



23.004

## **Rapport annuel 2022 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales**

du 23 janvier 2023

---

Monsieur le Président,  
Madame la Présidente,  
Mesdames, Messieurs,

Conformément à l'art. 55 de la loi du 13 décembre 2002 sur l'Assemblée fédérale (Loi sur le Parlement, LParl ; RS 171.10), nous vous soumettons le rapport d'activité des Commissions de gestion et de leur délégation pour l'année 2022 et vous demandons de bien vouloir en prendre connaissance.

Le présent rapport donne des indications sur les principaux contrôles effectués durant l'année et dégage les résultats et les enseignements qui peuvent en être tirés.

Nous vous prions d'agréer, Monsieur le Président, Madame la Présidente, Mesdames et Messieurs, l'assurance de notre très haute considération.

23 janvier 2023

Au nom des Commissions de gestion  
des Chambres fédérales :

La présidente de la CdG-N,  
Prisca Birrer-Heimo

Le président de la CdG-E,  
Matthias Michel

---

## Table des matières

<b>1</b>	<b>Introduction</b>	<b>5</b>
<b>2</b>	<b>Mandat et organisation</b>	<b>7</b>
2.1	Mission et compétences des CdG	7
2.1.1	Missions des CdG dans le cadre de la haute surveillance	7
2.1.2	Droits à l'information et confidentialité des travaux	8
2.1.3	Collaboration des CdG et de la DélCdG avec leur secrétariat	10
2.1.4	Collaboration des CdG avec les Commissions des finances, la Délégation des finances et le Contrôle fédérale de finances	10
2.2	Organisation et composition des CdG	11
<b>3</b>	<b>Travaux des CdG en 2022</b>	<b>16</b>
3.1	Publications des CdG en 2022	16
3.2	Domaine DFAE/DDPS	18
3.2.1	Contrôle de suivi de l'inspection relative aux circonstances de la nomination de Roland Nef au poste de chef de l'armée	18
3.3	Domaine DFF/DEFR	19
3.3.1	Réglementation du négoce boursier de cryptomonnaies	19
3.3.2	Nomination des cadres supérieurs par le Conseil fédéral	22
3.3.3	Problèmes relatifs au transit de réfugiés par la Suisse	23
3.3.4	Interventions du SECO dans le cadre de la protection consulaire	24
3.4	Domaine DFI/DETEC	26
3.4.1	Pénurie de conductrices et conducteurs de locomotives aux CFF	26
3.4.2	Activités du Service suisse d'enquête de sécurité	28
3.4.3	Perturbation technique chez Skyguide SA	30
3.4.4	Risques liés à l'approvisionnement en électricité de la Suisse : activité passées des autorités fédérales	32
3.4.5	Laboratoire biologique de haute sécurité : assainissement du laboratoire de Mittelhäusern	34
3.4.6	Dossier électronique du patient	36
3.5	Domaine DFJP/ChF	38
3.5.1	Trafic de migrants	38
3.5.2	Situation en Ukraine – mesures du SEM	39
3.5.3	Violence dans les centres fédéraux pour requérantes et requérants d'asile	40

---

3.6	Domaine Tribunaux/MPC	42
3.6.1	Coordination avec la Commission judiciaire	42
3.6.2	Violation du secret de fonction : ordonnance de classement du procureur fédéral extraordinaire	43
3.6.3	Introduction du dossier judiciaire électronique (projet Justitia 4.0)	44
3.7	État des lieux des inspections ouvertes des CdG et de la DélCdG	45
3.8	Autres sujets traités par les CdG	48
3.9	Visites de service	52
3.10	Requêtes	53
<b>4</b>	<b>Inspection relative à la gestion de la pandémie de COVID-19</b>	<b>55</b>
4.1	Domaine DFF/DEFR	58
4.1.1	Crédits COVID-19	58
4.2	Domaine DFI/DETEC	61
4.2.1	Bases d'information internationales et échanges internationaux du DFI et de l'OFSP	61
4.2.2	Bases d'information scientifiques du DFI et de l'OFSP	63
4.2.3	Collaboration entre Confédération et cantons pour la gestion de pandémie	64
4.2.4	Gestion des données sanitaires : travaux du DFI et de l'OFSP pour la numérisation du système de santé	65
4.2.5	Gestion des données sanitaires : réforme du Service sanitaire cordonné	67
4.2.6	Surveillance de l'OFSP sur la fondation « mesvaccins »	68
4.2.7	Gestion des biens médicaux : redistribution, revente et destruction de vaccins non utilisés	71
4.3	Domaine DFJP/ChF	74
4.3.1	Évaluation de la gestion de crise par la Chancellerie fédérale	74
<b>5</b>	<b>Protection de l'État et services de renseignement</b>	<b>76</b>
5.1	Missions, droits et organisation de la DélCdG	76
5.2	Suivi de l'inspection relative à l'affaire Crypto AG	77
5.2.1	Contexte	77
5.2.2	Recommandation 4	78
5.2.3	Recommandation 8	79
5.2.4	Recommandation 9	81
5.2.5	Recommandation 11	82
5.3	Contacts avec l'étranger	83
5.4	Recherche d'informations soumise à autorisation, exploration du réseau câblé et exploration radio	84
5.5	Obligation de fournir et de communiquer des renseignements	85
5.6	Systèmes d'information et protection des données	87

