Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Autorité de surveillance indépendante
des activités de renseignement AS-Rens**

Rapport d'activités 2025

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

1 Résumé

Par le présent rapport d'activités, l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) présente son travail effectué au cours de l'année 2025. Celle-ci restera marquée par le changement de Chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS) et de Directeur du Service de renseignement de la Confédération (SRC).

L'AS-Rens a mené ses inspections selon une approche fondée sur les risques, couvrant la stratégie, l'organisation, la collaboration, la recherche d'informations, les ressources et le traitement des données. Elle était présente auprès de toutes les autorités soumises à sa surveilllance, à savoir le SRC, le service Actions dans le cyberspace et dans l'espace électromagnétique (ACEM), le Renseignement militaire (RM) et le Service pour la protection préventive de l'armée (SPPA).

En 2025, l'AS-Rens a intensifié la publication des résultats d'inspection et renforcé la transparence de son activité. Les inspections ont porté notamment sur les technologies de l'information (inventaire et portefeuille de projets), la lutte contre l'extrémisme violent de gauche, la prévention de l'espionnage interne, la collaboration du SRC avec d'autres autorités ou les services cantonaux de renseignement, l'utilisation d'agentes et d'agents virtuels (VirtA), les opérations impliquant des mesures de recherche soumises à autorisation (MRSA) ainsi que la gestion des informatrices et informateurs (HUMINT).

Dans le domaine du traitement des données, l'année 2025 a surtout été marquée par la clotûre de l'inspection 22-18 qui donnait suite aux différentes enquêtes menées dans le domaine cyber du SRC. L'AS-Rens a également examiné des systèmes clés comme le système d'information et d'analyse intégrale de l'application Allsource Control (IASA-ICC) et les consultations de systèmes de tiers. Elle a constaté une amélioration progressive, mais aussi des lacunes persistantes, surtout en matière de documentation, de conformité technique et de gestion des accès. L'AS-Rens a formulé plusieurs recommandations, par exemple sur la clarification des règles pour les VirtA, la prévention des risques d'espionnage interne, l'inventaire des technologies d'information et de communication (TIC) ou encore le stockage des données collectées par l'exploration du réseau câblé. L'AS-Rens a aussi relevé certains risques pour la conduite et les processus en lien avec la transformation du SRC.

En parallèle, l'AS-Rens a entretenu un dialogue constant avec ses différents partenaires. Au niveau national, elle a mis en évidence des besoins accrus d'échange d'expériences, notamment avec les cantons. Les échanges internationaux ont été marqués par l'organisation en Suisse de trois jours de conférences.

2 Table des matières

1 Résumé 2
2 Table des matières 3
3 Chiffres-clés au 31 décembre 2025 4
4 Note personnelle 5
5 Activités de surveillance 6
5.1 Plan des inspections 6
5.2 Inspections de l'année 2025 6
5.2.1 Stratégie et planification 6
5.2.2 Organisation et mandat 8
5.2.3 Collaboration 10
5.2.4 Recherche d'informations 12
5.2.5 Ressources 15
5.2.6 Traitement des données et archivage 16
5.3 Accueil 21
5.4 Mise en œuvre des recommandations 22
6 Regard interne 23
6.1 Personnel 23
6.2 Formations et perfectionnements 23
6.3 Accès à des informations et documents officiels 23
7 Coordination 23
7.1 Contacts nationaux 23
7.2 Contacts internationaux 25
8 Annexe 28
8.1 Plan des inspections 2025 28
8.2 Liste des abréviations 29

3 Chiffres-clés au 31 décembre 2025

Membres du personnel	01.01.2025	**10**
	31.12.2025	**10**
Inspections en cours au 01.01.2025		**10**
Inspections commencées en 2025		**11**
Inspections closes en 2025		**16**
Inspections en cours au 31.12.2025		**5**
Inspections planifiées		**11**
Inspections inopinées		**1**
Recommandations		**28**

4 Note personnelle

Chères lectrices et chers lecteurs,

L'année 2025 a été très particulière pour l'AS-Rens. En effet, la finalisation du rapport « Cyber » en février a été un moment spécial, marqué à la fois par des difficultés et un grand soulagement. La communication externe sur le contenu du rapport s'est avérée difficile car, après plus de deux ans de travail, nous avons voulu qu'elle soit aussi exhaustive que possible. La finalisation de l'inspection nous a également soulagés étant donné qu'elle a mobilisé beaucoup plus de ressources que toutes les inspections précédentes.

Heureusement, la surveillance ne se limite pas à un seul rapport et ne se concentre pas sur un thème particulier. **Grâce à des programmes annuels variés, aux inspections passées et à la situation actuelle, l'expérience de l'AS-Rens continue de se développer, tout comme sa capacité à identifier les problèmes et les progrès dans leur ensemble.** En 2025, le SRC a consolidé certains secteurs auparavant fragiles et a poursuivi ses efforts pour améliorer son organisation. Dans ce contexte, la surveillance a dû s'adapter régulièrement aux changements. Le Service de renseignement de l'armée (SRA) a également réfléchi à l'évolution des besoins et des risques, et donc aussi de son organisation. La surveillance doit ici aussi suivre le rythme des changements. Malheureusement, ce n'est pas toujours facile, raison pour laquelle une inspection du SRA, commencée à l'été 2025, n'est pas encore achevée, les changements organisationnels se prolongeant jusqu'en 2026.

Dans ce rapport annuel, vous trouverez des informations sur toutes les inspections closes et en cours. Je vous invite à vous concentrer sur la diversité des thèmes abordés qui concernent le quotidien de toutes les citoyennes et de tous les citoyens. À la fin de votre lecture, posez-vous la question suivante : « Ai-je obtenu satisfaction ? ». De notre côté, nous ne nous contentons jamais de ce qui a été accompli et nous continuons à aller de l'avant. Si vous avez un avis sur nos réflexions, n'hésitez pas à nous écrire.

Je vous souhaite une bonne lecture.

Meilleures salutations,

Prisca Fischer, cheffe de l'AS-Rens

5 Activités de surveillance

5.1 Plan des inspections

L'AS-Rens effectue ses inspections en fonction des risques dans les domaines suivants :

- stratégie et planification
- organisation et mandat
- collaboration
- recherche d'informations
- ressources
- traitement des données et archivage

Le plan des inspections est établi de sorte que chaque domaine soit couvert par au moins une inspection.

5.2 Inspections de l'année 2025

L'AS-Rens continue à faire évoluer son rapport d'activités et celui de 2025 contient quelques adaptations :

- Les résumés des inspections closes au 31 décembre 2025 sont publiés dans le rapport d'activités. Pour les inspections en cours, seul l'objectif de l'inspection est présenté.

- Toutes les inspections débutées sont précédées d'un tableau qui contient trois informations temporelles : la date du début de l'inspection (mandat), la date de l'envoi du projet de rapport pour prise de position des services examinés (consultation) et la date d'envoi du rapport définitif. Enfin, le tableau comporte deux autres informations relatives au nombre de recommandations prononcées et au nombre d'entretiens (oraux ou écrits) qui ont eu lieu jusqu'au 31 décembre 2025.

5.2.1 Stratégie et planification

Dans le domaine « Stratégie et planification », l'AS-Rens examine des thèmes qui touchent à la planification stratégique à court, moyen et long terme des autorités du renseignement suisses et à leurs objectifs. Durant l'année sous revue, l'AS-Rens s'est attelée aux inspections ci-après.

24-1 Intelligence artificielle (IA) au SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
19.09.2025				5

L'AS-Rens examine, sous l'angle de la légalité, de l'efficacité et de l'adéquation si le SRC acquiert, utilise et contrôle correctement cette technologie.

25-1 Lutte contre l'extrémisme violent de gauche par le SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
25.02.2025	16.07.2025	18.08.2025	1	8

L'AS-Rens a décidé d'inspecter les activités du SRC dans le domaine de la lutte contre l'extrémisme violent de gauche après s'être penchée sur la lutte contre l'extrémisme violent de droite par le SRC en 2021.

Elle a entendu des cadres et des membres du personnel du SRC qui agissent dans ce domaine ainsi que des représentantes et représentants de deux services de renseignement cantonaux et une personne de l'encadrement de l'Office fédéral de la police (fedpol). Elle a également mené un contrôle par échantillonnage dans les mandats de recherche d'informations que le SRC confie à ses propres capteurs ou à ses partenaires. Une clarification des besoins opérationnels a aussi été prise en compte.

L’objectif était d’établir une vue d’ensemble des activités du SRC dans la lutte contre l’extrémisme violent de gauche.

Une attention particulière a été portée au cadre légal de ces activités en vérifiant que les droits fondamentaux des personnes cibles soient respectés comme prévu dans la loi sur le renseignement (LRens). En effet, la collecte d’informations dans le domaine de l’extrémisme violent est soumise à des règles strictes qui permettent, par exemple, au SRC de traiter des informations seulement lorsqu’elles ont un lien avec le recours à la violence. Cette mesure vise à garantir l’exercice des droits fondamentaux de la population suisse. C’est pourquoi le SRC n’est pas autorisé à engager des MRSA dans ce contexte.

Le développement de la scène d’extrême gauche violente a aussi été pris en compte avec la possibilité que certains groupements soient appréhendés sous l’angle de la lutte contre le terrorisme. Cette possibilité existe et est compatible avec le cadre légal actuel, à condition que certains critères soient remplis. L’AS-Rens a constaté que le SRC a établi une pratique adaptée dans ce domaine, qui lui permet de fonder une demande d’autorisation aux autorités politiques et judiciaires dans de tels cas.

L’AS-Rens a également évalué si le SRC remplissait le mandat qui lui est confié dans le domaine de la lutte contre l’extrémisme violent de gauche. Ce mandat comprend notamment la collecte d’informations dans le but d’empêcher la réalisation des menaces liées à la violence de l’extrême gauche ainsi que le monitoring de la situation. Le rôle du SRC vis-à-vis de ses partenaires nationaux a aussi été abordé et une dégradation de la collaboration a été constatée. Le SRC a procédé au recrutement de personnes supplémentaires durant la période d’inspection. **L’AS-Rens est tout de même arrivée à la conclusion qu’au vu des ressources limitées et en considération de l’évaluation de la menace qui émane actuellement de l’extrême gauche violente en Suisse, le SRC n’est pas en mesure d’accomplir son mandat de manière optimale.** En effet, le SRC n’exploite pas l’intégralité des moyens conférés par la loi sur le renseignement, posant ainsi un problème d’adéquation et d’efficacité. Une recommandation a donc été formulée.

