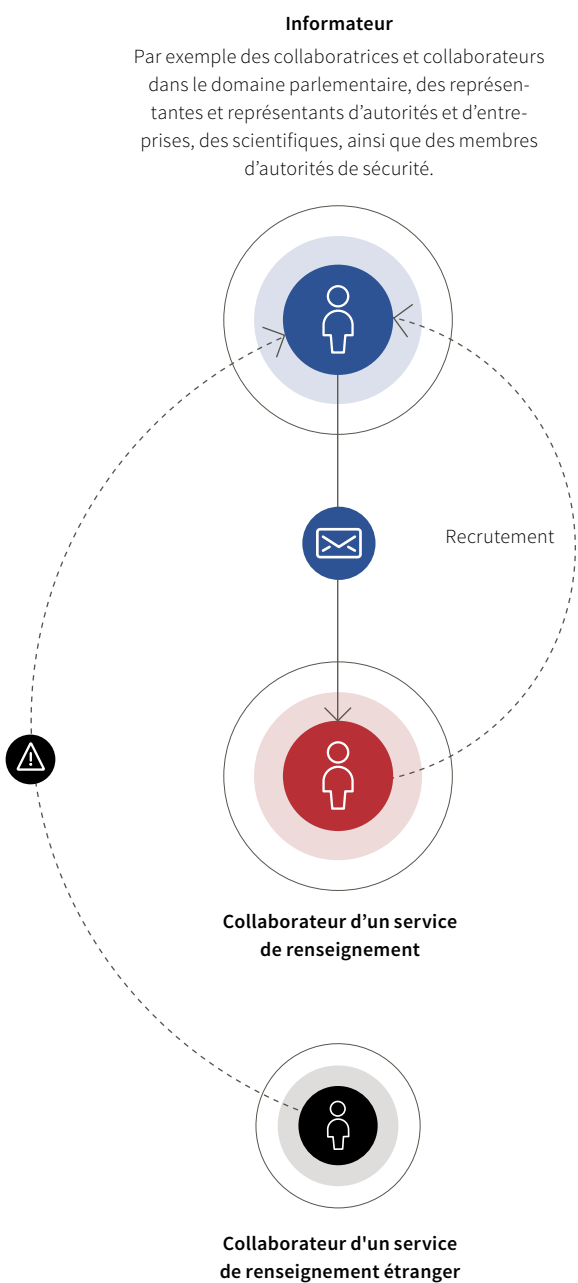
Optimiser et formaliser le processus de gestion et de contrôle des opérations pourrait contribuer à améliorer l'adéquation et l'efficacité des opérations dans leur ensemble.

19-11 Informateurs (HUMINT)

Dans l'inspection 19-11, l'AS-Rens s'est intéressée aux informateurs. Elle a examiné la manière dont le SRC gérait concrètement ses sources, sur la base de quatre cas pour lesquels elle a contrôlé la légalité, l'adéquation et l'efficacité. En raison de la protection des sources et des personnes, le maintien du secret est particulièrement crucial dans ce domaine. C'est pourquoi les inspections HUMINT de l'AS-Rens sont classées SECRET. L'inspection sera finalisée en 2020.

19-12 Protection des informateurs au sein du SRC avec un intérêt particulier sur les couvertures et les identités d'emprunt

L'art. 35 LRens prévoit la protection des sources à travers la garantie et le maintien de leur anonymat. Afin de protéger leur existence, les informateurs ou leurs proches peuvent ainsi bénéficier d'une couverture ou d'une identité d'emprunt au terme de leur collaboration avec le SRC. Celles-ci doivent être autorisées par la cheffe du DDPS.



→ **Informateurs (HUMINT)**

L'abréviation anglaise HUMINT (pour Human Intelligence) se réfère à la recherche d'informations par des informateurs. En d'autres termes, une personne fournit une information et un collaborateur d'un service de renseignement la réceptionne. La notion de reconnaissance opérationnelle est souvent utilisée comme un synonyme de HUMINT. Le terme opérationnel signifie qu'une opération de renseignement donnée permet de prendre une mesure ciblée afin de trouver une information, par exemple en observant une personne ou en mettant à contribution un informateur.

Les informateurs sont choisis et recrutés avec soin. Ils doivent disposer d'un accès à des informations et supports d'information sensibles particulièrement importants pour la Suisse. En raison de la protection des sources et des personnes, le maintien du secret est particulièrement crucial ici. Les personnes qui travaillent comme informateurs fournissent normalement des informations aux services de renseignement volontairement, le plus souvent en toute connaissance de cause, en partie gratuitement lorsque cela sert leurs objectifs personnels ou politiques. Les personnes que l'on cherche à recruter sont surtout celles qui semblent appropriées pour servir de sources d'information sur le long terme. Les possibilités d'accès actuelles et les perspectives professionnelles d'un informateur sont des critères importants. Entrent par exemple en ligne de compte des collaboratrices et collaborateurs dans le domaine parlementaires, des représentantes et représentants d'autorités et d'entreprises, des scientifiques ainsi que des membres d'autorités de sécurité. Les agents de renseignement appliquent toutefois également des méthodes conspiratrices afin d'acquérir des informations particulièrement sensibles.

Les services de renseignement étrangers s'efforcent également d'établir des contacts avec des personnes qui disposent de connaissances ou de possibilités d'accès particulières en Suisse. Ils sont souvent établis dans les ambassades et consulats de leurs pays en Suisse. Ils peuvent rechercher eux-mêmes des informations (de manière ouverte ou cachée) ou soutenir des opérations de renseignement menées directement depuis les quartiers généraux de leur pays d'origine. Ils disposent souvent d'un statut diplomatique et en profitent pour utiliser l'immunité qui y est liée. Si de telles personnes sont découvertes, elles peuvent être expulsées de Suisse.

Humint permet un contact direct et reste ainsi un instrument fondamental pour les services de renseignement, même si l'utilisation de moyens électroniques a relégué cette méthode traditionnelle au second plan. Les informateurs sont également indispensables dans le domaine de l'espionnage politique, car il s'agit ici surtout de rechercher des informations d'après des directives spécifiques des services de renseignement.

« Du point de vue de l'AS-Rens, des processus et responsabilités clairement définis réduisent la probabilité d'erreurs et d'utilisation frauduleuse. »

Des couvertures peuvent toutefois aussi être autorisées par le directeur du SRC pour des collaboratrices et collaborateurs du SRC ou des autorités cantonales d'exécution. Le but ici est de dissimuler l'appartenance de ces personnes à leur service. Les personnes en question peuvent aussi bénéficier d'identités d'emprunt pour une période limitée dans le temps mais prolongeable lorsque cela est nécessaire, afin de garantir leur sécurité ou la recherche d'informations.

Les couvertures permettent de fabriquer ou de modifier des titres (p. ex. un diplôme) au nom de la personne concernée. Pour les identités d'emprunt, des pièces d'identité peuvent être fabriquées ou modifiées, et ce, même en usant de fausses données biographiques (p. ex. nom ou date de naissance).

Comme la modification ou la fabrication de titres ou de pièces d'identité constituent une infraction pénale qui est justifiée à travers l'autorisation du directeur du SRC ou de la cheffe du DDPS, il est important de vérifier que le SRC utilise ces mesures en toute légalité.

