Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Standortbestimmung: Bewältigung des Cyber-Angriffs auf die RUAG

Bericht der Geschäftsprüfungskommission des Nationalrates

vom 8. Mai 2018

Das Wichtigste in Kürze

Im Januar 2016 wurde ein Cyber-Angriff auf die RUAG aufgedeckt und der Bundesrat informiert. Dieser stufte die Informationen zu diesem Vorfall zunächst als geheim ein, weshalb sich die Geschäftsprüfungsdelegation (GPDel) der Eidgenössischen Räte damit befasste. Nachdem der Angriff auch öffentlich bekannt wurde, schloss die GPDel ihre Arbeiten in dieser Sache weitestgehend ab und übergab das Geschäft für die weiteren Abklärungen an die Geschäftsprüfungskommission des Nationalrates (GPK-N). Diese legte den Fokus ihrer Abklärungen insbesondere auf die Frage, ob die verantwortlichen Bundesstellen – insbesondere der Bundesrat und das VBS – angemessen und mit der nötigen Dringlichkeit auf den Vorfall reagiert hatten und ob sie dabei auch die Wahrung der Eignerinteressen des Bundes sicherstellten. Die Prüfung der Umsetzung der Massnahmen zur Bewältigung des Cyber-Angriffs stand dagegen nicht im Fokus, da diese Aufgabe bereits durch andere Stellen, insbesondere durch die EFK, wahrgenommen wird.

Im Rahmen ihrer Abklärungen hörte die zuständige Subkommission der GPK-N den Vorsteher und weitere zuständige Personen des VBS an, ebenso analysierte sie zahlreiche Unterlagen zum Vorfall sowie zur Steuerung der RUAG wie beispielsweise die Protokolle der regelmässigen Sitzungen des Vorstehers VBS mit der RUAG-Leitung. Da die erhaltenen Informationen nicht immer fristgerecht oder in der erforderlichen Qualität eintrafen, war es der Kommission lange nicht möglich, eine Bewertung vorzunehmen. Im November 2017 kam sie zum Schluss, dass sie nun eine genügende Informationsbasis hat, um die wesentlichen Fragen zu beantworten und eine Standortbestimmung vorzunehmen.

Die Kommission erhielt im Rahmen ihrer Abklärungen detaillierte Angaben über die vom Angriff betroffenen Datenverzeichnisse und die damit verbundenen Risiken. Auf der Basis dieser Informationen stuft sie den Vorfall als gravierend ein. Sie stellte aber auch fest, dass der Bundesrat und das VBS rasch und angemessen auf den Vorfall reagiert haben, indem sie die Risiken analysierten und entsprechende Massnahmen anordneten. Sie begrüsst insbesondere, dass das VBS diesbezüglich auch die RUAG in die Pflicht nahm und eine enge Kooperation forderte.

Gestützt auf ihre Abklärungen und die bisherigen Prüfungen der EFK stellt die GPK-N fest, dass die Umsetzung der Massnahmen zur Bewältigung des Cyber-Angriffs grundsätzlich auf Kurs ist. Eine Ausnahme bildet die vom Bundesrat angeordnete Entflechtung der IT-Netze von Bund und RUAG. Diese stellte sich als weit komplexer und zeitaufwendiger heraus als erwartet. Die Kommission nimmt dies zu Kenntnis, ist aber auch der Ansicht, dass diese wichtig ist und daher mit grosser Dringlichkeit vorangetrieben werden muss.

Die GPK-N prüfte auch, wie der Cyber-Angriff und dessen Folgen im Rahmen der strategischen Steuerung aufgenommen wurden und wie sich das VBS als Eignervertreter für die Wahrung der Eignerinteressen des Bundes einsetzte. Dabei ergaben sich Zweifel, ob das VBS die Eignerinteressen des Bundes gegenüber der RUAG angemessen vertritt und auch durchsetzen kann. Die GPK-N ist der Ansicht, dass das VBS zwar über die nötigen Instrumente zur strategischen Steuerung verfügt,

diese aber nicht immer zweckmässig nutzt. So werden die Eignergespräche beispielsweise nicht (genügend) genutzt, um auch Probleme wie ein Cyber-Angriff sowie deren mögliche Folgen für die Erreichung der strategischen Ziele zu diskutieren, Forderungen zu stellen oder Aufträge zu erteilen. Stattdessen werden wichtige Diskussionen in einem informellen Rahmen geführt und nirgends schriftlich festgehalten. Auf diese Weise fehlt dem VBS nicht nur eine solide Informationsgrundlage, sondern auch die Möglichkeit bzw. ein Instrument, um Forderungen und strategische Vorgaben durchzusetzen.

Die Kommission erwartet daher vom VBS, dass es in Zukunft gegenüber der RUAG bestimmter auftritt und sich bei Bedarf stärker für die Forderungen des Bundes bzw. die Wahrung der Eignerinteressen einsetzt. Sie richtet zudem drei Empfehlungen an den Bundesrat und verlangt von diesem verschiedene Abklärungen, welche zu Verbesserungen der Corporate-Governance führen sollen.

Bericht

1 Einleitung

Ende Januar 2016 informierte das VBS die Geschäftsprüfungsdelegation der Eidgenössischen Räte (GPDel) über eine schwerwiegende Beeinträchtigung der Informatiksicherheit beim schweizerischen Rüstungsunternehmen RUAG[1], welches dem Bund gehört. Zunächst stufte der Bundesrat die Informationen zu diesem Vorkommnis als geheim ein, so dass zuerst die GPDel die weitere Entwicklung begleitete. Nachdem der Cyber-Angriff aber öffentlich bekannt wurde, informierte die GPDel die Öffentlichkeit am 4. Mai 2016 über ihre Arbeiten und Erkenntnisse. Da die Aufarbeitung solcher Vorkommnisse grundsätzlich nicht zum Zuständigkeitsbereich der GPDel gehören, schloss sie ihre Arbeiten in dieser Sache weitestgehend ab[2] und übergab das Geschäft für weitere Abklärungen den Geschäftsprüfungskommissionen (GPK) der Eidgenössischen Räte.[3]

Die GPK des Nationalrates (GPK-N) beschloss am 29. Juni 2016, dass ihre Subkommission EDA/VBS die Umsetzung gewisser Massnahmen zur Bewältigung des Vorfalls begleiten solle, welche der Bundesrat als Konsequenz des Cyber-Angriffs in Auftrag gegeben hatte. Die Subkommission legte in der Folge die Schwerpunkte ihrer Abklärungen insbesondere auf die Massnahme bezüglich der Entflechtung[4] der Netze von VBS und RUAG sowie auf die Konsequenzen für die RUAG aus der Cyber-Attacke. Sie stellte sich dabei die Frage, ob die Probleme, die durch den Angriff aufgedeckt wurden, durch die verantwortlichen Stellen – hauptsächlich durch das VBS und die RUAG – angemessen und mit der nötigen Dringlichkeit angegangen wurden und ob die getroffenen Massnahmen Wirkung zeigten. Im Verlaufe ihrer Arbeiten kamen zudem Fragen zur Wahrung der Eignerinteressen des Bundes und zur Rolle des VBS als Eignervertreter auf, so dass auch diese Thematik vertieft wurde.

Im Rahmen ihrer Untersuchungen wertete die Subkommission zahlreiche Dokumente der Verwaltung, aber auch der RUAG aus, darunter verschiedene heikle und streng vertrauliche Dokumente. Sie hörte zudem mehrmals Vertreter des VBS an, insbesondere den Vorsteher des VBS, die Generalsekretärin des VBS, den Delegierten für Cyber-Defence des VBS sowie den Leiter Beteiligungsmanagement VBS. Im Rahmen der Sitzung vom Mai 2017 zum Bericht des Bundesrates über die Zielerrei-

1 Die RUAG (RUAG Holding AG) wurde 1997 per Gesetz (Bundesgesetz über die Rüstungsunternehmen des Bundes) als verselbständigte Einheit geschaffen und ist zu 100 % im Besitz des Bundes. Sie ist heute an fast 80 Standorten tätig (davon befinden sich je rund die Hälfte in der Schweiz und im Ausland) und erzielte 2016 einen Nettoumsatz vom 1858 Mio. Franken und einen Reingewinn von 116 Mio. Franken, wovon mehr als ein Drittel als Dividende an den Bund ging (vgl. auch Kap. 4).

2 Die GPDel konzentrierte sich in der Folge auf die nachrichtendienstlichen und strafrechtlichen Aspekte des Vorfalls (vgl. Jahresbericht 2016 der GPK und GPDel, BBl **2017** 3794).

3 Vgl. Kap. 4.4 im Jahresbericht 2016 der GPK und GPDel (BBl **2017** 3792).

4 Die Entflechtung der RUAG betrifft deren Organisation, die Prozesse, die IKT-Infrastrukturen und -Systeme. Im vorliegenden Bericht ist damit nur die Entflechtung von Informationssystemen und Informatiknetzwerken gemeint.

chung der RUAG im Jahr 2016 mit der Unternehmensspitze der RUAG thematisierte diese den Vorfall in ihrem Votum zum Jahresrückblick. Auf weitere Anhörungen von RUAG-Vertretern wurde verzichtet, da die Subkommission bei ihren Abklärungen den Fokus klar auf das Verhalten der Akteure des Bundes und insbesondere des VBS legte. Die Subkommission befasste sich zwischen Juni 2016 und November 2017 insgesamt an acht Sitzungen mit diesem Thema.

Die Subkommission stiess dabei verschiedentlich auf Schwierigkeiten bei der Beschaffung von Informationen und Unterlagen und musste deshalb beim Departement bzw. beim Generalsekretariat des VBS intervenieren. Da die erhaltenen Informationen verschiedentlich nicht fristgerecht eintrafen und teilweise nicht vollständig oder zu wenig klar waren, war es ihr lange nicht möglich, sich ein angemessenes Bild der Situation zu verschaffen und zu einer Bewertung zu kommen. Erst im November 2017 kam sie zum Schluss, dass sie nun trotz einzelnen weiterhin fehlenden Informationen eine genügende Informationsbasis hat, um die wesentlichen Fragen im Sinne einer Standortbestimmung zu beantworten und ihre Abklärungen vorläufig abzuschliessen.

Der vorliegende Bericht der GPK-N ist daher als Standortbestimmung zu verstehen und enthält neben Bewertungen und Empfehlungen auch einige noch offene Fragen. Insbesondere stellen sich noch verschiedene Fragen bezüglich der Umsetzung der Entflechtung der Netze zwischen VBS und RUAG, welche bedeutend komplexer ist und mehr Zeit benötigt, als ursprünglich gedacht. Diese Thematik ist auch stark mit der Frage bezüglich der künftigen Organisations- und Rechtsform bzw. bezüglich der (Teil-)Privatisierung der RUAG und damit auch mit Überlegungen über den künftigen Einfluss des Bundes auf die Firma und deren Rolle für die Sicherstellung der Ausrüstung der Armee verbunden. Die GPK-N wird diese Thematik daher weiterverfolgen.

Im Rahmen der Verwaltungskonsultation wurde dem VBS und der RUAG der Berichtsentwurf der Subkommission bzw. die sie betreffenden Kapitel zum Sachverhalt zur Stellungnahme zugestellt (Korrektur von formellen und materiellen Fehlern). Die Rückmeldungen aus der Verwaltungskonsultation wurden anschliessend von der Subkommission behandelt und der Bericht wo nötig angepasst.

