Beschaffungspolitik im Kreuzfeuer

Autor(en): **Müller, Peter**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **184 (2018)**

Heft 12

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-813276

Beschaffungspolitik im Kreuzfeuer

Am diesjährigen Anlass von «Chance Miliz» standen zwei Themen im Zentrum: Welche Planungs- und Beschaffungsprozesse stehen hinter einem konkreten Rüstungsvorhaben? Welche Bedeutung hat die heimische Rüstungsindustrie für die Schweizer Sicherheitspolitik und insbesondere für die Armee? Grundlegende praktische Umsetzungsfragen blieben leider offen.

Peter Müller, Redaktor ASMZ

Die Zentralschule und die Kantonale Offiziersgesellschaft Luzern organisieren jährlich den Anlass «Chance Miliz». Am 3. November 2018 trafen sich über 200 Teilnehmende im Armeeausbildungszentrum (AAL) zur 15. Veranstaltung. Unter dem Thema «Beschaffungspolitik im Kreuzfeuer – Wie rüstet sich die Armee für die Zukunft?» wurde versucht, «hinter die Schlagzeilen zu blicken».

Nötig, möglich, umsetzbar?

Der Kommandant der Zentralschule Luzern, Br Peter Baumgartner, legte einleitend seinen Fokus auf die Finanzen. Mit dem Beschluss des Bundesrates vom 8. November 2017, für den Schutz des Luftraums insgesamt acht Mia. CHF zu investieren, sei ein wichtiger Eckstein gesetzt worden. Man wisse aber auch, dass für alle Erneuerungsvorhaben der Armee bis 2032 insgesamt 13–15 Mia. CHF erforderlich seien. Aus Spargründen sei der aktuelle vierjährige Zahlungsrahmen für die Armee bereits wieder auf rund 19,3 Mia. CHF geschrumpft. Die WEA kämpfe folglich mit den gleichen Problemen wie die Armee XXI. Vom vorgegebenen Ziel der Amerikaner, die westlichen Staaten müssten 2% ihres Bruttoinlandprodukts für Verteidigungsausgaben zur Verfügung stellen, sei die Schweiz mit – je nach Lesart – 0,7 bis 1,0% noch deutlich entfernt. Im Raum stünden deshalb mehr denn je die folgenden drei Fragen: Was ist nötig, was ist möglich und was ist politisch umsetzbar?

> **«Ist es verantwortbar, unseren Soldaten keine ausreichende Ausrüstung zur Verfügung zu stellen?»**
>
> Br Peter Baumgartner, Kdt ZS Luzern

Fähigkeitsorientierung

Divisionär Claude Meier, Chef Armeestab, rief in Erinnerung, dass anstelle einer bedrohungs- heute eine fähigkeitsorientierte Streitkräfteplanung erfolge. Die Unklarheit über künftige militärische Konflikte und die Vielfalt an möglichen Konfliktformen (meist in Kombination) gebiete es, flexibel «auf nicht vorhersehbare Ereignisse reagieren zu können». Dies bedinge auch einen «Blick in die übernächste Geländekammer» (nach 2030). Er rief in Erinnerung, dass die Armee ein Gesamtsystem darstelle; werde irgendwo geschraubt, so habe dies Auswirkungen auf viele andere Bereiche. Er zeigte auf, welche grösseren Systeme im Anschluss an das Programm «Air2030» (NKF und BODLUV) zu ersetzen seien, ohne dies allerdings zeitlich und inhaltlich zu präzisieren.

Gesucht: Spezialitäten

Urs Breitmeier, CEO der RUAG, wies darauf hin, dass früher noch mehrere Waffensysteme in der Schweiz hergestellt wurden. Heute konzentriere sich die rüstungsindustrielle Tätigkeit primär auf Wartung, Instandhaltung und Wertsteigerung. Zu bedenken sei auch, dass das industrielle Mengengerüst heute auf den Ausbildungs- und nicht auf den Konfliktfall ausgelegt sei. Verschiedenen Autonomiestufen (vom Tagesparkdienst bis zur eigenständigen Entwicklung/Herstellung) stünden häufig abnehmende Autonomiegrade bei der Beschaffung gegenüber (Lizenzproduktion, Endmontage oder – heute – Kauf ab Stange). Er bedauerte, dass die Schweizer Rüstungsindustrie kaum in internationale Kooperationsprojekte eingebunden sei und nur wenige nationale Entwicklungsprojekte bestünden. Er plädierte für eine weniger restriktive Exportpraxis und für Spezialitäten, um diese Schwächen zu kompensieren: Die Schweizer Rüstungsindustrie müsse andern nützen, um uns so interessant zu machen.

