



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Autorité de surveillance indépendante
des activités de renseignement

Rapport d'activités 2021

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



AS-Rens

SRC

RM

COE

SRCant

1. Résumé

Trois événements ont marqué les activités de l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) en 2021 : la résiliation des rapports de travail avec le directeur du Service de renseignement de la Confédération (SRC), l'augmentation notable du nombre de signalements et d'informations concernant des collaboratrices et des collaborateurs mécontents au SRC et les changements de personnel au sein de l'AS-Rens elle-même. La direction de l'AS-Rens est également concernée par ces changements, Thomas Fritschi quittant l'AS-Rens après presque cinq ans d'activité. Malgré ces développements, l'AS-Rens a pleinement rempli sa mission principale, à savoir la surveillance des activités de renseignement.

En 2021, l'AS-Rens a procédé à des inspections dans les domaines suivants :

- Stratégie et planification – 1 inspection
- Organisation – 3 inspections
- Collaboration – 8 inspections
- Recherche – 4 inspections
- Traitement des données et archivage – 2 inspections

Au total, 18 inspections ont été effectuées et achevées. Par rapport aux années précédentes, le nombre de recommandations formulées a nettement diminué. Cette évolution peut s'expliquer, d'une part, par les améliorations déjà apportées grâce à la mise en œuvre des recommandations formulées par l'AS-Rens au cours des dernières années. D'autre part, les contrôles faits par l'AS-Rens vont de plus en plus en profondeur, alors que lors des premières années, ses inspections lui permettaient surtout d'acquiescer une vue d'ensemble des différentes activités de renseignement. La formulation de recommandations adaptées à chaque niveau devient ainsi plus exigeante.

Sur la base de son évaluation des risques, l'AS-Rens a concentré ses activités sur le SRC. Par conséquent, elle a procédé au total à 17 inspections au sein du SRC.

L'inspection de la collaboration du SRC avec les services de renseignement cantonaux (SRCant), de la protection des in-

frastructures critiques au moyen de la cyberdéfense et de la recherche d'informations par des informateurs (HUMINT) a engagé une importante partie des ressources en personnel de l'AS-Rens. Dans le domaine HUMINT, elle a procédé à une inspection extraordinaire de grande ampleur qui ne figurait pas sur le plan des inspections 2021. Le SRC s'est penché sur les possibilités d'amélioration constatées. La longue période transitoire due au changement de direction et les collaboratrices et les collaborateurs manifestant leur mécontentement pèsent sur le service. Le SRC a obtenu une bonne note concernant sa collaboration avec les services de renseignement cantonaux et a ainsi contribué considérablement à la sécurité intérieure de la Suisse. Dans le domaine cyber, le SRC a examiné sa pratique en matière de recherche d'informations. L'AS-Rens s'est informée régulièrement et en détail à ce sujet afin de créer des bases de décision pour une éventuelle inspection.

L'AS-Rens a également procédé à une inspection au Centre des opérations électroniques (COE) dans le domaine cyberdéfense. L'inspection a montré que les compétences pour la protection des infrastructures critiques au sein du SRC et du COE sont développées et que la collaboration fonctionne. De plus, l'AS-Rens a participé en tant qu'observatrice aux réunions de l'organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé (OCI).

Durant l'année sous revue, le Renseignement militaire (RM) a été contrôlé par l'AS-Rens dans le domaine de la protection des données. Même si le RM traite des données personnelles, ces dernières ne sont pas au centre de son attention. Conformément au mandat légal, la recherche d'informations est principalement axée sur l'étranger. L'AS-Rens n'a pas relevé d'éléments lui permettant de douter de la légalité du traitement des données personnelles par le RM.

Une réunion a en outre permis d'entretenir et de consolider les échanges entre l'AS-Rens et les organes de surveillance cantonaux.

Le rapport d'activités 2021 était en consultation du 14 au 27 février 2022 auprès du DDPS et de la Délégation des Commissions de gestion des Chambres fédérales (DéICdG). Dans la

mesure où les réponses faisaient état d'erreurs formelles ou matérielles dans le rapport d'activités ou d'intérêts dignes de protection qui s'opposaient à la publication de certaines parties, celles-ci ont été prises en compte.

Bilan

L'AS-Rens a formulé 18 recommandations dans le cadre de 18 inspections. La mise en œuvre de ces recommandations permet de minimiser les risques des activités de renseignement et d'en accroître l'efficacité.

Durant l'année sous revue, les incertitudes en matière de personnel au sein du SRC ont interféré avec les activités de renseignement du service. Des premiers efforts d'amélioration ont été entrepris, mais ceux-ci ne devraient pas suffire à apaiser et clarifier durablement la situation. Les structures et processus existants au sein du service doivent être remis en question et éventuellement adaptés. Cela permettrait de créer une stabilité à plus long terme, ce qui minimiserait les risques. Pour y parvenir, le SRC est également tributaire du soutien du département. La diminution du nombre de recommandations indique que les risques inhérents aux activités de renseignement ont pu être exclus ou du moins réduits.

En fonction de l'évaluation des risques sur laquelle reposent les inspections, les deux organisations militaires actives dans le domaine du renseignement, le RM et le COE, ont été moins contrôlées. Aucune recommandation n'a dû être formulée pour ces organisations. Il faudra toutefois observer attentivement comment le COE s'intégrera au sein du futur commandement Cyber.



2. Table des matières

1 Résumé	2
2 Table des matières	4
3 Note personnelle	5
4 Systèmes d'information	6
4.1 Systèmes d'information contrôlés jusqu'à présent par l'AS-Rens	7
4.2 D'après l'AS-Rens, quels sont les défis et les chances relatifs aux systèmes d'information contrôlés?	9
4.3 Développements futurs	11
4.4 Nouvelle gestion des données: répercussions sur la LRens	11
5 Activités de surveillance	12
5.1 Plan des inspections	12
5.2 Inspections 2021	12
5.3 Acceptation	26
5.4 Controlling des recommandations	26
6 Regard interne	28
6.1 Personnel et formations continues	28
6.2 Révision de la LRens	28
6.3 Loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans)	28
6.4 Visites	28
6.5 Jurisprudence	28
7 Coordination	29
7.1 Contacts nationaux	29
7.2 Contacts internationaux	31
8 Regard externe	33
9 Chiffres clés au 31 décembre 2021	36
10 Annexe	37
10.1 Plan des inspections 2021	37
10.2 Abréviations	38

3. Note personnelle

« L'AS-Rens garantit des « checks and balances » au domaine du renseignement. »

Thomas Fritschi



Thomas Fritschi, chef de l'AS-Rens

La pandémie de COVID-19 et la tendance à la division sociale qui l'accompagne, la politique de puissance de certains États ou notre vulnérabilité aux cyberattaques nous font prendre conscience de la fragilité de notre sécurité et de l'importance de la prévention et de l'appréciation de la situation pour les décideurs politiques. Par ces temps toujours plus incertains et difficiles, le besoin d'informations et de faits sûrs est d'autant plus grand. Les services de renseignement ont été, et sont toujours sollicités et, par conséquent, leur surveillance également.

Au cours de l'année sous revue, nous avons continué à exercer notre activité de surveillance en nous basant sur une évaluation des risques et en nous adaptant aux évolutions actuelles. Le nombre de nos recommandations a notablement diminué. D'une part, cela est dû au fait que des améliorations ont déjà été apportées au cours des années précédentes. D'autre part, nous nous sommes davantage concentrés sur les défis fondamentaux qui résultent du travail de renseignement dans un État de droit démocratique, et avons contrôlé plus en profondeur, ce qui entraîne des exigences plus élevées pour la formulation de recommandations adaptées aux échelons hiérarchiques. Une inspection dans le domaine de la gestion des informateurs ainsi que des clarifications approfondies sur des faits survenus dans le domaine cyber du SRC ont été particulièrement exigeantes.

Notre attention s'est également portée sur l'organisation du SRC, qui a été mise à l'épreuve par le départ inattendu de son directeur. Mi-2021, des collaboratrices et des collaborateurs mécontents ont alerté la presse. Pour ces raisons, un changement de culture et l'examen des structures et des processus du SRC sont indiqués. La décision quant à la mise en œuvre de telles mesures ne relève toutefois pas de l'autorité de surveillance. On peut supposer que c'est un mandat qui incombe plutôt au directeur désigné du SRC.

Dans le présent rapport d'activités, nous souhaitons, en plus de rendre compte de notre activité de surveillance et des développements internes au SRC, nous consacrer de manière approfondie au thème des systèmes d'information et, par extension, à la protection des données. En la personne du préposé fédéral à la protection des données et à la transparence (PFPDT), Adrian Lobsiger, nous avons pu compter sur un spécialiste reconnu pour apporter un regard externe.

C'est la dernière fois que je signe un rapport d'activités de l'AS-Rens et je suis reconnaissant des presque cinq années de travail constructif passées dans un environnement hautement sensible et exigeant. L'AS-Rens garantit des « checks and balances » en lien avec les compétences élargies du SRC en 2017 et un service en constante croissance. Elle est conçue et développée de manière à pouvoir répondre à cette exigence. Son indépendance est respectée et prise en compte. L'échange et la coordination avec les autres organes de surveillance à l'échelon de la Confédération et des cantons sont établis. Il reste à souhaiter qu'à l'avenir un dialogue puisse enfin avoir lieu également avec la haute surveillance parlementaire.

L'existence de l'AS-Rens est juste et importante. Elle peut donner confiance dans les activités de renseignement. Je vous remercie pour la confiance que vous m'avez accordée ces dernières années et vous souhaite une bonne lecture.

Thomas Fritschi, chef de l'AS-Rens

4. Systèmes d'information

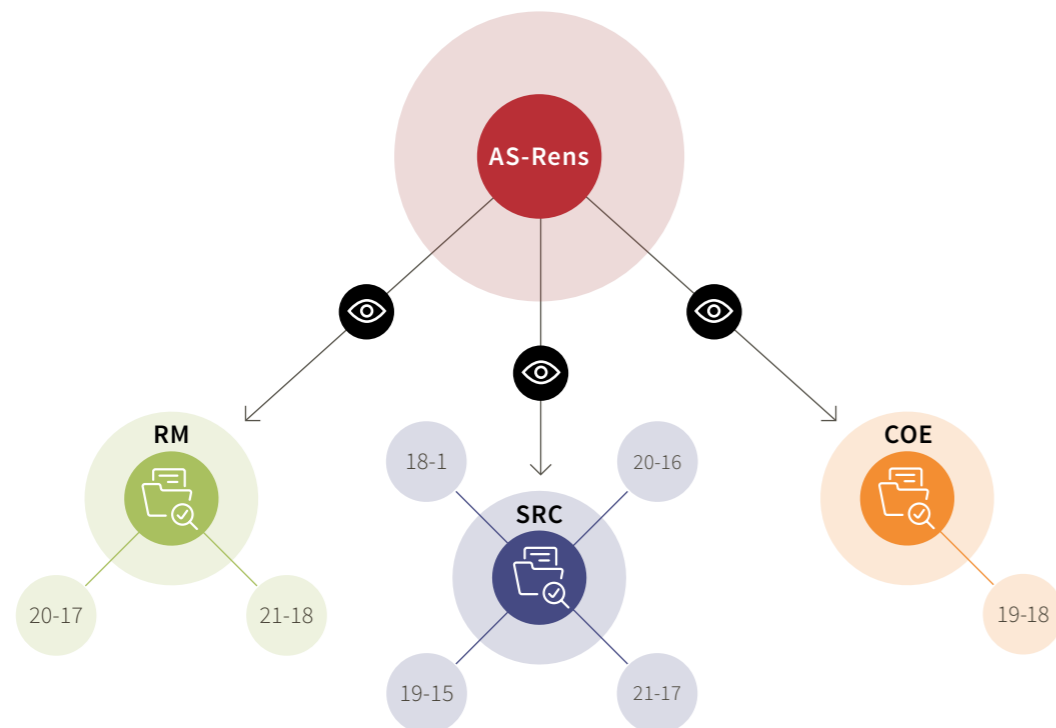
« Chaque année, l'AS-Rens contrôle un certain nombre de traitements de données ou de systèmes d'information. »

La recherche d'informations relatives aux tâches prescrites par la loi est l'une des tâches principales des services de renseignement suisses. Ces informations doivent être mises à la disposition des collaboratrices et des collaborateurs responsables le plus tôt possible afin de leur permettre d'accomplir leurs tâches. Les informations sont intégrées aux produits des services de renseignement, qui sont mis à la disposition des autorités de sécurité nationales et étrangères ainsi que des décideurs militaires et politiques. L'objectif de la recherche d'informations est l'appréciation de la situation actuelle en matière de menaces afin de prévenir les dangers nationaux et internationaux, à l'attention des décideurs politiques.

Les informations qui ne sont plus nécessaires à l'accomplissement des tâches des services de renseignement et dont le délai de conservation a expiré sont proposées aux Archives

fédérales. Si les Archives fédérales estiment qu'elles n'ont pas de valeur archivistique, elles doivent être détruites.

Les services de renseignement exploitent un ensemble de systèmes d'information dans lesquels les informations ou les données sont traitées tout au long de leur cycle de vie, de leur collecte à leur suppression. Les lois applicables contiennent un certain nombre de prescriptions relatives à la gestion des données. Ce domaine étant important pour les services de renseignement, l'AS-Rens a prévu un domaine de contrôle spécifique dans son plan des inspections: le traitement des données et l'archivage. Chaque année, l'AS-Rens contrôle un certain nombre de traitements de données ou de systèmes d'information. Étant donné leur importance, le présent rapport d'activités se concentre sur les systèmes d'information.



