Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

RUAG. Sécurité informatique – Situation en 2021

Rapport de la Commission de gestion du Conseil national

du 18 février 2022

L'essentiel en bref

Durant l'année écoulée, la Commission de gestion du Conseil national (CdG-N) a enquêté sur la sécurité informatique au sein de RUAG. Dans ce contexte, elle a vérifié si la Confédération, en sa qualité de propriétaire, avait réagi de manière adéquate au piratage supposé rendu public en mai 2021. Elle a par ailleurs cherché à déterminer le niveau de sécurité informatique de RUAG International et de RUAG MRO, à repérer les connexions qui existaient encore entre les deux entreprises et à identifier les risques qui y étaient liés. Elle s'est aussi demandé si les Commissions de gestion (CdG) avaient été informées correctement et en toute transparence par les départements compétents et par le Conseil fédéral de l'état d'avancement du processus de dissociation et de la cybersécurité au sein de RUAG.

Dans le cadre de son enquête, la CdG-N a consulté différents documents et auditionné les responsables à la Confédération – le chef du Département fédéral des finances (DFF) et la cheffe du Département fédéral de la défense, de la protection de la population et des sports (DDPS) en particulier – et chez RUAG ainsi qu'une délégation du Contrôle fédéral des finances (CDF).

La CdG-N a conclu que les services fédéraux compétents ont globalement réagi de manière adéquate à l'attaque supposée. Elle salue également la réaction rapide de RUAG International, qui a elle-même pris les mesures nécessaires et mandaté des spécialistes externes pour faire toute la lumière sur les critiques. Il est ressorti de cet examen qu'il n'y avait aucune preuve tangible que RUAG International ait effectivement été victime d'un piratage en mai 2021. Les analyses menées à la suite des révélations faites dans les médias ont néanmoins permis d'attirer l'attention de RUAG International sur certaines graves lacunes en matière de cybersécurité et ont conduit l'entreprise à prendre différentes mesures. La commission ne comprend pas pourquoi les lacunes n'ont pas été décelées plus tôt et pourquoi RUAG International n'a pas déjà fait tester son système informatique par une entreprise spécialisée plus tôt. Elle estime que ce genre de test devrait être mené périodiquement, autant dans l'intérêt de RUAG International que dans celui de la Confédération en sa qualité de propriétaire. Elle invite par conséquent le Conseil fédéral, par l'intermédiaire du DFF, compétent en la matière, à examiner l'opportunité d'imposer de tels tests à RUAG International.

Selon les responsables, le processus de dissociation entre RUAG International et RUAG MRO devait être achevé fin 2021. La CdG-N considère particulièrement important que les deux entreprises veillent conjointement à ce qu'aucune donnée sensible, en particulier aucune donnée de RUAG MRO, ne subsiste dans les systèmes de RUAG International. Puisqu'on ne peut exclure que de telles données se trouvent dans des archives ou des sauvegardes et, ayant échappé à l'effacement, parviennent à des tiers en cas de vente d'unités de l'entreprise, la CdG-N estime que des mesures supplémentaires devraient être étudiées. Un examen supplémentaire ciblé des données avant chaque vente pourrait notamment être envisagé. La CdG-N abordera cette question avec les services compétents du DFF et du DDPS. Elle demandera également des renseignements complémentaires et une confirmation de l'effacement des données des systèmes de RUAG International.

La CdG-N trouve que les informations relatives à l'état du processus de dissociation au cours des dernières années manquaient de transparence. Elle invite par conséquent le Conseil fédéral à communiquer plus clairement et plus rapidement aux commissions de haute surveillance, notamment par l'intermédiaire du DFF et du DDPS avec leurs services propriétaires, les défis que pourrait poser la dissociation de RUAG, en particulier en rapport avec le développement de RUAG International.

Rapport

1 Introduction

En 2016, le public a été informé du fait que RUAG avait été la cible d'une cyberattaque. La Commission de gestion du Conseil national (CdG-N) s'est alors chargée de se pencher en détail sur cet incident et a adressé plusieurs recommandations au Conseil fédéral[1]. À la suite de cette attaque, le Conseil fédéral a pris la décision, en juin 2017, de démembrer l'entreprise afin de séparer les parties qui travaillent essentiellement pour l'armée (aujourd'hui RUAG MRO Holding SA) de celles qui ont une orientation internationale (aujourd'hui RUAG International Holding SA). Ces deux sous-holdings sont réunies en une holding d'entreprises d'armement nommée BGRB (*Beteiligungsgesellschaft Rüstungsbetriebe*) Holding SA, qui est détenue en totalité par la Confédération.

