



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Rapport d'activités 2023

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

1 Résumé

En raison d'une situation sécuritaire en perpétuelle mutation, il est nécessaire d'adapter régulièrement les activités d'inspection de l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens). C'est ainsi que la pratique des services soumis à sa surveillance a été influencée par la pandémie de Covid-19, la guerre en Ukraine et les derniers développements au Proche-Orient, l'AS-Rens devant plus que jamais faire preuve de flexibilité et en tenir compte dans ses activités de surveillance.

La transformation du Service de renseignement de la Confédération (SRC) a également exigé de la souplesse et de l'agilité de la part de l'AS-Rens. En outre, les développements technologiques tels que l'utilisation de l'intelligence artificielle (IA) doivent être suivis, analysés et intégrés dans les activités d'inspection de l'AS-Rens. L'adaptation à un cadre en perpétuelle mutation fait par conséquent l'objet d'échanges et de discussions avec d'autres autorités de surveillance à l'échelle internationale.

En considérant l'année écoulée, l'inspection 22-15 OSINT s'avère être l'un des points forts des activités d'inspection de l'AS-Rens en 2023. Le renseignement en source ouverte ou open source intelligence (OSINT) est un secteur de la recherche d'informations par le renseignement qui évolue très rapidement. La combinaison d'innombrables données en libre accès offre aux services de renseignement des possibilités quasi infinies de récolter des informations. Elle pose des questions juridiques et éthiques, comme la délimitation entre l'OSINT et la recherche soumise à autorisation, ou l'acquisition et l'utilisation de données volées par des tiers. À l'échelle internationale, les autorités de surveillance suivent également de près ce type de recherche d'informations par les services de renseignement et en discutent. L'AS-Rens a inspecté ces recherches par le SRC et émis différentes recommandations.

L'AS-Rens a planifié seize inspections en 2023, dont quatre ont été annulées au cours de l'année. Une inspection commencée en 2021 s'est terminée en 2023. Sept rapports d'inspection définitifs portant sur des inspections menées en 2022 ont été remis en 2023. Durant l'année sous revue, l'AS-Rens a terminé ses activités d'inspection de sept des inspections planifiées en 2023 et a remis au Département fédéral de la défense, de la protection de la population et des sports (DDPS) trois rapports d'inspection définitifs pour des inspections planifiées pendant cette période.

Outre les inspections achevées au SRC, une inspection a été consacrée au Centre des opérations électroniques (COE ; dès le 1.1.2024 : service Actions dans le cyberspace et dans l'espace électromagnétique (ACEM)). Concernant le Renseignement militaire (RM), l'AS-Rens a mené différents entretiens à l'échelle du commandement relativement à sa compétence de surveillance dans le domaine du Service pour la protection préventive de l'armée (SPPA) et a intégré une inspection correspondante dans son plan des inspections en 2024.

2 Chiffres-clés au 31 décembre 2023

Collaborateurs/collaboratrices	01.01.2023	10
	31.12.2023	10
Inspections planifiées		16
Inspections inopinées		0
Inspections réalisées		11
Nombre d'entretiens réalisés en 2022	par oral et par écrit	109
Recommandations		10

3	Table des matières	
1	Résumé	2
2	Chiffres-clés au 31 décembre 2023	3
3	Table des matières	4
4	Note personnelle	5
5	Activités de surveillance	6
5.1	Plan des inspections	6
5.2	Inspections de l'année 2023	6
5.2.1	Stratégie et planification	6
5.2.2	Organisation	7
5.2.3	Collaboration	9
5.2.4	Recherche d'informations	11
5.2.5	Ressources	12
5.2.6	Traitement des données et archivage	14
5.3	Accueil	17
5.4	Mise en œuvre des recommandations	17
6	Regard interne	19
6.1	Personnel	19
6.2	Formations et perfectionnements	19
6.3	Inspection de l'AS-Rens par le Contrôle fédéral des finances (CDF)	20
6.4	Accès à des informations et documents officiels	21
7	Coordination	21
7.1	Contacts nationaux	21
7.2	Contacts internationaux	23
8	Annexe	26
8.1	Plan des inspections 2023	26
8.2	Liste des abréviations	27

4 Note personnelle

C'est une question de confiance

En tant que juriste, je sais que l'État ne peut faire que ce que la loi lui demande de faire, c'est-à-dire que je peux consulter une loi et comprendre (plus ou moins) tout ce que fait une autorité publique et pourquoi elle le fait. Mais si j'étais ingénieure, je comprendrais sans doute mieux pourquoi je peux rouler aujourd'hui dans le tunnel autoroutier du Saint-Gothard malgré le fait que des morceaux de béton sont tombés sur la route le 10 septembre 2023. En tant que personne normale, je dois souvent faire confiance à ceux qui en savent plus que moi, comme l'Office fédéral des routes.

Avec l'Etat il y a donc des choses que je comprends et d'autres pas, mais il y a toujours quelqu'un qui doit me l'expliquer. Puis, il y a les services de renseignement... Ces services ont parfois été accusés d'être "un État dans l'État", parce qu'on ne peut pas connaître certaines activités, comme s'ils avaient un pouvoir que personne d'autre ne possède. En fait, le pouvoir du secret est énorme.

Si l'on regarde concrètement ce que font les services de renseignement, on s'aperçoit vite que le secret est avant tout un outil de travail. Si les services de renseignement ne pouvaient pas agir dans certains contextes avec des moyens et des méthodes dissimulés, ils seraient inutiles.

Bien entendu, ce pouvoir s'accompagne d'une grande responsabilité. Qui peut m'assurer que quelqu'un n'abuserait pas du secret à des fins frauduleuses ou même égoïstes, comme la cupidité et la soif de pouvoir ?

Le législateur suisse sait depuis longtemps que ce pouvoir doit être soumis à un contrôle très strict. En particulier, la Délégation des Commissions de gestion de notre Parlement s'occupe de la surveillance parlementaire des services de renseignement depuis 1992. En 2015, avec l'adoption de la nouvelle loi sur les services de renseignement, approuvée par le peuple en 2016, le législateur a voulu développer davantage la vigilance en instituant une autorité de surveillance indépendante composée de spécialistes.

Ce système, qui combine un organe parlementaire et une autorité indépendante, correspond au choix fait par la quasi-totalité des démocraties occidentales. Il s'agit d'une légitimation importante pour les services de renseignement, puisqu'ils sont désormais contrôlés à la fois par un organe parlementaire représentant les différentes sensibilités politiques auxquelles chaque citoyen peut s'identifier, et par des experts tels que ceux que j'ai le plaisir de diriger et qui vous présentent leur travail dans ce rapport.

Les services de renseignement ne sont comparables à l'Office fédéral des routes à presque aucun égard, sauf celui de la confiance. Ils ont besoin de la confiance des citoyens pour fonctionner, tout comme le citoyen a besoin de ces services pour bénéficier d'un certain niveau de sécurité.

Le contrôle exercé par l'autorité que je représente consiste à surveiller des activités particulièrement complexes et délicates, à reconnaître leurs risques ou leurs défaillances et à présenter les mesures correctives qui s'imposent. En tant qu'autorité de surveillance, nous ne pouvons pas dévoiler tous les secrets des services de renseignement, mais nous pouvons y accéder.

L'Autorité indépendante de surveillance des activités de renseignement présente donc son rapport d'activité afin de permettre à chaque citoyen d'évaluer par lui-même s'il peut faire confiance.

Je vous souhaite une bonne lecture !

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
- Collaboration
- Recherche d'informations
- Ressources
- Traitement des données et archivage

Le plan des inspections est planifié de sorte à doter chaque domaine d'une inspection au moins. Celui prévu pour 2023 a été modifié durant l'année sous revue, quatre inspections ayant été supprimées pour les raisons suivantes :

- « 23-1 La production du Service de renseignement de la Confédération (SRC) en tenant compte des besoins des clients » : comme le SRC se trouve en phase de transformation, il faut s'attendre à des changements non seulement dans les différents secteurs organisationnels mais également dans leur production.
- « 23-3 La protection et la sécurité au SRC » : différents aspects de la sécurité ont déjà été examinés lors d'inspections passées. Certains liés à la sécurité du personnel ont par exemple été thématiques dans le cadre de l'inspection 22-14 « Processus de recrutement, d'encadrement et de départ ». C'est pourquoi d'autres inspections ont été privilégiées. La question de la sécurité du personnel reste toutefois toujours un thème inhérent aux inspections de l'AS-Rens.
- « 23-14 La mise en œuvre des recommandations de l'AS-Rens » : l'AS-Rens a lancé un projet interne pour améliorer la qualité de ses recommandations. Deux membres de son équipe ont ainsi suivi une formation continue et rédigé un travail sur cette thématique. Sur cette base, l'AS-Rens va adapter son manuel d'inspection et renforcer le monitoring des recommandations. C'est pourquoi elle a renoncé à l'exécution de cette inspection, au profit d'autres.
- « 23-15 La mise en œuvre du droit d'accès au SRC » : la loi fédérale sur la protection des données (LPD, RS 235.1) ayant été révisée au 1^{er} septembre 2023, le SRC a besoin de suffisamment de temps pour intégrer les modifications dans ses processus. Sur ce thème, l'AS-Rens continue d'échanger avec le SRC mais aussi avec le Préposé fédéral à la protection des données et à la transparence (PFPDT).

5.2 Inspections de l'année 2023

A partir du rapport d'activité 2023, l'AS-Rens modifie la manière de présenter les rapports afin de refléter la situation la plus actuelle possible. Dans ses précédents rapports d'activités, elle rendait uniquement compte des inspections terminées par un rapport durant l'année sous revue. Désormais, elle rend compte de chaque inspection pour laquelle elle a effectué tous les actes d'inspection durant l'année sous revue, y compris si elle n'est pas encore terminée formellement.

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 à l'inspection ci-après.