Der vorliegende Bericht ist wie folgt aufgebaut: Das zweite Kapitel widmet sich den Massnahmen zur Bewältigung des Angriffs, dazu gehört auch die Massnahme bezüglich einer Entflechtung der Netze. Das Kapitel 3 thematisiert den Schaden der Attacke. Das vierte Kapitel dreht sich um die strategische Steuerung der RUAG und die Wahrung der Eignerinteressen des Bundes durch das VBS. Der Bericht schliesst mit den Schlussfolgerungen und Empfehlungen in den Kapiteln 5 und 6.

2 Massnahmen zur Bewältigung des Angriffs

Im folgenden Kapitel liegt der Fokus auf der Frage, ob die Massnahmen zur Bewältigung des Cyber-Angriffs innert nützlicher Frist eingeleitet und deren Umsetzung zweckmässig begleitet bzw. geprüft wurde. Es ist hingegen nicht Aufgabe und Ziel der GPK-N, eine inhaltliche Bewertung der einzelnen Massnahmen vorzunehmen. Eine Ausnahme bildet dabei die eingeleitete Massnahme bezüglich einer Entflech-

tung der Netze von VBS und RUAG (vgl. Kap. 2.1.3 und 2.2.3). Wie bereits in der Einleitung erwähnt, legte die GPK-N hier einen besonderen Schwerpunkt. Die zuständige Subkommission liess sich daher mehrfach über den Stand der Umsetzung dieser Massnahme und die damit verbundenen Probleme informieren.

2.1 Sachverhalt

Nachdem der Nachrichtendienst des Bundes der (NDB) Anfang Dezember 2015 einen Hinweis erhielt, dass die Informatik der RUAG von einem Cyber-Angriff betroffen sein könnte, kontaktierte er umgehend die Firma. Für die weiteren Abklärungen wurden auch die Spezialisten der Melde- und Analysestelle Informationssicherung (MELANI/GovCERT)[5] des EFD beigezogen, diese konnten schliesslich rund eineinhalb Monate später ein Schadprogramm nachweisen.[6] Dabei handelte es sich um eine sich seit mehreren Jahren im Umlauf befindliche Schadsoftware der Turla-Familie.[7]

Daraufhin wurden die Kerngruppe Sicherheit des Bundes (KGSi)[8] und in der Folge auch der Bundesrat bzw. sein Sicherheitsausschuss (SiA)[9] informiert. Der Vorsteher des VBS brachte den Vorfall Ende Januar 2016 dann auch der GPDel zu Kenntnis.

5 MELANI besteht seit Oktober 2004. Es wurde vom Bundesrat mit dem Schutz der kritischen Infrastrukturen in der Schweiz beauftragt, indem es sowohl Aufgaben zur Früherkennung von Gefahren als auch Aufgaben bei deren Bewältigung übernimmt. Dazu unterstützt es insbesondere die Betreiber von kritischen Infrastrukturen. MELANI ist ein Kooperationsmodell zwischen dem Eidgenössischen Finanzdepartement (EFD), vertreten durch das Informatiksteuerungsorgan des Bundes (ISB) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), vertreten durch den Nachrichtendienst des Bundes (NDB). Das GovCERT wurde 2008 von MELANI geschaffen, um noch schneller auf Vorfälle reagieren zu können.

6 Vgl. Kap. 4.4 im Jahresbericht 2016 der GPK und GPDel (BBl **2017** 3792).

7 Zusammenfassung des technischen Berichts von MELANI vom 23.5.2017 über den Spionagefall bei der RUAG (www.melani.admin.ch/dam/melani/de/dokumente/2016/technischer_bericht_apt_case_ruag_summary.pdf.download.pdf/TR-ZF-d.pdf).

8 Die KGSi ist ein sicherheitspolitisches Gremium, das sich aus dem Staatssekretär des EDA, dem Direktor des NDB und der Direktorin des fedpol zusammensetzt. Ihr Auftrag besteht primär in der Lageverfolgung und -beurteilung sowie der Früherkennung von Herausforderungen im sicherheitspolitischen Bereich. Die KGSi analysiert dazu laufend die sicherheitspolitische Situation, rapportiert dem Sicherheitsausschuss des Bundesrates und stellt ihm bei Bedarf Anträge.

9 Der SiA ist ein Organ des Bundesrats. Er soll die sicherheitspolitische Führungsfähigkeit des Bundesrates stärken, indem er die Beratungen und Entscheide des Bundesrates in sicherheitspolitischen Fragen vorbereitet. Der SiA besteht aus den Vorstehern oder Vorsteherinnen des EDA, des EJPD und des VBS. Vgl. auch die Verordnung über die Organisation der sicherheitspolitischen Führung des Bundesrats vom 24. Okt. 2007, SR **120.71**.

2.1.1 Eingeleitete Massnahmen

2.1.1.1 Massnahmen des Bundesrates

Der Sicherheitsausschuss des Bundesrates (SiA) beauftragte die KGSi am 4. Februar 2016 mit einer Einschätzung des Schadens, einer Beurteilung der Risiken und der Prüfung weiterer Massnahmen. Auf der Basis ihrer ersten Analyse beantragte die KGSi beim Bundesrat verschiedene Sofortmassnahmen sowie weitere kurz- und mittelfristig umzusetzende Massnahmen. Der Bundesrat verabschiedete am 23. März 2016 in einem geheimen Beschluss insgesamt 14 Massnahmen, für die verschiedene Bundesstellen verantwortlich waren – vor allem natürlich Dienststellen des VBS, aber auch das ISB und BIT. Für die Umsetzung der Massnahmen wurden zudem Termine fixiert und die KGSi mit der Überprüfung der Umsetzung beauftragt. Am 11. Mai 2016 beschloss der Bundesrat weitere vier Massnahmen als Reaktion für den Cyber-Angriff auf die RUAG.

Für die Begleitung der Massnahmenumsetzung waren verschiedene Akteure zuständig, hauptsächlich das VBS bzw. Stellen im VBS (vgl. dazu den folgenden Abschnitt 2.1.2), aber teilweise auch andere Bundesstellen wie das BIT. Diese rapportierten an die KGSi, welche ein Monitoring zur Umsetzung der Massnahmen führte.

2.1.1.2 Massnahmen des VBS

Neben den Massnahmen, welche der Bundesrat anordnete, traf auch das VBS verschiedene Vorkehrungen. Die vom VBS selber eingeleiteten Massnahmen betrafen dabei vor allem VBS-interne Prozesse und Überprüfungen. Viele davon betrafen die Führungsunterstützungsbasis (FUB) und die Logistikbasis (LBA) der Armee, welche innerhalb des VBS die beiden wichtigsten Partner der RUAG sind.

Der Vorsteher des VBS setzte kurz nach Bekanntwerden der Attacke die Taskforce RHINO ein.[10] Diese sollte sich zusammen mit der RUAG und den anderen involvierten Akteuren (u.a. NDB, MELANI[11], ISB[12]) um die Einleitung der nötigen Sofortmassnahmen und die Schadensabklärung kümmern. Die Taskforce begleitete dabei nicht nur die Massnahmen des VBS, sondern auch die vom Bundesrat angeordneten Massnahmen und die RUAG-internen Vorkehrungen zur Wiederherstellung der Sicherheit (vgl. nächster Absatz). Die Taskforce stand dabei in engem Austausch mit allen betroffenen Akteuren auf Stufe Bund sowie mit der RUAG und liess sich regelmässig über die ergriffenen Massnahmen und den Stand der Umsetzung informieren. Trotz gewissen Problemen auf der strategischen Ebene, insbesondere in der ersten Zeit nach Entdeckung des Angriffs (mangelhafte Zusammenarbeit

10 Diese setzte sich aus verantwortlichen Personen aus dem GS-VBS, der Armee, des NDB, armasuisse und weiteren involvierten Bundesstellen sowie Vertretern der RUAG zusammen.
11 Vgl. Fussnote 4.
12 Das Informatiksteuerungsorgan des Bundes (ISB) sorgt für die Umsetzung der Strategie zur Informations- und Kommunikationstechnik (IKT) in der Bundesverwaltung. Es leitet auch die Melde- und Analysestelle Informationssicherung (MELANI).

mit dem VBS; vgl. Kap. 4.1.3)[13] funktionierte die Zusammenarbeit auf der operativ-technischen Ebene mit der RUAG gemäss den befragten Personen aus dem VBS grundsätzlich gut.[14]

Im Juli 2016 wurde die Taskforce vom Vorsteher des VBS in eine Arbeitsgruppe umgewandelt.[15] Diese sollte sich weiterhin mit der Aufarbeitung des Angriffs bzw. der Umsetzung der Massnahmen zur Bewältigung dieses Angriffs befassen, daneben aber auch grundsätzlichere, strategische Überlegungen zum Umgang mit Cyber-Risiken im VBS anstellen und einen «Aktionsplan Cyberdefence» erarbeiten.

2.1.1.3 Massnahmen der RUAG

Wie einleitend dargelegt wurde der Cyber-Angriff bzw. die Schadsoftware bei der RUAG erst nach einem Hinweis durch den NDB und umfassenden Abklärungen, bei denen die Firma massgeblich durch die Spezialisten von MELANI unterstützt wurden, gefunden. Später wurde bekannt, dass die von den Angreifern verwendete Software zu einer bereits seit längerem bekannten Software-Familie gehörte. So wies der Bundesrat in einer Antwort auf einen parlamentarischen Vorstoss darauf hin, dass man die technischen Indikatoren zur erwähnten Malware-Familie über MELANI bereits seit Jahren mit Betreibern von kritischen Infrastrukturen, darunter auch die RUAG, ausgetauscht habe. Es liege dann aber an den Unternehmen, diese Informationen für ihre betriebseigenen Sicherheitssysteme zu nutzen.[16] Die RUAG wies den Vorwurf, sie habe die Informationen von MELANI nicht genutzt, zurück.[17]

Nachdem die Schadsoftware nachgewiesen wurde, wurde die RUAG vom Bund bzw. VBS mit der Umsetzung von acht Sofortmassnahmen beauftragt. Diese zielten darauf, den Schaden einzudämmen bzw. die Sicherheit wiederherzustellen und die Überwachung der IT-Systeme der RUAG zu verbessern. Daneben startete die Firma ein eigenes Massnahmenprogramm zur Erhöhung des Schutzes vor Cyberangriffen. Dieses sogenannte Programm IMPACT umfasst neun Massnahmen zur Prävention, Detektion und Bewältigung solcher Attacken. Die Umsetzung dieser Massnahmen soll rund 10 Mio. Franken kosten und bis Ende 2019 abgeschlossen sein.

13 Gemäss der Stellungnahme der RUAG im Rahmen der Verwaltungskonsultation ging es dabei insbesondere um die Klärung von rechtlichen Fragestellungen, insbesondere bezüglich dem Zugang zu klassifizierten Dokumenten von Dritten. Zudem waren anfänglich auch die verfügbaren personellen Ressourcen mit dem richtigen IT-Know-how und der für die Bearbeitung des Vorfalls notwendigen Stufe der Personensicherheitsüberprüfung begrenzt.

14 Anhörung der Generalsekretärin und des Delgierten des VBS für Cyber-Defence vom 3.7.2017.

15 Die Arbeitsgruppe besteht aus mehr als 25 Personen aus allen Bereichen des VBS und trifft sich zu monatlichen Sitzungen. Mit der Umwandlung ging auch eine kleine Veränderung in der Zusammensetzung einher, insbesondere was die Vertretung der RUAG betrifft. Diese war in der Taskforce noch vertreten, aber nicht mehr in der Arbeitsgruppe.