---

5.7	Indemnisation des cantons pour l'exécution de la LRens	88
5.8	Évènements survenus au sein du domaine Cyber du SRC	90
5.8.1	Haute surveillance concomitante de la DélCdG	90
5.8.2	Constatations relatives aux activités du domaine Cyber du SRC	91
5.8.3	Processus de surveillance au niveau du SRC et du DDPS	92
5.8.4	Activité de surveillance de l'AS-Rens	93
5.8.5	Appréciation de la DélCdG	94
5.9	Contrat de prestations entre le SRC et un particulier	97
5.9.1	Haute surveillance concomitante de la DélCdG	97
5.9.2	Appréciation de la DélCdG	99
5.10	Conduite de la politique de sécurité par le Conseil fédéral	100
5.10.1	Haute surveillance exercée sur la conduite de la politique de sécurité	100
5.10.2	Tâches et fonctionnement de la Délséc et du GS	101
5.10.3	Mission d'évacuation à Kaboul en août 2021 – Appréciation de la DélCdG	102
5.10.4	Attaque russe contre l'Ukraine en février 2022	103
5.10.5	Entretien de la DélCdG avec la Délséc de mai 2022	105
5.10.6	Suite des travaux du GCUR et de la Délséc	106
5.10.6.1	Scénarios d'évolution de la situation	106
5.10.6.2	Demandes d'autres pays concernant du matériel de guerre suisse	107
5.10.6.3	Préparation à un événement nucléaire	107
5.10.7	Entretien de la DélCdG avec le DDPS d'octobre 2022	108
<b>6</b>	<b>Rapports de gestion et rapports récurrents</b>	<b>110</b>
6.1	Rapport de gestion 2021 du Conseil fédéral	110
6.2	Rapport de gestion 2021 du Tribunal fédéral	111
6.3	Autres rapports traités par les CdG	112

---

## **5.8 Événements survenus au sein du domaine Cyber du SRC**

### **5.8.1 Haute surveillance concomitante de la DélCdG**

Dans son rapport annuel 2021, la DélCdG avait consacré un sous-chapitre à des faits problématiques constatés au SRC quelque temps auparavant<sup>159</sup>. Pour des raisons liées au maintien du secret, elle avait jugé préférable de ne pas encore révéler, à ce moment-là, que les événements concernés étaient survenus dans le domaine Cyber du SRC, lequel était alors rattaché à la division Gestion de l'information (NDBI). Après que le DDPS en a informé le Conseil fédéral, celui-ci a publié un communiqué de presse à ce sujet, le 26 janvier 2022<sup>160</sup>.

La DélCdG a découvert les activités problématiques du domaine Cyber à la fin août 2021. Le 28 octobre 2021, elle a demandé des informations à la cheffe du DDPS concernant les investigations en cours que le SRC avait ordonnées en interne et l'avis de droit qu'il avait demandé à un cabinet d'avocats. La délégation a pris connaissance de ce dernier et du rapport final de l'enquête interne le 21 décembre 2021.

Considérant que ces documents permettaient de clarifier en grande partie la situation juridique et les faits concernés, elle a prié la cheffe du DDPS de l'informer, au plus tard à la mi-janvier 2022, des mesures concrètes que son département comptait prendre sur cette base et d'examiner rapidement l'opportunité de déposer une plainte pénale.

Dans sa réponse du 20 janvier 2022, la cheffe du DDPS a indiqué que le SRC avait décidé, à titre de mesure immédiate, de transférer le domaine Cyber, jusqu'ici rattaché à la division NDBI, dans l'unité de direction Analyse du SRC (NDBA). La cheffe du DDPS avait par ailleurs décidé d'ordonner l'ouverture d'une enquête administrative. À cet égard, elle a prié la DélCdG de lui faire savoir, au plus tard à la fin janvier 2022, si elle avait elle-même l'intention de mener une enquête formelle à ce sujet au sens de l'art. 154a LParl.

À sa séance du 26 janvier 2022, la DélCdG n'a pas jugé nécessaire, à ce moment-là, de transformer ses investigations en cours en une inspection formelle. Partant, la question de savoir si elle autorisait le DDPS à lancer une enquête administrative ne se posait pas. Parallèlement, la délégation a indiqué, dans son communiqué de presse du 27 janvier 2022, qu'elle continuerait de suivre de près la façon dont le DDPS

<sup>159</sup> Rapport annuel 2021 des CdG et de la DélCdG du 25.1.2022, ch. 5.14 (FF 2022 513 134)

<sup>160</sup> Enquête administrative dans le domaine Cyber du SRC, communiqué de presse du Conseil fédéral du 26.1.2022

---

organiserait les tâches de lutte contre les cyberrisques à l'avenir et la manière dont il tiendrait compte des aspects pénaux des événements survenus<sup>161</sup>.