22-1 Détection précoce et d'anticipation

Cet examen s'est concentré sur la question de savoir comment le SRC peut remplir son mandat légal primaire de détection précoce et d'anticipation. La recherche et le traitement des informations du SRC servent à identifier et à prévenir à temps les menaces contre la sécurité intérieure et extérieure. Pour ce faire, il doit disposer de capacités lui permettant d'identifier et d'évaluer à temps une

situation et ses menaces. Les impondérables concernant l'évolution future des menaces ont fortement augmenté en raison de la complexité croissante du système géopolitique international. **Les évolutions sociales et techniques ainsi que les menaces hybrides actuelles de dimension mondiale rendent nécessaire l'identification de ces menaces par le SRC et sa capacité à y réagir rapidement et efficacement.** L'anticipation précoce des menaces pertinentes et des développements et opportunités stratégiques revêt donc une importance capitale. Le SRC joue à cet égard un rôle important pour ses clients dans la détection précoce des menaces et des crises.

L'AS-Rens a constaté que la détection précoce et l'anticipation sont un objectif stratégique du DDPS, que le SRC poursuit depuis longtemps déjà et qu'il a pris des mesures opérationnelles correspondantes, dont certaines sont déjà bien avancées et d'autres doivent encore être intensifiées. Pour l'AS-Rens, le thème est donc largement soutenu au niveau stratégique avec l'importance nécessaire. Si l'on se réfère à l'inscription de la détection précoce et de l'anticipation dans les stratégies respectives du DDPS et du SRC ainsi qu'aux déclarations des collaborateurs concernés, tous les participants s'accordent sur l'importance considérable de ce thème.

Mais elle a également constaté que les réflexions (théoriques) du SRC ne se répercutent que très lentement dans les domaines d'évaluation du service. Le lien entre les instruments à disposition et les produits ne fonctionnait pas encore de manière optimale. Le SRC ne parvient donc pas encore à transférer suffisamment et de manière profitable les efforts conceptuels dans les produits. L'AS-Rens recommande donc au SRC de poursuivre systématiquement les différentes mesures de mise en œuvre dans la détection précoce et l'anticipation de la stratégie 2020-2025 du SRC et de vérifier au moins une fois par an l'état de la mise en œuvre.

L'AS-Rens part du principe que le SRC utilise sa transformation actuelle comme base pour devenir un futur service agile, innovant et capable de s'adapter. Il convient de noter que ce travail ne s'achève pas avec une réorganisation. Maintenir le service à jour en ce qui concerne la structure, les nouvelles méthodes de travail et les nouvelles technologies, afin de pouvoir réagir en temps utile et de manière adéquate à l'évolution des menaces, est une tâche de gestion permanente, en particulier pour la direction du SRC.

5.2.2 Organisation

Dans le domaine « Organisation », l'AS-Rens examine la structure des services de renseignement et leurs processus de travail, en se posant notamment la question de savoir si ceux-ci permettent aux autorités concernées de remplir leur mandat légal dans le respect du droit, de manière efficace et adéquate. En 2023, l'AS-Rens a mené les inspections ci-après dans ce domaine.

23-2 Les prestations juridiques du SRC

Le respect de la loi revêt une grande importance dans les activités du renseignement. Si le SRC ne se conformait pas à la loi, c'est-à-dire s'il ne s'en tenait pas à sa mission légale, il nuirait à sa réputation et il minerait la confiance du public. Il peut en résulter des violations des droits de la personnalité conformément aux directives sur la protection des données, du droit à la vie privée ou des secrets d'affaires. En contrepartie, si le SRC, faute de certitude, n'exploitait pas pleinement ses possibilités légales, il ne remplirait pas sa mission, et il en résulterait aussi un risque marqué pour la sécurité de la Suisse.

Sur cette base, l'AS-Rens a donc examiné les tâches, les compétences et les responsabilités des fournisseurs de prestations juridiques au SRC du point de vue de l'adéquation et de l'efficacité. Dans le cadre de cette inspection, il faut entendre par prestations juridiques des activités du SRC pouvant par exemple englober la réponse à une question concrète, les clarifications générales en lien avec le contexte juridique, des projets de loi et des décisions de justice, l'exercice de droits litigieux ou non ainsi que la participation à des projets et à la conclusion de contrats. L'AS-Rens n'a en revanche pas examiné le contenu des prestations juridiques fournies du point de vue de leur qualité (légalité).

L'AS-Rens a mené huit entretiens, en particulier avec des cadres. Elle a également interrogé 30 collaborateurs/collaboratrices à l'aide d'un questionnaire, pour connaître leur appréciation sur les prestations fournies. Elle a aussi pris connaissance dans le système de gestion des affaires du SRC de différents documents se rapportant aux tâches et responsabilités, et des prestations juridiques fournies, qu'elle a ensuite analysés et appréciés.

Cette inspection, lancée en 2023, n'était pas terminée à la clôture de la rédaction du présent rapport d'activités, raison pour laquelle ses résultats ne sont pas commentés ici. L'AS-Rens prévoit de publier le résumé de cette inspection sur son site web en 2024.

23-4 IT Service continuity management (ITSCM) et Disaster Recovery-IT au SRC

Lors de la présente inspection, l'AS-Rens a examiné si le SRC disposait de processus efficaces et appropriés pour pouvoir garantir le maintien de l'exploitation informatique et donc de son activité principale, en cas de scénario de crise ou de catastrophe, et pour pouvoir restaurer ses données.

Les événements majeurs imprévus tels que les incendies, les inondations ou les activités criminelles constituent une menace pour toute organisation. De tels événements sont de nature à potentiellement causer des dommages, notamment à l'infrastructure des technologies de l'information, qui peuvent être bien plus graves qu'une simple panne. Il appartient dès lors aux organisations d'assurer une continuité de leur activité (Business continuity management [BCM]). Le BCM se concentre ainsi sur un événement et s'emploie à réduire l'impact d'un risque sur les prestations et processus opérationnels essentiels.

Une informatique fiable et hautement disponible est essentielle à la survie d'une entreprise, étant donné la grande dépendance de son activité principale envers les technologies de l'information. L'IT Service continuity management (ITSCM), qui découle du BCM, a pour objectif de pouvoir fournir les prestations informatiques critiques identifiées par l'entreprise conformément aux exigences, même en cas d'événement majeur. Pour ce faire, des mesures préventives (renforcement de la résilience) et des mesures préparées en cas de survenue d'un événement (renforcement de la réaction) sont évaluées et mises en œuvre. L'ITSCM doit garantir que les services et l'infrastructure des technologies de l'information et de la communication (TIC) sont disponibles suite à une défaillance ou qu'ils puissent être rétablis dans un délai convenu. Le Disaster Recovery-IT vise quant à lui à remettre les services et l'infrastructure TIC en état suite à une défaillance.

Le thème de l'ITSCM répond ainsi à des risques très actuels et concrets. **La numérisation continuant ses progrès et le traitement des données étant au cœur de l'activité du SRC, celui-ci est d'autant plus dépendant d'une exploitation continue et fiable de ses infrastructures informatiques, et ce dans un monde où la pénurie d'électricité menace, où les cyber-attaques se multiplient et où la guerre n'est plus étrangère au continent européen.** De même, des pertes de données seraient de nature à menacer sa capacité à exécuter sa mission.

La partie BCM avait déjà fait l'objet d'un rapport de l'organe de révision interne du DDPS (rapport I 2022-01 du 15 août 2022). Une des recommandations de ce rapport invitait les unités administratives du DDPS à mettre à jour leur documentation relative au BCM. Le SRC travaille pour appliquer cette recommandation. De plus, la direction du SRC a décidé de n'approuver et de mettre en œuvre un nouveau BCM qu'au terme de sa transformation actuellement en cours. L'AS-Rens a donc fait preuve de retenue quant à ce qui avait trait au BCM.

S'agissant de l'ITSCM, l'AS-Rens a constaté l'absence de documentation. Cette absence de documentation relève d'un défaut de gouvernance TIC au sein du SRC. En effet, les mesures existent, mais ont été prises au niveau technique uniquement. L'unité TIC a ainsi adopté de nombreuses mesures pour garantir une continuité de l'activité en cas d'événement majeur. Ces mesures sont efficaces et adéquates. Elles permettent de limiter les risques de manière conséquente. En particulier, la redondance de l'infrastructure TIC de même que la stratégie de sauvegarde des données sont adéquates et efficaces. Cela étant, il n'existe aucune stratégie de test, de sorte que si les services

TIC bénéficient d'une grande stabilité, il n'est pas certain qu'il en soit de même en cas d'événement majeur. De même, l'absence de tests variés et réguliers ne permet pas de mettre à jour l'ITSCM. Des recommandations ont été prononcées en lien avec la documentation de l'ITSCM et l'organisation de tests.

5.2.3 Collaboration

Dans le domaine « Collaboration », l'AS-Rens examine la collaboration des services avec des autorités nationales et internationales. Dans ce contexte, l'AS-Rens contrôle chaque année la collaboration avec un certain nombre d'organes d'exécution cantonaux (SRCant). En 2023, l'AS-Rens a mené des activités dans les inspections ci-après. La réunion de lancement des audits "23-6 KND NW" et "23-7 KND OW" a encore eu lieu en 2023 et les autres actes d'inspection ont été menées en 2024. L'AS-Rens publiera les résumés des inspections sur son site web dès qu'ils seront terminés.

En 2023, l'AS-Rens a réalisé des actes dans les audits suivants :

23-5 Service de renseignement cantonal Lucerne

L'AS-Rens a examiné la collaboration entre le SRC et le SRCant Lucerne sous l'angle de la légalité, de l'adéquation et de l'efficacité. Elle a abouti à la conclusion que le SRC et le SRCant Lucerne collaboraient étroitement et de bien à très bien dans beaucoup de domaines thématiques. Le SRCant Lucerne exécute les mandats du SRC dans les délais impartis et le contenu est conforme aux attentes. Sur la base de ses activités d'inspection l'AS-Rens a constaté que le SRCant Lucerne disposait d'un très bon réseau, de bonnes connaissances du domaine du renseignement et que les conditions et la motivation pour l'exécution des tâches de renseignement étaient pleinement réunies.

L'AS-Rens a en particulier examiné si l'enregistrement des données personnelles répondait aux exigences légales, en lien avec les tâches, le respect des restrictions de traitement des données ainsi que l'exactitude et la pertinence des informations. Elle n'a constaté aucune anomalie grave à ce sujet, mais a néanmoins suggéré de procéder à un examen systématique dans tous les systèmes d'information.

