Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bilan de la gestion de la cyberattaque menée contre RUAG

Rapport de la Commission de gestion du Conseil national

du 8 mai 2018

Condensé

En janvier 2016, les experts de la Confédération ont découvert qu'une cyberattaque avait été lancée contre RUAG et en ont informé le Conseil fédéral. Comme les informations relatives à cet incident avaient été classifiées «SECRET» dans un premier temps, le dossier a d'abord été confié à la Délégation des Commissions de gestion (DélCdG) des Chambres fédérales. Après que la nouvelle de l'attaque a été rendue publique, la DélCdG a essentiellement mis un terme à ses travaux sur ce dossier, qu'elle a transmis à la Commission de gestion du Conseil national (CdG-N). Les travaux de la CdG-N visaient avant tout à déterminer si les autorités fédérales responsables – notamment le Conseil fédéral et le DDPS – avaient réagi à l'incident de manière adéquate et avec la diligence requise et si elles avaient veillé à assurer la défense des intérêts de la Confédération en tant que propriétaire. Ils n'étaient par contre pas focalisés sur le contrôle de la mise en œuvre des mesures prises à la suite de la cyberattaque, car cette tâche était déjà assumée par d'autres organes, notamment par le CDF.

Dans le cadre de son enquête, la sous-commission compétente de la CdG-N a entendu le chef du DDPS ainsi que d'autres représentants du département. Elle a également analysé de nombreux documents en rapport avec l'incident lui-même, mais aussi avec le pilotage de RUAG (par ex. procès-verbaux des réunions régulières du chef du DDPS avec la direction de RUAG). Comme les informations qu'elle avait requises ne lui étaient pas toujours livrées dans les délais ou étaient de qualité insuffisante, il ne lui a longtemps pas été possible d'évaluer la situation. Ce n'est qu'en novembre 2017 qu'elle a estimé disposer d'une base d'informations suffisante pour pouvoir faire le point et répondre aux questions essentielles.

Parmi les informations obtenues par la sous-commission figuraient des renseignements détaillés sur les fichiers piratés et sur les risques résultant de ce vol. Sur la base de ces données, elle a qualifié l'incident de grave. Elle a cependant aussi constaté que le Conseil fédéral et le DDPS avaient réagi de manière diligente et adéquate, en analysant les risques et en ordonnant les mesures qui s'imposaient. Elle salue plus particulièrement le fait que le DDPS ait mis RUAG face à ses responsabilités dans cette affaire en exigeant de l'entreprise une coopération étroite.

Compte tenu des résultats de ses propres travaux, mais aussi des contrôles opérés par le CDF, la CdG-N constate que la mise en œuvre des mesures prises à la suite de la cyberattaque progresse essentiellement comme prévu. Seule exception: le désenchevêtrement des réseaux TI de la Confédération et de RUAG ordonné par le Conseil fédéral. Cette tâche s'est en effet révélée beaucoup plus complexe et nettement plus longue que prévu. La Commission en prend acte, mais estime néanmoins que cette mesure est importante et qu'il est donc très urgent de faire avancer sa mise en œuvre.

La CdG-N a aussi souhaité savoir comment la cyberattaque et ses conséquences avaient été traitées dans le cadre du pilotage stratégique et quelles dispositions le DDPS avait prises en sa qualité de représentant du propriétaire pour défendre les intérêts de la Confédération en tant que propriétaire. Les résultats de ses travaux

l'ont portée à douter de la capacité du DDPS à représenter et à défendre dûment les intérêts de la Confédération en tant que propriétaire face à RUAG. La CdG-N estime en effet que si le DDPS dispose bien des instruments nécessaires au pilotage stratégique de l'entreprise, il ne s'en sert pas toujours de manière appropriée. Les entretiens avec le propriétaire, par exemple, n'ont ainsi pas été (suffisamment) mis à profit pour y discuter aussi de problèmes tels que la cyberattaque et de leurs conséquences potentielles sur la réalisation des objectifs stratégiques, pour poser des exigences ou pour attribuer des mandats. Au lieu de cela, certaines discussions importantes sont conduites dans un cadre informel et il n'en existe aucune trace écrite. En procédant de la sorte, le DDPS se prive non seulement de bases d'information solides, mais aussi d'un moyen ou d'un instrument lui permettant de faire respecter ses exigences et ses directives stratégiques.

En conséquence, la Commission attend du DDPS qu'il se montre plus ferme dans ses rapports avec RUAG et qu'il veille, le cas échéant, à imposer les exigences de la Confédération et à défendre ses intérêts avec plus de force. Elle adresse en outre trois recommandations au Conseil fédéral et exige de sa part différentes clarifications en vue d'obtenir une amélioration du gouvernement d'entreprise.

Rapport

1 Introduction

Fin janvier 2016, le DDPS a informé la Délégation des Commissions de gestion des Chambres fédérales (DélCdG) qu'un incident grave avait compromis la sécurité informatique au sein du groupe d'armement suisse RUAG[1], aux mains de la Confédération. Dans un premier temps, les informations relatives à cet événement avaient été classifiées «SECRET» par le Conseil fédéral. En conséquence, c'est la DélCdG qui s'est d'abord occupée de suivre ce dossier. A la suite de la divulgation de la cyberattaque, la DélCdG a informé le public de ses travaux et des résultats de ses recherches le 4 mai 2016. Comme l'enquête sur de tels événements ne relève par principe pas de sa compétence, la DélCdG a essentiellement mis un terme à ces travaux dans cette affaire[2] et a transmis le dossier aux Commissions de gestion (CdG) des Chambres fédérales.[3]

Le 29 juin 2016, la CdG du Conseil national (CdG-N) a chargé sa sous-commission DFAE/DDPS de suivre la mise en œuvre de certaines mesures que le Conseil fédéral avait ordonnées à la suite de la cyberattaque. La sous-commission a alors concentré ses recherches sur les aspects du désenchevêtrement[4] des réseaux du DDPS et de RUAG ainsi que des conséquences de la cyberattaque pour RUAG. Elle a notamment souhaité savoir si les services responsables – essentiellement au DDPS et chez RUAG – avaient fait preuve de la diligence requise dans leur recherche de solutions aux problèmes mis au jour par l'intrusion et si les mesures prises pour y remédier s'étaient révélées efficaces. En cours d'enquête, des questions ont été soulevées concernant la défense des intérêts du propriétaire par la Confédération ainsi que le rôle du DDPS en sa qualité de représentant du propriétaire. La sous-commission a donc inclus ces questions dans ses travaux.

Dans le cadre de ses travaux, la sous-commission a étudié de nombreux documents de l'administration, mais aussi de RUAG, dont plusieurs étaient sensibles, voire strictement confidentiels. Elle a en outre entendu plusieurs fois des représentants du DDPS, notamment le chef du DDPS, la secrétaire générale du DDPS, le délégué DDPS pour la cyberdéfense et le chef de la gestion des participations du DDPS. En mai 2017, à l'occasion d'une séance consacrée au rapport du Conseil fédéral sur la

1 RUAG (RUAG Holding SA) a été créée par voie législative en 1997 (loi fédérale sur les entreprises de la Confédération) sous la forme d'une entité devenue autonome. L'entreprise, qui appartient à 100 % à la Confédération, compte aujourd'hui près de 80 sites (dont la moitié à peu près se situent à l'étranger). En 2016, elle a réalisé un chiffre d'affaires net de 1858 millions de francs et un bénéfice net de 116 millions de francs, dont plus d'un tiers a été reversé à la Confédération sous forme de dividendes (cf. aussi ch. 4).

2 La DélCdG s'est alors concentrée sur les aspects relatifs aux activités de renseignement et sur le volet pénal de l'affaire (cf. rapport annuel 2016 des CdG et de la DélCdG, FF **2017** 3578).

3 Cf. ch. 4.4 du rapport annuel 2016 des CdG et de la DélCdG (FF **2017** 3578).

4 La dissociation des activités chez RUAG touche l'organisation, les processus ainsi que les infrastructures et les systèmes informatiques. Dans le présent rapport, elle ne concerne toutefois que les systèmes d'information et les réseaux informatiques.

réalisation des objectifs de RUAG pour l'exercice 2016 avec la direction de l'entreprise, celle-ci a abordé l'incident lors de l'intervention concernant le bilan de l'exercice écoulé. La sous-commission a renoncé à entendre d'autres représentants de RUAG, car l'enquête de la sous-commission était clairement focalisée sur les décisions prises par les acteurs de la Confédération, plus précisément du DDPS. Entre juin 2016 et novembre 2017, la sous-commission a discuté ce sujet à l'occasion de huit séances au total.

A plusieurs reprises, la sous-commission a eu des difficultés à se procurer les informations et les documents souhaités, au point qu'elle a été contrainte d'intervenir auprès du département ou, plus précisément, auprès du Secrétariat général du DDPS. Comme, plus d'une fois, les renseignements demandés n'ont pas été fournis dans les délais ou n'étaient pas complets ou pas suffisamment clairs, la sous-commission a dû patienter longtemps avant de pouvoir se faire une idée cohérente de la situation et d'être en mesure de juger de la gravité du problème. Ce n'est en effet qu'en novembre 2017 qu'elle a estimé disposer d'une base d'informations suffisante – bien que toujours incomplète à certains égards – pour lui permettre de faire le point sur les questions essentielles et de mettre un terme provisoire à son enquête.

Le présent rapport de la CdG-N doit clairement être compris comme un bilan intermédiaire: il contient certes des évaluations et des recommandations, mais aussi plusieurs questions encore sans réponse. La majeure partie des incertitudes tourne autour de la mise en œuvre du désenchevêtrement des réseaux du DDPS et de RUAG. Cette entreprise est non seulement sensiblement plus complexe et plus longue qu'on ne l'imaginait, mais elle est aussi intimement liée à la question de la structure organisationnelle et de la forme juridique que devra prendre RUAG et à la question d'une privatisation (partielle) de RUAG, et donc de l'influence que la Confédération pourra conserver au sein du groupe ainsi que du rôle de celui-ci comme garant de l'équipement de l'armée. La CdG-N restera donc attentive à ce sujet.

Dans le cadre de la consultation de l'administration, le projet de rapport de la sous-commission respectivement les chapitres du projet de rapport consacrés aux faits les concernant ont été envoyés au DDPS et à RUAG pour avis (correction d'erreurs formelles et matérielles). La sous-commission a ensuite traité les réponses issues de la consultation de l'administration et de l'audition, avant d'adapter son rapport lorsque cela se révélait nécessaire.

