Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 186 (2020)

Heft: 4

Artikel: Wunsch und Wirklichkeit

Autor: Müller, Peter / Ruef, Marc

DOI: https://doi.org/10.5169/seals-880752

Wunsch und Wirklichkeit

Cyber Security ist eine der strategischen Herausforderungen der Zukunft. Das VBS unternimmt erhebliche Anstrengungen, um diesbezüglich gewappnet zu sein. Die RUAG versuchte in den vergangenen Jahren, einen entsprechenden Geschäftsbereich neu aufzubauen. Das Vorhaben scheiterte nicht zuletzt aus Kommunikationsgründen kläglich. Der Bundesrat hat daraus erste Lehren gezogen; es ist jedoch fraglich, ob diese ausreichend sind.

Peter Müller, Marc Ruef, Redaktoren ASMZ

Mit dem Aufkommen des *Internet of Things* und der weltweiten Vernetzung rückte die Cyber Security, gemeinhin die Sicherheit der Informationstechnologie, immer mehr in den Fokus der Öffentlichkeit. Angesprochen sind alle: Privatpersonen, Unternehmen, die öffentliche Hand wie auch die Armee. Sowohl die Bundesverwaltung als insbesondere auch das VBS unternahmen diesbezüglich in den vergangenen Jahren beachtenswerte Anstrengungen. Stichworte dazu sind beispielsweise: Nationale Strategien zum Schutz der Schweiz von Cyber-Risiken (NCS, 2012 und 2018), Cyber-Defence Campus bei armasuisse und an der ETH Zürich, neues Berufsbild «Cyber Security Specialist mit Eidg. Fachausweis» oder der neue 40-wöchige Cyber-Lehrgang der Schweizer Armee. Die ASMZ berichtete verschiedentlich darüber (siehe unter anderem Nr. 01-02/2020, S. 20–21 und Nr. 03/2020, S. 38–41).

Die RUAG, eine 100%ige Tochter des Bundes, erkannte die strategische Bedeutung des Themas Cyber Security schon vor mehreren Jahren. Mittels Eigenentwicklungen und einem bedeutenden Firmenzukauf baute sie schrittweise eine eigene Geschäftseinheit Cyber Security mit zuletzt über 200 Mitarbeitenden auf. Nach der durch den Bundesrat beschlossenen Reorganisation der RUAG erfolgte Ende 2019 die überraschende Auflösung dieser Geschäftseinheit und der Rückzug aus der Cyber Security-Strategie des Konzerns (siehe Kasten «Meilensteine»). Was war geschehen? Mittels schriftlichen Interviews sowohl beim VBS wie auch bei der RUAG und nach Auswertung umfangreicher öffentlich zugänglicher Dokumente soll hier versucht werden, gewissermassen die Chronik eines Scheiterns nachzuzeichnen.

Cyber Defence RUAG (Meilensteine)

Datum	Ereignis
2015	Eigenentwicklung und Inbetriebnahme des RUAG Traffic Analyzer (RTA)
19.10.2015	Inbetriebnahme der Cyber Training Range (Schulungszentrum)
Januar 2016	Aufdeckung durch Dritte eines Cyber-Angriffs auf die RUAG
2016	Schaffung der neuen Business Unit Cyber Security bei RUAG Defence
20.12.2016	Übernahme des britischen Cyber Security Spezialisten «Clearswift»
01.01.2018	Business Unit Cyber Security wird direkt dem CEO unterstellt
18.03.2019	Beschluss Bundesrat: Entflechtung der RUAG in zwei Subholdings
18.03.2019	Zuordnung der Business Unit Cyber Security zu RUAG International
18.03.2019	Grundsatzbeschluss zum Verkauf von «Clearswift»
02.12.2019	Verkauf «Clearswift» an amerik. Unternehmen Help-Systems
02.12.2019	Auflösung der Business Unit Cyber Security

Quelle: RUAG, Medienmitteilungen, Geschäftsberichte und weitere Publikationen

Bisherige Eignerstrategie RUAG (Auszug)

