Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Gestione del ciberattacco contro la RUAG: punto della situazione

Rapporto della Commissione della gestione del Consiglio nazionale

dell'8 maggio 2018

Compendio

Nel gennaio 2016 il Consiglio federale è stato informato che la RUAG aveva subito un ciberattacco. Siccome in un primo momento il Governo aveva classificato «SEGRETA» l'informazione sull'incidente, l'affare è passato alla Delegazione delle Commissioni della gestione delle Camere federali (DelCG). Dopo che la notizia dell'attacco è stata diffusa, la DelCG ha terminato in ampia misura i suoi lavori sull'affare e lo ha trasmesso alla Commissione della gestione del Consiglio nazionale (CdG-N) per ulteriori accertamenti. I lavori della CdG-N miravano principalmente a chiarire se gli organi federali responsabili – in particolare il Consiglio federale e il DDPS – avevano reagito in maniera adeguata e con la dovuta tempestività all'incidente, tutelando in tal modo gli interessi della Confederazione come azionista unica della RUAG. I lavori non si sono per contro soffermati sulla verifica dell'attuazione delle misure necessarie per affrontare il ciberattacco, poiché questo compito è assunto da altri servizi, in particolare dal CDF.

Nel quadro dei suoi accertamenti la competente sottocommissione della CdG-N ha sentito il capo del DDPS e altri rappresentanti del Dipartimento. Ha altresì analizzato numerosi documenti non solo sull'incidente ma anche sulla gestione della RUAG, come ad esempio i verbali delle sedute periodiche del capo del DDPS con la direzione della RUAG. Siccome le informazioni richieste non le pervenivano sempre puntuali o nella qualità necessaria, per lungo tempo alla Commissione non è stato possibile valutare la situazione. Nel novembre 2017 ha ritenuto di essere finalmente in possesso di una base sufficiente di informazioni per rispondere alle domande essenziali e fare il punto della situazione.

Nel quadro dei suoi accertamenti la Commissione ha ottenuto indicazioni precise sugli elenchi dei dati interessati dall'attacco e sui rischi ad esso connessi. In base alle informazioni raccolte la Commissione ha giudicato grave l'incidente. Ha però anche affermato che il Consiglio federale e il DDPS hanno affrontato l'emergenza con la dovuta tempestività, analizzando i rischi e attuando misure adeguate. Accoglie con favore in particolare che il DDPS abbia messo la RUAG davanti alle sue responsabilità, esigendo dall'impresa una stretta collaborazione.

Basandosi sui suoi accertamenti e sulle verifiche del CDF, la CdG-N constata che le misure adottate in seguito al ciberattacco sono fondamentalmente in atto, con una sola eccezione: la separazione delle reti informatiche della Confederazione e della RUAG ordinata dal Consiglio federale. Questa operazione si è in effetti rivelata molto più complessa e più lunga del previsto. Pur prendendone atto, la Commissione ritiene però anche che questa misura sia importante e che vada attuata con la massima urgenza.

La CdG-N ha anche esaminato come il ciberattacco e le sue conseguenze erano stati recepiti nell'ambito della gestione strategica e come il competente DDPS si era adoperato per tutelare gli interessi della Confederazione in quanto proprietaria. Non era infatti sicura che nei confronti della RUAG il DDPS rappresenti in maniera adeguata gli interessi della Confederazione in quanto proprietaria e riesca anche a farli valere. Ritiene che il DDPS disponga sì degli strumenti appropriati per la

gestione strategica dell'impresa, ma che non li usi sempre in modo adeguato allo scopo. Ad esempio, i colloqui con la proprietaria non sono stati (sufficientemente) messi a profitto per discutere anche di problemi quali il ciberattacco e le relative possibili conseguenze sulla realizzazione degli obiettivi strategici, per porre esigenze o per assegnare mandati. Le discussioni importanti sono state condotte invece in un contesto informale e senza alcuna traccia scritta. Agendo in questo modo, il DDPS si priva non solo di una solida base di informazioni ma anche della possibilità o, più precisamente, di uno strumento con cui imporre le sue richieste e direttive strategiche.

La Commissione si aspetta pertanto dal DDPS che in futuro intervenga in maniera più decisiva presso la RUAG e faccia valere maggiormente le richieste e gli interessi della Confederazione. Rivolge inoltre al Consiglio federale tre raccomandazioni e sollecita da esso diversi accertamenti che dovrebbero indurre miglioramenti nel governo d'impresa.

Rapporto

1 Introduzione

A fine gennaio 2016 il DDPS ha informato la Delegazione delle Commissioni della gestione delle Camere federali (DelCG) che un grave incidente ha compromesso la sicurezza informatica presso l'impresa svizzera di armamento RUAG[1], appartenente alla Confederazione. In un primo momento il Consiglio federale aveva classificato come «SEGRETE» le informazioni relative a questo incidente; la DelCG si è occupata dunque in prima sede di seguirne gli sviluppi. Una volta diffusa la notizia del ciberattacco, la DelCG ha informato il pubblico, il 4 maggio 2016, sui suoi lavori e sui risultati delle sue ricerche. Dato che l'indagine su simili eventi non rientra in linea di massima tra i suoi settori di competenza, la DelCG ha terminato in ampia misura i suoi lavori[2] sull'affare e lo ha trasmesso alle Commissioni della gestione delle Camere federali (CdG) per ulteriori accertamenti[3].

Il 29 giugno 2016 la Commissione della gestione del Consiglio nazionale (CdG-N) ha incaricato la sua sottocommissione DFAE/DDPS di seguire l'attuazione di alcune misure ordinate dal Consiglio federale in seguito al ciberattacco. La sottocommissione ha quindi concentrato i suoi accertamenti sugli aspetti legati alla separazione[4] delle reti del DDPS e della RUAG nonché sulle conseguenze del ciberattacco. Si è chiesta difatti se gli organi federali responsabili – soprattutto il DDPS e la RUAG – avessero reagito in maniera adeguata e con la dovuta tempestività ai problemi venuti alla luce con l'attacco e se le misure adottate si fossero dimostrate efficaci. Nel corso dei suoi lavori si sono inoltre presentate questioni sulla difesa degli interessi della Confederazione e sul ruolo del DDPS come rappresentante della proprietaria, questioni che la sottocommissione ha quindi approfondito.

Durante i suoi lavori la sottocommissione ha esaminato numerosi documenti non soltanto dell'Amministrazione ma anche della RUAG, tra cui diversi documenti sensibili e altamente confidenziali. Ha sentito a più riprese rappresentanti del DDPS, in particolare il capodipartimento, la segretaria generale, il delegato alla ciberdifesa e il capo della gestione delle partecipazioni. Nell'ambito della seduta tenutasi nel maggio 2017 con la direzione della RUAG e incentrata sul rapporto del Consiglio federale relativo al raggiungimento degli obiettivi della RUAG per l'esercizio 2016, la

1 La RUAG (RUAG Holding AG) è stata fondata nel 1997 con la legge federale concernente le imprese d'armamento della Confederazione, quale unità autonoma appartenente al 100 per cento alla Confederazione. Oggi comprende 80 sedi (di cui una metà si trova in Svizzera e l'altra all'estero) e nel 2016 ha conseguito una cifra d'affari netta pari a 1858 mio. di franchi e un utile netto di 116 mio. di franchi, di cui oltre un terzo sotto forma di dividendi a beneficio della Confederazione (cfr. anche n. 4).

2 La DelCG si è concentrata in seguito sugli aspetti dell'incidente legati al Servizio delle attività informative e al diritto penale (cfr. rapporto annuale 2016 delle CdG e della DelCG, FF **2017** 3219, in particolare pag. 3272).

3 Cfr. n. 4.4 del rapporto annuale 2016 delle CdG e della DelCG (FF **2017** 3219, in particolare pag. 3269).

4 La separazione della RUAG concerne non solo l'organizzazione e i processi ma anche le infrastrutture e i sistemi informatici. Nel presente rapporto si intendono tuttavia soltanto i sistemi di informazione e le reti informatiche.

RUAG è ritornata sull'incidente al momento del suo voto sul bilancio 2016 dell'impresa. La sottocommissione ha rinunciato a sentire altri rappresentanti della RUAG, poiché ha chiaramente focalizzato i suoi accertamenti sulle decisioni prese dagli attori della Confederazione e in particolare del DDPS. Tra giugno 2016 e novembre 2017 ha discusso questa tematica in occasione di otto sedute.

La sottocommissione ha avuto più volte difficoltà a procurarsi le informazioni e i documenti desiderati a un punto tale da essere costretta a intervenire presso il Dipartimento, o più precisamente, la Segreteria generale. Siccome le informazioni ricevute non pervenivano puntuali e in parte erano incomplete o non abbastanza chiare, per lungo tempo non le è stato possibile farsi un'idea adeguata della situazione ed effettuarne una valutazione. È soltanto nel novembre 2017 che ha ritenuto di essere in possesso di una base sufficiente di informazioni – benché ancora lacunose – per fare un bilancio delle domande essenziali e concludere provvisoriamente i suoi accertamenti.

Il presente rapporto della CdG-N è pertanto da interpretare come un punto della situazione che contiene da un lato valutazioni e raccomandazioni e dall'altro questioni ancora irrisolte. La maggior parte delle incertezze riguarda in particolare l'attuazione della separazione delle reti del DDPS e della RUAG, operazione che non solo si dimostra essere ben più complessa e lunga di quanto previsto all'inizio, ma anche strettamente legata alla questione della struttura organizzativa e della forma giuridica che dovrà assumere la RUAG nonché alla questione di una privatizzazione (parziale) dell'impresa, e quindi all'influenza che la Confederazione potrà conservare nel gruppo e al ruolo di quest'ultimo come garante dell'equipaggiamento dell'esercito. La CdG-N continuerà quindi a seguire questa tematica.

Nel quadro della consultazione dell'Amministrazione è stato sottoposto per parere al DDPS e alla RUAG il progetto del rapporto della sottocommissione, più precisamente i capitoli relativi ai fatti (correzione di errori formali e materiali). La sottocommissione ha trattato le risposte ottenute dalla consultazione dell'Amministrazione, per poi adattare, ove necessario, il suo rapporto.