25-2 Portefeuille de projets informatiques du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d’entretiens
21.07.2025	14.11.2025	09.12.2025	0	11

Un portefeuille de projets informatiques permet notamment de recenser toutes les informations relatives aux projets en cours ou prévus dans le domaine des technologies de l’information d’une unité administrative. La gestion des projets ou d’autres études internes peut être facilitée grâce à cet outil.

Au sein du SRC, un projet peut notamment répondre à de nouveaux besoins informatiques en matière d’acquisition, de traitement, d’analyse ou de transmission d’informations issues des activités de renseignement. Il existe différents risques pour le SRC dans ce contexte. Des déficits au niveau de l’exhaustivité de la vue d’ensemble, une transmission inadéquate des informations aux échelons supérieurs ou un manque de coordination aboutiraient à une réalisation inadéquate et inefficace desdits projets.

L’AS-Rens a donc vérifié si le SRC dispose d’un tel portefeuille et a examiné la manière dont il est géré. Elle a ainsi évalué si le service dispose d’une vue d’ensemble de tous ses projets informatiques et la manière dont les échelons décisionnels supérieurs reçoivent les informations clés. L’AS-Rens a aussi vérifié si la coordination des projets permet une identification efficace des synergies et des doublons.

Le SRC a récemment développé un concept innovant pour la gestion de portefeuille de projets. Il y inclut les projets informatiques ou d’autres types de projets assortis d’une composante stratégique pour le service. Il a aussi créé un organe spécifique qui permet d’évaluer et de prioriser la réalisation des besoins stratégiques identifiés. Les processus mis en place permettent à la direction du SRC de disposer d’informations clés issues des grands projets informatiques et d’assumer ainsi ses responsabilités dans ce contexte. Les projets informatiques sans composante stratégique ne sont pas

intégrés au portefeuille et ne sont donc pas toujours portés à l'attention de la direction du SRC. Ainsi, le SRC ne dispose pas actuellement d'une vue d'ensemble exhaustive de son portefeuille de projets qui inclut des projets informatiques aussi bien stratégiques qu'opérationnels. De ce fait, l'AS-Rens a observé des manquements en matière d'identification efficace des synergies et des doublons. L'AS-Rens a constaté que le SRC a déjà identifié des améliorations pour la gestion de son portefeuille de projets informatiques et qu'il travaille concrètement à leur mise en œuvre. L'AS-Rens juge ces travaux pertinents et n'a pas formulé de recommandation.

5.2.2 Organisation et mandat

Dans le domaine « Organisation et mandat », l'AS-Rens examine la structure des services de renseignement et leurs processus de travail en se posant notamment la question de savoir s'ils permettent aux autorités concernées de remplir leur mandat légal dans le respect du droit, de manière efficace et adéquate. En 2025, l'AS-Rens a mené les inspections ci-après dans ce domaine.

24-2 Activités de renseignement du SPPA

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
06.08.2025				1

L'AS-Rens examine les recoupements dans la collaboration entre le SRC et le SPPA afin d'identifier les activités de renseignement soumises à sa surveillance. Elle utilise cette base pour examiner la légalité, l'efficacité et l'adéquation de cette collaboration.

24-11 Mesures de sécurité selon la LRens

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
16.10.2024	27.02.2025	25.03.2025	0	2

Le SRC est tenu de veiller à la sécurité de ses collaboratrices et collaborateurs, des données traitées ainsi que de ses installations. L'AS-Rens a vérifié, sur certains postes de travail, si le SRC respecte cette obligation et a pris les mesures de sécurité adéquates. Ces postes de travail ont été créés sur la base d'un concept justifiant leur nécessité et d'une analyse des forces, des faiblesses, des opportunités et des risques d'un tel projet. Le projet poursuit trois objectifs : renforcer la coopération, l'agilité / l'attractivité du SRC et la gestion de la continuité opérationnelle (Business Continuity Management, BCM). La mise en œuvre s'est déroulée progressivement et s'est achevée en janvier 2025.

L'AS-Rens a participé à la formation interne et a visité les lieux de travail. Sur la base des entretiens et de la documentation, elle a constaté que la sécurité des membres du personnel du SRC et des données traitées était une priorité lors de la mise en œuvre. Les objectifs fixés sont atteints (BCM) ou sont réalisables. Les moyens utilisés sont adéquats. Le SRC continuera à surveiller l'utilisation des postes de travail et améliorera, si nécessaire, les mesures de sécurité. Dans certains domaines, il en évaluera l'efficacité à un moment opportun. L'AS-Rens n'a émis aucune recommandation.

L'inspection ne figurait pas sur le plan des inspections 2024 de l'AS-Rens. L'urgence de sa mise en œuvre a découlé de la mise en service de ces postes de travail.

25-3 Lutte contre l'espionnage au sein du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
29.04.2025	03.09.2025	30.09.2025	3	8

La menace d'espionnage en Suisse en lien avec l'aggravation de la situation géopolitique s'est accrue. En parallèle, la frustration des collaboratrices et collaborateurs du SRC durant la transformation de ce service a également augmenté. L'AS-Rens estime que ces deux facteurs créent un risque important pour les activités de renseignement car la frustration du personnel peut entre autres être instrumentalisée par des services de renseignement étrangers dans le but de dérober des informations

classifiées ou d'influencer les institutions politico-sécuritaires suisses. Plusieurs recommandations visant à renforcer les mesures d'autoprotection du SRC ont été formulées par l'AS-Rens par le passé, elles ont été prises en compte dans la présente inspection.

L'AS-Rens a voulu clarifier le cadre légal en matière de prévention de l'espionnage au sein du SRC et évaluer si les dispositions existantes à cet effet sont appropriées. Au moment de l'inspection, le DDPS poursuivait le développement de ses directives sécuritaires, notamment en matière de protection de l'information. Ceci implique que le SRC, en tant qu'office du DDPS, devra bientôt appliquer ces règles et, le cas échéant, adapter ses propres directives. Entre-temps, l'AS-Rens estime que les directives internes et les mesures prises par le SRC entrent dans le cadre légal en vigueur. Le SRC s'appuie aussi sur la révision de la LRens pour développer certaines mesures de son dispositif sécuritaire suite à la constatation de lacunes. Cette démarche est perçue de manière positive par l'AS-Rens.

Le traitement de cas de soupçons d'espionnage est souvent multidimensionnel. En effet, des aspects de conduite du personnel et des problématiques purement sécuritaires peuvent se mélanger. Ceci implique que plusieurs actrices et acteurs doivent se coordonner pour appréhender un cas dans son ensemble. L'AS-Rens a pu constater que la communication entre les différentes parties prenantes au sein du service (sécurité, ressources humaines, supérieures et supérieurs directs ou direction) est désormais prévue et possible. Toutefois, le SRC peut encore augmenter sa vigilance lors du traitement des cas concrets. En effet, il peine à adopter une ligne stricte, même lorsqu'il existe des indices de risque pour certains membres du personnel. L'AS-Rens a donc formulé une recommandation à ce sujet.

Lors du recrutement, le SRC et le Service spécialisé des contrôles de sécurité relatifs aux personnes du Secrétariat d'État à la politique de sécurité (SEPOS) effectuent un important travail de vérification. Les constatations de la révision interne du DDPS en lien avec ces contrôles de sécurité relatifs aux personnes ont été prises en compte dans le cadre de cette inspection. Il en ressort que le SRC peut encore apporter quelques améliorations à la procédure suivie actuellement. L'AS-Rens a formulé une recommandation en ce sens.

Durant la période d'engagement des collaboratrices et collaborateurs au sein du service ou lors de la rupture des rapports de travail, peu de mesures sont prises spécifiquement en vue de réduire le risque d'espionnage. Bien que d'importants efforts aient déjà été réalisés en matière de sécurité, l'AS-Rens attend du SRC qu'il continue d'identifier les lacunes et de renforcer son programme de formation continue et de sensibilisation à l'interne. L'AS-Rens a formulé une recommandation sur des risques sécuritaires spécifiques constatés.

Les démarches du SRC dans le cas d'une collaboratrice ou d'un collaborateur du DDPS en poste à l'étranger dont le comportement pourrait s'apparenter à de l'espionnage ont été prises en compte dans cette inspection. L'AS-Rens a analysé plusieurs incidents de sécurité survenus au sein du SRC entre 2023 et juillet 2025 et aucun cas d'espionnage n'a été détecté en lien avec un ou une membre du personnel du SRC. Toutefois, dans le contexte du conflit hybride actuel, il n'est pas possible d'exclure que les fuites d'informations dans la presse qui ont eu lieu à plusieurs reprises avant et durant l'inspection soient malgré tout instrumentalisées en vue de déstabiliser les institutions. L'AS-Rens salue le fait que le SRC s'adresse aux autorités de poursuite pénale dans ces cas-là.

25-5 Prestations de traduction au SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
29.07.2025				18

L'AS-Rens vérifie si les services de traduction (sélectionnés) sont utilisés de manière appropriée et efficace, si la sécurité des informations est garantie et si le service a mis en place des mesures de contrôle et d'assurance qualité efficaces.

5.2.3 Collaboration

Dans le domaine « Collaboration », l'AS-Rens examine la collaboration des services avec les autorités nationales et internationales. Elle examine aussi la collaboration entre les services de renseignement fédéraux et les services de renseignement cantonaux (SRCant).

En 2025, l'AS-Rens a procédé à des actes dans les inspections suivantes.

24-4 Collaboration du SRC avec le Secrétariat d'État aux migrations (SEM)

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
17.05.2024	18.12.2024	23.01.2025	1	15

L'AS-Rens a examiné la collaboration du SRC avec le SEM. Ces deux autorités ont leurs propres tâches et compétences légales en matière de sécurité intérieure et extérieure de la Suisse. Le SRC accomplit les tâches mentionnées dans la loi sur le renseignement. Le SEM a un champ d'activité très large, à savoir le domaine de la migration, qui couvre tant les entrées et le séjour des étrangers que l'asile, la naturalisation, les visas, etc. Chaque domaine ou presque est régi par une loi et des ordonnances ad hoc. Les compétences des deux autorités fédérales peuvent se recouper dans la mesure où une personne relevant du droit des migrations peut également relever du domaine de compétence du SRC, et inversement. Par exemple, dans le cadre de ses compétences, le SEM doit traiter une demande de naturalisation faite par une personne soupçonnée d'espionnage au profit de son État d'origine, la lutte contre l'espionnage relevant de la compétence du SRC. Le SRC et le SEM sont donc amenés à collaborer dans un certain nombre de domaines, par exemple en matière de droit des étrangers, d'asile, des visas ou des naturalisations.

