

**Zeitschrift:** ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift  
**Herausgeber:** Schweizerische Offiziersgesellschaft  
**Band:** 175 (2009)  
**Heft:** 01-02

**Artikel:** Vernetzte Operationsführung braucht durchgängige Informationssicherheit  
**Autor:** Meier, Rudolf / Huber, Beatrice  
**DOI:** <https://doi.org/10.5169/seals-238>

### **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:** 12.01.2026

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

# Vernetzte Operationsführung braucht durchgängige Informationssicherheit

**Kaum eine Armee betreibt noch ausschliesslich eigene Netze, sondern nutzt (auch) offene, globale Transportnetze. Diese sind anfällig für Attacken unterschiedlicher Art – denn elektronische Kriegsführung ist heute Dauerzustand. Um sensible Informationen zu schützen, welche einen geschützten Bereich verlassen, ist es de facto zwingend, durchgängig «harte Chiffrierung» anzuwenden. Mit dem Zusatzvorteil, dass sie auch bei Kombination unterschiedlicher Netztechnologien ein identisches Sicherheitsniveau garantieren kann.**

Rudolf Meier und Beatrice Huber

In früheren Zeiten bedingten die technischen Möglichkeiten, dass pro Anwendung (Telefon, Funk, ...) ein getrenntes Netz genutzt wurde. Dies ist heute nicht mehr nötig: Die Vernetzte Operationsführung in einer modernen Verteidigungsorganisation muss sich auf eine durchgängige ICT-Infrastruktur<sup>1</sup> abstützen können, in welche auch mobile Teilnehmer eingebunden werden. Dabei geistert das geflügelte Wort «everything over IP»<sup>2</sup> herum: E-Mail, Telefonieren mit IP (Voice over IP, VoIP), Video-Konferenzen, Da-

tenzugriff usw. «IP» ist jedoch nur ein Teil der Vernetzungstechnologie, mit besonderer Bedeutung auf der Anwender-nahen Ebene: Hier werden die so genannten Triple-play-Anwendungen (Daten, Sprache, Video) in IP-Pakete verpackt und zusammengeführt.

Auf der Transportebene – also dort, wo alles dann physisch durchs Netz transportiert wird – kommen weitere Technologien zum Einsatz. Konzentriert man sich dabei auf einige wenige, weltweit etablierte Technologien (zu nennen sind hier vor allem Gigabit-Ethernet und Synchron Digital Hierarchy, SDH), erleichtert dies die globale Vernetzung und fördert sie. Ein grosses Netz hat jedoch den Nachteil, dass darin eine grosse Anzahl aktiver Elemente (und es werden immer mehr) vorhanden sind, die nicht gegen elektronische Attacken geschützt werden können

und ausserdem Netzzugänge bestehen, die kaum kontrollierbar sind.

Besonders heikel für Organisationen sind so genannte Storage-Netzwerke, d.h. Netzwerke, in denen – teils auch sehr sensible – Daten zentral archiviert werden, auf die viele Benutzer Zugriff haben. Für diese Storage-Netzwerke schien es bisher – bedingt durch Security-Policies – sinnvoll zu sein, physisch separierte Netze mit eigenem Netzwerkmanagement zu verwenden (meistens Fibre Channel). Die aktuelle technische Entwicklung besonders des Ethernet-Protokolls (10-Gigabit-Leistungsstufe) eröffnet hier jedoch effiziente, kostengünstige und sichere Lösungen als Bestandteile der allgemeinen ICT-Infrastruktur.

**Szenerie in einer Verteidigungsorganisation: die Vernetzte Operationsführung in einer modernen Verteidigungsorganisation muss sich auf eine durchgängige ICT-Infrastruktur abstützen können.** Quelle: VBS



## Attacken auf globale Netze

Mit der globalen Vernetzung verändern sich auch die Risiken für sensible Informationen. Ein Angriff auf die ICT-Infrastruktur (über irgendeine Schwachstelle) kann verschiedene Ziele gleichzeitig haben: Eindringen in Datenbanken, Abfangen von Nachrichten, Denial-of-Service-Attacken<sup>3</sup> und vieles mehr. Im schlimmsten Fall stört oder blockiert ein Angreifer auf elektronischem Weg die Vernetzte Operationsführung als Ganzes massiv. Offensichtlich ist damit das Schadenspotenzial viel grösser als bei einem Angriff beispielsweise im Telefonnetz.