Il presente rapporto è strutturato nel seguente modo: il numero 2 si incentra sulle misure adottate in seguito all'attacco, tra cui anche quelle per la separazione delle reti; il numero 3 tematizza i danni del ciberattacco; il numero 4 tratta la gestione strategica della RUAG e il ruolo svolto dal DDPS nella difesa degli interessi della Confederazione in qualità di proprietaria; i numeri 5 e 6 terminano il rapporto presentando le conclusioni e le raccomandazioni della CdG-N.

2 Misure adottate in seguito all'attacco

Nel capitolo qui appresso la CdG-N esamina se le misure volte ad affrontare il ciberattacco sono state adottate in tempo utile e se la loro attuazione sia stata seguita e controllata in maniera adeguata. La valutazione delle misure sul piano materiale non rientra nelle competenze e negli obiettivi della CdG-N, ad eccezione della misura relativa alla separazione delle reti del DDPS e della RUAG (cfr. n. 2.1.3 e 2.2.3). Come già menzionato nell'introduzione, la CdG-N attribuisce a questa misura una

particolare importanza. La sottocommissione competente si è quindi informata a più riprese sullo stato dell'attuazione di questa misura e sui problemi ad essa connessi.

2.1 Fatti

A inizio dicembre 2015 il Servizio delle attività informative della Confederazione (SIC) aveva ricevuto una segnalazione secondo cui l'informatica della RUAG poteva essere nel mirino di un ciberattacco. Ha così contattato immediatamente l'impresa e, un mese e mezzo più tardi, gli specialisti della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI/GovCERT)[5] del DFF hanno potuto rilevare nel sistema della RUAG un malware[6] appartenente alla famiglia di programmi nocivi Turla, attivi da vari anni[7].

La notizia di questa scoperta è stata in seguito comunicata al Comitato ristretto Sicurezza della Confederazione (CrS)[8], quindi anche al Consiglio federale e alla sua Giunta in materia di sicurezza (GSic)[9]. A fine gennaio 2016 il capo del DDPS ha infine informato dell'incidente anche la DelCG.

5 MELANI, creata nell'ottobre 2004, è incaricata dal Consiglio federale di proteggere le infrastrutture critiche in Svizzera, adempiendo i compiti di depistaggio precoce e risoluzione dei problemi che insorgono nell'infrastruttura dell'informazione e della comunicazione. Assiste inoltre gli esercenti di infrastrutture critiche. MELANI è un modello di cooperazione tra il Dipartimento federale delle finanze (DFF), rappresentato dall'Organo direzione informatica della Confederazione (ODIC), e il Dipartimento della difesa, della protezione della popolazione e dello sport (DDPS), rappresentato dal Servizio delle attività informative della Confederazione (SIC). Il GovCERT è stato creato nel 2008 da MELANI per permetterle di reagire ancor più rapidamente agli incidenti.

6 Cfr. n. 4.4 del rapporto annuale 2016 delle CdG e della DelCG (FF **2017** 3219, in particolare pagg. 3269 seg.).

7 Sintesi del 23.5.2017 del rapporto tecnico sul caso di spionaggio alla RUAG (www.melani.admin.ch/dam/melani/it/dokumente/2016/technischer_bericht_apt_case_ruag_summary.pdf.download.pdf/TR-ZF-i.pdf).

8 Il CrS è un organo di politica di sicurezza composto dal segretario di Stato del DFAE, dal direttore del SIC e dalla direttrice di fedpol. Ha il compito principale di osservare e valutare costantemente l'evoluzione della situazione in materia di politica di sicurezza e provvedere all'individuazione tempestiva di sfide nel campo della politica di sicurezza. Il CrS analizza inoltre la situazione in materia di politica di sicurezza, riferisce alla GSic e, se necessario, le presenta proposte.

9 La GSic è un organo del Consiglio federale il cui compito è rafforzare la capacità di condotta del Consiglio federale in materia di politica di sicurezza preparando le deliberazioni e le consulenze del Governo concernenti questioni di politica di sicurezza. La GSic si compone del capo del DFAE, del capo del DFGP e del capo del DFF. Cfr. anche l'ordinanza del 24 ott. 2007 sull'organizzazione della condotta in materia di politica di sicurezza del Consiglio federale, RS **120.71**.

2.1.1 Misure adottate

2.1.1.1 Misure del Consiglio federale

Il 4 febbraio 2016 la GSic ha incaricato il CrS di stimare il danno subito, di valutare i rischi e di esaminare ulteriori misure. Sulla base delle sue prime analisi, il CrS ha proposto al Consiglio federale diverse misure urgenti e una serie di altre misure da attuare a breve o medio termine. Il 23 marzo 2016 il Consiglio federale ha deciso segretamente 14 misure per le quali erano responsabili vari servizi federali – in particolare, naturalmente, del DDPS, ma anche dell'ODIC e dell'UFIT. Ha inoltre fissato le scadenze per l'attuazione e incaricato il CrS di verificarla. L'11 maggio 2016 ha deciso quattro ulteriori misure in reazione al ciberattacco contro la RUAG.

La supervisione dell'attuazione delle misure era ripartita tra diversi attori, tra cui principalmente il DDPS, ossia alcuni servizi del DDPS (cfr. n. 2.1.2), ma in parte anche altri servizi federali come l'UFIT. Questi attori hanno reso conto dei loro lavori al CrS, il quale ha proceduto al monitoraggio dell'attuazione delle misure.

2.1.1.2 Misure del DDPS

Parallelamente alle misure ordinate dal Consiglio federale, anche il DDPS ha adottato diversi provvedimenti che riguardavano essenzialmente le procedure e le verifiche interne al Dipartimento. Molti di questi provvedimenti interessavano la Base d'aiuto alla condotta (BAC) e la Base logistica dell'esercito (BLEs), i due principali partner della RUAG presso il DDPS.

Dopo essere venuto a conoscenza dell'attacco, il capo del DDPS ha istituto la taskforce RHINO[10], il cui scopo era collaborare con la RUAG e gli altri attori coinvolti (tra gli altri SIC, MELANI[11], ODIC[12]) per occuparsi dell'introduzione delle misure urgenti necessarie e della valutazione dei danni subiti. La taskforce ha seguito non solo i provvedimenti del DDPS, ma anche le misure ordinate dal Consiglio federale e le misure interne alla RUAG per ripristinare la sicurezza (cfr. numero qui appresso). La taskforce era in stretto contatto con tutti gli attori interessati a livello della Confederazione e con la RUAG e si teneva regolarmente informata sulle misure prese e sul relativo stato di attuazione. Nonostante alcuni problemi sul piano strategico, in particolare subito dopo la scoperta dell'attacco (collaborazione lacunosa

10 Composta delle persone responsabili della SG-DDPS, dell'esercito, del SIC, di armasuisse e di altri servizi della Confederazione interessati nonché di rappresentanti della RUAG.
11 Cfr. nota 5.
12 L'Organo direzione informatica della Confederazione (ODIC) provvede all'attuazione della strategia in materia di tecnologie dell'informazione e della comunicazione (TIC) nell'Amministrazione federale. Dirige anche la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

con il DDPS; cfr. n. 4.1.3)[13], la collaborazione sul piano operativo e tecnico con la RUAG, stando alle persone sentite del DDPS, ha generalmente funzionato bene[14].

Nel luglio 2016 il capo del DDPS ha trasformato la taskforce in gruppo di lavoro[15], il cui compito era continuare a gestire le conseguenze dell'attacco e a seguire l'attuazione delle misure adottate; doveva inoltre avviare una riflessione più fondamentale su una strategia di gestione delle minacce cibernetiche al DDPS ed elaborare un «Piano di azione Ciberdifesa».

2.1.1.3 Misure della RUAG

Come precisato nell'introduzione, il ciberattacco e il malware utilizzato sono stati scoperti presso la RUAG soltanto grazie alla segnalazione ricevuta dal SIC e dopo ricerche molto intense per le quali l'impresa ha beneficiato dell'aiuto determinante degli specialisti di MELANI. In un secondo momento si è dimostrato che il malware apparteneva a una famiglia di programmi nocivi conosciuta da tempo. Nella sua risposta a un intervento parlamentare il Consiglio federale ha anche sottolineato che già anni addietro tutti gli indicatori tecnici di questa famiglia di programmi nocivi erano stati comunicati, tramite MELANI, a tutti gli esercenti di infrastrutture critiche, tra cui la RUAG, ma che spettava in seguito alle imprese stesse utilizzare queste informazioni per migliorare i loro sistemi di sicurezza[16]. La RUAG ha respinto l'accusa di non aver utilizzato le informazioni di MELANI[17].

Dopo la scoperta del programma nocivo la Confederazione, e più precisamente il DDPS, ha incaricato la RUAG di attuare otto misure urgenti, volte ad arginare i danni, a ripristinare la sicurezza dei sistemi informatici dell'impresa e a migliorarne la sorveglianza. Parallelamente l'impresa ha avviato un proprio programma di misure per aumentare la protezione dai ciberattacchi. Questo programma, detto IMPACT, comprende nove misure di prevenzione, depistaggio e gestione dei ciberattacchi e la sua attuazione, che terminerà presumibilmente a fine 2019, costerà circa 20 milioni di franchi.

In una nota informativa del DDPS al Consiglio federale[18] le misure adottate dalla RUAG sono classificate «corrette». Nella stessa occasione il DDPS fa però notare che il miglioramento della cibersicurezza può essere raggiunto soltanto se le misure

13 Secondo il parere della RUAG presentato nell'ambito della consultazione dell'Amministrazione si trattava in particolare di chiarire le questioni giuridiche, soprattutto quanto all'accesso a documenti classificati di terzi. Inoltre, erano inizialmente limitate anche le risorse umane disponibili che presentavano le giuste conoscenze informatiche e il livello di controllo della sicurezza relativo alle persone richiesto per gestire l'incidente.

14 Audizione del 3.7.2017 della segretaria generale del DDPS e del delegato del DDPS alla ciberdifesa.

15 Il gruppo di lavoro, che si riunisce ogni mese, è composto di oltre 25 persone provenienti da tutti i settori del DDPS. La trasformazione a gruppo di lavoro è stata accompagnata da lievi cambiamenti della sua composizione, soprattutto per quanto concerne la rappresentanza della RUAG: era sì presente nella taskforce, ma non più nel gruppo di lavoro.