16 Antwort des Bundesrates vom 10.6.2016 auf eine dringliche Anfrage der CVP vom 2.6.2016 (16.1022).

17 Medienmitteilung der RUAG vom 16.6.2016.

In einer Informationsnotiz des VBS an den Bundesrat[18] werden die von der RUAG eingeleiteten Massnahmen als «korrekt» bezeichnet. Gleichzeitig weist das VBS aber auch darauf hin, dass die Verbesserung der Cyber-Sicherheit nur erreicht werden kann, wenn die Massnahmen kontinuierlich weiterentwickelt werden und mit einem Wandel der Sicherheitskultur in der Firma einhergehen.

Das VBS forderte von der RUAG zudem schon früh genauere Angaben zum Zeitplan des Programms IMPACT, ebenso wie ein regelmässiges Reporting dazu. Gemäss eigenen Angaben stellte es aber fest, dass es als Departement nicht über die rechtlichen Möglichkeiten verfügt, diese Auskünfte selber einzufordern.[19] In der Folge beantragte das VBS beim Bundesrat, dass dieser von der RUAG verlangt, dem VBS quartalsweise einen Reportingbericht zum Fortschritt des Programms IMPACT zuzustellen.[20]

Das VBS stufte die Berichterstattung der RUAG in der Folge aber als ungenügend ein und verlangte von der RUAG bis Ende November 2017 eine detailliertere Berichterstattung. Gemäss Auskunft des VBS entspricht diese jetzt der gewünschten Qualität und dem geforderten Detaillierungsgrad, um fundierte Schlüsse ziehen zu können.[21]

2.1.2 Prüfung der Massnahmen

Wie oben beschrieben, war das VBS und insbesondere die damalige Taskforce (und heutige Arbeitsgruppe) RHINO diejenige Stelle, welche die Übersicht über die Massnahmen zur Bewältigung des Cyber-Angriffs auf den verschiedenen Stufen gewährleistete und die Umsetzung der Massnahmen begleitete. Dabei war das VBS bis zu einem gewissen Grad auch für eine (kritische) Überprüfung der Massnahmen zuständig. Neben dem VBS übernahm auch die KGSi teilweise Prüfaufgaben.

Eine grundsätzlichere und unabhängige Prüfung der Massnahmen erfolgte aber insbesondere durch die Eidgenössische Finanzkontrolle (EFK) und die GPDel.

2.1.2.1 Eidgenössische Finanzkontrolle EFK

Die EFK leitete im Frühling 2016 eine Überprüfung der Umsetzung der Massnahmen aus dem Bundesratsbeschluss vom 23. März 2016 ein. Im Januar 2017 informierte sie den SiA, die KGSi und den Vorsteher des VBS über ihre Erkenntnisse, im März 2017 dann auch die FinDel.

Die EFK kam auf der Basis ihrer Abklärungen zum Schluss, dass insbesondere die Umsetzung von zwei Massnahmen grösseren Aufwand bereitet, darunter die Massnahme bezüglich einer Entflechtung der Netze von Bund und RUAG (vgl.

18 Informationsnotiz des VBS an den Bundesrat vom 10.4.2017.
19 Anhörung des Delegierten des VBS für Cyber-Defence vom 3.7.2017.
20 Bericht des VBS an die Subkommission vom 28.6.2017.
21 Schreiben des Delegierten des VBS für Cyber-Defence an die Subkommission vom 19.12.2017.

Kap. 2.1.3). Sie wies insbesondere darauf hin, dass sich die Umsetzung der Entflechtung als komplexer und langwieriger als erwartet herausstellte und dass diese auch von Relevanz für die Diskussionen über die Teilprivatisierung der RUAG ist. Die EFK gab ausserdem bekannt, dass sie ihre Prüfungen bezüglich der Umsetzung der Massnahmen zur Bewältigung des Cyber-Angriffs auf die RUAG im Jahr 2017 weiterführen wird. Die weiteren Prüfungen wurden auch vom VBS begrüsst, welches dem Bundesrat den Antrag stellte, dass dieser die EFK beauftragt, die RUAG im Bereich Informationssicherheit dauerhaft zu überwachen.[22]

Im Juni 2017 führte die EFK eine zweite Prüfung durch und informierte im August den Bundesrat über den Stand der Umsetzung der von ihm angeordneten Massnahmen. Die EFK hielt fest, dass die Massnahmen zum grössten Teil bereits umgesetzt oder auf Kurs sind. Eine Ausnahme bildet die Massnahme zur Entflechtung, diese werde noch einige Zeit in Anspruch nehmen. Die EFK wird die Umsetzung der Massnahmen im Verlauf des Jahres 2018 erneut prüfen, die Ergebnisse sollen bis Ende Juni 2018 vorliegen.[23]

2.1.2.2 GPDel / GPK

Da die Informationen zum Cyber-Angriff bis im Mai 2016 nicht öffentlich bekannt und im Bundesrat als «geheim» klassifiziert waren, befasste sich anfänglich vor allem auch die GPDel mit dem Angriff und dessen Konsequenzen. Sie hörte dabei verschiedentlich Vertreter des VBS und der RUAG an und erörterte, welche Massnahmen zur Bewältigung des Vorfalls getroffen werden sollten. Später diskutierte sie insbesondere auch die Zuständigkeiten und Strukturen zur Bewältigung des Vorfalls und nahm dazu auch in einem Schreiben an den Bundesrat Stellung.[24] Ende Juni 2017 beschloss die GPDel, sich fortan auf die nachrichtendienstlichen und strafrechtlichen Aspekte des Falls zu konzentrieren. Denn nachdem der Vorfall öffentlich bekannt wurde, konnte die Umsetzung der übrigen Massnahmen auch durch andere Gremien kontrolliert werden und die GPK die Oberaufsicht über den Vorfall ausüben.

Die Subkommission EDA/VBS der GPK-N liess sich daher ab dem Sommer 2016 mehrmals über die Bewältigung des Vorfalls und Stand der Umsetzung der Massnahmen informieren. Sie fokussierte dabei vor allem auf die Frage, ob die zuständigen Aufsichtsorgane – insbesondere der Bundesrat und das VBS – ihre Aufgabe angemessen wahrnehmen und nicht auf eine detaillierte Prüfung der einzelnen Massnahmenumsetzung, die ja Gegenstand der EFK-Abklärungen ist. Eine Ausnahme bildet dabei, wie bereits erwähnt, die Massnahme bezüglich einer Entflechtung der Netze von VBS und RUAG (vgl. das folgende Kap. 2.1.3).

22 Bericht des VBS an die Subkommission vom 28.6.2017.
23 Stand: 17.1.2018
24 Vgl. Kap. 4.4 im Jahresbericht 2016 der GPK und GPDel (BBl **2017** 3792).

2.1.3 Massnahme «Entflechtung Netze VBS-RUAG»

Auf Anregung der GPDel prüfte die GPK-N insbesondere die Umsetzung der Entflechtung der IT-Netze[25] von Bund und RUAG. Der Bundesrat beauftragte das VBS am 23. März 2016, so rasch wie möglich für die Entflechtung sowohl auf der Geschäfts- als auch auf der Systemebene zwischen dem Bund und der RUAG zu sorgen.[26] Gemäss dem ursprünglichen Zeitplan hätte dazu bis Ende September 2016 ein Sanierungsplan erarbeitet werden sollen. Dieser musste sich auf die Ergebnisse einer anderen vom Bundesrat angeordneten Massnahme stützen, mit der das VBS beauftragt wurde, bis Mitte April 2016 alle Verbindungen zwischen dem VBS und der RUAG zu erheben, inkl. den sich daraus ergebenden Abhängigkeiten für die Einsatzbereitschaft der Armee.[27]

Dabei stellte sich relativ bald heraus, dass bereits die Erhebung der Verflechtung und im Anschluss daran auch die Umsetzung der Entflechtung von grösserer Komplexität ist als angenommen und dementsprechend auch (viel) mehr Zeit benötigt als vorgesehen. Vertreter des VBS informierten die Kommission bereits im Oktober 2016, dass die Frist für die Umsetzung der Massnahme zur Entflechtung bzw. für die Erarbeitung eines Sanierungsplans bis Ende März 2017 verlängert wurde. Der Bundesrat beauftragte das VBS anschliessend am 10. Mai 2017, ihm bis Ende Juni in einem Bericht die Verflechtungen von RUAG und Armee darzustellen und die Möglichkeiten zur Entflechtung aufzuzeigen.

Der Bericht des VBS zuhanden des Bundesrates vom 21. Juni 2017 hält fest, dass die bestehende Verflechtung sehr eng ist und dass die Armee heute viele Leistungen nur mit Unterstützung der RUAG erbringen kann. Der Bericht legt dabei detailliert dar, welche Leistungen die RUAG für die Armee erbringt, und beschreibt die Verflechtungen auf Ebene der Leistungen, Prozesse, Informatik und Immobilien. Er legt anschliessend dar, was Entflechtung bedeutet («wenn die RUAG in allen Belangen zu einem ganz normalen externen Dienstleister des VBS geworden ist») und skizziert drei Varianten zur Umsetzung der Entflechtung. Alle drei Varianten hätten erhebliche Konsequenzen für die Armee und die RUAG und, müssten sowohl einsatzbezogen, sicherheitspolitisch als auch wirtschaftlich vertieft geprüft werden.

Der Bundesrat hat den Bericht des VBS an seiner Sitzung vom 28. Juni 2017 behandelt. Gemäss einem Schreiben des VBS an die zuständige Subkommission vom 25. Oktober 2017 hat er beschlossen, die Abklärungen bezüglich einer (Teil-)Privatisierung der RUAG zu sistieren, bis die Entflechtung realisiert sei. In der Folge hätten weitere Abklärungen des VBS und Diskussionen zwischen VBS und RUAG gezeigt, dass weitere, vertiefte Abklärungen nötig sind, bis dem Bundesrat ein detaillierter Plan zur Entflechtung (Umfang, nötige Massnahmen, Aufwand und Zeitbedarf) unterbreitet werden könne. Der Bundesrat werde sich aber voraussichtlich im März 2018 wieder mit Fragen zur Entflechtung beschäftigen.

25 Die Entflechtung der IT-Netze betrifft dabei bei Weiten nicht nur die Informatik, sondern auch Verflechtungen auf Ebene von Leistungen, Prozessen oder Immobilien.
26 Massnahme 11 gemäss Bundesratsbeschluss vom 23.3.2016.
27 Massnahme 3 gemäss Bundesratsbeschluss vom 23.3.2016.

Im Rahmen der Anhörungen informierte das VBS die zuständige Subkommission darüber, dass die Entflechtung unter anderem auch mit der Reorganisation der FUB gekoppelt werden müsse und aufgrund der grossen Komplexität voraussichtlich erst im Jahr 2023 abgeschlossen werden kann.

2.2 Bewertung

2.2.1 Eingeleitete Massnahmen

Obwohl die GPK-N die verschiedenen Massnahmen nicht im Einzelnen analysiert hat, ist sie der Ansicht, dass diese grundsätzlich als sinnvoll bewertet werden können. Sie stellt auch fest, dass der Bundesrat rasch gehandelt und die KGSi mit weiteren Abklärungen beauftragt hat, auf deren Basis er dann auch rasch über Massnahmen beschliessen konnte.[28] Ebenso ist es zu begrüssen, dass sich der SiA und damit der für Sicherheitsfragen zuständige Ausschuss des Bundesrates[29] selber schon früh mit dem Vorfall befasste.