L'AS-Rens a principalement examiné le risque que les deux autorités ne se coordonnent pas (suffisamment) ou suivent des intérêts divergents ou incompatibles, ce qui ne leur permettrait pas d'accomplir efficacement et adéquatement leurs tâches respectives. Les risques en termes de légalité, d'efficacité et d'adéquation de la collaboration ont aussi été pris en compte. Cette collaboration se traduit également par des échanges de données qui comprennent également plusieurs risques.

D'un point de vue stratégique, les deux autorités n'ont pas de stratégie commune à proprement parler. La coordination se fonde principalement sur la liste non publique établie par le Conseil fédéral. Cette liste indique notamment les événements et les constatations qui doivent être communiqués spontanément au SRC. Les deux autorités considèrent que cette liste est suffisante, un avis partagé par l'AS-Rens. Elle a prononcé une recommandation relative aux aspects stratégiques de la collaboration entre le SRC et le SEM et au développement interne du SRC.

Sous l'angle opérationnel, l'AS-Rens a constaté que les deux autorités collaborent de manière conforme au droit. Elles ont développé ces dernières années une compréhension mutuelle de leurs capacités, mais aussi de leurs contraintes respectives, en particulier juridiques. Les deux autorités connaissent le cadre légal. **L'AS-Rens a pu constater que le SRC maîtrise sa marge d'appréciation et l'utilise à bon escient.** Son travail consiste principalement à chercher une aiguille dans une botte de foin. Heureusement, comme il l'a admis lui-même, il y a plus de foin que d'aiguilles. Le SEM et le SRC sont tous deux d'avis que la collaboration fonctionne à l'entière satisfaction des deux parties et aucune divergence d'intérêts n'a été constatée. Les informations échangées sont utiles et permettent aux deux autorités de mettre en œuvre leur mandat légal. La collaboration est, en l'état, adéquate et efficace. Les deux autorités échangent afin d'améliorer certains aspects techniques. L'AS-Rens a constaté que l'unité compétente du SRC a tenu le cap malgré la transformation en cours.

L'AS-Rens a procédé à trois échantillonnages de données. Le premier a porté sur 40 dossiers ouverts en 2024 dans le système d'information GEVER SRC. Il a permis de constater que le SRC traite les dossiers de manière conforme au droit. Des défauts mineurs en matière de documentation ont été corrigés au cours de l'inspection. Le deuxième échantillonnage a concerné l'examen de 133 journalisations de consultation de données dans le système d'information central sur la migration (SYMIC) par le SRC. Ces consultations de données étaient conformes au droit. Enfin, le troisième

échantillonnage a porté sur les délais de conservation des données « Advance Passenger Information (API) ». Les délais de conservation des données API étaient respectés.

25-6 Collaboration du SRC avec les SRCant

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
15.05.2025	01.10.2025	04.12.2025	0	8

Le SRC et les organes cantonaux d'exécution (les services de renseignement cantonaux, SRCant) ont pour mission de contribuer de manière substantielle à la sauvegarde des intérêts de la Suisse et à la sécurité intérieure et extérieure du pays, tout en respectant les droits fondamentaux des citoyennes et des citoyens. Ils doivent recueillir les informations nécessaires à l'aide de moyens et de méthodes propres aux services de renseignement (c'est-à-dire en utilisant des sources d'information publiques et non publiques), les traiter, les évaluer et les transmettre sous une forme appropriée, en particulier aux décideuses et décideurs politiques (Confédération et cantons).

L'AS-Rens a visité tous les SRCant et toutes les autorités cantonales de surveillance en 2024-2025. Elle s'est renseignée sur la collaboration entre le SRC et les SRCant. Elle a ensuite examiné dans la présente inspection comment le SRC remplit ses obligations légales envers les SRCant. Ces obligations concernent en particulier la vérification du stockage des données des SRCant, la mise à disposition de moyens techniques et la formation du personnel.

Des risques tels qu'un manque de coopération, une communication perturbée, des attentes injustifiées ou une répartition inappropriée des tâches compliquent ou empêchent l'application de la loi sur le renseignement et compromettent la sécurité intérieure et extérieure. L'AS-Rens a donc vérifié si de tels risques existaient.

L'AS-Rens a pu constater que le SRC avait pris un large éventail de mesures et de dispositions visant à améliorer la collaboration avec les cantons. Celles-ci concernent notamment les domaines de la communication, de la formation et des activités opérationnelles.

Communication

Le SRC communique avec les SRCant en utilisant de nombreux formats, dont certains sont nouveaux. Le SRC va évaluer tous les formats et veiller à ce qu'il n'y ait pas d'offre excédentaire. Il convient de mentionner les travaux du panel au sein duquel neuf SRCant discutent de différents cas d'application issus du travail opérationnel avec le SRC et débattent de solutions. Ceci a permis de passer d'une collaboration bilatérale à une collaboration en réseau. En outre, en 2025, le SRC a adressé deux circulaires fondamentales aux cantons dans lesquelles il expose l'interprétation des bases légales sur des questions spécifiques.

Lors de ses visites dans les cantons, l'AS-Rens a pris note de quelques remarques concernant des informations soi-disant manquantes. Ces informations étaient pourtant disponibles sur l'intranet des SRCant et donc à disposition des cantons. L'AS-Rens en conclut que certains SRCant ne s'informent pas régulièrement via l'intranet des SRCant.

Formation

Depuis 2025, les SRCant sont intégrés dans la formation de base générale du SRC qui est suivie par l'ensemble des nouvelles et nouveaux membres du personnel du SRC, ce qui favorise la compréhension mutuelle (connaissances et terminologie) et la mise en réseau. Les besoins particuliers des SRCant sont pris en compte (traduction simultanée des modules de formation et documents traduits).

Coopération opérationnelle

La loi permet au SRC d'imposer une collaboration opérationnelle aux SRCant. Cependant, le SRC privilégie une approche collaborative.

Le SRC doit encore évaluer les opportunités et les risques qui en découlent avec les SRCant. Le SRC doit remédier aux défauts constatés dans la récente collaboration opérationnelle en introduisant des mesures appropriées et en les mettant en œuvre à l'avenir. L'AS-Rens a renoncé à formuler une recommandation car le SRC a connaissance des défauts et une solution appropriée est en bonne voie.

Assurance de la qualité

Comme lors des inspections précédentes (18-10 et 21-5), l'AS-Rens a vérifié les contrôles d'assurance qualité du SRC. Les contrôles sont effectués par trois services du SRC selon un concept éprouvé. Les SRCant sont soumis à un contrôle tous les 6 à 7 ans. Les contrôles annuels des autorités cantonales de surveillance sont donc importants.

L'AS-Rens n'a émis aucune recommandation, sur aucun sujet.

5.2.4 Recherche d'informations

La recherche d'informations est une tâche clé des services de renseignement qui peuvent déployer divers moyens à cet effet. L'AS-Rens accorde une attention particulière aux moyens qui portent le plus atteinte aux droits fondamentaux, par exemple à la vie privée des personnes concernées. Les inspections Opérations (OP) et HUMINT ont lieu au moins une fois par an en raison des risques associés à ces activités. En 2025, l'AS-Rens s'est attelée aux inspections dans le domaine « Recherche d'informations » ci-après.

23-13 Engagement d'agentes et d'agents virtuels (VirtA) au SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
14.05.2024	21.11.2024	08.01.2025	4	10

Du point de vue du SRC, l'état des menaces au niveau mondial a évolué ces dernières années, de sorte que la communication des personnes cibles et des groupes, en particulier dans les domaines du terrorisme et de l'extrémisme violent, s'est éloignée des plateformes publiques. En raison de cette nouvelle situation, le SRC est contraint d'améliorer et d'adapter sa surveillance sur internet. Afin de continuer à obtenir des informations pertinentes pour le renseignement, le SRC doit recourir à des VirtA.

Le cadre juridique pour l'utilisation des VirtA doit être clairement défini, car le SRC pourrait interférer avec les droits fondamentaux (droit à la liberté personnelle et protection de la sphère privée) et collecter des informations avec une intensité comparable à une mesure de recherche soumise à autorisation. C'est pourquoi l'AS-Rens a vérifié si le cadre juridique pour l'utilisation des VirtA était clairement défini et était connu des collaboratrices et collaborateurs concernés.

Avec les articles 17 (couverture) et 18 (identité d'emprunt) de la loi fédérale sur le renseignement, le SRC dispose d'une base juridique pour l'utilisation des VirtA. Du point de vue de l'AS-Rens, l'utilisation de VirtA est fondamentalement légale. Cependant, ce qui est autorisé lors de l'utilisation des VirtA n'a pas encore été clarifié de manière concluante au sein du SRC.

Les actes d'inspection ont montré que le SRC était sensibilisé à cet aspect depuis les incidents de collecte illégale d'informations par le secteur cyber (voir rapport 22-18) et qu'il essaie de ne pas commettre les mêmes erreurs lors de l'utilisation des VirtA. Au moment de l'inspection, des questions restaient en suspens sur les règles et directives d'utilisation des VirtA. **Cependant, rien n'indique que des VirtA aient été utilisés pour obtenir des informations illégalement.** Certaines questions en suspens préoccupent le SRC depuis plusieurs années, même si le SRC n'a longtemps pas été clair sur

la manière dont les VirtA devaient être utilisés. Tant que ces points ne seront pas clarifiés dans le service et soumis sous forme de questions individuelles spécifiques au service juridique du SRC, l'expertise juridique pour la collecte opérationnelle d'informations dans l'espace virtuel ne pourra pas être développée efficacement. L'AS-Rens a recommandé que le SRC renforce son expertise dans le domaine de la collecte d'informations dans l'espace virtuel qui deviendra de plus en plus pertinent à l'avenir.

S'il n'engage pas ses propres VirtA, le SRC dépend de services partenaires étrangers et court le risque de ne pas être en mesure de reconnaître les menaces imminentes dans l'espace virtuel ou de ne pas les reconnaître à temps. C'est pourquoi l'AS-Rens a examiné s'il était opportun pour le SRC de créer sa propre section VirtA.

L'histoire montre que, depuis 2016, le SRC réfléchit à la création de VirtA et à leur utilisation pour la collecte opérationnelle d'informations dans l'espace virtuel. À partir de 2019, les efforts sont devenus plus concrets et, en 2021, la direction du SRC a finalement décidé de créer sa propre section VirtA. Les procédures de test ont montré que la responsabilité de la mise en œuvre du projet au sein du SRC a changé à plusieurs reprises ces dernières années. Dans son projet de créer une section VirtA, le SRC a procédé de manière inefficace et peu opportune. À chaque transfert de responsabilité vers une autre personne ou une autre section du SRC, des questions fondamentales similaires ont été discutées à maintes reprises et décrites dans différents concepts. Ce transfert multiple de responsabilités n'a pas permis de créer rapidement et efficacement une section VirtA.