4.1 Systèmes d'information contrôlés jusqu'à présent par l'AS-Rens

Au SRC, l'AS-Rens a déjà examiné les systèmes d'information suivants:

Inspection	Objectif	Année/indication de la source
18-1 Aperçu des données du SRC et du contenu du système de stockage	La loi fédérale sur le renseignement (loi sur le renseignement, LRens) ¹ mentionne à l'art. 47 les systèmes d'information exploités par le SRC. Les systèmes d'information sont réglementés une nouvelle fois au niveau de l'ordonnance y afférente. ² Cette inspection a permis à l'AS-Rens d'obtenir une vue d'ensemble de tous les systèmes d'information du SRC. Elle a servi de point de départ à d'autres inspections. Conformément à la loi, le système de stockage peut contenir des données qui ne peuvent être attribuées à aucun autre système d'information. C'est pourquoi l'AS-Rens a examiné le contenu de ce système afin de déterminer la nature des données qui y sont traitées.	2018 (Rapport d'activités 2018, page 13)
19-15 Fonctionnement, contenu et utilisation des systèmes d'information GEVER SRC ³ , BURAUT ⁴ , SiLAN ⁵ (analyse temporaire)	Le SRC a introduit en 2012 un système de gestion des affaires. L'ensemble du personnel du SRC a accès à ce système. Des données administratives et de renseignement y sont traitées. Considérant les données traitées et le grand nombre de personnes autorisées à y accéder, l'AS-Rens a choisi ce système pour une première inspection approfondie d'un système d'information.	2019 (Rapport d'activités 2019, pages 23 ss.)
20-16 Exploitation, contenu et utilisation des systèmes d'information IASA ⁶	IASA contient les trois systèmes d'information de base en matière de renseignement et constitue l'instrument de travail central du SRC, c'est pourquoi ce système a été examiné par l'AS-Rens.	2020 (Rapport d'activités 2020, page 23)

¹ RS 121

² Ordonnance sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC; RS 121.2)

³ Système de gestion des affaires du SRC

⁴ Stockage des données du SRC

⁵ Réseau sécurisé du SRC

⁶ Système d'analyse intégrale du SRC

« Les bases légales déterminantes pour le SRC concernant l'exploitation des systèmes d'information sont élaborées de manière plus détaillée et transparente que celles pour le RM et le COE. »

Inspection	Objectif	Année/indication de la source
21-17 Système d'information du SRC sélectionné (Quattro P)	Un grand nombre de déplacements de personnes étrangères sont enregistrés et traités dans ce système d'information. Le nombre élevé de données personnelles traitées dans ce système et le fait que les données Quattro P soient utilisées pour le système de reconnaissance faciale du SRC ont incité l'AS-Rens à examiner ce système.	2021 (Rapport d'activités 2021, pages 22 ss.)

Au RM, l'AS-Rens a examiné les systèmes d'information suivants:

Inspection	Objectif	Année/indication de la source
20-17 Systèmes d'information du RM (gestion des autorisations)	Les résultats de l'inspection ont permis à l'AS-Rens de comprendre et de planifier d'autres inspections.	2020 (n'a pas été traitée spécifiquement dans le rapport d'activités, résumé disponible sur le site Internet de l'AS-Rens)
21-18 Protection des données au sein du RM	Le RM traite des données personnelles, même si ce n'est pas l'objectif principal de ses activités. Pour cette raison, l'AS-Rens a examiné les aspects de protection des données de son activité dans certains systèmes d'information.	2021 (Rapport d'activités 2021, pages 25 ss.)

Au COE, l'AS-Rens a examiné les systèmes d'information suivants:

Inspection	Objectif	Année/indication de la source
19-18 Paysage des systèmes d'information du COE	Cette inspection a permis à l'AS-Rens d'avoir une vue d'ensemble et a servi de point de départ pour d'autres inspections. Il n'existe pas de base légale spécifique régissant les systèmes d'information du COE. Les bases se trouvent dans différentes lois et ordonnances.	2019 (Rapport d'activités 2019, page 27)

Outre les inspections spécifiques dédiées aux systèmes d'information, l'AS-Rens a réalisé d'autres inspections dans le domaine du traitement des données et de l'archivage. Depuis le début de ses activités de surveillance, cela représente neuf inspections supplémentaires. Autrement dit, depuis le début de ses activités d'inspection et au cours de seize inspections, l'AS-Rens s'est principalement occupée des systèmes d'information des services de renseignement et du traitement des données dans ces systèmes. Les conclusions tirées de ces activités d'inspection sont présentées ci-après.

4.2 D'après l'AS-Rens, quels sont les défis et les chances relatifs aux systèmes d'information contrôlés?

4.2.1 Bases légales pour les systèmes d'information en matière de renseignement

Les bases légales pour les systèmes d'information du SRC, du RM et du COE sont élaborées de manière différente. Les bases légales déterminantes pour le SRC concernant l'exploitation des systèmes d'information sont élaborées de manière plus détaillée et transparente que celles pour le RM et le COE. Ces dispositions légales plus claires facilitent l'inspection par l'AS-Rens de la légalité des systèmes d'information exploités par le SRC. L'AS-Rens s'engage donc à ce que les bases légales soient à l'avenir élaborées de manière plus claire et plus différenciée, y compris pour le RM et le COE.

4.2.2 Accès de l'AS-Rens aux systèmes d'information en matière de renseignement

Les directrices et directeurs d'inspections de l'AS-Rens reçoivent uniquement du SRC un accès direct et limité dans le temps aux systèmes d'information à examiner. En outre, ils ont un accès permanent au système de gestion des affaires du

SRC. Cela facilite les activités d'inspection, car la documentation nécessaire peut être obtenue de manière autonome par l'AS-Rens. Ce processus est plus difficile au RM et au COE. Pour ces deux organisations, l'AS-Rens doit se faire présenter les systèmes ou organiser un accès sur place, ce qui complique par exemple le traitement autonome d'échantillons dans ces systèmes d'information.

4.2.3 Destinataires et mise en œuvre des recommandations

Le COE et le RM sont des unités organisationnelles relativement petites au sein de l'armée. C'est pourquoi leur marge de manœuvre pour la conception spécifique de systèmes d'information selon leurs propres besoins est limitée. Pour l'AS-Rens, cela comporte des défis dans la formulation de recommandations réalisables, car ces dernières ne peuvent concerner que les services de renseignement eux-mêmes et non d'autres parties de l'armée. Or, dans ce domaine, les éventuelles recommandations ne concernent pratiquement jamais que le RM ou le COE, mais touchent souvent l'ensemble de l'armée.

4.2.4 Priorités de l'AS-Rens lors de l'inspection des systèmes d'information

Gestion des accès et suppression des données – systèmes d'information du SRC

Lors des inspections des systèmes d'information du SRC, l'AS-Rens attache une importance particulière au respect des délais de conservation des données et à une gestion des accès adéquate et conforme au droit. Le SRC a plus que dix délais de conservation différents pour les données de ses systèmes d'information, allant de six mois à 45 ans. Le respect de ces délais légaux est garanti principalement par un programme de suppression automatique. L'AS-Rens contrôle la suppression au moyen d'échantillonnages dans les systèmes d'information.

« Les nouvelles technologies ne présentent pas seulement des risques pour la sécurité de la Suisse, elles peuvent aussi avoir une influence positive sur le travail des services de renseignement. »

La gestion des accès représente d'importants défis pour le SRC. Pour des raisons de protection des informations et des données, les collaboratrices et les collaborateurs ne peuvent avoir accès qu'aux données nécessaires pour l'accomplissement de leur travail. Après des changements internes, mais aussi lors de l'arrivée ou du départ de membres du personnel, les autorisations doivent à chaque fois être adaptées en temps réel. Pour ce faire, le SRC a instauré des processus et l'AS-Rens contrôle les autorisations d'accès au moyen d'échantillonnages dans les systèmes d'information. En outre, elle peut demander à voir les possibilités d'accès aux systèmes d'information sur les postes de travail individuels des collaboratrices et des collaborateurs.

Retard lors du traitement d'informations

Pour les services de renseignement, il est important que les informations collectées ou reçues soient saisies le plus rapidement possible dans les systèmes d'information prévus à cet effet. Pour des raisons de protection des informations, les données collectées sont parfois d'abord stockées dans des dossiers temporaires particulièrement protégés. Ce n'est qu'ensuite qu'elles sont transférées dans les systèmes d'information auxquels les collaboratrices et les collaborateurs ont accès pour évaluer les informations et les exploiter dans des produits. En outre, elles doivent parfois être anonymisées avant d'être enregistrées dans un système d'information. Pour ces raisons, l'AS-Rens est particulièrement attentive à l'inspection de ces processus.

4.3 Développements futurs

Les services de renseignement doivent pouvoir anticiper les changements sociaux et technologiques qui s'avèrent négatifs pour la sécurité de la Suisse. À cet égard, les nouvelles technologies ne présentent pas seulement des risques pour la sécurité de la Suisse, elles peuvent aussi avoir une influence positive sur le travail des services de renseignement. Ainsi, un moteur de recherche inter-systèmes du SRC a grandement facilité le travail des collaboratrices et des collaborateurs depuis son introduction il y a six ans.

Les trois services suivent de près les développements technologiques et les utilisent pour leurs activités de renseignement. Désormais, un système de reconnaissance faciale doit permettre au SRC d'afficher des profils d'images personnelles enregistrées dans ses systèmes (nous l'évoquons en page 24 et suivantes). De son côté, le RM encourage de plus en plus l'analyse des images satellites. Et le COE se penche sur la question de savoir comment la surveillance des communications radio qui diminue à cause de nouveaux moyens de communication peut être compensée par d'autres capteurs techniques.

4.4 Nouvelle gestion des données: répercussions sur la LRens

Les lois qui traitent de la conservation des données utilisent le plus souvent le terme de « système d'information ». C'est aussi le cas de la LRens. L'art. 47 LRens énumère les différents systèmes d'information exploités par le SRC. Le message relatif à la loi précise que le SRC doit saisir les informations collectées ou qui lui ont été communiquées dans des systèmes d'information intégrés en fonction de la thématique, de la source et de la sensibilité des données.⁷

Le lien établi au niveau législatif entre la notion de « système d'information » et les buts poursuivis par le traitement des données ne correspondent peut-être plus aux concepts modernes de gestion des données. C'est pourquoi la nouvelle loi sur la protection des données renonce à la notion de « fichier ». La raison invoquée est que, grâce aux nouvelles technologies, les données peuvent être utilisées comme un fichier, même si elles ne sont pas enregistrées de manière centralisée.⁸

Le projet de révision de la LRens prévoit d'adapter les dispositions légales relatives aux systèmes d'information du SRC. Le terme « information » doit être remplacé par celui de « données ». Les données doivent pouvoir être catégorisées conformément aux exigences légales. Le contenu de ces catégories doit correspondre à peu près à celui des systèmes d'information actuels décrits dans la LRens.

⁷ FF 2014 2106

⁸ FF 2017 6643

5. Activités de surveillance

Comme l'année dernière, l'AS-Rens ne rend pas non plus compte, dans le présent rapport d'activités, de chaque inspection réalisée. En fonction du sujet principal traité dans le présent rapport d'activités, certaines inspections sont développées, tandis que d'autres sont seulement mentionnées. Cependant, un résumé de chaque inspection est publié sur le site Internet de l'AS-Rens⁹.

5.1 Plan des inspections

L'AS-Rens établit chaque année un plan des inspections axé sur les risques¹⁰. Il contient les domaines d'inspections suivants :

- Stratégie et planification
- Organisation
- Collaboration
- Recherche
- Ressources
- Traitement des données et archivage

Au total, l'AS-Rens a planifié 18 inspections pour l'année 2021. De plus, elle a mis en œuvre l'inspection « 20-3 Compétences et responsabilités respectives du SRC A¹¹ et du RM », prévue en 2020, ainsi qu'une inspection extraordinaire dans le domaine HUMINT. L'AS-Rens a totalement renoncé à réaliser les inspections « 20-1 Changement (gestion du changement) » et « 21-3 Sécurité au sein du SRC », d'une part, en raison d'un manque temporaire de ressources en personnel, et d'autre part parce que, entre le moment de la planification et celui de la réalisation de l'inspection, les conditions réelles ont tellement changé que la mise en œuvre de ces inspections n'était plus pertinente. Certains aspects de ces inspections prévues ont déjà été pris en compte dans d'autres inspections ou le seront dans des inspections à venir. La mise en œuvre de l'inspection « 21-16 Services de télécommunication » a débuté en 2022.

Sur la base d'événements actuels et de certains développements, l'AS-Rens a procédé à court terme à des clarifications individuelles dans trois cas au cours de l'année sous revue, en vue d'une éventuelle inspection. Les connaissances ainsi acquises ont été en partie intégrées dans des inspections en cours ou prévues.

5.2 Inspections 2021

5.2.1 Stratégie et planification

Dans le domaine « Stratégie et planification », sont examinés des sujets qui concernent la planification stratégique à court, moyen et long terme des services de renseignement suisses ainsi que leurs objectifs. L'inspection ci-dessous était planifiée pour ce domaine en 2021:

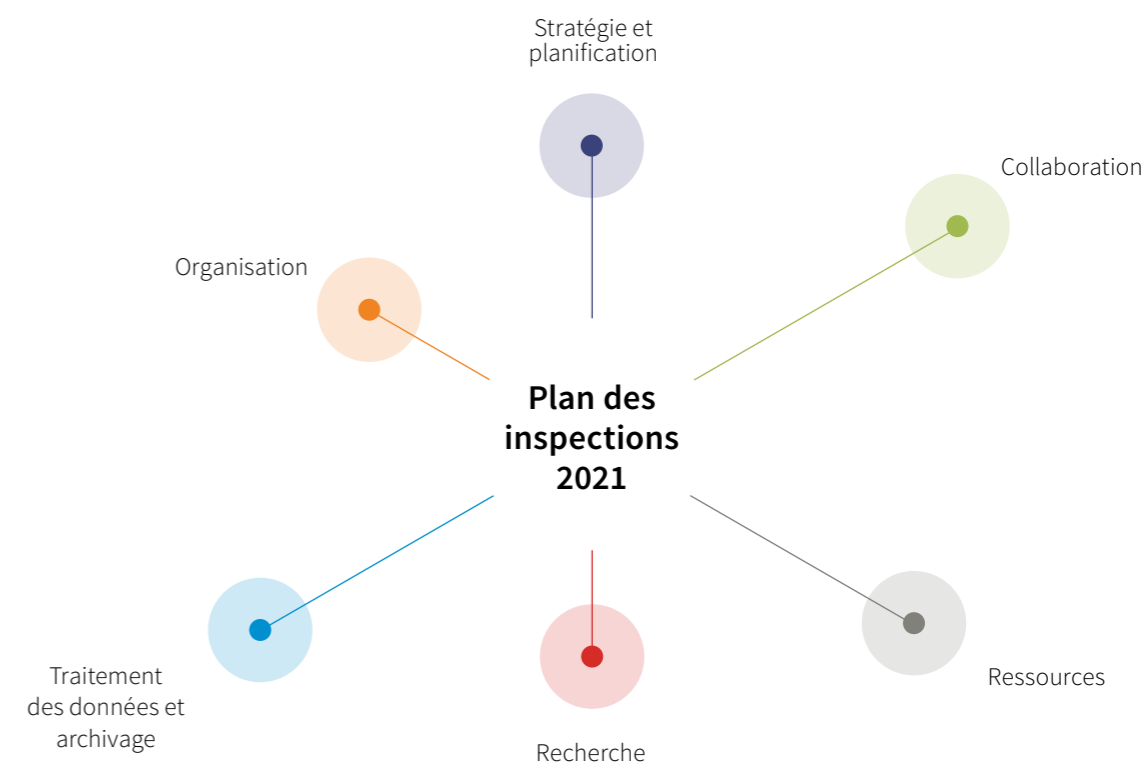
- **21-1 Engagement de collaboratrices et de collaborateurs du SRC dans les représentations suisses à l'étranger (SRC)**

Cette inspection faisait suite à l'inspection « 19-2 Gestion de l'information en matière de renseignement entre le senseur « Attachés de défense » (AD) et le SRC » et visait notamment à contrôler la mise en œuvre de la recommandation. C'est pourquoi l'inspection 21-1 est expliquée au point 5.4 « Controlling des recommandations ».