La structure du présent rapport est la suivante: le ch. 2 traite des mesures prises en réponse à la cyberattaque, dont le désenchevêtrement des réseaux évoqué plus haut. Les dommages causés par le piratage sont l'objet du ch. 3 et le ch. 4 porte sur le pilotage stratégique de RUAG ainsi que sur le rôle à jouer par le DDPS dans la défense des intérêts de la Confédération en sa qualité de propriétaire. Le rapport se termine par les ch. 5 et 6, consacrés aux conclusions et aux recommandations.

2 Mesures prises à la suite de la cyberattaque

Dans le présent chapitre, la CdG-N a cherché à déterminer si les mesures destinées à remédier aux conséquences de la cyberattaque avaient été prises en temps utile et si leur mise en œuvre avait été suivie et contrôlée de manière adéquate. L'évaluation des mesures elles-mêmes n'entre pas dans les attributions de la CdG-N et n'est donc pas l'objet de ses travaux. La mesure portant sur le désenchevêtrement des réseaux du DDPS et de RUAG fait toutefois exception (cf. ch. 2.1.3 et 2.2.3). Ainsi qu'il en a déjà été fait mention dans l'introduction, la CdG-N accorde en effet une importance particulière à cet élément. En conséquence, la sous-commission compétente s'est renseignée de manière répétée sur l'état de la mise en œuvre de cette mesure et sur les problèmes rencontrés dans ce contexte.

2.1 Rappel des faits

Début décembre 2015, le Service de renseignement de la Confédération (SRC) a reçu des informations selon lesquelles le système informatique de RUAG pouvait être la cible d'une cyberattaque. Il en a immédiatement informé l'entreprise. Avec l'assistance des spécialistes de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI/GovCERT)[5] du DFF, la présence d'un logiciel malveillant dans le système de RUAG[6] a pu être établie un mois et demi plus tard. Il s'agissait d'un maliciel de la famille Turla qui existe déjà depuis plusieurs années.[7]

La nouvelle de cette découverte a alors été annoncée au Groupe Sécurité de la Confédération[8], puis au Conseil fédéral ainsi qu'à sa Délégation pour la sécurité (Délséc)[9]. Finalement, le chef du DDPS en a aussi informé la DélCdG à la fin du mois de janvier 2016.

5 MELANI est opérationnelle depuis le 1er octobre 2004. Chargée par le Conseil fédéral de protéger les infrastructures critiques, elle a pour objectif le dépistage précoce et la résolution de problèmes se posant dans l'infrastructure de l'information et de la communication. MELANI est un modèle de coopération entre le Département fédéral des finances (DFF), représenté par l'Unité de pilotage informatique de la Confédération (UPIC) et le Département fédéral de la défense, de la protection de la population et des sports (DDPS), représenté par le Service de renseignement de la Confédération (SRC). GovCERT a été créé par MELANI en 2008 pour lui permettre de réagir encore plus rapidement aux incidents.

6 Cf. ch. 4.4 dans le rapport annuel 2016 des CdG et de la DélCdG (FF **2017** 3576).

7 Résumé: rapport technique sur la cyberattaque contre RUAG du 23.05.2016 (www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-techniques/technical-report_apt_case_ruag_summary.pdf.download.pdf/TR-ZF-f.pdf).

8 Le Groupe Sécurité de la Confédération est constitué du secrétaire d'État du DFAE, du directeur du SRC et de la directrice de fedpol. Sa principale mission est de suivre et d'évaluer l'évolution de la situation sécuritaire ainsi que d'identifier à temps les défis qui se présentent. Le Groupe Sécurité assure un suivi permanent de la situation sécuritaire, en rend compte à la Délégation de sécurité du Conseil fédéral et lui soumet des propositions lorsqu'il le juge utile.

9 La Délséc est un organe du Conseil fédéral. Elle renforce la capacité de diriger du Conseil fédéral en préparant les délibérations et les décisions du Conseil fédéral dans le domaine de la politique de sécurité. La Délséc est composée des chefs du DFAE, du DFJP et du DDPS. cf. ordonnance sur l'organisation de la conduite de la politique de sécurité du Conseil fédéral du 24 octobre 2007, RS **120.71**.

2.1.1 Mesures mises en place

2.1.1.1 Mesures du Conseil fédéral

Le 4 février 2016, la Délégation pour la sécurité du Conseil fédéral (Délsec) a chargé le Groupe Sécurité d'évaluer le dommage subi, de déterminer les risques et d'examiner les mesures à prendre. En conclusion d'une première analyse, le Groupe Sécurité a proposé au Conseil fédéral différentes mesures d'urgence ainsi qu'une série d'autres mesures à mettre en œuvre à court ou à moyen terme. Le 23 mars 2016, le Conseil fédéral a arrêté secrètement 14 mesures relevant de la responsabilité de différents services de la Confédération, dont la plupart sont rattachés au DDPS, mais aussi de l'UPIC et de l'OFIT. Il a aussi fixé des délais pour la mise en œuvre de ces mesures et chargé le Groupe Sécurité de la superviser. Le 11 mai 2016, le Conseil fédéral a ordonné quatre mesures supplémentaires en réaction à la cyberattaque contre RUAG.

La supervision de la mise en œuvre des mesures a été répartie entre plusieurs acteurs, dont le DDPS principalement, ou des services du DDPS (cf. à ce propos le ch. 2.1.2 infra), mais aussi d'autres services de la Confédération comme l'OFIT. Ils ont été chargés de rendre compte de leurs travaux au Groupe Sécurité, qui a procédé au monitorage de la mise en œuvre des mesures.

2.1.1.2 Mesures du DDPS

En plus des mesures ordonnées par le Conseil fédéral, le DDPS a lui aussi pris certaines dispositions. Ces mesures mises en place à l'initiative du DDPS portaient essentiellement sur des procédures et des vérifications internes. Bon nombre d'entre elles visaient la Base d'aide au commandement (BAC) et la Base logistique de l'armée (BLA), qui sont les deux principales partenaires de RUAG au sein du DDPS.

Peu après avoir eu connaissance de la cyberattaque, le chef du DDPS a institué la *task force* RHINO[10], qui avait pour mission de collaborer avec RUAG et les autres acteurs engagés (notamment le SRC, MELANI[11] ou l'UPIC[12]) en vue de prendre les mesures d'urgence nécessaires et d'évaluer les dommages causés. Cette *task force* a assuré le suivi non seulement des mesures du DDPS, mais aussi des mesures ordonnées par le Conseil fédéral et des dispositions internes prises par RUAG pour rétablir la sécurité (cf. titre suivant). La *task force* était en contact étroit avec tous les acteurs engagés au niveau de la Confédération tout comme avec RUAG et se tenait régulièrement informée des mesures prises ainsi que des progrès réalisés dans la mise en œuvre. Malgré certains problèmes sur le plan stratégique, en particulier durant les

10 Elle était composée de responsables du SG-DDPS, de l'armée, du SRC, d'armasuisse, d'autres services de la Confédération intéressés ainsi que de représentants de RUAG.
11 Cf. note de bas de page 4.
12 L'Unité de pilotage informatique de la Confédération (UPIC) est chargée de mettre en œuvre la Stratégie de la Confédération en matière de technologies de l'information et de la communication dans l'administration fédérale. Elle dirige aussi la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

premiers temps qui ont suivi la découverte de l'attaque (déficiences dans la coopération avec le DDPS; cf. ch. 4.1.3)[13], la coopération sur les plans opérationnel et technique a généralement bien fonctionné selon les représentants du DDPS interrogés.[14]

En juillet 2016, le chef du DDPS a transformé la *task force* en groupe de travail[15]. Celui-ci devait continuer de gérer les conséquences de l'attaque et de suivre la mise en œuvre des mesures prises par la suite; il avait également pour mission d'entamer une réflexion plus fondamentale sur une stratégie de gestion des cybermenaces au DDPS et d'élaborer un «Plan d'action cyberdéfense».

2.1.1.3 Mesures de RUAG

Comme cela a été précisé en introduction, la cyberattaque et le maliciel utilisé n'ont été découverts chez RUAG que grâce à l'information reçue par le SRC et au terme de recherches très poussées pour lesquelles l'entreprise a bénéficié de l'aide substantielle des spécialistes de MELANI. Il s'est avéré que le maliciel en cause appartenait à un type de logiciels malveillants connu depuis longtemps. Dans sa réponse à une intervention parlementaire, le Conseil fédéral a ainsi souligné que cela faisait des années que l'on avait, par l'intermédiaire de MELANI, communiqué les caractéristiques techniques de la famille de maliciels en question aux exploitants d'infrastructures critiques, dont RUAG, mais que c'est ensuite aux entreprises elles-mêmes qu'il appartenait de tirer parti de ces informations pour améliorer leurs systèmes de sécurité.[16] RUAG a rejeté l'accusation selon laquelle elle n'aurait pas pris en compte les informations fournies par MELANI.[17]

Après la découverte du logiciel malveillant, la Confédération, ou le DDPS plus précisément, a chargé RUAG de mettre en œuvre huit mesures d'urgence. Elles visaient à enrayer le dommage et à rétablir la sécurité des systèmes informatiques de l'entreprise tout en améliorant leur surveillance. Parallèlement, RUAG a mis en oeuvre son propre programme de mesures afin de renforcer la sécurité contre les cyberattaques: ce programme appelé IMPACT comprend neuf mesures de prévention, de détection et de gestion des cyberattaques. Il est prévu que sa mise en œuvre, qui devrait être terminée d'ici la fin de 2019, coûte quelque 10 millions de francs.

13 Selon l'avis de RUAG transmis dans le cadre de la consultation de l'administration, il s'agissait à ce moment-là notamment de clarifier certaines questions d'ordre juridique, en particulier en ce qui concerne l'accès à des documents classifiés de tiers. En outre, les ressources humaines disponibles présentant les connaissances informatiques nécessaires et le niveau de contrôle de sécurité relatif aux personnes requis pour gérer l'incident étaient initialement limitées.

14 Audition de la secrétaire générale du DDPS et du délégué DDPS pour la cyberdéfense du 3.7.2017.

15 Le groupe de travail, qui se réunit une fois par mois, est composé de plus de 25 personnes représentant tous les secteurs du DDPS. La transformation en groupe de travail s'est accompagnée de légers changements dans sa composition, notamment en ce qui concerne la représentation de RUAG: présente dans la *task force*, elle ne l'est plus dans le groupe de travail.