L'AS-Rens a jugé utile et bienvenu l'échange d'expériences du SRC avec des services partenaires étrangers comparables. Leurs expériences positives ont été intégrées dans les considérations conceptuelles du SRC et la structure organisationnelle finale de la section VirtA du SRC était largement basée sur celle des services partenaires interrogés. La collaboration prévue du SRC avec des services partenaires dans le domaine de la formation vise à garantir que les VirtA du SRC puissent bénéficier de la longue expérience opérationnelle de leurs homologues étrangers. L'AS-Rens juge appropriée l'intention du SRC de mettre en place à l'avenir sa propre formation afin de réduire sa dépendance à l'égard des services partenaires.

L'AS-Rens a également vérifié si le SRC dispose du cadre technique et organisationnel lui permettant d'obtenir des succès en matière de renseignement grâce à l'utilisation de VirtA ou d'évaluer correctement les chances de succès dès le départ. Les procédures de tests ont montré que les critères précis permettant de mesurer l'impact des déploiements de VirtA n'étaient pas encore disponibles. Il est toutefois ressorti des discussions que le standard pour approuver un engagement VirtA est exigeant car, par exemple, une indication isolée d'un service partenaire ne constitue pas une base suffisante pour approuver un engagement. Le SRC doit plutôt disposer de ses propres informations fiables issues de la surveillance qu'il opère sur internet afin de démarrer un engagement VirtA prometteur. L'AS-Rens a recommandé d'intensifier les efforts pour définir les critères de mesure de l'impact des déploiements de VirtA.

24-5 Opérations, besoins de clarifications opérationnels et mesures de recherche soumises à autorisation du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
25.07.2024	29.01.2025	26.02.2025	3	10

Par rapport aux activités quotidiennes, les opérations et les besoins de clarifications opérationnels se caractérisent par une plus grande complexité dans la planification et la mise en œuvre des activités de renseignement. En outre, selon la réglementation interne du SRC, les mesures de recherche soumises à autorisation peuvent être mises en œuvre uniquement dans le cadre d'opérations. Celles-ci présentent toujours un risque pour les droits fondamentaux, en raison de l'ingérence dans la vie privée des personnes concernées. Il semble donc nécessaire de contrôler régulièrement la légalité, l'efficacité et l'adéquation du portefeuille des opérations et des besoins en matière de clarifications opérationnels.

Cette année, l'AS-Rens a également examiné les effets de la transformation du SRC sur la mise en œuvre des opérations et des besoins de clarifications opérationnels. Les travaux liés à cette transformation n'étaient pas encore terminés au moment de l'inspection. Le SRC a remplacé ses processus établis par de nouveaux processus. Ces changements ont une influence profonde sur la mise en œuvre des opérations, des besoins de clarifications opérationnels et des mesures de recherche soumises à autorisation, et peuvent donc entraîner de nouveaux risques. Mais ils peuvent aussi ouvrir de nouvelles perspectives.

Dans le domaine de la définition des processus de recherche d'informations et du respect de l'obligation de documentation, l'AS-Rens a constaté un besoin d'amélioration et formulé des recommandations.

Par ailleurs, l'AS-Rens a examiné en détail trois opérations et, d'un point de vue formel, toutes les mesures de recherche soumises à autorisation qui ont été demandées dans ce cadre. Sur la base de ses actes d'inspection, l'AS-Rens a jugé que les opérations incluses dans l'échantillon étaient légales, appropriées et efficaces. L'AS-Rens a vérifié si quatre mesures de recherche approuvées et validées par le Tribunal administratif fédéral (TAF) avaient été mises en œuvre (dans le cadre de deux opérations en cours) conformément aux décisions correspondantes. Dans les mesures de recherche soumises à autorisation examinées, elle n'a pas constaté d'optimisation nécessaire et n'a émis aucune recommandation.

24-6 Informatrices et informateurs (HUMINT) du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
29.10.2024	10.06.2024	03.07.2025	1	3

Le domaine HUMINT fait partie des activités les plus sensibles du SRC. Ceci engendre des mesures de sécurité et de protection particulièrement élevées par rapport au personnel impliqué (notamment le recours à des identités d'emprunt et/ou à des légendes afin de cacher l'appartenance au SRC), aux lieux de travail (légendés), aux flux financiers légendés nécessaires afin de cacher la provenance des fonds, aux obligations de protection des sources, etc. Les risques dans ces domaines sont variés et évoluent en permanence, justifiant une inspection de l'AS-Rens à intervalles réguliers.

L'inspection 24-6 visait à assurer un suivi de l'inspection « 23-12 HUMINT » et des projets en cours au sein du domaine HUMINT. Les constats faits sont globalement positifs, les projets examinés avancent dans la bonne direction. Une recommandation a été émise en lien avec des analyses de risques. Le domaine HUMINT semble à présent trouver le juste équilibre entre ses nombreux projets, ses ressources limitées et la préservation de son cœur de métier qui est la conduite de sources.

D'autre part, l'AS-Rens a examiné des dossiers de conduite de sources incluant l'examen de l'infrastructure mise en place pour protéger ses sources. Aucune irrégularité n'a été relevée dans le cadre de la présente inspection.

25-7 Opérations, besoins de clarifications opérationnels et mesures de recherche soumises à autorisation du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
14.05.2025	24.09.2025	30.10.2025	2	6

Par rapport aux affaires courantes, les opérations et les besoins de clarifications opérationnels se caractérisent par une plus grande complexité dans la planification et la mise en œuvre des activités de renseignement. Selon le SRC, les mesures de recherche soumises à autorisation ne peuvent être mises en œuvre que dans le cadre d'opérations. Celles-ci présentent toujours un risque pour les droits fondamentaux, en raison de l'ingérence dans la vie privée des personnes concernées. L'AS-Rens a estimé que ces points constituaient des raisons suffisantes pour examiner les risques liés à la réalisation d'opérations, aux besoins de clarifications opérationnels et aux mesures de recherche soumises à autorisation au sein du SRC.

Suite à la transformation du SRC, la structure organisationnelle dans le domaine des opérations et des besoins de clarifications opérationnels a été repensée et redéfinie. La nouvelle organisation du SRC est en place depuis mars 2024. Le SRC a remplacé ses processus établis par de nouveaux processus. Ces changements ont une influence profonde sur la mise en œuvre des opérations, des besoins de clarifications opérationnels et des mesures de recherche soumises à autorisation, et peuvent donc entraîner de nouveaux risques. Mais ils peuvent aussi ouvrir de nouvelles perspectives.

Cette année, l'AS-Rens a examiné un échantillon de deux opérations dans le domaine de la lutte contre le terrorisme. Sur la base de ses travaux d'inspection, l'AS-Rens a jugé que les opérations incluses dans l'échantillon étaient légales, adéquates et efficaces. Elle a émis une recommandation concernant le maintien de la capacité opérationnelle du matériel technique.

En ce qui concerne le respect formel des obligations en matière de documentation, elle a examiné de manière approfondie l'ensemble des cas ouverts de l'année 2024 nécessitant des besoins de clarifications opérationnels, ainsi qu'un échantillon supplémentaire de cas dans les divisions Counter Proliferation et Counter Terrorism / Counter Violent Extremism.

Elle considérait que les principales obligations en matière de documentation étaient remplies. Afin de faciliter les analyses statistiques et d'optimiser ainsi la gestion du portefeuille des besoins de clarifications opérationnels en matière d'évaluation, l'AS-Rens a tout de même formulé une recommandation en lien avec les obligations de documentation internes du SRC.

L'AS-Rens a vérifié si 11 mesures de recherche soumises à autorisation demandées dans deux opérations réalisées avaient été mises en œuvre conformément aux décisions correspondantes du TAF. **Sur la base de l'échantillon, l'AS-Rens a estimé que ces mesures avaient été mises en œuvre conformément aux décisions du tribunal.**

25-8 Informatrices et informateurs (HUMINT) du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
26.08.2025	18.12.2025			5

L'AS-Rens vérifie la légalité, l'adéquation et l'efficacité d'un certain nombre de conduites de source.

25-9 Cyberexploration au RM

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
03.12.2025				1

L'AS-Rens vérifie si le RM utilise des moyens légaux, appropriés et efficaces pour la cyberexploration.

5.2.5 Ressources

Dans le domaine « Ressources », l'AS-Rens examine si les services utilisent les ressources de manière adéquate et garantissent ainsi une activité de renseignement efficace. Dans ce domaine, l'AS-Rens s'est attelée en 2025 aux inspections ci-après.

24-7 Inventaire des TIC au SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
22.10.2024	19.03.2025	10.04.2025	1	5

Dans le domaine des TIC, il est important pour diverses raisons qu'une organisation dispose d'un aperçu du matériel utilisé. Cette vue d'ensemble permet de gérer les composants matériels tout au long de leur cycle de vie. De plus, un inventaire systématique permet d'éviter que des personnes non autorisées se procurent et utilisent du matériel au sein de l'organisation. Ce dernier point en particulier comporte pour le SRC à la fois un risque de réputation et un risque de traitement illégal des données en raison de l'absence de mécanismes de contrôle.

L’AS-Rens a donc vérifié si le SRC dispose d’un inventaire de son matériel informatique utilisé dans l’environnement du renseignement et si cet inventaire est tenu de manière efficace et appropriée. Du point de vue de l’AS-Rens, la tenue d’un inventaire des TIC est un moyen de détecter les acquisitions non autorisées et d’éviter ainsi que des composants matériels ne soient utilisés de manière non autorisée.

Lors de son examen, l’AS-Rens a constaté que le processus d’acquisition se situe en amont du processus d’inventaire et que les deux processus sont bien établis au SRC. En outre, les processus d’acquisition et d’inventaire sont tous deux soutenus par des logiciels. Même si les deux systèmes ne sont pas couplés automatiquement et qu’il est nécessaire de passer manuellement du système d’acquisition au système d’inventaire, des analyses ponctuelles ont montré qu’il n’y a pas de divergences notables entre les deux systèmes.

De même, les champs gérés dans le système d’inventaire semblent, du point de vue de l’AS-Rens, efficaces et appropriés pour gérer d’autres fonctionnalités, comme, par exemple, le cycle de vie d’un objet TIC, ou afin de déterminer où se trouve un composant TIC au sein du SRC.

