

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

**Herausgeber:** Schweizerische Offiziersgesellschaft

**Band:** 177 (2011)

**Heft:** 4

## **Werbung**

### **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:** 02.04.2025

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

sem technischem und logistischem Aufwand zurück.

Die organisierte Kriminalität ist jedoch bei weitem nicht die einzige Bedrohung im Cyberspace. Für die Nachrichtendienste ist dieser schon seit langem eine wichtige Informationsquelle für die passive

**«Diese Angriffe werden immer gezielter und technisch raffinierter.»**

Ermittlung im Kampf gegen Terrorismus und andere Bedrohungen gegen den Staat. Einige Nachrichtendienste nutzen aber auch die Möglichkeiten des Netzes, um sich aktiv unerlaubten Zugang zu Informationen zu verschaffen. Auch das ist keinesfalls ein neues Phänomen. Bereits Mitte der 80er-Jahre wurde ein spektakulärer Fall aufgedeckt, bei dem deutsche Hacker gegen Bezahlung für den KGB massenhaft in amerikanische Rechner eingedrungen waren, um sensible Daten zu entwenden. Seither wurden immer wie-

der Angriffe entdeckt, welche mehr oder weniger eindeutig als Tat staatlicher Akteure identifiziert werden konnten. Auch die Schweiz wurde schon Opfer solcher Angriffe. Diese Attacken werden in den Medien oft als Zeichen für den Cyberwar gewertet; allerdings handelt es sich dabei wohl eher um unerlaubten Nachrichtendienst denn um einen bewaffneten Angriff, was völkerrechtlich eindeutig unter der Kriegsschwelle liegt.

**Kosovo, Estland, Georgien, Iran**

Die Frage, was ein bewaffneter Angriff im Sinne des Völkerrechts und damit eine kriegerische Handlung im Cyberspace ist, ist nicht abschliessend beantwortet. In der jungen Geschichte des Cyberspace wurden schon verschiedenste Ereignisse als erster Cyberwar betitelt. Als populärstes Beispiel gelten sicherlich die Attacken gegen Estland im Sommer 2007. Bereits 1999 war aber im Zusammenhang mit den NATO-Angriffen im Kosovo auch schon vom ersten Cyberwar gesprochen worden. Der damalige NATO-Kommandant General Wesley Clark war allerdings der Meinung, dass man in diesem Bereich

noch mehr hätte tun können. Wegen der rechtlich unsicheren Situation und den schwer abzuschätzenden Folgen solcher Angriffe wurde jedoch davon abgesehen. So waren es am Ende primär die Amerikaner, die im Internet unter Angriffen zu leiden hatten. Nach dem versehentlichen Beschuss der chinesischen Botschaft wurden amerikanische Webseiten – unter anderem die des Weissen Hauses – von chinesischen Hackern angegriffen. Der angerichtete Schaden war zwar deutlich geringer als derjenige in Estland 2007, die Ereignisse sind aber durchaus vergleichbar. In beiden Fällen ist davon auszugehen, dass die jeweiligen Regierungen von China bzw. Russland wohl nicht direkt an den Angriffen beteiligt waren, diese aber zumindest geduldet haben.

Im Konflikt um Ostossetien, zwischen Russland und Georgien, kam es begleitend zum Einmarsch der russischen Truppen zu Attacken im Cyberspace. Das Timing der Angriffe deutet darauf hin, dass die Angriffe vom Kreml zumindest indirekt koordiniert wurden, auch wenn dies offiziell dementiert wird.

Bei all den genannten Angriffen normalisierte sich die Lage relativ schnell

# Wanderkarten 1:50 000

Weg weisend, mit offiziellem Wanderwegnetz



- Offizielle Karte der Schweizer Wanderwege
- Öffentliche Verkehrsmittel (Bus, Bahn, Schiff) mit Haltestellen
- Hütten und abgelegene Gasthöfe
- Detailliert und genau
- Für Wanderer und Spaziergänger



Neu aktualisierte Ausgaben 2011





Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Bundesamt für Landestopografie swisstopo**  
www.swisstopo.ch



Schweizer Wanderwege  
Suisse, Bando  
Svizzera Svizzera  
Svizzera Svizzera



## Kanton Zug

Für die einjährige Grundausbildung sucht die Zuger Polizei

### Polizeianwärter/innen

Sie besitzen das Schweizer Bürgerrecht sowie einen einwandfreien Leumund. Sie sind eine natürliche und ausgeglichene Persönlichkeit bis ca. 35-jährig und verfügen über eine gute Schulbildung sowie eine erfolgreich abgeschlossene Berufslehre, Matura oder gleichwertige Ausbildung. Die Grundausbildung findet an der Interkantonalen Polizeischule Hitzkirch statt. Sie wird mit dem eidgenössisch anerkannten Fachausweis als Polizistin oder Polizist abgeschlossen.

**Informationsabend:** 23. März 2011, 19.00 Uhr, Zuger Polizei, An der Aa 4, 6301 Zug.

Weitere Informationen finden Sie unter [www.zug.ch/stellen](http://www.zug.ch/stellen).

## EIN BERUF IN DER ARMEE

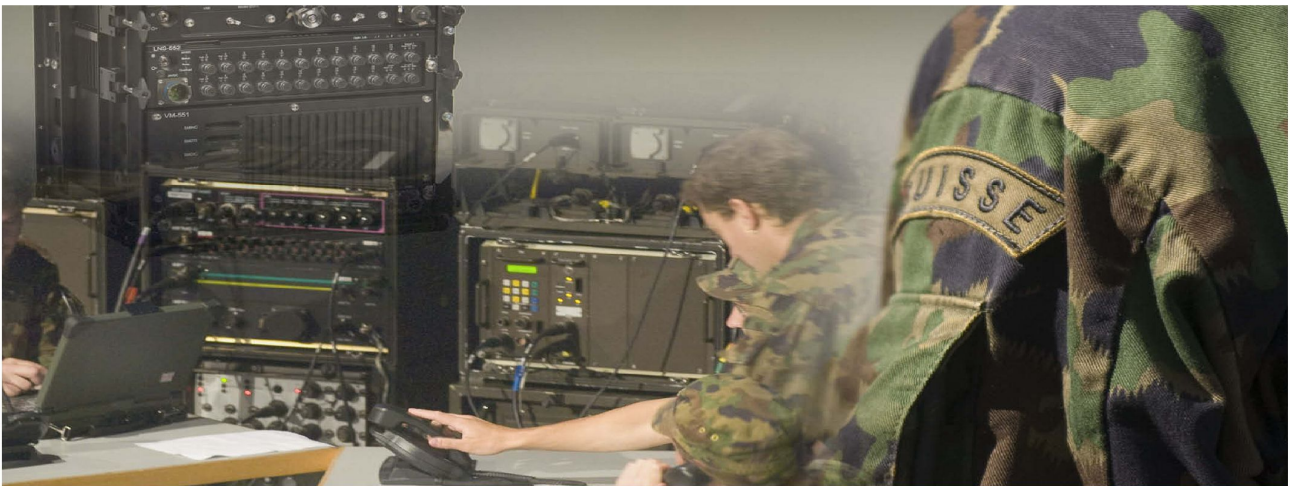


Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Schweizer Armee



**Vielseitig und interessant** [www.armee.ch/berufsmilitaer](http://www.armee.ch/berufsmilitaer)



### 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](http://www.ascom.com/defense) | [securitycommunication@ascom.com](mailto:securitycommunication@ascom.com)

**ascom**