Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Sicurezza informatica della RUAG Situazione nel 2021

Rapporto della Commissione della gestione del Consiglio nazionale

del 18 febbraio 2022

L'essenziale in breve

Nel 2021 la Commissione della gestione del Consiglio nazionale (CdG-N) ha esaminato la sicurezza informatica della RUAG e verificato se la Confederazione, in qualità di proprietaria, aveva reagito in modo adeguato al presunto ciberattacco reso noto nel maggio 2021. Ha inoltre cercato di determinare il livello di sicurezza informatica di RUAG International e RUAG MRO nonché di individuare le interdipendenze ancora esistenti tra le due imprese e i rischi ad esse connessi. In questo contesto la Commissione si è anche chiesta se negli ultimi anni le Commissioni della gestione (CdG) erano state informate in modo corretto e trasparente dai dipartimenti competenti e dal Consiglio federale sullo stato di avanzamento dello scorporo e sulla sicurezza informatica della RUAG.

Nell'ambito della sua verifica la CdG-N ha consultato diversi documenti e sentito i rappresentanti della Confederazione – in particolare il capo del Dipartimento federale delle finanze (DFF) e il capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) –, della RUAG e del Controllo federale delle finanze (CDF).

La CdG-N è giunta alla conclusione che gli enti federali competenti hanno in linea di massima reagito in modo adeguato al presunto ciberattacco. Approva inoltre che RUAG International stessa abbia rapidamente avviato le misure necessarie e incaricato esperti esterni di esaminare approfonditamente le asserzioni. Ne è emerso che non sussistevano prove tangibili del presunto ciberattacco a RUAG International nel maggio 2021. A prescindere da ciò, le verifiche condotte in seguito al reportage dei media hanno permesso di attirare l'attenzione di RUAG International su gravi lacune in materia di sicurezza informatica e di avviare diverse misure. La Commissione non comprende perché le lacune non fossero state individuate prima e RUAG International non avesse incaricato più precocemente una ditta specializzata di testare i suoi sistemi informatici. A suo parere tali test avrebbero dovuto essere eseguiti periodicamente non solo nell'interesse dell'impresa, ma anche della Confederazione in qualità di proprietaria. La Commissione invita pertanto il Consiglio federale, in particolare il DFF in qualità di dipartimento competente, a valutare la possibilità di imporre una simile esigenza nei confronti di RUAG International.

Secondo i responsabili le ultime interdipendenze esistenti tra RUAG International e RUAG MRO sarebbero state separate entro la fine del 2021 e lo scorporo sarebbe stato così completamente concluso. Per la CdG-N è estremamente importante che le due imprese garantiscano congiuntamente che nessun dato sensibile, in particolare nessun dato di RUAG MRO, rimanga sui sistemi di RUAG International. Siccome non può essere escluso che tali dati si trovino negli archivi e nei backup e che quindi passino inosservati e cadano nelle mani di terzi in caso di vendita di parti di RUAG International, la Commissione ritiene opportuno esaminare ulteriori misure, tra cui in particolare un ulteriore controllo dei dati mirato prima di ogni vendita. La CdG-N chiarirà questa tematica con i servizi competenti del DFF e del DDPS. Chiederà inoltre maggiori informazioni e una conferma della cancellazione dei dati dai sistemi di RUAG International.

La Commissione giudica che l'informazione sullo stato dello scorporo sia stata troppo poco trasparente negli ultimi anni. Invita pertanto il Consiglio federale a garantire che il Collegio governativo, il DFF e il DDPS con i loro enti proprietari informino in futuro le commissioni di alta vigilanza in modo più trasparente e rapido sulle difficoltà incontrate durante lo scorporo di RUAG e, in particolare, nell'ambito dello sviluppo di RUAG International.

Rapporto

1 Introduzione

Nel 2016 è stata data la notizia di un ciberattacco contro la RUAG, in seguito al quale la Commissione della gestione del Consiglio nazionale (CdG-N) ha trattato approfonditamente l'incidente e ha rivolto raccomandazioni al Consiglio federale[1]. Come conseguenza dell'attacco, nel giugno 2017 il Consiglio federale ha deciso di scindere la RUAG e di separare le parti che lavorano principalmente per l'esercito (RUAG MRO Holding SA) dagli altri settori orientati agli affari internazionali (RUAG International Holding SA). Oggi entrambe le subholding sono riunite nella società mantello chiamata BGRB Holding SA (società di partecipazione delle aziende d'armamento), di proprietà della Confederazione.