En résumé, l’AS-Rens a eu l’impression que le système d’inventaire du SRC pourrait être amélioré par un couplage plus étroit avec les systèmes d’acquisition ou de support informatique. Les résultats de la sélection de l’échantillon, les entretiens avec les responsables techniques et les processus d’autorisation rigoureux qui ont été mis en place ne permettent pas de conclure que le SRC est exposé à un risque important en raison d’un inventaire inefficace et inadéquat.

L’AS-Rens n’a donc formulé une recommandation qu’en ce qui concerne une directive à réviser, car elle ne correspond plus à l’état actuel du point de vue organisationnel et qu’il existe donc un risque de saisies erronées ou incomplètes dans le processus d’inventaire.

25-10 Armement au SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d’entretiens
27.06.2025	30.09.2025	30.10.2025	0	7

L’armement au SRC est fondé sur la Loi fédérale sur le renseignement. Il sert à protéger les collaboratrices et collaborateurs particulièrement exposés aux dangers pour leur intégrité physique ou leur vie, ceci dans l’exercice de leur fonction. L’AS-Rens a évalué comment le SRC gérait l’attribution, le retrait et le stockage de ses armes de service et si le cadre légal en la matière était respecté. Elle a aussi vérifié si l’équipement et la formation dispensée répondaient dans la pratique aux besoins de protection du personnel. Pour ce faire, elle a procédé à des entretiens et à des actes d’inspection dans différents lieux.

Une nouvelle directive du SRC concernant l’armement est récemment entrée en vigueur. Les exigences pour qu’une arme soit attribuée aux membres du personnel ont été précisées et durcies. Ainsi, l’attribution et le retrait de l’arme de service peuvent être améliorés. L’AS-Rens est arrivée à la conclusion que des développements étaient envisageables en ce qui concerne l’équipement du personnel. Elle n’a pas formulé de recommandations, mais elle a encouragé le SRC à poursuivre ses efforts actuels.

5.2.6 Traitement des données et archivage

Dans le domaine « Traitement des données et archivage », l’AS-Rens examine en particulier la légalité du traitement des informations étant donné la sensibilité élevée des informations traitées ainsi que l’étendue et la complexité des prescriptions légales. En 2025, l’AS-Rens s’est attelée dans ce domaine aux inspections ci-après.

22-18 Recherche d'informations par le domaine Cyber du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
07.06.2024	18.11.2024	20.02.2025	4	17

Rappel des faits et déroulement de l'inspection

En traitant de possibles cyberattaques, le SRC a collecté, entre 2015 et 2020, des renseignements protégés par le secret des télécommunications. Ces mesures de recherche sont soumises à autorisation et ne peuvent donc être mises en œuvre qu'après obtention de l'autorisation du TAF.

En avril 2021, le directeur du SRC de l'époque a appelé l'AS-Rens pour l'avertir de possibles irrégularités commises par l'unité Cyber du SRC dans la recherche d'informations et de l'ouverture d'une enquête interne. L'AS-Rens a suivi l'enquête interne du SRC concernant ces évènements et le SRC l'a régulièrement informée de l'avancement des investigations. En outre, l'AS-Rens a reçu des informations complémentaires sur le fond de l'affaire.

À la suite de l'enquête interne, le DDPS a mandaté l'ancien juge fédéral Niklaus Oberholzer en 2022 pour mener une enquête administrative. C'est pourquoi l'AS-Rens a renoncé à l'époque à lancer sa propre inspection.

Une fois l'enquête administrative du DDPS conclue, l'AS-Rens a estimé que les incidents survenus dans l'unité Cyber avaient été largement éclaircis concernant la légalité de la recherche d'informations.

Par contre, selon l'AS-Rens, l'enquête interne du SRC et l'enquête administrative du DDPS n'ont pas permis d'éclaircir certaines questions encore en suspens, comme les contacts et les informations échangées avec des entreprises privées.

En juin 2022, l'AS-Rens a donc lancé une inspection visant à répondre aux questions encore en suspens concernant les événements survenus entre 2015 et 2020 au sein de l'unité Cyber du SRC. En outre, l'AS-Rens a vérifié si les mesures prises par le SRC sous la forme d'ajustements des processus et de l'organisation de l'unité Cyber étaient appropriées et suffisantes pour garantir à l'avenir une collecte de données légale et appropriée.

À cette fin, l'AS-Rens a notamment analysé un vaste ensemble de données (concernant les contacts et les informations échangées avec des entreprises privées) que ni l'enquête interne du SRC ni l'enquête administrative du DDPS n'avaient examiné. Le SRC avait procédé à une sauvegarde forensique de ces données dans le cadre de l'enquête interne en 2021, mais il avait décidé de ne pas les évaluer lui-même, principalement pour des raisons liées au droit du personnel. En revanche, l'AS-Rens se considérait habilitée, en tant qu'autorité de surveillance, à analyser cet ensemble de données.

L'inspection de l'AS-Rens a porté sur les faits concernant les événements dans le domaine cyber qui se sont produits jusqu'en 2021 ainsi que sur les mesures organisationnelles prises dans le même domaine jusqu'en mars 2023. Les entretiens avec le personnel et les cadres concernés ont eu lieu jusqu'en décembre 2022. L'AS-Rens a demandé des informations spécifiques sur certaines questions concrètes jusqu'au printemps 2024. Enfin, le SRC a eu la possibilité de commenter les résultats de l'inspection entre décembre 2024 et janvier 2025.

Résultats de l'analyse

Concrètement, l'AS-Rens a répondu aux questions suivantes :

1. Les faits pertinents pour l'évaluation des incidents survenus dans l'unité Cyber ont-ils été entièrement saisis ?
2. Comment le SRC assurera-t-il la légalité de l'analyse du trafic de données des fournisseurs à l'avenir ?

3. Les mesures organisationnelles prises par le SRC et les contrôles mis en place sont-ils adéquats et efficaces pour éviter que de tels incidents se produisent à l'avenir ?

1. Les faits pertinents pour l'évaluation des incidents survenus dans l'unité Cyber ont-ils été entièrement saisis ?

Tant l'enquête interne que l'enquête administrative ont conclu que les données traitées par l'unité Cyber dans le cadre de l'analyse des cyberincidents étaient presque exclusivement de nature technique et ne présentaient aucun lien avec des personnes. L'unité Cyber n'a pas besoin de rechercher des données personnelles ; ce qui l'intéresse, ce sont les procédures et les indicateurs techniques qui sont totalement indépendants des personnes. Les données évaluées à la suite de cyberattaques ne peuvent pas être associées à une personne en particulier.

L'analyse par l'AS-Rens des données sauvegardées de manière forensique a toutefois également révélé que des données personnelles avaient été traitées et peut-être même échangées avec des services externes. L'ensemble de données contenait notamment des adresses IP (*Internet Protocol*) qui sont considérées comme des données personnelles d'un point de vue juridique. Selon la loi fédérale sur la protection des données (LPD), les données personnelles sont toutes les informations concernant une personne physique identifiée ou identifiable. Dans son message de 1988 sur la LPD, le Conseil fédéral avait déjà précisé que « […], si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre (p. ex. parce qu'il lui faudrait procéder à une analyse sophistiquée d'une statistique), on ne peut guère parler de possibilité d'identification ». Conformément aux art. 37 et 38 de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT), par exemple, le SRC a la possibilité d'obtenir des informations sur l'identification des utilisateurs d'adresses IP attribuées en Suisse de manière univoque ou non. Il ne doit donc pas déployer de gros efforts pour identifier les personnes concernées, du moins pour une partie des adresses IP traitées en Suisse. C'est pourquoi l'AS-Rens estime que ces adresses IP doivent être considérées comme des données personnelles dans l'environnement de travail du SRC.

Dans le cadre de ses activités de contrôle, l'AS-Rens a trouvé quelques rares indices d'une éventuelle transmission d'informations. L'analyse des données n'a cependant pas permis de clarifier cette question de manière approfondie et définitive. L'AS-Rens a formulé une recommandation visant à examiner les risques liés à la collaboration avec des services externes dans le domaine cyber.

2. Comment le SRC assurera-t-il la légalité de l'analyse du trafic de données des fournisseurs à l'avenir ?

Sur la base des conclusions de l'enquête interne, le SRC a pris diverses mesures d'urgence le 20 mai 2022. Pendant l'enquête, il avait déjà révisé les directives du 1er octobre 2021 concernant ses activités de renseignement dans le domaine cyber, lesquelles sont entrées en vigueur le 23 mai 2022. Contrairement à ce que prévoit le contenu révisé, le SRC n'a toutefois pas encore mis hors service le système de stockage dans lequel les données obtenues lors de cyberattaques étaient sauvegardées et traitées. Selon le SRC, le domaine Analyse technique cyber ne pourrait plus du tout faire son travail sans cette infrastructure et l'unité Cyber ne pourrait plus que très partiellement s'acquitter de ses tâches. Le SRC a toujours l'intention de mettre cette infrastructure hors service, mais il faut d'abord trouver une nouvelle solution technique. Dès le 15 décembre 2022, l'AS-Rens a adressé un courrier au SRC pour lui signaler que les mesures communiquées n'étaient toujours pas mises en œuvre. Le système utilisé pour le traitement des données cyber n'étant qu'une solution temporaire, il convenait de le remplacer par un système définitif. Dans ce contexte, l'AS-Rens a enfin formulé une recommandation au SRC pour qu'il traite cette question de toute urgence.

Les actes d'inspection effectués par l'AS-Rens ont montré que les mesures d'urgence décidées et annoncées par le SRC n'étaient pas toutes mises en œuvre. Pour pallier les manquements dans la

conduite de l'unité Cyber constatés tant dans l'enquête interne que dans l'enquête administrative, il a fallu attendre 2024 pour que le SRC mette en place des instruments de conduite adéquats.

Le SRC n'a pas mis en place de nouveaux contrôles. Le principe de la double vérification n'est toujours pas appliqué en dehors de l'unité Cyber du SRC. Sur ce point l'AS-Rens a également formulé une recommandation.

L'AS-Rens a remarqué qu'il n'existait aucun règlement du personnel du SRC précisant les droits et les devoirs pour l'utilisation des appareils professionnels. Elle a recommandé au SRC de réglementer la distinction entre l'usage privé et l'usage professionnel et d'informer son personnel que les appareils du SRC, en cas de soupçon, pouvaient être mis en sécurité et faire l'objet d'une enquête.

3. Les mesures organisationnelles prises par le SRC et les contrôles mis en place sont-ils adéquats et efficaces pour éviter que de tels incidents se produisent à l'avenir ?

De manière générale, la recherche d'informations par le biais de mesures soumises à autorisation n'était pas au centre de cette inspection. D'après les actes d'inspection effectués dans le domaine cyber, rien ne suggère que des informations soient encore obtenues illégalement auprès de fournisseurs d'accès.