Diese neuen Risiken werden häufig unter «elektronischer Kriegsführung» zusammengefasst, was vorgaukelt, dass solche Massnahmen zu «kriegerischen Aktivitäten» gehören. Dies ist jedoch definitiv nicht der Fall: Sie kommen laufend vor (sei es mit geplanter Wirkung oder als





Modernes Verschlüsselungsgerät  
von Crypto AG: Das Ethernet Encryption  
HC-8555 10G verschlüsselt 10 Gigabit  
pro Sekunde. Quelle: Crypto AG

«Testläufe») und sind in den wenigsten  
Fällen erkennbar.

### Chiffrierung schützt sensible Information

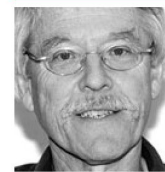
Für eine Organisation – sei sie nun  
militärisch oder zivil – ist es wichtig, die  
Risiken für die sensiblen Informationen  
äusserst konsequent aus der Welt zu schaf-  
fen. Eine effiziente Möglichkeit dazu ist  
die «harte Chiffrierung» aller Informa-  
tionen, welche einen geschützten Bereich  
verlassen, kombiniert mit weiteren Mass-  
nahmen im Rahmen der Security-Policy.

«Harte Chiffrierung» bedeutet in diesem  
Fall, dass die Chiffrierung ausschliesslich  
in separater, manipuliertsicherer Hard-  
ware erfolgt, die je nach Szenario alle ge-  
wünschten militärischen Standards er-  
füllt. In der Regel gehört dazu im mili-  
tärischen Umfeld auch die Verwendung  
geheimer, proprietärer Algorithmen.

Diese Grundsätze sind im militärischen  
Umfeld kaum bestritten. Was jedoch si-  
cherheitsmässig für einzelne Verbindun-  
gen leicht zu schaffen ist, kann innerhalb  
eines durchgängigen Netzes echte Her-  
ausforderungen stellen – muss doch logi-  
scherweise auch die Informationssicher-  
heit durchgängig organisiert sein, damit  
keine ungeschützten Netzbereiche in Be-  
trieb genommen werden. Grossflächige  
Sicherheitslösungen sind deshalb in je-  
dem Fall nur als individuelle Projekte  
und mit grosser Technologiekompetenz  
realisierbar. Im Weiteren muss ein Sys-  
tem für Informationssicherheit die Hie-  
rarchien innerhalb einer militärischen  
Organisation unterscheiden und unter-  
stützen können. Entscheidend für den  
Erfolg ist dabei, dass das Security Ma-  
nagement, d.h. das Management des Sys-

tems, das gleiche Schutzniveau aufweisen  
muss wie die Infrastruktur und die Kom-  
munikation selber und weitgehend feh-  
lervorhersehend aufgebaut ist. ■

- 1 Die Abkürzung ICT steht für englisch «Infor-  
mation and Communication Technology».
- 2 Die Abkürzung IP steht für englisch «Internet  
Protocol».
- 3 Denial-of-Service-Attacken haben zum Ziel, einen  
bestimmten Dienst für deren Benutzer uner-  
reichbar zu machen oder zumindest die Erreich-  
barkeit des Dienstes erheblich einzuschränken.



Dr. Rudolf Meier  
Publizist mit den Schwer-  
punkten Politologie,  
Wirtschaft und Technologie  
8127 Forch



Beatrice Huber  
Corporate Editor  
bei Crypto AG  
6301 Zug

# NEW RescueTool

Für Rettungs- und Sicherheitsdienste



#### 0.8623.MN RescueTool

enthält folgende Teile  
und Funktionen:

1. Feststell-Einhandklinge
2. Phillips-Schraubendreher
3. Scheibenzertrümmer
4. starker Schraubendreher /  
Kistenöffner mit
5. – Kapselheber
6. – Drahtabsolierer
7. Stech-Bohrhale
8. Gurtenschneider
9. Ring, inox
10. Pinzette
11. Zahnstocher
12. Frontscheibensäge  
für Verbundglas
13. nachleuchtende Schalen
14. Nylon-Kordel
15. Nylon-Etui

#### 0.8623.N RescueTool

gleiches Messer mit normaler  
Klinge (statt Einhandklinge)



MAKERS OF THE ORIGINAL SWISS ARMY KNIFE