Au cours de l'inspection 19-12, l'AS-Rens a donc vérifié si le SRC utilisait les outils permettant de protéger les informateurs, en particulier les couvertures et les identités d'emprunt, de manière légale, adéquate et efficace. Elle a pu constater que la protection des sources jouait un rôle important au sein du SRC et qu'elle y était prise au sérieux. Le SRC a ainsi protégé ses sources à l'aide de diverses mesures à différents niveaux. L'AS-Rens n'a ainsi pas observé d'irrégularités dans le cadre de ses inspections sur le plan des processus d'autorisation se rapportant aux couvertures et aux identités d'emprunt. Cependant, toutes les autorisations de couvertures ont été soumises à l'avance. En d'autres termes, elles ont été sollicitées et autorisées mais sans être nécessairement mises en œuvre et utilisées, ce qui n'était pas adéquat aux yeux de l'AS-Rens.

L'AS-Rens a par ailleurs constaté que les processus et responsabilités se rapportant à la demande, à l'administration, à la fabrication, à l'entretien et à la destruction des couvertures et des identités d'emprunt (ainsi que de l'infrastructure mise en place à cet effet) n'étaient pas intégralement définis et n'étaient que peu harmonisés. Du point de vue de l'AS-Rens,

des processus et des responsabilités clairement définis réduisent la probabilité d'erreurs et d'utilisation frauduleuse. Une harmonisation des processus permettrait dans le même temps d'utiliser les ressources de manière plus efficace.

5.2.6 Ressources

19-13 Processus de recrutement, d'encadrement et de sortie

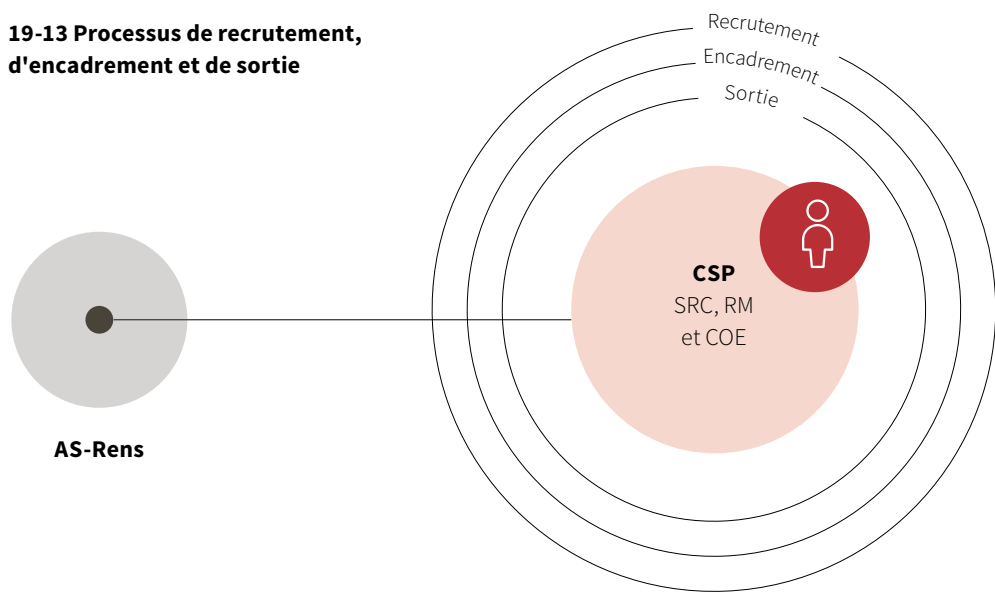
Un risque important pour l'exercice d'activités de renseignement peut émaner du personnel interne (trahison, vol de données, espionnage, etc.). Le vol de données qui a eu lieu en 2012 au SRC en a été un exemple concret. Afin de minimiser les risques, la sélection, le contrôle, l'accompagnement et l'encadrement du personnel par les ressources humaines et la hiérarchie revêtent une importance cruciale.

L'inspection 19-13 a été subdivisée, et un rapport d'inspection distinct a été rédigé pour les deux services examinés que sont le RM (inspection 19-13a) et le COE (inspection 19-13b). À l'origine, le SRC devait également constituer un élément d'inspection. En raison de la charge pesant déjà sur le SRC à cause des autres inspections menées en 2019, l'AS-Rens a renvoyé cette inspection à une date ultérieure.

L'accent a été mis sur les contrôles de sécurité relatifs aux personnes (CSP) pour les trois processus en lien avec le personnel que sont le recrutement, l'encadrement et la sortie. Sur la base d'entretiens, de l'étude de documents et de contrôles ponctuels effectués aux différentes étapes du processus, l'inspection devait déterminer s'il existait un processus pour les CSP et si celui-ci était considéré comme conforme à la loi, adéquat et efficace.

Les processus CSP ayant cours au sein du RM et du COE fonctionnent bien. Au sein du COE, nombreux sont les postes à être catégorisés dans l'échelon le plus élevé, à savoir 12 (CSP 12). Comme ces contrôles impliquent d'interroger davantage de personnes, ils prennent du temps et exigent une initiation précoce. Par le passé, il y a eu des retards dans le renouvelle-

19-13 Processus de recrutement, d'encadrement et de sortie



ment de CSP 12 dont la validité avait expiré pour des collaborateurs engagés depuis plusieurs années. L'AS-Rens a dès lors recommandé que le service compétent au sein du DDPS initie le processus de renouvellement suffisamment tôt.

L'AS-Rens a comparé et analysé les échelons de contrôle des trois services actifs dans le domaine du renseignement – ce qui inclut donc aussi le SRC. Elle a constaté que les pratiques de catégorisation CSP du personnel actif dans le domaine du renseignement divergeaient entre le SRC, le RM et le COE, ce qui est incohérent d'un point de vue légal, factuel et logique. Les différents systèmes de catégorisation CSP actuellement en vigueur au sein du SRC, du RM et du COE devraient être examinés et uniformisés afin d'en accroître l'efficacité. Cet examen devrait aussi tenir compte des éventuelles nouveautés qui pourraient découler de la proposition de nouvelle loi sur la sécurité de l'information, qui était en instance devant le Parlement au moment de l'inspection.

L'inspection a montré que les deux services examinés ont suffisamment tenu compte des risques dans le processus de recrutement. En effet, le CSP était généralement achevé avant la prise de fonction. Après leur arrivée, les nouveaux collaborateurs ont de plus été sensibilisés aux aspects liés à la sécurité et ont reçu des formations correspondantes.

Les risques liés au personnel déjà en place ont été pris en compte de manière adéquate et les supérieurs ont joué un rôle-clé dans l'identification des changements dans l'environnement des collaborateurs. Des contrôles de sécurité organisationnels et techniques ont par ailleurs été effectués à chaque fois que cela était possible et pertinent.

Lors de départs de collaborateurs, il a été veillé à ce que les autorisations d'accès soient désactivées ou supprimées. Une attention suffisante a été consacrée au transfert de savoir, et le personnel sortant a dû signer une déclaration de confidentialité.

19-14 Utilisation sûre de la vidéoconférence

Les systèmes de vidéoconférence constituent aujourd'hui un moyen de communication efficace et largement répandu. Ils sont utilisés par le SRC pour la transmission d'informations à des partenaires.

Dans la plupart des cas, le contenu des conversations est classé SECRET. Pour cette raison, il est impératif d'éviter que des défaillances techniques ou une mauvaise manipulation de la part des usagers ne cause une fuite d'informations.