5.2.2 Organisation

Dans le domaine « Organisation », l'AS-Rens examine dans quelle mesure la structure et les processus des services leur permettent de remplir leur mandat légal conformément au droit, de façon adéquate et efficace.

En 2021, l'AS-Rens a réalisé l'inspection « 20-3 Compétences et responsabilités respectives du SRC A et du RM » qui n'avait pas pu l'être en 2020. Cette inspection est expliquée dans le présent rapport d'activités. En outre, selon le plan des inspections 2021, les inspections ci-dessous étaient prévues:



- **21-2 Protection des infrastructures critiques / cyberdéfense (SRC/COE)**
- 21-3 Sécurité au sein du SRC (SRC)
- **21-4 Extrémisme violent de droite (SRC)**

L'inspection « 21-3 Sécurité au sein du SRC » n'a pas été effectuée.

20-3 Compétences et responsabilités respectives du SRC A et du RM (SRC/RM)

L'inspection a principalement porté sur la question de savoir si les produits du SRC et du RM étaient suffisamment différenciés les uns des autres. En outre, il a été examiné si, là où ils se recoupent, les potentiels de synergie, par exemple l'échange mutuel du savoir-faire professionnel, étaient suffisamment exploités. L'inspection était déjà prévue en 2020 mais elle a été reportée en raison de réorganisations dans la division Analyse du SRC. Elle a été relancée en septembre 2021. En tenant compte des mandats de base et de la convention de collaboration entre le SRC et le RM, l'AS-Rens a procédé à de vastes analyses des produits et des formes de collaboration des services inspectés. Il a été constaté qu'il n'y a que peu de thèmes pour lesquels un chevauchement des domaines d'intérêt est possible dans les activités d'analyse du SRC et du RM.

Dans le but d'éviter les doublons, un échange régulier, en partie formalisé, a lieu entre les domaines concernés du SRC et du RM. Entre autres, les services s'informent mutuellement de

la planification de leur production et mettent leurs produits à la disposition de l'autre service. L'échange d'informations se reflète également dans les produits eux-mêmes, qui ont tendance à se compléter plutôt qu'à se répéter lorsqu'ils traitent des domaines d'intérêt communs. Souvent, il y a des produits qui, partant de la même situation, transmettent chacun des perspectives différentes. C'est pourquoi l'AS-Rens a conclu que la délimitation entre les domaines d'analyse du SRC et du RM était adéquate et efficace.

21-2 Protection des infrastructures critiques / cyberdéfense (SRC/COE)

Dans le rapport de situation « La Sécurité de la Suisse 2021 », le SRC décrit l'augmentation de l'exposition aux cyberattaques. La pression en matière de numérisation, renforcée par les mesures de protection contre la pandémie, en serait la cause. Les nombreuses entreprises suisses qui proposent des accessoires et des services aux exploitants d'infrastructures critiques en Suisse et à l'étranger constitueraient également des cibles intéressantes pour les acteurs d'origine étatique. Les cyberattaques classiques ainsi que le cyberespionnage, le cybersabotage et le cyberterrorisme, dirigés directement contre les infrastructures critiques, ne représentent qu'une petite partie de l'ensemble des cybermenaces identifiées, selon le SRC. Les infrastructures critiques en Suisse n'ont pas été jusqu'à présent une cible directe d'actes de sabotage. Toutefois, le potentiel de dommages est considéré par le SRC comme le plus élevé dans ce domaine, car les services

⁹ <https://www.ab-nd.admin.ch/fr/pruefplan-und-pruefberichte.html>

¹⁰ Voir Rapport d'activités de l'AS-Rens 2020, page 9.

¹¹ SRC, division Analyse

d'infrastructure correspondants, tels que l'approvisionnement en électricité ou les services de télécommunication, sont essentiels au fonctionnement de la société.

En raison de ces risques incontestés, l'AS-Rens a contrôlé si les deux services, SRC et COE, disposaient de compétences et de capacités qualitatives et quantitatives suffisantes pour rechercher et traiter les informations nécessaires¹² et perturber, empêcher ou ralentir d'éventuelles attaques contre des infrastructures critiques¹³.

Le secteur Cyber du SRC, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (OIC MELANI¹⁴) et des parties de l'armée sont les acteurs déterminants pour faire face aux cybermenaces. Ils sont intégrés dans une structure organisationnelle interdépartementale complexe pour la protection des infrastructures critiques et la cyberdéfense. La tâche principale du SRC, avec la collaboration du COE, est d'identifier les cyberattaques et de savoir qui en sont les auteurs à l'aide de moyens du renseignement. En outre, il soutient les exploitants d'infrastructures critiques en leur présentant la situation actuelle dans le cyberspace. Les moyens du COE sont utilisés par le SRC pour l'analyse technique des cybermenaces.

L'analyse opérationnelle et l'analyse technique sont regroupées au sein du SRC dans le secteur Cyber. Parallèlement, le COE dispose également, dans le domaine des Cyber Network Operations (CNO), d'une unité Cyber Threat Intelligence (CTI) qui s'occupe de l'analyse des cybermenaces. Le secteur Cyber du SRC se voit sollicité dans le champ d'action cyber lorsqu'il s'agit d'incidents relevant de la politique de sécurité et pou-

vant être attribués à un autre État. Les activités purement cybercriminelles ne relèvent pas de son domaine de compétences.

En cas d'approbation d'une demande du SRC d'agir contre un agresseur conformément à l'art. 37, al. 1, LRens, le SRC chargerait le COE de mener la contre-attaque, car le SRC ne dispose pas lui-même des ressources pour mener une cyberattaque. Ces ressources sont du ressort de l'armée selon la cyberstratégie du DDPS. Le Joint Cyber Technical Analysis Center (JC-TAC) représente une forme de coopération qui va au-delà de la simple relation mandant/mandataire. Il ne s'agit pas d'une nouvelle unité organisationnelle, mais du regroupement de collaboratrices et de collaborateurs du SRC et du COE analysant ensemble les cybermenaces sur le plan technique.

L'inspection a montré que les compétences sont disponibles au SRC et au COE et que l'interaction entre les deux services fonctionne.

Clarification individuelle CYBER du SRC

L'AS-Rens a connaissance d'irrégularités dans le secteur Cyber du SRC depuis mai 2021. Elle a suivi de près les démarches internes entreprises par le SRC et a également demandé des éclaircissements quand cela était nécessaire. Sur le fond, l'AS-Rens approuve les démarches entreprises par le SRC et le DDPS. Éclaircir la pertinence d'une action pénale est pour l'AS-Rens de la plus haute importance. Nous allons suivre de près les développements, aussi à l'avenir, et exercer une influence lorsque cela nous paraîtra nécessaire. À ce jour, nous ne voyons aucune plus-value à poursuivre nos propres démarches (p. ex. au moyen d'une inspection).

¹² Art. 6, al. 1, let. a, ch. 4, LRens.

¹³ Art. 37, al. 1, LRens.

¹⁴ Operation Information Center, domaine de Melani

« Le juste équilibre entre le traitement des données autorisé et souhaité et le traitement interdit dans cette thématique est très difficile à trouver pour les collaboratrices et les collaborateurs du SRC. »

21-4 Extrémisme violent de droite (SRC)

Le SRC est responsable de la recherche et du traitement d'informations afin de détecter et d'empêcher à temps les menaces contre la sécurité intérieure et extérieure de la Suisse. Cela vaut également lorsque les menaces proviennent de l'extrémisme violent (EXTR)¹⁵.

Le SRC et son activité dans le domaine de l'extrémisme violent de droite – en tant que partie du domaine thématique EXTR – ont été à plusieurs reprises remis en question et critiqués de divers côtés. D'une part, le SRC se voit reprocher le fait d'être « aveugle de l'œil droit » et de ne pas prendre cette thématique suffisamment au sérieux¹⁶. D'autre part, le SRC se voit aussi régulièrement reprocher de rechercher illicitement des informations sur des activités politiques¹⁷.

Selon le rapport du SRC « La Sécurité de la Suisse 2020 », les membres des milieux d'extrême droite ont fait un usage modéré de la violence. Le plus grand risque d'un attentat motivé par l'extrême droite en Suisse proviendrait donc de personnes agissant seules avec des convictions d'extrême droite, mais sans appartenance ferme à des groupes extrémistes violents établis. Dans le rapport 2021, le SRC a montré que les milieux d'extrême droite ont un potentiel de menace élevé. Des groupes existants ont été dissous et de nouveaux ont été formés. Cependant, « seul » un événement lié à la violence a été constaté au cours de l'année sous revue.

Avec l'inspection 21-4, entre autres, l'AS-Rens cherchait à savoir si des concepts et processus adéquats existent au sein du SRC pour le domaine de l'extrémisme violent de droite, s'ils sont mis en œuvre efficacement et si la gestion d'informations

se fait conformément au droit. Lors de ses inspections, elle a constaté que le SRC avait de nombreux concepts et processus pour les activités de renseignement dans le domaine de l'extrémisme violent de droite.

Le SRC n'est autorisé ni à rechercher ni à traiter aucune information relative aux activités politiques ou à l'exercice de la liberté d'opinion, de réunion et d'association en Suisse. Cette interdiction est qualifiée de restriction de traitement des données¹⁸.

Parallèlement, le SRC doit toutefois anticiper les dangers émanant de l'extrémisme violent de droite et qui menacent la sécurité intérieure et extérieure de la Suisse. Le juste équilibre entre le traitement des données autorisé et souhaité et le traitement interdit dans cette thématique est très difficile à trouver pour les collaboratrices et les collaborateurs du SRC, qui doivent, dans le cadre de leur travail quotidien, se pencher sur diverses questions de délimitation:

- Dans quelle mesure l'extrémisme se différencie-t-il de l'extrémisme violent et du terrorisme?
- Comment l'extrémisme violent¹⁹ est-il défini exactement et quand peut-on parler de commettre, d'encourager ou d'approuver des actes de violence²⁰?
- Quand est-ce qu'un sujet relève de l'EXTR (et peut donc être traité par le SRC) et quand est-ce qu'un sujet relève d'une activité politique et de l'exercice de la liberté d'opinion, de réunion ou d'association en Suisse (et ne peut pas être traité par le SRC)²¹?
- Quand le SRC peut-il néanmoins traiter des informations sur l'activité politique et sur l'exercice de la liberté d'opinion, de réunion ou d'association en Suisse, précisément

¹⁵ Art. 6, al. 1, let. a, ch. 5, LRens

¹⁶ P. ex. postulat 02.3059; postulat 17.3831; heure des questions/question 19.5677; heure des questions/question 21.7312; Die braune Gefahr – Die Schweiz ist keine Insel, SRF, 12 mai 2019; Wie neutral ist unsere Polizei?, « Walliser Bote », 23 juillet 2020; Geheimdienst soll Rechtsextreme ins Visier nehmen, « Zeitung für die Region Basel », 25 mai 2021.

¹⁷ P. ex. interpellation 19.3868; Geheimdienst überwacht Menschenrechtsorganisation seit 15 Jahren, Netzpolitik.org, 10 août 2021

¹⁸ Art. 5, al. 5, LRens

¹⁹ Art. 6, al. 1, let. a, ch. 5, LRens

²⁰ Art. 19, al. 2, let. e, LRens

²¹ Art. 5, al. 5, LRens

« Le SRC doit garantir l'exécution conforme au droit de la LRens, tant au sein du SRC que dans les SRCant, par des mesures d'assurance qualité et de contrôle appropriées. »

parce qu'il existe des indices concrets que ces personnes exercent leurs droits pour préparer ou mener des activités extrémistes violentes²²?

En se basant sur ces questions et réflexions, le SRC a élaboré divers outils pour soutenir le travail quotidien des collaboratrices et des collaborateurs. Par exemple, un recueil de cas (casuistique) et les décisions qui en découlent doivent faciliter le travail des collaboratrices et des collaborateurs et les prises de décision futures dans des cas similaires.

L'anonymisation est une méthode pour le respect de la restriction de traitement des données: selon la loi, les informations non autorisées, mais néanmoins collectées concernant l'activité politique et l'exercice de la liberté d'opinion, de réunion ou d'association en Suisse doivent être anonymisées. Dans l'inspection 21-4, l'AS-Rens a constaté qu'il y avait des incohérences internes en ce qui concerne l'anonymisation des produits/annonces en rapport avec la restriction de traitement des données.

La liste d'observation est une autre référence importante pour le travail quotidien des collaboratrices et des collaborateurs du SRC. Il s'agit d'un instrument de pilotage politique du Conseil fédéral, qui l'approuve chaque année. Cette liste énumère les organisations et les groupements dont il y a lieu de penser qu'ils menacent la sûreté intérieure ou extérieure de la Suisse²³ et permet à ces derniers de franchir la restriction de traitement des données²⁴.

Dans l'inspection 21-4, l'AS-Rens a contrôlé si la procédure de vérification du SRC pour l'inscription des organisations de l'extrémisme violent de droite sur la liste d'observation²⁵ était adéquate. Sur la base d'échantillons, elle a analysé la manière de procéder du SRC et l'a jugée adéquate.

En ce qui concerne la légalité de la gestion des informations, l'AS-Rens n'a pas non plus constaté d'illégalités dans ses échantillons. Elle a en outre interrogé des tiers afin de vérifier l'efficacité des rapports et de la transmission d'informations sur le phénomène de l'extrémisme violent de droite. Ils ont estimé que les informations reçues du SRC étaient en principe efficaces

5.2.3 Collaboration

Ce domaine d'inspection regroupe les sujets concernant la collaboration nationale et internationale des services. À cet égard, les SRCant représentent chaque année un élément central de l'activité de contrôle de l'AS-Rens. Cette année, elle rendra compte des inspections sous forme de synthèse.