Afin d'approfondir ses connaissances en matière de cyberdéfense et de se faire une idée du fonctionnement de la surveillance au sein du SRC et du DDPS ainsi que de la surveillance exercée par l'AS-Rens, la DélCdG a mené, au cours du premier semestre, onze auditions, qui lui ont permis d'entendre treize personnes au total, et compilé des documents pertinents établis principalement dans le cadre de l'enquête interne du SRC.

Au mois de mai 2022, la délégation a été informée des grandes lignes de l'enquête administrative menée par l'ancien juge fédéral Niklaus Oberholzer, ensuite de quoi elle a entendu ce dernier au sujet de son travail, à sa séance du mois d'août. Le rapport d'enquête du 15 août lui est parvenu à la fin septembre. En novembre, pour clore ses investigations, elle a auditionné le DDPS concernant les résultats de l'enquête administrative et s'est enquis auprès de l'AS-Rens de l'état de son inspection en cours.

### **5.8.2 Constatations relatives aux activités du domaine Cyber du SRC**

Les constatations de la DélCdG concernant les activités menées par le domaine Cyber par le passé s'appuient largement sur les travaux et le rapport final de l'enquête interne ainsi que sur les auditions auxquelles elle a procédé. Selon le rapport, le domaine Cyber s'est procuré, dès 2015, des données de serveurs auprès de plusieurs fournisseurs privés. À cet effet, les données enregistrées étaient copiées à partir des serveurs concernés (images de serveur) ou le trafic de données de ceux-ci (contenu et données secondaires) était surveillé et capté. Cela s'est fait avec l'accord ou la participation des fournisseurs concernés, mais à l'insu des personnes qui avaient loué ces serveurs<sup>162</sup>. Le domaine Cyber n'a suspendu ses activités opérationnelles que lorsque le directeur du SRC de l'époque a lancé l'enquête interne, à la fin avril 2021.

Faute de documentation à ce sujet, il n'était pas possible de faire toute la lumière sur les activités du domaine. Dans le cadre de l'enquête interne, il a toutefois été considéré que plus de 50 images de serveur et une centaine de mesures prises pour surveiller le trafic de données avaient valeur de documentation. Les données obtenues servaient à identifier les cyberattaques en cours. Les principales informations concernant ces attaques étaient tirées des communications des serveurs ainsi que des

<sup>161</sup> Événements survenus au sein du domaine Cyber du SRC, communiqué de presse de la DélCdG du 27.1.2022

<sup>162</sup> Une partie de ces serveurs avaient été loués exprès par des cyberattaquants pour attaquer en particulier des objectifs hors de Suisse. L'autre partie des serveurs avaient été piratés par des agresseurs et utilisés pour des attaques sans l'accord des personnes qui les avaient loués.

---

images de serveur<sup>163</sup>. Par ailleurs, les communications électroniques sécurisées dans le cadre de l'enquête interne permettent de conclure que les informations obtenues de cette façon étaient également partagées avec des entreprises de sécurité privées.

D'après les constatations de la DélCdG, le fait que le domaine Cyber était rattaché à la division NDBI lui avait permis de procéder à des recherches d'informations en dehors des procédures de renseignement prescrites. De ce fait, ni l'élaboration d'une documentation interne ni l'établissement de rapports à l'intention de la direction du SRC et des organes de surveillance n'étaient garantis.

### **5.8.3 Processus de surveillance au niveau du SRC et du DDPS**

Une reconstitution des événements montre que, à partir du mois de septembre 2020 au plus tard, la majorité des membres de la direction du SRC étaient conscients de ce qu'impliquait le fait de chercher des informations auprès de fournisseurs privés. À ce moment-là, le chef de la division NDBB, qui était également le vice-directeur du SRC, avait décidé que le chef du domaine Cyber devait établir une note à l'attention de son supérieur hiérarchique (le chef de la division NDBI) au sujet de sa collaboration avec les fournisseurs. Avant la mi-décembre 2020, une telle note, qui n'était toutefois pas datée, est parvenu au directeur du SRC.

Ce document, qui n'était probablement qu'à l'état de projet, n'a toutefois pas été discuté au sein de la direction du SRC. En automne 2021, il a été retrouvé parmi les documents que l'ancien directeur du SRC avait laissés derrière lui et qui avaient été mis à la disposition de l'enquête interne. Quant à savoir si ce document avait été transmis au directeur du SRC par la voie hiérarchique, la DélCdG a tiré des renseignements divergents des documents consultés et de ses auditions.