Ce dégroupement de l'organisation visait également une dissociation complète des systèmes informatiques. Il était prévu que les données et les systèmes de RUAG SA, qui est au service de l'armée et qui fait donc partie de RUAG MRO Holding SA, soient transférés dans le périmètre de sécurité de la Base d'aide au commandement de l'armée (BAC) dans un souci d'augmentation de la sécurité informatique. RUAG, pour sa part, a réagi à la cyberattaque en lançant le projet «Impact», destiné à améliorer la sécurité de son réseau. Ce projet a été poursuivi et achevé par RUAG International.

En mai 2021, l'émission «Rundschau» de la télévision suisse alémanique[2] a révélé que des pirates informatiques seraient parvenus à s'introduire dans le réseau de RUAG International. Selon les journalistes, cette attaque serait d'autant plus dangereuse qu'il existerait toujours de nombreuses connexions non sécurisées ou sécurisées de manière insuffisante avec d'autres réseaux, en particulier avec des systèmes de RUAG MRO.

La CdG-N a alors décidé de mener des investigations sur la cybersécurité au sein de RUAG International et de RUAG MRO et de vérifier les critiques portant sur l'attaque qui aurait été perpétrée par des pirates. Il s'agissait principalement de déterminer si la cybersécurité de RUAG International et de RUAG MRO était suffisante, de repérer les connexions qui existaient encore entre les deux entreprises et d'identifier les risques qui y étaient liés. En outre, la commission a vérifié si la Confédération, en sa qualité de propriétaire, avait réagi de manière adéquate au piratage supposé et si, ces dernières années, les Commissions de gestion (CdG) avaient été informées correctement et en toute transparence par les départements compétents et par le Conseil fédéral de l'état d'avancement du processus de dissociation et de la cybersécurité au sein de RUAG.

Pour répondre aux questions susmentionnées, la sous-commission a auditionné des représentants de RUAG International et de RUAG MRO, la cheffe du Département de la défense, de la protection de la population et des sports (DDPS) et le chef du

1 Gestion de la cyberattaque menée contre RUAG: rapports de la CdG-N du 8.5.2018 (FF **2018** 4683) et du 19.11.2019 (FF **2020** 2467).
2 Émission «Rundschau», SRF 1, diffusé le 19.5.2021.

Département fédéral des finances (DFF) ainsi que d'autres responsables de ces deux départements. En effet, le contrôle et le pilotage de BGRB Holding SA ainsi que les dossiers concernant RUAG MRO Holding relèvent du DDPS, alors que les activités de RUAG International sont supervisées par le DFF.

Par ailleurs, la sous-commission s'est penchée sur des rapports du Contrôle fédéral des finances (CDF), qui a mené plusieurs audits concernant la cybersécurité au sein de RUAG, de RUAG MRO et de RUAG International, et s'est aussi directement adressée au CDF pour qu'il lui présente ses résultats et ses appréciations.

2 Cybersécurité et état d'avancement du processus de dissociation

2.1 Cybersécurité au sein de RUAG International

Les représentants de RUAG International ont déclaré à la sous-commission compétente que ni les experts de RUAG International, ni le cabinet externe[3] mandaté pour l'occasion ne pouvaient comprendre les faits évoqués lors de l'émission «Rundschau» et qu'il n'existait aucune preuve d'un accès non autorisé aux systèmes de RUAG International.