23-8 SRCant Uri

L'AS-Rens a examiné la collaboration entre le SRC et le SRCant UR sous l'angle de la légalité, de l'adéquation et de l'efficacité. Elle a abouti à la conclusion que le SRC et le SRCant Uri collaboraient étroitement et bien dans beaucoup de domaines thématiques. Le SRCant Uri exécute les mandats du SRC dans les délais impartis et le contenu est conforme aux attentes. L'AS-Rens a eu l'impression que le SRCant Uri disposait de bonnes connaissances du domaine du renseignement et des qualités inhérentes, et que les conditions et la motivation pour l'exécution des tâches étaient présentes.

En outre, l'AS-Rens a examiné si les données enregistrées et les données relatives aux personnes correspondaient aux exigences légales, en lien avec le mandat et en matière de respect des restrictions de traitement des données ainsi que de l'exactitude et de la pertinence des informations. Aucune anomalie n'a été constatée à ce sujet.

23-9 Traitement des mandats de capteurs techniques au Centre des opérations électroniques (COE ; dès le 01.01.2024 : « service Actions dans le cyberspace et dans l'espace électromagnétique (ACEM) »)

Les capteurs techniques sont une source importante d'informations pour les services de renseignement. Comme la technique sous-jacente à cette acquisition évolue constamment et que l'efficacité de cette activité de renseignement peut potentiellement s'améliorer avec le développement technique, les services d'exécution sont contraints de réfléchir en permanence à l'évolution de leurs possibilités d'acquisition d'informations pertinentes pour les services de renseignement. Un risque pourrait survenir que le cadre juridique ne soit pas pris en compte dans ces réflexions.

L'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) a donc examiné le traitement des mandats au sein du Service ACEM au profit des services de renseignement de la confédération dans le domaine des capteurs techniques. Elle a constaté qu'un mandat détaillé et écrit de la part des services était toujours nécessaire. La saisie de ces mandats dans un système central de gestion administrative des mandats permet de garantir à tout moment la traçabilité, le respect des délais légaux et l'attribution des résultats aux mandats.

En ce qui concerne les activités opérationnelles, le Service ACEM cherche des moyens d'utiliser des outils intelligents afin, d'une part, de décharger les ressources humaines limitées des activités de routine et, d'autre part, de mieux utiliser les données obtenues par la reconnaissance radio et radar, notamment en ce qui concerne les futures cybermenaces.

En ce qui concerne le respect des bases légales dans les activités opérationnelles, l'AS-Rens a pu constater que les collaborateurs du Service ACEM sont régulièrement sensibilisés à la pertinence des bases légales pour leurs activités quotidiennes, mais qu'il existe également des mesures organisationnelles, comme par exemple des *peer reviews* internes des résultats ou des directives par les responsables du Service ACEM.

Dans l'ensemble, l'AS-Rens n'a pas trouvé d'indices selon lesquels le Service ACEM violerait les bases légales lors de l'utilisation des capteurs techniques pour le traitement des mandats des services ou qu'il ne les utiliserait pas de manière efficace et appropriée.

23-10 La collaboration du SRC avec des particuliers

Le SRC mène une partie de ses activités de recherche sous couverture, évitant que les États concernés ou d'autres acteurs n'identifient et n'empêchent ses recherches d'informations. Ainsi, tant le personnel que les infrastructures et les sources d'information du SRC sont protégés.

Pour dissimuler l'appartenance d'une personne au SRC ou son activité pour le compte de ce dernier, il faut créer et maintenir des couvertures efficaces. Pour ce faire, le SRC a notamment besoin de l'aide de particuliers. Dans le cadre de cette inspection, le terme de « particulier » a été utilisé pour désigner tout ce qui n'est pas considéré comme un service officiel suisse ou étranger.

Selon la LRens, le SRC peut collaborer avec des particuliers, des entreprises ou des organisations. Ceux-ci peuvent fournir des prestations au SRC servant à l'accomplissement de ses tâches conformément à la LRens et le soutenir dans sa recherche d'informations. Le SRC peut par ailleurs confier des mandats de recherche à des particuliers, lorsque c'est nécessaire pour des raisons techniques ou d'accès au renseignement. Des questions se posent à cet égard quant à la légitimité du mandat et de l'organisation. Les éléments à considérer sont par exemple le contournement de mesures de recherche soumises à autorisation, le comportement illégal des particuliers, des paiements sans contre-prestations ou la collaboration avec des personnes à la réputation douteuse. Il est important de garder une vue d'ensemble des particuliers engagés en lien avec leur recrutement, les contrôles de sécurité, l'indemnisation, la documentation de suivi, etc.

Des activités menées sans précaution – notamment par des particuliers – peuvent permettre à des tiers de tirer des conclusions indésirables sur des personnes ou des infrastructures du SRC ou sur ses sources et ainsi les mettre en péril. Les particuliers engagés par le SRC peuvent aussi, consciemment ou non, se comporter de manière illégale en fournissant des prestations au SRC. Outre des effets opérationnels – par exemple entrave, voire même empêchement, à la recherche d'informations – l'exposition à ces risques aurait inmanquablement des conséquences aussi sur la réputation et la crédibilité du SRC.

L'AS-Rens a dès lors examiné si la collaboration du SRC avec des particuliers et le fait de leur confier des mandats sont conformes au droit. Elle a également vérifié que les mandats confiés à des particuliers par le SRC fassent l'objet d'une analyse systématique du rapport bénéfice/risques. Enfin, elle a veillé à ce que la collaboration avec des particuliers et leur engagement soient organisés et coordonnés de manière efficace et adéquate tout en veillant à les documenter de manière compréhensible et probante.

Cette inspection, lancée en septembre 2023 n'était pas terminée à la clôture de la rédaction du présent rapport d'activités. C'est la raison pour laquelle ses résultats ne sont pas commentés ici. L'AS-Rens prévoit de publier le résumé de cette inspection sur son site web dans le courant de l'année 2024.

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 à la vie privée des personnes concernées. En 2023, l'AS-Rens s'est attelée aux inspections ci-après.

22-10 Mesures de recherche non soumises à autorisation

Le SRC peut recourir de manière autonome et sans autorisation externe particulière à des mesures de recherche non soumises à autorisation pour collecter des informations, car l'intensité de l'atteinte aux droits fondamentaux occasionnée par ces mesures est relativement faible. Si ces mesures de recherche ne suffisent pas à obtenir des informations élémentaires pour le maintien de la sécurité de la Suisse, le SRC peut porter atteinte plus gravement aux droits fondamentaux des personnes concernées au moyen de mesures de recherche soumises à autorisation. Plus l'atteinte aux droits fondamentaux est grave, plus le besoin de contrôle est élevé. C'est pourquoi les mesures de recherche soumises à autorisation doivent être approuvées par le Tribunal administratif fédéral (TAF) et validées par le chef ou la cheffe du DDPS, après consultation préalable de la Délégation du Conseil fédéral pour la sécurité, avant que le SRC ne puisse les exécuter. Il n'existe toutefois pas de contrôle externe pour les mesures de recherche non soumises à autorisation. Un risque subsiste en conséquence que de telles mesures de recherche – lorsqu'elles portent par exemple sur des activités et des installations qui relèvent de la sphère privée protégée – soient mises en œuvre de manière illicite.

L'AS-Rens a donc examiné si le SRC recourt aux mesures de recherche non soumises à autorisation conformément à la loi. Elle a constaté que le SRC dispose en principe des moyens opérationnels praticables ainsi que des capacités correspondantes pour mettre en œuvre toutes les mesures de recherche non soumises à autorisation selon les art. 14 et 16 LRens de manière adaptée et proportionnée à la situation.

Elle a en outre constaté que le processus défini par le SRC pour engager une mesure de recherche non soumise à autorisation selon les art. 14 et 16 LRens créait les conditions nécessaires à l'exécution légale de ces mesures. En principe, les mesures de recherche sans autorisation sont mises en œuvre par le SRC conformément à la loi.

Les informations collectées dans le cadre de toutes les mesures de recherche sont inutiles si elles ne peuvent pas être exploitées en temps utile et de manière systématique (de manière efficace et appropriée). Pour l'évaluation de vidéos par exemple, le SRC mise sur un soutien électronique en utilisant un logiciel d'analyse. Dans ce cas concret, l'AS-Rens conclut que l'utilisation d'un tel logiciel d'analyse pour soutenir l'activité d'évaluation est conforme au droit.

En ce qui concerne l'utilisation du système de recherches informatisées de police (RIPOL) et de la partie nationale du Système d'information Schengen (N-SIS), l'AS-Rens a examiné les processus de signalement ainsi que les autorisations d'accès et les consultations de données effectuées dans ces deux systèmes. L'AS-Rens a constaté que le processus de signalement dans le RIPOL et le N-SIS est en principe conforme à la loi. En revanche, l'AS-Rens a constaté que toutes les consultations du RIPOL et du N-SIS effectuées par le SRC n'étaient pas documentées de manière à permettre de voir si elles étaient justifiées par des raisons de service. L'AS-Rens recommande donc au SRC de soumettre les consultations RIPOL et N-SIS effectuées par ses collaborateurs à un contrôle régulier et de documenter les contrôles effectués.

Le SRC dispose de possibilités de recherche (par exemple des appareils techniques particuliers pour la surveillance des télécommunications, des appareils de localisation, des techniques de fermeture

ou d'ouverture, etc.) qui, selon l'art. 26 LRens, nécessitent dans tous les cas une autorisation du TAF ainsi qu'un aval selon l'art. 30 LRens. Bien que de telles mesures nécessitent une autorisation et un aval, elles pourraient être utilisées par le SRC à l'insu et sans l'autorisation correspondante des autorités prévues par la LRens. Dans le cadre de ses opérations de contrôle, l'AS-Rens n'a pas trouvé d'indices montrant que le SRC utilise ses possibilités de recherche selon l'art. 26 LRens sans les autorisations et avals correspondants.