Questo scorporo organizzativo aveva anche lo scopo di separare completamente i sistemi informatici. I dati e i sistemi di RUAG SA, che fa parte di RUAG MRO Holding SA ed è dunque al servizio dell'esercito, dovevano essere migrati nel perimetro di sicurezza della Base d'aiuto alla condotta (BAC) per aumentare la sicurezza informatica. Dal canto suo, la RUAG ha reagito al ciberattacco lanciando il progetto «Impact» volto a migliorare la sicurezza della sua rete. Il progetto è stato proseguito e concluso da RUAG International.

Nel maggio 2021 il programma «Rundschau» della televisione svizzera tedesca[2] ha asserito che pirati informatici sarebbero riusciti a penetrare la rete di RUAG International. Secondo i giornalisti questo attacco era particolarmente pericoloso poiché la rete continuava a presentare numerose connessioni non sicure o non sufficientemente sicure con altre reti, in particolare con quelle dei sistemi di RUAG MRO.

La CdG-N ha quindi deciso di eseguire accertamenti sulla sicurezza informatica di RUAG International e RUAG MRO e di esaminare le asserzioni fatte in merito al presunto ciberattacco. Gli accertamenti dovevano soprattutto determinare se la sicurezza informatica delle due imprese era sufficiente, individuare le interdipendenze ancora esistenti e i rischi ad esse connessi. La Commissione ha inoltre esaminato se la Confederazione, in qualità di proprietaria, aveva reagito in modo adeguato al presunto ciberattacco e se in questi ultimi anni le CdG erano state informate in modo corretto e trasparente dai dipartimenti competenti e dal Consiglio federale sullo stato di avanzamento dello scorporo e sulla sicurezza informatica della RUAG.

Per rispondere alle domande di cui sopra, la sottocommissione ha sentito rappresentanti di RUAG International e RUAG MRO, il capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e il capo del Dipartimento federale delle finanze (DFF) nonché altri responsabili di questi dipartimenti. Il DDPS è infatti responsabile della condotta e del controllo di BGRB Holding nonché degli affari di RUAG MRO, mentre il DFF della gestione degli affari di RUAG International.

1 Gestione del ciberattacco contro la RUAG: rapporto della CdG-N dell'8 mag. 2018 (FF **2018** 3895) e del 19 nov. 2019 (FF **2020** 2280).
2 Programma televisivo «Rundschau» della SRF 1, trasmesso il 19 mag. 2021.

La sottocommissione ha inoltre trattato i rapporti del Controllo federale delle finanze (CDF) – il quale ha condotto diversi esami sulla sicurezza informatica di RUAG, RUAG MRO e RUAG International – e si è informata anche direttamente presso il CDF in merito ai risultati a cui è giunto e alle relative valutazioni.

2 Sicurezza informatica e stato dello scorporo

2.1 Sicurezza informatica presso RUAG International

I rappresentanti di RUAG International hanno ribadito alla sottocommissione che né i propri esperti né la ditta esterna[3] potevano comprendere quanto mostrato nel programma televisivo e che non sussistevano prove di un accesso non autorizzato ai sistemi di RUAG International.

Nel loro esame gli esperti esterni non soltanto hanno verificato i fatti alla base delle asserzioni fatte nel programma televisivo, ma, indipendentemente da esse, hanno anche testato a fondo i sistemi e cercato lacune e problemi impiegando l'energia e l'inventiva di cui sono capaci i pirati informatici. Secondo il CEO di RUAG International la ditta esterna ha individuato alcune serie lacune in materia di sicurezza cui si è posto rimedio con provvedimenti immediati e misure a lungo termine. RUAG International ha indicato che tra i problemi individuati figuravano soprattutto carenze nella formazione e ritardi nell'aggiornamento dei programmi e dei sistemi informatici e che non si trattava delle stesse lacune riscontrate nelle precedenti verifiche[4]. Il CEO ha ammesso che queste lacune avrebbero dovuto essere individuate prima. Di conseguenza, RUAG International si è separata dal responsabile della sicurezza informatica e ha proceduto ad adeguamenti organizzativi.