16 Réponse du Conseil fédéral du 10.6.2016 à une question urgente du groupe PDC du 2.6.2016 (16.1022).

17 Communiqué de presse de RUAG du 16.6.2016.

Dans une note d'information du DDPS au Conseil fédéral[18], les mesures mises en place par RUAG sont qualifiées de «correctes». Le DDPS y relève néanmoins que la cybersécurité ne pourra être renforcée qu'au prix d'un développement continuel de ces mesures et de changements dans la culture de sécurité de l'entreprise.

Rapidement, le DDPS a demandé à RUAG qu'elle précise l'échéancier du programme IMPACT et qu'elle rende compte régulièrement des progrès réalisés dans sa mise en œuvre. Après avoir constaté, selon sa propre admission, qu'il n'était légalement pas en droit, en tant que département, de requérir ce genre de renseignements de la part de RUAG[19], le DDPS a demandé au Conseil fédéral d'exiger de l'entreprise qu'elle lui soumette des rapports trimestriels rendant compte de l'état d'avancement du programme IMPACT.[20]

Cependant, le DDPS a par la suite jugé ces rapports insuffisants et a exigé la présentation d'un rapport plus détaillé avant fin novembre 2017. Selon les renseignements obtenus du DDPS, ce nouveau rapport répond maintenant aux exigences de qualité et au degré de précision requis pour permettre une évaluation solide.[21]

2.1.2 Examen des mesures

C'est le DDPS, et plus particulièrement la *task force* (aujourd'hui transformée en groupe de travail) RHINO, qui s'est occupé de garder une vue d'ensemble sur les mesures de gestion de la cyberattaque prises aux différents niveaux ainsi que de suivre leur mise en œuvre. Jusqu'à un certain point, il est aussi revenu au DDPS de revoir ces mesures (d'un œil critique). Le Groupe Sécurité de la Confédération a lui aussi assumé une partie des tâches de supervision.

Pour ce qui est de l'examen plus approfondi des mesures par une autorité indépendante, ce sont le Contrôle fédéral des finances (CDF) et la DélCdG qui s'en sont chargé pour l'essentiel.

2.1.2.1 Contrôle fédéral des finances CDF

Au printemps 2016, le CDF a dirigé une procédure de contrôle de la mise en œuvre des mesures décidées par le Conseil fédéral le 23 mars 2016. En janvier 2017, il a fait part de ses conclusions à la Délséc, au Groupe Sécurité de la Confédération ainsi qu'au chef du DDPS et en mars 2017, il en a informé la DélFin.

Se fondant sur les informations recueillies, le CDF a constaté que la mise en œuvre des mesures, dont le désenchevêtrement des réseaux de la Confédération et de RUAG (cf. ch. 2.1.3), a engendré davantage de travail. Il a notamment souligné que ce désenchevêtrement se révélait plus complexe et plus long que prévu et que ces difficultés avaient des répercussions sur les discussions relatives à une privatisation

18 Note d'information du DDPS au Conseil fédéral du 10.4.2017.
19 Audition du délégué du DDPS pour la cyberdéfense du 3.7.2017.
20 Rapport du DDPS à la sous-commission du 28.6.2017.
21 Courrier du délégué DDPS pour la cyberdéfense à la sous-commission du 19.12.2017.

partielle de RUAG. Le CDF a aussi annoncé qu'il allait poursuivre ses contrôles de la mise en œuvre des mesures prises en réaction à la cyberattaque contre RUAG en 2017. Cette poursuite des contrôles a été saluée par le DDPS, qui a proposé au Conseil fédéral de mandater le CDF pour l'exercice d'une surveillance durable du secteur sécurité de l'information chez RUAG.[22]

En juin 2017, le CDF a procédé à un deuxième contrôle et c'est en août 2017 qu'il a informé le Conseil fédéral de l'état de la mise en œuvre des mesures ordonnées. Le CDF a conclu que la mise en œuvre des mesures était en majeure partie terminée ou du moins en bonne voie, à l'exception des opérations de désenchevêtrement des réseaux. La mise en œuvre de cette mesure prendra encore bien quelque temps, selon lui. Le CDF procédera à un nouveau contrôle de la mise en œuvre des mesures en 2018. Les résultats de ce contrôle devraient pouvoir être présentés d'ici fin juin 2018[23].

2.1.2.2 DélCdG/CdG

Comme la nouvelle de la cyberattaque n'a pas été rendue publique avant mai 2016 et comme le dossier avait été classé «SECRET» par le Conseil fédéral, c'est avant tout la DélCdG qui s'est penchée sur l'attaque et ses conséquences dans un premier temps. Elle a entendu à ce propos différents représentants du DDPS et de RUAG afin de discuter des mesures qui devaient être prises pour gérer l'incident. Dans un second temps, elle s'est aussi penchée sur la question des compétences et des structures nécessaires pour regagner le contrôle de la situation et a adressé un courrier au Conseil fédéral à ce sujet.[24] Fin juin 2017, la DélCdG a décidé de se concentrer sur les mesures relatives aux activités de renseignement ainsi que sur le volet pénal de l'affaire. Celle-ci ayant été rendue publique, il n'y avait plus aucune raison que la mise en œuvre des autres mesures ne soit pas contrôlée par des organismes tiers et que les CdG ne supervisent pas elles-mêmes la gestion de l'incident.

En conséquence, dès l'été 2016, la sous-commission DFAE/DDPS s'est réunie plusieurs fois pour être mise au courant de l'état d'avancement de la gestion de l'affaire et de la mise en œuvre des mesures adoptées. Son principal objectif était de déterminer si les organes de surveillance compétents – avant tout le Conseil fédéral et le DDPS – assumaient leur tâche de manière appropriée et non d'examiner dans le détail la mise en œuvre de chacune des mesures ordonnées, puisque c'était là l'objet du contrôle du CDF. Seule exception: la mesure déjà mentionnée plus haut se rapportant au désenchevêtrement des réseaux du DDPS et de RUAG (cf. ch. 2.1.3 ci-après).

22 Rapport du DDPS à la sous-commission du 28.6.2017.
23 État: 17.1.2018
24 Cf. ch. 4.4. du rapport annuel 2016 des CdG et de la DélCdG (FF **2017** 3578).

2.1.3 Mesure «Désenchevêtrement des réseaux du DDPS et de RUAG»

Sur la suggestion de la DélCdG, la CdG-N s'est intéressée tout particulièrement à la mise en œuvre de la dissociation des réseaux TI[25] de la Confédération et de RUAG. Le 23 mars 2016, le Conseil fédéral avait en effet chargé le DDPS de veiller à une dissociation aussi rapide que possible des affaires et des systèmes de la Confédération et de RUAG.[26] Selon l'échéancier initial, un plan d'assainissement devait être élaboré avant fin septembre 2016. Ce plan devait reposer sur les résultats d'une autre mesure ordonnée par le Conseil fédéral, qui avait chargé le DDPS de répertorier, jusqu'à la mi-avril 2016, toutes les connexions existant entre le DDPS et RUAG, y compris les interdépendances en matière de disponibilité de l'armée.[27]

Il est apparu assez rapidement que le simple recensement des interconnexions, mais avant tout le désenchevêtrement en tant que tel, étaient des tâches plus complexes que prévu, qui allaient donc prendre (beaucoup) plus de temps que prévu. En octobre 2016 déjà, les représentants du DDPS ont averti la CdG-N que le délai fixé pour la mise en œuvre de la mesure de désenchevêtrement et pour l'élaboration d'un plan d'assainissement avait été prolongé jusqu'à fin mars 2017. Le 10 mai 2017, le Conseil fédéral a finalement donné au DDPS jusqu'à fin juin pour lui présenter un rapport mettant en évidence les imbrications entre RUAG et l'armée ainsi que les moyens de dissocier les deux entités.

Dans son rapport du 21 juin 2017 à l'intention du Conseil fédéral, le DDPS relève que les liens entre RUAG et l'armée sont très étroits et que l'armée ne peut fournier aujourd'hui de nombreuses prestations qu'avec l'appui de RUAG. Les prestations de RUAG destinées à l'armée y sont décrites de manière détaillée, tout comme les interdépendances au niveau des prestations, des processus, de l'informatique et de l'immobilier. Le DDPS y donne ensuite un aperçu de ce que le désenchevêtrement signifie («si RUAG devient, sur tous les plans, un prestataire externe parmi d'autres pour le DDPS») et présente trois variantes de dissociation. Quelle que soit la variante choisie, le DDPS estime que ce désenchevêtrement aura des conséquences majeures pour l'armée et pour RUAG et qu'il doit donc être étudié très soigneusement non seulement par rapport aux engagements de l'armée, mais aussi pour ce qui est des répercussions en matière de politique de sécurité et sur le plan économique.

Le Conseil fédéral a traité le rapport du DDPS lors de sa séance du 28 juin 2017. Selon une lettre du DDPS à la sous-commission compétente datée du 25 octobre 2017, le Conseil fédéral a décidé de suspendre l'examen relatif à une privatisation (partielle) de RUAG jusqu'à ce que les opérations de dissociation soient terminées. Il est manifestement ressorti des travaux du DDPS sur ce projet ainsi que des discussions entre le DDPS et RUAG qu'une étude plus approfondie était nécessaire pour permettre la présentation d'un plan de désenchevêtrement détaillé (portée du projet, mesures à prendre, volume de travail et temps nécessaire). Selon cette même lettre,

25 La dissociation des réseaux TI va beaucoup plus loin que le simple désenchevêtrement des réseaux informatiques: elle doit aussi viser les interconnexions existant aux niveaux des prestations, des processus ou de l'immobilier.
26 Mesure 11 selon la décision du Conseil fédéral du 23.3.2016.
27 Mesure 3 selon la décision du Conseil fédéral du 23.3.2016.

le Conseil fédéral prévoirait de reprendre sa discussion relative au désenchevêtrement en mars 2018.

Dans le cadre des auditions, le DDPS a précisé à l'intention de la sous-commission compétente que la dissociation devait être coordonnée notamment avec la réorganisation de la BAC et que le degré de complexité de la tâche ne permettrait probablement pas d'achever les travaux avant 2023.