23-11 Les opérations, les besoins de clarifications opérationnels et les mesures de recherche soumises à autorisation du SRC

Les opérations de renseignement (OP) et les enquêtes opérationnelles (OPAB) font partie des missions de base du SRC. Elles se caractérisent par leur complexité par rapport aux affaires courantes et la nécessité d'une conduite opérationnelle. Des mesures de recherche soumises à autorisation (MRSA) peuvent par ailleurs être requises au titre d'opérations de renseignement. La complexité des OP et des OPAB et les besoins de clarifications opérationnels induisent régulièrement des risques en termes d'efficacité et d'adéquation. Quant aux MRSA, elles entraînent toujours un risque juridique pour la protection de la vie privée, raison pour laquelle l'AS-Rens examine régulièrement les activités du SRC dans ce domaine.

Dans le cadre de son inspection annuelle récurrente, l'AS-Rens a analysé la légalité, l'adéquation et l'efficacité de cinq OP et de treize OPAB. Elle a vérifié par ailleurs que la mise en œuvre de douze mesures de recherche validées et autorisées correspondait aux décisions du TAF. Les activités d'inspection ont englobé l'étude de documents et des entretiens avec les spécialistes compétents.

Cette inspection a été lancée en 2023 et s'est achevée en février 2024 avec le rapport. L'AS-Rens a publié le résumé de cette inspection sur son site web au début de l'année 2024.

23-12 Les informateurs (HUMINT) du SRC

Pour accomplir ses tâches, le SRC recherche des informations à partir de sources en libre accès et de sources non accessibles au public. Pour ce faire, il recourt à des mesures de recherche, soumises ou non à autorisation. La recherche d'informations par des informateurs est une mesure de recherche non soumise à autorisation. Les informateurs sont des personnes qui communiquent au SRC des informations ou des renseignements, qui fournissent des prestations au SRC servant à l'accomplissement des tâches définies par la LRens ou qui soutiennent le SRC dans sa recherche d'informations. Le renseignement d'origine humaine entraîne souvent des risques personnels élevés, que ce soit pour le personnel du SRC ou les sources elles-mêmes. Il en résulte une responsabilité et un engagement particuliers pour le SRC, qu'il doit prendre au sérieux et qui confèrent plus de poids à la surveillance exercée par l'AS-Rens.

L'AS-Rens a examiné comment le SRC gère concrètement et développe son portefeuille de sources. Elle a effectué des échantillonnages dans la gestion des sources humaines et en a vérifié la légalité, l'adéquation et l'efficacité. En raison de la protection des sources et des personnes, il est particulièrement nécessaire de maintenir le secret dans ce domaine. C'est la raison pour laquelle les inspections HUMINT de l'AS-Rens sont classifiées SECRET.

Cette inspection, lancée en août 2023, n'était pas terminée à la clôture de la rédaction du présent rapport d'activités. C'est la raison pour laquelle ses résultats ne sont pas commentés ici. L'AS-Rens prévoit de publier le résumé de cette inspection sur son site web dans le courant de l'année 2024.

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. L'inspection « 23-14 La mise en œuvre des recommandations de l'AS-Rens » a été supprimée. Dans le domaine « Ressources », l'AS-Rens s'est attelée en 2023 aux inspections ci-après.

22-13 Financements légendés

L'AS-Rens a examiné si le SRC disposait de méthodes légales, adéquates et efficaces pour exécuter des flux financiers de manière à ce que le SRC ne soit pas identifié comme étant l'expéditeur. Elle a en outre vérifié si les moyens financiers ainsi transférés étaient utilisés exclusivement pour l'accomplissement des tâches visées à l'art. 6 LRens.

L'AS-Rens a constaté que le SRC disposait de différentes méthodes éprouvées et opérationnelles pour faire parvenir des fonds à des destinataires de manière à ce que le SRC n'apparaisse pas comme l'expéditeur.

Le SRC qualifie de supporteurs les personnes privées qui l'aident à transférer des fonds de manière dissimulée et les compte parmi les « informateurs ». La LRens qualifie les « informateurs » également les personnes qui soutiennent le SRC dans ses activités et qui lui fournissent des prestations servant à l'accomplissement de sa mission. L'AS-Rens partage cet avis et recommande donc au SRC de rapprocher la gestion des supporteurs de la gestion des « sources humaines au sens strict » et de la réglementer de manière contraignante. Une telle réglementation comprend notamment une analyse systématique et fondée des risques, de l'utilité, du potentiel et des coûts par supporter. En outre, les supporteurs doivent être mentionnés sommairement en tant que « sources humaines » dans le rapport annuel selon l'art. 19 de l'ordonnance du 16 août 2017 sur le service de renseignement (ordonnance sur le renseignement, RS 121.1).

Pour l'exécution de la LRens, le SRC peut collaborer avec des services de renseignement étrangers dans le cadre d'activités communes de collecte et d'analyse d'informations ainsi que d'évaluation de la menace. L'AS-Rens a constaté que le SRC a certes mené des réflexions sur la légalité, le risque (de réputation) encouru et le bénéfice attendu de deux activités communes concrètes avec des services partenaires étrangers, mais qu'il n'a pas suffisamment documenté ces réflexions. L'AS-Rens invite donc le SRC à accorder à l'avenir plus d'attention à une documentation minutieuse et détaillée de ces réflexions et des décisions prises en conséquence.

22-14 Processus de recrutement, d'encadrement et de départ

Le SRC peut être confronté à des risques internes pour sa sécurité, tels que la trahison, le vol de données ou l'espionnage. Des membres du personnel mécontents sont susceptibles de démissionner, ce qui peut mener à des fluctuations délicates sur le plan des ressources humaines (RH). Un savoir-faire précieux peut se perdre et le recrutement rendu ainsi nécessaire mobilise des ressources.

L'AS-Rens estime que ces risques se sont accrus ces dernières années. L'augmentation flagrante des indices et informations relatifs au mécontentement dans les rangs du SRC, les changements à la tête du service, les résultats de la dernière enquête auprès du personnel et les importantes fluctuations au sein du SRC en général confortent cette analyse.

L'AS-Rens a mené de nombreux entretiens et échantillonné des dossiers personnels entre juillet et mi-novembre 2022. Ce contrôle a eu lieu alors que le SRC préparait puis réalisait une phase de transformation, pendant laquelle il a été décidé de réviser des documents et des processus importants dans les domaines du recrutement, de l'encadrement et du départ des membres du personnel. L'AS-Rens a tenu compte de cet état particulier du développement de l'organisation dans son rapport et a constaté, en définitive, que le SRC avait formulé des objectifs pertinents dans sa stratégie RH. Ceux-ci se sont également reflétés dans les objectifs de la transformation.

L'AS-Rens a relevé quelques carences graves dans l'administration et l'encadrement des membres du SRC. Celles-ci doivent être éliminées de toute urgence. Elles concernent la documentation dans les dossiers personnels, le déroulement des entretiens et des évaluations, ainsi que la définition du déroulement des enquêtes relatives à des personnes en situations particulièrement délicates. L'AS-Rens émet différentes recommandations à cet égard. Les ressources des services d'appui du SRC, tels que les RH, doivent notamment être réévaluées pour que les tâches liées aux

processus de recrutement, d'encadrement et de départ puissent être réalisées correctement. Cette réévaluation des ressources est essentielle pour que le SRC puisse tout bonnement mener à bien sa transformation.

5.2.6 Traitement des données et archivage

Dans le domaine « Traitement des données et archivage », l'AS-Rens vérifie 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 2023, l'AS-Rens s'est attelée dans ce domaine aux inspections ci-après.

21-16 Services de télécommunication (SRC)

L'AS-Rens a examiné si les informations du SRC concernant les prestations d'opérateurs de télécommunications choisis étaient fournies de manière légale et adéquate.

Le SRC reçoit des demandes d'accès à des informations de fournisseurs de services de communication dérivés (FSCD), notamment à des données secondaires d'applications de chiffrement de bout en bout d'opérateurs suisses. Par le passé, il a constaté une augmentation de ce type de requêtes.

Comme les plateformes des FSCD faisant l'objet de l'examen sont exploitées en Suisse, elles sont soumises aux dispositions de la loi fédérale du 30 avril 1997 sur les télécommunications (LTC, RS 784.1). Se fondant sur la LRens¹, le SRC peut obtenir des données en vertu de la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS 780.1). Pour que les tâches puissent être accomplies conformément à la LRens, le service Surveillance de la correspondance par poste et télécommunication (service SCPT), rattaché au Département fédéral de justice et police, transmet au SRC, sur demande, des renseignements relatifs aux données².

S'agissant des applications de chiffrement de bout en bout, la loi permet au SRC d'obtenir des informations non soumises à autorisation auprès du service SCPT et d'effectuer des surveillances soumises à autorisation.

Le contrôle a montré que le SRC n'a traité que des demandes liées à sa mission de base. L'AS-Rens a jugé approprié le processus de traitement centralisé des demandes. Les demandes examinées par l'AS-Rens n'étaient pas toujours entièrement documentées par le SRC. En outre, dans un cas s'inscrivant dans le cadre d'une recherche d'informations conforme à la loi, le SRC a traité, sans y être invité, des informations supplémentaires qui lui avaient été communiquées sans base légale. L'AS-Rens a formulé des recommandations concernant ces deux points.

22-15 Open Source Intelligence (OSINT)

Le renseignement en source ouverte ou open source intelligence (OSINT) est un domaine de la recherche d'informations qui évolue très rapidement. Étant donné le recoupement d'un nombre illimité de données en libre accès (Open Source Information, OSINF), les possibilités de récolter des informations sont quasi infinies pour les services de renseignement. L'analyse de ces OSINF, dans le but d'en retirer des informations utiles, est désignée comme OSINT. L'OSINT au sens de mesures de recherche non soumises à autorisation selon l'art. 13 LRens, qui permet au SRC de rechercher des informations pertinentes pour le renseignement dans une grande quantité de données. L'OSINT ne cesse d'évoluer, posant des questions à la fois juridiques et éthiques au sein de la communauté internationale du renseignement, comme par exemple sa délimitation par rapport aux informateurs ou Human Intelligence (HUMINT), notamment en ce qui concerne l'utilisation active d'identités virtuelles dans les relations avec les personnes ciblées ou l'acquisition de banques de données illicite proposée

¹ Art. 25 al. 2 LRens

² Art. 21 et 22 LSCPT

sur internet (*leaks*). C'est la raison pour laquelle l'AS-Rens a décidé d'examiner le risque lié à la gestion de l'OSINT au sein du SRC.