Nell'ambito dei suoi accertamenti la sottocommissione si è anche informata in merito alla verifica della sicurezza informatica condotta dal CDF presso RUAG International[5]. Il CDF ha constatato che diverse misure volte a migliorare la sicurezza informatica erano state attuate o erano in corso e a suo parere, se venivano attuate come previsto, la sicurezza informatica ne sarebbe risultata notevolmente aumentata. Ha inoltre indicato che nel frattempo RUAG International aveva sistematicamente raccolto i dati ITAR[6], ma che non esisteva ancora un inventario più preciso di altri dati sensibili. Ritiene che sussista quindi un rischio residuo difficile da stimare per cui, in caso di vendita di parti dell'impresa, dati sensibili potrebbero cadere nelle mani sbagliate se prima non vengono individuati e cancellati (cfr. n. 2.3).

3 Si tratta della ditta SEC Consult.
4 Verifiche del CDF, del Politecnico federale di Zurigo («Sicherheitsaudit Projekt IMPACT», 2019) e della ditta EY («IMPACT Audit Follow-up», 2019).
5 Nell'ambito di questa verifica il CDF ha esaminato dal giugno 2021 lo stato dell'attuazione di raccomandazioni anteriori concernenti la sicurezza informatica. La verifica doveva anche stimare i rischi che presentavano eventuali fughe di dati sensibili al momento della vendita di RUAG Ammotec.
6 Si tratta di dati e informazioni sottostanti al quadro normativo degli Stati Uniti sul commercio di armi e l'armamento (*International Traffic in Arms Regulations*).

Per quanto concerne la vendita di RUAG Ammotec[7], attualmente in discussione, il CDF ha assicurato che la situazione è meno allarmante: dato che questa impresa ha separato già nel 2014 gran parte della sua infrastruttura informatica da quella di RUAG ai cui dati non ha dunque più accesso – e quindi neanche a quelli ITAR – il CDF stima che il rischio di una divulgazione di dati sensibili in caso di vendita sia esiguo.

Secondo i rappresentanti di RUAG International anche la ditta esterna incaricata ha esaminato in quale misura le vendite previste di determinati settori di attività possono influire sulla sicurezza informatica. Sono giunti alla conclusione che la complessità delle questioni informatiche verrebbe ridotta semplificando al contempo la sorveglianza dei sistemi e aumentando la sicurezza informatica.

Una tematica che la sottocommissione ha altresì trattato durante i suoi accertamenti è stata l'esternalizzazione delle prestazioni informatiche di RUAG International al fornitore indiano Tech Mahindra. I rappresentanti di RUAG International hanno spiegato che questa società fornisce a RUAG International e a molti altri grandi gruppi prestazioni di infrastruttura e prestazioni alle imprese, ma non ha accesso a dati sensibili, in particolare a dati ITAR. Hanno anche spiegato che oggi RUAG International non dispone più di dati militari, poiché questi sono conservati presso RUAG MRO e quindi nel perimetro di sicurezza della BAC. Anche il CDF, che ha parimenti verificato questa tematica, è giunto alla conclusione che l'esternalizzazione è stata pianificata ed eseguita con la dovuta attenzione e che erano state adottate le misure necessarie per proteggere i dati sensibili[8].

2.2 Sicurezza informatica presso RUAG MRO

Per quanto riguarda le asserzioni fatte dai media nella primavera del 2021, anche i rappresentanti di RUAG MRO hanno indicato che non solo non sono stati constatati accessi non autorizzati, ma persino non sono più stati individuati incidenti seri dopo il ciberattacco del 2016. Hanno precisato che al momento dello scorporo i dati e i sistemi principali di RUAG MRO erano stati trasferiti nel perimento della BAC e quindi godevano della stessa protezione dei sistemi informatici dell'esercito.