16 Risposta del Consiglio federale del 10.6.2016 a una domanda urgente del gruppo PPD del 2.6.2016 (16.1022).

17 Comunicato stampa della RUAG del 16.6.2016.

18 Nota informativa del DDPS al Consiglio federale del 10.4.2017.

sono costantemente sviluppate e sono apportati cambiamenti alla cultura aziendale in materia di sicurezza.

Il DDPS ha chiesto molto tempestivamente alla RUAG di precisare lo scadenziario del programma IMPACT e di rendere conto regolarmente sullo stato dell'attuazione. Dopo aver constatato, secondo le sue dichiarazioni, che non aveva il diritto, in qualità di dipartimento, di chiedere alla RUAG questo genere di informazioni[19], il DPPS ha chiesto al Consiglio federale di esigere che l'impresa gli sottoponesse rapporti trimestrali sui progressi del programma IMPACT[20].

Il DDPS ha tuttavia ritenuto questi rapporti insufficienti e ha quindi chiesto la presentazione di un rapporto più dettagliato prima di fine novembre 2017. Secondo le informazioni ottenute dal DDPS questo nuovo rapporto soddisfa ora le esigenze relative alla qualità e al grado di precisione necessario per permettere una valutazione fondata[21].

2.1.2 Esame delle misure

Come descritto sopra, il DDPS e in particolare l'allora taskforce (oggi gruppo di lavoro) RHINO erano gli organi che si occupavano di garantire il quadro d'insieme delle misure adottate in seguito al ciberattacco ai diversi livelli e di seguirne l'attuazione. Fino a un certo punto il DDPS era anche responsabile della verifica (critica) delle misure, compito che condivideva con il CrS.

Un esame delle misure più approfondito e autonomo è stato però eseguito soprattutto dal Controllo federale delle finanze (CDF) e dalla DelCG.

2.1.2.1 Controllo federale delle finanze

Nella primavera 2016 il CDF ha avviato una verifica dell'attuazione delle misure decise dal Consiglio federale il 23 marzo 2016. Ha poi informato sui risultati la GSic, il CrS e il capo del DDPS nel gennaio 2017 e la DelFin nel marzo 2017.

Sulla base dei suoi accertamenti il CDF è giunto alla conclusione che l'attuazione delle misure, soprattutto di due, una delle quali riguardante la separazione delle reti della Confederazione e della RUAG (cfr. n. 2.1.3), ha richiesto un onere supplementare. Ha infatti sottolineato che questa separazione era più complessa e più lunga del previsto e che queste difficoltà erano prese in considerazione nelle discussioni relative a una privatizzazione parziale della RUAG. Il CDF ha anche comunicato che avrebbe proseguito l'esame dell'attuazione delle misure adottate in seguito al ciberattacco contro la RUAG nel 2017. Il DDPS ha approvato il proseguimento dell'esa-

19 Audizione del 3.7.2017 del delegato del DDPS alla ciberdifesa.
20 Rapporto del 28.6.2017 del DDPS alla sottocommissione.
21 Lettera del 19.12.2017 del delegato del DDPS alla ciberdifesa all'attenzione della sottocommissione.

me e ha proposto al Consiglio federale di incaricare il CDF della sorveglianza duratura della RUAG nel settore della sicurezza informatica[22].

Nel giugno 2017 il CDF ha eseguito un secondo esame e nell'agosto dello stesso anno ha informato il Consiglio federale sullo stato dell'attuazione delle misure che il Governo aveva ordinato. Il CDF ha constatato che le misure erano in gran parte già attuate o stavano per esserlo, tranne quella riguardante la separazione, che avrebbe richiesto ancora del tempo. Il CDF ne riesaminerà l'attuazione nel corso del 2018 e presenterà i risultati entro fine giugno 2018[23].

2.1.2.2 DelCG / CdG

Siccome le informazioni sul ciberattacco non sono state diffuse fino al maggio 2016 e il Consiglio federale le aveva classificate «SEGRETE», all'inizio è stata soprattutto la DelCG a occuparsi dell'attacco e delle sue conseguenze, sentendo a tal proposito diversi rappresentanti del DDPS e della RUAG per discutere le misure da adottare per gestire l'incidente. In un secondo momento si è occupata in particolar modo anche delle competenze e delle strutture necessarie per rimediare alla situazione e ha preso posizione a riguardo in una lettera indirizzata al Consiglio federale[24]. A fine giugno 2017 la DelCG ha deciso di concentrarsi sugli aspetti dell'incidente legati al Servizio delle attività informative e al diritto penale, anche perché da quando l'affare era stato portato all'attenzione dell'opinione pubblica, l'attuazione delle restanti misure poteva essere controllata anche da altri organi e la CdG poteva esercitare l'alta vigilanza sul caso.

Di conseguenza, nell'estate 2016 la sottocommissione DFAE/DDPS della CdG-N si è riunita a più riprese per informarsi sullo stato dell'attuazione delle misure. Il suo principale obiettivo era determinare se gli organi di vigilanza responsabili – in particolare il Consiglio federale e il DDPS – adempivano il loro compito in modo appropriato senza esaminare in dettaglio l'attuazione di ogni misura ordinata, poiché questo, appunto, era l'oggetto degli accertamenti del CDF. Sola eccezione: la misura già menzionata relativa alla separazione delle reti del DDPS e della RUAG (cfr. n. 2.1.3 qui appresso).

2.1.3 Misura «Separazione delle reti del DDPS e della RUAG»

Su proposta della DelCG, la CdG-N ha esaminato in particolar modo l'attuazione della separazione delle reti informatiche[25] della Confederazione e della RUAG. Il Consiglio federale aveva in effetti incaricato il DDPS il 23 marzo 2016 di far sì che la separazione non solo degli affari ma anche dei sistemi tra la Confederazione e la

22 Rapporto del 28.6.2017 del DDPS alla sottocommissione.
23 Stato: 17.1.2018
24 Cfr. n. 4.4 del rapporto annuale 2016 delle CdG e della DelCG (FF **2017** 3219).
25 La separazione delle reti informatiche non si limita alla sola infrastruttura informatica, bensì si estende anche alle prestazioni, ai processi o agli immobili.

RUAG avvenga il più rapidamente possibile[26]. Secondo lo scadenziario iniziale, entro fine settembre 2016 doveva essere elaborato un piano di risanamento che doveva basarsi sui risultati di un'altra misura ordinata dal Consiglio federale in cui il Governo aveva incaricato il DDPS di inventariare entro metà aprile 2016 tutte le connessioni tra il DDPS e la RUAG, incluse le interdipendenze in materia di disponibilità dell'esercito[27].

Abbastanza rapidamente è emerso che già solo l'inventario e in seguito la separazione sarebbero stati molto più complessi del previsto e avrebbero quindi richiesto (molto) più tempo di quanto pianificato. I rappresentanti del DDPS hanno comunicato alla Commissione già nell'ottobre 2016 che la scadenza dell'attuazione della misura relativa alla separazione e quindi dell'elaborazione di un piano di risanamento entro fine marzo 2017 era stata prorogata. Il 10 maggio 2017 il Consiglio federale ha infine concesso al DDPS fino a fine giugno per presentare un rapporto sulle interrelazioni tra la RUAG e l'esercito e illustrarne le possibilità di separazione.

Nel suo rapporto del 21 giugno 2017 al Consiglio federale il DDPS constata che le relazioni tra la RUAG e l'esercito sono molto strette e che oggi l'esercito può espletare molte prestazioni soltanto con l'appoggio della RUAG. Il rapporto descrive dettagliatamente le prestazioni che l'impresa fornisce all'esercito nonché le interdipendenze a livello delle prestazioni, dei processi, dell'informatica e degli immobili. Illustra infine un quadro di cosa significa la separazione («se la RUAG diventasse un normalissimo fornitore di prestazioni esterno del DDPS») e presenta tre varianti di attuazione. Ognuna di queste varianti avrebbe notevoli ripercussioni per l'esercito e la RUAG e andrebbe accuratamente esaminata considerando da un lato l'impiego dell'esercito e dall'altro gli aspetti legati alla politica di sicurezza e all'economia.

Il Consiglio federale ha trattato il rapporto del DDPS nella sua seduta del 28 giugno 2017. Secondo una lettera del 25 ottobre 2017 del DDPS alla sottocommissione competente, ha deciso di sospendere gli accertamenti relativi a una privatizzazione (parziale) della RUAG fino a quando la separazione non sarà realizzata. Dagli ulteriori accertamenti del DDPS e dalle discussioni tra il Dipartimento e la RUAG sarebbe emerso che sono necessari altri accertamenti approfonditi prima di poter sottoporre al Consiglio federale un piano dettagliato sulla separazione (portata del progetto, misure da adottare, volume di lavoro e tempo necessario). Sempre secondo questa lettera il Consiglio federale avrebbe ridiscusso la questione della separazione presumibilmente nel marzo 2018.

Nel quadro delle audizioni il DDPS ha informato la sottocommissione competente che la separazione doveva essere coordinata soprattutto con la riorganizzazione della BAC e che il grado di complessità del compito non permetteva probabilmente di terminare i lavori prima del 2023.

26 Misura 11 secondo la decisione del Consiglio federale del 23.3.2016.
27 Misura 3 secondo la decisione del Consiglio federale del 23.3.2016.

2.2 Valutazione

2.2.1 Misure adottate

Anche se non ha esaminato le misure nel dettaglio, la CdG-N ritiene che esse possano essere in linea di massima considerate opportune. Constata inoltre che il Consiglio federale ha agito rapidamente chiedendo ulteriori delucidazioni al CrS sulla base delle quali ha potuto adottare misure senza perdere tempo[28]. Ha altresì accolto con favore il fatto che la GSic, un comitato del Consiglio federale competente per le questioni in materia di sicurezza[29], si sia occupata molto in fretta dell'incidente.

Constata inoltre che anche il DDPS ha reagito tempestivamente all'incidente e, creando la taskforce RHINO, composta di rappresentanti della RUAG e di tutti gli attori interessati a livello della Confederazione, ha istituito un organismo capace di valutare i danni e prendere misure urgenti. La CdG-N approva anche il buon funzionamento della collaborazione a questo livello più che altro operativo, nonostante all'inizio la direzione della RUAG abbia completamente sottovalutato l'incidente e non si sia sempre dimostrata cooperativa nei confronti del DDPS.