Selon l'art. 13 LRens, on entend notamment par sources d'informations publiques : les médias accessibles au public, les registres des autorités fédérales et cantonales qui sont accessibles au public, les données personnelles que les particuliers rendent accessibles au public et les déclarations faites en public. La délimitation entre OSINT et les mesures de recherche soumises à autorisation (MRSA) n'est pas toujours évidente, et fait également l'objet de discussions avec des services partenaires du SRC et des autorités de surveillance étrangères. S'il n'y a pas de compréhension commune de ces limites, il existe un risque de collecte illicite de données. Les entretiens menés avec le personnel du secteur OSINT du SRC ont montré que les personnes concernées sont conscientes que la situation juridique est complexe. Il n'existe cependant ni critères ni directives structurées sur le cadre juridique de l'OSINT. Les mesures de recherche autorisées par le SRC dans le domaine OSINT ne font pas l'objet de règles claires et uniformes. L'AS-Rens a donc formulé une recommandation visant à ce que le cadre juridique des opérations concrètes menées lors de recherches OSINT du SRC soit défini et des règles uniformes soient fixées pour la gestion de ce domaine.

L'AS-Rens a examiné un certain nombre de recherches OSINT sans trouver la moindre trace de recherche illégale d'information. Selon l'art. 22 al. 1 de l'ordonnance sur l'organisation du gouvernement et de l'administration (OLOGA), en lien avec l'art. 52 LRens, le SRC est tenu de consigner ses propres activités au moyen d'une gestion systématique des affaires. La directive du 7 juillet 2022 relative au classement et à l'archivage de documents au SRC définit par ailleurs en son chapitre 2, sur la base de l'ordonnance sur la gestion électronique des affaires dans l'administration fédérale (ordonnance GEVER), que tous les documents ayant un rapport avec les activités du SRC doivent être enregistrés et classés. Dans quelques cas, la documentation des clarifications OSINT était lacunaire et ne correspondait pas aux directives en vigueur au sein de l'administration fédérale, empêchant l'AS-Rens d'apprécier la légalité de ces recherches, ce qui l'a incitée à formuler une recommandation à cet égard.

Afin de pouvoir générer des informations pertinentes pour les services de renseignement à partir de l'énorme quantité de données accessible dans le domaine public sur Internet de manière adéquate et efficace, on recourt à ce que l'on appelle des outils OSINT. Le SRC utilise à la fois des produits commerciaux standards et des produits développés par lui-même. Grâce à ces outils, le SRC effectue un monitoring permanent et des recherches ciblées, notamment avec des identités d'emprunt virtuelles (VTI). Ces VTI présentent des particularités en raison de leur utilisation pour le renseignement et pourraient donc être considérés comme des cibles potentielles par d'autres services, au point de se retrouver dans la ligne de mire de services partenaires étrangers par exemple. Afin de contrer ce risque, l'AS-Rens a invité de transférer ces identités du SRC dans la banque de données internationale déjà existante et de veiller à ce que le SRC et les Services de renseignement cantonaux (SRCant) s'informent mutuellement sur les identités d'emprunt virtuelles qu'ils utilisent.

Pour la recherche d'information OSINT anonymisée, le SRC recourt à une infrastructure informatique spéciale, qui présente des lacunes de sécurité et devrait être remplacée dans un avenir proche. L'AS-Rens a formulé une recommandation en conséquence.

Il n'est pas toujours facile de vérifier les résultats des recherches OSINT, en particulier lorsqu'il s'agit d'informations générées par le Darknet. Selon le SRC, entretenir une saine méfiance à l'égard des informations fait partie du travail des services de renseignement. Quand une information ne peut pas être vérifiée et que sa véracité ne peut être démontrée, il le mentionne dans les rapports OSINT. La problématique de la vérification des sources joue par exemple un rôle important dans l'identification et la divulgation de fake news. Elle touche en particulier l'utilisation d'outils OSINT commerciaux complexes et fait aussi l'objet de discussions régulières au sein de la communauté du renseignement.

Outre le SRC, les SRCant effectuent aussi des clarifications OSINT. L'AS-Rens a examiné des possibles chevauchements et inefficiences. Elle est arrivée à la conclusion que les deux entités étaient sensibilisées à ces risques et veillaient à avoir des échanges réguliers sur la thématique OSINT, notamment à travers un nouveau cadre.

Le contenu du système d'information du portail ROSO (résultats de recherches et matériel brut issu de sources ouvertes) respecte l'art. 54 al. 2 LRens, et les art. 46ss de l'ordonnance sur les systèmes

d'information et les systèmes de stockage de données du SRC (OSIS-SRC, RS 121.2). Le système d'information permet au SRC de mettre à disposition à l'interne des données issues de sources accessibles au public. Les actes d'inspection, notamment les contrôles par échantillonnage, ont confirmé l'adéquation et l'efficacité de la gestion des données dans le portail OSINT. Il n'y avait pas de risque de prolongation illicite du délai de conservation en raison d'une donnée générée par d'autres capteurs et marquée à tort comme OSINT, car les données OSINT ont un délai de conservation plus court.

22-17 Follow-up 20-19 : les archives du SRC

L'inspection 22-17 a donné suite à l'inspection 20-19 « Archives SRC avec focus sur les archives secrètes ». Cette dernière avait été organisée après que des médias ont rapporté, dans le cadre de l'affaire Crypto AG, que le SRC avait des « archives secrètes ». L'inspection 20-19 avait notamment constaté que des documents analogiques classifiés SECRET étaient conservés dans un emplacement également classifié SECRET. A cette période, le SRC et les Archives fédérales suisses (AFS) étaient en pourparlers pour livrer des documents, dont certains mentionnés par les médias, aux AFS à des fins d'archivage. Ces documents portaient essentiellement sur les organisations précédentes le SRC, soit des documents antérieurs à 2010. L'AS-Rens avait en conséquence renoncé à émettre des recommandations et avait annoncé qu'une inspection de suivi aurait lieu.

Outre des risques réputationnels, l'inspection 22-17 a examiné des risques en termes de légalité, d'adéquation et d'efficacité de l'archivage et de la conservation des documents. En matière d'archivage, il s'agissait d'éclaircir si les documents ont été proposés et livrés conformément à la loi et à la convention et de contrôler si des documents ont été soustraits ou détruits, ceci respectivement avant ou après avoir été proposés aux AFS ou après qu'une valeur archivistique leur soit reconnue. Concernant la conservation des documents, l'inspection devait vérifier si des documents conservés auraient dû être archivés et si les normes régissant la conservation étaient respectées.

Au cours de l'inspection 22-17, l'AS-Rens a organisé des visions locales des emplacements dans lesquels des documents sont encore conservés et a procédé à des échantillonnages. Elle a pu constater que les travaux d'archivage des documents analogiques (principalement des documents papier et des microfiches) ont notablement avancé dans les différents emplacements dans lesquels le SRC conserve ses documents. D'une manière générale, l'AS-Rens constate que la situation a concrètement et positivement évolué et que les engagements pris lors de l'inspection 20-19 (principalement la mise en œuvre de la convention avec les AFS) ont été tenus. Ces travaux sont conformes à la convention conclue entre le SRC et les AFS. Les délais de livraison n'ont pas pu être respectés pour des raisons compréhensibles et plausibles et pas nécessairement imputables au SRC. Plusieurs milliers de documents (près de 200 mètres-linéaires) et des millions de microfiches concernant principalement les organisations précédentes le SRC ont ainsi été inventoriés et livrés aux AFS. Les documents livrés couvrent une période allant de 1938 à 2021.

Etant donné que les documents des organisations précédentes n'étaient pas inventoriés, l'AS-Rens n'a pas été en mesure d'examiner les risques identifiés, à savoir si tous les documents ont bien été proposés et livrés aux AFS, ou si des documents auraient été – accidentellement ou intentionnellement – détruits. Sur ce dernier point, l'AS-Rens n'a trouvé aucun indice indiquant que ces risques se seraient réalisés.

Les travaux de tri et d'archivage des documents sont toujours en cours. A cet égard, la convention n'a pas encore été pleinement mise en œuvre et le SRC a été invité à y remédier. L'AS-Rens, constatant que les documents conservés ne sont pas inventoriés, a émis une recommandation au sens de la laquelle le SRC devra dresser un inventaire des documents qui ne seront pas livrés au AFS et conservés par le SRC.

22-18 Recherche d'informations par l'unité Cyber du SRC

La recherche illégale d'informations par l'unité Cyber du SRC, thématisée dans différents médias, a été traitée par le SRC lui-même à travers une enquête interne et une enquête administrative externe. Du point de vue de l'AS-Rens, les deux rapports d'enquête laissaient des questions ouvertes, raison pour laquelle l'AS-Rens a initié sa propre inspection afin de clarifier les zones d'ombre restantes. L'analyse des vastes fichiers de données, qui n'ont été ni examinées ni évaluées jusqu'à présent par le SRC lui-même ou dans le cadre de l'enquête administrative, s'est révélée complexe et requiert un investissement considérable en temps, raison pour laquelle l'inspection n'était pas achevée à la clôture de la rédaction du présent rapport d'activités et ses résultats ne sont pas commentés ici. L'AS-Rens prévoit de publier le résumé de cette inspection sur son site web dans le courant de l'année 2024.

23-16 Les systèmes d'information, les systèmes de stockage et stockage des données en dehors du cadre de l'art. 47 de la loi fédérale sur le renseignement

La LRens comporte des règles en matière de traitement des données dont l'article 47 LRens qui livre une liste de systèmes d'information exploités par le SRC. L'exhaustivité de cette liste a déjà fait débat lors de la création de la nouvelle loi sur le renseignement. L'AS-Rens a voulu clarifier cette question juridique et également évaluer quels autres systèmes sont utilisés et pour quelles raisons. Les bases légales y relatives ont également été analysées.

Cette inspection, lancée en août 2023, n'était pas achevée à la date de clôture du présent rapport d'activités. C'est pourquoi il n'est pas encore possible de faire d'autres déclarations sur les résultats de l'audit à ce stade. L'AS-Rens prévoit de publier le résumé de cette inspection sur son site web dans le courant de l'année 2024.