I rappresentanti di RUAG MRO hanno sottolineato che i sistemi informatici dell'infrastruttura scientifica e tecnica (TWI)[9] e di RUAG Real Estate, che appartengono a RUAG MRO, non fanno parte del settore militare centrale e quindi non sono stati migrati nel perimetro della BAC. Hanno precisato che sarebbero stati avviati lavori

7 RUAG Ammotec produce soprattutto munizioni e fa parte di RUAG International.

8 Durante la consultazione dell'amministrazione, il CDF ha precisato che la sua verifica su questa tematica era stata conclusa prima della cancellazione dei dati di MRO da parte di RUAG International e pertanto nel rapporto la cancellazione dei dati di MRO Svizzera da parte di RUAG International figura come pendenza che la RUAG doveva evadere prima della fine del 2021.

9 Infrastrutture informatiche decentrali per uso commerciale, dotate di macchinari, apparecchi di verifica e applicazioni specifiche e che non possono essere gestite o messe a disposizione dalla BAC.

volti anche a migliorare la sicurezza informatica. Questi lavori dovevano essere terminati a fine 2021.

Il CDF ha dichiarato alla sottocommissione che dal 2016 la sicurezza informatica di RUAG MRO era «nettamente migliorata» e riteneva esigui sia i rischi esterni ai quali i sistemi di RUAG MRO Svizzera erano esposti sia i rischi che provenivano da RUAG International. Nel suo rapporto del febbraio 2021 sulla sicurezza informatica presso RUAG MRO[10] il CDF è giunto alla conclusione che, nonostante l'elevata complessità e diversi ritardi, lo scorporo informatico si sia concluso con successo e che globalmente le sue precedenti raccomandazioni sono state attuate. Ha tuttavia individuato un potenziale di miglioramento nella sicurezza dell'esercizio e vari rischi che potrebbero sorgere al momento della revisione di archivi e di backup (cfr. n 2.3).

2.3 Stato dello scorporo

Come già esposto, i responsabili di RUAG MRO, così come i responsabili della SG DDPS, hanno indicato alla sottocommissione che nel frattempo tutti i dati di RUAG MRO riguardanti la sicurezza sono stati migrati nel perimetro di sicurezza della BAC. Al momento di questa migrazione sono state prese importanti misure per garantire la protezione dei sistemi della BAC da malware. Attualmente sono ancora in corso diversi «lavori residui» che riguardano lo smantellamento di sistemi diventati inutili nonché la rettifica di dati presso RUAG International, i sistemi della TWI[11] e l'informatica di RUAG Real Estate (questi due ultimi sistemi non verranno integrati nel perimento della BAC).

Secondo RUAG MRO e RUAG International questi lavori si trovano in uno stadio molto avanzato: la rettifica dei dati è terminata nel secondo trimestre 2021 e la maggior parte dei sistemi informatici di RUAG International è stata smantellata. Anche i lavori relativi a Real Estate e alla TWI sarebbero in corso e dovrebbero concludersi entro fine 2021. Per quanto riguarda lo smantellamento dei sistemi e la rettifica dei dati, i rappresentanti di RUAG MRO e RUAG International hanno indicato che le due subholding stanno collaborando strettamente per concludere questi lavori con successo. Concretamente RUAG MRO verifica i dati e i sistemi per poi affidare il mandato di cancellarli o disconnetterli a RUAG International, la quale lo esegue e conferma la cancellazione dei dati o la disconnessione dei sistemi. Tutti i dati, in particolare i dati sensibili di cui disponeva RUAG International prima dello scorporo, sono stati cancellati a fine maggio 2021, ad eccezione dei dati ancora esistenti nei sistemi di Real Estate e della TWI, da cancellare entro fine 2021.

I responsabili della RUAG e di RUAG MRO hanno spiegato che le due subholding dispongono oggi di una vista d'insieme completa dei dati, dei server e degli archivi, condizione *sine qua non* per la migrazione dei dati militari nel settore BAC e anche per i lavori attualmente in corso.