Afin de déterminer si l'acquisition et l'entretien des systèmes utilisés étaient conformes à la loi, l'AS-Rens a analysé la documentation existante et mené des entretiens avec les personnes responsables au SRC et certains partenaires. Elle a également participé à des vidéoconférences du SRC pour se faire sa propre image du matériel utilisé.

L'examen mené par l'AS-Rens a démontré que ces systèmes avaient été acquis conformément au droit et que leur utilisation était adéquate et efficace. Les normes de sécurité inhérentes au renseignement ont par ailleurs été respectées. L'AS-Rens n'a identifié un potentiel d'amélioration que dans le domaine de l'exploitation.

« Les deux services examinés ont suffisamment tenu compte des risques dans le processus de recrutement. »

« L'examen mené par l'AS-Rens a démontré que ces systèmes de vidéoconférence avaient été acquis conformément au droit et que leur utilisation était adéquate et efficace. »

5.2.7 Traitement des données et archivage

19-15 Fonctionnement, contenu et utilisation des systèmes d'information GEVER SRC, BURAUT, SiLAN (analyse temporaire)

Dans l'inspection 19-15, l'AS-Rens a examiné l'exploitation, le contenu et l'utilisation du système d'information GEVER SRC¹² ainsi que les systèmes de fichiers de BURAUT¹³ et de SiLAN¹⁴ (analyses temporaires) quant à leur légalité. Vu l'étendue de l'inspection et la complexité du système GEVER SRC, les résultats des observations ont été répartis dans deux rapports d'inspection distincts. Le rapport d'inspection 19-15a s'est intéressé exclusivement à GEVER SRC alors que les deux systèmes d'information SiLAN et BURAUT ont été décrits dans le rapport d'inspection 19-15b.

19-15a GEVER SRC

S'agissant de GEVER SRC, l'AS-Rens s'est focalisée sur la légalité de l'octroi des droits d'accès, de la saisie des données et du respect des délais de conservation des données ainsi

que de la suppression et de l'archivage des données. Elle a de plus examiné l'efficacité des contrôles mis en place. Outre une analyse étendue de la documentation, les questions d'inspection ont également été traitées sur la base d'entretiens avec des spécialistes du SRC et des Archives fédérales ainsi que de contrôles ponctuels effectués sur place auprès de dix collaborateurs du SRC.

Les directives en matière de protection des informations et des données exigent que le personnel du SRC n'ait accès qu'aux données dont il a besoin pour l'accomplissement de sa mission. Les conséquences possibles en cas de violation de ces directives par le SRC seraient les suivantes :

- une menace pour la sécurité de la Suisse ;
- une implication du SRC dans des procédures juridiques ;
- une perte de réputation du service dans la population et auprès des services partenaires.

L'inspection effectuée par l'AS-Rens a montré que le SRC disposait d'un concept d'accès complexe pour le système GEVER SRC. Les accès sont gérés à l'aide de différents rôles. L'analyse de la liste d'autorisation et les échantillonnages effectués au-

¹² Système de traitement et de contrôle des dossiers
¹³ Système de fichiers exploité par la BAC
¹⁴ Système de fichiers pour le dépôt de fichiers dans des répertoires

→ GEVER

GEVER (en allemand GEschäftsVERwaltung, gestion des affaires) est utilisé en Suisse comme notion générique pour la gestion électronique des dossiers dans l'administration publique et constitue l'une des bases de la cyberadministration.

Avec l'introduction de GEVER au sein de l'administration fédérale, toutes les informations revêtant une importance du point de vue de la gestion des affaires sont gérées par les unités administratives de manière électronique. Cela englobe tous les dossiers que ces dernières traitent dans le cadre de leur mandat légal.

Axé sur les processus d'affaires, GEVER permet une gestion des dossiers à la fois transparente, traçable, conforme au droit et efficace. Le cycle de vie des documents y est intégralement géré, de leur création à leur archivage ou à leur destruction en passant par leur utilisation, leur enregistrement ou leur tri.

« L’inspection de l’AS-Rens a montré qu’il n’y avait dans GEVER SRC aucun dossier consacré à des politiciennes ou politiciens uniquement en raison de leurs activités politiques. »

près de dix collaborateurs du SRC ont montré que les autorisations étaient pilotées adéquatement et conformément aux prescriptions légales. Du point de vue de l’AS-Rens, le processus de gestion des autorisations peut toutefois encore être amélioré. Le soutien par des organes externes pour la maintenance et le support de GEVER SRC devrait par ailleurs être examiné de plus près.

Toutes les informations revêtant une importance pour la gestion des affaires doivent être traitées dans le système GEVER SRC. Cela concerne en particulier tous les produits du renseignement transmis à l’extérieur, ainsi que toutes les activités officielles (réponses aux lettres des citoyens, réponses aux initiatives parlementaires, activités législatives). Cette procédure est identique pour tous les offices de l’administration fédérale. Si les affaires ne peuvent pas être retracées dans GEVER SRC, le SRC ne peut pas justifier les informations figurant dans ce type de produits. Il est interdit de récolter ou de traiter dans GEVER SRC des informations sur l’activité politique ou sur l’exercice de la liberté d’opinion, de réunion ou d’association en Suisse.¹⁵ Exception : en présence d’indices concrets selon lesquels les droits en question sont exercés pour préparer ou exécuter des activités terroristes, d’espionnage ou d’extrémisme violent.

L’AS-Rens a examiné la légalité de la saisie des données en effectuant des échantillonnages des données saisies dans GEVER SRC en lien avec onze politiciennes et politiciens et en respectant le cadre informationnel selon l’art. 5 al. 5 LRens. L’AS-Rens a par ailleurs vérifié le traitement de cinq demandes d’accès émanant de particuliers et d’organisations ainsi que d’une politicienne et d’un politicien, également saisis dans GEVER SRC. L’inspection de l’AS-Rens a confirmé que le SRC avait répondu aux demandes d’accès correctement et intégralement. Les informations collectées respectaient globalement les prescriptions légales. Il faut mentionner ici que la majorité des informations liées aux personnes contenues dans GEVER SRC sont issues d’articles de presse publics. Sur

la base des échantillonnages effectués, l’AS-Rens a constaté qu’il n’y avait dans GEVER SRC aucun dossier sur des politiciennes ou politiciens uniquement en raison de leurs activités politiques. L’AS-Rens a recommandé à cet égard au SRC d’examiner sa pratique actuelle en matière de collecte d’informations à partir de sources publiques quant à sa légalité.

À ce jour, il n’y a eu encore aucune livraison de documents issus de GEVER SRC aux Archives fédérales. Ce n’est toutefois pas problématique, puisque le délai légal de 20 ans laisse une marge de manœuvre largement suffisante à cet égard. L’AS-Rens a considéré la pratique du SRC consistant à livrer régulièrement les dossiers aux Archives fédérales comme judicieuse, afin de ne pas se retrouver sous la pression du temps à l’approche du terme de la durée de conservation légale.

19-15b SiLAN / BURAUT

SiLAN est une plateforme informatique protégée interne au SRC utilisée pour le traitement de données de tous les niveaux de classification jusqu’à l’échelon SECRET. Ce réseau comprend notamment un stockage de données permettant de traiter des analyses temporaires. L’inspection de l’AS-Rens devrait vérifier la légalité de l’utilisation de ce dépôt.

