

**Zeitschrift:** Armee-Logistik : unabhängige Fachzeitschrift für Logistiker = Organo indipendente per logistica = Organ independenta per logistichers = Organ indépendant pour les logisticiens

**Herausgeber:** Schweizerischer Fourierverband

**Band:** 92 (2019)

**Heft:** 7-8

**Rubrik:** Herausgegriffen

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. 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. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **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. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **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. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 02.04.2026

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

## ARMEE-LOGISTIK

92. Jahrgang. Erscheint 10-mal jährlich (monatlich, Doppelnummern 7/8 und 11/12).  
ISSN 1423-7008.  
Beglaubigte Auflage 3540 (WEMF 2016).

### Offizielles Organ:

Schweizerischer Fourierverband (SFV) /  
Verband Schweizerischer Militärköchchenchefs (VSMK) /  
Schweizerischer Feldweibelverband (SFWW)

**Jährlicher Abonnementpreis:** Für Sektionsmitglieder im Mitgliederbeitrag inbegriffen. Für nicht dem Verband angeschlossene Angehörige der Armee und übrige Abonnenten Fr. 32.–, Einzelnummer Fr. 3.80.  
Postkonto 80-18 908-2

**Verlag/Herausgeber:** Schweizerischer Fourierverband, Zeitungskommission, Präsident Four Stefan Walder (sw), Aufdorfstrasse 193, 8708 Männedorf, Telefon Privat: 079 346 76 70, Telefon Geschäft: 044 752 35 35, Fax: 044 752 35 49, E-Mail: swalder@bluewin.ch

**Redaktion:** Armee-Logistik, Sdt Florian Rudin (fr), Notariat Riesbach-Zürich, Postfach, 8034 Zürich, Telefon Privat: 078 933 04 69, Telefon Geschäft: 044 752 35 35, Fax: 044 752 35 49, E-Mail: redaktion@armee-logistik.ch

### Chefredaktor:

Oberst Roland Haudenschild (rh)

**Sektionsnachrichtenredaktor:** Sdt Florian Rudin (fr)

**Mitarbeiter:** Hartmut Schauer (Deutschland/Amerika).

Oberst Heinrich Wirz (Bundeshaus/Mitglied EMPA);

Member of the European Military Press Association (EMPA).

**Freier Mitarbeiter:** Oberst i Gst Alois Schwarzenberger (as), E-Mail: schwarzenberger.alois@bluewin.ch,

Telefon 078 746 75 75

### Redaktionsschluss:

Nr. 09 – 05.08.2019, Nr. 10 – 05.09.2019,

Nr. 11/12 – 15.10.2019, Nr. 1 – 05.12.2019

Grundsätzlich immer am 5. des Monats für die

Ausgabe des kommenden Monats.

### Adress- und Gradänderungen:

#### SFV und freie Abonnenten:

Zentrale Mutationsstelle SFV, Postfach,

5036 Oberentfelden, Telefon 062 723 80 53,

E-Mail: mut@fourier.ch

**VSMK-Mitglieder:** Verband Schweizerischer Militärköchchenchefs, Zentrale Mutationsstelle VSMK,

8524 Uesslingen, mutationen.vsmk@bluewin.ch

**Insertate:** Anzeigenverwaltung Armee-Logistik,

Sdt Florian Rudin, Notariat Riesbach-Zürich, Postfach,

8034 Zürich, Telefon Geschäft: 044 752 35 35

(Hr. Walder), Fax: 044 752 35 49,

E-Mail: swalder@bluewin.ch

Insertatenschluss: am 1. des Vormonats

**Druck:** Triner Media + Print, Schmiedgasse 7, 6431

Schwyz, Telefon 041 819 08 10, Fax 041 819 08 53

**Satz:** Triner Media + Print

**Vertrieb/Beilagen:** Schär Druckverarbeitung AG,

Industriestrasse 14, 4806 Wikon,

Telefon 062 785 10 30, Fax 062 785 10 33

Der Nachdruck sämtlicher Artikel und Illustrationen – auch teilweise – ist nur mit Quellenangabe gestattet. Für den Verlust nicht einverlangter Beiträge kann die Redaktion keine Verantwortung übernehmen.

Die irgendwie geartete Verwertung von in diesem Titel abgedruckten Anzeigen oder Teilen davon, insbesondere durch Einspeisung in einen Online-Dienst, durch dazu nicht autorisierte Dritte ist untersagt. Jeder Verstoß wird gerichtlich verfolgt.