Il CDF valuta la situazione in modo più critico di quanto facciano i rappresentanti delle subholding della RUAG. Nei suoi rapporti sulla sicurezza informatica presso

10 Rapporto del CDF del 22 feb. 2021, pubblicato.
11 Cfr. nota a piè di pagina 9.

RUAG MRO e RUAG Holding[12] e nelle sue spiegazioni alla sottocommissione ha indicato che la rettifica dei dati comportava taluni rischi ai quali la RUAG dovrebbe conferire la necessaria attenzione. In particolare il CDF ritiene centrale verificare, al momento della cancellazione dei dati di RUAG MRO, se esistono sui sistemi di RUAG International archivi e backup di dati e se questi ultimi contengono anche dati che dovrebbero essere cancellati. Il CDF dubita che la RUAG abbia una vista d'insieme completa della situazione[13]. Constata altresì che RUAG International aveva sì raccolto e classificato dati rilevanti ITAR, ma non lo aveva fatto per altri dati sensibili. La mancanza di una vista d'insieme completa degli archivi, dei backup e dei dati sensibili potrebbe portare alla fuga di dati sensibili in caso di vendita di settori di attività. Il CDF ha quindi invitato RUAG MRO e RUAG International[14] a conferire a questa problematica la necessaria attenzione; probabilmente procederà anche a una verifica della cancellazione dei dati.

2.4 Valutazione della CdG-N

Sulla base dei suoi accertamenti la CdG-N è giunta alla conclusione che non sussistono prove tangibili di un presunto ciberattacco nei confronti di RUAG International nel maggio 2021. A prescindere da ciò, le verifiche condotte in seguito alle asserzioni fatte dai media hanno permesso di attirare l'attenzione di RUAG International sulle gravi lacune in materia di sicurezza informatica e di avviare diverse misure. Secondo la Commissione RUAG International ha reagito in modo adeguato facendo sottoporre la sua sicurezza informatica a una prova di resistenza approfondita da una ditta esterna. Tuttavia la Commissione non comprende perché RUAG International non abbia individuato già prima queste lacune e fatto perciò testare più precocemente i suoi sistemi informatici da una ditta specializzata. La CdG-N ritiene che un simile test debba essere eseguito periodicamente, da un lato nell'interesse della ditta (protezione dei segreti d'affari), dall'altro anche nell'interesse della Confederazione in qualità di proprietaria. Invita pertanto il Consiglio federale, specialmente il DFF, a esaminare se sia possibile e opportuno obbligare RUAG International a eseguire simili test per difendere gli interessi della proprietaria in caso di vendita.

Per quanto concerne lo scorporo, la CdG-N parte dal principio che questo processo terminerà a fine 2021. Ritiene particolarmente importante che RUAG MRO e RUAG International uniscano le loro forze per evitare che sui sistemi di RUAG International rimangano dati sensibili e in particolare dati di RUAG MRO. Nel 2022 la CdG-N chiederà maggiori informazioni in merito e una conferma dell'avvenuta cancellazione.

12 Rapporti del CDF del 22 feb. 2021 (pubblicato) e del 21 ott. 2019 (non pubblicato).
13 Secondo il riscontro presentato da RUAG MRO nell'ambito della consultazione dell'amministrazione, non può essere totalmente escluso un rischio residuo che alcuni supporti di archiviazione dei dati non siano stati registrati. Secondo l'impresa questo rischio è tuttavia molto esiguo, ossia «nell'ordine del per mille».
14 La responsabilità della cancellazione dei dati rilevanti per la sicurezza dei sistemi di RUAG International è ripartita tra le due subholding. RUAG MRO non è deresponsabilizzata fintanto che i dati ripresi per il suo lavoro e migrati nel perimetro della BAC non sono stati cancellati presso RUAG International.

Visti i risultati del CDF secondo cui dati sensibili potrebbero nascondersi anche negli archivi e nei backup e quindi potrebbero passare inosservati e cadere nelle mani di terzi in caso di vendita, la CdG-N si chiede tuttavia se siano necessarie ulteriori misure. In particolare occorrerebbe verificare se la Confederazione, in qualità di proprietaria, non debba obbligare RUAG International, prima di ogni vendita di un'unità, a procedere a una verifica dei dati supplementare e mirata o affidare questo incarico a terzi. La verifica consisterebbe nell'allestire un inventario di tutti i dati e nell'analizzare se tra questi si nascondono ancora dati sensibili di RUAG MRO, dati ITAR o altri. La CdG-N e anche la sua omologa del Consiglio degli Stati discuteranno la questione nel 2022 con la Confederazione in qualità di proprietaria, nello specifico con i suoi rappresentanti presso il DFF e il DDPS.