Début 2021, le chef du domaine Cyber a quitté le SRC, à un moment où le fonctionnement du domaine était de plus en plus remis en question au sein du service. Par conséquent, le directeur du SRC a jugé nécessaire, fin avril 2021, de charger le chef de la sécurité du SRC de procéder à une enquête interne portant sur la recherche et le traitement des informations par le domaine Cyber et sur les relations que ce dernier entretenait avec des fournisseurs et des entreprises de sécurité privées. Le mandat ne portait pas sur une analyse complète des bases légales relatives à ces activités.

Lors de la séance de direction d'office du 17 mai 2021, le directeur du SRC a informé la cheffe du DDPS de l'enquête qui avait été lancée sur les événements survenus au domaine Cyber du SRC<sup>164</sup>. Contacté, le MPC aurait indiqué que les règles légales étaient respectées dans le domaine Cyber du SRC. Comme il l'a expliqué à la DélCdG en octobre 2021, le MPC n'était pas au courant de la surveillance en temps

<sup>163</sup> Ces méthodes sont connues dans le domaine de la cybersécurité et décrites dans la littérature spécialisée, notamment dans *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*, Timo Steffens, Springer, ISBN: 978-3-662-61312-2

<sup>164</sup> À cette séance, il a été décidé que la DélCdG serait informée de l'enquête interne à la discussion du 27.5.2021, mais cela n'a pas été fait.

---

réel pratiquée par le SRC auprès des fournisseurs et il ne s'est jamais prononcé sur la légalité de cette pratique.

En mai 2021, des appareils et des données du domaine Cyber du SRC ont été mis en sûreté et des entretiens ont été menés avec une douzaine de membres du SRC. Dans son premier rapport intermédiaire de juin 2021, le chef de la sécurité a proposé au directeur du SRC de confier l'appréciation juridique à un cabinet d'avocats, ce qui a été approuvé. La cheffe du DDPS n'a appris l'existence d'un tel mandat qu'après que celui-ci a été attribué.

Les premières informations que la DélCdG a reçues le 25 août 2021 ont immédiatement incité cette dernière à demander au SRC de lui fournir une chronologie des événements. Ce n'est que ce jour-là que la cheffe du DDPS a reçu du SRC des informations concrètes sur les méthodes de recherches du domaine Cyber.

Lors de l'entretien du 28 octobre 2021, la cheffe du DDPS a informé la DélCdG des travaux qui avaient été menés jusqu'alors par le SRC. Elle n'a souhaité livrer une appréciation des événements survenus au sein du domaine Cyber qu'après avoir pris connaissance du rapport d'enquête interne.

Le rapport d'enquête interne de décembre 2021 contenait neuf recommandations adressées à la direction du SRC. Il s'agissait notamment d'examiner l'éventualité de procéder à des changements d'ordre organisationnel concernant la subordination du domaine Cyber, mais surtout de diligenter une enquête administrative externe afin de clarifier la pertinence des événements survenus au domaine Cyber sur le plan pénal. Mi-janvier 2022, la cheffe du DDPS a décidé d'ouvrir une enquête administrative afin de faire la lumière sur les processus de conduite et les décisions des personnes responsables ainsi que d'élucider des questions de détail soulevées par l'enquête interne.

Le 7 novembre 2022, le secrétaire général du DDPS et le directeur du SRC ont informé la DélCdG des conclusions que le DDPS a tirées du rapport de l'enquête administrative, la conclusion principale étant que le domaine Cyber du SRC a exercé ses activités sans base légale mais que, selon l'expert, il n'y avait pas lieu de déposer une plainte pénale. En outre, le département souhaitait prendre en considération des propositions visant à simplifier le dispositif légal relatif à la recherche de données secondaires dans le cadre de la révision de la LRens. En ce qui concerne l'organisation des tâches du SRC dans le cyberspace, le directeur du SRC a souligné que l'examen en cours des structures de la Confédération relatives au cyberspace pourrait encore avoir une influence sur cette question (cf. ch. 5.10.3).

#### **5.8.4                   Activité de surveillance de l'AS-Rens**

Dans son plan des inspections pour l'année 2021, l'AS-Rens avait prévu, au chiffre 21-2, un contrôle de la protection des infrastructures critiques et de la cyberdéfense. Après s'être penchée une première fois sur la question à la mi-mai, l'AS-Rens a mené des entretiens formels avec des cadres jusqu'à fin juin 2021. Certaines de ces personnes avaient déjà été interrogées dans le cadre de l'enquête interne.

---

Début juin 2021, l'AS-Rens a reçu une lettre anonyme l'enjoignant de mener une enquête approfondie sur les incidents graves survenus au SRC, son auteur menaçant de s'adresser aux médias si elle ne le faisait pas. Le chef de l'AS-Rens a informé la cheffe du DDPS de cette menace anonyme par écrit puis il l'a rencontrée début août, mais il n'a pas été informé de l'ampleur des problèmes concernant le domaine Cyber.