Lors d’une inspection effectuée sur place auprès de dix collaborateurs du SRC, l’AS-Rens a examiné leurs autorisations d’accès au système temporaire de fichiers. Ces dernières étaient toutes nécessaires et justifiées. L’analyse des contenus du système temporaire de fichiers n’a montré aucune anomalie ou violation des prescriptions en vigueur. Les données traitées n’étaient pas antérieures aux cinq ans autorisés. Du point de vue de l’AS-Rens, l’analyse annuelle effectuée par le service interne de contrôle de qualité du SRC et l’autorisation nécessaire octroyée par le détenteur des données ont garanti un contrôle suffisant du respect des prescriptions légales. Depuis les inspections 18-1 et 18-2, le SRC avait continuellement développé et amélioré les mesures prises à cet effet.

En plus de l’environnement SiLAN, les collaboratrices et collaborateurs du SRC disposent d’un poste de travail BURAUT. Ce système de stockage est une plateforme standard de la Confédération exploitée sur un serveur de la BAC¹⁶ et sert – dans des cas exceptionnels devant être autorisés par le chef de la Gestion de l’information – à enregistrer des fichiers pour la collaboration avec les autres offices et départements. Comme ces données sont exploitées hors du réseau protégé du SRC, elles sont moins bien protégées contre une fuite non autorisée d’informations. Il est par conséquent interdit de traiter dans l’environnement BURAUT des informations classées CONFIDENTIEL non cryptées ou des informations classées SECRET.

Une action de nettoyage initiée par le service interne de contrôle de qualité du SRC a été couronnée de succès aux yeux de l’AS-Rens et a entraîné une sensibilisation, ainsi qu’une réduction marquée des données.

19-16 Classification de l’information

L’inspection 19-16 a été menée en parallèle auprès du SRC, du RM et du COE. Dans ce cadre, il a été examiné si les informations physiques et électroniques étaient traitées de manière conforme au droit.

Le thème de la classification des informations touche à différents autres thèmes et ne peut dès lors pas être considéré séparément. Les aspects liés à la sécurité de l’information, à la conservation des données et à la sécurité physique jouent donc un rôle important dans le maniement d’informations classifiées.

Sécurité de l’information

La société, l’économie, la politique et l’administration sont de plus en plus déterminées par la disponibilité d’informations interconnectées. Il est dès lors de la plus haute importance

que ces informations soient suffisamment protégées et que cette protection soit économiquement viable. Ce principe doit s’appliquer non seulement aux informations elles-mêmes, mais également aux systèmes d’information et de communication qui permettent de saisir, de traiter, de transporter ou d’enregistrer ces informations. C’est la raison pour laquelle on parle dans ce contexte de sécurité de l’information. Celle-ci englobe, outre la protection des informations et la sécurité informatique, aussi la protection des données.

Protection des informations

Elle comprend la protection des informations de la Confédération et de l’armée, en particulier leur classification et leur traitement. Classifier signifie attribuer un niveau de classification (SECRET, CONFIDENTIEL ou INTERNE) à une information en fonction du degré de protection qu’elle nécessite. Les informations sont protégées en garantissant leur confidentialité, leur intégrité, leur disponibilité et leur traçabilité.

L’AS-Rens constate que les différents termes utilisés dans la pratique ne le sont pas de manière cohérente, ce qui peut semer la confusion. On parle ainsi parfois de l’ordonnance concernant la protection des informations et parfois de systèmes de gestion de la sécurité des informations (SGSI). Le Parlement travaille par ailleurs sur un projet de loi sur la sécurité de l’information, qui se trouve actuellement dans le processus législatif et vise à éliminer les incertitudes.

L’inspection 19-16 (classification de l’information) a été menée en parallèle auprès du SRC, du RM et du COE. Dans ce cadre, il a été examiné si les informations physiques et électroniques étaient traitées conformément aux prescriptions en vigueur en matière de protection des informations. L’AS-Rens a ainsi pu constater que la protection des informations de la Confédération était clairement établie par les services examinés par l’intermédiaire du DDPS.

¹⁵ Art. 5, al. 5, LRens

¹⁶ Base d’aide au commandement

« Le thème de la classification des informations touche à différents autres thèmes et ne peut dès lors pas être considéré séparément. »

Grâce à un SGSI complet, bien documenté et suivi, le SRC a veillé à ce que les informations soient traitées conformément au droit et que toutes les exigences posées en termes de sécurité de l'information soient remplies. Après du RM et du COE, le processus inhérent à la sécurité de l'information n'était qu'esquissé sous la forme de concepts isolés, de manuels et de présentations. L'AS-Rens s'attend à ce que cette situation s'améliore dès le milieu de l'année 2020, après l'introduction du SGSI du COE, actuellement en cours de mise en place auprès du commandement des Opérations.

Au sein de l'environnement sécurisé constitué par les systèmes d'information internes, il est moins important de déterminer si le fait que des personnes non autorisées prennent connaissance d'une information risque de causer un préjudice (INTERNE), un dommage (CONFIDENTIEL) ou un dommage sévère (SECRET) aux intérêts nationaux. En revanche, pour les destinataires situés hors de cet environnement sécurisé, une classification CONFIDENTIEL ou SECRET entraîne un surcroît de travail administratif. L'auteur d'informations classifiées doit en être conscient et utiliser l'instrument de la classification de manière pondérée. S'il n'y parvient pas et que les documents sont surclassifiés de manière chronique, la classification risque en fin de compte de ne plus être prise au sérieux. Il se peut alors qu'elle protège moins efficacement les informations qui doivent l'être, voire cesse entièrement de fonctionner. Afin de mettre en place un certain standard permettant notamment d'opérer des comparaisons au sein de l'organisation, il est par exemple possible d'effectuer régulièrement des échantillonnages. Ces derniers devraient être réalisés par un organe qui n'est pas directement impliqué dans les activités principales du service en question.

19-18 Paysage des systèmes d'information du COE

Rattaché à l'armée, le COE assume toute une série de tâches techniques au profit de l'armée, ainsi que des services de renseignement militaire et civil. Il est responsable de l'exploration des voies de communication, ce qui inclut la communication vocale au moyen de téléphones satellitaires et la communication de données via des câbles terrestres. En outre, il joue un rôle important dans le domaine cyber, notamment en ce qui concerne la cyberdéfense, les cyberattaques et la cyberexploration.

L'AS-Rens était dès lors intéressée à connaître les systèmes d'information utilisés par le COE pour ses activités liées au renseignement. En effet, elle avait besoin de solides connaissances des systèmes employés afin de pouvoir s'exprimer sur d'autres thématiques telles que la gestion des données.

Au final, l'AS-Rens a constaté que les systèmes étaient bien documentés. Leur exploitation reposait sur une base juridique solide, et le COE a consenti de gros efforts pour protéger les systèmes en question contre des accès non autorisés depuis l'extérieur.

Pour le COE, les grands défis résident essentiellement dans les nouvelles technologies de communication, en perpétuelle évolution, dans la variété des voies de communication et dans l'énorme volume de données à traiter. Les systèmes d'information et les bases légales qui les régissent doivent dès lors être régulièrement adaptés, afin de répondre, aujourd'hui comme à l'avenir, aux besoins des bénéficiaires de prestations que sont par exemple le SRC ou le RM.

« Les systèmes d'information du COE doivent être adaptés. »

19-19 Systèmes d'analyse des données du COE

Cette inspection n'ayant été lancée qu'à la fin du mois de décembre 2019, le présent rapport ne contient aucune information à son sujet.