Clarification de la cyberattaque visant l'entreprise Xplain AG

En raison de la cyberattaque ayant visé l'entreprise Xplain AG, l'AS-Rens a procédé à une clarification en dehors de sa planification annuelle des inspections. L'accent a été mis sur la question de savoir si et dans quelle mesure l'attaque concernait aussi des données du SRC et comment celui-ci a traité ce cyberincident dans le cadre de sa mission de base. Les observations tirées de cette clarification ont été intégrées en partie à l'inspection « 23-10 La collaboration du SRC avec des particuliers ».

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. Quant aux personnes concernées, elles étaient à leur disposition. Des réponses ont par ailleurs été apportées aussi vite que possible aux questions additionnelles.

5.4 Mise en œuvre des recommandations

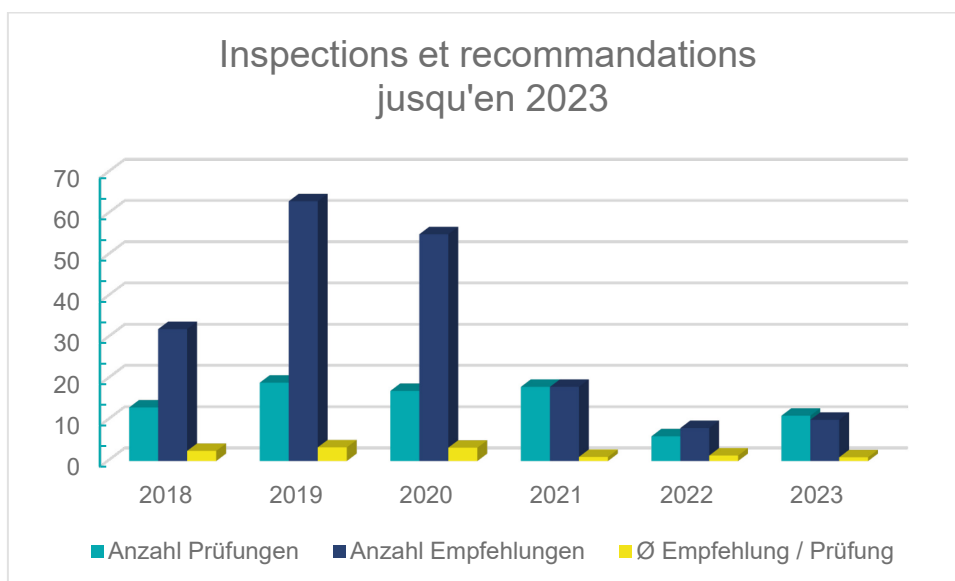
L'AS-Rens peut formuler des recommandations sur la base de ses activités d'inspection. Ses recommandations sont adressées à la cheffe ou au chef du DDPS, qui veille à leur mise en œuvre concrète. Si le DDPS venait à rejeter une recommandation, il devrait la soumettre à l'ensemble du Conseil fédéral pour décision, mais un tel cas n'est encore jamais survenu.

Les bases légales précisent que l'AS-Rens peut formuler des recommandations et que le DDPS veille à leur mise en œuvre. Les bases légales du renseignement prévoient certes la possibilité pour l'AS-Rens de formuler une recommandation, mais ne précisent pas la manière dont cette recommandation doit être mise en œuvre ou contrôlée.

Une surveillance efficace et crédible n'est toutefois possible que si les recommandations émises sont mises en œuvre, d'une part, et si, d'autre part, leur application correcte est également vérifiée. D'entente avec les services inspectés et le DDPS, l'AS-Rens cherche donc continuellement à affiner cette partie complexe de la surveillance.

Le tableau ci-après montre le rapport entre le nombre d'inspections et les recommandations correspondantes sur les six dernières années. Après une première phase de trois ans pendant laquelle chaque inspection a été assortie de deux à trois recommandations en moyenne, ce nombre a baissé ces trois dernières années à environ une recommandation par inspection. L'AS-Rens applique une approche systématique qui vise à fournir une utilité concrète en termes de réduction ou d'élimination des risques qui se reflète dans les chiffres. Il en résulte des recommandations en moins grand nombre, mais plus ciblées et efficaces. D'ailleurs, le nombre de recommandations n'est pas un indicateur d'amélioration atteinte ou de détérioration de la situation, puisqu'aucune inspection ne ressemble à une autre.

	2018	2019	2020	2021	2022	2023
Nombre d'inspections	13	19	17	18	6	11 ³
Nombre de recommandations	32	63	55	18	8	10
Ø Recommandation / inspection	2,46	3,32	3,24	1,00	1,33	0,91



³ 21-16 (2) / 22-1 (1) / 22-5 (0) / 22-8 (0) / 22-10 (1) / 22-13 (1) / 22-14 (4) / 22-17 (1) / 23-5 (0) / 23-8 (0) / 23-9 (0)

6 Regard interne

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

6.1 Personnel

En 2023, l'AS-Rens comptait un effectif réglementaire de dix personnes. Au cours de l'année, deux personnes ont quitté l'AS-Rens et ont été remplacées par deux nouvelles personnes.

6.2 Formations et perfectionnements

Formation continue en science des données auprès d'armasuisse

Pendant l'année sous revue, l'AS-Rens a profité de la possibilité offerte par armasuisse de s'informer sur l'état des projets de recherche actuels. Comme l'année précédente, le programme de recherche en science des données s'est retrouvé au cœur de l'intérêt de l'AS-Rens. Alors qu'en 2022, les conférenciers avaient mis l'accent sur les méthodes d'authentification des contenus visuels et médiatiques, le symposium de cette année s'est penché sur l'utilisation de l'intelligence artificielle dans l'analyse des données, et plus précisément sur les outils basés sur l'IA, dont l'évolution est extrêmement rapide. L'IA est désormais en mesure de récolter des informations à partir de données qui permettent à leur tour de générer du savoir. C'est ainsi que les outils IA d'aujourd'hui sont utilisés afin d'identifier des modèles et des redondances dans des fichiers de données. Le but de la recherche consiste actuellement à développer l'IA de manière à pouvoir en tirer des conclusions utiles pour l'avenir. La compréhension des corrélations, y compris fictives, de données joue ici un rôle important, de même que celle des méthodologies permettant de garantir la robustesse des inductions.

Formation continue sur la réalisation d'audits

Deux personnes de l'AS-Rens ont suivi un perfectionnement proposé en allemand par le centre de formation de l'administration fédérale (CFAF) qui portait sur l'exécution d'audits. Le choix s'est porté sur ce perfectionnement, qui permet d'aborder les meilleures pratiques en matière d'audit, de rafraîchir certaines compétences et de comparer sa propre pratique avec celle d'autres services de l'administration fédérale qui réalisent des audits.

Le contenu était axé sur les différentes étapes d'un audit, de la préparation à la finalisation. Le rôle des auditrices et auditeurs et les principes d'un audit ont aussi été abordés. Les personnes participant au cours ont pu échanger leurs expériences lors de différents travaux de groupe. Le dernier sujet traité a été celui de la formulation de recommandations et de conclusions dans un audit.

Cette dernière partie a apporté une plus-value toute particulière au personnel de l'AS-Rens, car la formulation de recommandations est un sujet discuté en interne dans un but d'amélioration. Les deux personnes de l'AS-Rens ont pu traiter cette thématique de manière approfondie dans le cadre d'un travail de transfert. Le document qu'ils ont rédigé dans ce but servira de base de réflexion pour les optimisations visées à l'AS-Rens. Il conclut que, dans la formulation de recommandations, il faut trouver un équilibre entre d'une part aborder tous les points en détail et d'autre part laisser une marge de manœuvre à l'autorité inspectée, qui va mettre la recommandation en œuvre. Une bonne formulation permet au service inspecté de bien comprendre le risque à minimiser, ce qui favorise la mise en œuvre.

Certificate of Advanced Studies (CAS) *Digital Forensics and Cyber-Investigation-Fundamentals*

Durant l'année sous revue, un collaborateur de l'AS-Rens a effectué un CAS sur la thématique de la criminalistique numérique et de la cyber-investigation, englobant les quatre modules conçus sous forme de blocs que sont « Bases de criminalistique digitale », « Bases de cyber-investigation », « Panorama de la cybercriminalité » et « Recherche grâce à la criminalistique digitale ». Les leçons tirées de ce perfectionnement ont profité directement à l'inspection 22-18 et à l'analyse de données qui en a découlé. C'est ainsi qu'une procédure connue de criminalistique digitale a été utilisée pour analyser un large jeu de données.

CAS en communication

L'AS-Rens élabore les contenus qu'elle publie sur son site web de manière autonome, y compris son rapport d'activités annuel. Une collaboratrice a entamé un CAS en communication, qu'elle terminera en 2024, pour approfondir le savoir-faire technique du service en matière de communication.

Conférence Europe de l'ISACA⁴ : *Digital Trust World*, 18-19 octobre 2023, Dublin

L'ISACA est une association professionnelle indépendante qui rassemble une large communauté professionnelle (experts-comptables, auditeurs, contrôleurs de gestion, etc.) active dans les domaines de la gouvernance des systèmes d'information et de la sécurité de l'information. Un collaborateur de l'AS-Rens disposant d'une certification ISACA en audit informatique a participé à la conférence européenne annuelle de deux jours de l'association.

Différents exposés spécialisés sur des sujets d'actualité en rapport avec un écosystème numérique sûr et fiable ont permis d'élargir les connaissances spécialisées, d'échanger et de discuter des enseignements à tirer, des tendances et des bonnes pratiques. L'accent a été mis aussi sur l'influence que pourrait avoir l'intelligence artificielle et l'apprentissage automatique (*machine learning*) sur la situation en matière de sécurité, mais aussi sur l'activité de révision dans le domaine cyber. Les leçons qui en ont été tirées ont profité tant à la gestion des risques interne à l'AS-Rens qu'à ses activités d'inspection.

Séance d'information du PFPDT sur la protection des données, 17 août 2023, Fribourg (CH)

Dans la perspective de l'entrée en vigueur de la nouvelle LPD, le PFPDT a organisé une séance d'information pour les préposés à la protection des données des organes fédéraux. Les deux personnes de l'AS-Rens qui y ont participé ont notamment eu l'occasion de rencontrer des membres des services soumis à la surveillance de l'AS-Rens.