Dans son rapport d'inspection du 23 septembre 2021, l'AS-Rens fait état du risque que, en consultant les données secondaires des serveurs, le SRC n'agisse dans une zone grise au niveau juridique<sup>165</sup>. C'est pourquoi le SRC devait vérifier dans quelles circonstances l'obtention par le SRC de métadonnées auprès d'un fournisseur était licite.<sup>166</sup> La question de la création d'images de serveurs, également problématique d'un point de vue juridique, n'a pas été abordée par l'AS-Rens.

En janvier 2022, le chef de l'AS-Rens a confirmé à la DélCdG que l'AS-Rens avait renoncé à procéder à ses propres clarifications juridiques, car le SRC avait déjà ordonné une expertise externe à ce sujet. En outre, il s'est appuyé sur le fait que l'ancien directeur du SRC aurait déjà clarifié les faits avec le MPC en mai 2021 et que ce dernier n'aurait pas constaté d'infraction pénale (cf. ch. 5.8.3).

En octobre 2021, se fondant sur les documents établis par le SRC à l'intention de DélCdG à l'issue de la séance du 25 août 2021, l'AS-Rens a lancé de nouvelles investigations approfondies auprès du domaine Cyber. Les questions de l'AS-Rens concernaient des thèmes importants sur lesquels la DélCdG se penchait dans le cadre de sa haute surveillance, ou des questions explicites auxquelles l'enquête interne devait répondre d'ici la fin de l'année.

Comme la DélCdG l'a appris ultérieurement, l'AS-Rens a ouvert un nouvel examen spécifique au sujet du domaine Cyber et a interrogé, en janvier 2022, deux membres du SRC. La DélCdG a été informée des travaux en cours le 22 novembre 2022 par la nouvelle cheffe de l'AS-Rens. Après avoir reçu le rapport de l'ancien juge fédéral Oberholzer, l'AS-Rens a décidé d'approfondir certaines questions par d'autres analyses.

## **5.8.5 Appréciation de la DélCdG**

Pour la DélCdG, qui se fonde sur l'avis de droit externe et l'enquête administrative, il est clair que la recherche d'informations effectuée par le domaine Cyber du SRC auprès des fournisseurs était contraire aux prescriptions légales, donc illégales. En outre, en sa qualité d'organe de haute surveillance, la DélCdG souhaitait évaluer le fonctionnement de la surveillance au sein du DDPS à tous les niveaux. S'agissant du SRC, il s'agissait donc de déterminer si le chef de la division NDBI et la direction du service étaient informés du fait que le domaine Cyber collectait des informations

<sup>165</sup> Protection des infrastructures critiques / Cyberdéfense : rapport d'inspection 21-2 de l'AS-Rens du 23.9.2021, p. 12

<sup>166</sup> La recommandation avait été abandonnée après que le SRC avait indiqué dans sa prise de position qu'un cabinet d'avocats procédait à des clarifications.

---

auprès de fournisseurs privés. Eu égard aux renseignements contradictoires reçus par la DélCdG, il apparaît difficile d'effectuer une appréciation définitive de la période précédant 2020.

Il est par contre possible d'évaluer la façon dont la surveillance a été assurée au niveau de la division NDBI à partir du moment où le vice-directeur du SRC et chef a.i. de la division NDBB a chargé le chef du domaine Cyber du SRC, en septembre 2020, de rédiger une note à l'intention du chef de division sur les activités de recherche de son domaine (voir ch. 5.1.3). Il apparaît que le chef de la division NDBI n'a pas suffisamment surveillé cette tâche, qui était pourtant d'une importance certaine, au cours des mois suivants.

Étant donné qu'une surveillance hiérarchique efficace faisait défaut, la direction du SRC était dans l'incapacité de réagir adéquatement, à son niveau, aux méthodes de travail problématiques du domaine Cyber, si bien que l'ancien directeur du SRC n'avait finalement plus d'autre choix, en avril 2021, que de recourir à l'instrument de l'enquête interne. Une conséquence de cette dernière était l'interruption de l'importante mission accomplie par le domaine Cyber du SRC (séparation du réseau, interdiction de prendre contact avec les fournisseurs concernés). L'enquête ayant été menée en interne, on peut en outre se demander si les personnes concernées étaient impartiales et si elles ont pu procéder à leurs investigations de façon indépendante et sans restriction. Par ailleurs, peu de temps après le lancement de l'enquête, les ressources qui y avaient été affectées ont été réduites.

En dépit de ces difficultés, il a été possible d'étendre le champ de l'enquête interne lorsque cela s'est avéré nécessaire au cours des investigations. Par exemple, un avis de droit externe a été commandé afin d'évaluer la légalité de la recherche d'informations effectuée par le domaine Cyber du SRC. Le SRC étant tenu de garantir la légalité de son activité en prenant des mesures de contrôle appropriées (voir art. 75 LRens), l'ancien directeur aurait toutefois dû ordonner immédiatement la clarification des questions juridiques.