19-20 Communication de données personnelles à des autorités étrangères (art. 61 LRens)

L'échange d'informations avec des partenaires étrangers fait partie du quotidien du SRC, raison pour laquelle l'AS-Rens a aussi examiné cet aspect. La transmission de données personnelles à des autorités étrangères est expressément réglée à l'art. 61 LRens.

L'inspection a révélé que le cercle des personnes impliquées dans la communication est défini, que des processus existent pour les divers canaux de communication avec des partenaires étrangers et que les informations échangées étaient enregistrées et facilement accessibles. Les entretiens menés et les contrôles ponctuels effectués sur une trentaine de messages envoyés à des partenaires étrangers ont montré que la pratique développée par le SRC à cet égard permettait globalement de remplir les critères légaux. Le respect de ces critères semblait toutefois plutôt résulter d'une routine que d'une connaissance juridique active des critères applicables. L'AS-Rens a donc recommandé que le SRC améliore l'état des connaissances sur le contexte juridique d'une telle communication, à travers diverses mesures telles que l'adaptation des lignes directrices internes et/ou la formation régulière du personnel concerné. Ces mesures devraient permettre au SRC de veiller à ce que la communication de données personnelles à l'étranger reste conforme à la loi à l'avenir également.

L'AS-Rens a aussi constaté que les données transmises à des tiers devaient être issues du système d'information IASA SRC. Ce critère est connu des collaborateurs et a été largement respecté. Lors de communications émanant du secteur des opérations, les informations peuvent toutefois être communiquées quelques jours avant la saisie dans le système d'information correspondant. Ce problème, lié à des retards dans l'introduction des données, était connu du SRC et devrait être résolu dans les années à venir en partie grâce à la mise à disposition de ressources supplémentaires pour le triage. Dans l'intervalle, il est du ressort du SRC de faire tout ce qui est en son pouvoir pour garantir le respect du texte de l'ordonnance.

6. Regard interne

5.3 Acceptation

Conformément à l'art. 78, al. 6, LRens, l'AS-Rens communique au DDPS les résultats de ses inspections et peut émettre des recommandations à ce sujet. Outre ses recommandations, l'AS-Rens adresse également des suggestions aux services inspectés.

Selon la pratique habituelle de l'AS-Rens, elle formule des suggestions dans les deux cas suivants :

- 1) points observés dont une éventuelle optimisation n'est pas de la compétence de la cheffe du DDPS, mais qui relève d'un échelon opérationnel moins élevé (p. ex. utilisation des téléphones portables lors de séances durant lesquelles un contenu confidentiel est discuté) ;
- 2) points observés par hasard au cours d'une inspection qui ne sont pas directement couverts par le mandat d'inspection mais qui revêtent tout de même une certaine importance.

Il n'existe pas de base juridique pour les suggestions et une vérification de leur mise en œuvre par l'AS-Rens n'est pas prévue. Les suggestions sont un instrument méthodologique important afin de générer des inspections subséquentes. D'une part, les décisions et les travaux de services externes ont un impact sur les activités de renseignement, d'autre part, les recommandations et les suggestions de l'AS-Rens aux services de renseignement peuvent également concerner des services externes, dont la surveillance ne relève pas du champ de compétence de l'AS-Rens.

Conformément à l'art. 78, al. 7, LRens, c'est le DDPS qui doit veiller à la mise en œuvre des recommandations. Il ordonne par conséquent aux autorités surveillées d'appliquer les recommandations émises. S'agissant des suggestions, le département exige en règle générale que le service inspecté les prenne en compte, même si ces dernières ne sont pas contraignantes. En 2019, l'AS-Rens a formulé 63 recommandations et 40 suggestions. Au final, toutes les recommandations ont été acceptées.

Dans le cadre de leur activité, les directeurs d'inspections ont été accueillis de manière constructive et professionnelle par l'ensemble des services contrôlés, obtenant l'accès aux documents et systèmes d'information nécessaires à l'exécution des mandats d'inspection. Le personnel inspecté était à la disposition des directeurs d'inspections. Les entretiens ont pu être planifiés et menés à brève échéance, et les réponses aux questions additionnelles ont été données dans les meilleurs délais possibles.

5.4 Controlling des recommandations et des suggestions

La vérification de la mise en œuvre des recommandations n'est pas explicitement réglée par la législation sur le renseignement. D'entente avec le DDPS et les autorités surveillées, il a été convenu que celles-ci informent le département par écrit de la mise en œuvre desdites recommandations et de l'examen des suggestions formulées, avec copie à l'AS-Rens. Les premiers délais pour la mise en œuvre des recommandations sont arrivés à échéance en 2019. Le processus d'annonce et de vérification interne à l'AS-Rens peut encore être amélioré. À l'heure actuelle, les déclarations portant sur le nombre et, avant tout, sur la qualité des recommandations mises en œuvre sont encore peu représentatives. Alors qu'il est prévu que 40 d'entre elles soient formellement concrétisées en 2019, une annonce de mise en œuvre a eu lieu pour 26 recommandations. Si l'AS-Rens n'accepte pas les mesures de mise en œuvre qui ont été prises, elle peut éventuellement les contrôler dans le cadre d'inspections subséquentes.

6.1 Révision de la LRens

Cette année, le DDPS a été chargé de procéder à de premiers travaux de révision de la LRens. Le 27 août 2019, le SRC a invité des représentants des services fédéraux et cantonaux concernés à une première séance, au cours de laquelle différents groupes de travail ont été formés. L'AS-Rens a participé au groupe de travail « Surveillance » avec trois collaborateurs, aux côtés également d'un représentant de l'organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé (OCI) et d'un représentant du SG DDPS.

Des propositions de modification de l'art. 142, al. 2 et 3, de la loi sur le Parlement (LParl)¹⁷, en lien avec les art. 77 à 79b LRens, ont été transmises au SRC. Le 3 décembre 2019, l'AS Rens a participé à la séance finale de cette phase du projet législatif. Outre des adaptations formelles du processus budgétaire, les éléments principaux portaient sur la fusion entre l'OCI et AS-Rens, ainsi que la création d'une base légale pour les activités internationales de cette dernière.

¹⁷ RS 171.10

6.2 Formation continue du personnel de l'AS-Rens

En 2019, les collaboratrices et collaborateurs de l'AS-Rens ont participé à des colloques, consacrés par exemple à la sécurité de l'information ou à la protection des données, et ont suivi des formations individuelles, en particulier dans le domaine de la gestion des risques.

En parallèle, l'AS-Rens a organisé aussi des formations continues internes sur les thématiques suivantes :

- lutte contre l'espionnage
- MRSA
- techniques et tactiques d'audition
- présentation du système d'information GEVER SRC
- cours de rafraîchissement sur l'aide d'urgence
- protection des données
- présentation du système d'information IASA SRC

Ces cours ont été donnés tant par des spécialistes internes au SRC que par des services externes tels que le Service spécialisé chargé des contrôles de sécurité relatifs aux personnes, rattaché à la Sécurité des informations et des objets, ou le PFPDT. L'AS-Rens en profite pour les remercier du soutien dont elle a bénéficié.