2.2 Appréciation

2.2.1 Mesures adoptées

Bien que n'ayant pas étudié en détail chacune des mesures, la CdG-N est d'avis qu'elles peuvent être considérées comme judicieuses dans l'ensemble. Elle constate que le Conseil fédéral est intervenu rapidement en chargeant le Groupe Sécurité de recueillir toutes les informations utiles, informations sur la base desquelles il a ensuite pu mettre en place des mesures sans perdre de temps.[28] Elle salue également le fait que la Délséc – une délégation du Conseil fédéral[29], donc – se soit très tôt saisie de l'affaire.

La CdG-N constate en outre que le DDPS a lui aussi réagi promptement à l'incident et qu'il a, en créant la *task force* RHINO, composée de représentants de RUAG, mais aussi de tous les acteurs concernés au niveau de la Confédération, mis en place un organisme qui a su gérer l'évaluation des dégâts et prendre les mesures d'urgence nécessaires. La CdG-N salue également le bon fonctionnement de la collaboration à ce niveau essentiellement opérationnel, d'autant plus que la direction de RUAG a eu tendance à sous-estimer l'incident dans un premier temps et à ne pas toujours se montrer très coopérative envers le DDPS.

S'agissant des mesures prises par RUAG, la sous-commission attend du DDPS qu'il continue de suivre leur mise en œuvre d'un œil critique et qu'il exige des améliorations ou une augmentation des moyens financiers à chaque fois qu'il le jugera nécessaire. Elle renvoie à ce propos à l'avis exprimé par le DDPS, selon lequel ces mesures ne suffiront pas si elles ne s'accompagnent pas de changements dans la «culture de sécurité» de l'entreprise (cf. ch. 2.1.1.3). Ce qui importe, c'est de défendre dûment les intérêts du propriétaire (cf. ch. 4).

28 La DélCdG a constaté dans le cadre de ses travaux que les membres du Groupe Sécurité et leurs offices ne disposaient pas eux-mêmes des connaissances techniques nécessaires pour pouvoir évaluer correctement la menace. Il aurait donc été plus judicieux à son sens de gérer cette affaire en se fiant directement aux structures régulières que le Conseil fédéral a lui-même mises en place au moyen de l'ordonnance sur l'informatique dans l'administration fédérale (OIAF) (cf. ch. 4.4 du rapport annuel 2016 des CdG et de la DélCdG [FF **2017** 3578]). Les travaux de la CdG-N n'étaient pas spécifiquement axés sur l'examen des structures.

29 Cf. Note de bas de page 9.

2.2.2 Examen des mesures

La CdG-N salue le fait que le Conseil fédéral a mandaté le CDF, soit un organe indépendant, pour contrôler la mise en œuvre des mesures prises à la suite de la cyberattaque.

Elle invite le Conseil fédéral à réfléchir, sur la base des conclusions du CDF, à l'opportunité de certains changements stratégiques dans le cadre du pilotage de l'entreprise, notamment dans la perspective des décisions qui seront prises quant à la structure organisationnelle et à la forme juridique de RUAG et quant à une éventuelle privatisation partielle de l'entreprise.

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.

2.2.3 Mesure «Désenchevêtrement des réseaux du DDPS et de RUAG»

La commission prend aussi acte du fait que les interconnexions entre les réseaux de la Confédération et de RUAG sont manifestement si complexes qu'un désenchevêtrement n'est pas réalisable à relativement brève échéance, comme cela avait été prévu initialement, mais seulement à l'horizon 2023. Elle se félicite néanmoins de voir le Conseil fédéral persévérer sur la voie du désenchevêtrement et l'invite, de même que le DDPS en particulier, à prendre toutes les dispositions et à mettre en œuvre tous les moyens nécessaires pour permettre l'aboutissement des efforts de désenchevêtrement dans les délais prévus.

Du point de vue de la commission, la cyberattaque contre RUAG a mis en exergue de manière plus générale le problème de l'interconnexion entre les réseaux de la Confédération et ceux des entités devenues indépendantes. En complément des mesures prises en réaction à la cyberattaque, le Conseil fédéral a aussi ordonné un examen critique de l'imbrication des réseaux de la Confédération et des autres entités devenues autonomes. Saluant cette mesure, la CdG-N attend du Conseil fédéral qu'il ne perde pas de vue ce problème et qu'il prenne les mesures qui s'imposent. Elle l'invite en outre à accorder à la question des interdépendances et de leurs conséquences toute l'importance qu'elle mérite dans la perspective des externalisations ou des privatisations qui pourraient avoir lieu dans le futur.

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.

3 Dommages causés par l'attaque

Le présent chapitre porte sur les dommages causés par l'attaque. Etant donné que les informations relatives à l'ampleur exacte de ces dommages et les détails de l'attaque sont extrêmement sensibles, la CdG-N se prononce à ce sujet en s'en tenant à une forme générale. La sous-commission compétente a toutefois eu accès aux informations pertinentes: elle a donc disposé d'une base d'information suffisante pour la description et l'appréciation des éléments ci-après.

3.1 Rappel des faits

Le 20 juillet 2016, après que l'attaque contre RUAG eut été rendue publique, la DélSéc a chargé le Groupe Sécurité de déterminer l'ampleur des dommages et de montrer les points sur lesquels il était difficile, voire impossible de tirer des conclusions définitives.

Dans son rapport du 25 août 2016, le Groupe Sécurité souligne que rien n'indique que le logiciel malveillant ait touché ou touche encore les systèmes de l'administration fédérale et que les auteurs de l'attaque aient ainsi eu accès à des données de la Confédération, notamment du DDPS. Il estime toutefois que les fuites de données de RUAG étaient très importantes. Pour plusieurs raisons, le Groupe Sécurité n'a pas pu évaluer précisément les dommages, notamment parce que RUAG refusait de fournir au DDPS toutes les informations demandées[30] (cf. ch. 2.1.1.2). RUAG a alors été invitée à livrer des informations complémentaires.

30 Selon l'avis de RUAG, cette dernière ne pouvait au début pas fournir au DDPS toutes les informations souhaitées car il fallait d'abord définir un processus permettant à RUAG de donner également accès au DDPS à des documents pour lesquels elle avait elle-même signé des déclarations de confidentialité avec des tiers (déclarations de confidentialité avec des collaborateurs du DDPS et aménagement de sa propre salle protégée dans laquelle tous les documents sensibles pouvaient être consultés).

Après avoir repris les investigations ultérieures de la DélCdG concernant l'attaque, la CdG-N a analysé le rapport du Groupe Sécurité du 25 août 2016. Par la suite, elle a demandé au DDPS de lui présenter un nouveau rapport concernant les dommages fondé sur les informations complémentaires que RUAG avait été invitée à fournir. Le DDPS a satisfait à la demande de la commission avec un certain retard: le 28 juin 2017, il a présenté à la sous-commission le rapport concerné[31]. Celui-ci contient des données plus détaillées relatives aux listes concernées par le vol, une analyse plus précise des éventuels conséquences ou risques ainsi que les mesures de protection qui ont été prises. Toutefois, il ressort surtout de ce rapport qu'il est impossible de déterminer définitivement l'ampleur du vol, pour différentes raisons, et que les estimations des experts et de RUAG concernant les dommages causés varient considérablement. Alors que RUAG met essentiellement l'accent sur l'aspect quantitatif en fondant son avis sur le volume des données volées, le DDPS estime quant à lui que l'importance des données est décisive, et non le volume en soi.

Le chef du DDPS a indiqué au groupe de travail que la Confédération et RUAG avaient évalué différemment le risque et que RUAG avait clairement sous-estimé les risques dans la phase qui a immédiatement suivi l'attaque[32]. Toutefois, il a précisé que, depuis, la collaboration fonctionnait bien et que RUAG avait pris plusieurs mesures d'amélioration.

Dans le cadre de ses investigations, la sous-commission compétente s'est renseignée à plusieurs reprises sur l'ampleur des dommages (financiers) ainsi que sur les réactions des clients et les éventuelles conséquences sur les coopérations ou sur les mandats. Vu que le DDPS n'était pas lui-même en possession de ces informations, il a transmis les questions de la sous-commission à RUAG. Il a ensuite transmis la réponse de RUAG à la sous-commission sans l'avoir lui-même analysée. Dans la lettre qu'elle a envoyée à la secrétaire générale du DDPS le 15 janvier 2018, RUAG explique que les conséquences financières de l'attaque se limitent aux coûts engendrés par la gestion de l'affaire (mise en œuvre de mesures, dispositif pour répondre aux questions des clients) ainsi que par le lancement du programme IMPACT[33]. A l'exception de ces coûts, RUAG indique qu'elle n'a subi aucun dommage direct et qu'elle n'a notamment perdu aucun client directement après l'attaque.

3.2 Appréciation

Dans le cadre des investigations, la CdG-N (par l'intermédiaire de la sous-commission compétente) a reçu des informations détaillées concernant les listes de données touchées par l'attaque et les risques qui en ont découlé. Sur cette base, elle est arrivée à la conclusion que l'attaque menée contre RUAG devait être considérée comme

31 Il s'agit d'un rapport établi exclusivement à l'intention de la sous-commission. La CdG-N ne sait pas dans quelle mesure le Conseil fédéral ou la DélSéc ont été informés de la nouvelle appréciation des dommages.

32 Audition du chef du DDPS du 28.4.2017.

33 Les coûts du programme IMPACT, qui doit être progressivement mis en œuvre d'ici 2019, se montent au total à 10 millions de francs, auxquels s'ajoutent des coûts annuels de 1 million de francs environ en raison de l'augmentation du personnel dans les domaines de l'organisation et de la sécurité de l'informatique.

un événement grave. De plus, elle estime clairement qu'il faut mesurer l'importance des données volées non seulement sous l'angle quantitatif, mais également du point de vue qualitatif, partageant ainsi l'avis du DDPS.

La CdG-N prend acte des informations fournies par RUAG selon lesquelles l'entreprise n'a jusqu'à présent subi aucun dommage direct en raison de l'attaque et n'a constaté aucun départ immédiat de clients. La commission estime toutefois qu'un tel incident n'est certainement pas positif pour les affaires de l'entreprise, raison qui justifie à elle seule d'accorder une grande importance à l'attaque.