En 2021, l'AS-Rens a effectué les inspections suivantes dans ce domaine :

- **21-5 Assurance qualité du SRC auprès des services de renseignement cantonaux (SRCant)**
- **21- 6 Inspection du SRCant Bâle-Ville (SRC / SRCant)**
- **21- 7 Inspection du SRCant Bâle-Campagne (SRC / SRCant)**
- **21- 8 Inspection du SRCant Appenzell Rhodes-Extérieures (SRC / SRCant)**
- **21- 9 Inspection du SRCant Appenzell Rhodes-Intérieures (SRC / SRCant)**
- **21- 10 Inspection du SRCant Argovie (SRC / SRCant)**
- **21- 11 Inspection du SRCant Vaud (SRC / SRCant)**
- **21- 12 Inspection du SRCant Neuchâtel (SRC / SRCant)**

21-5 Assurance qualité du Service de renseignement de la Confédération auprès des services cantonaux de renseignement (SRCant) (SRC)

L'assurance qualité est une mesure de réduction des risques. En complément des inspections régulièrement effectuées dans les SRCant, l'AS-Rens a vérifié si cette mesure avait un impact sur les SRCant. Cela permet de garantir qu'une surveillance adéquate des SRCant soit assurée en coordination avec l'AS-Rens. Une assurance qualité fiable et gérable est importante pour la qualité des données et des informations du SRC et des SRCant. Le SRC doit donc garantir l'exécution conforme au droit de la LRens, tant au sein du SRC que dans les SRCant, par des mesures d'assurance qualité et de contrôle appropriées. Le service d'assurance qualité du SRC (AQ SRC), rattaché au domaine Gestion de l'information/Cyber, est chargé de cette tâche.

L'AQ SRC contrôle au moins une fois par an, au moyen d'échantillonnages, la légalité, l'adéquation, l'efficacité et l'exactitude du traitement des données dans tous les systèmes d'information du SRC. Pour ce faire, elle établit un plan de contrôle et vérifie notamment la pertinence et l'exactitude des rapports périodiques enregistrés par les SRCant. En outre, elle efface les données issues d'examens préalables menés par les SRCant et dont la saisie remonte à plus de cinq ans, et procède à la suppression de données demandée par les SRCant. En outre, l'AQ SRC assure également des formations internes sur les questions liées à la protection des données.

L'AQ SRC choisit toujours le même processus pour effectuer des échantillonnages auprès des SRCant. Les différentes étapes de ce processus sont planifiées avec des délais et clairement attribuées aux collaboratrices et collaborateurs de l'AQ SRC. Ces différentes étapes comprennent notamment l'attribution du mandat, la collecte de données statistiques selon des instructions identiques, un questionnaire basé sur les statistiques recueillies, l'avis des SRCant sur le questionnaire ainsi que le rapport final. Celui-ci est mis en consultation au sein de la direction du SRC, puis approuvé par cette dernière. Lors de la dernière étape, les SRCant reçoivent ce rapport définitif et l'AQ SRC suit la mise en œuvre de ses éventuelles recommandations. L'impli-

cation de la direction et l'adoption définitive des rapports par la direction du SRC confèrent à ces rapports également le poids nécessaire vis-à-vis des SRCant.

L'AQ SRC applique son mandat de contrôle de manière adéquate et efficace dans le cadre des SRCant. Cela se traduit, par exemple, par le fait qu'elle a développé un processus de prélèvement d'échantillons qui garantit que ce prélèvement est toujours effectué sur la base d'actions identiques. L'AS-Rens a pu s'en convaincre à l'aide de deux échantillons. Des missions internes claires et un principe des quatre yeux permanent garantissent que les contrôles sont effectués efficacement et que les risques correspondants peuvent être détectés.

Grâce à la coordination interne au SRC et à l'harmonisation avec les plans d'inspections de l'AS-Rens, ainsi qu'en tenant compte des résultats d'inspections antérieures, l'AQ SRC coordonne ses activités de contrôle des SRCant de manière adéquate et efficace. Cela permet de garantir que le même SRCant ne soit pas contrôlé deux fois par année, bien que cela soit également possible si nécessaire. En outre, les contrôles internes au SRC sont répartis entre plusieurs personnes. Cela garantit que les aspects opérationnels et sécuritaires sont pris en compte en plus du contrôle du traitement des données.

De 21-6 à 21-12: inspections des SRCant Bâle-Ville, Bâle-Campagne, Appenzell Rhodes-Extérieures, Appenzell Rhodes-Intérieures, Argovie, Vaud et Neuchâtel (SRC / SRCant)

En 2021, l'AS-Rens a examiné les activités de renseignement des SRCant d'Argovie, des deux Appenzell, des deux Bâle, de Neuchâtel et de Vaud. Leur collaboration avec le SRC a également été examinée. Depuis le début de ses activités de surveillance, l'AS-Rens a donc contrôlé au total 17 SRCant²⁶. L'examen des neuf SRCant restants suivra au cours des deux prochaines années.

²² Art. 5, al. 6, LRens

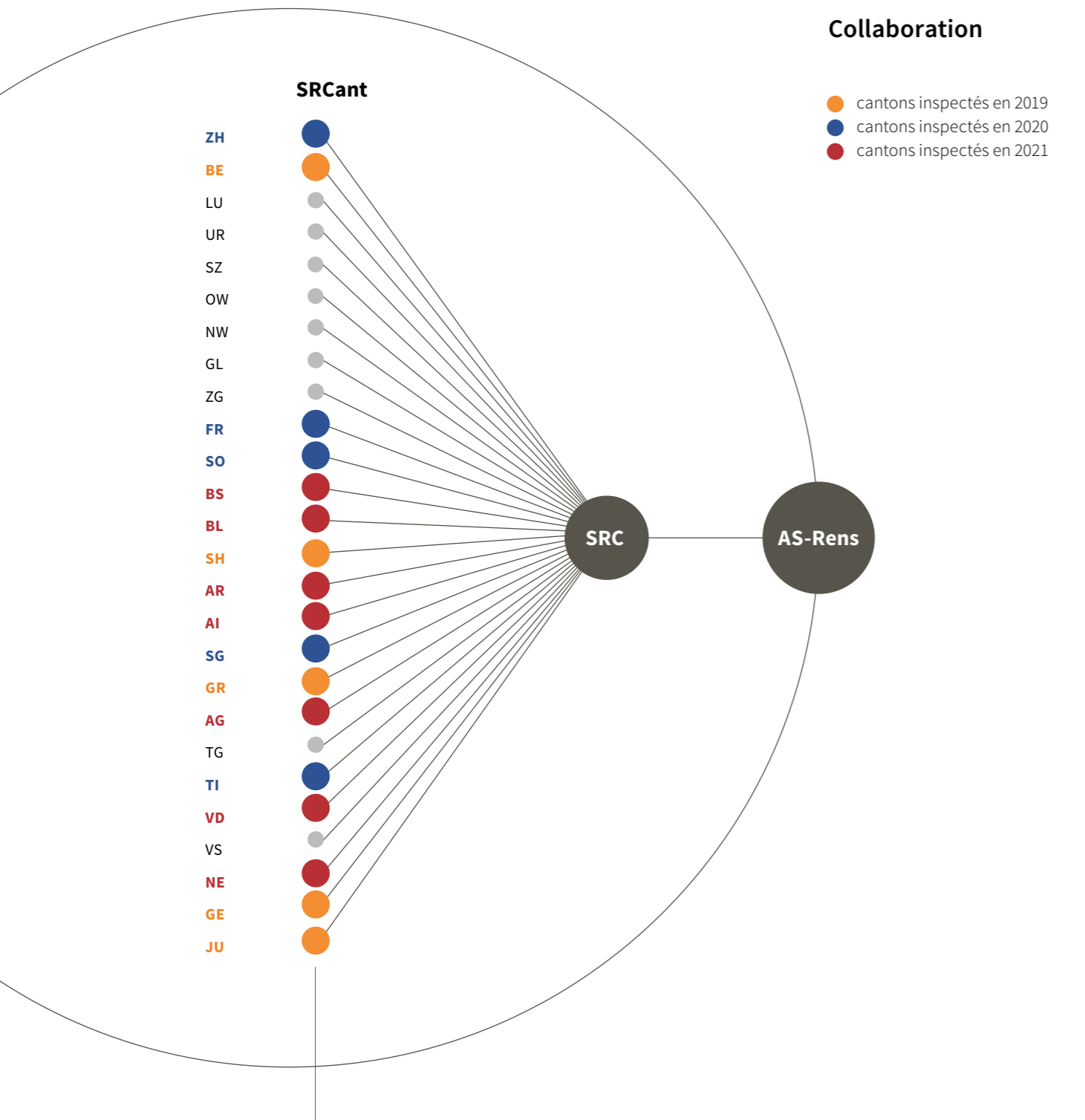
²³ Art. 70, al. 1, let. b et art. 72 LRens

²⁴ Art. 5, al. 8, LRens

²⁵ Art. 72 LRens

²⁶ En 2020, l'AS-Rens a contrôlé les SRCant de St-Gall, de Zurich, du Tessin, de Soleure et de Fribourg. En 2019, les SRCant de Berne, des Grisons, de Genève, du Jura et de Schaffhouse.

Collaboration



150 EPT (équivalent plein temps)



Il est ressorti de toutes les inspections des SRCant en 2021 que le SRC et les SRCant collaborent en principe bien en ce qui concerne tous les thèmes liés au renseignement. En ce qui concerne la réalisation d'actions opérationnelles communes, les deux parties souhaitent toutefois une meilleure coordination. Les divergences d'opinions entre le SRC et certains SRCant sur l'évaluation annuelle des performances ont pu être résolues lors d'entretiens de clarification.

Les SRCant disposent de bonnes à très bonnes connaissances en matière de renseignement et exécutent les mandats du SRC conformément au droit, dans les délais et avec une qualité satisfaisante pour le SRC. Ce dernier met à la disposition des SRCant, sur le poste de travail décentralisé²⁷, plusieurs applications et dossiers relatifs au renseignement, notamment une gestion des mandats ainsi qu'une application spécialisée (FA KND). La FA KND permet aux cantons de recenser des objets de manière structurée²⁸. L'AS-Rens n'a constaté, auprès des SRCant, ni l'existence de fichiers propres, ni de données personnelles dont le traitement ne repose sur aucune base légale. En revanche, les FA KND contenaient parfois des données qui n'avaient pas été saisies en temps réel pour les événements/constatations concernés. Par conséquent, ces données restaient stockées dans les FA KND plus longtemps que les cinq ans prévus par la loi. La cause de ces saisies incorrectes est supposément une migration de données antérieure (2017/2018) et devrait disparaître au cours des deux prochaines années grâce au bon fonctionnement de la suppression automatique. L'AS-Rens continuera à suivre cette évolution en coordination avec l'AQ SRC.

5.2.4 Recherche

La recherche d'informations est une tâche clé des services de renseignement. Pour ce faire, ils peuvent recourir à divers moyens. L'AS-Rens accorde une attention particulière aux moyens qui interfèrent le plus fortement avec la sphère privée des personnes concernées. En 2021, l'AS-Rens a en outre mené une inspection extraordinaire dans le domaine HUMINT, annoncée préalablement au SRC.

En 2021, l'AS-Rens a effectué les inspections suivantes dans le domaine « Recherche » :

- 21-13 Gestion du risque pour les engagements à l'étranger (SRC)
- 21-14 Opérations (SRC)
- 21-15 HUMINT (SRC)
- 21-19 Inspection extraordinaire HUMINT (SRC)

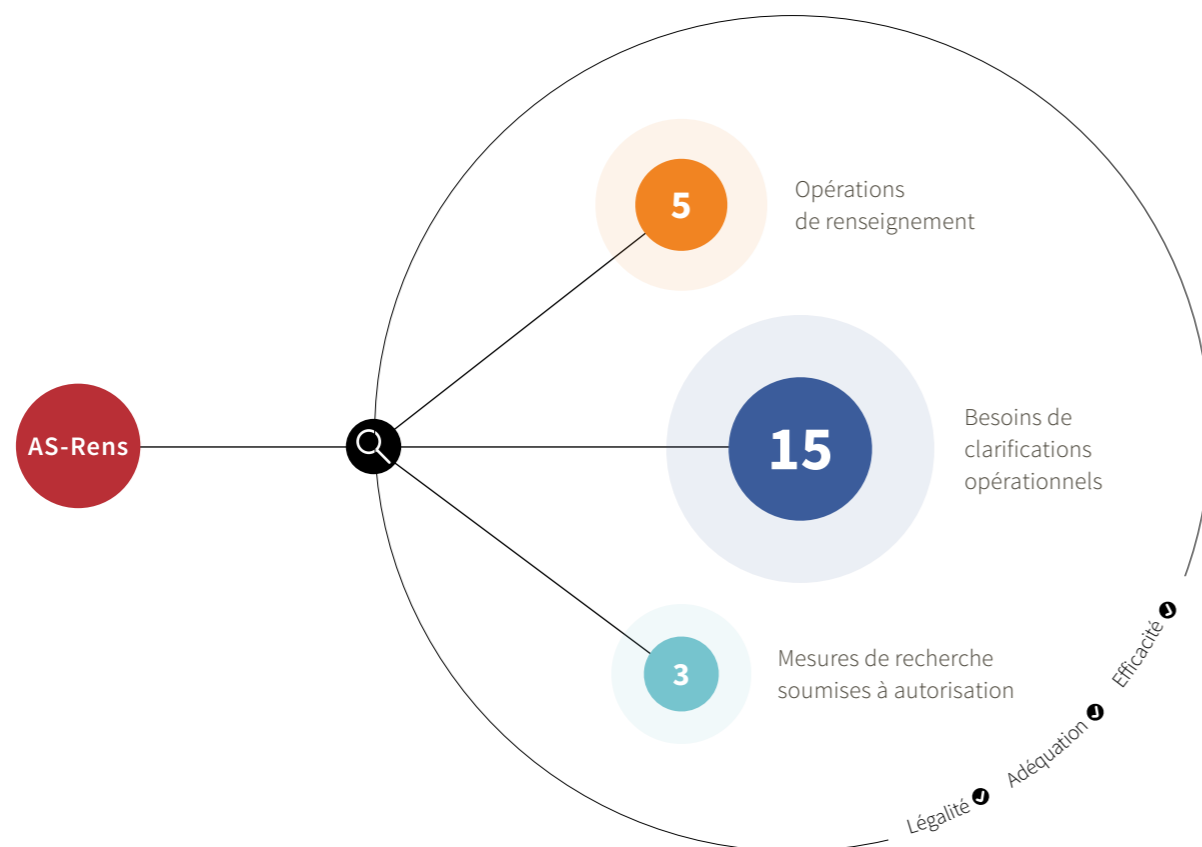
21-13 Gestion des risques pour les engagements à l'étranger (SRC)

Le SRC engage des collaboratrices et des collaborateurs pour des activités opérationnelles à l'étranger. Les cibles sont entre autres également des pays dans lesquels les principes de l'État de droit ne sont que partiellement ou pas du tout respectés, ou des zones où la sécurité peut être compromise. Des tiers apportent parfois leur soutien au SRC. Les recherches à l'étranger comportent par conséquent des risques pour les collaboratrices et les collaborateurs mandatés pour ce faire. Le SRC doit donc veiller à ce que les risques pris ne soient pas disproportionnés par rapport au but à atteindre²⁹ et que ses collaboratrices et collaborateurs en mission à l'étranger

²⁷ Le poste de travail décentralisé est un segment au sein du réseau sécurisé SiLAN du SRC qui permet d'accéder aux systèmes du SRC depuis un site décentralisé. La notion de « poste de travail décentralisé » est également utilisée pour désigner l'ordinateur portable qui permet de travailler à distance. Le poste de travail SRCant est la variante du poste de travail décentralisé mise à disposition des SRCant.