Dans le cadre de leur contrôle, les experts externes ne se sont pas uniquement penchés sur les allégations de l'émission «Rundschau»: indépendamment de ces critiques, ils devaient également tester les systèmes en profondeur et déceler les failles et les problèmes en déployant toute l'énergie et la créativité dont feraient preuve des pirates informatiques. Selon le CEO de RUAG International, le cabinet externe a détecté plusieurs failles de sécurité sérieuses, auxquelles des mesures immédiates et des mesures à long terme ont été opposées. RUAG International a indiqué que des manquements dans la formation et des retards dans la mise à jour de logiciels et de systèmes faisaient partie des problèmes identifiés et qu'il ne s'agissait pas des mêmes lacunes qui avaient été décelées lors d'audits antérieurs[4]. Le CEO a admis qu'il aurait fallu identifier ces lacunes plus tôt. En réaction, RUAG International s'est séparée de son responsable de la sécurité des systèmes d'information et a procédé à des adaptations organisationnelles.

Dans le cadre de ses investigations, la sous-commission également s'est informée de l'audit que menait alors le CDF à propos de la cybersécurité au sein de RUAG International[5]. Le CDF a constaté que différentes mesures visant à améliorer la cybersécurité avaient été mises en œuvre ou étaient en voie de réalisation. Il a estimé que, si ces mesures étaient mises en œuvre comme prévu, cela renforcerait considérablement la

3 Il s'agit de l'entreprise SEC Consult.
4 Audits du CDF, de l'EPFZ («Sicherheitsaudit Projekt IMPACT», 2019) et de l'entreprise EY («IMPACT Audit Follow-up», 2019).
5 Lors de cet audit subséquent, le CDF a examiné, à partir de juin 2021, l'état de la mise en œuvre de recommandations antérieures concernant la cybersécurité. L'audit devait également évaluer les risques posés par d'éventuelles fuites de données sensibles en cas de vente de RUAG Ammotec.

cybersécurité. En outre, il a indiqué que, entre-temps, RUAG International avait systématiquement relevé les données ITAR[6], mais qu'il n'existait pas encore d'inventaire plus précis d'autres données sensibles. Selon lui, il existe ainsi un «risque résiduel, difficile à évaluer», que, en cas de vente de parties de l'entreprise, des données sensibles tombent entre de mauvaises mains si elles n'ont pas été détectées et effacées au préalable (cf. ch. 2.3).

En ce qui concerne la vente de RUAG Ammotec[7], actuellement en discussion, le CDF a souligné que la situation était moins préoccupante: vu que cette société a, depuis 2014, en grande partie dissocié ses activités informatiques de celles de RUAG International et qu'elle n'a pas accès aux données de RUAG – et donc pas non plus aux données ITAR –, il a estimé que le risque d'une divulgation de données sensibles lors d'une éventuelle vente était faible.

Selon les représentants de RUAG International, le cabinet externe mandaté a également examiné dans quelle mesure les ventes prévues de certains secteurs d'activité auraient des conséquences sur la cybersécurité. Ils sont parvenus à la conclusion que la dissociation des activités permettrait de réduire la complexité des questions informatiques, ce qui simplifierait la surveillance des systèmes et conduirait plutôt à un renforcement de la cybersécurité.

Lors de ses investigations, la sous-commission compétente s'est aussi penchée sur l'externalisation des services informatiques de RUAG International auprès du fournisseur indien Tech Mahindra. Les représentants de RUAG International ont expliqué que cette société fournissait à RUAG International ainsi qu'à d'autres grands groupes des services d'infrastructure et des services aux entreprises, mais qu'elle n'avait pas accès aux données sensibles, en particulier aux données ITAR. Ils ont précisé que RUAG International n'avait plus aucune donnée militaire à sa disposition, les données militaires étant conservées auprès de RUAG MRO et, donc, dans le périmètre de sécurité de la BAC. Le CDF a lui aussi examiné cette externalisation et est parvenu à la conclusion que celle-ci avait été planifiée et exécutée avec le soin requis et que les mesures nécessaires avaient été prises pour protéger les données sensibles[8].

2.2 Cybersécurité au sein de RUAG MRO

En ce qui concerne les révélations faites par les médias au printemps 2021, les représentants de RUAG MRO ont eux aussi indiqué qu'ils n'avaient pu constater aucun accès non autorisé. Selon eux, aucun incident sérieux n'a même été détecté depuis la cyberattaque de 2016. Ils ont précisé que les données et les systèmes principaux du

6 Il s'agit de données et d'informations soumises à la réglementation des États-Unis sur le commerce d'armes et d'équipements militaires (International Traffic in Arms Regulations).

