

Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift
Herausgeber: Schweizerische Offiziersgesellschaft
Band: 176 (2010)
Heft: 12

Artikel: Neue Rüstungspolitik in der Umsetzung, Armee und Cyberwar
Autor: Markwalder, Alfred
DOI: <https://doi.org/10.5169/seals-131262>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 04.05.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

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

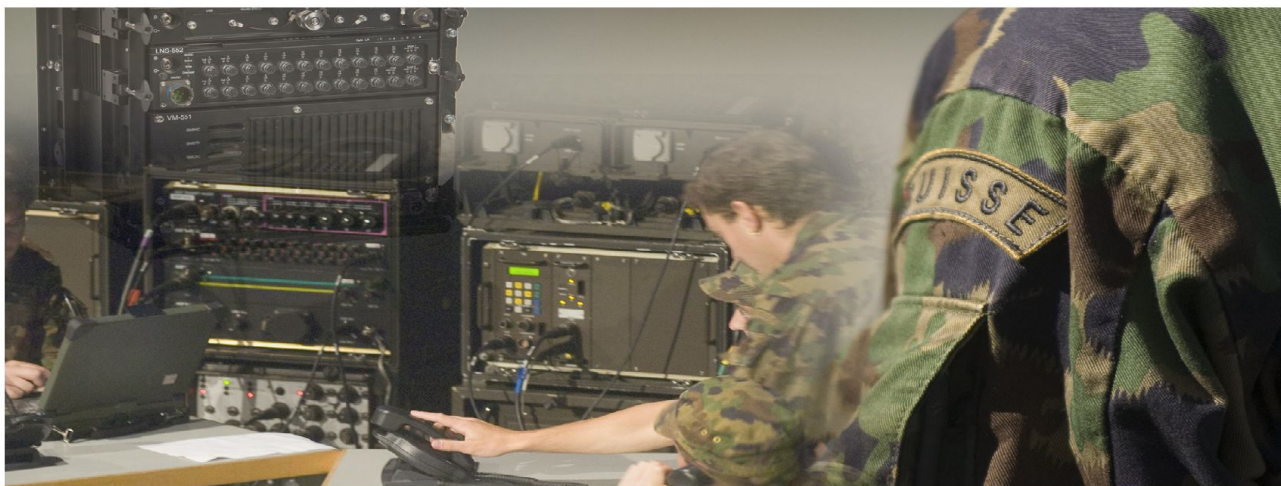
Vor einem zahlreich erschienenen Publikum erläuterte Rüstungschef Jakob Baumann die in die Wege geleitete Umsetzung der neuen Rüstungspolitik des Bundesrates, welche auf vier Säulen basiert. Das Schwergewicht seiner Ausführungen legte er auf die Sicherheitsrelevante Technologie- und Industriebasis (STIB), welche zurzeit analysiert wird. Mit der Beschaffungsstrategie wird ausgeleuchtet, welche Beschaffungen in der Schweiz erfolgen können und sollen, während die Indus-

triebbeteiligungsstrategie 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 auszu-leuchten. 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 Swissemem und GRPM unterstützt das Büro interessierte Firmen bei der Vorbereitung und Durchführung von Offsettätigkeiten im Zusammenhang mit Rüstungsgeschäften.

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

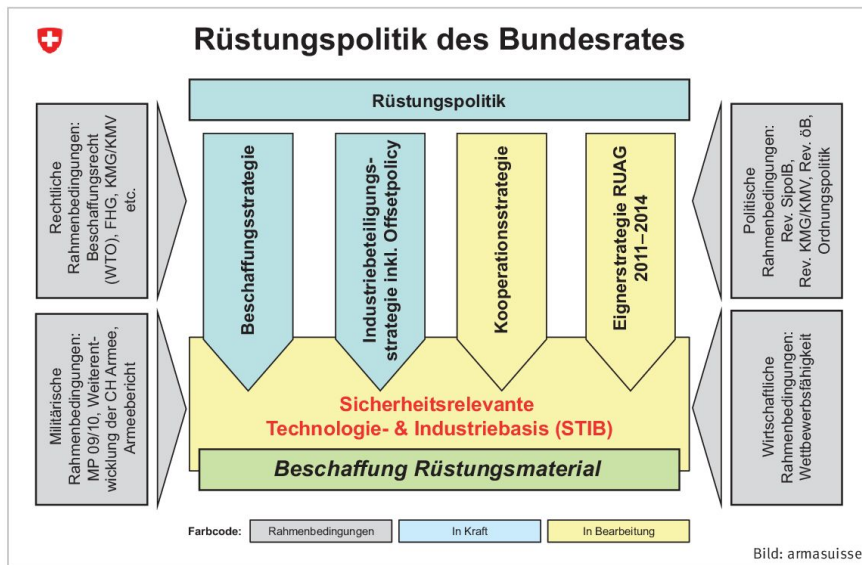


TAKTISCHE KOMMUNIKATIONS-LÖSUNGEN VON ASCOM ERMÖGLICHEN DIE VERNETZTE OPERATIONS-FÜHRUNG

Anspruchsvolle Kunden wie die Schweizer Armee vertrauen bei der professionellen Ausübung ihrer Aufgaben auf sichere Kommunikationstechnologien und -systeme von Ascom.

Ascom (Schweiz) AG
Belpstrasse 37 | 3000 Bern 14
T +41 31 999 11 11 | F +41 31 999 16 82
www.ascom.com/defense | securitycommunication@ascom.com

ascom



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»! ■



Ihr Ziel. Unser Engagement.

Management und Technologieberatung.

3'250 Mitarbeiter engagieren sich täglich für Unternehmen und Organisationen.

In der Schweiz und weltweit.

www.bearingpoint.ch

© 2010 BearingPoint Switzerland AG. All rights reserved.