Der Bundesrat erwartet, dass die RUAG

- die Schweizer Armee bei der Instandhaltung der Systeme und der Sicherstellung der Einsatzbereitschaft als industrieller Partner unterstützt;
- in der Schweiz Schlüsselkompetenzen erhält und weiterentwickelt, die für die Schweizer Armee oder den Bund von strategischer Bedeutung sind;
- den Aktionär bei bedeutenden Kooperationen und Beteiligungen vorgängig informiert und ihm die Konformität der geplanten Massnahmen mit den hier aufgeführten strategischen Zielen bestätigt;
- Geschäftsfelder veräussert, die für den Aktionär und die RUAG nicht von strategisch-industrieller Logik sind;
- zwischen dem Aktionär und dem Verwaltungsrat der RUAG Holding quartalsweise Aussprachen stattfinden.

Quelle: Strategische Ziele des Bundesrates für die RUAG Holding AG 2016–2019 (https://www.newsd.admin.ch/newsd/message/attachments/42355.pdf)

Eigentümer, Auftraggeber und Kunde

Zur besseren Einordnung der nachfolgenden Ausführungen sei einleitend noch einmal in Erinnerung gerufen: Der Bund (vertreten durch das VBS) ist Alleineigentümer der RUAG. Er steuert seine Tochtergesellschaft mittels einer sogenannten Eignerstrategie. Diese wird durch den Gesamtbundesrat alle vier Jahre neu beschlossen. Es handelte sich bisher jeweils um ein rund zweiseitiges Dokument, welches neben strategischen Schwerpunkten auch finanzielle und personalpolitische Ziele vorgab, Kooperationen und Beteiligungen regelte und die Berichterstattung ansprach. Ein Auszug der wesentlichsten Punkte ist im Kasten «Bisherige Eignerstrategie RUAG» zusammengefasst.

Dem Bund kommt dabei eine nicht ganz alltägliche und auch nicht konfliktfreie Rolle zu: Als Eigentümer ist er an einer gewinnorientierten Unternehmung mit möglichst hoher Dividendenausschüttung interessiert. Als Auftraggeber (z.B. armasuisse) kämen ihm Direktvergaben ohne Wettbewerb am gelegensten. Und als Kunde (z.B. Schweizer Armee) möchte er möglichst kostengünstige und trotz-

dem wettbewerbsfähige Produkte erhalten. Umgekehrt bietet sich dem Bund die einmalige Gelegenheit, mittels Direktzugriff strategische Projekte gewissermassen «inhouse» voranzutreiben und so tendenziell von massgeschneiderten, preisattraktiven Lösungen zu profitieren. Wurden diese Chancen sowohl auf Seiten Bund wie auch auf Seiten RUAG genutzt?

Nicht auf Bedürfnisse der Armee ausgerichtet

2015 entwickelte die RUAG in eigener Regie den *Traffic Analyzer* (Ziel: Rechtzeitiges Erkennen von Anomalien im elektronischen Datenverkehr und Einleiten von Gegenmassnahmen). Parallel baute sie ihre *Cyber Training Range* auf (Schulungszentrum, um «die richtigen Entscheidungen zur richtigen Zeit zu treffen»). Die ASMZ hat darüber ausführlich berichtet (siehe Nr. 03/2016, S. 36–37). Das VBS war weder Treiberin dieser beiden Projekte noch in deren Entwicklung involviert. Zweck war gemäss RUAG vielmehr, «Unternehmen oder Behörden zu ermöglichen, sich im geschützten Rahmen mit dem Thema auseinanderzusetzen». Das VBS war lediglich «ein potenzieller Kunde». Es nutzte die Dienstleistungen der *Cyber Training Range* ein einziges Mal im Rahmen einer integralen Übung des Sicherheitsverbunds Schweiz.