²⁸ Personnes, événements et moyens de communication sont les objets les plus fréquemment recensés par la FA KND.

²⁹ Art. 36, al. 3, LRens



soient protégés³⁰. Un pilotage et des processus internes sont de rigueur afin que ces directives puissent être respectées. Une gestion des risques adéquate et efficace est d'autant plus importante.

Cette inspection de l'AS-Rens a plus particulièrement porté sur les engagements opérationnels de trois domaines du SRC. En plus des entretiens et de l'étude de la documentation, les procédures du DFAE et de fedpol lors d'engagements à l'étranger ont été analysées à titre de comparaison.

L'AS-Rens est d'avis que le SRC applique au niveau stratégique la gestion des risques lors d'engagements à l'étranger. Il est néanmoins important d'accroître l'adéquation de la gestion des risques pour les engagements à l'étranger. L'objectif principal consiste à garantir la sécurité physique des collaboratrices et des collaborateurs. De plus, le pilotage des engagements à l'étranger devrait être centralisé au SRC et les processus devraient être standardisés. L'AS-Rens peut confirmer que l'intégration de tiers dans des engagements risqués à l'étranger est conforme au droit et clairement documentée.

21-14 Opérations (SRC)

Le SRC mène des opérations de renseignement parfois en utilisant des mesures de recherche soumises à autorisation. Les projets moins critiques en termes de temps et de sécuri-

té, dans lesquels seules des mesures de recherche n'étant pas soumises à autorisation entrent en ligne de compte, sont réalisés comme besoins de clarifications opérationnels. Le SRC rend compte chaque année des opérations au Conseil fédéral. En cas de besoins de clarifications opérationnels, la cheffe du DDPS n'est informée sur leur contenu que ponctuellement et en cas de besoin.

Dans le cadre d'une inspection annuelle récurrente, l'AS-Rens a analysé la légalité, l'adéquation et l'efficacité de cinq opérations de renseignement sélectionnées et de 15 besoins de clarifications opérationnels. En outre, pour trois mesures de recherche soumises à autorisation, elle a vérifié que leur mise en œuvre était conforme aux décisions du Tribunal administratif fédéral. Au cours des années précédentes, ces trois thèmes avaient été examinés séparément. Néanmoins, en raison des nombreuses interfaces et dépendances, l'AS-Rens a décidé de les regrouper en une seule inspection.

Les activités d'inspection comprenaient l'étude de documents et des entretiens avec les spécialistes responsables au SRC. Sur la base des résultats des activités d'inspection, l'AS-Rens peut en principe confirmer la légalité, l'adéquation et l'efficacité des opérations.

« L'AS-Rens contrôle HUMINT au sein du SRC chaque année au moyen d'échantillonnages. Dans le cadre de ces contrôles, elle couvre tout le spectre de la gestion des sources humaines. »

21-15 HUMINT (SRC)

Le recours à des informateurs reste l'un des principaux moyens d'exploration des services de renseignement, malgré des possibilités de surveillance technique très développées et l'accès à des informations publiques quasiment infinies. Les personnes ayant un accès particulier à des informations spécifiques sont donc intéressantes et importantes pour tout service de renseignement.

Le public a pu lire comment le SRC utilisait des informateurs dans le rapport de la DélCdG intitulé « Inspection consécutive à l'arrestation d'une ancienne source du SRC en Allemagne ». En 2017, un ancien informateur du SRC a été arrêté en Allemagne pour soupçon d'activité d'espionnage. La DélCdG a alors décidé d'analyser, dans le cadre d'une inspection, les dessous de cette affaire ainsi que le rôle du SRC, du Conseil fédéral et du Ministère public de la Confédération. La mise en œuvre des recommandations de ce rapport imprègne aujourd'hui encore le travail du SRC avec les informateurs.

HUMINT est souvent lié à des risques personnels élevés, tant pour les collaboratrices et les collaborateurs du SRC que pour les informateurs. Il en résulte une responsabilité et une obligation particulière pour le SRC qu'il doit prendre très au sérieux et qui jouent un rôle important dans la surveillance exercée par l'AS-Rens. Les officiers traitants doivent non seulement disposer de connaissances techniques dans leur domaine respectif, mais également d'une formation complète en matière de renseignement et de connaissances de différentes langues. Ils doivent également disposer de compétences sociales supérieures à la moyenne, à commencer par des compétences interculturelles et une sensibilité psychologique, afin de pouvoir relever des défis extraordinaires.

En tant qu'officiers traitants responsables des sources humaines, ils doivent comprendre ce qui motive et pousse les gens, indépendamment de leur origine ou de ce qu'ils font. Les collaboratrices et les collaborateurs opérationnels reçoivent

donc une formation spéciale, aussi bien en langues étrangères que pour l'utilisation des technologies ou la conduite du personnel. Il convient également de mentionner que le quotidien en tant qu'officier traitant implique de nombreuses restrictions à la vie privée.

L'AS-Rens contrôle HUMINT au sein du SRC chaque année au moyen d'échantillonnages. Dans le cadre de ces contrôles, elle couvre tout le spectre de la gestion des sources humaines, y compris les risques pour la sécurité, les dépenses financières et l'impact concret obtenu par l'évaluation des informations recueillies à partir d'informateurs. L'AS-Rens sélectionne les engagements des informateurs à inspecter sur la base d'une analyse des risques et mène, entre autres, des entretiens avec les officiers traitants, la direction d'HUMINT et les collaboratrices et les collaborateurs de la division Analyse. Ces dernières et ces derniers intègrent finalement les informations recueillies dans les produits de renseignement.

Ces inspections supposent des exigences considérables en matière de confidentialité. Ainsi, par exemple, les noms des sources humaines et de leurs responsables restent secrets, même pour l'AS-Rens, dans la mesure où ils ne sont pas pertinents pour l'inspection. Cela correspond au principe need-to-know. Concrètement, cela signifie ici que l'accès aux données à caractère personnel est limité aux personnes qui en ont impérativement besoin pour accomplir leurs tâches.

La protection des informateurs est un bien précieux, qui est également protégé par la loi³¹. C'est pourquoi l'AS-Rens doit remplir les mêmes conditions relatives à la protection des informateurs dans le cadre de ses inspections. Pour des raisons liées à la protection de l'État, l'AS-Rens ne peut pas informer sur le résultat de ses inspections dans le domaine HUMINT de manière aussi détaillée qu'elle le fait dans d'autres domaines d'inspection.

³⁰ Art. 36, al. 7, LRens

³¹ Art. 35 LRens

5.2.5 Ressources

Afin de garantir une activité de renseignement efficace, une gestion adéquate des ressources est indispensable.

En 2021, l'AS-Rens n'a ni planifié, ni mené d'inspections dans ce domaine.

5.2.6 Traitement des données et archivage

La sensibilité des informations traitées par les services est élevée. En outre, les prescriptions légales sont vastes et complexes. C'est pourquoi l'autorité de surveillance doit apporter une attention particulière à la légalité du traitement des informations.

En 2021, dans ce domaine, l'AS-Rens a planifié les inspections suivantes:

- 21-16 Services de télécommunication (SRC)
- **21-17 Système d'information du SRC sélectionné (Quattro P)**
- **21-18 Protection des données au sein du RM**

L'inspection « 21-16 Services de télécommunication » n'a débuté qu'au quatrième trimestre 2021. Jusqu'à la date de clôture de la rédaction du présent rapport d'activités, aucun résultat pertinent pour le rapport n'était encore disponible.

21-17 Système d'information du SRC sélectionné (Quattro P)

En 2020, l'AS-Rens a décidé d'intégrer le système d'information Quattro P au plan des inspections 2021. La raison à cela est que ce système d'information permet de saisir et traiter un nombre important de déplacements de personnes de certaines nationalités. Les données personnelles dans Quattro P servent en outre de base pour le système de reconnaissance faciale que le SRC utilise depuis 2020 et qui servait jusqu'à présent uniquement à la recherche de données propres. Finalement,

le cercle des personnes autorisées à accéder à Quattro P comprend la moitié des collaboratrices et des collaborateurs du SRC ; il est donc important. Dans cette inspection, l'AS-Rens a contrôlé le fonctionnement, l'utilisation et les contenus du système d'information sur les plans de l'adéquation et de la légalité. De plus, l'une des questions de l'inspection concernait la légalité du système de reconnaissance faciale exploité par le SRC.

Dans le cadre de l'inspection, les directrices d'inspections ont eu accès aux systèmes d'information Quattro P, IASA SRC, SILAN et au système de reconnaissance faciale. Cela a permis de garantir que l'AS-Rens puisse planifier et effectuer ses échantillonnages de manière indépendante.

Légalité de la saisie et du traitement des données dans Quattro P

Le Conseil fédéral détermine dans une liste non publique les voyageuses et les voyageurs dont les données doivent être communiquées spontanément au SRC³². Il se fonde pour cela sur l'appréciation actuelle de la menace. Les données des voyageurs au sein de l'espace Schengen ne sont pas enregistrées dans Quattro P en raison des contrôles aux frontières inexistantes.

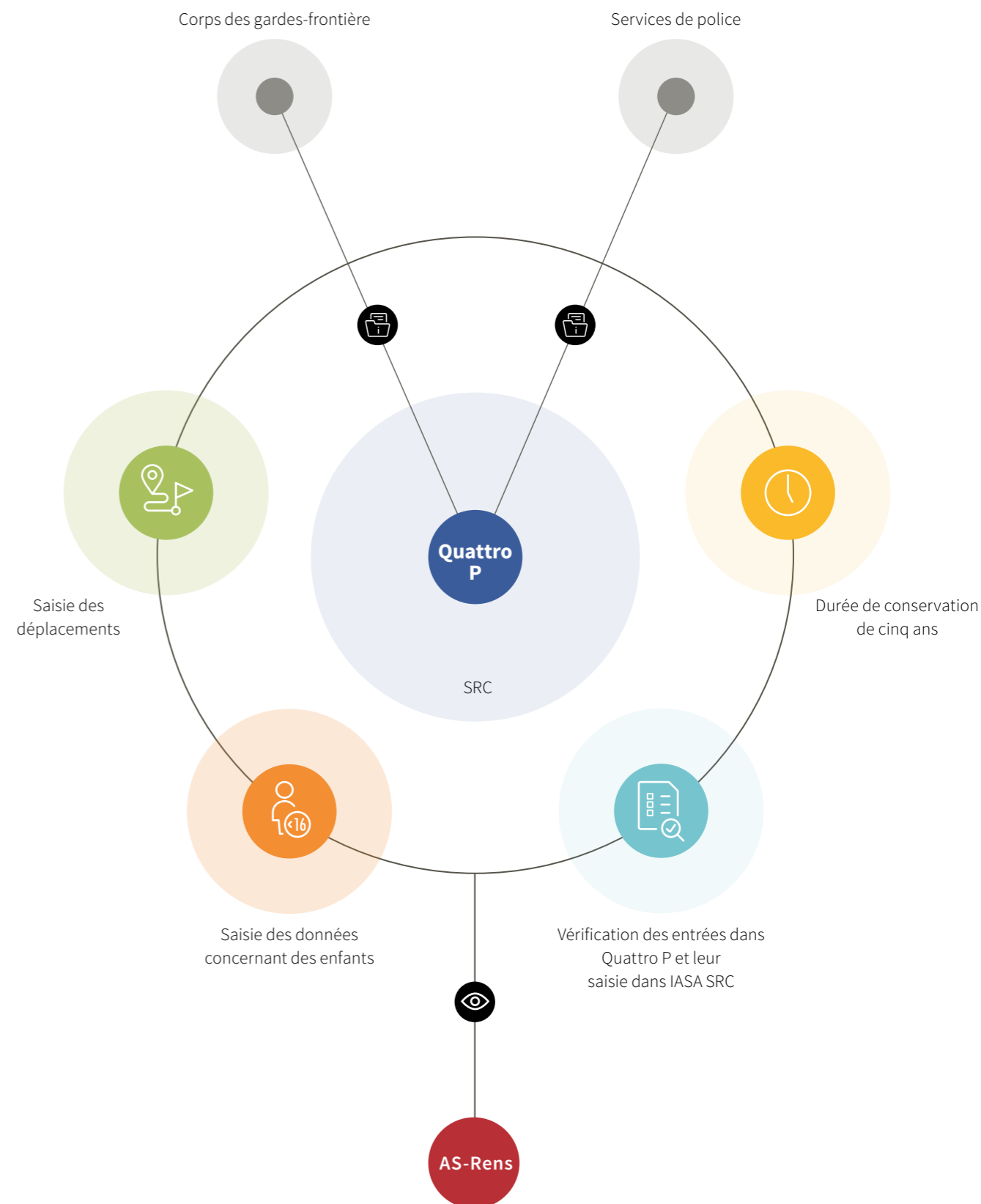
Les données personnelles ci-dessous sont saisies dans Quattro P³³:

- nom, prénom, date de naissance, nationalité;
- numéro du document d'identité; numéro de visa; date de validité;
- photo du document d'identité;
- lieu, date et description du contrôle à la frontière;
- sexe;
- données provenant de la puce du document d'identité;
- données provenant du visa.