La DélCdG a pu constater, lors de son entretien d'octobre 2021 avec la cheffe du DDPS, que cette dernière n'avait pas été associée à la définition des objectifs et du calendrier de l'enquête interne. La cheffe du DDPS ne s'est pas non plus penchée sur les résultats intermédiaires de l'enquête, préférant attendre le rapport final pour se forger une opinion sur la problématique. En janvier 2022, elle a ordonné une enquête administrative, qui est venue s'ajouter à l'enquête interne du SRC et qui a été menée parallèlement à d'autres investigations de l'AS-Rens : en conséquence, il a finalement fallu deux ans au DDPS pour mener à leur terme les travaux de surveillance relatifs aux événements survenus au sein du domaine Cyber du SRC.

Par conséquent, la DélCdG se demande si la cheffe du DDPS n'aurait pas pu opter pour une stratégie de surveillance plus efficace en lançant une enquête administrative en été 2021. Si les enquêtes avaient été menées à terme plus rapidement, il aurait peut-être été possible de réduire les inquiétudes au sein du personnel et de garantir la capacité opérationnelle de ce domaine important.

S'agissant de l'activité de surveillance de l'AS-Rens, la DélCdG peut comprendre que cette dernière, eu égard à la décision du SRC de commander un avis de droit externe, n'ait émis aucune recommandation en la matière, n'ait pas effectué

---

d'appréciation juridique définitive et ait rapidement achevé son rapport d'inspection. Toutefois, elle ne comprend pas que l'AS-Rens ait ensuite repris ses investigations, notamment après que la haute surveillance est intervenue en confiant des mandats clairs au SRC.

Il aurait été judicieux que le DDPS coordonne les activités de l'enquête administrative externe et celles de l'AS-Rens. Toutefois, étant donné que l'autorité de surveillance n'a intensifié ses investigations qu'une fois conclue l'enquête administrative, il est désormais possible d'approfondir des questions auxquelles l'enquête administrative n'avait pas répondu.

Si elle déplore les longs processus de surveillance du DDPS, la DélCdG se félicite du développement positif des activités de recherche dans le domaine Cyber, auxquelles la division NDBB est désormais formellement associée. En octobre 2021, le directeur suppléant du SRC, qui dirigeait alors le service, avait déjà émis une directive interne selon laquelle il fallait, avant toute recherche d'informations auprès de fournisseurs, vérifier dans quelle mesure il y avait lieu de tenir compte des dispositions de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)<sup>167</sup> et de la LRens relatives aux mesures de recherche soumises à autorisation.

Pour soutenir ce processus, la DélCdG a déjà prié le SRC, en février 2022, de faire parvenir le plus rapidement possible au TAF l'avis du cabinet d'avocats. Pendant l'année sous revue, la DélCdG a observé les premières expériences faites par le SRC avec les instruments de recherche prévus par la loi, toujours sous réserve d'une approbation du tribunal. Sur la base de ces constatations, la DélCdG décidera de la suite de la procédure, notamment en ce qui concerne l'éventuelle nécessité de modifier la LRens. Sur la base de ses clarifications, la DélCdG part du principe que le succès de la cyberdéfense ne pourra pas être assuré seulement par la recherche de données secondaires.

<sup>167</sup> Loi fédérale du 18.3.2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT ; SR 780.1)

---

## Abréviations

ADN	Acide désoxyribonucléique
ADS 15	Système de drones de reconnaissance
AFC	Administration fédérale des contributions
AFD	Administration fédérale des douanes
AFF	Administration fédérale des finances
AFS	Archives fédérales suisses
AI	Assurance-invalidité
Al.	Alinéa
APG	Allocations pour perte de gain
API	Advance Passenger Information
Art.	Article
AS-MPC	Autorité de surveillance du Ministère public de la Confédération
AS-Rens	Autorité de surveillance indépendante des activités de renseignement
BiG	Bibliothèque am Guisanplatz
BLA	Base logistique de l'armée
BNS	Banque nationale suisse
BO	Bulletin officiel de l'Assemblée fédérale
CAJ-E	Commission des affaires juridiques du Conseil des Etats
CASO	<i>Civil aviation safety office</i>
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des Commandants des Polices Cantonales de Suisse
CdA	Chef de l'armée
CdC	Conférence des gouvernements cantonaux
CDF	Contrôle fédéral des finances
CdF	Commissions des finances des Chambres fédérales
CdG	Commissions de gestion des Chambres fédérales
CdG-E	Commission de gestion du Conseil des États
CdG-N	Commission de gestion du Conseil national
Cdmt Op	Commandement des Opérations
CDS	Conférence des directrices et directeurs cantonaux de la santé
CEATE	Commissions de l'environnement, de l'aménagement du territoire et de l'énergie des Chambres fédérales
CEDH	Cour européenne des droits de l'homme
CENAL	Centrale nationale d'alarme
CEO	<i>Chief Executive Officer</i> , directeur
CEP	Commission d'enquête parlementaire