Auf die Gründe der fehlenden Zusammenarbeit angesprochen, will sich die RUAG nicht dazu äussern. Das VBS legt demgegenüber offen dar, «die Dienstleistung sei nicht auf die Bedürfnisse der Armee ausgerichtet» gewesen, so dass sich die FUB für eine eigene Lösung entschied, «die sie vollständig unter ihrer Kontrolle hatte». Ergänzend wird darauf hingewiesen, die *Cyber Training Range* sei «für den offenen Markt» konzipiert gewesen; dabei sei dem Fakt zu wenig Rechnung getragen worden, dass in der Armee neben Profis «auch die Milizkomponente ausgebildet und eingesetzt werden müsse».

Hackerangriff und Datenabfluss

Erschwerend kam für die RUAG hinzu, dass sie während des Aufbaus der neuen Geschäftseinheit Cyber Security mit den beiden oben beschriebenen Hauptkomponenten von einem schwerwiegenden Hackerangriff betroffen war, den sie nicht selbst bemerkte. Erst Hinweise von aussen – unter anderem von Bundesstellen – legten das Datenleck offen. Wegen der engen, historisch bedingten Verknüpfung der EDV-Systeme von RUAG und VBS kam es auch zu einem Datenabfluss geheimer Dokumente beim VBS. Diese enge Verknüpfung wurde denn in der Folge vordergründig auch immer als eines der Hauptargumente aufgeführt, weshalb die RUAG in zwei völlig getrennte Subholdings aufgespalten werden müsse. Dieser Hackerangriff erfolgte zum denkbar unglücklichsten Zeitpunkt. Zusammen mit der ungenügenden oder gar fehlenden Ausrichtung auf die Bedürfnisse der Armee litt der Aufbau der neuen (strategischen) Geschäftseinheit Cyber Security unter ungünstigen Voraussetzungen und Rahmenbedingungen.

Ungenügende Kommunikation

Auf dem «Weg zu einem der führenden Cyber Security Spezialisten» realisierte die RUAG Ende 2016 einen wesentlichen Schritt: Sie übernahm den britischen Spezialisten «Clearswift». Dieser Erwerb wurde am 20.12.2016 kommuniziert. Der Kaufpreis wurde nicht offiziell bekanntgegeben; je nach Quelle und Lesart lag er wohl zwischen 55 und 87 Mio. CHF. Bereits im Vorfeld dazu, speziell aber im darauffolgenden Jahr, betonte die RUAG immer wieder die strategische Bedeutung und den Wachstumseffekt der Geschäftseinheit Cyber Security (siehe Kasten «Aussagen zur strategischen Bedeutung»). Die ganze Euphorie gipfelte darin, angeblich zur weiteren Stärkung des Wachstums diese Geschäftseinheit ab 01.01.2018 neu auf Konzernebene anzugliedern.

Der Bund bzw. das dossierverantwortliche VBS wurde über die Kaufpläne «zu einem sehr späten Zeitpunkt informiert», nämlich erst am Eignergespräch vom 13.12.2016, also genau eine Woche vor Vertragsunterzeichnung und der offiziellen Kommunikation der Übernahme. Der damalige Chef VBS zeigte sich wenig erfreut über dieses Vorgehen und er verlangte von der RUAG eine «Bestätigung, dass die Akquisition mit den strategischen Zielen des Bundesrates konform sei». Diese Erklärung wurde am 13.01.2017 nachgeliefert. Die ungenügende Kommunikation und die fehlenden Absprachen bescherten ein weiteres Mal suboptimale Startbedingungen.

Ungleiche Verhandlungspartner

Damit wird eine Schwachstelle im Umgang zwischen Eigner und Tochter offensichtlich: Der Bundesrat delegiert die Aufsicht über die RUAG an das VBS; innerhalb des VBS ist ein Sachbearbeiter (zum damaligen Zeitpunkt ein Jurist) offiziell Delegierter für die Umsetzung der Eignerstrategie. Diesem fehlten – neben der nötigen Hierarchie – aus naheliegenden Gründen die industriell/betriebs-

