Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2020
www.droitfederal.admin.ch
La version électronique
signée fait foi

Gestion de la cyberattaque menée contre RUAG: évaluation de l'avis rendu par le Conseil fédéral le 28 septembre 2018

Rapport de la Commission de gestion du Conseil national du 19 novembre 2019

Avis du Conseil fédéral

du 19 février 2020

Monsieur le Président,
Mesdames, Messieurs,

Conformément à l'art. 158 de la loi sur le Parlement, nous sur le rapport du 19 novembre 2019[1] de la Commission de gestion du Conseil national concernant la gestion de la cyberattaque menée contre RUAG.

Nous vous prions d'agréer, Monsieur le président, Mesdames, Messieurs, l'assurance de notre haute considération.

19 février 2020

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Simonetta Sommaruga
Le chancelier de la Confédération, Walter Thurnherr

1 FF **2020** 2467

Avis

1 Contexte

Le 19 novembre 2019, la Commission de gestion du Conseil national (CdG-N) a publié le rapport «Gestion de la cyberattaque menée contre RUAG: évaluation de l'avis rendu par le Conseil fédéral le 28 septembre 2018»[2], dans lequel elle revient sur les trois recommandations qu'elle a émises dans le premier rapport «Bilan de la gestion de la cyberattaque menée contre RUAG», publié le 8 mai 2018[3]. S'appuyant sur ses clarifications et les examens effectués par le Contrôle fédéral des finances (CDF), elle constate que les mesures décidées par le Conseil fédéral et le Département fédéral de la défense, de la protection de la population et des sports (DDPS) pour gérer la cyberattaque étaient adaptées et que leur mise en œuvre est en cours. Parallèlement, la CdG-N émet des recommandations sur le pilotage stratégique de l'entreprise d'armement appartenant à la Confédération.

Lors de sa séance du 15 mars 2019, le Conseil fédéral a pris des décisions fondamentales quant à la structure organisationnelle et la forme juridique ainsi qu'à l'orientation stratégique que prendra RUAG à l'avenir. À cette occasion, il s'est fortement inspiré des conclusions tirées par les organes de surveillance. Ainsi, il a notamment déterminé comment les diverses entités de RUAG devaient dorénavant être scindées en deux sous-groupes: RUAG MRO Holding SA et RUAG International Holding SA (ci-après respectivement MRO Suisse et RUAG International). Depuis, ces décisions se sont rapidement concrétisées. À intervalles réguliers, le Conseil fédéral s'est penché sur la scission et a pris des décisions d'orientation à mesure de l'avancée du projet. Les membres des conseils d'administration de la société de participation faîtière et des deux sous-groupes ont été élus le 23 octobre 2019. La scission organisationnelle des deux sociétés a pris effet le 1er janvier 2020.

2 Avis du Conseil fédéral sur la mise en œuvre des recommandations du 19 novembre 2019

Ci-après l'avis du Conseil fédéral.

Recommandation 1 *Prendre en compte les principales conclusions dans le cadre du pilotage stratégique*

La CdG-N invite le Conseil fédéral à examiner s'il est nécessaire, compte tenu des conclusions du CDF, d'opérer certains changements stratégiques dans le cadre du pilotage de RUAG, notamment dans le cadre des décisions qui seront prises quant à la structure organisationnelle et la forme juridique de RUAG et quant à une éventuelle privatisation partielle de l'entreprise.

2 FF **2020** 2467
3 FF **2018** 4683

Dans son avis du 28 septembre 2018[4], le Conseil fédéral a décrit les effets de la mise en œuvre des conclusions importantes du CDF dans le cadre du pilotage stratégique. Entre-temps, les secteurs d'activités dont profite principalement l'Armée suisse et ceux agissant sur le marché libre ont été séparés sur le plan organisationnel. Cette séparation prendra effet sur le plan juridique et sur le plan financier à l'été 2020. Ensuite, les deux sous-groupes MRO Suisse et RUAG International travailleront indépendamment l'un de l'autre. Le conseil d'administration de la société faîtière nouvellement formée (BGRB Holding), qui est chargé d'appliquer les objectifs stratégiques du Conseil fédéral, a commencé ses travaux.

Dans son rapport du 19 novembre 2019, la CdG-N pose des questions supplémentaires sur la recommandation 1[5].

Intégration de l'informatique et des données de RUAG dans le périmètre de sécurité de l'armée: la CdG-N souhaite voir le DDPS prendre, si nécessaire, de plus amples mesures en s'appuyant sur les conclusions tirées du contrôle des données.