---

CEPI	<i>Coalition for Epidemic Preparedness Innovations</i> , Coalition pour les innovations en matière de préparation aux épidémies
Cf.	confer
CFF	Chemins de fer fédéraux
CG MPS	Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
CH	<i>Confoederatio helvetica</i> , Confédération suisse
Ch.	Chiffre
Chap.	Chapitre
ChF	Chancellerie fédérale
CJ	Commission judiciaire
CLM	<i>Conversation Leader Migration</i> ; meneurs d'entretien migration
CO	Loi fédérale du 30 mars 1911 complétant le code civil suisse (Livre cinquième: Droit des obligations; RS 220)
COE	Centre des opérations électroniques
COVID-19	coronavirus disease 2019 (maladie à coronavirus 2019)
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
CPA	Contrôle parlementaire de l'administration
CPO	Centre des publications officielles
CSP	Contrôle(s) de sécurité relatif(s) aux personnes
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS 101)
DDC	Direction du développement et de la coopération
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DéICdG	Délégation des Commissions de gestion des Chambres fédérales
DéFin	Délégation des finances des Chambres fédérales
Délséc	Délégation du Conseil fédéral pour la sécurité
DEP	Dossier électronique du patient
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DMF	Département militaire fédéral
ECDC	European Centre for Disease Prevention and Control (Centre européen de contrôle et de prévention des maladies)
ECS	Exercice de conduite stratégique

---

ECSC	État-major de conduite stratégique de la Confédération
e-ID	Identité électronique
EiCom	Commission fédérale de l'électricité
EMFP	Etat-major fédéral Protection de la population
ENCASIA	<i>European Network of Civil Aviation Safety Investigation Authorities</i>
EPF	Ecoles polytechniques fédérales
EPFL	Ecole polytechnique fédérale de Lausanne
ERNS	Exercices du Réseau national de sécurité
ESYSP	Plateforme de saisie des données biométriques
ETP	<i>exchange traded products</i> ; produit négocié en bourse
ETP	Equivalent temps plein
EWRS	<i>Early Warning and Response System</i> , Système d'alerte précoce et de réaction
FATCA	<i>Foreign Account Tax Compliance Act</i>
fedpol	Office fédéral de la police
FF	Feuille fédérale
FIFA	Fédération internationale de Football Association
FINMA	Autorité fédérale de surveillance des marchés financiers
Fintech	<i>financial technology; Technologie financière</i>
FSG	Fédération suisse de gymnastique
GAFI	Groupe d'action financière
GAVI	<i>Global Alliance for Vaccines and Immunization</i>
GCUR	Groupe de coordination interdépartemental Ukraine / Russie
GEVER	Gestion électronique des affaires
GS	Groupe Sécurité
HCR/UNHCR	Haut-Commissariat des Nations unies pour les réfugiés
HSC	<i>Health Security Committee</i> , comité de sécurité sanitaire
IASA	Système d'analyse intégrale
IASA-EXTR	Système d'analyse intégrale de l'extrémisme violent
ICO	<i>initial coin offering</i>
IFSN	Inspection fédérale de la sécurité nucléaire
Innosuisse	Agence suisse pour l'encouragement de l'innovation
IPI	Institut fédéral de la protection intellectuelle
IVI	Institut de virologie et d'immunologie
LAAM	Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (Loi sur l'armée ; RS 510.10)
LB	Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargne (Loi sur les banques; RS 952.0)

---

LBA	Loi fédérale du 10 octobre 1997 concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (Loi sur le blanchiment d'argent; RS 955.0)
LBN	Loi fédérale du 3 octobre 2003 sur la Banque nationale suisse (Loi sur la Banque nationale ; RS 951.11)
LCF	Loi fédérale du 28 juin 1967 sur le Contrôle fédéral des finances (Loi sur le Contrôle des finances ; RS 614.0)
LDEP	Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (RS 816.1)
LEI	Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (RS 142.20)
LEne	Loi du 30 septembre 2016 sur l'énergie (RS 730.0)
LEp	Loi fédérale du 28 septembre 2012 sur la lutte contre les maladies transmissibles de l'homme (Loi sur les épidémies; RS 818.101)
LFMG	Loi fédérale du 13 décembre 1996 sur le matériel de guerre ( ;RS 514.51)
LIMF	Loi fédérale du 19 juin 2015 sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés (Loi sur l'infrastructure des marchés financiers; RS 958.1)
LLGV	Loi fédérale du 18 mars 2005 sur le raccordement de la Suisse orientale et occidentale au réseau européen des trains à haute performance (RS 742.140.3)
LOAP	Loi fédérale du 19 mars 2010 sur l'organisation des autorités pénales de la Confédération (RS 173.71)
LOGA	Loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration ( ;RS 172.010)
LParl	Loi fédérale du 13 décembre 2002 sur l'Assemblée fédérale (Loi sur le Parlement ; RS 171.10)
LPers	Loi sur le personnel de la Confédération du 24 mars 2000 ( ;RS 172.220.1)
LRCF	Loi fédérale du 14 mars 1958 sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires (Loi sur la responsabilité ; RS 170.32)
LREC	Loi fédérale du 23 mars 1962 sur la procédure de l'Assemblée fédérale, ainsi que sur la forme, la publication et l'entrée en vigueur des actes législatifs (Loi sur les rapports entre les conseils ; abrogée le 3 décembre 2007)
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 (SR 780.1)
LSEtr	Loi du 26 septembre 2014 sur les Suisses de l'étranger (RS 195.1)