« La transparence est une attitude de base et non un projet. »

Contacts internationaux

Oversight Network Meetings

- La Haye, 24 janvier 2019
- Bruxelles, 7 mars 2019
- Copenhague, 27 juin 2019
- European Intelligence Oversight Conference 2019, La Haye, 12 décembre 2019
- 3ème symposium sur le droit des services de renseignement, Berlin, 7 et 8 novembre 2019

7. Coordination

7.1 Contacts nationaux

La coordination de l'activité de surveillance est une tâche centrale de l'AS-Rens. Cette dernière a donc aussi eu des échanges à ce sujet avec des organes nationaux et d'autres autorités de surveillance en 2019.

Délégation des Commissions de gestion (DélCdG)

La DélCdG a invité l'AS-Rens à des auditions le 23 janvier, le 12 avril et le 23 octobre 2019. Dans ce cadre, l'AS-Rens a notamment fourni des informations à la DélCdG sur les rapports d'inspection des années 2018 et 2019 (18-5 Conduite / rythme des opérations, 19-12 Protection des informateurs au sein du SRC avec intérêt particulier sur les couvertures et les identités d'emprunt) ainsi que sur son premier rapport d'activités.

La DélCdG a invité l'AS-Rens à une conférence le 26 février 2019 à Berne, avec des représentantes et représentants d'organes de surveillance parlementaires issus de 21 cantons. L'AS-Rens a profité de l'occasion pour présenter ses compétences de surveillance des services de renseignement cantonaux.

Organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé (OCI)

Le 4 janvier 2019, une rencontre a eu lieu entre le chef de l'AS-Rens et le président de l'OCI. Leurs échanges ont notamment porté sur les défis futurs liés à la surveillance de l'exploration du réseau câblé. La coordination des activités de surveillance et de contrôle s'effectue bilatéralement à chaque fois que cela est nécessaire.

Tribunal administratif fédéral (TAF)

La Cour I du TAF décide des requêtes du SRC dans le domaine des MRSA et de l'exploration du réseau câblé. L'échange d'expériences avec cette institution est important pour l'AS Rens, même si le tribunal n'est pas soumis à la surveillance de cette dernière. Des échanges d'expériences bilatéraux ont ainsi eu lieu le 30 janvier, ainsi que le 2 octobre 2019.

Demandes de citoyennes et citoyens

En 2019, l'AS-Rens a reçu huit demandes de citoyennes et citoyens. Certaines émanaient d'étudiants et portaient sur les activités de surveillance, tandis que d'autres provenaient de personnes qui se sentaient perturbées ou menacées par de potentielles activités de renseignement. L'AS-Rens peut intégrer les informations reçues dans son activité d'inspection. Elle peut par exemple vérifier si une action décrite peut être attribuée à un service de renseignement et, dans l'affirmative, si le principe de légalité a été préservé. Ainsi, les informations obtenues grâce à l'association «grundrechte.ch» ont été prises en compte et intégrées dans l'inspection 19-15a (GE-VER NDB). L'AS-Rens n'est toutefois pas un organe de recours et n'a par conséquent pas autorité à informer un individu sur des observations le concernant éventuellement. Une requête peut être déposée auprès du PFPDT pour savoir si les éventuelles données concernant un individu sont traitées conformément à la loi et si le report d'une réponse est justifié.

En 2019, la direction de l'AS-Rens a eu des échanges avec les personnes ci-dessous :

- la cheffe du DDPS (19 mars, 29 août) ;
- le secrétaire général du DDPS (6 mai) ;
- le directeur du SRC (12 mars, 11 juin, 4 octobre et 29 novembre) ;
- le chef du RM (12 février, 28 juin et 1er octobre) ;
- le chef du COE (9 janvier) ;
- le PFPDT (16 janvier).

7.2 Contacts internationaux

Les compétences des organes de surveillance des services de renseignement s'arrêtent en règle générale aux frontières nationales, et ce, même si des données et des informations sont échangées entre services de renseignement par-delà les frontières. La collaboration internationale entre les services est quotidienne et particulièrement étroite avec les services partenaires. D'où l'importance des échanges internationaux pour les organes de surveillance également. En échangeant leurs expériences et leurs méthodes d'inspection et en com-

« Etre transparent ne signifie pas partager chaque détail. »

parant leurs résultats et leurs conclusions, les autorités de surveillance peuvent développer une meilleure compréhension mutuelle et améliorer leur travail quotidien.

Oversight Network Meetings à La Haye, à Bruxelles et à Copenhague

La Haye, 24 janvier 2019

Des représentantes et représentants des autorités de surveillance des services de renseignement de Belgique, du Danemark, des Pays-Bas, de Norvège et de Suisse ont discuté à La Haye des possibilités de projets de surveillance communs, concernant notamment l'utilisation des données PNR¹⁸ par les services de renseignement. L'AS-Rens n'a certes pas participé activement au projet, mais elle a pu profiter de ces échanges. Les autorités de surveillance ont par ailleurs discuté des innovations relevant de la surveillance technique et électronique. Concrètement, il s'agissait par exemple de voir comment les systèmes d'information des services de renseignement pouvaient être surveillés de manière efficace.

Bruxelles, 7 mars 2019

Outre les représentantes et représentants susmentionnés présents à la rencontre de La Haye, deux représentants de la surveillance britannique ont rejoint le réseau à Bruxelles. Toutes les délégations étaient unanimes à dire que la collaboration future exigeait une croissance équilibrée et raisonnable des membres du réseau et de la fréquence des rencontres internationales. Outre la composition du réseau, les participantes et participants ont discuté d'une méthode de surveillance dénommée « surveillance systémique ». Cette méthode n'est pas destinée à remplacer d'autres formes de surveillance plus classiques telles que l'examen approfondi.

Elle aurait cependant l'avantage de reposer sur une norme d'inspection internationale restant à créer, ce qui pourrait faciliter la collaboration, tout en pouvant être adaptée au contexte national. Pour certaines parties de ses inspections, l'AS-Rens a déjà utilisé la surveillance systémique, par exemple lors de son inspection 18-10 « Aperçu des mesures du SRC visant à atténuer les risques (y c. inspections des services de renseignement cantonaux) ». Un suivi de cette thématique sera assuré au sein du réseau.

Copenhague, 27 juin 2019

Le réseau a poursuivi ses efforts visant à mettre en place une surveillance systémique et a discuté de normes communes possibles pour ce type de surveillance. S'appuyant sur des exemples concrets, les participantes et participants ont échangé des expériences et des bonnes pratiques, en particulier dans les domaines de l'appréciation du risque, des processus liés à l'infrastructure informatique et à l'infrastructure de données, et des solutions techniques en matière de surveillance. Lors de quatre ateliers, les autorités de surveillance ont discuté des normes communes possibles dans ces domaines. Cette rencontre incluait pour la première fois des autorités de surveillance venant d'Allemagne et de Suède, avec un statut d'observateurs.

European Intelligence Oversight Conference 2019, La Haye, 12 décembre 2019

La conférence européenne de surveillance des services de renseignement était placée sous le signe de la consolidation de la surveillance de la collaboration internationale en matière de renseignement. Les participantes et participants y ont discuté de thèmes tels que les défis futurs pour la surveillance internationale des services de renseignement ou les normes présidant à la surveillance multilatérale.

Autres contacts

Les 7 et 8 novembre 2019 à Berlin, des collaborateurs de l'AS-Rens ont en outre participé au troisième symposium sur le droit des services de renseignement, consacré notamment à l'architecture de sécurité interconnectée.