Le Conseil fédéral confirme que la Base d'aide au commandement (BAC) a pris des mesures préventives exhaustives avant la migration des données de MRO Suisse dans le périmètre de sécurité du Groupement Défense; ces données se trouvent désormais dans une zone qui leur est réservée. Après leur identification, elles sont mises en quarantaine et soumises à un dépistage de tous les types de maliciels connus avant d'être acceptées. Puisque la quantité des données destinées à migrer n'a été concrètement établie qu'avec la définition détaillée de la structure définitive de MRO Suisse, les capacités rendues initialement disponibles pour leur identification et leur scannage ont dû être massivement élargies, ce qui n'a été possible qu'avec la mise en service d'une masse importante d'équipements techniques supplémentaires. C'est pourquoi, jusqu'à fin janvier 2020, les données n'ont pas toutes pu être soumises au contrôle et à la procédure de migration. Ce processus exigeant n'a révélé jusqu'ici aucun maliciel, rendant inutile la prise de mesures supplémentaires.

Mandats de tiers que MRO Suisse devra assumer à l'avenir: la CdG-N craint que certains mandats émanant de tiers puissent être problématiques pour des raisons de sécurité informatique et donnent lieu à de nouveaux enchevêtrements.

MRO Suisse, en tant que maillon de la chaîne logistique de l'armée, entretient obligatoirement des interfaces avec des partenaires commerciaux. Les enchevêtrements (d'interfaces spécifiques) sont ainsi intentionnels. Étant donné que le domaine informatique de MRO Suisse sera cantonné à une zone séparée des autres (contrôles au travers de pare-feu et de ports) du Groupement Défense, des interfaces pour la communication à travers les limites de zones doivent être définies au sein du DDPS déjà, par exemple en ce qui concerne la Base logistique de l'armée ou armasuisse. Des mesures analogues doivent être prises pour chaque type de contact avec un partenaire commercial ou les marchés tiers. Concernant le genre d'interface choisie au cas par cas, le type de rapport entre le partenaire commercial, qu'il s'agisse d'un tiers ou non, et MRO Suisse importe peu. C'est plutôt le processus commercial liant

4 FF **2018** 6409

5 La troisième des quatre questions abordées dans cette section n'est traitée par la CDG-N que sous la recommandation 3, d'où le traitement analogue qui lui est réservé dans le présent avis.

MRO Suisse aux divers clients, fabricants originels, fournisseurs ou sous-traitants qui est déterminant.

Afin d'assurer que l'état des pièces d'équipement soit documenté tout au long du cycle de vie de celles-ci tout en répondant aux normes de l'industrie, il importe que les constructeurs, utilisateurs et entreprises d'entretien travaillent sur la base d'un seul et même document d'accompagnement. L'installation nécessaire à cet effet de portails Internet ou d'autres possibilités permettant l'échange de paquets de données est examinée et approuvée au cas par cas par la BAC. Les interfaces indispensables aux processus d'affaires sont cloisonnées par des pare-feu et des contrôles d'accès. Elles ne sont accessibles qu'aux seuls utilisateurs autorisés, et chaque transaction est documentée. Plus aucun enchevêtrement ne pourra encore se faire en dehors de tout contrôle, et MRO Suisse respectera les normes de sécurité du Groupement Défense. L'amélioration des processus et la garantie de la cybersûreté et de la sécurité des informations est une tâche permanente. Le Secrétariat général du DDPS (SG-DDPS) effectue des audits et des contrôles auprès des partenaires externes, sur mandat des responsables de la sécurité des groupements ou des offices.

Risques liés à la privatisation: la CdG-N fait valoir que la privatisation implique des risques financiers. Les recettes escomptées des désinvestissements, comme le montant des investissements qu'il faudrait engager pour que RUAG puisse être privatisée, sont difficiles à estimer. Ces montants sont forcément établis sur la base d'estimations, lesquelles pourraient rapidement varier en cas de changement des conditions générales ou de la situation sur le marché.