Raccomandazione 1: protezione dei dati militari e di altri dati sensibili

La CdG-N invita il Consiglio federale ad adottare le misure necessarie per garantire che, dopo la cancellazione pianificata dei dati, RUAG International non disponga effettivamente più di dati militari o di altri dati sensibili (neanche negli archivi o nei backup). Occorre valutare se la cancellazione debba essere verificata anche da esperti esterni. Va altresì esaminata l'opportunità di chiedere un controllo supplementare della situazione dei dati prima di ogni vendita di parti di RUAG International.

3 Reazione della proprietaria

3.1 Misure del DFF e del DDPS

Gli accertamenti della sottocommissione hanno mostrato che il 12 maggio 2021 (ossia una settimana prima della trasmissione) il DDPS ha ricevuto una domanda scritta di presa di posizione da parte del programma televisivo in merito al presunto ciberattacco e ne ha subito informato il DFF. Il capo del DDPS ha indicato alla sottocommissione a più riprese che il presunto attacco concerneva in realtà RUAG International, di cui è competente il DFF. Tuttavia, è stato soltanto il DDPS – e non il DFF o entrambi i dipartimenti – a inviare una presa di posizione al programma televisivo[15].

Il capo del DDPS e il capo del DFF hanno però precisato che i due dipartimenti collaborano strettamente sulle questioni legate a RUAG International e RUAG MRO, in particolare per preparare le sedute del Consiglio di amministrazione di BGRB Holding SA. Dal 1° aprile 2021 la direttrice dell'Amministrazione federale delle finanze (AFF) e il segretario generale del DDPS siedono nel Consiglio di amministrazione, mettendo in pratica quello che la CdG-N chiedeva già da tempo[16]. Il Consiglio federale intende così seguire da vicino lo scorporo e la privatizzazione di RUAG International[17].

15 Parere del DPPS del 15 mag. 2021 (pubblicato).
16 Gestione del ciberattacco contro la RUAG: rapporto della CdG-N dell'8 mag. 2018 (FF **2018** 3895) e del 19 nov. 2019 (FF **2020** 2280).
17 La Confederazione siederà nel Consiglio di amministrazione della RUAG, comunicato stampa del Consiglio federale del 12 mar. 2021.

Il capo del DFF ha indicato che il presunto ciberattacco e le questioni sulla sicurezza informatica sono state trattate nelle riunioni del Consiglio di amministrazione di BGRB Holding il 18 maggio 2021 e il 1° giugno 2021. Il DFF e il DDPS da parte loro non hanno proceduto ad ulteriori accertamenti, valutando la situazione soprattutto in base alle informazioni fornite da RUAG International e dalla ditta esterna da essa incaricata.

Inoltre, il DFF ha dichiarato alla CdG-N anche di non aspettarsi che le asserzioni sul presunto ciberattacco abbiano un impatto negativo sul mantenimento del valore di RUAG International e sulle vendite previste dei settori di attività. Secondo il Dipartimento sono piuttosto informazioni attendibili fornite da RUAG International sullo stato dei suoi sistemi informatici e sui rischi ad essi connessi a essere determinanti. Ha aggiunto che per la Confederazione è essenziale evitare che durante le vendite dati rilevanti per la sicurezza dell'esercito e di RUAG MRO siano trasferiti involontariamente agli acquirenti. Per questo motivo, ha spiegato che RUAG International seguiva le procedure generalmente applicate nell'ambito di vendite di imprese che consistono a separare i sistemi informatici e ad assicurare che i dati trasferiti non contengano malware.