Per quanto concerne le misure della RUAG, la sottocommissione si aspetta che il DDPS continui a seguire la loro attuazione con un occhio critico e migliori o metta a disposizione più fondi laddove necessario. A tal proposito rimanda alla valutazione del DDPS secondo la quale queste misure non saranno sufficienti se non si cambia fondamentalmente anche la «cultura in materia di sicurezza» (cfr. n. 2.1.1.3). Quello che conta è difendere debitamente gli interessi della Confederazione in qualità di proprietaria (cfr. n. 4).

2.2.2 Esame delle misure

La CdG-N accoglie con favore che il Consiglio federale abbia incaricato il CDF, ossia un organo indipendente, di controllare l'attuazione delle misure adottate in seguito al ciberattacco.

A tal proposito invita il Consiglio federale ad esaminare, sulla base delle conclusioni del CDF, l'eventualità di operare taluni cambiamenti nel quadro della condotta strategica dell'impresa, in particolare in vista delle decisioni che saranno prese sulla futura forma organizzativa e giuridica della RUAG e sull'eventuale privatizzazione parziale.

28 Nell'ambito dei suoi accertamenti la DelCG ha constatato che i membri del CrS e i loro uffici non disponevano delle necessarie conoscenze specifiche per poter valutare adeguatamente la situazione di minaccia. Riteneva che per la gestione di questo caso sarebbe stato più opportuno affidarsi direttamente alle strutture ordinarie che il Consiglio federale stesso aveva previsto nell'ordinanza sull'informatica dell'Amministrazione federale (OIAF) (cfr. n. 4.4 del rapporto annuale 2016 delle CdG e della DelCG (FF **2017** 3219, in particolare pag. 3272). I lavori della CdG-N non si sono particolarmente soffermati sulle strutture.

29 Cfr. nota 9.

Raccomandazione 1 Considerare le principali conclusioni nel quadro della gestione strategica

La CdG-N invita il Consiglio federale a valutare, sulla base delle conclusioni del CDF, se sia necessario operare determinati cambiamenti nel quadro della gestione strategica, in particolare nel quadro delle decisioni che saranno prese quanto alla struttura organizzativa e alla forma giuridica della RUAG e quanto a un'eventuale privatizzazione parziale dell'impresa.

2.2.3 Misura «Separazione delle reti del DDPS e della RUAG»

La Commissione prende anche atto che apparentemente le interconnessioni tra le reti della Confederazione e della RUAG sono talmente complesse che una separazione non può essere pianificata come previsto all'inizio e non è realizzabile entro un termine relativamente breve, bensì soltanto entro il 2023. Accoglie però con favore l'intenzione del Consiglio federale di perseguire la separazione e invita il Collegio governativo, e anche in particolare il DDPS, a prendere i provvedimenti necessari e a mettere a disposizione fondi adeguati per concretizzare la separazione entro il termine previsto.

Dal punto di vista della Commissione il ciberattacco contro la RUAG ha esacerbato in maniera generale la problematica della separazione delle reti tra la Confederazione e le unità scorporate. Nel quadro delle misure adottate in seguito al ciberattacco il Consiglio federale ha ordinato un esame critico delle interconnessioni della Confederazione con altre unità scorporate. La Commissione approva questa misura e si aspetta dal Consiglio federale che non perda di vista la problematica e, se necessario, adotti misure. Invita inoltre il Governo ad attribuire la dovuta importanza alla questione della separazione e delle conseguenze ad essa connesse in vista di un'eventuale esternalizzazione o privatizzazione delle unità amministrative.

Raccomandazione 2 Tenere conto della problematica della separazione delle reti in caso di future esternalizzazioni o nel quadro dei principi del governo d'impresa

La CdG-N invita il Consiglio federale a garantire che in caso di future esternalizzazioni la problematica della separazione delle reti sia tenuta in debito conto. In particolare dovrà chiarire se la questione della separazione debba essere considerata nel quadro dei criteri d'idoneità per un'esternalizzazione o nelle direttive e nei rapporti rilevanti in materia di governo d'impresa.

3 Danni causati dall'attacco

Il presente capitolo esamina i danni causati dall'attacco. Poiché le informazioni sulla portata esatta dei danni e sui dettagli dell'attacco sono altamente sensibili, anche la CdG-N si esprime in merito soltanto in forma generica. Avendo tuttavia accesso alle informazioni pertinenti, la sottocommissione competente dispone di sufficienti informazioni su cui basare la descrizione e la valutazione degli elementi qui appresso.

3.1 Fatti

Il 20 luglio 2016, dopo che l'attacco contro la RUAG è stato reso noto, la GSic ha incaricato il CrS di chiarire la portata dei danni e di mostrare al contempo i punti in cui è difficile, se non addirittura impossibile, trarre conclusioni definitive.

Nel rapporto del 25 agosto 2016 il CrS constata che non vi sono indizi per cui il malware era o è ancora attivo anche nei sistemi dell'Amministrazione federale e quindi l'autore dell'attacco aveva o ha ancora accesso ai dati della Confederazione e soprattutto del DDPS. Ritiene tuttavia che le fughe di dati della RUAG erano significative. Il CrS non è in grado di valutare con esattezza i danni per diversi motivi, anche perché la RUAG non ha voluto mettere a disposizione del DDPS tutte le informazioni chieste[30] (vedi anche n. 2.1.1.2). La RUAG è quindi stata invitata a consegnare le informazioni complementari.

Dopo aver ripreso dalla DelCG gli ulteriori accertamenti sul ciberattacco contro la RUAG, la CdG-N ha esaminato il suddetto rapporto del CrS del 25 agosto 2016. Ha in seguito chiesto al DDPS di presentarle un rapporto aggiornato sui danni che si basi sulle informazioni complementari consegnate dalla RUAG dietro richiesta. Il DDPS ha soddisfatto questo invito con un certo ritardo, il 28 giugno 2017, presentando alla sottocommissione il rapporto chiesto[31]. Questo rapporto contiene informazioni dettagliate sugli elenchi interessati dal furto di dati, un'analisi più precisa delle eventuali conseguenze, compresi i rischi, e le misure di protezione adottate. Tuttavia, dal rapporto emerge soprattutto che, per diversi motivi, è impossibile determinare la portata del furto e che la stima degli esperti del DDPS e della RUAG sui danni subiti differisce notevolmente. Mentre la RUAG pone l'accento principalmente sull'aspetto quantitativo fondando il suo parere sul volume dei dati rubati, il DDPS ritiene invece determinante l'importanza dei dati e non il volume in sé.

30 Secondo il parere della RUAG l'impresa non poteva all'inizio fornire al DDPS le informazioni desiderate, poiché dapprima occorreva definire un processo che le permettesse di dare al DDPS anche l'accesso a documenti per i quali essa stessa aveva firmato dichiarazioni di confidenzialità con terzi (dichiarazioni di confidenzialità con collaboratori del DDPS e allestimento di una propria sala protetta in cui potevano essere consultati tutti i documenti critici).

31 Si tratta di un rapporto redatto esclusivamente per la sottocommissione. La CdG-N non sa in quale misura il Consiglio federale o la sua Giunta in materia di sicurezza siano stati informati della nuova stima dei danni.

Il capo del DDPS ha indicato al gruppo di lavoro che la Confederazione e la RUAG avevano stimato i rischi in modo diverso e che la RUAG li aveva chiaramente sottovalutati nella fase immediatamente successiva all'attacco[32]. Tuttavia ha precisato che da allora la collaborazione funzionava bene e che la RUAG aveva adottato diverse misure di miglioramento.

Nel quadro dei suoi accertamenti la sottocommissione competente si è informata a più riprese sulla portata dei danni (finanziari) nonché sulle reazioni dei clienti e le eventuali conseguenze sulle cooperazioni o sui mandati. Siccome nemmeno il DDPS era in possesso di queste informazioni, il Dipartimento ha trasmesso le domande della sottocommissione alla RUAG. Ha in seguito trasmesso le risposte della RUAG alla sottocommissione senza la propria valutazione. Nella lettera che ha inviato alla segretaria generale del DPPS il 15 gennaio 2018, la RUAG spiega che le conseguenze finanziarie del ciberattacco si limitano ai costi generati dalla gestione dell'affare (attuazione delle misure, dispositivo per rispondere alle domande dei clienti) e dal lancio del programma IMPACT[33]. A parte i costi, la RUAG indica di non aver subito danni diretti e di non aver registrato una particolare perdita di clienti subito dopo l'attacco.

3.2 Valutazione

Nel quadro dei suoi accertamenti la CdG-N o, più precisamente, la sottocommissione competente ha ricevuto informazioni dettagliate in merito agli elenchi dei dati interessati dall'attacco e ai rischi ad esso connessi. Su questa base è giunta alla conclusione che l'attacco contro la RUAG deve essere considerato un incidente grave. Afferma inoltre chiaramente che occorre commisurare l'importanza dei dati rubati non solo sotto l'aspetto quantitativo, ma anche qualitativo, condividendo così il parere del DDPS.

La CdG-N prende atto delle informazioni fornite dalla RUAG secondo le quali finora l'impresa non avrebbe subito danni diretti dovuti al ciberattacco e non avrebbe registrato una perdita di clienti. Ritiene tuttavia che un tale incidente non sia sicuramente positivo per gli affari dell'impresa; già questo è motivo sufficiente per attribuire grande importante all'attacco.

In questo contesto non comprende perché la RUAG, una volta scoperto l'attacco, abbia messo in risalto soltanto gli aspetti quantitativi del furto e si sia mostrata poco cooperativa rifiutando di fornire al DDPS tutte le informazioni richieste (per maggiori ragguagli cfr. n. 4). La CdG-N accoglie con favore l'insistenza del DDPS per ottenere le informazioni dalla RUAG, poiché i chiarimenti hanno permesso di effettuare un'analisi dei danni approfondita e soddisfacente nonché di adottare diversi provvedimenti per rimediare ai danni o ridurre i rischi (cfr. n. 2).