Sie stellt weiter fest, dass auch das VBS schnell auf den Vorfall reagierte und mit der Taskforce RHINO ein Gremium schuf, dass sich unter Einbezug der RUAG und aller betroffenen Akteure auf Stufe Bund um die Schadensabklärung und Sofortmassnahmen kümmerte. Sie begrüsst auch, dass die Zusammenarbeit auf dieser eher operativen Ebene gut funktionierte, obwohl die Leitung der RUAG den Vorfall zu Beginn wohl unterschätzte und sich gegenüber dem VBS nicht immer kooperativ zeigte.

Bezüglich der Massnahmen der RUAG erwartet die Subkommission, dass das VBS die Umsetzung weiterhin kritisch begleitet und wo nötig Verbesserungen oder mehr Mittel fordert. Sie verweist in diesem Zusammenhang auf die Einschätzung des VBS, welches darauf hinwies, dass neben diesen Massnahmen auch ein grundsätzlicher Wandel in der «Sicherheitskultur» der Firma nötig sei (vgl. Kap. 2.1.1.3). Es gilt die Eignerinteressen des Bundes gebührend durchzusetzen (vgl. Kap. 4).

2.2.2 Prüfung der Massnahmen

Die GPK-N begrüsst, dass der Bundesrat mit der EFK ein unabhängiges Organ mit der Überprüfung der Umsetzung der Massnahmen zur Bewältigung des Cyber-Angriffs beauftragte.

28 Die GPDel stellte im Rahmen ihrer Abklärungen fest, dass die Mitglieder der KGSi und ihre Ämter nicht über die notwendigen Fachkenntnisse verfügten, um die Bedrohungslage adäquat beurteilen zu können. Sie hätte es als zweckmässiger erachtet, wenn der Bundesrat sich für die Bewältigung des Vorfalls direkt auf die regulären Strukturen verlassen hätte, die er mit der Bundesinformatikverordnung (BinfV) selber geschaffen hat (vgl. Kap. 4.4 im Jahresbericht der GPK und GPDel 2016 der GPK und GPDel [BBl **2017** 3792]). Die GPK-N hat sich im Rahmen ihrer Abklärungen nicht vertieft mit den Strukturen befasst.

29 Vgl. Fussnote 9.

Sie fordert den Bundesrat in diesem Zusammenhang auf, auf der Basis der Erkenntnisse der EFK zu prüfen, ob er allenfalls im Rahmen der strategischen Steuerung der Firma gewisse Weichenstellungen vornehmen will, insbesondere auch in Hinblick auf die anstehenden Entscheide zur künftigen Organisations- und Rechtsform der RUAG bzw. deren allfällige Teilprivatisierung.

Empfehlung 1 Aufnahme der wesentlichen Erkenntnisse im Rahmen der strategischen Steuerung

Die GPK-N fordert den Bundesrat auf, auf der Basis der Erkenntnisse der EFK zu prüfen, ob sich daraus eine Notwendigkeit ergibt, im Rahmen der strategischen Steuerung der RUAG gewisse Weichenstellungen vorzunehmen, insbesondere im Rahmen der anstehenden Entscheide zur künftigen Organisations- und Rechtsform der RUAG bzw. deren allfällige Teilprivatisierung.

2.2.3 Massnahme «Entflechtung Netze VBS-RUAG»

Die Kommission nimmt auch zur Kenntnis, dass die Verflechtungen zwischen den Netzen des Bundes und der RUAG offenbar so komplex sind, dass eine Entflechtung nicht wie ursprünglich geplant bzw. erwartet in relativ kurzer Zeit realisiert werden kann, sondern voraussichtlich erst bis 2023 zu einem Abschluss gebracht werden kann. Sie begrüsst aber, dass der Bundesrat an der Entflechtung festhält und fordert diesen und insbesondere auch das VBS auf, die notwendigen Vorkehrungen zu treffen und die nötigen Mittel bereit zu stellen, damit die Entflechtung bis zur jetzt vorgesehenen Frist verwirklicht werden kann.

Aus Sicht der Kommission hat der Cyber-Angriff auf die RUAG den Fokus für die Problematik der Verflechtung der Netze zwischen dem Bund und ausgelagerten Einheiten grundsätzlich geschärft. Der Bundesrat hat im Rahmen der Massnahmen zur Bewältigung des Cyber-Angriffs angeordnet, dass auch die Verflechtungen des Bundes mit anderen ausgelagerten Einheiten einer kritischen Prüfung unterzogen werden. Die GPK begrüsst diese Massnahme und erwartet, dass der Bundesrat die Problematik weiterverfolgt und bei Bedarf Massnahmen einleitet. Zudem fordert sie dem Bundesrat auf, der Frage der Verflechtung und der damit verbundenen Konsequenzen bei allfälligen künftigen Auslagerungen oder Privatisierungen von Verwaltungseinheiten die nötige Bedeutung beizumessen.

Empfehlung 2 Berücksichtigung der Verflechtungsproblematik bei zukünftigen Auslagerungen bzw. im Rahmen der Corporate-Governance-Grundsätze

Die GPK-N fordert den Bundesrat auf, zu gewährleisten, dass bei künftigen Auslagerungen der Problematik der Verflechtung angemessen Rechnung getragen wird. Dabei soll er insbesondere die Frage klären, ob diese im Rahmen der Eignungskriterien für eine Auslagerung bzw. in den relevanten Corporate-Governance-Vorgaben und Berichten aufgenommen werden sollte.

3 Schaden des Angriffs

Im folgenden Kapitel geht es um den Schaden des Angriffs. Weil die Informationen zum genauen Ausmass des Schadens sowie Details zum Angriff äusserst sensitiv sind, wird sich auch die GPK-N nur in allgemeiner Form dazu äussern. Die zuständige Subkommission hatte aber Zugang zu den relevanten Informationen und damit eine genügende Informationsbasis für die folgende Beschreibung und Bewertung.

3.1 Sachverhalt

Nachdem der Angriff auf die RUAG bekannt wurde, beauftragte der Sicherheitsausschuss des Bundesrates (SiA) die Kerngruppe Sicherheit (KGSi) am 20. Juli 2016, das Ausmass der Schäden abzuklären und auch aufzuzeigen, wo definitive Erkenntnisse nur schwer oder gar nicht möglich sind.

Der Bericht der KGSi vom 25. August 2016 hält fest, dass es keine Hinweise gibt, wonach die Schadsoftware auch in den Systemen der Bundesverwaltung aktiv war oder ist und die Angreifer damit Zugang zu Daten des Bundes und insbesondere des VBS hatten. Den Datenabfluss bei der RUAG stuft der Bericht aber als signifikant ein. Eine genaue Abschätzung des Schadens sei aber aufgrund verschiedener Aspekte nicht möglich, unter anderem auch, weil die RUAG dem VBS nicht alle geforderten Informationen zur Verfügung stellen wollte[30] (siehe dazu auch Kap. 2.1.1.2). Die RUAG wurde daraufhin aufgefordert, ergänzende Informationen zu liefern.

Nachdem die GPK-N die weiteren Abklärungen zum Cyber-Angriff auf die RUAG von der GPDel übernommen hatte, analysierte sie den oben erwähnten Bericht der KGSi vom 25. August 2016. In der Folge forderte sie vom VBS einen aktualisierten Bericht zum Schaden, welcher auf den von der RUAG eingeforderten, ergänzenden Informationen basiert. Das VBS kam dieser Aufforderung mit einigen Verzögerungen nach und stellte der Subkommission schliesslich am 28. Juni 2017 den verlangten Bericht zu.[31] Dieser umfasst detailliertere Angaben zu den vom Datendiebstahl betroffenen Verzeichnissen, möglichen Folgen bzw. Risiken und den eingeleiteten Schutz-Massnahmen. Vor allem wird aus dem Bericht aber auch deutlich, dass das Ausmass des Diebstahls aus verschiedenen Gründen letztlich nicht abschliessend bestimmt werden kann und dass sich die Beurteilung des entstandenen Schadens durch die Experten des VBS und die RUAG wesentlich unterscheiden. Während die RUAG stark quantitativ argumentiert, indem sie ihre Einschätzung vor allem auf das

30 Gemäss der Stellungnahme der RUAG konnte sie dem VBS zu Beginn nicht alle gewünschten Informationen liefern. Dies habe daran gelegen, dass zuerst ein Prozess festgelegt werden musste, welcher es der RUAG ermöglichte, dem VBS auch Zugang zu Dokumenten zu verschaffen, für welche sie ihrerseits Vertraulichkeitserklärungen gegenüber Dritten abgegeben hatte (Geheimhaltungserklärungen mit VBS Mitarbeitern und Einrichtung eines eigenen, geschützten Datenraumes, in welchen alle kritischen Dokumente eingesehen werden konnten).

31 Dabei handelt es sich um einen Bericht, der eigens für die Subkommission erstellt wurde. Der GPK-N ist nicht bekannt, inwiefern der Bundesrat oder der SiA über die aktualisierte Schadensbeurteilung informiert wurden.

Volumen der gestohlenen Daten stützt, ist aus Sicht des VBS nicht die Datenmenge an sich, sondern die Bedeutung der Daten entscheidend.

Der Vorsteher des VBS gab gegenüber der Arbeitsgruppe an, dass der Bund und die Firma das Risiko unterschiedlich eingeschätzt hatten und dass die RUAG die Risiken in einer ersten Phase nach dem Angriff klar unterschätzt habe.[32] Inzwischen funktioniere die Zusammenarbeit aber und die RUAG habe verschiedene Verbesserungsmassnahmen getroffen.

Die zuständige Subkommission erkundigte sich im Rahmen ihrer Abklärungen mehrmals über das Ausmass des (finanziellen) Schadens und auch über die Reaktionen der Kunden bzw. allfällige Auswirkungen auf Kooperationen oder Aufträge. Da das VBS selber nicht über diese Informationen verfügte, leitete es die Fragen an die RUAG weiter. Umgekehrt leitete es dann auch die Antwort der RUAG ohne eigene Bewertung wiederum an die Subkommission weiter. In ihrem Schreiben an die Generalsekretärin des VBS vom 15. Januar 2018 hält die RUAG fest, dass sich die finanziellen Folgen des Cyber-Angriffs auf die Kosten für die Bearbeitung des Vorfalls (Umsetzung Massnahmen, Dispositive für Kundenanfragen) sowie auf das daraufhin eingeleitete Programm IMPACT[33] beschränken. Abgesehen davon habe die RUAG bisher keinen direkten Schaden aus der Attacke erlitten, insbesondere habe man keine unmittelbaren Kundenabgänge verzeichnet.

3.2 Bewertung

Die GPK-N bzw. die zuständige Subkommission erhielt im Rahmen ihrer Abklärungen detaillierte Informationen über die vom Angriff betroffenen Datenverzeichnisse und die dadurch entstandenen Risiken. Auf dieser Basis kam sie zum Schluss, dass der Angriff auf die RUAG als gravierender Vorfall eingestuft werden muss. Die GPK-N ist weiter klar der Ansicht, dass die Bedeutung der entwendeten Daten nicht allein quantitativ, sondern auch qualitativ bemessen werden muss; sie teilt damit die Einschätzung des VBS.

Die GPK-N nimmt zu Kenntnis, dass die RUAG gemäss eigenen Angaben aufgrund des Cyber-Angriffs bisher keinen direkten Schaden erlitten bzw. keine unmittelbaren Kundenabgänge verzeichnet hat. Sie ist aber dennoch der Ansicht, dass ein solcher Vorfall sicher nicht förderlich für den Geschäftsgang ist und diesem daher nur schon aus diesem Grund eine grosse Bedeutung zugemessen werden muss.