Cyber Security: Aussagen zur strategischen Bedeutung

2015: «Im Bereich Cyber Security will RUAG Defence zum kompetenten Partner für Armeen und zivile Organisationen werden.»
2016: «Für die Zukunft des ganzen Konzerns zentral ist die Entwicklung der neu formierten Business Unit Cyber Security.»
2016: «Unter den Aktivitäten, die das profitable Wachstum in den nächsten Jahren sicherstellen, sind die Investitionen in den strategischen Wachstumsbereichen Flugzeugstrukturbau, kommerzielle Raumfahrt und Cyber Security hervorzuheben.»
2016: «Clearswift wird uns dem Ziel, RUAG Defence zu einem der führenden Cyber Security Spezialisten zu entwickeln, einen grossen Schritt näherbringen.»
2017: «Der Bereich Cyber Security zählt zu den wichtigsten Wachstumspfeilern der RUAG.»
2017: «Dank eigenständiger Einheit auf Konzernebene wird die Business Unit Cyber Security ab 01.01.2018 für das geplante und notwendige Wachstum zusätzlich gestärkt.»
2017: «Vielversprechend sind die Aussichten der drei strategischen Wachstumspfeiler Space, Flugzeugstrukturbau und Cyber Security.»
2017: «Für die Business Unit Cyber Security wird auch 2018 der weltweite Megatrend Digitalisierung der Wachstumstreiber sein.»
2018: Zur Business Unit Cyber Security und zu Clearswift erfolgen im Geschäftsbericht keine Ausführungen mehr.
2019: «Mit der Entscheidung des Bundesrates zur Entflechtung von RUAG endet die Cyber Security Strategie des Konzerns. Damit bringen wir unsere Aktivitäten im Bereich Cyber Security im Einklang mit unserer Strategie zu einem erfolgreichen Abschluss.»

Quelle: RUAG, Geschäftsberichte und Medienmitteilungen

+ASMZ
Sicherheit Schweiz

Abo-Bestellcoupon ASMZ
Zum Monatsanfang in Ihrem Briefkasten

Bitte Zutreffendes ankreuzen

Preise inkl. MwSt.

☐ Jahresabo Fr. 78.– / Ausland Fr. 98.–

☐ Einzelausgabe Fr. 8.– / Ausland Fr. 12.–

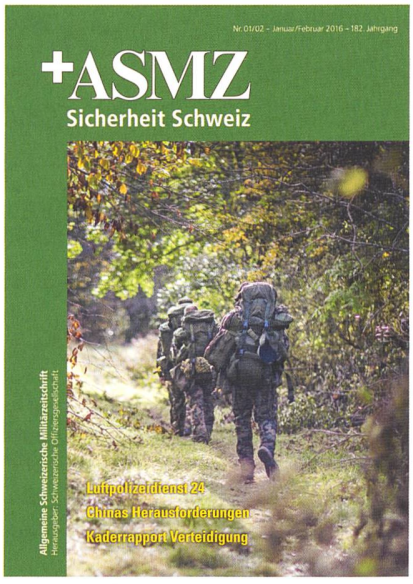
Name: _____ Vorname: _____

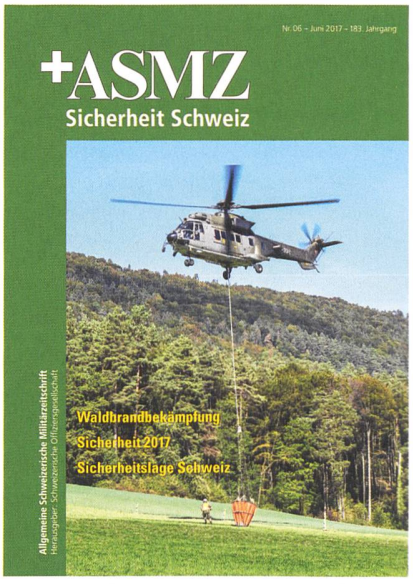
Strasse: _____ PLZ/Ort: _____

Telefon Nr: _____ E-Mail: _____

Datum: _____ Unterschrift: _____

Verlag Equi-Media AG
Brunnenstrasse 7
Postfach 732
8604 Volketswil
Telefon 044 908 45 65
Fax 044 908 45 40
abo@asmz.ch
www.asmz.ch