Offene Fragen (Beispiele)

- Wie sehen die Beschaffungsvorhaben auf der Zeitachse aus (Br Peter Baumgartner)?
- Ist die Schweizer Rüstungsindustrie gegenüber Europa und der NATO nicht konkurrenzfähig (Frage aus dem Publikum)?
- Wie definiert und begründet sich die «vollständige Ausrüstung» (SR Josef Dittli)?

Bekannte Schlagzeilen

Das abschliessende Streitgespräch zwischen Ständerat Josef Dittli (Präsident SiK Ständerat) und Nationalrat Fabio Molina sowie die Podiumsdiskussion mit diesen Parlamentariern, den Referenten sowie Oberst i Gst Stefan Holenstein (Präsident SOG) und Eva Novak (Journalistin Neue Luzerner Zeitung) brachte zwar ein paar «süffige» Dispute. Aber sie kamen leider kaum über die bekannten Schlagzeilen hinaus: Armeeabschaffung, Art. 58 BV (Auftrag der Schweizer Armee), Wachstum der Bundesausgaben, Kriegsmaterialexporte, vollständige Ausrüstung der Armee oder Kommunikationsdefizite bei VBS und armasuisse. Der «Blick hinter die Schlagzeilen» erschöpfte sich in Fragen, die unbeantwortet blieben (siehe Kasten). ■

> **«Eine Armee ist genauso stark wie ihre Industriebasis.»**
>
> Urs Breitenmeier, CEO RUAG

Teile und herrsche: Cyber-Sicherheit durch Fusionszentren

Effektive Cyber-Abwehr erfordert die Kombination relevanter Information aus einer Vielzahl von Quellen und Organisationen. Fusionszentren sind eine öffentlich-private Organisationsform, in der diese Kombination stattfindet. Das Ziel ist die Schaffung eines komplexen Lagebildes, das eine schnellere und präzisere Cyber-Abwehr ermöglicht.

Marcus M. Keupp, Dimitri Percia David, Alain Mermoud

Unser letzter Artikel in der ASMZ 07/2018 präsentierte einige Erkenntnisse, wie und warum die Cyber-Sicherheit durch Informationsaustausch in *Information Sharing and Analysis Centers (ISACs)* verbessert wird. In diesem Artikel dehnen wir unsere Betrachtungen auf Fusionszentren *(fusion centers)* aus.

Das Teilen sicherheitsrelevanter Informationen innerhalb von ISACs hat den Nachteil, dass pro Transaktion nur ein diskreter Informationswert geteilt wird. Die für eine effektive Cyber-Abwehr komplexer Bedrohungen notwendige Information ist zudem zwischen vielen Organisationen und Akteuren fragmentiert, sodass die Gewinnung eines vollständigen Lagebildes teuer ist oder lange dauert. Trotz umfassender Aufklärungsbemühungen kommt daher ein nur unvollständiges Lagebild zustande. Abbildung 1 illustriert schematisch diese Problematik.

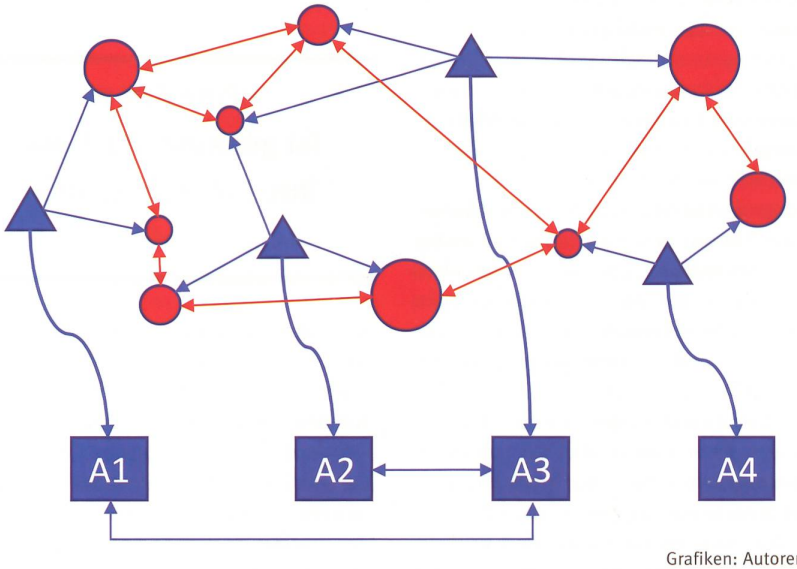
Die Akteure A1 bis A4 haben jeweils einen Sensor in einer hybriden gegnerischen Struktur etabliert. Jede dieser Quellen liefert Information zugunsten jedes einzelnen Akteurs. Obwohl jedes gegnerische Strukturelement von mindestens einer Quelle beobachtet wird, besitzt kein einzelner Akteur ein korrektes oder auch nur vollständiges Lagebild. Im Gegenteil erhält er nur fragmentierte Information, die die gegnerische Struktur unzureichend beschreibt. Erschwerend kommt hinzu, dass die Akteure ihre fragmentierte Information nicht unbedingt miteinander teilen. Der Akteur 3 tauscht zwar Information mit den Akteuren 1 und 2, nicht jedoch mit Akteur 4 aus. Akteur 1 spricht nicht mit Akteur 2, und Akteur 4 teilt überhaupt keine Informationen. Diese Fragmentierung der Nachrichtenlage macht eine Entschlussfassung daher riskant, wenn nicht gar unmöglich.