Dans ce contexte, elle ne comprend pas pourquoi RUAG, une fois que l'attaque a été découverte, n'a mis en avant que les aspects quantitatifs du vol et s'est montrée peu coopérative en refusant de fournir au DDPS toutes les informations qu'il avait demandées (cf. ch. 4). La CdG-N salue la décision du DDPS d'insister auprès de l'entreprise; les investigations ont ainsi pu déboucher sur une analyse claire et satisfaisante des dommages et différentes dispositions ont pu être prises afin d'éliminer les dommages ou réduire les risques (cf. ch. 2).

4 Pilotage stratégique et défense des intérêts du propriétaire

4.1 Rappel des faits

4.1.1 RUAG: informations de base sur l'entreprise et la manière dont elle est pilotée

Bases juridiques et principales caractéristiques de RUAG

RUAG (RUAG Holding SA) est un groupe d'armement né de l'externalisation des anciennes entreprises d'armement de la Confédération, devenues autonomes. RUAG est une société anonyme de droit privé, dont l'actionnaire unique est la Confédération suisse.

En 2016, RUAG comptait plus de 8500 collaborateurs, répartis sur près de 80 sites. Environ la moitié des emplacements et des emplois se trouvent en Suisse (près de 4500 employés sur 39 sites). Bien implantée en Europe (26 sites), RUAG est aussi présente aux États-Unis (7 sites), en Australie (5 sites) et en Asie (2 sites). En 2016, son chiffre d'affaires net était de 1858 millions de francs et son bénéfice net de 116 millions de francs, dont 47 millions de francs ont été versés sous forme de dividende à la Confédération, en sa qualité de propriétaire.

La base légale des rapports entre RUAG et la Confédération a été établie avec la loi fédérale sur les entreprises d'armement de la Confédération.[34] Dans la disposition définissant le but de la loi, il est en effet prévu que la Confédération peut exploiter des entreprises d'armement «pour garantir l'équipement de l'armée».[35] Le cadre juridique de l'entreprise est établi dans les statuts de RUAG (but, capital social,

34 Loi fédérale du 10.10.1997 sur les entreprises d'armement de la Confédération (LEAC), RS **934.21**.

35 Art. 1 de la loi fédérale sur les entreprises d'armement de la Confédération (LEAC), RS **934.21**.

organes, leurs droits et obligations, etc.). Le Conseil fédéral pilote l'entreprise selon les principes formulés dans son rapport sur le gouvernement d'entreprise de 2006[36] et en fixant à RUAG des objectifs stratégiques:

Rapport sur le gouvernement d'entreprise

Avec le rapport sur le gouvernement d'entreprise[37] et les documents explicatifs qui le complètent[38], le Conseil fédéral a voulu créer une base solide lui permettant d'externaliser des activités et de piloter ensuite les entités devenues autonomes en fonction de principes consistants. Il y a formulé des principes directeurs pour chacun des principaux éléments de gestion; ils se rapportent notamment à la présence de représentants de la Confédération dans les conseils d'administration, au contrôle par le Conseil fédéral ou encore aux objectifs stratégiques.[39] Les éléments essentiels de ces principes directeurs sont les suivants:

– *Organes:* les organes des entités devenues autonomes doivent disposer des connaissances nécessaires sur le plan technique et sur le plan de l'exploitation pour exercer leur fonction conformément à leurs responsabilités. Le Conseil fédéral doit cependant aussi veiller à ce que la défense des intérêts de la Confédération au sein du conseil d'institut ou du conseil d'administration soit assurée. Dans l'exercice de son droit de nomination, il doit dès lors veiller à ce que les personnes élues s'identifient aux objectifs stratégiques du Conseil fédéral et défendent donc les intérêts de la Confédération au sein du conseil d'administration ou d'institut.

– *Représentants de la Confédération au conseil d'administration:* le Conseil fédéral doit limiter la présence au conseil d'administration de personnes recevant ses instructions aux cas dans lesquels une telle représentation s'impose (par ex. lorsque les intérêts de la Confédération ne seraient pas défendus de manière suffisante sans cette représentation). Dans le rapport explicatif de l'Administration fédérale des finances, il est précisé que la nomination de représentants de la Confédération au conseil d'administration pouvait se justifier avant tout dans le cas des entités transformées en sociétés anonymes de droit privé qui proposent leurs prestations sur le marché (car les objectifs stratégiques ne sont pas juridiquement contraignants pour elles, cf. infra).

– *Contrôle du Conseil fédéral:* le contrôle du Conseil fédéral en sa qualité de propriétaire est le corollaire des fonctions de pilotage qu'il exerce et sert donc en principe les mêmes objectifs: il vise d'une part à préserver, voire à augmenter la performance et la valeur intrinsèque des entités devenues indépendantes (contrôle axé sur l'entreprise) et d'autre part à garantir une exécution des tâches visant le bien commun (contrôle axé sur les tâches). Dans

36 Rapport du Conseil fédéral sur l'externalisation et la gestion des tâches de la Confédération (Rapport sur le gouvernement d'entreprise) du 13 septembre 2006, FF **2006** 7799.
37 Cf. note de bas de page 33.
38 Rapport explicatif de l'Administration fédérale des finances concernant le rapport du Conseil fédéral sur le gouvernement d'entreprise; Rapport du Conseil fédéral du 25 mars 2009 complétant le rapport sur le gouvernement d'entreprise (FF **2009** 2299).
39 Les autres éléments de gestion sont: forme juridique, organes, responsabilités, compétences particulières, haute surveillance du Parlement, finances et impôts.

le cas des sociétés anonymes de droit privé, les instruments de contrôle des actionnaires – et donc de la Confédération – sont régis par le droit des sociétés anonymes.

– *Objectifs stratégiques:* sur le plan stratégique, le Conseil fédéral pilote les entités devenues autonomes en leur fixant des objectifs supérieurs à moyen terme. Il peut formuler des directives relatives à l'entreprise ou des directives relatives aux tâches. Dans le cas de RUAG, l'accent est clairement mis sur les directives relatives à l'entreprise, puisque l'accomplissement des tâches dépend essentiellement du marché, qui est censé guider les choix de l'entreprise. Si les objectifs stratégiques ne sont pas juridiquement contraignants pour le conseil d'administration d'une entité devenue autonome sous la forme d'une société anonyme de droit privé (comme RUAG), ils déploient malgré tout un effet contraignant, car le conseil d'administration ne peut pas se permettre d'aller à l'encontre des instructions données par l'actionnaire majoritaire s'il veut rester en place.[40]

  Le Conseil fédéral doit contrôler annuellement si les objectifs ont été atteints. Ce contrôle est fondé essentiellement sur le rapport de l'entreprise relatif à la réalisation des objectifs. Ce rapport est examiné par les départements compétents, qui en discutent avec l'entreprise avant d'en référer au Conseil fédéral, qui rédige ensuite son propre rapport (rapport du Conseil fédéral sur la réalisation des objectifs stratégiques) à l'intention des commissions de surveillance du Parlement.

Entretiens avec le propriétaire

Les entretiens périodiques entre la Confédération et les entités devenues autonomes sont un instrument important du pilotage stratégique. En règle générale, ces entretiens ont lieu environ quatre fois par année. La Confédération y est représentée par le département compétent – normalement le chef du département, le secrétaire général ainsi que différents spécialistes – et, le plus souvent, par une délégation de l'Administration fédérale des finances. L'entreprise, pour sa part, y est représentée par le président du conseil d'administration ainsi que par le CEO, assistés, le cas échéant, d'autres membres de la direction de l'entreprise. Lors de ces entretiens, l'entreprise rend compte de la marche des affaires, des défis majeurs qui se présentent ou encore de décisions stratégiques importantes, par exemple de coopération avec d'autres entreprises ou du rachat d'entreprises. Les représentants de la Confédération évaluent ces informations à la lumière des objectifs fixés à l'entreprise et abordent plus particulièrement les problèmes ou événements susceptibles de faire obstacle à la réalisation de ces objectifs. C'est au chef du département responsable qu'il revient d'assurer la défense des intérêts du propriétaire.

40 Rapport du Conseil fédéral complétant le rapport sur le gouvernement d'entreprise du 25.3.2009 (FF **2009** 2321).

4.1.2 Objectifs stratégiques assignés à RUAG

Selon les objectifs stratégiques actuels[41], RUAG «permet en premier lieu de garantir l'équipement de l'armée» et ses objectifs sont «axés avant tout sur les intérêts de la Confédération en tant qu'actionnaire» tout en tenant «aussi raisonnablement compte des intérêts de la Confédération en tant que cliente importante de RUAG». Outre les priorités stratégiques relatives à la garantie de l'équipement de l'armée, le Conseil fédéral définit aussi des objectifs financiers – notamment le versement d'un dividende qui ne soit pas inférieur à 40 % du bénéfice net[42] – ainsi que des objectifs en matière de participations, de politique du personnel et de politique régionale.

4.1.3 Pilotage de RUAG dans le cadre de la cyberattaque/ défense des intérêts du propriétaire

Le Conseil fédéral et le DDPS ont réagi à la cyberattaque contre RUAG non seulement en créant des structures spéciales en vue de la gestion des conséquences de l'incident au sein de l'administration fédérale (notamment la «task force» RHINO), mais aussi en ordonnant que soient prises différentes mesures (cf. ch. 2).

Dans le présent chapitre, il s'agit maintenant de démontrer comment l'incident a été perçu dans la perspective du pilotage stratégique ou plutôt du contrôle de l'entreprise par le DDPS (en qualité de représentant du Conseil fédéral) et, en corollaire, comment le DDPS veille de manière générale à la défense des intérêts de la Confédération en tant que propriétaire.

4.1.3.1 Pilotage dans le cadre des entretiens avec le propriétaire

Les procès-verbaux des entretiens avec le propriétaire[43] qui ont suivi l'incident[44] ne contiennent que peu d'informations sur la cyberattaque ou n'en contiennent même pas du tout. Si l'incident a figuré à l'ordre du jour à trois reprises, il n'y a pas trace des discussions conduites à ce sujet dans les procès-verbaux.[45]

Il ressort des trois autres PV, notamment de celui qui porte sur le premier entretien qui a suivi la nouvelle de l'attaque, que l'incident ne figurait pas à l'ordre du jour et qu'il n'a pas été discuté (ou que la discussion n'a pas été consignée au procès-verbal).