Allgemeine Schweizerische Militärzeitschrift
Herausgeber: Schweizerische Offiziersgesellschaft

wirtschaftlichen Fachkenntnisse, um den Konzernverantwortlichen der RUAG auf Augenhöhe begegnen zu können. Und falls er sich doch mal getraute, etwas konkret zu fordern, so wurde das Ungebetene mit Top-Gesprächen und/oder auf politischem Weg zurechtzubiegen versucht.

Dass – wie im vorliegenden Fall – der Akteur im Nachhinein die «Richtigkeit» seines Vorgehens und die Übereinstimmung mit den strategischen Vorgaben bestätigen muss, entspricht zwar dem Wortlaut der damals gültigen Eignerstrategie RUAG. Aber eigentlich müsste der Eigner selbst kritisch überprüfen, ob seine Vorgaben eingehalten werden. Man erkennt hier ein verbreitetes Handlungsmuster in der Bundesverwaltung (wie beispielsweise auch im Seilbahnbereich): Mangels genügender personeller und fachlicher Qualitäten in der Verwaltung, wird der «Nachweis» des gesetzeskonformen Verhaltens an den Ausführenden delegiert. Ob damit die Objektivität Schritt halten kann?

Abschied von Cyber Security

Gewisse Beobachtungen im darauffolgenden Geschäftsjahr warfen zwar Fragen auf: Weshalb verlor die RUAG im Jahresbericht 2018 unvermittelt kein einziges Wort mehr zur Geschäftseinheit Cyber Security und zu «Clearswift»? Trotzdem kamen der Verkauf von «Clearswift» am 02.12.2019 und die ersatzlose Auflösung der Geschäftseinheit Cyber Security wohl für die meisten überraschend. Weshalb nahm die RUAG (also eine Tochter) von einem strategischen Geschäftsbereich Abschied, obwohl der Bund (also der Eigentümer) zeitgleich seine Anstrengungen in diesem Bereich markant verstärkte? Eine indirekte erste Antwort ergibt sich aus dem folgenden Tatbestand: Das VBS ist daran, eine neue Cyber Strategie zu erarbeiten, welche bis im Herbst 2020 vorliegen soll. Die RUAG ist nicht in diese Arbeiten involviert! Fachwissen und Zusammenarbeit: Irgendwo scheinen da Diskrepanzen zu bestehen.

Die offizielle Begründung der RUAG für ihren bemerkenswerten Rückzug lautet wie folgt: Einerseits gehöre Cyber Security («Clearswift») nicht zu RUAG International, wo man sich neu auf den Aerospace-Bereich konzentriere und eng mit dem Ausland vernetzt sei; andererseits passe dieser Bereich auch nicht zu RUAG MRO Schweiz, wo man sich «grundsätzlich auf die Bedürfnisse der Armee fokussiere» und «auf international ausgerichtete Geschäftstätigkeiten weitestgehend verzichte». Der Verkauf sei folglich eine logische Konsequenz. Vor allem aber betonen sowohl das VBS wie auch die RUAG, der Entscheid «basiere auf dem vom Bundesrat genehmigten Konzept der Entflechtung und Weiterentwicklung der RUAG», erfolge also mithin «in Absprache mit dem Eigner». Es sei bloss als Randnotiz darauf hingewiesen: Nach einem gescheiterten Eigenversuch übertrug der Bundesrat die Federführung zur Reorganisation der RUAG und deren Geschäftsleitung. Damit wären wir wieder bei den ungleichen Verhandlungspartnern.