7 RUAG Ammotec produit principalement des munitions et fait partie de RUAG International.

8 Lors de la consultation de l'administration, le CDF a précisé que son audit à ce sujet avait été clos avant l'effacement des données de MRO par RUAG International. C'est pourquoi, dans le rapport concerné, l'effacement des données de MRO Suisse par RUAG International est indiqué comme tâche en suspens, que RUAG devait effectuer avant fin 2021.

RUAG MRO avaient été transférées dans le périmètre de la BAC dans le cadre de la dissociation et que, partant, ils bénéficiaient désormais de la même protection que les systèmes informatiques de l'armée.

Les représentants de RUAG MRO ont souligné que les systèmes informatiques de l'infrastructure scientifique et technique (TWI)[9] et de RUAG Real Estate – qui appartiennent à RUAG MRO –, ne faisaient pas partie du domaine militaire central et, partant, n'avaient pas été migrées dans le périmètre de la BAC. Ils ont précisé que des travaux subséquents, qui devraient s'achever à la fin de l'année 2021, devraient conduire à une amélioration de la cybersécurité.

Le CDF a déclaré à la sous-commission que, depuis 2016, RUAG MRO avait «nettement amélioré» sa cybersécurité. Il a jugé faibles les risques extérieurs auxquels les systèmes de RUAG MRO Suisse étaient exposés, tout comme les risques provenant de RUAG International. Dans son rapport de février 2021 concernant la cybersécurité au sein de RUAG MRO[10], le CDF a estimé que la dissociation des systèmes informatiques avait été menée à bien, en dépit de la forte complexité et des retards, et que ses recommandations antérieures avaient globalement été mises en œuvre. Il a toutefois identifié un potentiel d'amélioration s'agissant de la sécurité d'exploitation et des risques qui pourraient survenir lors du nettoyage des archives et des copies de sauvegarde (cf. ch. 2.3).

2.3 État d'avancement du processus de dissociation

Les responsables de RUAG MRO, mais également ceux du Secrétariat général du DDPS (SG DDPS), ont indiqué à la sous-commission que, entre-temps, toutes les données de RUAG MRO pertinentes en matière de sécurité avaient été transférées dans le périmètre de sécurité de la BAC. Lors de cette migration, d'importantes mesures ont été prises pour garantir qu'aucun logiciel malveillant n'infecte les systèmes de la BAC. En outre, différents travaux résiduels sont encore en cours concernant le démontage de systèmes devenus inutiles et le nettoyage de données au sein de RUAG International ainsi que les systèmes de la TWI[11] et les systèmes informatiques de RUAG Real Estate (ces deux derniers systèmes ne sont pas intégrés dans le périmètre de la BAC).

Aux dires de RUAG MRO et de RUAG International, ces travaux sont déjà bien avancés: le nettoyage des données a été achevé au deuxième trimestre 2021 et la majeure partie des systèmes informatiques de RUAG International ont été démantelés. Les travaux concernant Real Estate et TWI sont également en cours et devraient être achevés d'ici fin 2021. En ce qui concerne les responsabilités relatives au démantèlement des systèmes et au nettoyage des données, les représentants de RUAG MRO et de RUAG International ont indiqué que les deux sous-holdings collaboraient étroitement pour mener à bien ces travaux. Concrètement, RUAG MRO examine les données et

9 Infrastructure informatique décentralisée destinée à des utilisations commerciales de machines, d'appareils de mesure et d'applications spécifiques qui ne peut pas être exploitée ou mise à disposition par la BAC.
10 Rapport du CDF du 22.2.2021, publié.
11 Cf. note de bas de page 9.

les systèmes, puis en confie l'effacement ou la déconnexion à RUAG International, qui s'exécute et confirme que les données ont été effacées ou les systèmes, déconnectés. Toutes les données, en particulier les données sensibles dont disposait RUAG International avant la dissociation, avaient été effacées à fin mai 2021, à l'exception des données qui existaient encore dans les systèmes de RUAG Real Estate et de la TWI et qui devraient être effacées d'ici la fin de l'année 2021.

Les responsables de RUAG MRO et de RUAG International ont expliqué que RUAG – ou plutôt les deux sous-holdings – disposait désormais d'une vue complète des données, des serveurs et des archives, condition nécessaire à la migration des données militaires dans le périmètre de la BAC et aux travaux encore en cours.