Sie hat in diesem Zusammenhang mit Unverständnis zu Kenntnis genommen, dass die RUAG nach Bekanntwerden des Angriffs rein quantitativ argumentierte und sich überdies wenig kooperativ zeigte, indem sie dem VBS nicht alle geforderten Informationen zur Verfügung stellen wollte (mehr dazu im Kap. 4). Die GPK-N begrüsst es, dass das VBS diesbezüglich insistierte, so dass die Abklärungen letztlich dennoch zu einer weitgehend klaren und befriedigenden Schadensanalyse führten und

32 Anhörung des Vorstehers VBS vom 28.4.2017.
33 Die Kosten des Programms IMPACT, welches bis 2019 umgesetzt werden soll, belaufen sich insgesamt auf rund 10 Mio. Franken. Hinzu kommen jährlich wiederkehrende Kosten von rund 1 Mio. Franken aufgrund der Aufstockung der IT-Organisation bzw. -Sicherheit.

so verschiedene Vorkehrungen getroffen werden konnten, um den Schaden zu beheben bzw. Risiken zu minimieren (vgl. Kap. 2).

4 Strategische Steuerung und Wahrung der Eignerinteressen

4.1 Sachverhalt

4.1.1 Grundsätzliche Informationen zur RUAG und deren Steuerung

Rechtliche Grundlage und wesentliche Fakten zur RUAG

Die RUAG (RUAG Holding AG) ist ein Rüstungsunternehmen, welches aus der Auslagerung bzw. Verselbständigung der ehemaligen Rüstungsbetriebe des Bundes entstanden ist. Sie ist eine privatrechtliche Aktiengesellschaft, deren Aktienkapital zu 100 % im Besitz des Bundes ist.

Im Jahr 2016 beschäftigte die RUAG an fast 80 Standorten über 8500 Personen. Rund die Hälfte der Standorte und Stellen befinden sich in der Schweiz (fast 4500 Stellen an 39 Standorten). Daneben verfügt die RUAG über zahlreiche weitere Standorte in Europa (26), aber auch in den USA (7 Standorte), Australien (5 Standorte) und Asien (2 Standorte). Im Jahr 2016 erzielte die Firma einen Nettoumsatz vom 1858 Mio. Franken und einen Reingewinn von 116 Mio. Franken. Davon gingen 47 Mio. Franken als Dividende an den Bund als Eigner.

Die rechtliche Grundlage für die RUAG findet sich im Bundesgesetz über die Rüstungsunternehmen des Bundes.[34] Dort ist im Zweckartikel festgehalten, dass der Bundesrat zur «Sicherstellung der Ausrüstung der Armee» Rüstungsunternehmen betreiben kann.[35] Weitere Vorgaben sind in den Statuten der RUAG festgehalten (Zweck, Aktienkapital, Organe sowie deren Rechte und Pflichten etc.). Der Bundesrat steuert die RUAG nach den eignerpolitischen Grundsätzen des Corporate-Governance-Berichtes des Bundesrates von 2006[36] und insbesondere über die Vorgabe von strategischen Zielen:

Bericht zur Corporate Governance

Der Corporate-Governance-Bericht[37] sowie die dazugehörigen Zusatzdokumente[38] wurden vom Bundesrat erarbeitet, um eine bessere Grundlage für die Auslagerung von Aufgaben und eine einheitlichere Steuerung verselbständigter Einheiten zu

34 Bundesgesetz vom 10. Oktober 1997 über die Rüstungsunternehmen des Bundes (BGRB), SR **934.21**.
35 Artikel 1 des Bundesgesetzes über die Rüstungsunternehmen des Bundes (BGRB), SR **934.21**.
36 Bericht des Bundesrates zur Auslagerung und Steuerung von Bundesaufgaben (Corporate-Governance-Bericht) vom 13. September 2006, BBl **2006** 8233.
37 Vgl. Fussnote 33.
38 Erläuternder Bericht der Eidg. Finanzverwaltung zum Corporate-Governance-Bericht des Bundesrates vom 13. September 2006; Zusatzbericht des Bundesrates zum Corporate-Governance-Bericht vom 25. März 2009 (BBl **2009** 2659).

schaffen. Dazu werden Leitsätze zu wesentlichen Steuerungselementen festgehalten, u. a. zum Einsitz von Bundesvertretern im Verwaltungsrat, zur Kontrolle durch den Bundesrat und zu den strategischen Zielen.[39] Die wesentlichen Leitsätze hierzu sind die folgenden:

- *Organe:* Die Organe der ausgelagerten Einheiten müssen über das nötige fachliche und betriebliche Wissen verfügen, um ihre Funktion verantwortungsgemäss ausüben zu können. Zugleich muss der Bundesrat aber auch dafür sorgen, dass die Interessen des Bundes im Instituts- oder Verwaltungsrat hinreichend vertreten werden. Daher muss er bei der Ausübung seines Wahlrechts auch darauf achten, dass sich die gewählten Personen mit der Stossrichtung der strategischen Ziele des Bundesrates identifizieren können und diese im Verwaltungs- oder Institutsrat vertreten.
- *Einsitz von Bundesvertretern im Verwaltungsrat:* Der Bundesrat soll nur noch dort mit instruierbaren Personen im Verwaltungsrat vertreten sein, wo dies notwendig ist, z.B., wenn sich seine Interessen ohne Vertretung nicht genügend wahrnehmen lassen. Im erläuternden Bericht der Eidgenössischen Finanzverwaltung ist festgehalten, dass Bundesvertreter insbesondere bei Einheiten mit Dienstleistungen am Markt in der Rechtsform einer privatrechtlichen Aktiengesellschaft sinnvoll sein können (da die strategischen Ziele für diese rechtlich nicht verbindlich sind, vgl. weiter unten).
- *Kontrolle des Bundesrates:* Die Kontrolle des Bundesrates als Eigner ist das Korrelat zu seiner Steuerungsfunktion und dient damit grundsätzlich den gleichen Zwecken. Sie bezweckt einerseits den Erhalt bzw. die Steigerung des Unternehmenswertes der verselbständigten Einheiten und ihrer Leistungsfähigkeit (unternehmensbezogene Kontrolle) und anderseits die Sicherstellung einer auf das Gemeinwohl ausgerichteten Aufgabenerfüllung (aufgabenseitige Kontrolle). Bei den privatrechtlichen Aktiengesellschaften richten sich die Kontrollmöglichkeiten der Aktionäre und damit auch des Bundes nach den Vorgaben des Aktienrechts.
- *Strategische Ziele:* Der Bundesrat steuert die verselbständigten Einheiten auf strategischer Ebene mit übergeordneten und mittelfristigen Zielvorgaben. Er kann dazu unternehmensbezogene und aufgabenseitige Vorgaben formulieren. Bei der RUAG liegt der Fokus dabei klar auf unternehmensbezogenen Vorgaben, da die Aufgabenerfüllung ja hauptsächlich am Markt erfolgt und entsprechend durch ihn gesteuert werden soll. Gegenüber dem Verwaltungsrat einer verselbständigten Einheit in der Rechtsform einer privatrechtlichen Aktiengesellschaft (wie z.B. der RUAG) sind die strategischen Ziele zwar rechtlich grundsätzlich nicht bindend, faktisch entfalten sie aber dennoch bindende Wirkung, denn der Verwaltungsrat kann es sich eigentlich nicht leisten, die Vorgaben des Haupt- oder Mehrheitsaktionärs zu missachten, andernfalls riskiert er die Abwahl.[40]

39 Bei den übrigen Steuerungselementen handelt es sich um Rechtsform, Organe, Haftungen, besondere Kompetenzen, Oberaufsicht, Finanzen und Steuern.

40 Zusatzbericht des Bundesrates zum Corporate-Governance-Bericht vom 25.3.2009 (BBl **2009** 2681).

Der Bundesrat muss die Zielerreichung jährlich überprüfen. Die wesentliche Grundlage dazu bildet ein Bericht der Unternehmung über die Zielerreichung. Dieser wird von den zuständigen Departementen geprüft und mit dem Unternehmen diskutiert, woraufhin der Bundesrat selber eine Beurteilung vornimmt (Bericht des Bundesrates über die Erreichung der strategischen Ziele) und diese den parlamentarischen Oberaufsichtskommissionen vorlegt.

Eignergespräche

Ein wichtiges Instrument der strategischen Steuerung bilden die regelmässigen «Eignergespräche» zwischen dem Bund und den ausgelagerten Einheiten. Diese Gespräche finden üblicherweise etwa vier Mal pro Jahr statt. Von Seiten Bund nimmt das zuständige Departement – in der Regel der Departementsvorsteher, der/die Generalsekretär/in und weitere, fachlich zuständige Personen – und meist auch eine Vertretung der Eidgenössischen Finanzverwaltung teil, von Seiten der Unternehmen der/die Präsidentin des Verwaltungsrates und der CEO sowie bei Bedarf weitere Personen aus der Unternehmensleitung. In diesen Gesprächen informiert das Unternehmen über den Geschäftsgang, wesentliche Herausforderungen oder auch über wichtige strategische Entscheide, wie beispielsweise Kooperationen mit anderen Unternehmen oder Unternehmens-Käufe. Die Vertreter des Bundes bewerten diese Informationen im Hinblick auf die Zielerreichung und sprechen insbesondere Probleme oder Vorkommnisse an, welche die Erreichung der strategischen Zielvorgaben gefährden könnten. Die Federführung für die Gewährleistung der Eignerinteressen gegenüber der Unternehmung liegt bei der zuständigen Departementsvorsteherin bzw. beim zuständigen Departementsvorsteher.

4.1.2 Strategische Ziele für die RUAG

In den aktuellen strategischen Zielen[41] ist festgehalten, dass die RUAG «vorab der Sicherstellung der Ausrüstung der Armee» dient und dass die Ziele «in erster Linie auf die Interessen des Bundes als Aktionär der RUAG ausgerichtet» sind, daneben aber «in angemessener Weise auch den Interessen des Bundes als bedeutender Kunde der RUAG Rechnung» tragen sollen. Neben den strategischen Schwerpunkten, welche die Sicherstellung der Ausrüstung der Armee betreffen, definiert der Bundesrat auch finanzielle Ziele – u. a. die Ausschüttung einer Dividende, die nicht unter 40 % des ausgewiesenen Reingewinns fällt[42] – sowie Vorgaben für Beteiligungen, Personal- und Regionalpolitik.

41 Strategische Ziele des Bundesrates für die RUAG Holding AG 2016–2019.
42 Bis 2015 waren es lediglich 20 % des Reingewinns.

4.1.3 Steuerung der RUAG im konkreten Fall/ Wahrung der Eignerinteressen

Wie in Kapitel 2 beschrieben, reagierten der Bundesrat und das VBS im Fall des Cyber-Angriffs auf die RUAG sowohl durch die Schaffung spezieller Strukturen zur Bewältigung des Vorfalls in der Bundesverwaltung (insbesondere Taskforce RHINO) als auch durch die Anordnung verschiedener Massnahmen.

In diesem Absatz soll nun dargelegt werden, wie der Vorfall im Rahmen der strategischen Steuerung bzw. der Kontrolle der Firma durch das VBS (als Vertreter des Bundesrates) aufgenommen und bewältigt wurde und, damit verbunden, wie das VBS generell für die Wahrung der Eignerinteressen des Bundes sorgt.