32 Audizione del 28.4.2017 del capo del DDPS.

33 I costi del programma IMPACT, che verrà realizzato entro il 2019, ammontano complessivamente a circa 10 mio. di franchi, ai quali si aggiungono costi annuali di circa 1 mio. di franchi per il potenziamento dell'organizzazione e della sicurezza nel settore informatico.

4 Gestione strategica e tutela degli interessi della proprietaria

4.1 Esposizione dei fatti

4.1.1 RUAG: informazioni di base sull'impresa e sulla sua gestione

Base legale e dati principali della RUAG

La RUAG (RUAG Holding SA) è un'impresa d'armamento nata dallo scorporo delle ex aziende d'armamento della Confederazione rese autonome. È una società anonima di diritto privato il cui capitale sociale appartiene interamente alla Confederazione.

Nel 2016 la RUAG contava più di 8500 collaboratori distribuiti in quasi 80 sedi. Circa la metà delle sedi e dei posti si trova in Svizzera (quasi 4500 posti in 39 sedi). La RUAG dispone inoltre di numerose altre sedi in Europa (26) ed è presente anche negli Stati Uniti (7 sedi), in Australia (5 sedi) e in Asia (2 sedi). Nel 2016 ha realizzato un fatturato netto di 1858 milioni di franchi. L'utile netto è stato di 116 milioni di franchi, di cui 47 milioni di franchi sono stati versati sotto forma di dividendi alla Confederazione quale proprietaria.

La base legale della RUAG è costituita dalla legge federale concernente le imprese d'armamento della Confederazione[34]. L'articolo che ne definisce lo scopo stabilisce che la Confederazione può gestire imprese d'armamento «per assicurare l'equipaggiamento dell'esercito»[35]. Ulteriori disposizioni sono inoltre contenute negli statuti della RUAG (scopo, capitale sociale, organi, relativi diritti e obblighi ecc.). Il Consiglio federale gestisce la RUAG secondo i principi formulati nel rapporto sul governo d'impresa del 2006[36], fissandone in particolare gli obiettivi strategici:

Rapporto sul governo d'impresa

Il Consiglio federale ha elaborato il rapporto sul governo d'impresa[37] e i documenti supplementari che lo completano[38] al fine di creare basi migliori per lo scorporo dei compiti delle unità rese autonome e per una maggiore uniformità nella loro gestione. Sono stati inoltre formulati principi guida concernenti gli elementi principali della gestione che riguardano in particolare la presenza di rappresentanti della Confederazione nel consiglio d'amministrazione, il controllo da parte del Consiglio federale e

34 Legge federale del 10 ottobre 1997 concernente le imprese d'armamento della Confederazione (LIAC), RS **934.21**.
35 Articolo 1 della legge federale concernente le imprese d'armamento della Confederazione (LIAC), RS **934.21**.
36 Rapporto del Consiglio federale del 13 settembre 2006 sullo scorporo e la gestione strategica di compiti della Confederazione (Rapporto sul governo d'impresa), FF **2006** 7545.
37 Cfr. nota 33.
38 Rapporto esplicativo dell'Amministrazione federale delle finanze al rapporto sul governo d'impresa del Consiglio federale del 13 settembre 2006 (disponibile in tedesco e in francese); rapporto supplementare del Consiglio federale del 25 marzo 2009 concernente il rapporto sul governo d'impresa (FF **2009** 2225).

gli obiettivi strategici[39]. Gli elementi essenziali contenuti in tali principi guida sono i seguenti:

- *Organi:* gli organi delle unità rese autonome devono disporre delle conoscenze tecniche e aziendali necessarie per esercitare la loro funzione conformemente alle loro responsabilità. Al contempo il Consiglio federale deve anche garantire una tutela adeguata degli interessi della Confederazione in seno al consiglio d'amministrazione o d'istituto. Per questo motivo, nell'esercizio del suo diritto di nomina il Consiglio federale deve anche fare in modo che le persone elette possano identificarsi con le linee direttrici dei suoi obiettivi strategici e garantire che le tutelino in seno al consiglio d'amministrazione o d'istituto.
- *Rappresentanti della Confederazione in seno al consiglio d'amministrazione:* il Consiglio federale deve essere rappresentato in seno al consiglio d'amministrazione, per il tramite di rappresentanti cui possono essere impartite istruzioni, solo laddove questo è necessario, ad esempio se senza tali rappresentanti i suoi interessi non possono essere tutelati in modo adeguato. Il rapporto esplicativo dell'Amministrazione federale delle finanze (AFF) precisa che la presenza di rappresentanti della Confederazione potrebbe essere opportuna in particolare nelle unità con prestazioni sul mercato dotate della forma giuridica della società anonima di diritto privato (per tali unità gli obiettivi strategici non sono giuridicamente vincolanti, cfr. qui di seguito).
- *Controllo del Consiglio federale:* il controllo del Consiglio federale quale proprietario integra la sua funzione di gestione e risponde in linea di principio agli stessi obiettivi. Mira, da un lato, a salvaguardare o ad aumentare il valore e le prestazioni delle unità rese autonome (controllo incentrato sull'impresa) e, dall'altro, a garantire un adempimento dei compiti orientato al bene comune (controllo incentrato sui compiti). Nel caso di società anonime di diritto privato le possibilità di controllo degli azionisti e quindi della Confederazione sono disciplinate dal diritto della società anonima.
- *Obiettivi strategici:* il Consiglio federale dirige le unità rese autonome sul piano strategico, fissandone gli obiettivi di livello superiore da raggiungere a medio termine. Può inoltre formulare direttive concernenti l'impresa e direttive concernenti i compiti. Nel caso della RUAG l'accento è chiaramente posto sulle direttive concernenti l'impresa dato che l'adempimento dei compiti è condizionato e quindi anche guidato principalmente dal mercato. Per il consiglio d'amministrazione di un'unità resa autonoma dotata della forma giuridica di società anonima di diritto privato (come nel caso della RUAG), gli obiettivi strategici non sono giuridicamente vincolanti, ma lo sono di fatto: il consiglio d'amministrazione non può infatti permettersi di ignorare le direttive dell'azionista principale o di maggioranza, altrimenti rischia di essere destituito[40].

39 I restanti elementi della gestione sono i seguenti: forma giuridica, organi, responsabilità, competenze specifiche, alta vigilanza nonché finanze e imposte.

40 Rapporto supplementare del Consiglio federale del 25 marzo 2009 concernente il Rapporto sul governo d'impresa (FF **2009** 2225).

Il Consiglio federale deve controllare annualmente se gli obiettivi sono stati raggiunti. Tale controllo si basa essenzialmente sul rapporto dell'impresa relativo al raggiungimento degli obiettivi, il quale viene esaminato dai dipartimenti competenti. Essi lo discutono con l'impresa e poi informano il Consiglio federale, il quale elabora infine una valutazione indirizzata alle Commissioni di vigilanza del Parlamento (rapporto del Consiglio federale sul raggiungimento degli obiettivi).

Colloqui con la proprietaria

I colloqui periodici tra la Confederazione, quale proprietaria, e le unità rese autonome sono un importante strumento di gestione strategica. Generalmente questi colloqui si svolgono circa quattro volte all'anno. La Confederazione vi è rappresentata dal dipartimento competente – di norma il capodipartimento, il segretario generale così come diversi specialisti – e spesso anche dall'AFF. Dal suo canto l'impresa vi è rappresentata dal presidente del consiglio d'amministrazione, dal direttore e, se necessario, da altri membri della direzione. Durante questi colloqui l'impresa fornisce informazioni sull'andamento degli affari, sulle principali sfide o anche su importanti decisioni strategiche concernenti, ad esempio, cooperazioni con altre imprese o acquisizioni. I rappresentanti della Confederazione valutano queste informazioni nell'ottica degli obiettivi fissati e discutono in particolare i problemi o gli eventi che potrebbero ostacolarne il raggiungimento. Il capodipartimento è responsabile di garantire la tutela degli interessi della proprietaria nei confronti dell'impresa.

4.1.2 Obiettivi strategici per la RUAG

Secondo gli attuali obiettivi strategici[41] la RUAG ha il compito di «assicurare l'equipaggiamento dell'esercito» e i suoi obiettivi «sono in primo luogo orientati agli interessi della Confederazione in quanto azionista della RUAG, ma tengono anche adeguatamente conto degli interessi della Confederazione in quanto cliente importante della RUAG». Oltre alle priorità strategiche concernenti la garanzia dell'equipaggiamento dell'esercito, il Consiglio federale definisce anche obiettivi finanziari – in particolare la distribuzione di un dividendo non al di sotto del 40 per cento dell'utile netto[42] – e obiettivi in materia di partecipazioni, politica del personale e politica regionale.

4.1.3 Gestione della RUAG nel caso del ciberattacco/ tutela degli interessi della proprietaria

Il Consiglio federale e il DDPS hanno reagito al ciberattacco contro la RUAG creando strutture specifiche volte a gestire l'incidente in seno all'Amministrazione federale (in particolare la task force RHINO) e proponendo l'adozione di diverse misure (cfr. n. 2).

41 Obiettivi strategici del Consiglio federale per la RUAG Holding SA 2016–2019.
42 Fino al 2015 tale quota raggiungeva solo il 20 % dell'utile netto.

Qui di seguito si illustra come il DDPS (in qualità di rappresentante del Consiglio federale) ha valutato e gestito l'incidente nel quadro della gestione strategica e del controllo dell'impresa e, di conseguenza, come esso garantisce in generale la tutela degli interessi della Confederazione quale proprietaria.

4.1.3.1 Gestione nel quadro dei colloqui con la proprietaria

I verbali dei colloqui che si sono svolti con la proprietaria[43] in seguito all'incidente[44] contengono poche informazioni sul ciberattacco oppure non ne contengono affatto. Anche se in tre casi l'incidente era all'ordine del giorno, le discussioni al riguardo non sono state verbalizzate[45]. Negli altri tre verbali, in particolare anche in quello del primo colloquio dopo la notizia dell'attacco, l'evento non era all'ordine del giorno e dalla loro analisi emerge che non è stato discusso (o che si è rinunciato alla verbalizzazione della relativa discussione).