Le CDF estime quant à lui que la situation est plus problématique que l'affirment les représentants des deux sous-holdings. Dans ses rapports relatifs à la cybersécurité au sein de RUAG MRO et de RUAG Holding[12] et dans les explications qu'il a fournies à la sous-commission, il a indiqué que le nettoyage des données comportait certains risques auxquels RUAG devrait accorder l'attention nécessaire. En particulier, le CDF estime essentiel de vérifier, lors de l'effacement des données de RUAG MRO, s'il existe des archives et des sauvegardes de données sur les systèmes de RUAG International et si ces dernières contiennent aussi des données qui devraient être effacées. Le CDF doute que RUAG ait une vue d'ensemble complète de la situation[13]. Il a en outre constaté que RUAG International avait certes collecté et classifié les données ITAR mais ne l'avait pas fait pour d'autres données sensibles. L'absence de vue d'ensemble complète sur les archives, les sauvegardes et les données sensibles pourrait conduire à des fuites de données en cas de vente de secteurs d'activité. Par conséquent, le CDF a invité RUAG MRO et RUAG International[14] à accorder à cette problématique l'attention qu'elle mérite; en outre, il devrait probablement effectuer un audit à propos de l'effacement des données.

2.4 Appréciation de la CdG-N

Sur la base de ses investigations, la CdG-N est parvenue à la conclusion qu'il n'y avait aucune preuve tangible que RUAG International ait effectivement été victime d'un piratage en mai 2021. Quoi qu'il en soit, les vérifications qui ont été menées à la suite des révélations faites dans les médias ont permis d'attirer l'attention de RUAG International sur certaines graves lacunes en matière de cybersécurité et ont conduit l'entreprise à prendre différentes mesures. De l'avis de la commission, RUAG International a bien réagi, soumettant sa cybersécurité à un test de résistance rigoureux mené par un cabinet externe. La CdG-N ne comprend toutefois pas pourquoi les lacunes

12 Rapports du CDF du 22.2.2021 (publié) et du 21.10.2019 (pas publié).

13 Selon le retour transmis par RUAG MRO lors de la consultation de l'administration, un risque résiduel que des supports de données n'aient pas été saisis ne peut pas être totalement exclu. Selon l'entreprise, il est toutefois très faible, soit «de l'ordre du pour mille».

14 La responsabilité de l'effacement des données pertinentes pour la sécurité des systèmes de RUAG International est partagée entre les deux sous-holdings. RUAG MRO n'est pas relevée de sa responsabilité avant que les données qu'elle a reprises pour son travail et qu'elle a transférées dans le périmètre de la BAC aient été effacées au sein de RUAG International.

n'avaient pas déjà été décelées et pourquoi RUAG International n'avait pas fait tester son système informatique par une entreprise spécialisée plus tôt. La commission estime que ce genre de test devrait être mené de manière périodique, ce qui serait autant dans l'intérêt de RUAG International (protection du secret des affaires) que dans celui de la Confédération en sa qualité de propriétaire. Par conséquent, elle invite le Conseil fédéral, par l'intermédiaire du DFF, à examiner s'il serait possible et judicieux d'enjoindre à RUAG International de mener de tels tests, afin de défendre les intérêts du propriétaire en vue d'une éventuelle vente.

En ce qui concerne l'état du processus de dissociation, la CdG-N part du principe que ce processus sera achevé d'ici la fin de l'année 2021. Elle estime particulièrement important que RUAG MRO et RUAG International veillent conjointement à ce qu'aucune donnée sensible, en particulier aucune donnée de RUAG MRO, ne subsiste sur les systèmes de RUAG International. En 2022, la CdG-N demandera de plus amples informations à ce sujet, notamment une confirmation que les données concernées ont bel et bien été effacées.