41 Objectifs stratégiques du Conseil fédéral assignés à RUAG Holding SA pour la période 2016 à 2019.
42 Jusqu'en 2015, cette part n'était que de 20 % du bénéfice net.
43 Les entretiens avec le propriétaire ont duré environ deux heures.
44 La sous-commission de la CdG compétente a obtenu et analysé les procès-verbaux des entretiens avec le propriétaire qui ont eu lieu en 2016 et au début de 2017 (2016: 4 PV des 9.3., 27.6., 20.9. et 13.12.; 2017: 2 PV des 8.3. et 4.7.).
45 Dans l'un des cas, l'absence de PV est justifiée par le fait que cela avait été souhaité par le CEO de RUAG. Dans le cas des deux autres PV, l'absence de compte rendu n'a pas été motivée.

Incident à l'ordre du jour et discussion rapportée dans le PV	–
Incident à l'ordre du jour, mais discussion non rapportée dans le PV	*27.6.2016; 8.3.2017; 4.7.2017*
Incident ne figure pas à l'ordre du jour et n'a pas été discuté selon PV	*9.3.2016; 20.9.2016; 13.12.2016*

Si l'on en croit les procès-verbaux, les conséquences de la cyberattaque n'ont jamais été discutées de manière approfondie dans le cadre des entretiens avec le propriétaire. Il n'y a par exemple jamais été question des réactions des clients de RUAG au piratage, malgré le fait que RUAG avait été chargée par le DDPS d'informer ses clients et malgré le fait que cet incident a pu avoir des retombées sur la confiance des clients dans l'entreprise et donc sur ses résultats financiers (et, en conséquence, sur le montant des dividendes versés à la Confédération). Selon les témoignages du chef du DDPS, le département n'a pas considéré ces informations comme étant pertinentes de son point de vue ou du point de vue du propriétaire. Dans ses entretiens avec la sous-commission, le chef du DDPS a affirmé que l'on ne s'était pas renseigné de manière détaillée pour connaître les réactions des clients, mais que RUAG n'avait pas, à sa connaissance, perdu de clients et que la Confédération n'avait pas non plus reçu de plaintes de clients en sa qualité de propriétaire.[46] Le DDPS a demandé à RUAG de fournir des compléments d'information à la sous-commission compétente.[47]

D'une manière générale, les procès-verbaux ne contiennent que peu d'éléments indiquant que le DDPS profite de ces entretiens pour discuter des problèmes à résoudre ou des défis à relever ou encore pour adresser des exigences à l'entreprise. Normalement, les procès-verbaux commencent par des informations relativement détaillées sur la situation économique de RUAG. Cette première partie est suivie de sujets spécifiques, qui ne sont souvent résumés que brièvement. Un des procès-verbaux a fait ressortir certaines divergences ou du moins un manque de coordination entre le DDPS et l'AFF: le représentant de l'AFF y fait part de son étonnement au sujet de certaines déclarations du chef du DDPS relatives au développement de RUAG en affirmant avoir obtenu «des informations différentes à ce propos».[48]

En complément des procès-verbaux des entretiens avec le propriétaire, le DDPS tient des listes des affaires en cours se rapportant à ces entretiens. Encore une fois, l'étude de ces listes[49] n'a pas permis de trouver des indices d'exigences ou de mandats concrets qui auraient été adressés à l'entreprise par le DDPS en rapport avec la cyberattaque ou avec d'autres problèmes susceptibles de remettre en cause la réalisation des objectifs stratégiques. L'élément frappant qui est ressorti de ces listes est la présence permanente, dès juillet 2017, d'une instruction demandant à RUAG d'avertir rapidement le chef du DDPS de la publication d'articles de presse ayant des implications politiques ou de projets de RUAG sensibles sur le plan de la politique

46 Audition du chef du DDPS du 26.11.2017.
47 Cf. ch. 3.
48 Procès-verbal du 13.12.2016, point 4.
49 La sous-commission compétente n'a pu obtenir que les listes des affaires en cours de 2017 (listes au 28.2., au 8.3. et au 4.7.2017).

régionale (avant cette date, l'instruction ne portait que sur les décisions ayant des implications de politique régionale).

Si les procès-verbaux et les listes des affaires en cours ne contiennent pratiquement pas trace de mandats explicitement adressés à RUAG par le DDPS, d'autres documents analysés indiquent pourtant que de tels mandats existent bel et bien. Ainsi, dans une lettre de RUAG au DDPS, l'entreprise précisait, un mois à peu près après l'entretien avec le propriétaire, qu'elle jugeait un projet de rachat d'entreprise conforme aux objectifs stratégiques en se référant à une discussion qui avait eu lieu à l'occasion du dernier entretien avec le propriétaire. Dans le procès-verbal correspondant, ce rachat par RUAG est bien mentionné dans le contexte des informations sur la marche des affaires, mais on n'y trouve pas trace de questions ou de mandats du DDPS à ce sujet.

S'agissant des entretiens avec le propriétaire, le chef du DDPS a précisé que les discussions qui avaient lieu dans ce cadre portaient essentiellement sur des sujets d'ordre général et financier. Selon lui, les questions de sécurité, et plus particulièrement les capacités de RUAG dans le cyberespace, n'y sont pas discutées, avant tout pour éviter des indiscrétions, car ces entretiens – a-t-il expliqué – ont tout de même lieu en présence d'une douzaine de participants. D'après le chef du DDPS, les entretiens avec le propriétaire servent essentiellement à la transmission d'informations relatives, d'une part, à la marche des affaires dans les différents secteurs d'activité et, d'autre part, aux défis qui se présentent dans la perspective des objectifs stratégiques. Selon lui, l'AFF, qui prend également part à ces séances, s'intéresse avant tout à l'opportunité de l'acquisition de telle ou telle prestation.[50] Il a affirmé que la cyberattaque et le sujet de la cybersécurité avaient été traités dans d'autres cadres, notamment au sein du Groupe Sécurité de la Confédération, de la Délégation pour la sécurité ainsi que de la DélCdG.[51] Les documents analysés ne contiennent aucune trace de retours formels à l'attention du chef du département. Les représentants du DDPS auditionnés ainsi que le chef du département lui-même ont affirmé que la cyberattaque et le sujet de la cybersécurité avaient été discutés à plusieurs reprises à l'occasion d'entretiens bilatéraux entre le chef du DDPS et des représentants de RUAG (cf. infra).

En conclusion, on constate donc que la cyberattaque dirigée contre RUAG ainsi que les mesures prises ensuite n'ont pas été discutées dans le cadre formel des entretiens avec le propriétaire ou qu'elles y ont tout au plus été abordées de manière superficielle (pour ce qui est du traitement du sujet à l'occasion d'autres contacts entre le chef du DDPS et des représentants de RUAG, cf. ch. 4.1.3.2).

50 Audition du chef du DDPS du 16.11.2017.
51 Cf. Note de bas de page 44.

4.1.3.2 Pilotage dans le cadre des entretiens bilatéraux entre le chef du DDPS et la direction de RUAG

Habituellement, les entretiens avec le propriétaire sont suivis d'un entretien bilatéral entre le chef du DDPS et le président du conseil d'administration de RUAG. Il n'y a pas de procès-verbal de ces discussions et celles-ci n'ont d'ailleurs pas lieu à chaque fois. Il n'y a ainsi pas eu d'entretien bilatéral au terme de la première séance qui a suivi l'annonce de la cyberattaque. Le DDPS a fourni à la sous-commission un aperçu des entretiens bilatéraux ayant eu lieu entre le chef du DDPS et le président du conseil d'administration ou le CEO de RUAG, avec indication sommaire des sujets discutés. Il ressort de cet aperçu que le chef du DDPS s'est entretenu à trois reprises avec les dirigeants de RUAG dans les semaines qui ont suivi la découverte du piratage, en janvier et février 2016, et qu'il a souligné la gravité de l'incident à ces occasions. Dans le cadre de deux autres de ces entretiens, en août 2016 et en mars 2017, la discussion a porté sur les conséquences de ces attaques ainsi que sur les dommages causés. Lors des auditions, le chef du DDPS et les autres représentants du département ont certifié d'une manière générale que la cyberattaque avait bel et bien été discutée dans le cadre d'entretiens bilatéraux entre le chef du DDPS et les représentants de RUAG. Comme ces discussions n'ont pas été documentées plus en détail, la sous-commission n'a pas été en mesure de vérifier ces informations.

Le chef du DDPS a précisé qu'il renonçait sciemment à conserver des traces de ces entretiens bilatéraux sous la forme de procès-verbaux ou de notes personnelles. Il souhaite en effet éviter – dit-il – que les sujets parfois très sensibles discutés à ces occasions puissent un jour être rendus publics par un journaliste qui pourrait y avoir accès en vertu de la loi sur la transparence (LTrans). Selon le chef du DDPS, l'expérience aurait en effet montré que l'administration n'avait aucun moyen de se défendre contre ce type de requête étant donné que les tribunaux tranchaient systématiquement en faveur de la publication.

Si nécessaire, le chef du DDPS a aussi affirmé pouvoir prendre contact directement avec le président du conseil d'administration de RUAG à n'importe quel moment, en dehors des entretiens avec le propriétaire et des entretiens bilatéraux prévus périodiquement. Il a déclaré que ces contacts directs avaient toujours très bien fonctionné, même s'il lui était arrivé d'avoir «des discussions animées» avec le président du conseil d'administration de RUAG.[52]

Depuis que RUAG a créé un poste de chargé des relations avec le propriétaire[53] (remarque: cette fonction existe depuis le 1er septembre 2017), la collaboration s'est nettement améliorée et les réponses aux requêtes sont données dans les délais.

Le fait que la communication avec RUAG n'a pas toujours été facile, en raison des circonstances (cf. ch. 2.1.1.2), notamment lorsqu'il s'est agi d'obtenir des informations sur la cyberattaque, a été confirmé tant par les autres personnes entendues que par les documents étudiés. Il ressort en effet des documents analysés que le DDPS

52 Audition du chef du DDPS du 26.11.2017.

53 Pour occuper cette nouvelle fonction de «vice-président Relations avec le propriétaire», le conseil d'administration de RUAG a désigné Alexandre Schmidt, ancien directeur de la Régie fédérale des alcools et ancien membre du Conseil municipal (Exécutif) de la Ville de Berne.

n'a pas obtenu certains renseignements ou qu'il a dû insister lourdement pour les obtenir (cf. ch. 3 relatif aux dommages) ou encore que les renseignements demandés n'avaient pas été fournis dans les délais ou étaient incomplets (cf. ch. 2). Lors des auditions, les représentants du DDPS[54] ont souligné à plusieurs reprises que le chef du département avait dû batailler sans relâche pour obtenir suffisamment d'informations et que ce point devait être amélioré dans les relations avec RUAG. Selon eux, il est actuellement très important pour le DDPS d'obtenir du conseil d'administration des informations plus précises sur la marche des affaires afin de permettre à la Confédération d'assumer son rôle d'actionnaire en toute connaissance de cause. En conséquence, les exigences auxquelles RUAG doit satisfaire en matière de reddition de compte au DDPS ont – affirment-ils – été accrues au cours des derniers dix-huit mois.