4.1.3.1 Steuerung im Rahmen der Eignergespräche

Die Protokolle der Eignergespräche[43] nach dem Vorfall[44] enthalten wenig bis keine Informationen in Bezug auf den Cyber-Angriff. Zwar wurde der Vorfall in drei Fällen traktandiert, die Diskussion dazu wurde aber nicht protokolliert.[45] In den drei anderen Protokollen, notabene auch im Protokoll des ersten Gesprächs nach Bekanntwerden des Angriffs, war der Vorfall nicht traktandiert und aus den Protokollen zeigt sich, dass er auch nicht behandelt wurde (oder auf die Protokollierung der entsprechenden Diskussion verzichtet wurde).

Vorfall traktandiert und Diskussion protokolliert	–
Vorfall traktandiert, Diskussion nicht protokolliert	*27.6.2016; 8.3.2017; 4.7.2017*
Vorfall nicht traktandiert und gemäss Protokoll auch nicht diskutiert	*9.3.2016; 20.9.2016; 13.12.2016*

Gemäss den Protokollen wurden die Folgen des Cyber-Angriffs in den Eignergesprächen nie vertieft diskutiert. So wurde beispielsweise nie thematisiert, wie die Kunden der RUAG auf den Vorfall reagiert haben, obwohl die RUAG vom VBS mit der Benachrichtigung der Kunden beauftragt wurde und obwohl deren Reaktionen sich allenfalls auf die Zusammenarbeit mit diesen Kunden und auf die Ertragslage der RUAG (und damit letztlich möglicherweise auch auf die Höhe der Dividende des Bundes) auswirken können. Wie die Aussagen des Vorstehers des VBS zeigen, erachtet das VBS diese Informationen für sich bzw. für den Eigner als nicht relevant. Er gab gegenüber der Subkommission an, man habe sich nie im Detail nach den Reaktionen der Kunden erkundigt, soweit ihm bekannt sei, habe die RUAG aber keine Kunden verloren und der Bund als Eigner habe auch keine Beschwerden von

43 Die Eignergespräche dauerten jeweils ca. zwei Stunden.
44 Die zuständige Subkommission der GPK hat die Protokolle der Eignergespräche aus dem Jahr 2016 und der ersten Hälfte 2017 erhalten und ausgewertet (2016: 4 Protokolle vom 9.3., 27.6., 20.9., 13.12.; 2017: 2 Protokolle vom 8.3., 4.7.).
45 In einem Fall wird der Verzicht auf die Protokollierung damit begründet, dass der CEO der RUAG dies gewünscht habe. In den beiden anderen Protokollen findet sich keine Angabe von Gründen.

Kunden erhalten.[46] Das VBS forderte die RUAG auf, der zuständigen Subkommission genauere Informationen zukommen zu lassen.[47]

Wie im Fall des Cyber-Angriffs ergeben sich aus den Protokollen grundsätzlich wenig Hinweise darauf, dass das VBS die Gespräche nutzt, um Probleme oder Herausforderungen anzusprechen und allenfalls auch Forderungen an das Unternehmen zu stellen. Die Protokolle enthalten in der Regel zuerst eine relativ ausführliche Information der RUAG über den Geschäftsgang; danach folgen spezifische Themen, die im Protokoll oft nur kurz zusammengefasst werden. Aus einem Protokoll ergab sich zudem ein Hinweis auf Differenzen bzw. eine mangelhafte Koordination zwischen dem VBS und der EFV: Der Vertreter der EFV zeigt sich erstaunt über gewisse Aussagen des Vorstehers VBS zur Weiterentwicklung der RUAG, er sei diesbezüglich «anders informiert worden».[48]

Neben den Protokollen der Eignergespräche führt das VBS eine Pendenzenliste zu diesen Aussprachen. Aus den analysierten Pendenzenlisten[49] ergeben sich ebenfalls keine Hinweise auf konkrete Aufträge oder Forderungen des VBS an die Firma in Bezug auf den Cyber-Angriff oder andere Probleme, welche die Erreichung der strategischen Ziele gefährden könnte. Auffallend ist insbesondere, dass die Pendenzenliste als ständige Pendenz ab Juli 2017 die Vorgabe enthält, dass die RUAG den Vorsteher des VBS frühzeitig über politisch relevante Presseartikel sowie regionalpolitisch bedeutsame Absichten der RUAG informiert (davor: nur Information über regionalpolitische Entscheide gefordert).

Obwohl sich aus den Protokollen und der Pendenzenliste wenig bis keine expliziten Aufträge des VBS an die RUAG ergeben, zeigen andere analysierte Unterlagen, dass es solche geben muss. In einem Fall legt die RUAG in einem Schreiben an das VBS rund einen Monat nach dem Eignergespräch nämlich dar, dass sie eine geplante Firmenübernahme als konform zu den strategischen Zielen einschätzt, und verweist auf eine mündliche Besprechung anlässlich der vorhergehenden Eignergesprächs. Im entsprechenden Protokoll wird diese Übernahme von der RUAG zwar im Rahmen der Informationen zum Geschäftsgang erwähnt, es finden sich dazu aber weder Nachfragen noch Aufträge des VBS.

Der Vorsteher des VBS hielt in Bezug auf die Eignergespräche fest, dass in deren Rahmen vor allem generelle und finanzielle Aspekte diskutiert werden. Sicherheitsfragen und insbesondere auch die Kapazitäten der RUAG im Cyberbereich würden dort hingegen nicht erörtert, nicht zuletzt auch, um Indiskretionen zu verhindern, denn es nähmen immerhin rund ein Dutzend Personen an diesen Sitzungen teil. Die Eignergespräche dienten im Wesentlichen dazu, Informationen zum Geschäftsgang der einzelnen Bereiche und deren Herausforderungen zu erhalten, dies im Hinblick auf die strategischen Ziele. Die EFV, die auch den Sitzungen teilnehme, interessiere sich vor allem dafür, ob die Beschaffung der einen oder anderen Dienstleitung zweckmässig sei.[50] Der Cyber-Angriff und das Thema Cybersicherheit seien dem-

46 Anhörung des Vorstehers VBS vom 26.11.2017.
47 Vgl. dazu Kap. 3.
48 Protokoll vom 13.12.2016, Trakt. 4.
49 Die zuständige Subkommission hat lediglich die Pendenzenlisten aus dem Jahr 2017 erhalten (Listen mit Stand vom 28.2., 8.3. und 4.7.2017).
50 Anhörung des Vorstehers VBS vom 16.11.2017.

gegenüber in anderen Gefässen behandelt worden, konkret in der KGSi, im Sicherheitsausschuss des Bundesrates sowie in der GPDel.[51] Aus den analysierten Unterlagen ist nicht ersichtlich, dass es aus diesen Gremien einen formalisierten «Rückfluss» zum Departementsvorsteher gab. Die angehörten Vertreter des VBS und insbesondere auch der Departementsvorsteher des VBS selber gaben an, dass der Cyber-Angriff und das Thema Cybersicherheit verschiedentlich in bilateralen Gesprächen des Vorstehers VBS mit Vertretern der RUAG behandelt worden sei (siehe unten).

Insgesamt lässt sich festhalten, dass die Bewältigung Cyber-Angriffs auf die RUAG in den formalisierten Eignergesprächen nicht bzw. höchstens am Rand thematisiert wurde (zur Behandlung der Thematik im Rahmen von anderen Kontakten zwischen dem Vorsteher des VBS und Vertretern der RUAG: vgl. Kap. 4.1.3).

4.1.3.2 Steuerung im Rahmen der bilateralen Gespräche zwischen dem Vorsteher VBS und der Leitung RUAG

Nach den Eignergesprächen ist jeweils noch ein bilaterales Gespräch zwischen dem Vorsteher des VBS und dem Verwaltungsratspräsidenten der RUAG vorgesehen. Dieses wird nicht protokolliert und teilweise wird auf dessen Durchführung verzichtet, so u. a. auch nach der ersten Sitzung nach Bekanntwerden des Cyber-Angriffs. Das VBS lieferte der Subkommission eine Übersicht der bilateralen Gespräche des Vorstehers VBS mit dem Verwaltungsratspräsidenten und/oder dem CEO der RUAG inkl. Stichworte zum Inhalt der Diskussion. Aus der Übersicht ergibt sich, dass sich der Vorsteher kurz nach Aufdeckung des Angriffs im Januar und Februar 2016 dreimal mit der RUAG-Spitze über den Vorfall ausgetauscht hat und auf die Ernsthaftigkeit des Vorfalls hinwies. In zwei weiteren Gesprächen im August 2016 und März 2017 wurde über die Folgen und Schäden der Attacke diskutiert. Der Vorsteher des VBS und die Vertreter des VBS wiesen in den Anhörungen aber allgemein daraufhin, dass der Vorfall in den bilateralen Gesprächen zwischen dem Vorsteher VBS und den Vertretern der RUAG durchaus thematisiert worden sei. Da es zu diesen Gesprächen keine weiteren Unterlagen gibt, konnte die Subkommission diese Informationen nicht verifizieren.

Der Vorsteher des VBS gab ausserdem an, dass er bei den bilateralen Gesprächen bewusst auf eine Protokollierung und auch auf persönliche Notizen verzichte. Denn in den Gesprächen würden sehr sensible Themen diskutiert und er wolle nicht, dass diese möglicherweise eines Tages öffentlich würden, weil ein Journalist diese gestützt auf das Öffentlichkeitsgesetz verlange und die Erfahrung gezeigt habe, dass man sich vor den Gerichten nicht dagegen wehren könne, sondern entsprechende Prozesse systematisch verliere.

Der Vorsteher des VBS gab aber auch an, dass er sich neben den regelmässig stattfindenden Eigner- und bilateralen Gesprächen bei Bedarf auch jederzeit direkt an den Verwaltungsratspräsidenten der RUAG wende. Er wies darauf hin, dass der

51 Vgl. Fussnote 44.

direkte Austausch immer sehr gut funktioniert habe, auch wenn es natürlich verschiedentlich heftige Diskussionen («des discussions animées») zwischen ihm und dem Verwaltungsratspräsidenten der RUAG gegeben habe.[52]

Seit die RUAG eine Stelle bzw. Kontaktperson für die Eignerbeziehungen[53] geschaffen habe (Anmerkung: Diese besteht seit dem 1. September 2017), gebe es deutlich weniger Missverständnisse als vorher und Anfragen würden in der gesetzten Frist beantwortet.

Dass der Austausch mit der RUAG auf Grund der Umstände nicht immer einfach war, insbesondere in Bezug auf Informationen zum Cyber-Angriff (vgl. dazu Kap. 2.1.1.2), wird auch durch die anderen angehörten Personen und die Auswertung der Unterlagen bestätigt. Die Unterlagen zeigen, dass das VBS verschiedene Auskünfte nicht oder erst auf Drängen erhalten hat (vgl. dazu Kap. 3 zum Schaden) oder dass die erhaltenen Auskünfte nicht fristgerecht oder inhaltlich nicht genügend waren (vgl. dazu Kap. 2). Die Vertreter des VBS wiesen in den Anhörungen[54] mehrmals darauf hin, dass sich der Departementsvorsteher immer wieder dafür einsetzen musste, um genügende Informationen zu erhalten und dass man diesbezüglich mit der RUAG an Verbesserungen arbeiten müsse. Das VBS lege aktuell grossen Wert darauf, vom Verwaltungsrat präzisere Informationen zum Geschäftstätigkeit zu erhalten, damit der Bund seine Rolle als Aktionär wahrnehmen könne. Man habe aus diesem Grund auch die Anforderungen an die RUAG bezüglich Berichterstattung an das VBS in den letzten eineinhalb Jahren erhöht.