Le CDF ayant émis la possibilité que des données sensibles soient cachées dans les archives et les sauvegardes, et donc soient oubliées et parviennent à des tiers en cas de vente, la CdG-N se demande toutefois si des mesures supplémentaires ne devraient pas être prises. En particulier, il s'agirait de vérifier si la Confédération, en sa qualité de propriétaire, ne devrait pas contraindre RUAG International, avant chaque vente d'une unité, à procéder ou à faire procéder à un examen supplémentaire ciblé des données. Cet examen consisterait à dresser l'inventaire de toutes les données et à vérifier s'il y a encore parmi elles des données sensibles de RUAG MRO, des données ITAR ou d'autres données sensibles. La CdG-N, et son homologue du Conseil des États, clarifieront cette question en 2022 avec les représentants du propriétaire au sein du DFF et du DDPS.

Recommandation 1: Protection des données militaires et des autres données sensibles

La CdG-N demande au Conseil fédéral de prendre les mesures nécessaires pour que RUAG International ne dispose plus de données militaires ou d'autres données sensibles après l'effacement prévu des données (pas même dans des archives ou des sauvegardes). La question se pose de savoir si la suppression doit être contrôlée par des experts externes. Il convient par ailleurs d'examiner s'il serait opportun de demander un contrôle supplémentaire de la situation des données avant chaque vente de parties de RUAG International.

3 Réaction du propriétaire

3.1 Mesures du DFF et du DDPS

Les investigations de la sous-commission ont montré que, le 12 mai 2021 (soit une semaine environ avant la diffusion de l'émission «Rundschau»), les journalistes de

l'émission avaient demandé au DDPS, par écrit, de prendre position au sujet du piratage présumé et que le DDPS en avait immédiatement informé le DFF. La cheffe du DDPS a indiqué à la sous-commission à plusieurs reprises que le piratage présumé concernait en effet RUAG International, qui est de la responsabilité du DFF. C'est pourtant le DDPS – et non le DFF ou les deux départements ensemble – qui a fait parvenir une prise de position à l'émission «Rundschau»[15].

La cheffe du DDPS et le chef du DFF ont toutefois précisé que les deux départements avaient collaboré étroitement sur les questions liées à RUAG International et RUAG MRO, en particulier pour préparer les séances du conseil d'administration de BGRB Holding SA. Depuis le 1er avril 2021, la directrice de l'Administration fédérale des finances (AFF) et le secrétaire général du DDPS siègent au sein de ce conseil d'administration, ce qui répond à un souhait exprimé depuis un certain temps déjà par la CdG-N[16]. Le Conseil fédéral entend ainsi accompagner de près le processus de dissociation et de privatisation de RUAG International[17].

Le chef du DFF a indiqué que le piratage présumé ainsi que des questions liées à la cybersécurité ont été discutés aux séances du conseil d'administration de BGRB Holding SA des 18 mai et 1er juin 2021. Le DFF et le DDPS n'ont pas procédé eux-mêmes à des investigations, mais se sont surtout fondés, pour évaluer la situation, sur les informations fournies par RUAG International et par le cabinet externe mandaté par RUAG International.

Par ailleurs, le DFF a déclaré à la CdG-N qu'il ne s'attendait pas à ce que les révélations sur le piratage présumé aient des conséquences négatives majeures sur le maintien de la valeur de RUAG International et sur le projet de vente de secteurs d'activité. Selon le département, ce sont plutôt «les informations fiables fournies par RUAG International concernant l'état de ses systèmes informatiques et les risques qui y sont liés» qui sont déterminantes. Il a ajouté que, pour la Confédération, il est primordial d'éviter que les achats donnent lieu au transfert non intentionnel, à un acheteur, de données sensibles pour la sécurité de l'armée suisse ou de RUAG MRO. Pour ce faire, il a expliqué que RUAG International suivait «les procédures habituellement appliquées dans le cadre de ventes d'entreprises, qui consistent à séparer les systèmes informatiques et à s'assurer que les données transférées ne contiennent pas de logiciels malveillants».