4.1.3.3 Pilotage par le biais de la composition du conseil d'administration

Comme cela a été rappelé au ch. 4.1.1, la Confédération doit, par principe, renoncer à se faire représenter directement au conseil d'administration. Il peut néanmoins être justifié de faire entrer au conseil d'administration une personne suivant les instructions de la Confédération si les intérêts de celle-ci risquaient de ne pas être suffisamment défendus sans cette représentation.

Étant donné que la collaboration entre la Confédération et RUAG était plutôt tendue à la suite de la cyberattaque et comme le DDPS a dû intervenir de manière répétée auprès de l'entreprise pour obtenir les informations qu'il jugeait nécessaires, la CdG-N estime légitime de se demander si cette situation n'était pas suffisante à elle seule pour justifier une représentation répondant aux instructions afin de garantir une meilleure prise en compte des intérêts de la Confédération. La commission est d'avis que les tensions suscitées par le piratage ne sont pas le seul motif pouvant justifier la nomination d'un représentant direct au conseil d'administration, puisqu'il y a encore les travaux de désenchevêtrement très complexes en cours entre la Confédération et RUAG ou l'exploration de possibilités concernant la structure organisationnelle et la forme juridique que devra prendre RUAG et concernant une privatisation partielle de l'entreprise.

Interrogé à ce propos, le chef du DDPS a indiqué que le Conseil fédéral n'avait pas étudié cette question de manière approfondie jusqu'ici et a attiré l'attention sur les questions de responsabilité.[55] La secrétaire générale du DDPS a relevé que la question de la présence d'un représentant de la Confédération au conseil d'administration avait été discutée au moment de la création de l'entreprise et qu'elle sera probablement de nouveau à l'ordre du jour lorsqu'il sera question de l'avenir de RUAG.[56]

54 Audition de la secrétaire générale du DDPS, du délégué DDPS pour la cyberdéfense et du chef de la gestion des participations du DDPS du 3.7.2017; audition de la secrétaire générale du DDPS et du délégué DDPS pour la cyberdéfense du 10.10.2016.
55 Audition du chef du DDPS du 16.11.2017.
56 Audition de la secrétaire générale du DDPS du 3.7.2017.

4.1.3.4 Autres constatations relatives au pilotage et à la défense des intérêts du propriétaire

Pour la CdG-N, les auditions et l'analyse documentaire ont fait surgir encore d'autres questions et constatations relatives à la défense des intérêts de la Confédération en sa qualité de propriétaire par le DDPS:

- *Contrôle de la mise en œuvre des objectifs stratégiques:* comme les représentants de RUAG l'ont eux-mêmes déclaré – cela vient d'être relevé plus haut – le DDPS a renforcé les exigences auxquelles le conseil d'administration de RUAG doit satisfaire en matière d'obligation de rendre compte. Dorénavant, celui-ci doit en effet démontrer pour chacune des cibles et chacun des objectifs qui ont été fixés comment la mise en œuvre a été réalisée durant la période sous rapport et justifier toutes les différences par rapport à la période précédente. Dans ce contexte, il convient de relever que le DDPS a, en automne 2017, demandé à RUAG de détailler les conséquences que les réorganisations dans le domaine de la cybersécurité allaient avoir sur la réalisation des objectifs stratégiques fixés par le Conseil fédéral. Dans le courrier que le Conseil fédéral a rédigé à ce propos, il s'est aussi plaint que le chef du DDPS avait, un jour seulement après une séance entre la secrétaire générale du DDPS et le CEO de RUAG, appris par les médias que l'entreprise allait supprimer des emplois, entre autres dans le domaine de la cybersécurité. RUAG a répondu aux questions du DDPS dans les délais impartis. La sous-commission n'a plus été en mesure de déterminer dans le cadre du présent bilan intermédiaire comment cette réponse avait été reçue par le DDPS et quelles questions ou conséquences avaient pu en résulter.
- *Contrôle de la mise en œuvre des mesures internes prises par RUAG en réaction à la cyberattaque:* le DDPS – ce fait a déjà été mis en évidence au ch. 2.1.1.3 – a attendu plus d'une année avant de demander à RUAG de rendre compte des mesures prises en interne à la suite du piratage et il a dû patienter jusqu'en novembre 2017 pour obtenir un rapport qu'il jugeait d'une qualité et d'un niveau de détail suffisants.
- *Évaluation par le DDPS des mesures internes prises par RUAG:* dans une note d'information au Conseil fédéral[57], le DDPS relève que les mesures en tant que telles sont certes «correctes» à son sens, mais qu'une amélioration de la cybersécurité ne pourra être obtenue qu'au moyen d'un développement continuel de ces mesures prises en interne et au prix de changements dans la culture d'entreprise. L'analyse documentaire et les auditions n'ont toutefois pas permis de conclure que cette évaluation de la situation avait eu des conséquences ou que le DDPS serait intervenu auprès de RUAG à ce sujet pour demander, par exemple, une augmentation des moyens mis en œuvre.
- *Départs au conseil d'administration et à la direction de RUAG:* le fait que différents sujets jugés importants par la CdG-N ne sont pas discutés dans le cadre des entretiens avec le propriétaire est confirmé par l'exemple des départs enregistrés à la tête de l'entreprise. L'année dernière, RUAG a an-

57 Note d'information du DDPS au Conseil fédéral du 10.4.2017.

noncé que le président de son conseil d'administration ne briguerait pas un nouveau mandat. En 2016, l'entreprise avait déjà connu une démission au sein de son conseil d'administration et trois des huit directeurs de RUAG avaient dû être remplacés. Il ressort des procès-verbaux des entretiens avec le propriétaire que ces mutations y ont à peine été abordées, malgré le fait qu'elles représentent un certain risque dans l'optique du propriétaire (notamment une perte de savoir-faire). Le chef du DDPS a indiqué qu'il n'avait pas cherché à exercer une quelconque influence sur ces départs, mais qu'il avait toujours été tenu au courant des motifs. Les administrateurs sortants ont tous deux expliqué leur décision par un certain mécontentement («ingérence» croissante des milieux politiques, plafonnement des salaires). Selon le chef du DDPS, il a fallu créer une commission chargée de repourvoir ces postes, car les profils recherchés ne sont apparemment pas faciles à trouver, du moins en Suisse.[58]

4.2 Appréciation

Sur la base de ces constatations, la CdG-N constate en résumé qu'il ne lui est pas possible de déterminer avec certitude dans quelle mesure le DDPS a su gérer la situation à la suite de la cyberattaque subie par RUAG dans le cadre des moyens de pilotage stratégique de l'entreprise. Dans le contexte formel des entretiens avec le propriétaire, l'incident a en effet tout au plus été abordé de manière superficielle. Et si le DDPS affirme que le sujet a bel et bien été discuté dans le cadre de contacts bilatéraux informels qui ont eu lieu entre le chef du département et des représentants de RUAG, il n'existe ni procès-verbal ni note écrite qui puisse le confirmer.

Au vu de ce constat et des éléments mis en perspective plus haut, la CdG-N se pose différentes questions de principe et ne peut s'empêcher de se demander si les intérêts de la Confédération en sa qualité de propriétaire de RUAG sont défendus de manière adéquate par le DDPS et si celui-ci a bien la capacité de s'imposer face à l'entreprise. La commission estime en effet que le DDPS peine à défendre les intérêts du propriétaire, cela malgré le fait que RUAG soit à 100 % aux mains de la Confédération.

Cette situation s'explique sans doute au moins partiellement par l'attitude parfois peu coopérative de RUAG, qui ne cesse d'invoquer son indépendance. Cette indépendance n'est pas contestée, mais n'autorise pas l'entreprise – de l'avis de la CdG-N – à faire passer ses propres intérêts économiques avant les requêtes et la volonté de son propriétaire. Contrairement à l'indépendance d'autorités de réglementation ou de surveillance, l'indépendance de RUAG ne doit pas tant être comprise comme un «rempart contre les influences politiques», mais comme un privilège limité aux activités commerciales opérationnelles. Or, la gestion de l'impact de la cyberattaque de janvier 2016 a certes des conséquences sur les affaires courantes de l'entreprise, mais elle pose avant tout des questions d'ordre stratégique et appelle donc clairement l'intervention de la Confédération en sa qualité de propriétaire. La

58 Audition du chef du DDPS du 16.11.2017.

Confédération doit en effet garantir qu'elle est en mesure de réagir à une situation extraordinaire telle que la cyberattaque lancée contre RUAG, qui a mis en péril non seulement la valeur de l'entreprise, mais aussi la sécurité de la Suisse, en opérant des choix stratégiques par l'intermédiaire du conseil d'administration. Il va de soi que ces choix peuvent, en définitive, avoir des retombées sur le plan opérationnel.

Il est donc évident que la Confédération, et notamment le DDPS, a sa part de responsabilité dans ce que la commission considère être des défaillances dans la défense des intérêts du propriétaire. Ainsi que cela a été démontré plus haut, les procès-verbaux des entretiens avec le propriétaire ne laissent en effet transparaître aucune réelle volonté d'assurer le pilotage (stratégique) de RUAG et de préserver les intérêts du propriétaire. A ce propos, la CdG-N déplore le choix de canaux manifestement très informels utilisés pour influer sur les décisions et la situation et critique le fait que ces contacts bilatéraux ne fassent pas l'objet d'un procès-verbal. Si elle estime que cette pratique est déjà douteuse en temps normal, elle la juge carrément inadaptée dans une situation de crise comme celle qui a suivi la cyberattaque. En renonçant à garder une trace écrite des discussions et décisions importantes, le DDPS fait aussi une croix non seulement sur une base d'information solide, mais aussi sur un instrument de pilotage lui permettant d'imposer des exigences stratégiques à plus long terme.