³² Art. 55, al. 4, LRens; la liste des pays fait partie de la liste selon l'art. 20, al. 4, LRens (événements et données à communiquer spontanément)

³³ Annexe 8 OSIS-SRC

Quattro P



Ces données sont livrées par les services concernés (Corps des gardes-frontière, services de police). Le tri des données à livrer se fait au sein de ces services mêmes afin que le SRC ne reçoive que les données qu'il est autorisé à recevoir selon les dispositions légales. Les données concernant les enfants de moins de 16 ans ne sont pas saisies.

Après l'analyse des dispositions légales et de la documentation relative au système d'information, l'AS-Rens a effectué les échantillonnages ci-dessous pour l'inspection de la notion de légalité:

- saisie des déplacements uniquement des ressortissants figurant sur la liste des États établie par le Conseil fédéral;
- saisie des données concernant des enfants;
- respect de la durée de conservation de cinq ans³⁴;
- vérification des entrées dans Quattro P et leur saisie dans IASA SRC.

Lors de l'inspection des échantillons, l'AS-Rens a constaté des cas de saisies multiples de documents de voyage relatifs à des voyages individuels. Elle a donc recommandé au SRC d'étudier les mesures à prendre pour réduire ces cas, puis de les appliquer. Pour le reste, l'AS-Rens a considéré, sur la base des activités d'inspection réalisées, que les traitements de données dans Quattro P étaient conformes au droit.

Adéquation de la saisie et du traitement des données dans Quattro P

La notion d'adéquation comprend l'aptitude, la nécessité et la pertinence d'une procédure, ici le traitement des données dans Quattro P. Un traitement compliqué et fastidieux des données est source d'erreurs et peut conduire à ce que le SRC dispose trop tard d'informations pertinentes pour l'accomplissement de ses tâches.

La transmission automatisée des données par les bureaux extérieurs qui les fournissent semble faire ses preuves au vu de la grande quantité de données fournies. Seul un petit pourcentage des données livrées est traité manuellement. Si le pourcentage des données livrées incorrectement augmente, le SRC prend contact avec les autorités qui ont fourni les données et des mesures appropriées sont prises pour améliorer la qualité de ces données.

En ce qui concerne les échantillonnages effectués pour vérifier la légalité de la saisie des données, l'AS-Rens a constaté que, pour environ 25 % des données examinées, la destination du voyage était indiquée comme « non définie »³⁵. C'est pourquoi l'AS-Rens a recommandé que le SRC vérifie, en collaboration avec les organes de contrôle, quelles mesures permettraient de réduire ce pourcentage.

Légalité et adéquation de la gestion des accès à Quattro P

Pour des raisons liées à la sécurité de l'information et à la protection des données, l'accès à Quattro P doit être octroyé uniquement aux collaboratrices et collaborateurs du SRC qui en ont besoin pour accomplir leurs tâches. Si les autorisations ne sont plus actuelles, elles ne respectent pas le principe need-to-know. Des processus inadéquats dans la gestion des accès entraînent des retards dans l'ajustement des droits d'accès. Ces derniers doivent être adaptés à temps en cas de changements de poste ou de départs de personnel, afin d'éviter les accès illicites aux données et les éventuelles failles de sécurité qui en découlent.

Sur la base des échantillonnages effectués et de l'analyse des documents pertinents, l'AS-Rens a recommandé de vérifier régulièrement les droits d'accès et de supprimer les accès non nécessaires³⁶.

³⁴ Art. 55 OSIS-SRC

³⁵ Les possibilités ci-après sont à disposition: « entrée », « sortie » et « non défini ».

³⁶ Art. 5, al. 4, OSIS-SRC

« La reconnaissance faciale est un nouveau moteur de recherche qui suscite la controverse du point de vue de la protection des données. Comme elle est utilisée au SRC, l'AS-Rens a décidé de vérifier la légalité de son utilisation. »

Légalité du système de reconnaissance faciale

Les systèmes de reconnaissance faciale permettent d'identifier des personnes sur des photos, dans des vidéos ou en temps réel. Les images disponibles dans les bases de données sont analysées sur la base de la géométrie des visages saisis. Les traits caractéristiques du visage sont transformés en un ensemble de données numériques – une empreinte faciale. Cette dernière est aussi unique que les empreintes digitales. De telles données sont appelées « données biométriques »³⁷.

La reconnaissance faciale est un nouveau moteur de recherche qui suscite la controverse du point de vue de la protection des données. Comme elle est utilisée au SRC, l'AS-Rens a décidé de vérifier la légalité de son utilisation.

Elle a constaté qu'au début du projet, le SRC a initié différentes clarifications concernant la légalité. Ces clarifications ont servi à l'élaboration du règlement sur le traitement des données et à une analyse des bases légales. Le projet a continué à se développer par la suite sans que le service juridique ou le service interne de contrôle de qualité du SRC ne vérifient une nouvelle fois la légalité de la poursuite du développement.

Selon l'AS-Rens, le système de reconnaissance faciale permet de traiter des données biométriques. Ces données sont classées comme des données sensibles conformément à loi fédérale révisée (pas encore en vigueur) sur la protection des données (LPD)³⁸. En vertu de l'art. 47, al. 2, LRens, le Conseil fédéral règle le catalogue des données personnelles pour chaque système d'information. Il l'a fait dans l'OSIS-SRC, mais le traitement des données biométriques n'est prévu dans aucun des systèmes d'information qui y sont mentionnés.

De plus, le système de reconnaissance faciale permet d'établir des profils d'images qui peuvent, en outre, être enrichis à l'aide de métadonnées. Selon l'AS-Rens, cela conduit à la

création de profils de la personnalité. Sur la base de ces réflexions, l'AS-Rens a émis plusieurs recommandations qui concernaient notamment aussi l'implication du PFPDT dans la poursuite des clarifications juridiques du SRC.

21-18 Protection des données au sein du RM

Après avoir mis en lumière les systèmes d'informations pertinents en matière de renseignement utilisés par le Renseignement militaire (RM) dans son inspection 20-17, l'AS-Rens a vérifié au cours de l'année sous revue la légalité du traitement des données personnelles présentes dans deux systèmes du RM au moyen d'entretiens, d'une étude documentaire et d'un échantillonnage aléatoire. Parmi les différents systèmes d'informations, sous-systèmes et applications spéciales autorisées, l'AS-Rens a décidé de focaliser son examen sur les systèmes d'informations exploités par le RM et dont il est responsable, à savoir son outil principal de travail, le système Ik MND, ainsi que sur le système d'échange d'informations sécurisé avec l'étranger BICES³⁹. Selon l'évaluation faite par l'AS-Rens ces systèmes comportent potentiellement un risque élevé au regard de la protection des données (quant à la quantité, la nature des données, les destinataires et éventuels impacts en termes d'atteinte aux droits de la personnalité des personnes concernées).

Elle a pu constater que le RM traite dans le cadre de ses tâches légales des données personnelles et peut aussi être amené à traiter des données personnelles sensibles ou établir des profils de personnalité, bien que l'AS-Rens n'en ait pas constaté la présence lors de ses échantillonnages. Si l'AS-Rens a pu relever la présence de données personnelles dans certains produits du RM, elle constate toutefois que celles-ci ne constituent pas le centre d'intérêt du RM qui se focalise sur ses missions (recherche et évaluation d'informations sur l'étranger importantes pour l'armée, notamment du point de vue de la défense nationale, du service de promotion de la paix et du service d'appui à l'étranger). La recherche d'informations est axée prioritaire-

³⁷ Source: www.kaspersky.de/resource-center/definitions/what-is-facial-recognition, dernière consultation le 22 novembre 2021.

³⁸ RS 235.1

³⁹ Battlefield Information Collection and Exploitation System, Réseau international de communication de l'OTAN.

« Pendant l'année sous revue, l'AS-Rens a enregistré une nette augmentation des informations et des signalements transmis de manière informelle, dus principalement au mécontentement des collaboratrices et des collaborateurs du SRC. »

ment sur l'étranger. Elle n'est pas ciblée sur des personnes en Suisse qui ne sont par ailleurs pas saisies de manière structurée dans les systèmes du RM. Les données personnelles de ressortissants suisses qui sont collectées dans le cadre d'un service d'appui en Suisse (par exemple World Economic Forum), sont transmises aux autorités nationales compétentes et ne doivent pas être utilisées en lien avec les activités de renseignement militaire.

Si des données personnelles sont traitées, il s'agit des noms de personnalités politiques, de dirigeants étrangers, des chefs de réseaux ou de groupes armés permettant au RM d'assurer un suivi et une évaluation des développements stratégiques militaires et des forces armées avec un accent sur certains pays ou menaces de type militaire et des conflits armés ainsi que la situation dans les zones d'engagement de l'armée suisse à l'étranger.

Dans chaque cas examiné lors des échantillonnages, un lien a pu être établi avec les activités du RM. Par ailleurs, l'AS-Rens s'est également fait expliquer les droits d'accès des utilisateurs et la procédure d'archivage et de suppression des documents. Elle a constaté que les accès sont limités aux collaboratrices et collaborateurs qui en ont besoin pour l'accomplissement de leurs tâches et que les produits présents dans les systèmes inspectés sont proposés aux archives fédérales et ne sont pas conservés au-delà de la durée légale. Les systèmes utilisés par le RM sont bien documentés. Ils ne sont pas reliés entre eux par des interfaces communes permettant un échange automatisé de données, ce qui limite les risques d'abus.

A l'issue de son inspection, l'AS-Rens n'a pas constaté d'éléments qui pourraient la conduire à douter de la légalité du traitement des données personnelles effectué par le RM dans toutes ses phases ni que ce dernier fait un usage abusif ou disproportionné des données personnelles collectées tant au regard de sa propre législation que des dispositions sur la protection des données.

L'AS-Rens a également constaté que le RM peut s'appuyer sur des dispositions spécifiques pour ce qui a trait à la communication de données personnelles à l'étranger. En règle générale,

les produits qui sont transmis à l'étranger concernent des évaluations de situation (militaire, politique, militaro-politique). S'il ne peut être exclu que des données personnelles puissent occasionnellement apparaître dans les produits du RM, il n'y a pas d'échange de données en relation à une personne en particulier. Par ailleurs, les produits du RM ne sont fournis qu'aux services des pays qui partagent les valeurs occidentales et disposent d'une législation sur la protection des données.

5.3 Acceptation

L'accueil réservé aux directrices et directeurs d'inspections de l'AS-Rens par les services soumis à la surveillance a été constructif et professionnel. L'accès aux documents et systèmes d'information nécessaires à la réalisation des mandats d'inspection a pu se faire très simplement. Les personnes interrogées étaient à la disposition des directrices et des directeurs d'inspections. Les entretiens ont pu être planifiés et réalisés dans un délai raisonnable malgré les restrictions imposées par la pandémie. Les réponses aux questions supplémentaires ont été fournies aussi rapidement que possible.

Pendant l'année sous revue, l'AS-Rens a enregistré une nette augmentation des informations et des signalements transmis de manière informelle, dus principalement au mécontentement des collaboratrices et des collaborateurs du SRC. Les informations ont été analysées dans la mesure du nécessaire et du possible et intégrées dans les procédures d'inspections ou ont donné lieu à des clarifications individuelles. La cheffe du DDPS a été informée par écrit de ces développements, le 13 juillet et le 22 octobre 2021. Cette thématique n'est pas terminée et occupera l'AS-Rens à l'avenir aussi.

5.4 Controlling des recommandations

La vérification de la mise en œuvre des recommandations n'est pas explicitement réglementée par les bases légales du renseignement. En accord avec le DDPS et les autorités surveillées, il a été convenu que ces dernières informeraient le département par écrit au sujet de la mise en œuvre des

recommandations. L'AS-Rens en reçoit une copie. En 2021, l'AS-Rens a reçu une notification de mise en œuvre pour 66 recommandations. À la fin de l'année il n'y a aucune recommandation en suspens au RM ni à la COE. En outre, au milieu de l'année et en présence du conseiller en renseignement de la cheffe du DDPS, une rencontre avec tous les services soumis à la surveillance a eu lieu pour faire le point sur les recommandations encore en suspens et celles qui avaient déjà été mises en œuvre.

Vérification des recommandations – un exemple concret

Avec l'entrée en vigueur de la LRens, le SRC dispose d'une base légale explicite en vue de détacher ses propres collaboratrices et collaborateurs dans les représentations suisses à l'étranger pour promouvoir des contacts internationaux⁴⁰. Le SRC utilise cette possibilité et fait appel à ce que l'on appelle des personnes de liaison pour les services de renseignement. En 2019, l'AS-Rens a donc examiné la gestion de l'information en matière de renseignement entre le senseur Attachés de défense (AD) et le SRC.

Les AD permettent à la Suisse de défendre la mise en œuvre de ses intérêts relevant de la politique étrangère et de la politique de sécurité. Bien que les AD soient des militaires, c'est en premier lieu le SRC qui est responsable de leur engagement en tant que senseurs et donc de leur conduite en matière de renseignement.

Suite à cette inspection, l'AS-Rens a recommandé au SRC d'élaborer un concept stratégique visant à mieux définir le recours aux personnes de liaison pour les services de renseignement et son interface avec les attachés de défense. L'objectif est d'améliorer l'adéquation et l'efficacité dans ce domaine du renseignement.

Durant l'année sous revue, l'AS-Rens a procédé à l'inspection « 21-1 Engagement de collaboratrices et de collaborateurs du SRC dans les représentations suisses à l'étranger ». La vé-

rification de la recommandation faite antérieurement quant à l'élaboration d'un concept stratégique pour le recours aux personnes de liaison pour les services de renseignement était un élément essentiel de l'inspection. Les recommandations formulées sont inscrites dans un système de monitoring auprès de l'AS-Rens et vérifiées à l'aide d'avis d'exécution reçus du SRC concernant leur mise en œuvre. Finalement, l'AS-Rens décide si la mise en œuvre décrite suffit ou si elle nécessite une vérification plus approfondie. Si elle parvient à cette dernière conclusion, soit la mise en œuvre à contrôler est intégrée dans une inspection planifiée, soit, comme dans le cas décrit ci-dessus, une inspection propre est créée.

⁴⁰ Art. 12, al. 2, LRens

6. Regard interne

Dans ce chapitre, l'AS-Rens rapporte ses affaires internes.

