# Neue Rüstungspolitik in der Umsetzung, Armee und Cyberwar

Autor(en): **Markwalder, Alfred**

Objekttyp: **Article**

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

Band (Jahr): **176 (2010)**

Heft 12

PDF erstellt am: **20.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-131262

# Neue Rüstungspolitik in der Umsetzung, Armee und Cyberwar

**Die traditionelle Industrietagung von armasuisse stand einerseits im Zeichen der Neuausrichtung der Rüstungspolitik, andererseits wurden aber auch Aspekte von deren Auswirkung auf Rüstungsprogramme sowie das Thema «Cyberwar» aufgegriffen, dies in Zusammenarbeit mit der Schweizerischen Gesellschaft Technik und Armee (STA).**

**Alfred Markwalder,**
**Stellvertretender Chefredaktor ASMZ**

Vor einem zahlreich erschienenen Publikum erläuterte Rüstungschef Jakob Baumann die in die Wege geleitete Umsetzung der neuen Rüstungspolitik des Bundesrates, welche auf vier Säulen basiert. Das Schwergewicht seiner Ausführungen legte er auf die Sicherheitsrelevante Technologie- und Industriebasis (STIB), welche zurzeit analysiert wird. Mit der Beschaffungsstrategie wird ausgeleuchtet, welche Beschaffungen in der Schweiz erfolgen können und sollen, während die Industriebeteiligungsstrategie festlegt, wie Beteiligungsgeschäfte (direkte und indirekte Offsetgeschäfte) abgewickelt werden. Die Kooperationsstrategie legt dar, wie und wo eine Zusammenarbeit angestrebt werden soll. Die Eignerstrategie für die RUAG schliesslich muss unter anderem ausleuchten, welche Fähigkeiten in der Schweiz erhalten und aufgebaut werden sollen.

Gegen 400 Firmen in der Schweiz wurden in eine Umfrage einbezogen, um die heute bestehende Sicherheitsrelevante Technologie- und Industriebasis auszuleuchten. Resultate und Konklusionen sollen Ende 2011 vorliegen.

Baumann erwähnte speziell das seit 1. Januar 2010 aktive Offsetbüro, welches bei armasuisse in Bern angesiedelt ist (Offsetbüro Schweiz, c/o armasuisse, 3003 Bern). In enger Zusammenarbeit mit Swissmem und GRPM unterstützt das Büro interessierte Firmen bei der Vorbereitung und Durchführung von Offsettätigkeiten im Zusammenhang mit Rüstungsgeschäften.

Brigadier Hans-Peter Walser, Chef Armeeplanung, erläuterte die Auswirkungen des Sicherheitspolitischen Berichts sowie des Armeeberichts auf die künftigen Rüstungsbeschaffungen. Bevor hier Klarheit besteht, können laut Walser nur

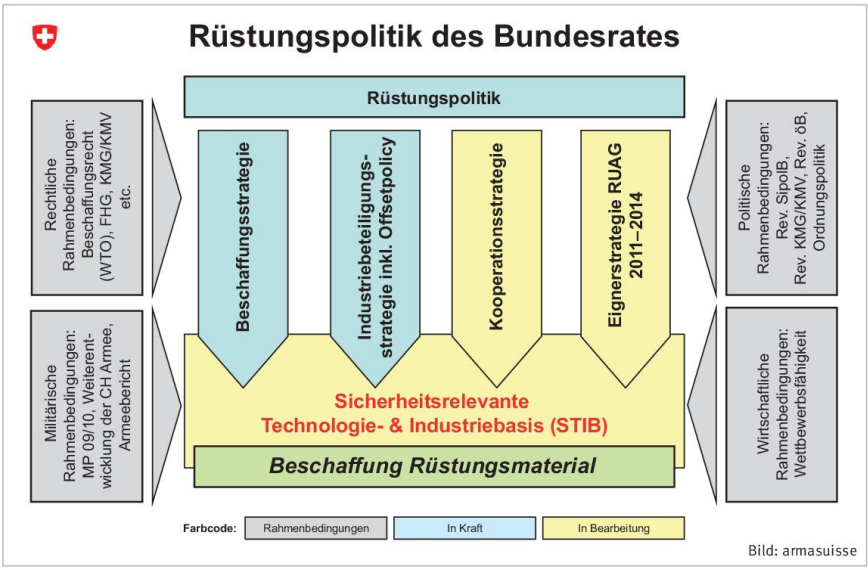

Bild: armasuisse

sehr vage Aussagen über Beschaffungen gemacht werden, dies umso mehr als betreffend der Beschaffung von Kampfflugzeugen noch sehr viele Fragen offen sind.

## Cyberwar

Armasuisse und STA setzten sich an dieser Tagung zum Ziel, die Gefahren von Cyberwar aufzuzeigen, auch wenn dieses Thema sowohl im Sicherheitspolitischen Bericht als auch im Armeebericht kaum erwähnt wird und dadurch auf dieser Ebene keine tiefer greifenden Analysen vorhanden, geschweige denn umfassende Antworten zur Bekämpfung sichtbar. Verschiedene Referenten wiesen auf die heimtückischen Aspekte der Bedrohung durch Cyberwar für die Wirtschaft, den Bürger, aber auch für den Staat und damit für die Armee hin. Heute hat jedermann mit technologischem Know-how die Möglichkeit, an diesem Krieg im Internet als Aggressor teilzunehmen. Finanzielle Hürden sind kaum vorhanden und durchsetzbare rechtliche Hürden existieren ebenfalls kaum. Es besteht ein Untergrundmarkt für das Aufspüren von Sicherheitslücken und nachfolgend wird gezielt Software eingesetzt, um in verschiedensten Bereichen Schaden zu stiften. In – schlechter – Erinnerung ist die Hacker-Attacke auf das Eidgenössische Departement für Auswärtige Angelegenheiten (EDA) im Herbst 2009 oder der Einsatz des Computer-Virus Stuxnet auf atomare Anlagen im Iran. Bei solchen Aktivitäten geht es nicht nur um Spionage, sondern um Manipulationen an Hardware und damit unter anderem an Steuerungen von Industrieanlagen.

Die Gefahren von Cyberwar mit täglichen Attacken sind vielerorts erkannt. Mit Information Operations (Info Ops) werden diese analysiert und Gegenmassnahmen aufgebaut. Quintessenz der Ausführungen verschiedener Referenten war die Aussage: «We need a secure system, not a system with security»! ■