Lehren zeichnen sich ab

Gewisse Fragen bleiben weiterhin im Raum. Die beiden wichtigsten sind: Warum kann oder will die Tochterunternehmung der Strategie der Eignerin nicht besser folgen? Weshalb wird ein hochgelobtes neues Strategiefeld innerhalb von knapp zwei Jahren totgeschwiegen und ersatzlos fallengelassen? Mehrere personelle Wechsel an der Spitze der RUAG können im Nachhinein Erklärungsansätze liefern. Aber noch selten haben Wunsch und Wirklichkeit sowohl auf Seiten des Bundes wie auch der RUAG derart auseinandergeklafft.

Die Geschäftsprüfungskommission des Nationalrats (GPK-N) hat einzelne Forderungen schon Mitte 2018 beim Bundesrat deponiert: Der Bundesrat und das VBS müssten «gegenüber der RUAG bestimmter auftreten und sich stärker für die Wahrung der Interessen des Bundes einsetzen». Die kommende Transformation «stelle besonders hohe Anforderungen an den Bund als Eigner der RUAG». Deshalb erwarte die GPK-N, dass «das VBS und die EFV diese eng und kritisch begleiten und die nötigen Ressourcen bereitstellen».

Die neue Eignerstrategie RUAG, welche durch den Bundesrat auf den 1. November 2019 in Kraft gesetzt wurde, ist denn auch viel detaillierter ausgefallen und umfasst neu sieben Seiten. Unter anderem finden sich präzisiere Regelungen zur Informationspolitik, zum Unternehmensrisikomanagement, zum Geschäftsgeheimnis und zur Zusammenarbeit generell (siehe Kasten). Nun müssen die neuen Ideen einfach noch gelebt werden. Etwas befremdend wirkt dabei, dass unter den strategischen Schwerpunkten von RUAG International recht detaillierte Vorgaben aufgeführt sind, wie und wann nicht mehr benötigte Konzernteile zu veräussern sind (z.B. RUAG Ammotec, Simulation & Training), zu Cyber Security jedoch Ausführungen fehlen. ■

Neue Eignerstrategie RUAG (Auszug)

Der Bundesrat erwartet von der Beteiligungsgesellschaft, dafür zu sorgen, dass die RUAG MRO Holding AG und die von dieser direkt oder indirekt kontrollierten Unternehmen

- die Schweizer Armee bei der Instandhaltung (Wartung, Inspektion, Instandsetzung) der ihr zugewiesenen Systeme sowie bei der Integration von neuen Komponenten in diese Systeme unterstützen;
- zugunsten der Armee die Rolle als industrieller Partner wahrnehmen, Dienstleistungen erbringen und das notwendige Ingenieur- und IKT-Wissen pflegen und weiterentwickeln;
- grundsätzlich die Rolle des Materialkompetenzzentrums (MKZ-Rolle) für neue, sicherheitsrelevante und komplexe Systeme wahrnehmen;
- sie ihn beim Eingehen von bedeutenden Kooperationen oder beim Veräussern von bedeutenden Beteiligungen vorgängig konsultieren;
- über ein Unternehmensrisikomanagementsystem verfügen, das sich an der ISO-Norm 31000 orientiert, und den Eigner über die wichtigsten Unternehmensrisiken informieren;
- quartalsweise für Aussprachen mit dem Eigner der Beteiligungsgesellschaft, vertreten durch das VBS und das EFD (EFV), zur Verfügung stehen;
- sich dabei auch gegenüber dem Verwaltungsrat der Beteiligungsgesellschaft nicht auf das Geschäftsgeheimnis der Subholdings und der von diesen direkt oder indirekt kontrollierten Unternehmen berufen;
- das VBS und das EFD (EFV) zudem über Tatsachen oder Beschlussfassungen im Konzern, die geeignet erscheinen, die Erreichung der strategischen Ziele erheblich zu beeinflussen, rechtzeitig und sachgerecht informieren;
- gemeinsam mit dem VBS geeignete Massnahmen zur Optimierung der Zusammenarbeit mit dem VBS ausarbeiten.

Quelle: Strategische Ziele des Bundesrates für die BGRB Holding AG 2020–2023 (http://www.admin.ch/opc/de/federalgazette/2020/961.pdf)