Le SRC n'a pas toujours respecté les mesures qu'il s'était lui-même imposées, comme la mise en œuvre rapide des points soulevés dans le rapport d'échantillonnage de son propre service d'assurance qualité.

Compte tenu de l'ampleur de la recherche illégale d'informations par l'unité Cyber, constatée et analysée après plusieurs années, il a été surprenant de constater que le SRC a renoncé à tout nouveau contrôle et s'appuie uniquement sur de nouveaux processus. Bien que ces derniers soient incontestablement nécessaires, il importe tout autant d'accorder une attention suffisante à leur respect. Jusqu'à la fin des actes d'inspection de l'AS-Rens en février 2024, tout portait à croire que la direction de l'unité Cyber, dans le contexte très tendu du renseignement, n'aurait toujours pas su détecter à temps d'éventuels dysfonctionnements. Entre-temps, le SRC a procédé à une transformation et, en janvier 2025, il a pu montrer de manière plausible des améliorations dans la conduite de l'unité Cyber. C'est pourquoi l'AS-Rens a finalement décidé de ne pas émettre de recommandation à ce sujet.

24-9 Échantillonnage dans le système IASA-ICC du SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
09.12.2024	13.05.2025	07.07.2025	4	7

Le système d'information et d'analyse intégrale de l'application Allsource Control (IASA-ICC) est l'application centrale utilisée par le SRC pour analyser et évaluer les documents originaux relatifs au système d'information et d'analyse intégrale du SRC pour l'extrémisme violent (IASA-EXTR) et au système d'information et d'analyse intégrale du SRC (IASA SRC). Il permet la réplication de données dans un système d'indexation (IASA INDEX) auquel les partenaires sécuritaires autorisés ont accès (par exemple, les organes d'exécution cantonaux). Les données saisies dans le système IASA-ICC constituent le savoir structuré du service. L'application IASA-ICC se base sur un répertoire de données brutes dans lequel les communications entrantes sont enregistrées en tant que documents originaux selon les délais de conservation fixés par la LRens.

Dans le cadre d'autres inspections, l'AS-Rens a eu connaissance de retards de saisie dans le système IASA-ICC, touchant notamment les rapports des organes d'exécution cantonaux qui doivent obligatoirement être saisis. De ce fait, des informations pertinentes pour la sécurité intérieure et extérieure de la Suisse pourraient ne pas être mises à la disposition des partenaires sécuritaires, créant ainsi un risque pour la sécurité.

Fin 2024, le SRC a lancé une force opérationnelle chargée de solutionner le problème des retards de saisie et d'optimiser les processus de saisie afin d'éviter un nouveau retard par la suite. L'AS-Rens a pris en compte ces travaux et a pu constater qu'ils ont déjà apporté des améliorations.

Dans ses investigations, l'AS-Rens a effectué trois échantillonnages dans le but de vérifier si le traitement des données dans le système IASA-ICC répondait aux exigences légales.
Deux échantillonnages n'ont révélé aucune irrégularité. En revanche, l'AS-Rens a constaté dans un échantillonnage que les restrictions imposées au SRC dans le traitement des données relatives à l'exercice des droits politiques n'étaient pas toutes respectées. Ce traitement de données porte sur la thématique de l'extrémisme Corona. L'AS-Rens a recommandé au SRC de procéder immédiatement aux modifications nécessaires ainsi qu'à des vérifications ultérieures dans le domaine de l'extrémisme monothématique dans le but de protéger les droits fondamentaux.

La révision de la LRens en cours prévoit un changement dans la manière d'approcher le traitement des données au sein du SRC en se détachant d'une approche par systèmes d'information pour favoriser une approche par type de données (données de renseignement ou données administratives). En parallèle, le service conduit divers projets visant à renouveler son infrastructure informatique. Devant la complexité de cette situation, la suppression ou le remplacement du système IASA-ICC est prévu.

Finalement, l'AS-Rens a constaté que l'obsolescence de l'application IASA-ICC empêche le SRC de capitaliser sur des données structurées. En effet, elle ne permet pas de garantir le suivi de la situation et les processus de saisie sont très lourds. L'AS-Rens a donc recommandé au SRC d'établir ses besoins afin de gérer les changements en cours sur le plan juridique et au niveau de l'infrastructure informatique en gardant à l'esprit le mandat de suivi et d'évaluation des menaces. L'objectif est de clarifier dans les plus brefs délais le remplacement ou la suppression de l'application IASA-ICC par une alternative profitable à l'accomplissement du mandat du SRC.

24-10 Consultations de systèmes d'information de tiers par le SRC

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
10.06.2024	31.01.2025	05.03.2025	3	5

Pour accomplir ses missions, le SRC doit pouvoir accéder aux systèmes d'information de tiers (SIT). Les SIT sont des applications et des bases de données d'opérateurs externes en Suisse et à l'étranger auxquelles les membres du personnel du SRC peuvent accéder pour obtenir des informations. En principe, les autorités (tierces) responsables du système ou des données décident, selon la base légale du système d'information concerné et des informations fournies par les autorités requérantes, qui peut accéder au système et avec quelles autorisations.

Bien que des tiers décident en dernier ressort des autorisations d'accès, il incombe au SRC de soumettre les demandes d'accès à des systèmes externes en fonction d'un besoin justifié ou de faire supprimer rapidement les droits d'utilisateur obsolètes. Pour cela, le SRC a besoin d'une gestion adéquate des accès. À défaut, il existe un risque que des membres du personnel aient accès à des données sensibles auxquelles elles ou ils ne devraient pas avoir légalement accès ou qu'il manque au SRC des autorisations qui seraient utiles pour une exécution efficace des missions.

Les vérifications de l'AS-Rens ont montré que le SRC ne dispose pas d'un aperçu complet et à jour des autorisations d'accès des membres de son personnel aux systèmes d'information de l'administration. Il manque des processus spécifiques et des contrôles internes systématiques. En outre, l'AS-Rens considère qu'une interface de recherche automatisée sur deux des systèmes d'information tiers examinés n'est pas conforme aux règles. Le SRC n'est responsable ni de l'interface ni du SIT, mais il assume une part de responsabilité en lien avec l'utilisation qu'il en fait. C'est pourquoi l'AS-Rens a recommandé au SRC de s'engager fermement en faveur d'une solution conforme à la loi afin d'agir en tout temps dans le cadre légal, faute de quoi les accès en question devront être supprimés. La gestion des accès au système de traitement des données doit être améliorée sur d'autres points.

De plus, l'AS-Rens a vérifié par échantillonnage dans certains SIT si les membres du personnel du SRC effectuaient des requêtes de manière légale et appropriée. L'absence de directives ou leur imprécision, ou encore la méconnaissance des modalités de consultation des données dans les SIT, augmentent le risque que les collaboratrices et collaborateurs consultent ces systèmes au-delà de leurs compétences légales ou à des fins personnelles, ce qui peut notamment entraîner des violations de droits fondamentaux et des risques de perte de réputation pour le SRC. C'est pourquoi l'AS-Rens a procédé à des contrôles aléatoires dans certains systèmes d'information de tiers pour vérifier la légalité et l'adéquation des requêtes de données effectuées par des membres du personnel du SRC choisis au hasard.

Les contrôles de l'AS-Rens n'ont révélé aucun indice de requêtes illégales ou inappropriées effectuées par les collaboratrices et collaborateurs du SRC dans les systèmes d'information de tiers sélectionnés.

25-11 Stockage des données par le service ACEM dans le domaine de l'exploration du réseau câblé

Mandat	Consultation	Envoi du rapport définitif	Recommandation(s)	Nombre d'entretiens
18.12.2024	03.07.2025	28.07.2025	1	6

L'exploration du réseau câblé fait désormais partie, avec la reconnaissance radio, des capteurs techniques les plus efficaces dans le domaine Signal Intelligence (SIGINT). Elle nécessite toutefois la collecte et le stockage d'une grande quantité de données. Il existe donc un risque d'enregistrer également des données qui ne doivent pas l'être en raison d'une base légale insuffisante ou qui ne peuvent pas être traitées ultérieurement car elles ne sont pas pertinentes pour la mission. Ce risque doit être traité de manière appropriée par le service ACEM qui effectue l'exploration du réseau câblé sur mandat du SRC.

Afin de déterminer si les différentes étapes du stockage des données et leur tri appliqué aux bases de données réduisent effectivement le risque, l'AS-Rens a décidé, dans son plan des inspections 2025, d'examiner l'efficacité, l'adéquation et la légalité du stockage et du tri des données dans le cadre de la reconnaissance par câble.

Il s'est avéré que le service ACEM atteint l'objectif visé grâce à un processus en cascade qui va de la saisie des flux de signaux jusqu'aux résultats finaux du stockage des données. À chaque étape, des critères d'exclusion (appelés « blacklists ») ou des filtres positifs (appelés « whitelists ») sont utilisés pour le tri des données, réduisant progressivement le stock de données brutes à chaque niveau du traitement jusqu'à ce qu'il ne reste plus que des données licites et irréprochables pour l'analyse. **L'AS-Rens est parvenue à la conclusion que la manière dont les données sont réduites peut être considérée comme efficace et appropriée.** Elle n'a pas non plus constaté que le service collecte systématiquement, au moyen de la surveillance des câbles, des données qu'il n'est pas autorisé à collecter d'un point de vue juridique ou qui ne correspondent pas à une mission du SRC.

Les données collectées et traitées par le service ACEM sont toutefois soumises aux règles de protection des données telles qu'elles sont définies dans la nouvelle loi sur la protection des données. Bien que les principes de la protection des données soient reconnus, l'AS-Rens a recommandé d'examiner si des mesures supplémentaires sont nécessaires en raison des modifications apportées à la nouvelle loi sur la protection des données de 2023.

5.3 Accueil

Les personnes chargées des inspections au sein de l'AS-Rens ont été reçues de manière constructive et professionnelle par les entités soumises à sa surveillance. Elles ont pu accéder facilement aux documents et aux systèmes d'information nécessaires pour mener à bien leurs mandats d'inspection. Le personnel interrogé s'est tenu à leur disposition et a par ailleurs répondu aussi vite que possible à leurs questions complémentaires.