6.1 Personnel et formations continues

L'AS-Rens compte toujours un effectif de dix collaboratrices et collaborateurs, répartis sur 9,1 équivalents plein temps (EPT). Une directrice et un directeur d'inspections ainsi que la responsable de la gestion administrative ont décidé de relever de nouveaux défis et de quitter l'AS-Rens à la fin de l'année 2021. À la fin du mois de novembre 2021, leur succession a pu être partiellement réglée et au premier semestre 2022, l'AS-Rens devrait à nouveau être au complet.

Les possibilités de formation continue ont été utilisées en 2021. Les collaboratrices et les collaborateurs ont suivi des formations continues exigeantes de niveau master et CAS⁴¹ dans les domaines techniques et de la gestion. Le stage prévu dès 2020 au Comité R en Belgique a dû être une nouvelle fois reporté.

Le travail à domicile, plus fréquent en raison des mesures destinées à lutter contre l'épidémie de COVID-19, a en principe bien fonctionné. Il atteint ses limites lorsque des informations classifiées doivent être traitées. Les collaboratrices et les collaborateurs ont souffert du manque de contacts et d'échanges directs après des semaines et des mois passés en télétravail. Les outils techniques ne peuvent pas pallier le manque d'échanges d'informations directs. Le télétravail est défavorable à la formation du nouveau personnel et risque de retarder considérablement la possibilité d'effectuer des inspections.

6.2 Révision de la LRens

Le projet de révision de la LRens était en consultation auprès des offices en 2021. L'AS-Rens a pu faire valoir ses intérêts, no-

tamment dans la deuxième section du sixième chapitre, qui concerne l'AS-Rens elle-même. Le projet est sous la responsabilité du DDPS.

6.3 Loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans)

Au cours de l'année sous revue, aucune demande d'accès à des documents officiels n'a été transmise à l'AS-Rens.

6.4 Visites

La cheffe du DDPS a rendu visite à l'AS-Rens en septembre dans ses locaux et s'est fait présenter brièvement les tâches et les possibilités de l'AS-Rens à trois postes de travail.

En outre, l'AS-Rens a envoyé une invitation à la DélCdG en janvier 2021 pour une visite de ses locaux. Le but était de lui fournir un aperçu du travail concret de l'AS-Rens. La DélCdG n'a pas donné suite à cette invitation.

6.5 Jurisprudence

L'AS-Rens s'informe de la jurisprudence aussi bien sur le plan national qu'international. Durant l'année sous revue, des décisions de la Cour européenne des droits de l'homme ont été analysées à l'interne et discutées en équipe. En outre, l'AS-Rens a reçu des informations importantes sur la jurisprudence au niveau européen lors de l'European Oversight Conference à Rome.

⁴¹ Certificate of Advanced Studies, des diplômes de formation continue de niveau universitaire en cours d'emploi

7. Coordination

L'AS-Rens coordonne ses activités avec la haute surveillance parlementaire et avec d'autres autorités de surveillance de la Confédération et des cantons⁴². En 2021 également, cette coordination a toutefois été influencée par la pandémie ainsi que par les mesures et les restrictions de voyage qui en découlent.

7.1 Contacts nationaux

Conférence avec les autorités de surveillance cantonales

Le 18 août 2021, l'AS-Rens a eu lieu la deuxième conférence avec les autorités de surveillance cantonales organisée par l'AS-Rens à la caserne des troupes bernoises. Quinze autorités de surveillance cantonales, des représentants du Service de renseignement de la Confédération, ainsi que deux chefs de services de renseignement cantonaux ont participé à cet événement. Les buts de la conférence étaient la formation continue, le réseautage et l'échange d'expériences.

Pour commencer, les représentantes et les représentants de deux autorités de surveillance cantonales (Soleure et Fribourg) ont exposé leurs résultats, leurs défis et leurs attentes. Suite à cela, deux collaborateurs du SRC ont présenté leur point de vue en matière de contrôle, notamment de la qualité, de la sécurité et des tâches administratives en général. Ensuite les chefs des services de renseignement cantonaux (de Bâle-Ville et de Fribourg) sont intervenus pour démontrer l'impact de la surveillance sur leur travail. Enfin, le chef de l'AS-Rens a présenté les activités de son organisation depuis la dernière conférence qui s'était tenue en 2018. L'après-midi, un panel de quatre orateurs a permis d'aborder des questions de fond et de proposer des pistes de réflexions pour l'avenir de la surveillance des activités de renseignement.

Les enseignements tirés de cette journée sont:

Pour les autorités de surveillance cantonales, l'accent est principalement mis sur la légalité des activités des services de renseignement cantonaux. En particulier l'utilisation des informateurs, les listes de surveillance, l'appréciation de la menace et la délimitation avec le travail de police sont des défis constants. La transparence, le dialogue et la proximité sont les clés de la confiance.

Pour le service de renseignement de la Confédération, l'information mutuelle et la coordination avec les SRCant sont primordiales. Le SRC reconnaît que de grands progrès ont été réalisés depuis l'entrée en vigueur de la LRens en septembre 2017. Toutefois, des divergences subsistent encore entre les divers SRCant pour ce qui est du traitement des données et de la collaboration. Le SRC demande instamment que les irrégularités à tous les niveaux soient signalées dans les meilleurs délais. Selon le SRC, « l'union fait la force et unis nous assurons la sécurité de la Suisse ».

Pour les services de renseignement cantonaux, le but principal de la surveillance est de démystifier l'activité de renseignement. Généralement, les échanges avec les autorités de surveillance sont constructifs, ils offrent la possibilité de communiquer les besoins, renforcent la transparence et la confiance et permettent un réel potentiel de développement et d'amélioration. Il a toutefois été relevé que le nombre de contrôles est extrêmement élevé (jusqu'à une fois par mois pour un certain SRCant) et qu'une meilleure planification des contrôles entre les diverses autorités cantonales et fédérales serait souhaitable. Il a également été relevé que les obstacles juridiques sont élevés pour les mesures de recherche soumises à autorisation, ce qui a pour conséquence de développer le domaine du renseignement humain.

Pour l'Autorité de surveillance indépendante des activités de renseignement, les points clairement positifs mis en évidence par les inspections effectuées depuis l'entrée en vigueur de la LRens sont la collaboration avec l'ensemble des acteurs de la surveillance, les flux d'informations et l'engagement des SRCant. L'AS-Rens note toutefois un potentiel d'amélioration dans le traitement des données, l'utilisation des ressources et

⁴² Art. 78, al. 2, LRens.

des moyens techniques. Le but déclaré est clairement d'ajouter de la valeur aux activités de renseignement, tout en renforçant la confiance.

Après une longue période d'incertitude et de report de la conférence en raison de la pandémie de COVID-19, cette réunion a été un succès. La prochaine édition aura lieu en 2023

Tribunal administratif fédéral (TAF)

Le 10 septembre 2021, l'AS-Rens s'est entretenue avec des représentants du TAF sur divers sujets, dont les mesures de recherche soumises à autorisation, les derniers développements de la jurisprudence et la révision de la LRens.

Contrôle fédéral des finances (CDF)

Le 21 mai 2021, la direction de l'AS-Rens a discuté et coordonné avec deux représentants du CDF, entre autres, des thèmes d'inspections possibles.

Délégation des Commissions de gestion (DélCdG)

La direction et un collaborateur de l'AS-Rens ont été invités une seule fois à une audition, le 20 janvier 2021. À cette occasion, l'AS-Rens a informé sur le rapport d'inspection « 20-13 enquêtes opérationnelles ». Nous considérons le rapport de la DélCdG sur l'AS-Rens comme étant arbitraire et tendancieux. L'AS-Rens a pris position dans un document de 4 pages sur le rapport annuel de la DélCdG. La plupart de nos demandes de rectifications n'ont pas été prises en compte, sans commentaire. De notre point de vue, cette manière de faire n'est ni dans l'intérêt de la cause ni souhaitable en termes d'impact extérieur. En matière de surveillance des activités de renseignement, un dialogue raisonnable doit enfin pouvoir avoir lieu entre les différentes autorités chargées de la surveillance

Révision interne DDPS (RI DDPS)

Le 22 janvier 2021, à l'occasion d'un échange téléphonique, la direction de l'AS-Rens et la RI DDPS ont notamment discuté de la manière dont la RI pourrait éventuellement profiter des connaissances préalables de l'AS-Rens, se sont demandé

dans quelle mesure l'activité de surveillance pourrait générer une plus-value pour les services également et ont envisagé la possibilité d'une sorte d'évaluation par les pairs pour contrôler l'AS-Rens. Ce dernier point signifierait que, par exemple, une autorité de surveillance contrôlerait les processus d'une autre autorité de surveillance sur le plan de l'adéquation.

Autorité cantonale de surveillance Bâle-Ville (ACS BS)

Le 15 juillet 2021, le chef de l'AS-Rens, accompagné de deux directeurs d'inspections, a rencontré les représentants de l'ACS BS afin d'échanger sur les thèmes des inspections dans le domaine de l'extrémisme violent de droite, des rapports annuels de l'AS-Rens et de l'ACS BS, des répercussions de la loi fédérale sur les mesures policières de lutte contre le terrorisme, des méthodes de surveillance ainsi que du rapport d'inspection « 21-6 SRCant Bâle-Ville ».

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

La révision de la LRens doit permettre la mise en œuvre de la fusion de l'OCI avec l'AS-Rens, déjà discutée lors de l'élaboration de la LRens. Pour ce faire, le président de l'OCI et le chef de l'AS-Rens ont convenu que l'AS-Rens accompagnerait l'OCI lors de ses séances d'inspection régulières. Un représentant différent pour chaque séance a donc participé aux séances de l'OCI des 26 juin, 17 septembre, 22 octobre et 18 novembre 2021.

L'objectif était d'obtenir une vue d'ensemble des activités d'inspection et d'acquiescer ainsi, du point de vue technique et du renseignement, le savoir-faire nécessaire à la reprise des activités de l'OCI par l'AS-Rens. Pour des raisons de compétence, l'AS-Rens a renoncé à jouer un rôle actif dans le processus d'inspection de l'OCI. De son côté, l'OCI transmet un rapport annuel à la DélCdG, et l'AS-Rens reçoit chaque rapport à titre d'information.

En outre, l'AS-Rens a participé à l'atelier d'exploration du réseau câblé, auquel l'OCI invite, à intervalles réguliers, des représentants du SRC, du COE, du TAF et de l'AS-Rens. L'objectif est l'échange mutuel d'informations concernant l'exploration du réseau câblé. Cette année, les discussions ont porté sur le développement de l'infrastructure technique, sur le défi parti-

culier que représente le pilotage du senseur Exploration du réseau câblé et sur les obstacles juridiques à la prolongation des mandats relatifs à l'exploration du réseau câblé.

Séminaire à huis clos de l'AS-Rens et de la direction du SRC

Dans l'expertise Koller de mars 2013 sur le thème « Inspection des tâches, de l'organisation et des prestations de la surveillance des services de renseignement (surveillance SR) du DDPS », une recommandation stipule notamment qu'un séminaire à huis clos annuel réunissant l'autorité de surveillance et le SRC pourrait être le début d'un développement stratégique à plus long terme et de l'identification des (grands) risques politiques⁴³.

Après environ quatre ans de collaboration entre le SRC et l'AS-Rens, cette recommandation reste d'actualité, même dans un contexte qui a changé entre-temps, et a également été soutenue par le SRC. Le 2 novembre 2021, la direction élargie du SRC s'est entretenue avec l'AS-Rens. Le conseiller en renseignement de la cheffe du DDPS a également participé au séminaire à huis clos. L'objectif de cette première rencontre était de favoriser la compréhension mutuelle et l'acceptation, et de décider de la suite des opérations. En conclusion, il a été constaté que cet événement était utile et qu'il pourrait être judicieux de le renouveler en présence du nouveau directeur.

En 2021, la direction de l'AS-Rens s'est entretenue au moins une fois avec les personnes suivantes:

- Cheffe du DDPS
- Secrétaire général du DDPS
- Directeur/Directeur suppléant du SRC
- Chef du RM
- Chef du COE
- Collaboratrices et collaborateurs du PFPDT

⁴³ Expertise « Inspection des tâches, de l'organisation et des prestations de la surveillance des services de renseignement du DDPS », établie par le prof. Dr. iur. et lic. oec. Heinrich Koller, p. 55

La rencontre avec les intervenants du DFAE, du DFJP et du DDPS (qui siègent à la Délégation du Conseil fédéral pour la sécurité) a dû être reportée et n'a pas eu lieu en 2021.

Citoyens et citoyennes

En 2021, l'AS-Rens a reçu onze demandes de citoyens et citoyennes qu'elle a traitées et auxquelles elle a répondu.

7.2 Contacts internationaux

L'AS-Rens ne peut surveiller les activités de renseignement de la Suisse que jusqu'aux frontières nationales. Il n'existe actuellement aucune base légale qui règle l'échange de contenus avec des autorités partenaires. L'AS-Rens peut toutefois échanger avec celles-ci sur les méthodes, les processus et les expériences en matière de surveillance.

Rencontre virtuelle du 20 septembre 2021: Intelligence Oversight Working Group (IOWG)

Avant la pandémie, l'IOWG se réunissait deux fois par année pour échanger. Ce type d'échange ayant été possible pour la dernière fois en janvier 2020 en raison des restrictions liées au COVID-19, le groupe de travail s'est réuni une fois virtuellement afin de maintenir le contact et de clarifier les questions relatives à la poursuite du groupe de travail.

Rome, les 7 et 8 octobre 2021: European Oversight Conference

Le ministère public italien a lancé une invitation pour un échange international notamment sur les décisions judiciaires nationales et internationales. Les discussions ont surtout porté sur les conséquences de ces décisions sur les services de renseignement respectifs, mais aussi sur les organes de surveillance correspondants. Outre les représentants des organes de surveillance italiens, des délégués de l'Allemagne, de l'Autriche, de la Belgique, de la Bulgarie, du Danemark, de la France, de la Grèce, de la Grande-Bretagne, du Luxembourg, de la Norvège, des Pays-Bas, du Portugal et de la Suisse étaient présents.

Contacts internationaux

- Intelligence Oversight Working Group (IOWG)
Rencontre virtuelle du 20 septembre 2021

- European Oversight Conference Rom,
7 et 8 octobre 2021



8. Regard externe

Le rapport d'activités comprend également un regard externe sur le champ d'activités de l'AS-Rens. Dans le cadre du thème principal du rapport d'activités de cette année, à savoir les systèmes d'information, Adrian Lobsiger présente son point de vue sur la question.