Die Idee eines Fusionszentrums ist es, diese Fragmentierung durch die Integration der Informationen aller Akteure zu beenden. Abbildung 2 illustriert den angestrebten Zustand. Alle Akteure speisen ihre individuell gewonnenen Erkenntnisse in das Fusionszentrum ein. Durch Verknüpfung der einzelnen Informationen ist es nun möglich, ein vollständiges Lagebild zu erstellen und zielführende Entschlüsse zu fassen.

Fusionszentren – de quoi s'agit-il?

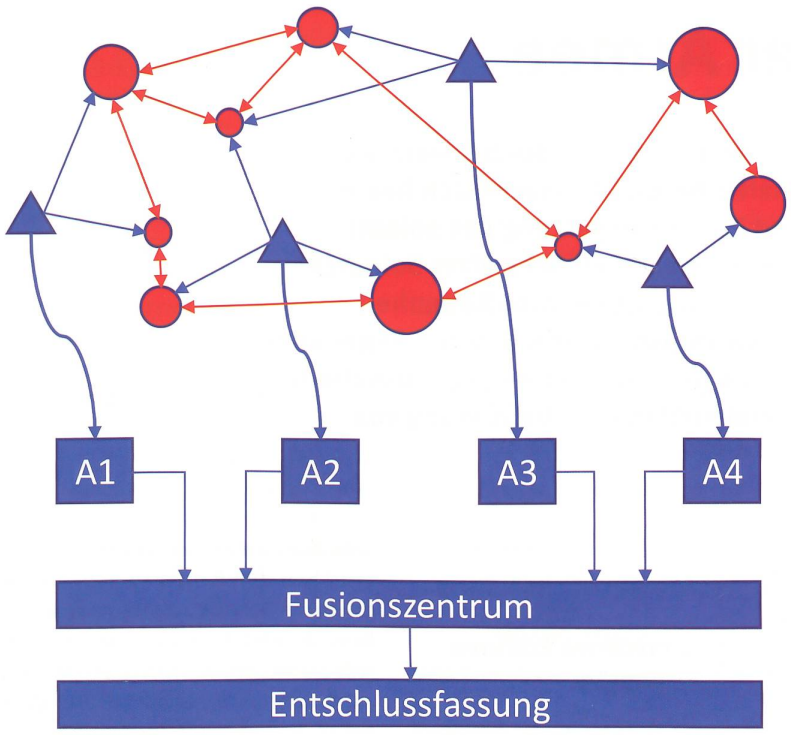
Fusionszentren (fusion centers) sind physische und/oder virtuelle Räume, in denen eine Zusammenarbeit zwischen verschiedenen Akteuren des öffentlichen und privaten Sektors zu einer Kombination von Cyber-Fachwissen aus vielen Quellen führt. Fusionszentren versuchen, Informationen aus verschiedenen Quellen aufzubereiten und themengerecht zu bündeln. Sowohl staatliche Strafverfolgungsbehörden (auf nationaler und regionaler Ebene) als auch Akteure des privaten Sektors teilen wechselseitig – idealerweise in Echtzeit – ihre Informationen, um präzisere und robustere Analysen zu generieren. Die so gewonnenen Erkenntnisse ermöglichen es, Cyber-Angriffe schneller zu erkennen und zu bekämpfen. Aktuelle Beispiele sind das *Kudelski Cyber Fusion Center* (https://www.kudelskisecurity.com/services/managed-security) sowie die Fusionszentren der *National Fusion Center Association* in den USA (https://nfcausa.org/). Im Verteidigungsbereich betreibt die NATO seit 2007 das *Intelligence Fusion Center*, wenngleich bei der Gründung noch nicht die Cyber-Sicherheit, sondern der internationale Terrorismus im Fokus der Analyse stand.