Le Conseil fédéral reconnaît que la dissociation des activités du groupe et la privatisation de RUAG International constituent un projet hautement complexe et risqué. Il rappelle qu'à l'origine de ses décisions sur la transformation de RUAG, en plus d'autres objectifs, il affichait aussi la volonté d'écarter les risques pour le propriétaire qu'il n'était plus prêt à supporter en raison de l'orientation internationale de RUAG et de l'enchevêtrement avec les services informatiques de la Confédération. La poursuite en l'état de la situation n'aurait plus été défendable juridiquement et aurait pu, à ses yeux, faire naître des risques financiers plus grands encore pour la Confédération à long terme. Le Conseil fédéral, conscient des risques liés à un tel processus, a dès lors sciemment opté pour une adaptation de la stratégie. Afin de défendre au mieux les intérêts de la Confédération, il se réserve encore deux options pour la privatisation complète à moyen terme de RUAG International. Au premier plan, la constitution d'un groupe aérospatial et, comme position de repli, la vente des diverses sociétés de RUAG International. En privatisant cette dernière, le Conseil fédéral s'efforce de limiter les risques à leur strict minimum et, si possible, de tirer un bon bénéfice de la vente, le tout au profit des caisses de l'État et, en fin de compte, des contribuables. Par ses décisions, il tiendra également compte du poids des sociétés concernées sur l'économie publique. Dans les régions périphériques, RUAG est un employeur important et contribue à l'essor de la place industrielle Suisse. Les effets de la dissociation sur les ressources fiscales du pays sont pluridimensionnels et ne peuvent pas être évalués à l'aune seule des recettes tirées des ventes et des privatisations. RUAG International soumettra au Conseil fédéral un plan de mise en œuvre présentant la transformation prévue du groupe partiel en un groupe aérospatial, en s'appuyant sur des chiffres et des jalons mesurables. Le

Conseil fédéral et les organes du Département fédéral des finances (DFF) et du DDPS représentant le propriétaire surveilleront en permanence et de très près l'avancée du projet. Le Conseil fédéral a aussi inscrit dans ses objectifs stratégiques le fait que BGRB Holding doit disposer d'un système de gestion des risques entrepreneuriaux axé sur la norme ISO 31000.

Le Conseil fédéral pense qu'il a fait les bons choix et estime donc la recommandation 1 comme étant mise en œuvre.

Recommandation 2	*Prendre en compte le problème du désenchevêtrement des réseaux dans la perspective des externalisations futures et dans le cadre des principes régissant le gouvernement d'entreprise*

La CdG-N invite le Conseil fédéral à garantir que le problème du désenchevêtrement des réseaux sera dûment pris en compte dans le contexte des externalisations futures. Il déterminera plus spécifiquement si la question de l'imbrication des réseaux ne devrait pas entrer dans les critères décisifs appliqués aux projets d'externalisation ou être prise en compte dans les prescriptions et rapports établis en matière de gouvernement d'entreprise.

Prérequis relatifs au thème de la dissociation dans les objectifs stratégiques des entreprises proches de la Confédération: vu la réponse du Conseil fédéral à la recommandation 2, la CdG-N considère qu'une question essentielle est restée sans réponse, à savoir que celui-ci ne savait pas encore s'il allait formuler des directives générales sur le traitement du problème du désenchevêtrement dans les objectifs stratégiques des entreprises proches de la Confédération.

Comme expliqué par le Conseil fédéral dans son avis du 28 septembre 2018, il peut, au besoin, émettre des directives spécifiques sur la dissociation ou l'enchevêtrement dans les objectifs stratégiques pour les unités existantes ou nouvelles. Il considère néanmoins que RUAG est, dans ce contexte, un cas spécial puisque l'imbrication de cette entreprise dans l'administration fédérale – plus précisément le DDPS – était particulièrement forte et étendue, et que des données sensibles pour la politique de sécurité étaient concernées. Il ressort de cette analyse qu'il serait extrêmement difficile de formuler globalement des principes contraignants sur le problème du désenchevêtrement qui soient significatifs tout en étant pertinents ne serait-ce que pour la majorité des entreprises proches de la Confédération. Le Conseil fédéral retient cependant que la gestion complexe de la cyberattaque contre RUAG suivie de la dissociation de ses activités ont sensibilisé fortement à cette problématique les organes représentant le propriétaire ainsi que ceux de la Confédération chargés de la sécurité et de la fourniture de services informatiques.

Le Conseil fédéral considère que la recommandation 2 a été suivie dans les faits.

Recommandation 3 *Recourir de manière judicieuse aux instruments de pilotage pour défendre les intérêts du propriétaire*

La CdG-N demande au Conseil fédéral d'expliquer par quels moyens il entend veiller à une mise en œuvre judicieuse des instruments de pilotage et donc à une défense plus résolue des intérêts du propriétaire.