Le PFPDT et son équipe ont présenté les thèmes en rapport avec les nouveautés introduites par la LPD. Le Centre national pour la cybersécurité (NCSC) et l'Office fédéral de la police (fedpol) sont également intervenus, présentant par exemple l'analyse d'impact relative à la protection des données personnelles (AIPD), l'utilisation du nouveau registre des activités de traitement, la nouvelle compétence du PFPDT en matière d'enquête portant sur des violations des prescriptions de protection des données, la journalisation et bien d'autres dimensions encore. Les présentations, très instructives, seront utiles à la fois pour l'activité administrative de l'AS-Rens et pour ses activités de surveillance.

6.3 Inspection de l'AS-Rens par le Contrôle fédéral des finances (CDF)

Organe suprême de surveillance financière de la Confédération, le CDF est à la fois autonome et indépendant, dans le respect des prescriptions légales. Il jouit comme l'AS-Rens d'une indépendance institutionnelle garantie par la loi.

Le CDF exerce sa surveillance financière selon les critères de la conformité, de la légalité et de la rentabilité. Il examine notamment les systèmes de contrôle internes ou, par pointage, les ordres de paiement émis par les unités administratives (UA). Il est responsable de la révision des UA, comptabilités et stocks compris. Ses critères d'inspection diffèrent de ceux de l'AS-Rens dont le mandat légal se distingue clairement de la surveillance financière exercée par le CDF.

Dans son programme annuel 2023, le CDF a annoncé un contrôle portant sur l'activité de surveillance de l'AS-Rens qui s'est tenu du 14 août au 1^{er} septembre 2023. Le but de cet audit était d'examiner l'efficacité et la rentabilité de la surveillance exercée par l'AS-Rens sur les activités de renseignement. En date du 12 juin 2023, le CDF a posé les questions suivantes à l'AS-Rens :

⁴ Information Systems Audit and Control Association.

1. La surveillance exercée par l'AS-Rens sur les activités de renseignement est-elle conforme aux bases légales ?
2. Les ressources de l'AS-Rens sont-elles suffisantes pour exercer une surveillance adéquate de tous les acteurs impliqués dans des activités de renseignement ?
3. L'infrastructure informatique en tant qu'outil de travail lui permet-elle d'exercer efficacement la surveillance ?

Au printemps 2023, l'AS-Rens avait déjà fourni au CDF six dossiers d'inspection complets comme échantillon pour les années 2021 et 2022, et d'autres documents (concepts, manuels). Le CDF a aussi mené de nombreux entretiens avec le personnel de l'AS-Rens, différents services soumis à la surveillance de l'AS-Rens et le Secrétariat général du DDPS.

Pendant leur évaluation, les réviseurs du CDF ont été confrontés au défi d'éviter toute comparaison excessive entre leur pratique et celle de l'AS-Rens. **Il était important pour l'AS-Rens que le CDF mesure qu'elle exerce un autre type d'activité de surveillance et ne fonctionne donc pas sur le même mode que le CDF.** Ces différences fondamentales ont été abordées à nouveau lors de la discussion finale, pour harmoniser les compétences différentes des deux autorités. Le CDF continue à exercer sa surveillance selon ses propres critères, la création de l'AS-Rens n'ayant rien changé à son rayon d'action.

6.4 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.

La loi fédérale sur le principe de la transparence dans l'administration (LTrans ; RS 152.3) régit l'étendue et les limites de l'information passive. Chaque personne a le droit de consulter des documents officiels, sans faire valoir d'intérêt particulier. Durant l'année sous revue, l'AS-Rens a reçu une demande en vue d'accéder à des documents officiels.

7 Coordination

Au sens de l'art. 78 al. 2 LRens, l'AS-Rens coordonne ses activités avec la haute surveillance parlementaire et avec d'autres autorités de surveillance de la Confédération et des cantons.

7.1 Contacts nationaux

Délégation des Commissions de gestion (DélCdG)

La DélCdG a invité l'AS-Rens à deux auditions. Au cours de celles-ci, les thèmes suivants ont notamment été abordés : le rapport d'inspection « 22-13 Financements légendés », les expériences de la cheffe pour sa première année de fonction, le développement de la pratique des recommandations de l'AS-Rens et le plan des inspections 2024.

Tribunal administratif fédéral (TAF)

Pendant l'année sous revue comme pendant celles qui l'ont précédée, l'AS-Rens a échangé avec le TAF autour de thèmes tels que les opérations en cours du SRC qui ont fait l'objet de mesures de recherche soumises à autorisation et ont été présentées au TAF pour approbation, et tels que les développements actuels dans le domaine de l'exploration du réseau câblé.

Ces échanges ont permis de constater que la jurisprudence ne cesse d'évoluer et que le TAF était de plus en plus souvent confronté à des questions techniques dans le domaine cyber.

L'AS-Rens se trouve confrontée au même défi, car ses activités d'inspection interviennent de plus en plus au niveau des systèmes d'information, en raison de la digitalisation galopante. Les deux autorités en ont conclu que, sans explication des services de renseignement sur les tenants et

aboutissants techniques, il n'était possible ni de statuer sur une proposition ni de procéder à une inspection suffisamment étendue.

Contrôle fédéral des finances (CDF)

Les rencontres suivantes ont eu lieu dans le cadre de la coordination avec le CDF :

- le 20 février 2023 pour présenter l'IIA (Institute of Internal Auditors) à l'AS-Rens, et discuter des avantages et des inconvénients d'une affiliation ;
- le 13 mars 2023 pour échanger sur les critères de protection en faveur des collaborateurs qui signalent un comportement préjudiciable au sein de l'administration fédérale (whistleblowing) ont été discutés ;
- le 6 décembre 2023 pour faire connaissance avec le nouveau responsable du mandat pour le DDPS et pour discuter de coordination, en vue de conclure, le cas échéant, un accord de coordination visant à définir les dimensions communes ou divergentes des compétences de contrôle et à éviter pouvant laisser dans l'ombre certains aspects des activités de renseignement.

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

L'AS-Rens a participé aux cinq séances de l'OCI.

L'intégration des activités de surveillance de l'AS-Rens prévue dans la révision de la LRens est retardée. C'est pourquoi l'AS-Rens continue d'accompagner le travail de coordination de l'OCI, en renonçant pour l'instant à d'autres préparatifs.

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

Dans le cadre de ses activités d'inspection, l'AS-Rens examine des systèmes d'information des services soumis à sa surveillance et la manière dont ceux-ci traitent les données. Elle peut par ailleurs examiner la recherche de données effectuée par lesdits services alors que ce sont d'autres autorités fédérales, non surveillées, qui s'occupent de traiter ces données. L'autorité de surveillance pour le traitement des données par les autorités fédérales est le PFPDT. Ce dernier et l'AS-Rens sont deux autorités totalement indépendantes de l'administration fédérale pour de l'accomplissement de leurs tâches respectives, et leurs responsabilités de se recoupent en partie. Afin d'éviter toute confusion ou redondance pour les autorités soumises à surveillance, l'AS-Rens et le PFPDT coordonnent leurs activités à travers des séances et des échanges réguliers.

Lors d'une séance de coordination entre le PFPDT et la cheffe de l'AS-Rens en février 2023, il a été convenu de formaliser la pratique actuelle, qui est efficace et judicieuse. En mai 2023, les deux instances ont signé une convention en ce sens.

Citoyennes et citoyens

En 2023, l'AS-Rens a reçu 20 demandes de citoyennes et citoyens.

Autres réunions

En 2023, la direction de l'AS-Rens a rencontré au moins une fois les personnes ci-après pour un échange :

- cheffe du DDPS
- chef de l'Armée
- secrétaire général du DDPS

- directeur du SRC et son suppléant
- chef du RM
- chef du COE
- chef de la Révision interne du DDPS
- chef du commandement des Opérations
- chef du commandement Cyber
- conseillère de la cheffe du DDPS en matière de renseignement
- les membres de l'OCI

7.2 Contacts internationaux

L'AS-Rens peut échanger des informations sur les méthodes, les processus et les expériences de surveillance avec des autorités de surveillance d'autres pays actives dans le même domaine d'activités, ce qui s'avère toujours avantageux pour les activités d'inspection. L'AS-Rens, au contraire des services de renseignement, n'a toutefois pas de base légale pour échanger des contenus avec des autorités partenaires étrangères. En 2023, les réunions internationales ci-après ont eu lieu.

Réunion virtuelle avec l'autorité canadienne de surveillance (National Security and Intelligence Review Agency [NSIRA]), 27 avril 2023

Après la visite d'une délégation de la NSIRA le 17 novembre 2022 à Berne, les deux autorités de surveillance ont organisé une réunion à distance en date du 27 avril 2023.

À cette occasion, la NSIRA a notamment présenté son histoire, son mandat et sa structure. Elle a été créée en 2019 en tant qu'organe indépendant qui répond de ses activités auprès du Parlement. Ses tâches consistent essentiellement à mener des inspections et à traiter des recours. Elle examine la légalité, l'adéquation, la nécessité et l'efficacité des activités menées au service de la sécurité nationale et des activités de renseignement de tous les ministères et services du gouvernement canadien. Elle prononce des recommandations dans ses inspections. L'activité de la NSIRA est semblable à celle de l'AS-Rens. Plus de 70 personnes travaillent au sein du Secrétariat de la NSIRA et son rayon d'action est bien plus large que celui de l'AS-Rens. Pour des raisons d'organisation, la NSIRA, au regard de l'évolution des technologies et de leur utilisation pour des activités de renseignement, profite du soutien d'une unité spécialisée dans ce domaine.

Intelligence Oversight Working Group (IOWG)

L'IOWG est un groupe de travail international réunissant les autorités de surveillance de l'Angleterre, de la Belgique, du Danemark, de la Norvège, des Pays-Bas, de la Suède et de la Suisse. Depuis novembre 2023, l'autorité canadienne NSIRA dispose du statut d'observateur pour 2024 auprès de ce groupe de travail.