---

LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, RS 128)
LTF	Loi fédérale du 17 juin 2005 sur le Tribunal fédéral ( ;RS 173.110)
LTrAlp	Loi fédérale du 4 octobre 1991 relative à la construction de la ligne ferroviaire suisse à travers les Alpes (RS 742.104)
METAS	Institut fédéral de métrologie
MPC	Ministère public de la Confédération
NAC	Nouvel avion de combat
NDBB	Division Recherche du SRC
NDBI	Division Gestion de l'information du SRC
NLR	<i>Royal Netherlands Aerospace Centre</i>
OCaS-COVID-19	Ordonnance du 25 mars 2020 sur l'octroi de crédits et de cautionnements solidaires à la suite du coronavirus (Ordonnance sur les cautionnements solidaires liés au COVID-19 ; RS 951.261)
OCI	Organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé
OCSP	Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (RS 120.4)
OEIT	Ordonnance du 17 décembre 2014 sur les enquêtes de sécurité en cas d'incident dans le domaine des transports (RS 742.161)
OEp	Ordonnance du 29 avril 2015 sur la lutte contre les maladies transmissibles de l'homme (Ordonnance sur les épidémies ; RS 818.101.1)
OFAC	Office fédéral de l'aviation civile
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFCL	Office fédéral des constructions et de la logistique
OFDF	Office fédéral de la douane et de la sécurité des frontières
OFEN	Office fédéral de l'énergie
OFJ	Office fédéral de la justice
OFL	Office fédéral du logement
OFPER	Office fédéral du personnel
OFPP	Office fédéral de la protection de la population
OFROU	Office fédéral des routes
OFSP	Office fédéral de la santé publique
OMC	Organisation mondiale du commerce
OMS	Organisation mondiale de la santé
ONU	Organisation des Nations Unies
Ordiséc	Organe de direction pour la sécurité

---

Ordonnance GEVER	Ordonnance du 3 avril 2019 sur la gestion électronique des affaires dans l'administration fédérale (RS 172.010.441)
ORens	Ordonnance du 16 août 2017 sur le Service de renseignement (RS 121.1)
OSAV	Office fédéral de la sécurité alimentaire et des affaires vétérinaires
OSEtr	Ordonnance du 7 octobre.2015 sur les personnes et les institutions suisses à l'étranger (Ordonnance sur les Suisses de l'étranger ; RS 195.1)
OSIS-SRC	Ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (RS 121.2)
OTAN	Organisation du traité de l'Atlantique nord
OTC	Obstacles techniques au commerce
OUC	Ordonnance du 9 mai 2012 sur l'utilisation des organismes en milieu confiné (Ordonnance sur l'utilisation confinée ; RS 814.912)
PFPDT	Préposé fédéral à la protection des données et à la transparence
PME	Petites et moyennes entreprises
Po.	Postulat
RCE	Règlement du 20 juin 2003 du Conseil des États (RS 171.14)
RCN	Règlement du 3 octobre 2003 du Conseil national (RS 171.13)
RDS	Réseau de données sécurisé
RM	Renseignement militaire
RNS	Réseau national de sécurité
RO	Recueil officiel du droit fédéral
RS	Recueil systématique du droit fédéral suisse
RSP	Règlement des Services du Parlement du 16 mai 2014
RUAG	Entreprise d'armement ( <i>Rüstungsunternehmen-Aktiengesellschaft</i> )
SA	Société anonyme
SAPR	Système d'alerte précoce et de réaction (en anglais : <i>Early Warning Response System, EWRS</i> )
SECO	Secrétariat d'État à l'économie
SEM	Secrétariat d'État aux migrations
SERV	Assurance suisse contre les risques à l'exportation
SESE	Service suisse d'enquête de sécurité
SFI	Secrétariat d'État aux questions financières internationales
SG-DDPS	Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports
SG-DFJP	Secrétariat général du Département fédéral de justice et police
SII	Système d'information et d'intervention
SNV	Stratégie nationale de vaccination
SONAS	État-major spécial Asile

---

SPPA	Service pour la protection préventive de l'armée
SRC	Service de renseignement de la Confédération
SRCant	Service de renseignement cantonal
SRM	Service de renseignement militaire
SSC	Service sanitaire coordonné
Swissmedic	Institut suisse des produits thérapeutiques
swisstopo	Office fédéral de topographie
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TFB	Tribunal fédéral des brevets
TMC	Tribunal militaire de cassation
TNI	Transformation numérique et informatique
TPF	Tribunal pénal fédéral
TRAVINT	Travel Intelligence
TRD	Technologie des registres distribués
UE	Union Européenne