5.4 Mise en œuvre des recommandations

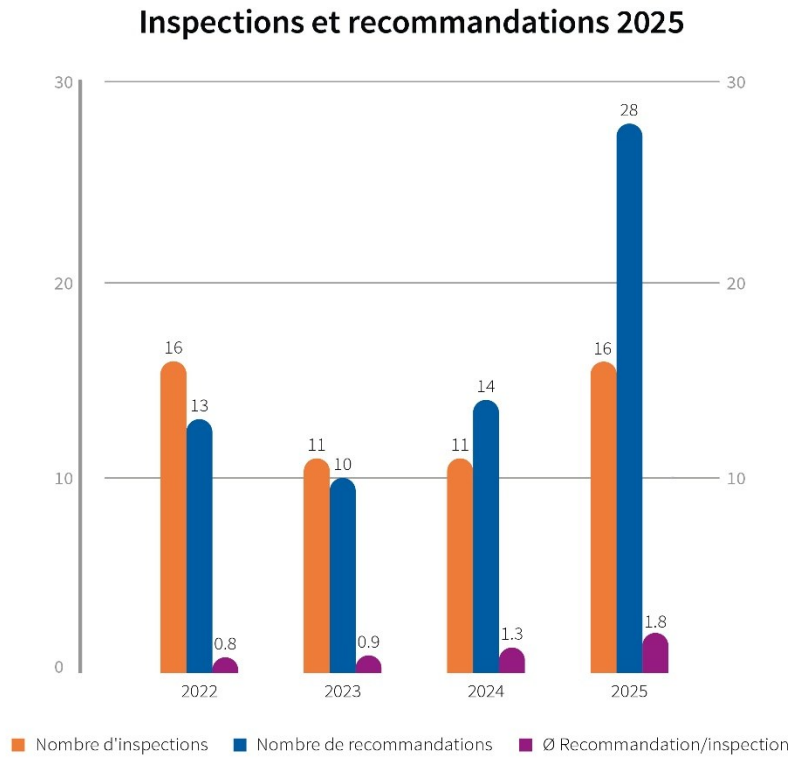
Les bases légales permettent à l'AS-Rens de s'appuyer sur ses actes d'inspection pour formuler des recommandations à l'intention du chef du DDPS. Le DDPS veille ensuite à leur mise en œuvre et, s'il rejette l'une d'entre elles, il doit la soumettre au Conseil fédéral pour décision. Mais un tel cas de figure ne s'est encore jamais présenté.

Aucune disposition légale n'oblige l'AS-Rens à vérifier la mise en œuvre de ses recommandations (monitorage des recommandations). **Toutefois, une surveillance n'est efficace et crédible que si les recommandations émises sont appliquées correctement et si cette application fait l'objet d'un contrôle.** L'AS-Rens accomplit cette part de son activité de surveillance en restant en contact avec les services examinés et le DDPS.

Le tableau suivant indique, par année de référence, le rapport entre le nombre d'inspections et les recommandations qui en résultent.

L'AS-Rens ne formule que des recommandations essentielles, ciblées et efficaces. Le nombre de recommandations ne constitue pas en soi un indicateur des améliorations ou des détériorations constatées.

	2022	2023	2024	2025
Nombre d'inspections	16	11	11	16
Nombre de recommandations	13	10	14	28
Ø Recommandation/inspection	0,8	0,9	1,3	1,8



6 Regard interne

Dans ce chapitre, l'AS-Rens rend compte de ses affaires internes.

6.1 Personnel

En 2025, l'AS-Rens comptait un effectif réglementaire de dix personnes. Au cours de l'année, l'une d'entre elles a quitté l'AS-Rens. Ce poste est à nouveau occupé.

6.2 Formations et perfectionnements

Au cours de l'année 2025, le personnel de l'AS-Rens a suivi des formations continues, notamment en matière de gestion des risques et d'intelligence artificielle. Des collaboratrices et collaborateurs ont également suivi certains modules de la formation de base du SRC dans le but de suivre l'évolution des activités de renseignement.

6.3 Accès à des informations et documents officiels

En tant que partie de l'administration fédérale décentralisée, l'AS-Rens travaille pour la population qui a le droit de connaître les prestations des autorités et la manière dont celles-ci s'acquittent de leur mission. Il en découle, pour la population, un droit à l'information et, pour les autorités, un devoir d'informer.

Au cours de l'année sous revue, l'AS-Rens a reçu cinq demandes d'accès. L'accès n'a été refusé dans aucun cas et partiellement accordé dans un cas. Dans trois cas, il n'y avait pas de documents officiels auxquels un accès devait être garanti. De plus, l'un des cas était toujours pendant à la fin de l'année et, là aussi, l'accès a dû être partiellement accordé.

7 Coordination

L'AS-Rens entretient des contacts avec différents partenaires en Suisse comme à l'étranger.

7.1 Contacts nationaux

Selon la loi sur le renseignement, l'AS-Rens coordonne ses activités avec la haute surveillance parlementaire et d'autres autorités de surveillance de la Confédération et des cantons. Elle échange également avec des personnes qui sont impliquées d'une manière ou d'une autre dans le domaine du renseignement et répond aux questions des citoyennes et citoyens.

Délégation des Commissions de gestion (DélCdG)

La Délégation des commissions de gestion a procédé à une visite d'office auprès de l'AS-Rens en février 2025. Lors de cette visite, l'AS-Rens lui a présenté en détail sa manière de travailler, notamment le cycle de la surveillance et divers outils utilisés, ainsi que deux rapports d'inspection. Un échange enrichissant sur divers points a suivi les présentations.

L'AS-Rens transmet tous ses rapports d'inspection à la DélCdG. Celle-ci examine les rapports et décide si elle invite l'AS-Rens à venir les présenter et en discuter. L'année dernière, l'AS-Rens a été invitée en mai à présenter les rapports 22-18 et 24-10 et en novembre à présenter les rapports 24-6 et 25-3 (ces rapports sont résumés dans le présent rapport d'activité).

Tribunal administratif fédéral (TAF)

Durant l'année sous revue, des représentantes et représentants du TAF et de l'AS-Rens se sont réunis lors de deux séances. Au cours de celles-ci, ils ont échangé sur la pratique du tribunal concernant les MRSA et les demandes d'exploration du réseau câblé et l'AS-Rens a présenté les inspections actuelles et le plan des inspections 2026. Du point de vue du TAF, il n'y avait aucune anomalie concernant les MRSA. Les demandes d'exploration du réseau câblé ont également pu être traitées par le tribunal dans les délais impartis.

L’échange a donc principalement porté sur les opérations menées par le SRC, ce qui a permis au TAF et à l’AS-Rens de vérifier mutuellement leurs informations respectives. De cette manière, un contrôle complet des MRSA est garanti, de l’autorisation ex ante à l’inspection ex post.

Contrôle fédéral des finances (CDF)

En vertu de la loi sur le Contrôle des finances, le CDF examine l’intégralité de la gestion financière lors de toutes les phases de l’exécution du budget et procède, par échantillonnage, à un contrôle préalable des engagements qui doivent être pris. Il surveille en particulier la gestion des crédits d’engagement et vérifie les systèmes de contrôle interne. Les unités administratives de la Confédération qui exercent des activités de renseignement, et qui sont donc soumises à la surveillance de l’AS-Rens, font également toutes partie du champ de contrôle du CDF. C’est pourquoi une bonne coordination entre les deux autorités de surveillance est importante.

En vertu de l’ordonnance sur la surveillance des activités de renseignement (OSRens), l’AS-Rens et le CDF peuvent échanger des informations sur leurs activités de surveillance et de contrôle ainsi que les données qui en résultent, pour autant qu’elles soient nécessaires à l’accomplissement de leurs tâches.

En 2025, les deux autorités de surveillance indépendantes ont eu plusieurs échanges par écrit et à l’oral sur la planification générale des inspections (planification annuelle) ainsi que sur des thèmes et questions spécifiques au sujet des inspections prévues. Elles se sont ainsi concertées sur les dates d’inspection dans le domaine du service ACEM. La cheffe de l’AS-Rens a rencontré le responsable du domaine d’examen correspondant au CDF à quatre reprises.

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

Dès sa création, il était prévu que l’AS-Rens reprenne les activités de l’OCI. La révision en cours de la LRens entrée en vigueur en 2017 doit désormais mettre en œuvre ce projet. Il apparaît donc judicieux d’anticiper cette reprise par un transfert de connaissances. À cette fin, le président de l’OCI et la cheffe de l’AS-Rens ont convenu que l’AS-Rens assisterait aux réunions de l’OCI. C’est pourquoi un représentant de l’AS-Rens a participé aux réunions de l’OCI en 2025.

L’AS-Rens et l’OCI ont également échangé au sujet de la participation de ce dernier à l’European Intelligence Oversight Conference (EIOC), une conférence annuelle qui a eu lieu en Suisse cette année, de ses contacts internationaux avec d’autres autorités de surveillance et de la révision de la LRens.

Préposé fédéral à la protection des données et à la transparence (PFPDT)

Une séance de coordination entre l’AS-Rens et le PFPDT a eu lieu à l’automne 2025. L’AS-Rens a renseigné le PFPDT sur les principaux éléments constatés lors des inspections arrivées à terme. Elle l’a également informé des inspections en cours et de celles planifiées dans la mesure où elles englobent des aspects de traitements de données. L’échange a aussi porté sur la mise en œuvre du droit d’accès conformément à la LRens.

Autorités cantonales de surveilllance

À l’été 2024, l’AS-Rens a entamé une tournée des cantons qui pris fin dans le courant de l’été 2025. Elle a échangé avec les personnes qui dirigent les SRCant, le personnel spécialisé et les autorités cantonales de surveillance. L’AS-Rens a consigné les résultats de ses entretiens dans un rapport. Elle a examiné certains aspects de la collaboration entre les SRCant et le SRC dans le cadre de l’inspection 25-6.

Concernant la surveillance par les cantons, l’AS-Rens a constaté qu’il existe de multiples formes d’organisation au sein des cantons. La surveilllance peut incomber au commandant de la police cantonale, à la direction du département compétent, à une personne d’un autre service cantonal ou

encore à une commission indépendante. Les formes d'organisation sont liées à la taille des SRCant ou encore à l'histoire des cantons en ce qui concerne les activités de renseignement.

Les cantons ont accueilli favorablement les visites de l'AS-Rens et ont apprécié d'avoir la possibilité d'échanger librement. Pour l'AS-Rens, les entretiens ont été utiles et précieux. Ils ont notamment démontrer combien les situations, les conditions, les attentes et les procédures peuvent varier d'un canton à l'autre.

Plusieurs entretiens ont mis en évidence le besoin d'un échange d'expériences entre les autorités cantonales de surveillance sur divers aspects de la surveillance et sur les bonnes pratiques. **Pour 2026, l'AS-Rens planifie une journée d'échange d'expériences entre et avec les autorités cantonales de surveillance.** En outre, ceci pourrait déboucher sur une éventuelle collaboration plus étroite entre l'AS-Rens et les autorités cantonales de surveillance, que ce soit sous la forme d'une inspection commune, d'un accompagnement de l'activité d'inspection ou d'un échange concret entre l'AS-Rens et une autorité de surveillance au moment de la planification et de la préparation de l'inspection.