Le pilotage stratégique, en particulier, ne doit pas avoir lieu à l'occasion de contacts informels, mais dans le cadre des entretiens avec le propriétaire. La CdG-N demande aussi que les discussions et décisions importantes soient consignées par écrit. Enfin, elle attend du Conseil fédéral qu'il envisage très sérieusement, au vu des défis à relever, d'introduire (au moins passagèrement) au Conseil d'administration de RUAG un représentant qui suivrait ses instructions.

Comme exposé par le Conseil fédéral dans son avis du 28 septembre 2018, il pilote les entreprises proches de la Confédération dans le cadre des principes directeurs relatifs au gouvernement d'entreprise en s'appuyant sur les rapports qu'il a établis[6], à travers l'élection du conseil d'administration, ainsi que par la définition des objectifs stratégiques et l'établissement d'un rapport sur la réalisation de ces objectifs. Ces dernières années, les principes de gouvernement n'ont cessé d'être développés et adaptés aux nouveaux défis économiques et politiques auxquels les entreprises sont confrontées.

Les derniers développements dans les entreprises proches de la Confédération ainsi que les débats politiques et les interventions parlementaires ont incité le Conseil fédéral à faire contrôler par des organismes externes le pilotage de ces entreprises. À cette occasion, l'attention a été portée sur les entreprises fournissant principalement des prestations sur le marché (La Poste, RUAG, CFF et swisscom). Par leurs recommandations, les experts ont souligné un certain nombre de possibilités d'optimisation[7]. Les mesures décidées le 26 juin 2019 par le Conseil fédéral, qui a tenu compte de ce rapport d'experts, sont concrétisées ou en voie de l'être. Le Conseil fédéral informera des résultats de la mise en œuvre dans le cadre de son rapport en exécution du postulat 18.4274 Abate «Stratégie du propriétaire pour les entités de la Confédération devenues autonomes».

Contacts informels et entretiens personnels: les contacts informels entre les dirigeants des entreprises et le propriétaire sont inévitables. Dans ce contexte, il faut veiller à ne pas empêcher, dévaloriser ou contourner l'échange d'informations dans le cadre des structures ordinaires existantes. Les informations tirées des contacts

6 Rapport du 13 septembre 2006 sur le gouvernement d'entreprise, FF **2006** 7799; rapport du Conseil fédéral du 25 mars 2009 complétant le rapport sur le gouvernement d'entreprise – Mise en œuvre des résultats des délibérations au sein du Conseil national, FF **2009** 2299; aperçu des 37 principes directeurs relatifs aux entités de la Confédération devenues autonomes (état e 2019) dans la version de 2009 www.efv.admin.ch > Thèmes > Politique budgétaire, Bases > Gouvernement d'entreprise > Bases.

7 Lienhard, Andreas; Rieder, Stefan; Sonderegger, Roger W.; Ladner, Andreas; Höchner, Claudia; Ritz, Manuel; Roose, Zilla (2019): Évaluation du gouvernement d'entreprise de la Confédération fondée sur l'analyse de quatre entreprises. Rapport à l'intention de l'Administration fédérale des finances. Berne, Lucerne, Saint-Gall, Lausanne. www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75607.html

informels peuvent, au demeurant, fournir des sujets à mettre à l'ordre du jour des entretiens avec le propriétaire.

Si le chef du DDPS ou le chef du DFF les perçoivent comme tels, ces contacts ne servent pas à la gestion stratégique. Comme indiqué par le Conseil fédéral dans son avis du 28 septembre 2018, ils constituent au plus un complément. Ils peuvent améliorer la transparence de l'entreprise aux yeux du propriétaire dans la mesure où ils donnent un cadre à l'exposition de considérations qui ne trouveraient pas leur place auprès d'un organe formel. La gestion stratégique s'opère par la concrétisation des objectifs stratégiques du Conseil fédéral dans le cadre des entretiens avec le propriétaire, rapportés par écrit, et de leurs séances de préparation, de même que, jusqu'à la fin du projet de dissociation, au travers de l'organisation spécifique du projet dirigée par le secrétaire général du DDPS, de ses séances et de ses décisions, également rapportées par écrit. La répartition des tâches et des responsabilités entre le DDPS et le DFF pour la dissociation des activités et la privatisation de RUAG Holding SA a été réglée dans le cadre d'une approche commune.