3.2 Appréciation de la CdG-N

Aux yeux de la CdG-N, il convenait de se demander en particulier si le DFF et le DDPS avaient réagi de façon adéquate au reportage de l'émission «Rundschau» et veillé à ce que les intérêts du propriétaire soient garantis. Elle a constaté que les deux départements avaient immédiatement pris en considération les critiques et les avaient examinées au sein du conseil d'administration de BGRB Holding SA. Vu que le DFF

15 Avis du DDPS du 15.5.2021 (publié)
16 Bilan de la gestion de la cyberattaque menée contre RUAG. Rapports de la CdG-N du 8.5.2018 (FF **2018** 4683) et du 19.11.2019 (FF **2020** 2467).
17 La Confédération sera représentée au conseil d'administration de RUAG, communiqué de presse du Conseil fédéral du 12.3.2020.

et le DDPS siègent au sein de cet organe depuis le printemps 2021 – comme l'avait demandé la CdG-N il y a quelque temps[18] –, cela devrait au moins améliorer l'échange d'informations. Dans ce contexte, et comme RUAG International a elle-même pris les mesures nécessaires pour faire toute la lumière sur les critiques (en particulier en mandatant des experts externes), la commission comprend que les organes fédéraux compétents aient, en l'espèce, renoncé à lancer eux aussi des investigations. Toutefois, on peut se demander si des spécialistes de la Confédération n'auraient pas dû vérifier l'opportunité de l'audit commandé par RUAG International.

S'il est important de répondre aux questions susmentionnées, la CdG-N estime néanmoins qu'il faut surtout souligner que le DFF et le DDPS n'accordent pas l'attention nécessaire au fait que des données militaires ou sensibles se trouvaient à l'époque dans des systèmes de RUAG International (et un risque résiduel qu'on en trouve peut-être encore ne peut pas être totalement exclu), comme le montrent les explications ci-dessus relatives au processus de dissociation ainsi que les audits du CDF. Il est donc difficile de comprendre pourquoi la cheffe du DDPS souligne que les données de l'armée pertinentes en matière de sécurité ne sont plus «traitées» que par RUAG MRO. De même, il ne suffit pas, lors de ventes d'unités, de séparer les systèmes informatiques et de s'assurer que les données ne contiennent pas de logiciels malveillants, comme l'a déclaré le chef du DFF.

Comme elle l'a déjà indiqué plus haut, la CdG-N attend de la Confédération, en tant que propriétaire, qu'elle s'assure que les données militaires et d'autres données sensibles soient effectivement effacées des systèmes de RUAG et qu'elle détermine s'il est nécessaire d'effectuer une vérification supplémentaire avant une vente (cf. ch. 2.4, recommandation 1).

4 Information des CdG

4.1 Premières informations fournies aux CdG concernant l'état d'avancement du processus de dissociation

Dans le cadre de ses investigations, la CdG-N a vérifié si le Conseil fédéral, en particulier le DDPS, l'a informée correctement et en toute transparence, ces dernières années, sur l'état d'avancement du processus de dissociation et sur la cybersécurité au sein de RUAG. En effet, le Conseil fédéral et le DDPS ont toujours souligné, devant la commission comme devant le public, que la dissociation et le développement du groupe RUAG étaient sur la bonne voie, en dépit de leur complexité. Par exemple, le 19 février 2020, le Conseil fédéral a confirmé, dans un avis qu'il a remis à la CdG-N, que la séparation prendrait effet à l'été 2020[19]. En juin 2020, la cheffe du DDPS a déclaré aux sous-commissions compétentes des CdG que les éléments principaux du

18 Cf. note de bas de page 15.
19 Avis du Conseil fédéral du 19.2.2020 sur le rapport de la CdG-N du 19.11.2020 concernant la gestion de la cyberattaque menée contre RUAG; communiqué de presse du Conseil fédéral du 24.2.2020.

processus de dissociation avaient été mis en œuvre sur le plan opérationnel au 1er janvier 2020 et que les systèmes informatiques de RUAG MRO avaient été migrés avec succès dans le périmètre de sécurité de la BAC pendant les fêtes de Pâques. En avril 2021, elle a indiqué aux mêmes sous-commissions que la mission de dissociation avait été accomplie dans les délais prévus, précisant que les principaux objectifs organisationnels, juridiques et informatiques du processus de dissociation avaient été mis en œuvre pour la fin du mois de juin 2020.

Dans le rapport que le Conseil fédéral a remis aux CdG le 19 mars 2021 concernant la réalisation des objectifs de RUAG en 2020, on peut cependant lire que «les travaux finaux de la dissociation [seraient intégrés] dans un deuxième programme». En outre, il y indique qu'il s'agit surtout de nettoyer les données et de dissocier les systèmes informatiques de la TWI et de RUAG Real Estate. Par conséquent, le DDPS estime que les CdG ont été informées de manière transparente.