Chances et risques de « l'évolution des mentalités » dus à la transformation numérique

Suite au « scandale des fiches » en 1989, la population suisse a brusquement perdu confiance dans la protection de l'État. Après avoir fait toute la lumière sur le traitement des données, appelé « fichage », par la police fédérale (alors connue sous l'acronyme allemand « Bupo » pour Bundespolizei), les politiques ont exigé une séparation des multiples tâches de cette autorité de sécurité. Le Conseil fédéral et le Parlement, en conflit avec les partisans d'une initiative visant à supprimer complètement la protection de l'État, qui n'était jusqu'alors réglementée que de manière rudimentaire, ont mis en route un processus de codification de celle-ci. Une première votation populaire en 1998 a tout d'abord permis la poursuite de l'activité de protection de l'État, désormais formellement réglementée par la loi. En 2016, un deuxième référendum ouvre la voie à l'adoption de l'actuelle loi fédérale sur le renseignement (LRens) et autorise désormais le Service de renseignement de la Confédération (SRC) à recourir à des moyens coercitifs pour collecter des données personnelles, mesure généralement exécutée secrètement et à l'insu des personnes concernées. Cet abandon de l'interdiction initiale de recourir à la contrainte a notamment incité le législateur à créer une autorité de surveillance spécialisée indépendante qui se consacre exclusivement au SRC.

Même si les avis divergent toujours quant à la surveillance par le SRC, les opposants doivent aussi admettre que, depuis l'entrée en vigueur de la LRens, le traitement des données par la protection de l'État s'appuie sur une base légale suffisamment déterminée et claire du point de vue de la systématique juridique. En revanche, par rapport au traitement de données personnelles également très sensible qui émane d'autres autorités de sécurité de la Confédération, le but d'une codification compréhensible par les citoyens est encore loin d'être réalisée. Ainsi, le traitement des données par fedpol et le Corps des gardes-frontière découle d'une multitude de dispositions spéciales mal coordonnées du point de vue de la systématique juridique, en constante augmentation.

La représentation du traitement des données personnelles dans la loi, intelligible pour les citoyens, est encore compliquée par les vastes projets de transformation numérique qui ont été entrepris entre-temps au sein des autorités de sécurité de la Confédération. Comme ces projets peuvent entraîner des modifications importantes des processus de traitement des données personnelles, la surveillance fédérale de la protection des données veille à ce que ces processus soient entièrement recensés dès le stade de la planification au moyen d'analyses d'impact sur la protection des données, et à ce que leurs conséquences sur la sphère privée de la population soient analysées.

Dans sa stratégie de transformation numérique de l'administration, le Conseil fédéral revendique une « évolution des mentalités » qui remet en question les formes traditionnelles de cohabitation et de gestion. Une évolution qui développe des compétences numériques



Adrian Lobsiger (*1959)

Après ses études à Berne et Bâle, Adrian Lobsiger, né le 27.12.1959, a obtenu un master en droit européen à Exeter (GB). En 1992, titulaire d'un doctorat en droit, il a commencé à travailler à l'Office fédéral de la justice dans le domaine du droit privé international. En 1995, il est entré à l'Office fédéral de la police (fedpol), où il devient directeur suppléant.

Adrian Lobsiger a été élu par le Conseil fédéral au poste de Préposé fédéral à la protection des données et à la transparence (PFPDT) en novembre 2015 et confirmé par le Parlement en mars 2016. Il est en fonction depuis juin 2016. Lors de sa séance du 10 avril 2019, le Conseil fédéral a confirmé la réélection d'Adrian Lobsiger au poste de PFPDT pour un second mandat arrivant à terme à fin 2023.

permettant la mise en réseau ainsi que le partage de données entre tous les acteurs. Les mots suscitent des images. C'est pourquoi certains promoteurs du changement numérique voient dans leur esprit un cloud dont les corps de police, les gardes-frontière et les services de renseignement se serviraient pour le bien de celles et ceux qui respectent la loi et n'ont rien à cacher.

Pour les partisans de cette vision, aux antipodes figure le maintien réprouvé des données dans ce qu'ils appellent des « silos », qui représentent les vestiges d'une pensée dépassée et que certains d'entre eux attribuent volontiers au stéréotype d'une protection des données qui favorise les auteurs de crimes au lieu de protéger les citoyens. Ces visionnaires désapprouvent également le fait que les cantons entretiennent des corps de police qui traitent les données personnelles qui y sont produites sous leur propre responsabilité et ne les partagent en général avec d'autres autorités de sécurité que sur demande. Ils reprochent aussi à la Confédération de répartir ses forces de police entre trois offices. En tant que détracteurs jurés des silos de données, ils voient dans cette réalité un problème qu'ils encouragent à éliminer, en mettant en réseau toutes les autorités de sécurité dans la mesure de ce qui est techniquement possible.

Quiconque fait abstraction des faits historiques qui ont incité les constituants à organiser les collectivités publiques de manière fédérale et à répartir le pouvoir de l'État central peut, en effet, avoir du mal à interpréter rationnellement la complexité des flux de données des autorités de sécurité. Une réflexion historique permet en revanche de comprendre que le système de sécurité intérieure de la Suisse est issu d'une succession de décisions de ses institutions politiques, que le peuple a l'habitude d'influencer directement par des référendums. C'est ce qui s'est passé, par exemple, en 1978 avec le succès du référendum contre la création d'une police fédérale de sécurité, qui peut être compris encore aujourd'hui comme un veto jamais révoqué contre une autorité centrale de sécurité au niveau de la Confédération.

Une « nouvelle mentalité et manière de penser », qui considère la mise à disposition numérique des données personnelles comme la mesure de toute chose et qui occulte les concepts politiques de limitation du pouvoir de l'État, n'est pas progressiste, mais rétrograde. Elle ramène à l'État policier qui a été aboli avec le dépassement des aristocraties absolutistes par les mouvements révolutionnaires des 18^e et 19^e siècles. La division de l'appareil de pouvoir omnicompétent de l'Ancien Régime en offices spécialisés a largement contribué à transformer l'État policier en service public et les sujets en citoyennes et citoyens conscients de leur valeur, qui exigent des offices spécialisés des prestations professionnelles et discrètes en échange des taxes versées.

Le professionnalisme exigé de l'administration en tant que fournisseur de prestations implique depuis lors que ses services spécialisés ne partagent les données des citoyens qu'ils produisent avec d'autres services que dans le cadre de procédures légales. Le fait que l'administration fédérale traite aujourd'hui les données de manière à les rendre lisibles par machine et à en permettre une utilisation interdisciplinaire peut également être considéré comme une

expression de professionnalisme. Il en va de même lorsqu'elle saisit des données de base et des attributs personnels selon le principe « once only » et qu'elle les gère en utilisant des identifiants uniformes tels que le numéro AVS. La protection des données ne s'oppose pas à de telles étapes de numérisation visant à accroître l'efficacité du service public, d'autant plus qu'elles peuvent également contribuer à améliorer la qualité des données.

En revanche, quiconque chercherait à créer, par le biais d'interconnexions non transparentes, une sorte de cloud dans lequel les autorités de sécurité, l'inspection des impôts et d'autres services de l'administration restrictive pourraient puiser toutes les données générées par les échanges entre la population et l'administration en tant que fournisseur de prestations naviguerait sur une trajectoire conflictuelle avec la protection des données. Une telle pêche aux données ébranlerait rapidement la confiance des citoyennes et des citoyens dans le rôle de l'État en tant que service public et garant de l'État de droit. Pour éviter cela, la surveillance fédérale de la protection des données exige des responsables de projets de transformation numérique qu'ils déclarent dans les analyses d'impact sur la protection des données l'étendue et l'intensité d'un futur traitement de données ainsi que le cercle des services autorisés à y accéder, et qu'ils les comparent avec le statu quo. Si des extensions et des intensifications du traitement actuel des données personnelles sont envisagées, elles doivent être justifiées.

Les offices fédéraux rétorquent parfois au préposé que les projets de transformation numérique doivent être planifiés de manière « agile » en raison de la rapidité des progrès techniques et qu'il ne serait donc pas possible de délimiter définitivement les traitements futurs ni de les comparer à un statu quo. De tels raisonnements sont intenable. Ils reviennent à donner une autorisation générale à l'administration, car ni les organes politiques, qui doivent assumer la responsabilité politique des interventions des autorités dans la sphère privée de la population, ni le grand public ne peuvent évaluer les risques « agiles ». Dans sa pratique, le préposé est régulièrement amené à faire en sorte que les analyses d'impact relatives à la protection des données soient précisées et complétées avant que leurs résultats ne soient intégrés dans les messages par lesquels le Conseil fédéral propose au législateur d'adapter les actes législatifs relatifs à la sécurité.

Au vu de ces défis, le préposé s'estime heureux que son travail dans le domaine du renseignement soit complété par l'autorité indépendante de surveillance du SRC.

9. Chiffres clés au 31 décembre 2021



Collaborateurs

1.1.2021
31.12.2021
Résiliations

10
9
4



Inspections

Inspections planifiées **18 (18)**
Inspections non annoncées **0 (1)**
Inspections réalisées **18 (17)**

Nombre d'entretiens réalisés

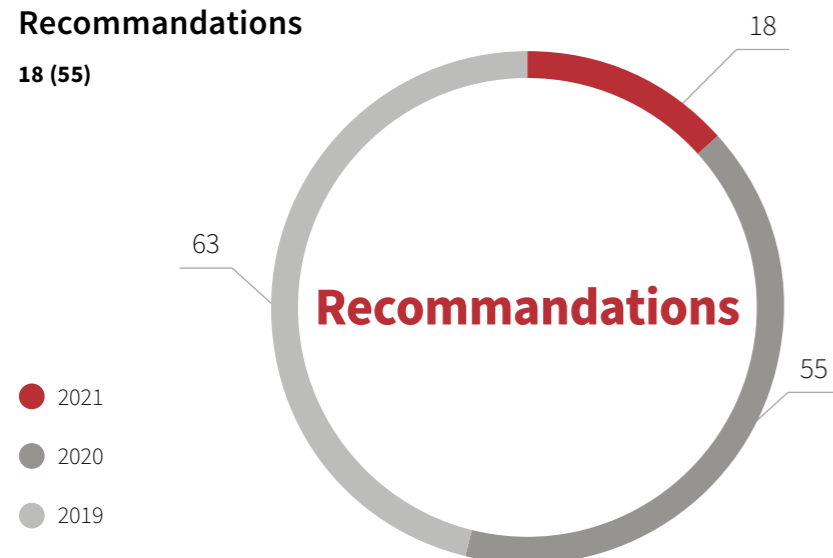
90 (102)

Effectif budgété

10 postes

Recommandations

18 (55)



10. Annexe

10.1 Plan des inspections 2021

No	Titre	Organe inspecté
Stratégie et planification		
21-1	Engagement de collaboratrices et de collaborateurs du SRC ¹ dans les représentations suisses l'étranger	SRC
Organisation		
21-2	Protection des infrastructures critiques / cyberdéfense	SRC / COE ²
21-3	Sécurité au sein du SRC	SRC
21-4	Extrémisme violent de droite	SRC
Collaboration		
21-5	Assurance qualité du SRC auprès des services de renseignement cantonaux (SRCant)	SRC
21-6	Inspection du SRCant BS	SRC / SRCant
21-7	Inspection du SRCant BL	SRC / SRCant
21-8	Inspection du SRCant AR	SRC / SRCant
21-9	Inspection du SRCant AI	SRC / SRCant
21-10	Inspection du SRCant AG	SRC / SRCant
21-11	Inspection du SRCant VD	SRC / SRCant
21-12	Inspection du SRCant NE	SRC / SRCant
Recherche d'informations		
21-13	Gestion du risque pour les engagements à l'étranger	SRC
21-14	Opérations	SRC
21-15	HUMINT ³	SRC
Ressources		
	Pas d'inspection prévue	
Traitement des données / archivage		
21-16	Services de télécommunication	SRC
21-17	Système d'information du SRC sélectionné (Quattro P ⁴)	SRC
21-18	Protection des données au sein du RM ⁵	RM

¹ Service de renseignement de la Confédération

² Centre des opérations électroniques

³ Human Intelligence, recherche de renseignements par des informateurs

⁴ Article 55 de la Loi fédérale sur le renseignement (loi sur le renseignement, LRens ; RS 121)

⁵ Renseignement militaire

10.2 Abréviations

ACS Autorités cantonales de surveillance	FF Feuille fédérale	Quattro P Système d'information du SRC qui sert à identifier certaines catégories de personnes étrangères qui entrent en Suisse
AD Attaché de défense	GEVER Système de gestion des affaires	resp. Respectivement
al. Alinéa	HUMINT Human Intelligence, recherche d'informations par des sources humaines	RI DDPS Révision interne DDPS
AQ SRC Assurance qualité du SRC	IASA SRC Système d'analyse intégrale du SRC	RM Renseignement militaire
art. Article	Ik MND Système informatique du Renseignement militaire	RS Recueil systématique du droit fédéral
AS-Rens Autorité de surveillance indépendante des activités de renseignement	IOWG Intelligence Oversight Working Group	SG Secrétariat général
BS Bâle-Ville	JCTAC Joint Cyber Technical Analysis Center	SiLAN Stockage de données dans le réseau sécurisé du SRC
BURAUT Stockage des données du SRC	LPD Loi fédérale sur la protection des données (RS 235.1)	SRC Service de renseignement de la Confédération
CDF Contrôle fédéral des finances	LRens Loi fédérale sur le renseignement (RS 121)	SRCant Service de renseignement cantonal
ch. Chiffre	MELANI Centrale d'enregistrement et d'analyse pour la sûreté de l'information	ss Suivantes
COE Centre des opérations électroniques	MRSA Mesures de recherche soumises à autorisation	TAF Tribunal administratif fédéral
Cyber Synonyme de monde des données et d'Internet	OCI Organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé	
DDPS Département fédéral de la défense, de la protection de la population et des sports	OPAB Enquêtes opérationnelles	
DéICdG Délégation des Commissions de gestion	OSIS-SRC Ordonnance sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (RS 121.2)	
EPT Équivalent plein temps, quantité auxiliaire pour la mesure du temps de travail	p. ex. Par exemple	
EXTR Extrémisme violent	PFPDT Préposé fédéral à la protection des données et à la transparence	
FA KND Application spécialisée des services de renseignement cantonaux		
fedpol Office fédéral de la police		



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

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