Élection d'un représentant de la Confédération au conseil d'administration de RUAG: la question des représentants recevant des instructions siégeant dans le conseil d'administration des entreprises proches de la Confédération a aussi été abordée dans le rapport de 2006 sur le gouvernement d'entreprise[8] et dans les addenda correspondants.

L'élection de membres de l'administration en qualité de représentants de la Confédération par l'assemblée générale de l'entreprise ou leur délégation directe par le Conseil fédéral conformément à l'art. 762 du droit des obligations[9] peut se révéler problématique, notamment parce que l'administration assume souvent les rôles de surveillant spécialisé et de commanditaire. L'interdépendance du personnel entre l'administration et l'unité devenue autonome peut être limitée à son minimum si les membres de l'administration ne sont dépêchés ou élus qu'exceptionnellement au sein du conseil d'administration[10]. Selon le principe nº 9 relatif au gouvernement d'entreprise, la Confédération ne doit dorénavant être représentée dans les conseils d'administration ou d'institut d'entités devenues autonomes par des personnes recevant des instructions que si ses intérêts ne peuvent pas être défendus adéquatement en l'absence de ces représentants ou si le profil d'exigences du conseil d'administration ou du conseil d'institut le requiert.

Le Conseil fédéral est conscient qu'il y aurait potentiellement des raisons d'appliquer des exceptions dans le cas de RUAG. Il a cependant emprunté une autre voie en fondant BGRB Holding. Tant que RUAG International reste la propriété de la Confédération, BGRB Holding chapeaute les deux sous-groupes juridiquement séparés que sont MRO Suisse et RUAG International. Le conseil d'administration de BGRB Holding est donc tenu de réaliser les objectifs stratégiques du Conseil fédéral dans ces deux sous-groupes, notamment en supervisant leur dissociation, puis la privatisa-

8 Il s'agit, en plus du rapport complémentaires de 2009, du rapport explicatif de l'Administration fédérale des finances du 13 septembre 2006; disponible également sous www.efv.admin.ch > Thèmes > Politique budgétaire, Bases > Gouvernement d'entreprise > Bases.

9 RS **220**

10 Rapport explicatif de l'Administration fédérale des finances du 13 septembre 2006, p. 32

tion de RUAG International. BGRB Holding continuera ces activités aussi longtemps que ce processus sera en cours. Le Conseil fédéral est convaincu qu'une solution adaptée a ainsi été donnée pour pouvoir défendre correctement les intérêts de la Confédération, même pendant le processus de restructuration.

De plus, les élaborateurs des profils pour les sous-groupes ont veillé à ce qu'un représentant ayant un profil militaire siège au conseil d'administration de MRO Suisse. Cette personne, qui répond au profil d'exigences requis, n'appartient pas à l'administration fédérale. Elle n'a pas d'instructions à recevoir; en d'autres termes, elle n'est juridiquement pas tenue de défendre des intérêts spécifiques de la Confédération. Elle doit par contre bien connaître les exigences et les intérêts de cette dernière et pouvoir les représenter.

Ressources pour le pilotage de RUAG: en automne 2018, lors de l'élaboration du projet de dissociation des activités de RUAG, le SG-DDPS a constaté que le pilotage stratégique de l'entreprise exigera plus de ressources en personnel que ce qui était consacré jusque-là à la gestion des participations de RUAG Holding SA (1 équivalent plein temps dans le domaine de la politique de sécurité). La direction du département du DDPS a donc décidé de mettre sur pied un domaine composé de trois personnes au maximum en augmentant les ressources pour le pilotage de RUAG au travers de restructurations internes au SG-DDPS. Le poste de chef Gestion des participations a été remplacé par celui plus élevé de chef Politique de propriétaire, en lui établissant pour l'occasion un nouveau cahier des charges, en le réoccupant et en le subordonnant directement au chef Politique de sécurité DDPS. La position de suppléant dans ce dernier domaine est occupée depuis le 1er février 2020. Le SG-DDPS examinera l'opportunité d'ajouter trois personnes l'effectif du domaine.

L'Administration fédérale des finances, par un examen interne des priorités, a pu dégager des ressources suite à un contrôle systématique de ses tâches et structures. Une partie de la marge de manœuvre ainsi gagnée a servi à intensifier le pilotage des entreprises proches de la Confédération.

En résumé, le Conseil fédéral considère que la recommandation 3 aussi a été suivie et donc que toutes les recommandations ont été suivies dans les faits.