Les représentants de RUAG MRO ont déclaré à la CdG-N que cette deuxième étape était prévue et qu'il est habituel, dans les projets de grande envergure, de liquider les travaux résiduels dans un deuxième temps.

4.2 Appréciation de la CdG-N

La commission prend acte du fait que le Conseil fédéral mentionne et décrit plus précisément la deuxième étape du processus de dissociation dans son rapport du 19 mars 2021. Toutefois, elle constate également que le DDPS n'a jamais évoqué ces travaux lors des différentes auditions. Au contraire, il a toujours souligné que les principaux éléments du processus de dissociation avaient été mis en œuvre dans les délais[20]. Par conséquent, la CdG-N est clairement d'avis que la communication du DDPS aurait dû être plus précise et plus transparente, notamment parce qu'il sait que les CdG se penchent depuis longtemps sur ce thème. Elle invite le DDPS et le Conseil fédéral à communiquer de manière plus transparente à l'avenir.

Recommandation 2: Communication plus transparente

La CdG-N invite le Conseil fédéral à prendre des mesures adéquates pour que, à l'avenir, le Conseil fédéral ainsi que les services propriétaires du DFF et du DDPS informent les commissions de haute surveillance de manière plus transparente et plus rapide des difficultés rencontrées lors de la dissociation de RUAG et, en particulier, dans le cadre du développement de RUAG International.

20 Lors de la consultation de l'administration, le DDPS a relevé que le Conseil fédéral avait fixé à BGRB Holding, dans le cadre des objectifs stratégiques, un délai à fin 2021 pour clore les travaux restants. Selon le département, ces travaux, qui ont été réunis en septembre 2020 dans une «deuxième étape de dissociation» sont «moins importants que la nécessité d'exécuter les travaux pour l'armée dans un environnement télématique sûr». C'est pourquoi le DDPS reste d'avis que l'essentiel de la dissociation était achevé en juin 2020 et que le délai fixé a ainsi été respecté. Le DDPS estime par ailleurs que le projet de la dissociation de RUAG s'est déroulé avec succès. Le CDF l'a confirmé, en indiquant dans son rapport d'audit que «les objectifs du projet ont été atteints tant sur le plan qualitatif que quantitatif».

5 Conclusions

Se fondant sur les explications et les conclusions qui font l'objet du présent document, la CdG-N a décidé de mettre un terme à ses investigations concernant le piratage présumé de 2021. Elle poursuivra son examen des aspects critiques et des questions mentionnées dans ce rapport et les traitera conjointement avec son homologue du Conseil des États, en particulier dans le cadre de son examen annuel du rapport du Conseil fédéral concernant la réalisation des objectifs stratégiques de RUAG. Lorsque cela s'avérera nécessaire et d'entente avec les autres commissions compétentes, Les CdG suivront l'évolution de RUAG International et des risques qui en découlent, en se concentrant sur la question de savoir si la Confédération assume son rôle de propriétaire de façon adéquate.

La CdG-N invite le Conseil fédéral à prendre position sur ce rapport et ses recommandations d'ici au 25 mars 2022.

18 février 2022

Au nom de la Commission de gestion
du Conseil national

La présidente: Prisca Birrer-Heimo

La secrétaire: Beatrice Meli Andres

Le président de la sous-commission DFAE/DDPS:
Nicolo Paganini

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

Abréviations

AFF	Administration fédérale des finances
BAC	Base d'aide au commandement de l'armée
BGRB	Société de participation financière aux entreprises d'armement (*Beteiligungsgesellschaft Rüstungsbetriebe*)
CDF	Contrôle fédéral des finances
CdG	Commissions de gestion des Chambres fédérales
CdG-N	Commission de gestion du Conseil national
DDPS	Département de la défense, de la protection de la population et des sports
DFF	Département fédéral des finances
ITAR	Réglementation des États-Unis sur le commerce d'armes et d'équipements militaires (*International Traffic in Arms Regulation*)
SG DDPS	Secrétariat général du DDPS
TWI	Infrastructure scientifique et technique (*Technisch-Wissenschaftliche Infrastrukturen;* cf. note de bas de page 9)