4.1.3.3 Steuerung über die Zusammensetzung des Verwaltungsrats

Wie im Kapitel 4.1.1 erwähnt, soll der Bund grundsätzlich auf eine direkte Vertretung im Verwaltungsrat verzichten. Ein Einsitz bzw. die Entsendung einer instruierbaren Person kann aber gerechtfertigt sein, wenn sich seine Interessen ohne Vertretung nicht genügend wahrnehmen lassen.

Da sich die Zusammenarbeit zwischen Bund und RUAG im Nachgang zum Cyber-Angriff schwierig gestaltete und das VBS verschiedentlich bei der Firma intervenieren musste, um genügende Informationen zu erhalten, stellt sich für die GPK-N die Frage, ob nicht diese Situation alleine die Entsendung einer instruierbaren Vertretung rechtfertigen würde, um so dafür zu sorgen, dass den Interessen des Bundes besser Rechnung getragen wird. Neben dieser Problematik könnten aus Sicht der Kommission zudem auch die laufenden, sehr komplexen Arbeiten bezüglich der Entflechtung zwischen Bund und RUAG sowie die Abklärungen bezüglich der

52 Anhörung des Vorstehers VBS vom 26.11.2017.
53 Für die neu geschaffene Funktion des «Vice President Eignerbeziehung» hat der RUAG-Verwaltungsrat den früheren Direktor der Eidg. Alkoholverwaltung und früheren Berner Gemeinderat Alexandre Schmidt berufen.
54 Anhörung der Generalsekretärin des VBS, des Delegierten des VBS für Cyber-Defence und des Leiters Beteiligungsmanagement VBS vom 3.7.2017; Anhörung der Generalsekretärin des VBS und des Delegierten des VBS für Cyber-Defence vom 10.10.2016.

künftigen Organisation und Rechtsform bzw. der Teilprivatisierung der Firma den Einsatz eines direkten Vertreters im Verwaltungsrat begründen.

Der Vorsteher des VBS gab diesbezüglich an, der Bundesrat habe sich mit dieser Frage bisher nicht vertieft auseinandergesetzt, und wies auf die Problematik der Verantwortlichkeiten (Haftung) hin.[55] Die Generalsekretärin des VBS wies darauf hin, dass die Frage der Einsitznahme eines Bundesvertreters bei der Schaffung der Firma diskutiert worden sei und im Zusammenhang mit der Zukunft der RUAG wohl erneut thematisiert werde.[56]

4.1.3.4 Weitere Feststellungen zur Steuerung und Wahrung der Eignerinteressen

Aus den analysierten Unterlagen und Anhörungen ergeben sich für die GPK-N folgende weitere Feststellungen oder Fragen im Hinblick auf die Wahrung der Eignerinteressen des Bundes durch das VBS:

- *Kontrolle der Umsetzung der strategischen Ziele:* Wie bereits oben erwähnt, erhöhte das VBS gemäss eigener Auskunft die Anforderungen an die Berichterstattung des Verwaltungsrates der RUAG. Dieser muss nun darlegen, wie er alle Ziele und auch die Teilziele in der Berichtsperiode umgesetzt hat und Abweichungen gegenüber der Vorperiode begründen. In diesem Zusammenhang ist zu erwähnen, dass das VBS von der RUAG im Herbst 2017 Auskunft darüber verlangt habe, welche Auswirkungen die Reorganisation des Cyber-Security-Bereichs der RUAG auf die Erfüllung der strategischen Ziele des Bundesrates habe. Im entsprechenden Schreiben des Bundesrates wird auch bemängelt, dass der Vorsteher des VBS einen Tag nach einem Treffen zwischen der Generalsekretärin VBS und dem CEO der RUAG aus der Presse von einem Stellenabbau der RUAG – insbesondere auch im Bereich Cyber-Sicherheit – erfahren musste. Die RUAG nahm zu den Fragen des VBS fristgerecht Stellung. Wie die Antwort durch das VBS behandelt und bewertet wurde und ob sich daraus allenfalls weitere Fragen oder Folgen ergaben, konnte die Subkommission im Rahmen der vorliegenden Standortbestimmung nicht mehr klären.
- *Kontrolle der Umsetzung der RUAG-internen Massnahmen zur Bewältigung des Cyber-Angriffs:* Wie bereits in Kapitel 2.1.1.3 erwähnt, forderte das VBS erst mehr als ein Jahr nach der Attacke ein Reporting zu den Massnahmen der RUAG und es dauerte dann noch bis im November 2017, bis diese Berichterstattung aus Sicht des VBS den gewünschten Detaillierungsgrad und die gewünschte Qualität erreichte.
- *Bewertung der RUAG-internen Massnahmen durch das VBS:* In einer Informationsnotiz des VBS an den Bundesrat[57] wies dieses darauf hin, dass die Massnahmen zwar «korrekt» sind, dass eine Verbesserung der Cyber-

55 Anhörung des Vorstehers VBS vom 16.11.2017.
56 Anhörung der Generalsekretärin VBS vom 3.7.2017.
57 Informationsnotiz des VBS an den Bundesrat vom 10.4.2017.

Sicherheit aber nur mit einer kontinuierlichen Weiterentwicklung der Massnahmen und einem Kulturwandel in der Firma erreicht werden kann. Aus den analysierten Unterlagen und Anhörungen ist aber nicht ersichtlich, dass diese Einschätzung Folgen hatte bzw. dass das VBS diesbezüglich bei der RUAG interveniert hat und beispielsweise eine Erhöhung des Mitteleinsatzes gefordert hat.

– *Abgänge im Verwaltungsrat und in der Leitung der RUAG:* Dass verschiedene, aus Sicht der GPK-N relevante Themen, in den Eignergesprächen nicht thematisiert werden, zeigt sich auch am Beispiel der personellen Abgänge bei der RUAG. Im vergangenen Jahr wurde bekannt, dass sich der Verwaltungsratspräsident der RUAG nicht mehr zur Wiederwahl stellen will, daneben kam es aber noch zu einem weiteren Rücktritt aus dem Verwaltungsrat und zahlreichen Wechseln in der Konzernleitung (3 von 8 Mitgliedern verliessen die RUAG). Aus den Protokollen der Eignergespräche ist ersichtlich, dass diese Wechsel dort kaum thematisiert werden, auch wenn diese aus Sicht des Eigners wohl gewisse Risiken bergen (insbesondere einen Know-how-Verlust). Der Vorsteher des VBS gab an, er habe bezüglich der Abgänge keinen Einfluss genommen, sei aber über deren Gründe jeweils informiert worden. Die beiden Personen hätten ihre Abgänge jeweils mit einer gewissen Unzufriedenheit gerechtfertigt (zunehmende «Einmischung» der Politik, Salärbegrenzung). Für die Besetzung dieser Funktionen habe das VBS einen Ausschuss eingesetzt, denn die gesuchten Profile seien nicht einfach zu finden und möglicherweise auch nicht in der Schweiz.[58]

4.2 Bewertung

Auf der Basis der obigen Ausführungen lässt sich zusammenfassend festhalten, dass nicht transparent ist, inwiefern die Bewältigung des Cyber-Angriffs auf die RUAG im Rahmen der strategischen Steuerung der Firma durch das VBS aufgenommen worden ist. Denn in den formalisierten Eignergesprächen wurde der Vorfall höchstens am Rand thematisiert; während das Thema im Rahmen von bilateralen und informellen Kontakten zwischen dem Vorsteher des VBS und Vertretern der RUAG gemäss Angaben des VBS zwar aufgenommen, die Diskussion aber in keiner Weise protokolliert oder schriftlich festgehalten wurde.

Daraus und aus den obigen Beschreibungen zum Sachverhalt ergeben sich aus Sicht der GPK-N verschiedene grundsätzliche Fragen und auch Zweifel, ob das VBS die Eignerinteressen des Bundes gegenüber der RUAG angemessen vertritt bzw. durchsetzen kann. Die Kommission ist der Meinung, dass sich das VBS mit der Wahrung der Eignerinteressen des Bundes schwertut, und dies obwohl die RUAG zu 100 % dem Bund gehört.

Dies liegt einerseits sicher am teilweise unkooperativen Verhalten der RUAG selbst, welche sich immer wieder auf ihre Unabhängigkeit beruft. Diese Unabhängigkeit ist unbestritten, sie bedeutet aber aus Sicht der GPK-N nicht, dass die Firma ihre eige-

58 Anhörung des Vorstehers VBS vom 16.11.2017.

nen (Geschäfts-)Interessen höher gewichtet als die Anliegen und den Willen ihres Eigners. Die Unabhängigkeit der RUAG ist, anders als die Unabhängigkeit von Regulierungs- und Aufsichtsbehörden, weniger als «Unabhängigkeit von politischer Einflussnahme» zu verstehen, sondern sie gilt lediglich für das operative Geschäft. Die Bewältigung des Cyber-Angriffs vom Januar 2016 ist aber nicht nur eine operative Aufgabe, sondern wirft ganz klar auch strategische Fragen auf und fordert so auch den Bund als Eigner. Der Bund muss sicherstellen, dass er in ausserordentlichen Fällen wie beim Cyber-Angriff auf die RUAG, aus dem sich sowohl gewisse Risiken für die Entwicklung des Unternehmenswerts als auch für die Sicherheit der Schweiz ergaben, über den Verwaltungsrat klare strategische «Weichenstellungen» vornehmen kann, wobei diese letztlich selbstverständlich auch Einfluss auf die operative Ebene haben können.

Damit ist auch klar, dass der Bund und insbesondere das VBS mitverantwortlich ist für die aus Sicht der Kommission mangelhafte Durchsetzung der Eignerinteressen. Wie oben dargelegt, ist aus den Protokollen der Eignergespräche kein wirklicher Wille zur (strategischen) Steuerung der RUAG und zur Durchsetzung der Interessen zu erkennen. Die GPK-N bemängelt in diesem Zusammenhang insbesondere auch die offenbar wenig formalisierte Einflussnahme über bilaterale Kontakte und die fehlende Protokollierung dieser Gespräche. Diese Praxis ist aus Sicht der GPK-N schon im «Courant normal» fragwürdig, in Krisensituationen wie beim Cyber-Angriff ist sie schlicht untragbar. Denn wenn wichtige Diskussionen und Entscheide nicht festgehalten werden, fehlt dem VBS nicht nur eine solide Informationsgrundlage, sondern auch ein Führungsinstrument, um strategische Vorgaben über die Zeit durchzusetzen.

Die GPK-N ist anders als der Vorsteher des VBS dezidiert der Ansicht, dass die Eignergespräche nicht nur dazu dienen, sich über den Geschäftsverlauf der Firma informieren zu lassen, sondern auch, um wesentliche Probleme zu diskutieren und Forderungen zu stellen, insbesondere, wenn die Probleme einen Einfluss auf den Geschäftsgang haben könnten. Wenn dies u. a. aus Angst vor Indiskretionen nicht passiert, sollte das Setting und allenfalls auch der Teilnehmerkreis dieser Gespräche überdacht werden, statt auf informelle und nicht-dokumentierte Kanäle auszuweichen. Die Kommission vermag in diesem Zusammenhang auch die Argumentation des Vorstehers VBS, welcher aus Angst von BGÖ-Gesuchen auf eine Protokollierung und Notizen zu Gesprächen verzichtet, nicht zu überzeugen.