3.2 Valutazione della CdG-N

Secondo il CdG-N occorre chiedersi in particolare se il DFF e il DDPS abbiano reagito in modo adeguato al reportage del programma televisivo e abbiano provveduto a garantire gli interessi della Confederazione in qualità di proprietaria. Ha constatato che i due dipartimenti hanno subito preso in considerazione le asserzioni e le hanno esaminate in seno al Consiglio di amministrazione di BGRB Holding. Il fatto inoltre che dalla primavera 2021 il DFF e il DDPS siedano in questo organo – come chiesto già da tempo dalla CdG-N[18] – dovrebbe se non altro aver migliorato il flusso di informazioni. Viste queste premesse e dato il fatto che RUAG International stessa ha preso le misure necessarie per far luce sulle asserzioni (in particolare incaricando esperti esterni), la Commissione comprende che gli organi federali competenti abbiano rinunciato in questo caso ad avviare anch'essi ulteriori accertamenti. Tuttavia, è legittimo chiedersi se l'esame eseguito da RUAG International non avrebbe dovuto essere svolto da esperti della Confederazione per verificarne l'adeguatezza.

Benché sia indispensabile chiarire la domanda di cui sopra, la CdG-N ritiene però che tanto il DFF quanto il DDPS conferiscano poca importanza al fatto che all'epoca nei sistemi di RUAG International si trovassero ancora dati militari o sensibili (e il rischio che vi si trovino ancora oggi non può essere completamente escluso), come mostrano le spiegazioni riportate sopra relative allo scorporo e le verifiche del CDF. Secondo la CdG-N è quindi difficile comprendere perché il capo del DDPS sottolinei che i dati dell'esercito rilevanti per la sicurezza siano trattati soltanto da RUAG MRO. Parimenti non è sufficiente, durante la vendita di un'impresa, separare i sistemi informatici e assicurare l'assenza di malware nei dati, come dichiarato dal capo del DFF.

18 Cfr. nota a piè di pagina 16.

Come già menzionato qui sopra, la CdG-N si aspetta dalla Confederazione in qualità di proprietaria che garantisca che i dati militari e altri dati sensibili siano effettivamente cancellati dai sistemi della RUAG e che determini se sia necessario effettuare una verifica supplementare prima di una vendita (cfr. n. 2.4, raccomandazione 1)

4 Informazione delle CdG

4.1 Prime informazioni fornite alle CdG sullo stato dello scorporo

Nell'ambito dei suoi accertamenti la CdG-N ha anche esaminato se negli ultimi anni il Consiglio federale, in particolare il DDPS, l'abbia informata correttamente e in tutta trasparenza sullo stato di avanzamento dello scorporo e sulla sicurezza informatica della RUAG. Infatti il Consiglio federale e il DDPS hanno sempre ribadito sia dinanzi alla Commissione sia dinanzi al pubblico che lo scorporo e lo sviluppo del gruppo RUAG erano sulla buona strada nonostante la loro complessità. Ad esempio, il 19 febbraio 2020 il Consiglio federale ha confermato in un parere all'attenzione della CdG-N che lo scorporo sarebbe stato concluso entro metà 2020[19]. Nel giugno 2020 il capo del DDPS ha dichiarato alle sottocommissioni delle CdG che gli elementi principali dello scorporo erano stati attuati sul piano organizzativo nel 2020 e che nella settimana di Pasqua i sistemi informatici di RUAG MRO erano stati migrati con successo nel perimetro di sicurezza della BAC. Nell'aprile 2021 ha indicato alle stesse sottocommissioni che lo scorporo è stato completato secondo le scadenze, precisando che i principali obiettivi organizzativi, giuridici e informatici dello scorporo erano stati realizzati entro fine giugno 2020.

Il rapporto presentato dal Consiglio federale alle CdG il 19 marzo 2021 sul raggiungimento degli obiettivi di RUAG nel 2020 indica invece che i lavori finali dello scorporo sono integrati in un secondo programma. Inoltre, precisa che si tratta soprattutto di rettificare i dati e scorporare i sistemi informatici della TWI e di RUAG Real Estate. Il DDPS ritiene quindi che le CdG siano state informate in maniera trasparente.

I rappresentanti di RUAG MRO hanno dichiarato alla CdG-N che questa seconda tappa era prevista e che in grandi progetti è consuetudine liquidare i lavori residui in un secondo tempo.