Abbildung 1



Grafiken: Autoren

Abbildung 2



Das US-amerikanische Beispiel: ein öffentlich-privates Quellennetzwerk

In den USA wird dieser Vernetzungsprozess seit 2003 durch das *Department of Homeland Security* vorangetrieben. Auslöser dieser Entwicklung war die Erkenntnis, dass die verschiedenen US-amerikanischen Sicherheitsbehörden im Jahr 2001 zusammengenommen über ausreichende Informationen verfügten, um die Terroranschläge des 11. September 2001 zu verhindern, ihre isolierten Informationen aber nicht zu einem komplexen Lagebild kombinieren konnten. Die heutigen Fusionszentren verknüpfen daher Information von Geheimdiensten (NSA, CIA, FBI), Bundesbehörden (DEA, TSA, Nationalgarde) und privaten Akteuren (Google, Apple, Facebook, Amazon, Microsoft). Die Zusammenarbeit ist föderal organisiert; jeder US-Bundesstaat betreibt ein eigenes Fusionszentrum. Zusammengenommen bilden diese ein nationales Netzwerk von Nachrichtenquellen. Bereits im Jahr 2014 hatten 63 von 78 Fusionszentren eine *cyber mission,* das heisst den Auftrag, ein Lagebild über Cyber-Angriffe und deren Abwehrmöglichkeiten zu erstellen.

«Die Schweiz verfügt über eine Vielzahl nachrichtendienstlicher Akteure und wettbewerbsfähiger IT-Unternehmen, sodass die Gründung von Fusionszentren attraktiv erscheint.»

Möglichkeiten für Schweizer Fusionszentren

Ein aktuelle Studie beleuchtet die Austauschbeziehungen zwischen verschiedenen Akteuren der schweizerischen Sicherheitspolitik.* Zwar ist eine gewisse Vernetzung zu erkennen, allerdings besteht immer noch eine erhebliche Fragmentierung. Die Schweiz verfügt über eine Vielzahl nachrichtendienstlicher Akteure und wettbewerbsfähiger IT-Unternehmen, sodass die Gründung von Fusionszentren attraktiv erscheint. Der föderalistische Staatsaufbau erweist sich hier als vorteilhaft, weil die einzelnen Fusionszentren analog zum US-amerikanischen Beispiel auf der kantonalen Ebene gegründet werden könnten.

Die Probleme der Umsetzung stellen sich vielmehr aus politökonomischer und rechtsstaatlicher Sicht. Einerseits hat nicht jeder Akteur, der Information besitzt, auch ein Interesse daran, diese zu teilen. Im Gegenteil besitzt Information gerade im nachrichtendienstlichen Bereich den Charakter einer Handelsware. Daher müssen nicht nur Organisationen, sondern auch zielführende Interaktionsregeln geschaffen werden, die den Akteuren einen Anreiz zum freiwilligen Austausch von Informationen geben. Andererseits untersteht zwar die individuelle Nachrichtengewinnung den Schranken des Rechtsstaats und gegebenenfalls einer parlamentarischen Aufsicht, nicht jedoch deren Verknüpfung. Wer in der Lage ist, viele Informationen dezentraler Akteure zu komplexen Lagebildern zu verknüpfen, wird selbst ein mächtiger Akteur. Dies gilt insbesondere dann, wenn das Fusionszentrum von privaten Firmen betrieben werden sollte, die auch kommerzielle Interessen verfolgen. Es reicht in einem entwickelten Rechtsstaat freiheitlicher Prägung daher nicht aus, nach digitaler Souveränität zu rufen, wenn der Weg dorthin in die totalitäre Überwachung führt. Die Cyber-Verteidigung der Zukunft wird daher einer politischen und fachlichen Aufsicht bedürfen, wie sie heute bereits bei den staatlichen Nachrichtendiensten besteht. ■

* Hagmann, J., Davidshofer, S., Tawfik, A., Wenger, A., Wildi, L. 2018. The Programmatic and Institutional (Re-)Configuration of the Swiss National Security Field. Swiss Political Science Review. doi:10.1111/spsr.12304


Marcus M. Keupp
PD Dr. oec. HSG
Dozent Militärökonomie
MILAK
8903 Birmensdorf ZH


Hptm
Dimitri Percia David
Msc
Wissenschaftlicher
Mitarbeiter der MILAK
8903 Birmensdorf ZH


Hptm
Alain Mermoud
Msc
Wissenschaftlicher
Mitarbeiter der MILAK
8903 Birmensdorf ZH