Autres rencontres

- Cheffe et Chef du DDPS
- Secrétaire général du DDPS
- Conseillère du Chef du DDPS en matière de renseignement
- Chef de la Révision interne du DDPS
- Directeur du SRC (ancien et nouveau)
- Chef de l'Armée
- Chef du commandement des opérations
- Chef du RM et du SPPA
- Chef du commandement Cyber
- Chef du service ACEM
- Directeur du CDF
- Responsable de mandat du CDF
- Directrice de fedpol
- Secrétaire général de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)

Citoyennes et citoyens

En 2025, l'AS-Rens a reçu des demandes de 13 citoyennes et citoyens.

7.2 Contacts internationaux

L'AS-Rens échange des informations sur les méthodes, les processus et les expériences de surveillance avec des autorités de surveillance d'autres pays agissant dans le même domaine d'activités. Ces échanges s'avèrent toujours avantageux pour les activités de surveillance.

En 2025, l'AS-Rens a participé à trois réunions à l'étranger et a organisé des rencontres à Zurich.

European Intelligence Oversight Network (EION) le 20 mai 2025, Bruxelles

L'EION, créé en 2018 par une fondation, la Stiftung Neue Verantwortung (devenue le *think tank* Interface), vise à favoriser et à améliorer le contrôle des services de renseignement en Europe. Il propose une plateforme d'échange aux autorités de surveillance et à d'autres experts et expertes (p. ex. du monde scientifique). Quant à la fondation interface, elle traite différents thèmes liés à la sécurité informatique, à la gestion des données, à la digitalisation et aux droits fondamentaux.

Le Conseil de l'Europe et onze autres pays étaient représentés à l'atelier organisé par l'EION à Bruxelles.

Le thème, repris des discussions de juin 2022, était les risques liés à une utilisation disproportionnée du renseignement par la publicité en ligne (Advertisement Intelligence, ADINT) par les autorités nationales de sécurité.

L'objectif était de recueillir des informations auprès des expertes et experts ainsi que des délégations des autorités de surveillance pour qu'Interface rédige et publie un rapport à ce sujet. La question principale était la suivante : les autorités de surveillance ont-elles les moyens et les instruments nécessaires pour contrôler l'utilisation de données à des fins commerciales par les services de renseignement ?

Le document présenté par interface propose un schéma analytique, décrit en détail les différentes phases liées à l'accès aux données ADINT ainsi qu'à leur utilisation et contient un résumé des risques identifiés par phase.

L'atelier était axé sur les bases légales des Pays-Bas, des États-Unis et du Royaume-Uni car ces trois pays réglementent désormais l'ADINT.

Intelligence Oversight Working Group (IOWG) du 22 au 23 mai 2025, *technical meeting* et *staff meeting*, Copenhague

Avant le *staff meeting* périodique, le Danemark a de nouveau organisé un *technical meeting* auquel les autorités de surveillance ont envoyé leurs expertes et experts techniques. Ce format encore récent a fait ses preuves et sera poursuivi.

Les représentations anglaises, belges, danoises, hollandaises, norvégiennes, suédoises et suisses ont ensuite participé au *staff meeting* de l'IOWG, auquel s'est jointe l'autorité canadienne *Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR)* en qualité d'observatrice.

Tous les pays avaient préparé un thème selon une structure prédéfinie (défi, solution, expériences) et l'ont présenté dans les groupes de travail.

Le *technical meeting* a mis l'accent sur les questions relatives à l'IA, comme l'inspection de son utilisation en général ou pour des activités d'inspection en particulier. D'autres contributions portaient sur le big data et les bases de données ainsi que sur les opérations de hacking. L'AS-Rens a présenté le thème *Access to third-party information systems* (accès aux systèmes d'information de tiers).

Le *staff meeting* était centré sur les méthodes d'inspection, les compétences nécessaires et la transmission des connaissances. L'AS-Rens a décrit son expérience en matière de fluctuations du personnel et son approche du recrutement et de la préservation des compétences essentielles pour la surveillance.

Les deux types de séances ont donné lieu à des échanges précieux. **L'AS-Rens a pu se faire une idée des méthodes de travail d'autres autorités et pourra mettre ces connaissances à profit pour son propre développement.** Il est clair que tous les pays sont confrontés à des défis de même ordre, notamment en raison de la transformation rapide de l'environnement géopolitique et technologique et de la nécessité de garantir en permanence les compétences de surveillance nécessaires.

Intelligence Oversight Working Group (IOWG) du 4 au 5 novembre 2025, *technical meeting*, *staff* et *chair meeting*, Zurich

Les 4 et 5 novembre 2025, l'AS-Rens elle a accueilli les membres de l'IOWG dans le cadre de plusieurs séances, y compris une séance des responsables des différentes autorités de surveillance participantes lors de laquelle l'autorité de surveillance canadienne a été formellement admise comme membre du groupe de travail. Pour rappel, elle disposait d'un statut d'observatrice depuis novembre 2023. Les

participantes et participants ont livré un état de situation de la surveillance dans leur État respectif et se sont intéressés plus concrètement à l'impact que celle-ci peut avoir sur les autorités inspectées et à la manière d'en rendre compte. Les échanges lors des séances de travail *staff* et *technical meetings* ont porté notamment sur les difficultés d'accès à l'information auprès des autorités inspectées et les besoins supplémentaires en matière de coopération. Les participantes et participants ont également pu échanger leurs expériences en matière d'inspection sur le plan technique, et plus particulièrement sur le thème des cryptomonnaies.

European Intelligence Oversight Conference (EIOC) du 5 au 6 novembre 2025, Zurich

Du 5 au 6 novembre 2025, l'EIOC a eu lieu à Zurich. Les autorités de surveillance des activités de renseignement de la Suisse, de la Lituanie et du Canada y ont livré des présentations sur des sujets variés, tels que la gestion des risques en matière de surveillance, les difficultés rencontrées lors de la mise en place de leur entité ou les défis propres liés à leur structure organisationnelle. Lors de la deuxième journée, un accent particulier a été mis sur l'IA dans le contexte de la surveillance, ainsi que sur les enjeux légaux liés à la collecte de données de communication de masse par les services de renseignement. Le CDF a livré une présentation sur les derniers développements de l'IA, illustrant la double nature du défi qui se pose quant à l'utilisation de ces nouvelles technologies par les autorités de surveillance ou l'utilisation de ces technologies au sein des services inspectés. Ces thématiques ont ensuite été discutées sous forme d'un panel incluant des représentantes et représentants des autorités de surveillance norvégienne et anglaise. De même, des spécialistes du domaine ont présenté les environnements suisse et allemand en matière de collecte de données de communication de masse. Les échanges des membres du panel à ce sujet ont permis de comparer les pratiques étatiques, y compris avec la France. Enfin, le SRC s'est exprimé sur l'impact que peut avoir la surveillance sur son service.

Outre les représentantes et représentants de l'AS-Rens, des membres de la délégation de l'Allemagne, de l'Autriche, de la Belgique, de la Bulgarie, du Canada, du Danemark, de la Finlande, de la France, de la Grèce, de la Grande-Bretagne, de l'Italie, de la Lituanie, de la Norvège, des Pays-Bas, du Portugal et de la Suède étaient présents. Le CDF, l'OCI, le PFPDT, le TAF et le secrétariat de la DélCdG étaient aussi représentés.

8 Annexe

8.1 Plan des inspections 2025

No	Titre	Organe inspecté
Stratégie et planification		
25-1	Lutte contre l'extrémisme violent de gauche	SRC
25-2	Portefeuille de projets informatiques du SRC	SRC
Organisation et mandat		
25-3	Lutte contre l'espionnage au sein du SRC	SRC
25-4	Mesures visant à empêcher une fuite de données au sein du service ACEM	Service ACEM
25-5	Prestations de traduction	SRC
Collaboration		
25-6	Collaboration entre le SRC et les SRCant	SRC
Recherche d'informations		
25-7	Opérations, besoins de clarifications opérationnels et mesures de recherche soumises à autorisation du SRC	SRC
25-8	Informatrices et informateurs (HUMINT)	SRC
25-9	Cyberexploration	RM
Ressources		
25-10	Armement au SRC	SRC
Traitement des données / archivage		
25-11	Classement des données dans le domaine de l'exploration du réseau câblé	Service ACEM

8.2 Liste des abréviations

ACEM	Service Actions dans le cyberespace et dans l'espace électromagnétique
ADINT	*Advertisement Intelligence*
API	*Advance Passenger Information*
Art.	Article
AS-Rens	Autorité de surveillance indépendante des activités de renseignement
BCM	*Business Continuity Management*
CDF	Contrôle fédéral des finances
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DélCdG	Délégation des Commissions de gestion
EIOC	*European Intelligence Oversight Conference*
EION	*European Intelligence Oversight Network*
etc.	Et cetera
fedpol	Office fédéral de la police
GEVER	Système de gestion des affaires
HUMINT	*Human Intelligence* (recherche d'informations par des informatrices et informateurs)
IA	Intelligence artificielle
IASA-ICC	Système d'information et d'analyse intégrale de l'application Allsource Control
IASA SRC	Système d'information et d'analyse intégrale du SRC
IASA-EXTR	Système d'information et d'analyse intégrale du SRC pour l'extrémisme violent
INDEX SRC	Système d'indexation des données du SRC
IOWG	*Intelligence Oversight Working Group*
IP	*Internet Protocol*
LPD	Loi fédérale du 25 septembre 2020 sur la protection des données (RS 235.1)
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement (RS 121)
MRSA	Mesures de recherche soumises à autorisation
OCI	Organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé
OP	Opérations
OSCPT	Ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (RS 780.11)
OSRens	Ordonnance du 16 août 2017 sur la surveillance des activités de renseignement (RS 121.3)
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
PFPDT	Préposé fédéral à la protection des données et à la transparence
RM	Renseignement militaire
RS	Recueil systématique
SEM	Secrétariat d'État aux migrations
SEPOS	Secrétariat d'État à la politique de sécurité
SIGINT	*Signal Intelligence*
SIT	Systèmes d'information de tiers
SPPA	Service pour la protection préventive de l'armée
SRC	Service de renseignement de la Confédération
SRCant	Services de renseignement cantonaux
SYMIC	Système d'information central sur la migration
TAF	Tribunal administratif fédéral
TIC	Technologies de l'information et de la communication
VirtA	Agentes et agents virtuels