L'evento era all'ordine del giorno e la discussione è stata verbalizzata	–
L'evento era all'ordine del giorno, ma la discussione non è stata verbalizzata	*27.6.2016; 8.3.2017; 4.7.2017*
L'evento non era all'ordine del giorno e, secondo i verbali, non è stato discusso	*9.3.2016; 20.9.2016; 13.12.2016*

I verbali mostrano che le conseguenze del ciberattacco non sono mai state discusse in maniera approfondita nel quadro dei colloqui con la proprietaria. Infatti non vengono tematizzate ad esempio le reazioni dei clienti della RUAG in seguito all'incidente, nonostante il DDPS avesse incaricato la RUAG di informare i propri clienti e le loro reazioni potessero avere conseguenze sulla collaborazione così come sui risultati finanziari dell'impresa (di conseguenza, eventualmente anche sull'ammontare dei dividendi versati alla Confederazione). Secondo le dichiarazioni del capo del DDPS, il Dipartimento ha ritenuto che tali informazioni non fossero rilevanti né per il Dipartimento stesso né per la proprietaria. Il capo del DDPS ha dichiarato alla sottocommissione che il Dipartimento non si è mai informato in maniera dettagliata in merito alle reazioni dei clienti. Per quanto a sua conoscenza, la RUAG non ha perso clienti e la Confederazione, quale proprietaria, non ha ricevuto reclami da parte loro[46]. Il DDPS ha chiesto alla RUAG di fornire alla sottocommissione competente informazioni più precise[47].

43 La durata dei colloqui con la proprietaria era di circa due ore ciascuno.
44 La sottocommissione della CdG competente ha ricevuto e analizzato i verbali dei colloqui con la proprietaria che si sono svolti nel 2016 e nel 2017 (2016: 4 verbali del 9.3, 27.6, 20.9, 13.12; 2017: 2 verbali 8.3, 4.7).
45 In un caso la rinuncia alla verbalizzazione è motivata dal fatto che era stata richiesta dal direttore della RUAG. Negli altri due verbali l'assenza di rendiconti non è motivata.
46 Audizione del capo del DDPS del 26.11.2017.
47 Cfr. n. 3.

In linea di massima i verbali contengono pochi elementi che lascino intendere che il DDPS utilizzi tali colloqui per discutere delle sfide e dei problemi da affrontare o eventualmente per presentare richieste all'impresa. Di norma i verbali presentano all'inizio informazioni relativamente dettagliate sull'andamento degli affari della RUAG, a cui seguono temi specifici riassunti spesso solo brevemente. Da un verbale sono emersi indizi di divergenze o perlomeno di lacune nel coordinamento tra il DDPS e l'AFF: il rappresentante dell'AFF ha espresso stupore in merito ad alcune dichiarazioni del capo del DDPS relative allo sviluppo della RUAG, affermando di aver ricevuto in merito informazioni diverse[48].

Oltre ai verbali dei colloqui con la proprietaria, il DDPS compila anche delle liste degli affari in corso. Anche dall'analisi di queste liste[49] non emergono indizi di richieste o incarichi concreti che il DDPS avrebbe indirizzato all'impresa in merito al ciberattacco o ad altri problemi che avrebbero potuto ostacolare il raggiungimento degli obiettivi strategici. In queste liste sorprende in modo particolare la presenza costante da luglio 2017 di un'istruzione che chiede alla RUAG di informare tempestivamente il capo del DDPS nel caso in cui siano stati pubblicati articoli di stampa con implicazioni politiche o in caso di importanti progetti della RUAG sul piano della politica regionale (prima di tale data, l'istruzione riguardava soltanto le decisioni di politica regionale).

Nonostante i verbali e le liste degli affari in corso non contengano quasi nessun indizio esplicito riguardante incarichi assegnati dal DDPS alla RUAG, l'analisi di altri documenti ne dimostra la presenza. In una lettera indirizzata al DDPS circa un mese dopo il colloquio con la proprietaria, la RUAG dichiara infatti di considerare l'acquisizione pianificata di un'impresa come conforme agli obiettivi strategici, facendo riferimento a una discussione orale che aveva avuto luogo in occasione dell'ultimo colloquio con la proprietaria. Nel relativo verbale la RUAG menziona tale acquisizione nel quadro delle informazioni relative all'andamento degli affari, ma in merito non si trovano né domande né incarichi da parte del DDPS.

Per quanto concerne i colloqui con la proprietaria, il capo del DDPS ha precisato che in tale quadro le discussioni riguardano soprattutto gli aspetti generali e finanziari. Le questioni di sicurezza e in particolare le questioni riguardanti le capacità della RUAG nel settore cibernetico non sono invece discusse, non per ultimo, anche per evitare indiscrezioni, dato che a questi colloqui è presente una dozzina di persone. I colloqui con la proprietaria hanno principalmente lo scopo di fornire informazioni sull'andamento degli affari nei singoli settori di attività e sulle sfide da affrontare nell'ottica degli obiettivi strategici. Secondo lui l'AFF, anch'essa presente a tali sedute, è soprattutto interessata a sapere se è opportuno acquistare determinate prestazioni[50]. Il capo del DDPS ha affermato che il ciberattacco e il tema della cibersicurezza sono stati discussi in altri contesti, in particolare in seno al CrS, alla GSic e alla DelCG[51]. Dai documenti analizzati non emerge alcun indizio relativo a una replica formale all'attenzione del capodipartimento. I rappresentanti del DDPS sen-

48 Verbale del 13.12.2016, punto 4.
49 La sottocommissione competente ha potuto ottenere solo le liste degli affari in corso del 2017 (liste del 28.2, 8.3 e 4.7.2017).
50 Audizione del capo del DDPS del 16.11.2017.
51 Cfr. nota 44.

titi, in particolare anche il capodipartimento, hanno dichiarato che il ciberattacco e il tema della cibersicurezza sono stati discussi a più riprese in occasione degli incontri bilaterali tra il capo del DDPS e i rappresentanti della RUAG (cfr. qui di seguito).

Nel complesso si può constatare che, nel quadro formale dei colloqui con la proprietaria, la gestione del ciberattacco contro la RUAG è stata discussa al massimo in maniera marginale oppure non è stata discussa (per quanto concerne il trattamento del tema nel quadro di altri incontri tra il capo del DDPS e i rappresentanti della RUAG, cfr. n. 4.1.3).

4.1.3.2 Gestione nel quadro dei colloqui bilaterali tra il capo del DDPS e la direzione della RUAG

Solitamente, dopo i colloqui con la proprietaria si svolge un colloquio bilaterale tra il capo del DDPS e il presidente del consiglio d'amministrazione della RUAG. Queste discussioni non sono verbalizzate e non hanno luogo ogni volta, come è accaduto ad esempio dopo la prima seduta che ha seguito l'annuncio del ciberattacco. Il DDPS ha consegnato alla sottocommissione una panoramica dei colloqui bilaterali tenutisi tra il capo del DDPS e il presidente del consiglio d'amministrazione o il direttore della RUAG, con indicazioni sommarie sul contenuto delle discussioni. Da tale panoramica emerge che, a gennaio e a febbraio 2016 poco dopo la scoperta dell'attacco, il capo del DDPS ha incontrato tre volte i dirigenti della RUAG, segnalando in tali occasioni la gravità dell'incidente. Nel quadro di altri due colloqui tenutisi ad agosto 2016 e a marzo 2017, le discussioni hanno riguardato le conseguenze e i danni dell'attacco. Durante le audizioni il capo del DDPS e gli altri rappresentanti del Dipartimento hanno dichiarato, in maniera generale, che nel quadro dei colloqui bilaterali tra il capo del DDPS e i rappresentanti della RUAG il ciberattacco è stato senz'altro discusso. Non avendo a disposizione ulteriori documenti concernenti tali colloqui, la sottocommissione non ha potuto verificare queste informazioni.

Il capo del DDPS ha inoltre precisato di aver rinunciato consapevolmente durante i colloqui bilaterali alla stesura dei verbali e alle note personali al fine di evitare che temi sensibili potessero eventualmente essere resi pubblici da un giornalista che ne avrebbe richiesto l'accesso in base alla legge sulla trasparenza (LTras). Secondo il capo del DDPS, l'esperienza ha dimostrato che l'Amministrazione non ha strumenti per poter opporsi a questo tipo di richieste e i tribunali si esprimono sistematicamente a favore della pubblicazione di tali informazioni.

Il capo del DDPS ha inoltre dichiarato di poter contattare direttamente e in qualsiasi momento il presidente del consiglio d'amministrazione della RUAG al di fuori dei colloqui con la proprietaria e dei colloqui bilaterali previsti regolarmente. Ha affermato che questo scambio diretto ha funzionato sempre molto bene, nonostante ci siano state anche accese discussioni («des discussions animées») con il presidente del consiglio d'amministrazione[52].

52 Audizione del capo del DDPS del 26.11.2017.

Da quando la RUAG ha creato un posto per un responsabile delle relazioni con la proprietaria[53] (nota: questa funzione esiste dal 1° settembre 2017), la comunicazione è notevolmente migliorata e le risposte alle richieste sono fornite nei termini fissati.

Le altre persone sentite e l'analisi dei documenti confermano il fatto che la comunicazione con la RUAG, a causa delle circostanze, non sia sempre stata facile, in particolare per quanto concerne le informazioni relative al ciberattacco (cfr. n. 2.1.1.2). Tali documenti mostrano che il DDPS in alcuni casi non ha ricevuto determinate informazioni o che ha dovuto insistere per poterle ottenere (cfr. n. 3 relativo ai danni), in altri, che le informazioni richieste non sono state fornite nei termini previsti o erano incomplete (cfr. n. 2). Durante le audizioni[54] i rappresentanti del DDPS hanno sottolineato più volte che il capodipartimento ha dovuto adoperarsi ripetutamente per poter ricevere sufficienti informazioni e che nel quadro delle relazioni con la RUAG questo aspetto doveva essere migliorato. Secondo loro per il DDPS è molto importante ottenere dal consiglio d'amministrazione informazioni precise sull'andamento degli affari affinché la Confederazione possa assumere pienamente il suo ruolo di azionaria. Per questo motivo, nel corso degli ultimi diciotto mesi sono stati innalzati i requisiti che la RUAG deve soddisfare nella stesura dei rapporti all'attenzione del DDPS.