19 Parere del Consiglio federale del 19 feb. 2020 in merito al rapporto della CdG-N del 19 nov. 2019 sulla gestione del ciberattacco contro la RUAG; comunicato stampa del Consiglio federale del 24 feb. 2020.

4.2 Valutazione della CdG-N

La Commissione prende atto che il Consiglio federale menziona e descrive più precisamente la seconda tappa dello scorporo nel suo rapporto del 19 marzo 2021. Tuttavia, constata anche che il DDPS non ha mai menzionato questi lavori nelle diverse audizioni. Anzi, ha sempre ribadito che i principali elementi dello scorporo sono stati attuati secondo le scadenze[20]. La CdG-N ritiene quindi che la comunicazione del DDPS – anche nel contesto dei primi accertamenti della CdG – avrebbe dovuto essere più precisa e trasparente. Invita il DDPS e il Consiglio federale a comunicare in futuro con maggiore trasparenza.

Raccomandazione 2: comunicazione trasparente

La CdG-N invita il Consiglio federale ad adottare misure adeguate affinché il Collegio governativo, il DFF e il DDPS con i loro enti proprietari informino in futuro le commissioni di alta vigilanza in modo più trasparente e rapido sulle difficoltà incontrate durante lo scorporo di RUAG e, in particolare, nell'ambito dello sviluppo di RUAG International.

5 Conclusione

Basandosi sulle spiegazioni e sulle conclusioni presentate, la CdG-N ha deciso di concludere i suoi accertamenti sul presunto ciberattacco del 2021. Proseguirà il suo esame degli aspetti critici e delle questioni menzionate nel presente rapporto e li tratterà insieme alla sua omologa del Consiglio degli Stati, in particolare nell'ambito dell'esame annuale del rapporto del Consiglio federale sul raggiungimento degli obiettivi strategici di RUAG. Se sarà necessario, e d'intesa con le altre commissioni competenti, le CdG seguiranno l'evoluzione di RUAG International e i rischi connessivi, concentrandosi sulla questione se la Confederazione assuma il ruolo di proprietaria in modo adeguato.

20 Durante la consultazione dell'amministrazione il DDPS ha constatato che nell'ambito degli obiettivi strategici il Consiglio federale aveva affidato a BGRB Holding l'incarico di concludere i lavori residui entro fine 2021. Secondo il Dipartimento questi lavori residui, che sono stati raggruppati nel settembre 2020 in una seconda tappa di scorporo, sono meno importanti della necessità di eseguire i lavori per l'esercito in un ambiente telematico sicuro. Per questo motivo, il DDPS rimane dell'opinione che l'essenziale dello scorporo sia stato concluso nel giugno 2020 e che la scadenza fissata sia stata quindi rispettata. Ritiene inoltre che il progetto di scorporo di RUAG sia stato concluso con successo. Il CDF lo ha confermato indicando nel suo rapporto di verifica che gli obiettivi del progetto sono stati raggiunti sia sul piano qualitativo sia sul piano quantitativo.

La CdG-N invita il Consiglio federale a prendere posizione sul presente rapporto e sulle sue raccomandazioni entro il 25 marzo 2022.

18 febbraio 2022

In nome della Commissione della gestione del Consiglio nazionale

La presidente, Prisca Birrer-Heimo

La segretaria, Beatrice Meli Andres

Il presidente della sottocommissione DFAE/DDPS, Nicolo Paganini

La segretaria della sottocommissione DFAE/DDPS, Céline Andereggen

Elenco delle abbreviazioni

AFC	Amministrazione federale delle finanze
BAC	Base d'aiuto alla condotta
BGRB	Società di partecipazione delle aziende d'armamento (*Beteiligungsgesellschaft Rüstungsbetriebe*)
CDF	Controllo federale delle finanze
CdG	Commissioni della gestione delle Camere federali
CdG-N	Commissione della gestione del Consiglio nazionale
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DFF	Dipartimento federale delle finanze
ITAR	Quadro normativo degli Stati Uniti sul commercio di armi e l'armamento (*International Traffic in Arms Regulations*)
SG DDPS	Segreteria generale del DDPS
TWI	Infrastruttura scientifica e tecnica (cfr. nota a piè di pagina 9)