All dies führt letztlich dazu, dass dem VBS wichtige Informationen fehlen, die als Eigner bedeutsam sind. Die GPK-N konnte in diesem Zusammenhang beispielsweise nicht nachvollziehen, dass das VBS von der RUAG offenbar nie Auskünfte zu den Reaktionen der Kunden forderte, als diese genauer über den Angriff informiert wurden. Das VBS erachtet diese Auskünfte offensichtlich anders als die Kommission als nicht relevant. Dabei könnten diese wichtigen Hinweise in Hinblick auf die künftige Zusammenarbeit mit den Kunden und die Entwicklung der Auftragslage der RUAG liefern. Und bei der Entwicklung der Auftragslage und des Geschäftsgangs handelt es sich unbestritten um wichtige Informationen für den Eigner, zumal diese auch einen Einfluss auf die Zielerreichung der Firma sowie die Dividende des Bundes haben können.

Angesichts der verschiedenen Herausforderungen in Bezug auf die RUAG – Bewältigung des Cyber-Angriffs, Entflechtung der Netze von Bund und RUAG, Abklärungen zur zukünftigen Organisations- und Rechtsform der RUAG bzw. deren Teilprivatisierung – ist es für die Kommission auch nicht nachvollziehbar, dass sich das VBS und der Bundesrat bisher nicht vertieft mit der Frage nach einem (allenfalls vorübergehenden) Einsitz im Verwaltungsrat befasst haben. Denn im Corporate-Governance-Bericht ist ein solcher explizit für Fälle vorgesehen, in denen der Bund seine Interessen ohne instruierbaren Vertreter nicht genügend durchsetzen kann.

Alles in allem ist die GPK-N der Ansicht, dass die notwendigen Instrumente zur Durchsetzung der Eignerinteressen des Bundes gegenüber der RUAG zwar vorhanden sind, dass diese aber nicht angemessen genutzt werden, insbesondere vom VBS.

Empfehlung 3 Zweckmässiger Einsatz der Steuerungsinstrumente zur Wahrung der Eignerinteressen

Die GPK-N fordert den Bundesrat auf, darzulegen, wie er für einen zweckmässigen Einsatz der Steuerungsinstrumente und damit für eine bessere Wahrung der Eignerinteressen sorgen will.

Dazu gehört insbesondere auch, dass die strategische Steuerung nicht im Rahmen informeller Kontakte erfolgt, sondern im Rahmen der Eignergespräche wahrgenommen wird. Ebenso erwartet sie, dass wichtige Diskussionen und Entscheide schriftlich festgehalten werden. Schliesslich erwartet sie vom Bundesrat auch eine vertiefte Prüfung der Frage, ob es angesichts der Herausforderungen sinnvoll wäre, (allenfalls vorübergehend) einen instruierbaren Vertreter in den Verwaltungsrat der RUAG zu entsenden.

Die GPK-N hofft zudem, dass mit der Wahl des neuen Verwaltungsratspräsidenten die Grundlage für ein optimales Zusammenspiel zwischen Eigner und Verwaltungsrat geschaffen wird.

5 Schlussfolgerungen

Auf der Basis ihrer Abklärungen kommt die GPK-N insgesamt zum Schluss, dass der Cyber-Angriff auf die RUAG von Seiten des Bundes ab dem Zeitpunkt seiner Entdeckung mit der nötigen Dringlichkeit und angemessenen Massnahmen angegangen wurde. Der Bundesrat und das VBS haben jeweils rasch und zweckmässig reagiert. Die RUAG bzw. deren Leitung benötigte hingegen mehr Zeit, bis sie das Ausmass des Angriffs und die damit verbundenen Risiken anerkannte und eigene Massnahmen anordnete. Die GPK-N begrüsst es daher, dass das VBS hier Druck ausübte und aufgrund des zu Beginn nicht immer kooperativen Verhaltens der Firma verschiedentlich intervenierte. Im Übrigen erachtet es die GPK auch als sinnvoll, dass der Bundesrat den Umsetzungstand der von ihm angeordneten Massnahmen durch die EFK prüfen lässt. Sie nimmt dabei zu Kenntnis, dass die zentrale Massnahme zur Entflechtung der Netze von Bund und RUAG komplex und zeitaufwendig ist, sie ist aber auch der Ansicht, dass diese trotzdem mit grösster Dringlichkeit

vorangetrieben werden muss. In Bezug auf die von der RUAG selber eingeleiteten Massnahmen erwartet sie, dass das VBS als Eignervertreter deren Umsetzung kritisch begleitet und falls nötig interveniert.

Die GPK-N erhielt im Rahmen ihrer Abklärungen auch detaillierte Angaben über die vom Angriff betroffenen Datenverzeichnisse und die damit verbundenen Risiken. Auf der Basis dieser Informationen stuft sie den Vorfall als gravierend ein. Sie nimmt zu Kenntnis, dass die RUAG gemäss eigenen Angaben aufgrund des Cyber-Angriffs bisher keinen direkten wirtschaftlichen Schaden erlitten hat. Da sich ein solcher Vorfall aber auch indirekt oder längerfristig auf den Geschäftsgang auswirken kann, dürfen die Folgen nicht unterschätzt werden.

Eine wesentliche Frage, welche die GPK-N mit dem vorliegenden Bericht zu klären suchte, bezieht sich auf die Wahrnehmung und Wahrung der Interessen des Bundes als Eigner der RUAG. Die Kommission prüfte dabei, inwiefern der Vorfall im Rahmen der strategischen Steuerung, namentlich bei den vierteljährlichen Eignergesprächen des Vorstehers VBS mit der RUAG-Spitze aufgenommen wurde und wie der Bund bzw. das VBS als dessen Vertreter dafür sorgte, dass die Firma den Eignerinteressen des Bundes (genügend) Rechnung trägt. Dabei gelangte sie auch zu kritischen Feststelllungen. Kern davon bildet die Einschätzung, dass das VBS gegenüber der RUAG bestimmter auftreten bzw. die Eignerinteressen stärker durchsetzen muss. Die RUAG gehört zu 100 % dem Bund. In der Privatwirtschaft üben schon Minderheitsaktionäre mit einem substantiellen Aktienanteil grossen Druck auf die Unternehmungen aus.[59]

Die Instrumente, um Einfluss zu nehmen, sind dabei aus Sicht der GPK-N ausreichend. Als besonders wichtig erachtet sie dabei die Vorgabe strategischer Ziele und deren Überprüfung, insbesondere auch im Rahmen der regelmässigen Eignergespräche. Bei diesen Gesprächen sollte es aus Sicht der GPK-N nicht bloss um eine Information zum Geschäftsgang gehen. Sondern diese sind auch zu nutzen, um wesentliche Probleme wie ein solcher Cyber-Angriff sowie deren mögliche Folgen für die Erreichung der strategischen Ziele zu diskutieren, Forderungen zu stellen oder Aufträge zu erteilen – sprich die Wahrung der Eignerinteressen zu gewährleisten. Für die GPK-N ist daher nicht nachvollziehbar, dass die Bewältigung und die Konsequenzen des Cyber-Angriffs im Rahmen der Eignergespräche zwischen dem VBS und der RUAG auf der strategischen Ebene kaum thematisiert wurden. Die GPK-N anerkennt zwar, dass es nicht Aufgabe des Bundesrates ist, auf der operativen Ebene zu führen. Wenn aber Probleme auf dieser Ebene bestehen, welche die Eignerinteressen beeinträchtigen können und damit auch die strategische Ebene tangiert sein könnte, so gilt es seitens des Bundesrates bzw. des VBS zu handeln.

Im Weiteren ist die GPK-N dezidiert der Ansicht, dass wichtige Diskussionen nicht bloss in einem informellen Rahmen geführt werden können, ohne dass die Kernpunkte in geeigneter Form schriftlich festgehalten werden. Denn damit fehlt dem VBS sowohl die notwendige Informationsgrundlage wie auch eine Möglichkeit bzw.

[59] Vgl. beispielsweise den Fall der Credit Suisse, bei dem ein Investor bzw. ein Hedge-Fund mit rund 0,3 % Aktienkapitel im Herbst 2017 die Aufspaltung der Grossbank in mehrere Teile forderte und dafür öffentlich Druck aufbaute, auch wenn die Erfolgschancen gering schienen (NZZ vom 17.10.2017: Hedge-Fund will die Credit Suisse aufspalten – und jetzt?).

ein Führungsinstrument, um Forderungen bzw. strategische Vorgaben durchzusetzen. Dies schwächt den Eigner bzw. erschwert die Wahrung und Durchsetzung der Eignerinteressen über die Zeit.

Ein anderes wichtiges Instrument der strategischen Steuerung bildet die Wahl des Verwaltungsrates. Die Kommission ist der Ansicht, dass schon bei der Wahl der Verwaltungsräte und insbesondere des Verwaltungsrats-Präsidenten darauf geachtet werden muss, dass sich diese hinter die Zielvorgaben des Bundesrates stellen und diesen dann auch Rechnung tragen. Falls dies nicht erfolgen würde, wäre auch auf dieser Ebene zu handeln.

Die GPK-N erwartet daher vom VBS, dass es in Zukunft gegenüber der RUAG bestimmter auftritt und sich bei Bedarf stärker für die Forderungen des Bundes eintritt bzw. die Eignerinteressen durchsetzt. In ihren drei Empfehlungen richtet sich die Kommission hingegen an den Bundesrat und verlangt von diesem verschiedene Abklärungen, welche zu Verbesserungen der Corporate-Governance führen sollen.

6 Weiteres Vorgehen

Die GPK-N ersucht den Bundesrat, bis spätestens am *28. September 2018* zu den obigen Ausführungen und Forderungen Stellung zu nehmen.

8. Mai 2018

Im Namen der Geschäftsprüfungskommission des Nationalrates

Die Präsidentin der GPK-N:
Nationalrätin Doris Fiala

Die Präsidentin der Subkommission EDA/VBS:
Nationalrätin Ida Glanzmann-Hunkeler

Die Sekretärin der GPK:
Beatrice Meli Andres

Die Sekretärin der Subkommission EDA/VBS:
Céline Andereggen

Abkürzungsverzeichnis

BIT	Bundesamt für Informatik und Telekommunikation
EDA	Eidg. Departement für auswärtige Angelegenheiten
EFD	Eidg. Finanzdepartement
EFK	Eidg. Finanzkontrolle
FinDel	Finanzdelegation der Eidg. Räte
GPDel	Geschäftsprüfungsdelegation
GPK	Geschäftsprüfungskommissionen
GPK-N	Geschäftsprüfungskommission des Nationalrates
ISB	Informatiksteuerungsorgan des Bundes
KGSi	Kerngruppe Sicherheit
NDB	Nachrichtendienst des Bundes
SiA	Sicherheitsausschuss des Bundesrates (weitere Erläuterung?)
VBS	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport

Verzeichnis der angehörten Personen

Falcone-Goumaz, Nathalie*	Generalsekretärin VBS
Fischer, Peter	Delegierter / Leiter ISB
Frauenknecht, Marcel	Leiter IKT-Sicherheit, ISB
Parmelin, Guy*	Bundesrat, Vorsteher des VBS
Rothenbühler, Stephan	Leiter/in Beteiligungsmanagement, GS VBS
Vernez, Gérald*	Delegierter des VBS für Cyber-Defence

* *Personen wurden mehrmals angehört*