4.1.3.3 Gestione per mezzo della composizione del consiglio d'amministrazione

Come già menzionato nel numero 4.1.1, in linea di massima la Confederazione deve rinunciare a essere rappresentata direttamente in seno al consiglio d'amministrazione. La presenza di una persona a cui la Confederazione può impartire istruzioni può essere giustificata se senza tali rappresentanti i suoi interessi non possono essere sufficientemente tutelati.

Dato che dopo il ciberattacco la collaborazione tra la Confederazione e la RUAG si è rivelata difficile e il DDPS è dovuto intervenire più volte presso l'impresa per ottenere le informazioni che riteneva necessarie, la CdG-N si chiede se la situazione non sia già di per sé sufficiente a motivare la presenza di rappresentanti in seno al consiglio d'amministrazione al fine di garantire una tutela migliore degli interessi della Confederazione. Secondo la Commissione, a giustificare la presenza di un diretto rappresentante della Confederazione non ci sono solo le tensioni emerse in seguito al ciberattacco, ma anche i complessi lavori in corso sulla separazione della Confederazione e della RUAG, gli accertamenti concernenti la struttura organizzativa e la forma giuridica che la RUAG dovrà assumere nonché la sua parziale privatizzazione.

53 Per occupare la nuova funzione di «vicepresidente Relazioni con la proprietaria», il consiglio d'amministrazione della RUAG ha designato Alexandre Schmidt, ex direttore della Regìa federale degli alcool ed ex membro del consiglio municipale della Città di Berna.

54 Audizione della segretaria generale del DDPS, del delegato del DDPS per la difesa cibernetica e del capo della gestione delle partecipazioni del DDPS del 3.7.2017; audizione della segretaria generale del DDPS e del delegato del DDPS per la difesa cibernetica del 10.10.2016.

A tal proposito il capo del DDPS ha dichiarato che fino a quel momento il Consiglio federale non si era occupato della questione in modo approfondito e ha segnalato la problematica legata alle responsabilità[55]. La segretaria generale del DDPS ha rilevato che la questione relativa alla presenza di un rappresentante della Confederazione in seno al consiglio d'amministrazione era stata discussa al momento della creazione dell'impresa e che sarà nuovamente tematizzata nei dibattiti sul futuro della RUAG[56].

4.1.3.4 Altre constatazioni relative alla gestione e alla tutela degli interessi della proprietaria

Secondo la CdG-N le audizioni e i documenti analizzati hanno inoltre fatto emergere le questioni o constatazioni seguenti relative alla tutela degli interessi della Confederazione quale proprietaria per il tramite del DDPS:

- *Controllo dell'attuazione degli obiettivi strategici:* come già menzionato sopra, secondo quanto dichiarato dai suoi rappresentanti, il DDPS ha innalzato i requisiti che il consiglio d'amministrazione della RUAG deve soddisfare nella stesura dei rapporti. Quest'ultimo deve ora indicare come gli obiettivi, compresi quelli parziali, sono stati attuati nel periodo in rassegna e motivare le differenze rispetto al periodo precedente. Al riguardo occorre menzionare il fatto che nell'autunno 2017 il DDPS ha chiesto alla RUAG di essere informato sulle ripercussioni che la riorganizzazione del settore della cibersicurezza può avere sul raggiungimento degli obiettivi strategici fissati dal Consiglio federale. Nella relativa lettera redatta dal Consiglio federale viene criticato il fatto che, il giorno successivo a un incontro tra la segretaria generale del DDPS e il direttore della RUAG, il capo del Dipartimento ha dovuto apprendere dalla stampa che la RUAG avrebbe soppresso posti di lavoro, in particolare anche nel settore della cibersicurezza. La RUAG ha risposto alle domande del DDPS nei termini previsti. Nel quadro del presente punto della situazione la sottocommissione non è stata più in grado di determinare come il DDPS abbia trattato e valutato tale risposta e se eventualmente sono emerse altre domande o conseguenze.
- *Controllo dell'attuazione delle misure interne adottate dalla RUAG per far fronte al ciberattacco:* come già menzionato al numero 2.1.1.3, il DDPS ha atteso più di un anno prima di chiedere alla RUAG di allestire un rapporto sulle misure adottate e ha dovuto pazientare fino a novembre 2017 prima di ottenere un rapporto che presentasse il livello di qualità e di dettaglio richiesto.

55 Audizione del capo del DDPS 16.11.2017.
56 Audizione della segretaria generale del DDPS del 3.7.2017.

– *Valutazione da parte del DDPS delle misure interne adottate dalla RUAG:* in una nota informativa all'attenzione del Consiglio federale[57] il DDPS ha rilevato che le misure sono «corrette», ma che un miglioramento della cibersicurezza si può ottenere solo tramite uno sviluppo continuo di tali misure e un cambiamento culturale all'interno dell'impresa. Tuttavia, i documenti analizzati e le audizioni non consentono di determinare se tale valutazione abbia avuto conseguenze o se il DDPS sia intervenuto chiedendo ad esempio un aumento dell'impiego di fondi.

– *Partenze in seno al consiglio d'amministrazione o alla direzione della RUAG:* il fatto che diversi temi, considerati importanti dalla CdG-N, non siano discussi nei colloqui con la proprietaria emerge ad esempio dalle partenze registrate in seno all'impresa. L'anno scorso è stato reso noto che il presidente del consiglio d'amministrazione della RUAG non si sarebbe ricandidato per un nuovo mandato. A questo evento si aggiungono le dimissioni di un altro membro del consiglio d'amministrazione e diverse sostituzioni in seno alla direzione dell'impresa (tre degli otto membri hanno lasciato la RUAG). Dai verbali dei colloqui con la proprietaria emerge che questi cambiamenti non sono stati quasi mai tematizzati, nonostante comportino determinati rischi per la proprietaria (in particolare in termini di perdita di competenze). Il capo del DDPS ha dichiarato di non aver influito su tali partenze, ma di essere stato informato sui relativi motivi. I due membri uscenti hanno motivato la propria partenza con un certo malcontento («ingerenza» politica crescente, limitazione dei salari). Il DDPS ha creato una commissione incaricata di assumere personale per tali funzioni perché i profili ricercati non sono facili da trovare, perlomeno in Svizzera[58].

4.2 Valutazione

In base alle constatazioni summenzionate la CdG-N constata in sintesi che non è chiaro il modo in cui il DDPS abbia valutato la gestione del ciberattacco contro la RUAG nel quadro della gestione strategica dell'impresa. Nei colloqui formali con la proprietaria l'incidente è stato tematizzato al massimo in maniera marginale. Anche se il DDPS afferma che il tema è stato affrontato nel quadro dei contatti bilaterali e informali tra il capodipartimento e i rappresentanti della RUAG, le discussioni al riguardo non sono state in alcun modo verbalizzate o documentate per scritto.

Considerati gli elementi di cui sopra, la CdG-N solleva diverse questioni di fondo e si chiede se il DDPS sia in grado di rappresentare e far valere nel modo adeguato gli interessi della Confederazione quale proprietaria nei confronti della RUAG. La Commissione ritiene che il DDPS abbia difficoltà a tutelare gli interessi della proprietaria, nonostante la RUAG appartenga interamente alla Confederazione.

57 Nota informativa del DDPS all'attenzione del Consiglio federale del 10.4.2017.
58 Audizione del capo del DDPS del 16.11.2017.

Questa situazione è certamente legata al comportamento non cooperativo della RUAG stessa, la quale si appella regolarmente alla propria autonomia. Secondo la CdG-N tale autonomia è incontestabile, ma non autorizza l'impresa a privilegiare i propri interessi economici rispetto alle richieste e al volere della proprietaria. A differenza dell'indipendenza delle autorità di vigilanza e di regolazione, l'indipendenza della RUAG è da intendersi non tanto come «un'indipendenza da influenze politiche», ma come un privilegio che concerne le attività operative. Tuttavia la gestione del ciberattacco di gennaio 2016 non riguarda soltanto il piano operativo, bensì solleva chiaramente anche questioni di natura strategica che coinvolgono la Confederazione quale proprietaria. In situazioni straordinarie come quella del ciberattacco contro la RUAG che ha comportato determinati rischi non solo per lo sviluppo del valore dell'impresa, ma anche per la sicurezza della Svizzera, la Confederazione deve garantire di essere in grado di definire in modo chiaro, per il tramite del consiglio d'amministrazione, gli orientamenti strategici dell'impresa. Ovviamente tali scelte possono, in definitiva, avere ripercussioni sul piano operativo.

È quindi evidente che anche la Confederazione, in particolare il DDPS, è corresponsabile della tutela degli interessi della proprietaria che, secondo la Commissione, si è rivelata lacunosa. Come illustrato in precedenza, dai verbali dei colloqui con la proprietaria non emerge una volontà reale di gestire (strategicamente) la RUAG e di far valere gli interessi della Confederazione. A tal proposito, la CdG-N critica in particolare anche la scelta di utilizzare canali evidentemente poco formali per influire sulla situazione e il fatto che tali contatti bilaterali non siano stati verbalizzati. Secondo la CdG-N questa prassi è già discutibile in periodi normali, ma si rivela semplicemente inaccettabile in situazioni di crisi come quella emersa in seguito al ciberattacco. Infatti, se le discussioni e le decisioni importanti non sono documentate, il DDPS si priva non solo di una solida base di informazioni, ma anche di uno strumento di gestione che gli permetterebbe di imporre scelte strategiche sul lungo periodo.

A differenza del capo del DDPS, la CdG-N è convinta che i colloqui con la proprietaria non debbano servire soltanto a ottenere informazioni sull'andamento degli affari dell'impresa, ma anche a discutere di problemi di fondo e a formulare richieste, in particolare quando tali problemi possono avere ripercussioni sui risultati finanziari. Se tali discussioni non hanno luogo tra l'altro per timore di indiscrezioni, occorre rivedere le modalità di questi colloqui ed eventualmente anche la cerchia dei partecipanti, invece di ripiegare su canali informali non documentati. A tal proposito, anche la motivazione del capo del DDPS, il quale ha dichiarato di aver rinunciato a verbali e note concernenti i colloqui per timore di richieste basate sulla LTras, non convince la Commissione.