## Cyberabwehr der Armee

**Ein Team aus der Führungsunterstützungsbasis (FUB) übte im April 2019 auf dem digitalen Gefechtsfeld den Ernstfall. Bei der internationalen Übung «Locked Shields» half die Schweizer Armee mit, die Netzwerke und Systeme des fiktiven Staates Berylia gegen Angriffe aus dem Cyberraum zu verteidigen.**

Kein Strom im ganzen Land, zu viel Chlor im Wasser und darum kranke Menschen, gehackte Webseiten der Regierung, keine Netzwerkverbindung im Hafen und verdächtige Aktivitäten im militärischen Netz: Die Mitglieder aus dem Verteidigungsteam der Schweiz hatten während der zweitägigen Übung an vielen Fronten zu helfen. Die Motivation schien unerschöpflich. Seite an Seite mit Verstärkung aus der Miliz sassen die Profis der FUB mehrere Tage hinter den Bildschirmen. Und auch wenn es bloss eine Übung war, der Einsatz dauerte für manche bis tief in die Nacht. «Die Leute sind sehr ehrgeizig. Sie möchten ihre Systeme möglichst gut verteidigen», erklärte Cederic Gaudard den grossen Einsatz. Er leitete das Schweizer Verteidigungsteam auf technischer Stufe und hatte so den Überblick über die Kräfte der FUB.

Im Raum nebenan sass das strategische Team. Dort waren Leute des GS-VBS, des EDA und der FUB. Die rechtliche Komponente ist für die neutrale Schweiz auch bei einer Übung von grosser Bedeutung. «Die Schweiz unterstützt Berylia innerhalb der rechtlich legitimen Grundlagen», war denn auch die Hauptaussage bei fast allen Anfragen aus der Übungsleitung. Diese befand sich in Tallinn, der Hauptstadt von Estland, und wurde gestellt vom Cooperative Cyber Defence Centre of Excellence der NATO.

«Locked Shields» ist die grösste und komplexeste internationale Live-Fire-Cyber-Abwehrübung der Welt. In diesem Jahr haben wieder 23 Nationen daran teilgenommen. Gewonnen hat das Schweizer Team vor allem viele Erkenntnisse: «Jetzt wissen wir genauer, wo wir uns verbessern müssen. Für die nächste Übung und auch für den Ernstfall», so bringt es Ueli Amsler auf den Punkt. Er war der Übungsleiter der Schweiz und arbeitet bei der FUB im Bereich Cyber Defence.

Cyberangriffe geschehen täglich. Für Staaten, Unternehmen und Individuen stellt sich nicht länger die Frage, ob sie tatsächlich im Cyberraum angegriffen werden, sondern nur noch, wie professionell und mit welcher Intensität. Ein bewährtes Prinzip für einen effizienten Schutz vor Cyberangriffen ist der Austausch über Informationen zu den Angreifern, über welchen Alain Mermoud, wissenschaftlicher Mitarbeiter an der MILAK an der ETH, in seiner Dissertation geforscht hat.

Murmeltierprinzip. Das erste Murmeltier, das einen Feind erspäh, warnt durch das unverkennbare Pfeifen seine Artgenossen, damit diese sich vor der Gefahr in Sicherheit bringen können. Dasselbe Prinzip ist in der Cyberabwehr anwendbar, in dem ein Netzwerkmitglied auf einer Plattform für Informationsaustausch möglichst rasch und transparent Informationen über den Angreifer und die Art des Angriffs verbreitet. So können die übrigen Mitglieder entsprechende Massnahmen treffen.

Diese Vorgehensweise führt bei den Betreibern kritischer Infrastrukturen zu einem Dilemma. Zum einen wollen die Betreiber die kostenintensiv gewonnenen Informationen nicht mit anderen teilen. Zudem können sie die Vertrauenswürdigkeit der anderen Partei nicht immer einschätzen. Zum anderen verbessert sich jedoch durch die Informationsteilung die technische Widerstandsfähigkeit des gesamten Cyberraums, und die Kosten der Informationsbeschaffung können auf alle aufgeteilt und damit signifikant reduziert werden.

Alain Mermoud hat für seine Dissertation eine Umfrage bei den Benutzern der Melde- und Analysestelle Informationssicherung der Bundesverwaltung (MELANI) durchgeführt. Im Zentrum stand die Frage, welche Faktoren gegeben sein müssen, damit die Benutzer bei einem Informationsaustausch mitwirken würden. Nach der empirischen Analyse haben sich fünf Faktoren herauskristallisiert, die eine Zusammenarbeit beeinflussen: die Gegenseitigkeit des Austausches, der Informationsgehalt, vorhandene institutionelle Hindernisse, die Reputation der Plattform sowie das Vertrauen in die anderen Partner.

Zusammengefasst tauschen Institutionen dann ihre Informationen zu Cyberangriffen freiwillig aus, wenn die Plattform gut geschützt und vertrauenswürdig ist, klare Regeln hat und sie sich davon einen Nutzen versprechen.

Quelle: [www.vtg.admin.ch](http://www.vtg.admin.ch)

(rh)