Contrairement à l'avis du chef du DDPS, la CdG-N est résolument persuadée que les entretiens avec le propriétaire ne doivent pas servir seulement à l'échange d'informations sur la marche des affaires, mais aussi à discuter les problèmes essentiels et à formuler des exigences, notamment lorsque les problèmes en question peuvent avoir des répercussions sur les résultats financiers. Si ces discussions ne peuvent pas avoir lieu par crainte d'indiscrétions, notamment, il importe d'en revoir les modalités ou le cercle des participants au lieu de s'accommoder de canaux informels non documentés. La commission n'a en outre pas été convaincue par l'argumentation du chef du DDPS lorsqu'il affirme qu'il renonce à conserver des procès-verbaux ou des notes de discussion par crainte de requêtes fondées sur la LTrans.

En fin de compte, le DDPS se trouvera simplement ne pas être en possession d'informations qui auraient été importantes dans la perspective du propriétaire. Dans ce même ordre d'idées, la CdG-N ne comprend par exemple pas que le DDPS n'ait apparemment jamais cherché à savoir comment les clients de RUAG avaient réagi lorsqu'ils ont été informés de l'incident. Contrairement à la commission, le DDPS a manifestement considéré que ces informations n'étaient pas pertinentes. Elles auraient pourtant pu fournir des indices très utiles pour l'évaluation du degré de fidélité de la clientèle et donc pour l'évolution future du carnet de commandes de RUAG. Comme ce dernier élément est déterminant de la marche des affaires, les informations en question étaient sans conteste importantes pour le propriétaire. D'autant plus qu'elles pouvaient avoir des répercussions sur la réalisation des objectifs de l'entreprise et donc sur les dividendes de la Confédération.

Au vu des différents défis qui doivent être relevés en rapport avec RUAG – conséquences de la cyberattaque, désenchevêtrement des réseaux de la Confédération et de RUAG, évaluation des possibilités concernant la structure organisationnelle et la forme juridique de RUAG et concernant une privatisation partielle – la commission ne comprend pas non plus que le DDPS et le Conseil fédéral n'aient jamais envisagé

d'occuper ne serait-ce que passagèrement un siège au conseil d'administration de RUAG. Dans le rapport sur le gouvernement d'entreprise, la désignation d'un représentant suivant ses instructions est en effet prévue expressément dans l'éventualité où la Confédération ne parviendrait pas à défendre ses intérêts de manière suffisante.

En conclusion, la CdG-N estime que, si les instruments nécessaires à la défense des intérêts du propriétaire face à RUAG existent, ils ne sont pas utilisés de manière judicieuse, notamment par le DDPS.

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 oeuvre 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.

La CdG-N espère que la nomination du nouveau président du conseil d'administration de RUAG permettra de construire les bases d'une collaboration optimale entre le propriétaire et le conseil d'administration.

5 Conclusions

Les informations qu'elle a réunies permettent à la CdG-N de conclure dans l'ensemble que la Confédération a réagi à la découverte de la cyberattaque avec la diligence requise et en prenant les mesures qui s'imposaient. Le Conseil fédéral, comme le DDPS, ont géré l'incident avec rapidité et pertinence. Les dirigeants de RUAG, par contre, ont mis plus de temps à reconnaître l'envergure du piratage ainsi que les risques qui en ont résulté et à prendre leurs propres mesures. La CdG-N salue donc le fait que le DDPS ait fait pression sur RUAG et soit intervenu à différentes reprises en réaction à l'attitude initialement peu coopérative de l'entreprise. La CdG-N estime d'ailleurs judicieux que le Conseil fédéral fasse suivre la mise en œuvre des mesures qu'il a ordonnées par le CDF. Elle prend acte du fait que la mesure fondamentale consistant à désenchevêtrer les réseaux de la Confédération et de RUAG est complexe et donc longue à mettre en œuvre, mais est néanmoins d'avis qu'il est très urgent d'accélérer le processus qui mène à sa réalisation. S'agissant des mesures mises en place par RUAG, elle attend du DDPS qu'il exerce sa fonction de représentant du propriétaire en suivant leur mise en œuvre d'un œil critique et en intervenant si nécessaire.

Dans le cadre de ses recherches, la CdG-N a obtenu des renseignements détaillés sur les fichiers piratés et sur les risques résultant de ce vol. Sur la base de ces informations, elle a qualifié l'incident de grave. Elle prend acte de la position de RUAG, qui affirme ne pas avoir subi de préjudice économique direct du fait de la cyberattaque. Estimant qu'un incident de ce type peut aussi avoir un impact indirect ou à plus long terme sur la marche des affaires, elle est néanmoins d'avis que les conséquences du piratage ne doivent pas être sous-estimées.

Un des sujets clés que la CdG-N a cherché à clarifier à la faveur du présent rapport touche à la représentation et à la défense des intérêts de la Confédération en sa qualité de propriétaire de RUAG. La Commission a voulu savoir dans quelle mesure l'incident avait été traité dans le cadre du pilotage stratégique, notamment à l'occasion des entretiens avec le propriétaire, qui ont lieu chaque trimestre entre le chef du DDPS et les dirigeants de RUAG, et comment la Confédération, et le DDPS qui la représente, avaient veillé à ce que l'entreprise prenne (suffisamment) en compte les intérêts de la Confédération en sa qualité de propriétaire. Elle se montre également critique dans ses conclusions, le principal problème résultant – à son avis – du fait que le DDPS ne se montre pas suffisamment ferme dans ses rapports avec RUAG et ne défend donc pas les intérêts du propriétaire avec suffisamment de force. RUAG est en effet à 100 % aux mains de la Confédération. Dans le secteur privé, même les actionnaires minoritaires sont en mesure d'exercer une pression considérable sur l'entreprise lorsqu'ils possèdent une part substantielle du capital.[59]

De l'avis de la CdG-N, ce ne sont pas les instruments qui manquent. Ce qui est particulièrement important à son sens, c'est de fixer des objectifs stratégiques et de contrôler qu'ils soient atteints, notamment dans le cadre des entretiens avec le propriétaire, qui ont lieu à intervalles réguliers. Selon la CdG-N, ces entretiens ne devraient en effet pas être un simple rapport sur la marche des affaires, mais servir de cadre à la discussion de problèmes importants, tels que la cyberattaque, et de leurs conséquences sur la réalisation des objectifs fixés. Ils sont aussi l'occasion de poser des exigences ou d'assigner des missions, autrement dit de garantir la défense des intérêts du propriétaire. La CdG-N ne comprend dès lors pas que la gestion et les conséquences de la cyberattaque n'aient qu'à peine été abordées sur un plan stratégique dans le cadre des entretiens avec le propriétaire ayant eu lieu entre le DDPS et RUAG. Si elle admet qu'il n'appartient pas au Conseil fédéral de prendre part à la direction de l'entreprise sur un plan opérationnel, elle reste persuadée que lorsqu'apparaissent à ce niveau des problèmes pouvant mettre en péril les intérêts du propriétaire et donc toucher aussi le plan stratégique, le Conseil fédéral et le DDPS se doivent d'intervenir.

La CdG-N est en outre résolument convaincue que les discussions importantes ne peuvent pas être conduites seulement dans un cadre informel, sans que les éléments clés de la discussion soient consignés par écrit sous une forme appropriée. En procédant ainsi de manière purement informelle, le DDPS se prive en effet non seulement

[59] Cf. par ex. le cas du Credit Suisse, dans lequel un investisseur, qui était en fait un fonds de couverture détenant environ 0,3 % du capital-actions, a exigé, en automne 2017, la division de la banque en plusieurs parties et a fait augmenter publiquement la pression dans cette perspective, bien que les chances de succès paraissaient minces (NZZ du 17.10.2017: *Hedge-Fund will die Credit Suisse aufspalten – und jetzt?*).

de la base d'information dont il a besoin, mais aussi d'un moyen, voire d'un instrument de pilotage lui permettant d'imposer ses exigences ou ses instructions stratégiques. Cela affaiblit la position du propriétaire et complique la défense des intérêts du propriétaire à plus long terme.

La nomination du conseil d'administration est un autre instrument important de pilotage stratégique. La Commission est d'avis qu'il importe, dès la nomination des membres et surtout du président du conseil d'administration, de veiller à ce que les candidats puissent se rallier aux objectifs fixés par le Conseil fédéral et s'emploient ensuite à les atteindre. Si cela ne devait pas être le cas, il importerait d'intervenir aussi à ce niveau.

En conséquence, la CdG-N attend du DDPS qu'il se montre plus ferme dans ses relations avec RUAG et qu'il défende les exigences de la Confédération et ses intérêts en sa qualité de propriétaire avec plus de force si nécessaire. Dans les trois recommandations qu'elle adresse au Conseil fédéral, elle exige de sa part différentes clarifications en vue d'obtenir une amélioration du gouvernement d'entreprise.

6 Suite de la procédure

La CdG-N invite le Conseil fédéral à prendre position sur l'analyse et les exigences formulées plus haut avant le *28 septembre 2018*.

8 mai 2018

Au nom de la Commission de gestion du Conseil national:

La présidente de la CdG-N,
Doris Fiala, conseillère nationale

La présidente de la sous-commission DFAE/DDPS,
Ida Glanzmann-Hunkeler, conseillère nationale

La secrétaire des CdG,
Beatrice Meli Andres

La secrétaire de la sous-commission DFAE/DDPS,
Céline Andereggen

Abréviations

CDF	Contrôle fédéral des finances
CdG	Commission de gestion
CdG-N	Commission de gestion du Conseil national
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DélCdG	Délégation des Commissions de gestion
DélFin	Délégation des finances des Chambres fédérales
Délséc	Délégation du Conseil fédéral pour la sécurité
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
OFIT	Office fédéral de l'informatique et de la télécommunication
SRC	Service de renseignement de la Confédération
UPIC	Unité de pilotage informatique de la Confédération

Index des personnes auditionnées

Falcone-Goumaz, Nathalie*	Secrétaire générale du DDPS
Fischer, Peter	Délégué au pilotage informatique de la Confédération / directeur de l'UPIC
Frauenknecht, Marcel	Responsable de la section Sécurité informatique de l'UPIC
Parmelin, Guy*	Conseiller fédéral, chef du DDPS
Rothenbühler, Stephan	Responsable de la gestion des participations du DDPS, SG-DDPS
Vernez, Gérald*	Délégué DDPS pour la cyberdéfense

* *Personnes auditionnées plusieurs fois*