Alla fine tutto questo porta il DDPS a non disporre di informazioni che sarebbero importanti per la proprietaria. A tal proposito, la CdG-N non ha potuto comprendere, ad esempio, le ragioni per cui evidentemente il DDPS non ha mai chiesto informazioni riguardo alle reazioni dei clienti dopo che essi erano stati informati nel dettaglio sul ciberattacco. A differenza della Commissione, il DDPS non considera queste informazioni come rilevanti, mentre potrebbero fornire indizi molto utili al fine di valutare la futura collaborazione con i clienti e lo sviluppo dell'andamento degli ordini della RUAG. Le informazioni relative allo sviluppo dell'andamento degli

affari e a quello degli ordini sono senza dubbio importanti per la proprietaria, soprattutto perché possono influire sul raggiungimento degli obiettivi dell'impresa e quindi sui dividendi della Confederazione.

Inoltre, considerate le diverse sfide legate alla RUAG – gestione del ciberattacco, separazione delle reti della Confederazione e della RUAG, accertamenti sulla futura forma organizzativa e giuridica dell'impresa nonché la sua parziale privatizzazione – per la Commissione è incomprensibile che il DDPS e il Consiglio federale non si siano finora occupati in modo approfondito della questione concernente una rappresentanza (anche solo temporanea) nel consiglio d'amministrazione della RUAG. Nel rapporto sul governo d'impresa questo è esplicitamente previsto nei casi in cui la Confederazione non è in grado di tutelare sufficientemente i propri interessi senza rappresentanti.

Nel complesso la CdG-N ritiene che esistano gli strumenti necessari per far valere gli interessi della Confederazione quale proprietaria nei confronti della RUAG, ma che non siano utilizzati nella maniera adeguata, in particolare dal DDPS.

Raccomandazione 3 Ricorrere in modo adeguato agli strumenti di gestione per tutelare gli interessi della proprietaria

La CdG-N chiede al Consiglio federale di spiegare in che modo intende garantire un ricorso adeguato agli strumenti di gestione e quindi migliorare la tutela degli interessi della proprietaria.

In particolare, la gestione strategica non deve avvenire durante contatti informali, ma nel quadro dei colloqui con la proprietaria. La CdG-N si aspetta anche che le discussioni e le decisioni importanti siano documentate per scritto. Chiede infine al Consiglio federale, alla luce delle sfide da affrontare, di valutare in modo approfondito la presenza (perlomeno temporanea) di un rappresentante cui poter impartire istruzioni nel consiglio d'amministrazione della RUAG.

La CdG-N spera inoltre che l'elezione del nuovo presidente del consiglio d'amministrazione consenta di creare le basi per una collaborazione ottimale tra la proprietaria e il consiglio d'amministrazione.

5 Conclusioni

Sulla base dei suoi accertamenti la CdG-N giunge alla conclusione che, in seguito alla notizia del ciberattacco contro la RUAG, la Confederazione ha reagito con l'urgenza necessaria adottando misure adeguate. Il Consiglio federale e il DDPS hanno gestito l'incidente con rapidità e nel modo opportuno. Per contro, i dirigenti della RUAG hanno impiegato più tempo a riconoscere la portata dell'attacco e i rischi ad esso correlati e ad adottare le proprie misure. La CdG-N apprezza pertanto il fatto che il DDPS abbia fatto pressione sulla RUAG e sia intervenuto a più riprese a causa del comportamento inizialmente poco cooperativo dell'impresa. La CdG-N considera inoltre opportuno che il Consiglio federale incarichi il CDF di verificare l'attuazione delle misure richieste. Prende atto del fatto che le principali misure volte

a separare le reti della Confederazione e della RUAG sono complesse e dispendiose in termini di tempo. Ciononostante, ritiene che sia molto urgente portarne avanti l'attuazione. Per quanto concerne le misure avviate dalla RUAG stessa, la Commissione si aspetta che il DDPS quale rappresentante della proprietaria ne accompagni in modo critico l'attuazione e, se necessario, intervenga.

Nel quadro dei suoi accertamenti la CdG-N ha inoltre ricevuto precise informazioni sugli elenchi di dati interessati dall'attacco e sui rischi che ne conseguono. Sulla base di queste informazioni, classifica l'incidente come grave. La CdG-N prende atto del fatto che la RUAG, secondo quanto dichiarato, non abbia finora subito alcun danno economico diretto. Siccome un incidente di questo tipo può avere anche ripercussioni indirette o sul lungo termine sull'andamento degli affari, le conseguenze non devono essere sottovalutate.

Una questione di fondo che la CdG-N ha cercato di chiarire nel quadro del presente rapporto riguarda la tutela degli interessi della Confederazione quale proprietaria della RUAG. A tale scopo, la Commissione ha esaminato in che modo il ciberattacco è stato valutato nel quadro della gestione strategica, in particolare nei colloqui con la proprietaria, che hanno luogo ogni trimestre tra il capo del DDPS e i dirigenti della RUAG. Ha altresì esaminato in che modo la Confederazione e il DDPS hanno garantito che l'impresa tenesse (sufficientemente) conto degli interessi della Confederazione quale proprietaria. A tal proposito, la Commissione giunge anche a conclusioni critiche in cui ritiene essenzialmente che il DDPS debba mostrarsi più deciso nei confronti della RUAG e far valere maggiormente gli interessi della proprietaria. La RUAG appartiene infatti interamente alla Confederazione. Nel settore privato anche gli azionisti di minoranza sono in grado di esercitare una pressione considerabile sull'impresa quando detengono un'importante quota di azioni[59].

Secondo la CdG-N gli strumenti a disposizione per poter influire sull'impresa sono sufficienti. A suo avviso è molto importante fissare degli obiettivi strategici e controllare che siano raggiunti, in particolare anche nel quadro dei regolari colloqui con la proprietaria. La CdG-N ritiene che questi colloqui debbano essere utilizzati non solo per ottenere informazioni sull'andamento degli affari, ma anche per discutere di problemi fondamentali, come nel caso del ciberattacco, e delle loro eventuali conseguenze sul raggiungimento degli obiettivi. Tali colloqui rappresentano anche l'occasione per esprimere richieste o per assegnare mandati, in altre parole per tutelare gli interessi della proprietaria. Pertanto, la CdG-N giudica incomprensibile che la gestione del ciberattacco e le sue conseguenze non siano state quasi mai discusse sul piano strategico nel quadro dei colloqui tra il DDPS e la RUAG. La Commissione riconosce che non spetta al Consiglio federale gestire l'impresa sul piano operativo. Tuttavia, ritiene che il Consiglio federale e il DDPS debbano intervenire quando sul piano operativo si presentano problemi che possono ostacolare gli interessi della proprietaria, toccando così anche il piano strategico.

59 Cfr. ad es. il caso di Credit Suisse in cui un investitore, che di fatto era un fondo d'investimento che deteneva circa lo 0,3 % del capitale sociale, ha chiesto nell'autunno 2017 di dividere la banca in più parti e ha aumentato pubblicamente la pressione in questo senso, nonostante le possibilità di successo sembrassero minime (NZZ del 17.10.2017: *Hedge-Fund will die Credit Suisse aufspalten – und jetzt?*).

La CdG-N è inoltre persuasa che le discussioni importanti non debbano essere condotte in un semplice quadro informale senza documentarne per scritto e in modo adeguato i punti chiave. In questo modo il DDPS si priva infatti non solo di una solida base di informazioni ma anche della possibilità o, più precisamente, di uno strumento con cui imporre le sue richieste e direttive strategiche. La mancanza di documentazione indebolisce la posizione della proprietaria e rende complicata la tutela dei suoi interessi sul lungo termine.

La nomina del consiglio d'amministrazione rappresenta un altro importante strumento di gestione strategica. La Commissione è dell'opinione che, a partire dalla nomina dei membri e soprattutto del presidente del consiglio d'amministrazione, occorra garantire che i candidati appoggino gli obiettivi del Consiglio federale e si impegnino affinché siano raggiunti. Se non dovesse essere il caso, occorrerebbe intervenire anche su questo piano.

La CdG-N si aspetta pertanto che in futuro il DDPS si mostri più deciso nei confronti della RUAG e, se necessario, si impegni maggiormente in favore delle richieste della Confederazione e dei suoi interessi quale proprietaria. Nelle tre raccomandazioni all'attenzione del Consiglio federale la Commissione chiede invece a quest'ultimo diverse chiarificazioni al fine di migliorare il governo d'impresa.

6 Seguito della procedura

La CdG-N chiede al Consiglio federale di prendere posizione sulle analisi e richieste formulate al più tardi entro il *28 settembre 2018*.

8 maggio 2018

In nome della Commissione della gestione del Consiglio nazionale:

La presidente della CdG-N,
consigliera nazionale Doris Fiala

La presidente della sottocommissione DFAE/DDPS,
consigliera nazionale Ida Glanzmann-Hunkeler

La segretaria delle CdG,
Beatrice Meli Andres

La segretaria della sottocommissione DFAE/DDPS,
Céline Andereggen

Elenco delle abbreviazioni

AFF	Amministrazione federale delle finanze
CDF	Controllo federale delle finanze
CdG	Commissioni della gestione
CdG-N	Commissione della gestione del Consiglio nazionale
CrS	Comitato ristretto Sicurezza
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DelCG	Delegazione delle Commissioni della gestione
DelFin	Delegazione delle finanze delle Camere federali
DFAE	Dipartimento federale degli affari esteri
DFF	Dipartimento federale delle finanze
GSic	Giunta del Consiglio federale in materia di sicurezza
ODIC	Organo direzione informatica della Confederazione
SIC	Servizio delle attività informative della Confederazione
UFIT	Ufficio federale dell'informatica e della telecomunicazione

Elenco delle persone sentite

Falcone-Goumaz, Nathalie*	Segretaria generale del DDPS
Fischer, Peter	Delegato / capo dell'ODIC
Frauenknecht, Marcel	Capo della sezione Sicurezza TIC dell'ODIC
Parmelin, Guy*	Consigliere federale, capo del DDPS
Rothenbühler, Stephan	Capo della gestione delle partecipazioni del DDPS, SG DDPS
Vernez, Gérald*	Delegato del DDPS per la difesa cibernetica

* *Persone sentite più volte*