¹⁸ Les données PNR sont des lots de données portant sur des passagers aériens – et donc des données personnelles – saisies et enregistrées par les compagnies aériennes. Ces lots de données englobent par exemple le nom du passager, son adresse électronique, sa date de naissance, ses données de passeport, ses données de voyage ou ses itinéraires.

8. Regard externe

Un point de vue externe doit aussi systématiquement trouver sa place dans le rapport d'activités. Tombant à point nommé pour le thème de la transparence, Martin Stoll présente son point de vue sur la question.

Stationné à l'écart

Souvent, mes informateurs ne reculaient devant rien. Les rencontres secrètes se déroulaient selon un scénario minutieusement préparé. Sur le trajet vers le lieu convenu, j'étais observé (personne ne devait me suivre). Parfois, des documents étaient déposés dans un casier anonyme. D'autres fois, j'ai dû me promener longtemps dans la forêt ou faire des heures de voiture. Des noms d'emprunt étaient convenus et des canaux de communication fixés. C'était un peu comme dans un film.

Mes informateurs étaient prudents pour de bonnes raisons. Ces collaborateurs des services de renseignement et des services secrets suisses auraient perdu leur travail et leur rente si leurs contacts avec moi avaient été dévoilés.

C'est ainsi que l'affaire sud-africaine du service de renseignement étranger de l'époque a été dévoilée. Dans le dos de la diplomatie helvétique, qui s'engageait pour mettre un terme au régime de l'apartheid, des militaires suisses entretenaient des liens douteux avec des services secrets au Cap. On a ainsi appris qu'un pilote du Comité international de la Croix-Rouge (CICR) avait été recruté comme espion par le service de renseignement suisse en Angola. On a ensuite aussi appris que le même service de renseignement avait subtilisé en 1982 des dossiers d'espionnage en toute illégalité lors de l'occupation de l'ambassade de Pologne à Berne.

Il s'agissait d'incidents politiquement hautement sensibles qui montrent que le service de renseignement autrefois affilié au Département militaire fédéral ne connaissait alors presque aucun tabou.

Plus récemment, on m'a raconté comment un informaticien du Service de renseignement de la Confédération (SRC) avait copié d'énormes quantités d'informations confidentielles et secrètes. Ce n'est qu'à la toute dernière minute, alors que l'homme se sentait victime de mobbing et voulait vendre les données, qu'il a été arrêté grâce à un avertissement d'une grande banque. On m'a raconté que le SRC avait provisoirement mis à pied un collaborateur de longue date. C'était là le début de l'affaire du détective privé zurichois Daniel M., qui devait espionner les autorités financières allemandes sur mandat des services secrets suisses.

Les pannes des services secrets sont du pain béni pour les journalistes

Les auteurs des indiscrétions avaient dans la très grande majorité des cas des motivations honorables. Il s'agissait de personnes qui se faisaient du souci pour le service. Aux yeux des informateurs, quelque chose avait échappé à tout contrôle et personne n'était là pour rectifier le tir.

Aux gros titres ont ensuite systématiquement suivi les enquêtes ainsi que les rapports de la surveillance parlementaire, qui ont remis les processus déviants sur le droit chemin de la nor-



Martin Stoll (né en 1962) travaille depuis 35 ans comme journaliste d'investigation. Comme reporter pour le Tages-Anzeiger, il a plongé dans les années 90 dans le milieu zurichois de la prostitution et y a découvert un lien caché entre les services secrets suisses et l'Afrique du Sud de l'apartheid. Il a aussi lancé le bureau d'enquête de la Sonntagszeitung. De plus, il est fondateur et gérant de la plateforme de transparence loitransparenz.ch, correspondant de la Sonntagszeitung pour l'administration fédérale, formateur dans le domaine des enquêtes et vice-président du collectif de journalistes investigativ.ch.

malité helvétique. Pour les services secrets, qui (à raison) opèrent régulièrement à la limite de la légalité, il s'agit là d'une procédure nécessaire et importante.

De mon point de vue de journaliste, les affaires internes qui étaient parvenues à mes oreilles étaient du pain béni. En Suisse, on a l'indignation facile lorsqu'il est question de services secrets. Si elle inclut un agent, même l'histoire la plus banale suffit à capter intégralement l'attention du lectorat et à lui faire secouer la tête en se demandant ce que les services secrets avaient bien pu avoir fait cette fois-ci.

On pourrait avoir la réprimande facile et prêter aux journalistes de mauvais desseins : égoïsme, volonté de maximiser les ventes du quotidien, sensationnalisme inutile. Bien sûr que nous voulons avoir du succès, aussi auprès de notre public. Mais c'est surtout notre mission et notre passion que de fouiner, d'éclairer les zones d'ombre et de signaler les abus.

La stratégie adoptée actuellement par les services secrets suisses pour gérer ce public critique n'est pourtant pas la bonne. Aujourd'hui, le SRC fait tout pour passer inaperçu. Il se parque sur le bas-côté, observe et semble impuissant lorsqu'il se retrouve sous le feu des projecteurs. Par conséquent, les services secrets devraient urgemment se demander pourquoi ils se retrouvent si rapidement le dos au mur en cas d'incident. Ils devraient chercher à savoir pourquoi même des explications raisonnables n'arrivent pas à calmer les esprits.

Lors de chaque affaire ou scandale, il devient évident que les services secrets suisses, même 30 ans après l'affaire des fiches, n'ont pas réussi à faire en sorte que leur mandant, la population suisse, comprenne leur travail. Le public ne sait pas à quoi servent les services secrets, ce que sont leurs tâches, leur utilité ou leur marge de manœuvre.

La politique de transparence à courte vue menée par le SRC ces dernières années n'y est certainement pas étrangère. La promesse du Conseiller fédéral Adolf Ogi, qui avait annoncé une « glasnost au Pentagone » après la grotesque affaire entourant le comptable des services secrets Dino Bellasi en 2001, est jusqu'ici restée un witz politique.

Une timidité exagérée face au public nuit à la réputation

Les chiffres relatifs à la mise en œuvre de la loi sur la transparence (LTrans) montrent clairement que l'importance de la transparence est secondaire pour les services secrets suisses. Cette loi permet aux citoyennes et citoyens du pays – et donc également aux journalistes – de consulter des dossiers de l'administration. Son objectif est de renforcer la compréhension de la population pour le travail de l'administration.

Le SRC est également soumis à cette loi. Entre 2012 et 2018, 62 journalistes, organisations non gouvernementales et citoyennes et citoyens ont adressé des demandes d'accès au SRC. Ce dernier n'a octroyé un accès intégral à un document que dans huit cas. Le service juridique de cette autorité en a par ailleurs rejeté intégralement 33, ce qui constitue, à n'en pas douter, un bilan extrêmement maigre du point de vue citoyen et journalistique.

Afin de comprendre la politique de transparence du SRC, j'ai exigé en 2014 de consulter toutes les demandes d'accès adressées au SRC au cours des trois dernières années, en m'appuyant sur la LTrans. Ce qui m'a réjoui, c'est que j'ai reçu l'ensemble des documents anonymisés. Ce qui m'a moins réjoui, c'est que la plupart des seize demandes d'accès ont été rejetées avec la même justification standardisée, à savoir que la sûreté intérieure ou extérieure de la Suisse serait menacée en cas de publication.