Réunion de l'équipe IOWG, 25-26 mai 2023, La Haye

Au début de la rencontre, les participants ont présenté différentes évolutions dans leurs États respectifs depuis la réunion de 2022. À l'avenir, les Pays-Bas vont mettre à la disposition des membres IOWG une plateforme numérique sur laquelle les représentations pourront s'enregistrer. La Norvège a présenté ses méthodes et son mode de travail dans le domaine de la communication. Le recours à des agents virtuels a été abordé à partir des différentes régulations juridiques existant dans les pays membres. Il convient de bien délimiter ce domaine par rapport à l'OSINT. Enfin, un technicien de l'autorité néerlandaise de surveillance a présenté ses réflexions sur l'IA et la prise de décision automatisée, un sujet dont les services et les organes de surveillance devaient davantage se préoccuper selon l'assemblée.

Réunion de l'équipe IOWG, 8-9 novembre 2023, Oslo

Le 8 novembre 2023, les membres du groupe de travail IOWG se sont rencontrés pour une réunion préparatoire à la séance des responsables, qui s'est tenue le lendemain. Une proposition de

calendrier pour les réunions de l'année suivante a pu être élaborée. Les thèmes suivants ont été proposés :

- jeux de données achetés commercialement utilisés par les services soumis à la surveillance ;
- organisation d'une réunion à distance pour traiter certains thèmes entre deux réunions ;
- contrôle de sécurité relatif aux personnes : échange sur les prescriptions et pratiques en matière de contrôle de sécurité relatif aux personnes dans les différents États membres ;
- discussion sur de possibles formes de collaboration internationale entre organes de surveillance ;
- surveillance en général : présentation des méthodes de surveillance utilisées dans les différents pays.

Réunion des responsables IOWG, 9 novembre 2023, Oslo

Les responsables des différents organes de surveillance se sont rencontrés le 9 novembre 2023. Le calendrier proposé par l'équipe a été approuvé et la volonté de mener une discussion approfondie sur la méthodologie a été saluée. À sa demande, un statut d'observatrice a été octroyé à l'autorité canadienne de surveillance au sein du groupe de travail IOWG.

Réunion IOWG avec une autorité américaine et diverses ONG, 27 novembre 2023, Washington DC

En date du 27 novembre 2023, le matin, le groupe de travail IOWG a organisé, en marge de l'IIOF à Washington (voir plus bas), une séance avec le Conseil de supervision sur la vie privée et les libertés civiles (*Privacy and Civil Liberties Oversight Board*, PCLOB). Le PCLOB est une agence exécutive indépendante, qui a été constituée à travers le *9/11 Commission Act* de 2007. Composé de cinq personnes, non partisan, ce conseil est nommé par le Président et confirmé par le Sénat. Son président exerce sa fonction à temps plein alors que les quatre autres membres sont engagés à temps partiel. Le conseil a pour mission de veiller à ce que les efforts du gouvernement fédéral en matière de lutte contre le terrorisme soient mis en œuvre en respectant le droit à la vie privée et les libertés civiles. Les échanges sur le terme d'open dans les recherches de type *open source* (OSINT) et sur l'évolution rapide et l'utilisation des outils d'IA ont été particulièrement intéressants.

L'après-midi, une réunion a eu lieu au *Center for Democracy & Technology*, ouverte à d'autres ONG. À cette occasion également, les recherches OSINT ont été largement discutées, avec un accent particulier mis sur la question des *data broker*. Les échanges se sont ensuite concentrés sur la question de savoir si ou comment les services de renseignement pourraient partager des informations et ainsi contourner les limites de l'obligation d'autorisation liées à de telles informations.

European Intelligence Oversight Conference (EIOC), 9-10 novembre 2023

Le programme de la conférence de cette année a abordé des sujets aussi variés que :

- méthodes de surveillance en général ;
- utilisation disproportionnée par les services de renseignement de données accessibles au public et mesures à prendre ;
- échange de fond sur la jurisprudence la plus récente de la Cour européenne des droits de l'Homme ;
- méthodes techniques de surveillance ;
- aspects de la communication par les autorités de surveillance.

L'AS-Rens a pu profiter des échanges personnels avec les différents participants aux séances pour discuter des questions de méthodes de surveillance et de cadre légal.

International Intelligence Oversight Forum (IIOF), 28-29 novembre 2023, Washington DC

Les 28 et 29 novembre 2023 s'est déroulé le 6ème « International Intelligence Oversight Forum (IIOF) » à l'*American University Washington College of Law* à Washington. La Cheffe de l'AS-Rens et un collaborateur s'y sont rendus aux côtés de nombreux membres d'organes de surveillance (administratifs et parlementaires) du renseignement, mais aussi des représentants d'agences de renseignement, d'autorités de protection des données et des organisations non-gouvernementales (ONG).

Les thématiques traitées ont été les suivantes :

- Surveillance nécessaire et proportionnée : protéger la vie privée et la sécurité nationale des deux côtés de l'Atlantique.
- La déclaration de l'Organisation de coopération et de développement économiques (OCDE) du 14 décembre 2022 sur l'accès des pouvoirs publics aux données à caractère personnel détenue par des entités du secteur privé : qu'est-ce que cela signifie et qu'est-ce qui va suivre ?
- Partage de bonnes pratiques sur la manière d'intégrer des garanties dans les opérations des agences de renseignement
- Des défis similaires, des cadres différents : Un examen comparatif de la manière dont les pays réglementent leurs activités de renseignement
- Article 11 de la convention 108+ du Conseil de l'Europe : état d'avancement, défis et enseignements tirés

A la suite des différentes présentations et des débats, une visite de l'*Intelligence Community Campus* à Bethesda a eu lieu.

Les thématiques traitées et les échanges amènent de réelles plus-values dans le cadre des activités de surveillance de l'AS-Rens. De même, les organes de surveillance sont susceptibles d'apprendre du monde de la recherche (universitaire, ONG, etc), lequel pose un regard (toujours) critique et (souvent) constructifs sur le sujet de la surveillance. Les différentes manières d'exercer la surveillance, qu'elles résultent de différences de cadre légal et/ou de culture, les contraintes ou les défis qui se posent aux activités de surveillance permettent à l'AS-Rens de remettre en question sa pratique, de la développer et de l'améliorer.

8 Annexe

8.1 Plan des inspections 2023

No	Titre	Organe inspecté
Stratégie et planification		
23-1	La production du Service de renseignement de la Confédération (SRC) en tenant compte des besoins des clients	SRC
Organisation		
23-2	Les prestations juridiques du SRC	SRC
23-3	La protection et la sécurité au SRC	SRC
23-4	La gestion de la continuité des affaires dans le domaine de l'informatique (IT) et le disaster-recovery IT au SRC	SRC
Collaboration		
23-5	Service de renseignement cantonal (SRCant) Lucerne	SRCant / SRC
23-6	SRCant Nidwald	SRCant / SRC
23-7	SRCant Obwald	SRCant / SRC
23-8	SRCant Uri	SRCant / SRC
23-9	Le traitement des mandats concernant les capteurs techniques au Centre des opérations électroniques (COE)	COE
23-10	La collaboration du SRC avec des particuliers	SRC
Recherche d'informations		
23-11	Les opérations, les besoins de clarifications opérationnels et les mesures de recherche soumises à autorisation du SRC	SRC
23-12	Les informateurs (HUMINT) du SRC	SRC
23-13	L'engagement d'agents virtuels au SRC	SRC
Ressources		
23-14	La mise en œuvre des recommandations de l'AS-Rens	SRC / RM ⁵ / COE
Traitement des données / archivage		
23-15	La mise en œuvre du droit d'accès au SRC	SRC
23-16	Les systèmes d'information, les systèmes de stockage et l'archivage des données en dehors du cadre de l'art. 47 de la loi fédérale sur le renseignement	SRC

⁵ Renseignement militaire

8.2 Liste des abréviations

ACEM	Service Actions dans le cyberspace et dans l'espace électromagnétique
AFS	Archives fédérales suisses
Al.	Alinéa
Art.	Article
AS-Rens	Autorité de surveillance indépendante des activités de renseignement
BCM	Business Continuity Management
CAS	Certificate of Advanced Studies
CDF	Contrôle fédéral des finances
CFAF	Centre de formation de l'administration fédérale
COE	Centre des opérations électroniques (jusqu'au 31.12.2023)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DéICdG	Délégation des Commissions de gestion
Etc	et cetera
Fedpol	Office fédéral de la police
FF	Feuille fédérale
FSCD	Fournisseurs de services de communication dérivés
HUMINT	Human Intelligence, recherche d'informations par des informateurs
IA	Intelligence artificielle
IIA	Institute of Internal Auditors
IIOF	International Intelligence Oversight Forum
IOWG	Intelligence Oversight Working Group
ISACA	Information Systems Audit and Control Association
IT	Information Technology, technologies de l'information
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)
LSCPT	Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
LTC	Loi fédérale du 30 avril 1997 sur les télécommunications (RS 784.1)
LTrans	Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (Lois sur la transparence, RS 152.3)
MRSA	Mesures de recherche soumises à autorisation
NSIRA	National Security and Intelligence Review Agency
N-SIS	Partie nationale du Système d'information Schengen
OCI	Organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé
OLOGA	Ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (RS 172.010.1)
ONG	Organisation non-gouvernementale
OP	Opérations de renseignement
OPAB	Enquêtes opérationnelles
ORens	Ordonnance du 16 août 2017 sur le service de renseignement (RS 121.1)
OSINF	Open Source Information
OSINT	Open Source Intelligence, recherche d'informations à partir de sources librement accessibles
OSIS-SRC	Ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du SRC (RS 121.2)
PCLOB	Privacy and Civil Liberties Oversight Board
PFPDT	Préposé fédéral à la protection des données et à la transparence
RH	Ressources humaines

RIPOL	Recherches informatisées de police
RM	Renseignement militaire
ROSO	Renseignement de sources ouvertes
RS	Recueil systématique
SCM	Service continuity management
SCPT	Surveillance de la correspondance par poste et télécommunication
Service SCPT	Service de surveillance de la correspondance par poste et télécommunication
SPPA	Service pour la protection préventive de l'armée
SRC	Service de renseignement de la Confédération
SRCant	Services de renseignement cantonaux
ss	et suivant(e)s
TAF	Tribunal administratif fédéral
TIC	Technologies de l'information et de la communication
UA	Unités administratives
VTI	Identités d'emprunt virtuelles