Lorsque les services secrets restent dans l'ombre de manière aussi systématique et ne laissent rien transparaître de leur travail, ils prêtent leur réputation. Un exemple tiré de la série de demandes que j'ai pu consulter et qui concernait un thème que je connaissais bien l'illustre à merveille. 23 ans après la chute du Mur de Berlin, un requérant a demandé l'accès au « Dossier Walter B. ». Pendant la guerre froide, Walter B., alias « Max », était l'un des principaux espions au service de la Suisse. L'ancien chauffeur à l'ambassade de la RDA a été recruté par le contre-espionnage après avoir été attrapé lors d'un vol à l'étalage dans un grand magasin bernois. Durant les années qui ont suivi, Walter B. a permis à la Suisse d'avoir un aperçu approfondi des opérations des services secrets de l'est. Et bien que « Max » m'ait conté son histoire lors d'entretiens longs de plusieurs heures, bien que des dossiers et documents filmés de la sûreté d'État de la RDA soient accessibles à Berlin (« Max » a plus tard été arrêté à Berlin-Est puis condamné), le SRC n'a pas autorisé le requérant à accéder au dossier. Il a ainsi raté une occasion de participer à la divulgation d'un morceau fascinant d'histoire et de légitimer de la sorte le travail risqué des services secrets.

On a par ailleurs eu un nouvel exemple de la réticence fondamentale du SRC à faire preuve de transparence lorsque ce dernier a fait exclure du principe de transparence tout le pan opérationnel de la nouvelle loi sur le renseignement. Un acte totalement inutile (les secrets peuvent aussi être efficacement protégés avec la LTrans), et une nouvelle occasion manquée : par principe, le SRC ne devrait pas être secret mais aussi transparent que possible. Cela lui permettrait d'expliquer son travail de manière crédible.

Si ce n'est pas le cas, les services secrets continueront à être mesurés à la seule aune de leurs défaillances et échecs. La surclassification cultivée aujourd'hui va tôt ou tard se transformer à nouveau en boomerang, car une chose est sûre : il y aura une prochaine affaire liée aux services secrets.

9. Chiffres-clés au 31 décembre 2019



Collaborateurs

1.1.2019 9
31.12.2019 10
Départ 0



Inspections

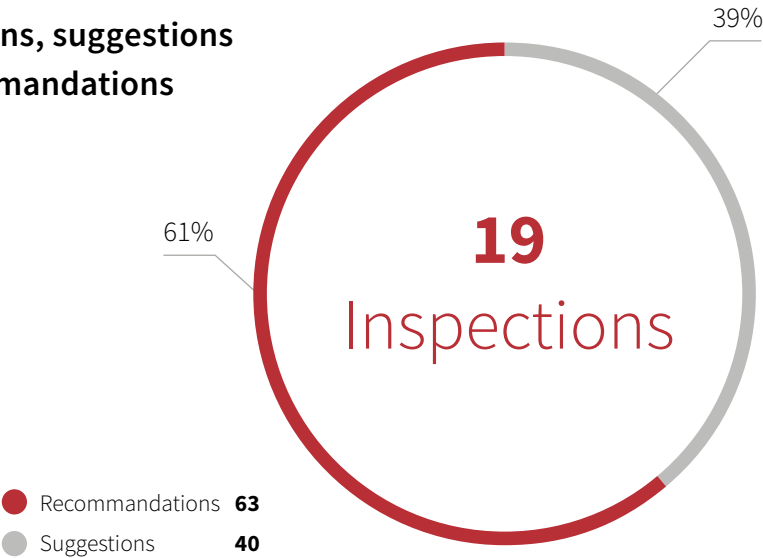
Inspections planifiées 21
Inspections non annoncées 0
Inspections effectuées 19



Nombre d'entretiens
réalisés en 2019 119

Effectif budgété
10 places

Inspections, suggestions et recommandations



10. Annexe

10.1 Plan des inspections 2019

No	Titre	Organe contrôlé
19-1	Stratégie de défense contre l'espionnage	SRC
19-2	Gestion de l'information en matière de renseignement entre le senseur « Attachés de défense » (AD) et le SRC	SRC
19-3	Inspection SRCant GE	SRCant GE
19-4	Inspection SRCant JU	SRCant JU
19-5	Inspection SRCant GR	SRCant GR
19-6	Inspection SRCant SH	SRCant SH
19-7	Inspection SRCant BE	SRCant BE
19-8	Adéquation et efficacité des MRSA	SRC
19-9	Mise en œuvre des MRSA	SRC
19-10	Opérations	SRC
19-11	Informateurs (HUMINT)	SRC
19-12	Protection des informateurs au sein du SRC avec un intérêt particulier sur les couvertures et les identités d'emprunt.	SRC
19-13	Processus de recrutement, d'encadrement et de sortie	SRM, COE
19-14	Utilisation sûre de la vidéoconférence	SRC
19-15	Fonctionnement, contenu et utilisation des systèmes d'information GEVER SRC, BURAUT, SiLAN (analyse temporaire)	SRC
19-16	Classification de l'information	SRC, SRM, COE
19-17	Paysage des systèmes d'information SRM	SRM
19-18	Paysage des systèmes d'information COE	COE
19-19	Systèmes d'analyse des données du COE	COE
19-20	Communication de données personnelles à des autorités étrangères (art. 61 LRens)	SRC
19-21	Accès à des systèmes d'information de tiers (Confédération, cantons, services étrangers, poursuite pénale)	SRC
19-22	Contrôle des recommandations	SRC, SRA, COE

10.2 Liste des abréviations

AD	Attaché de défense	RI D	Relations internationales de la Défense
al.	alinéa	RM	Renseignement militaire
Art.	article	RS	Recueil systématique du droit fédéral
AS-Rens	Autorité de surveillance indépendante des activités de renseignement	SEM	Secrétariat d'État aux migrations
BAC	Base d'aide au commandement	SG	Secrétariat général
BE	Berne	SGSI	Système de gestion de la sécurité des informations
CICR	Comité international de la Croix-Rouge	SH	Schaffhouse
COE	Centre des opérations électroniques	SiLAN	Base de données du SRC
CSP	Contrôle de sécurité relatif aux personnes	SRC	Service de renseignement de la Confédération
DDPS	Département fédéral de la défense, de la protection de la population et des sports	SRCant	Service de renseignement cantonal
DéICdG	Délégation des Commissions de gestion	Système de fichiers	Dépôt d'informations du SRC
DFAE	Département fédéral des affaires étrangères	BURAUT	
DFJP	Département fédéral de justice et police	TAF	Tribunal administratif fédéral
GE	Genève	WEF	World Economic Forum (Forum économique mondial) à Davos
GEVER	Gestion des affaires : notion générique désignant la gestion électronique des dossiers au sein de l'administration fédérale		
GR	Grisons		
HUMINT	Human Intelligence, recherche de renseignements par des informateurs		
JU	Jura		
LParl	Loi sur l'Assemblée fédérale (RS 171.10)		
LRens	Loi fédérale sur le renseignement (RS 121)		
LTrans	Loi sur la transparence (RS 152.3)		
MRSA	Mesures de recherche soumises à autorisation		
OCI	Organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé		
ORens	Ordonnance sur le renseignement (RS 121.1)		
PPPDT	Préposé fédéral à la protection des données et à la transparence		
PNR	Passenger Name Record		
RDA	République démocratique allemande		



**Autorité de surveillance indépendante
des activités de renseignement**

Maulbeerstrasse 9, 3003 Berne
Téléphone +41 58 464 20 75
www.ab-nd.admin.ch