

Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische
Militärzeitschrift
Herausgeber: Schweizerische Offiziersgesellschaft
Band: 147 (1981)
Heft: 2

Buchbesprechung

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: 02.02.2025

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

der Klarinformation, das heisst der geheimen Nachricht, zu kommen. Die geheime Nachricht ist mindestens dem Sender und dem Empfänger bekannt, meistens aber auch einem weiteren Kreis von Personen. Je kleiner dieser Personenkreis, desto geringer die Gefahr, dass die Nachricht durch Verrat oder Erpressung in die Hände des Gegners gerät.

Im Verlauf von kriegerischen Handlungen besteht immer eine gewisse Möglichkeit, dass ein **Gerät mit eingestelltem Schlüssel** in die Hände des Gegners fällt. Tritt dieser Fall ein, muss der im Netz verwendete Schlüssel kurzfristig gewechselt werden können.

Analog zur geheimen Nachricht kann auch **der geheime Schlüssel durch Verrat oder Erpressung** in die Hände des Gegners gelangen. Die betrieblichen Schutzmassnahmen sind dabei gleich, das heisst die Kenntnis des Schlüssels soll auf einen möglichst kleinen Personenkreis beschränkt sein. Wäre der Schlüssel überhaupt niemandem bekannt, könnte er auch nicht verraten oder erpresst werden.

4 Schutz vor Verrat und Erpressung durch Autogenschlüssel

Die Sicherheitsanalyse von Chiffriersystemen zeigt, dass mit den heutigen mathematischen und technischen Mitteln die **Schwachstellen im technischen Bereich praktisch vollständig ausgeschaltet werden können**. Dadurch gewinnen die Schwachstellen im betrieblichen Bereich an Bedeutung; zu diesen gehört der Verlust des Schlüssels durch Verrat und Erpressung.

In den **Entwicklungslaboratorien der Firma BBC Brown, Boveri** wurde in der Form des Autogenschlüssels eine Lösung für dieses Problem gefunden. Diese Lösung ist in den Chiffriergeräten der neuesten Generation bereits verwirklicht.

Mit den heutigen technischen Mitteln ist die Möglichkeit gegeben, an den Endstellen einer Verbindung durch die Chiffriergeräte selbst identische neue Schlüssels (sogenannte Autogenschlüssel) erzeugen zu lassen. Voraussetzung dazu ist, dass die Geräte mit einem bereits eingegebenen Schlüssel

synchronisiert sind. Der **Autogenschlüssel** ist eine komplizierte Funktion des früher eingegebenen Schlüssels und zusätzlich vom Zeitpunkt der Erzeugung abhängig.

Der Schutz vor Verrat und Erpressung wird dadurch erreicht, dass nach Inbetriebnahme einer Verbindung mit einem neu ins Gerät eingegebenen Schlüssel raschmöglichst ein Autogenschlüssel erzeugt und in den Chiffriergenerator eingegeben wird. Der neu erzeugte Autogenschlüssel wird durch das Gerät nicht angezeigt und kann auch nicht durch Manipulationen zugänglich gemacht werden.

Der **Autogenschlüssel wird innerhalb einer Punkt-Punkt-Verbindung erzeugt**, ohne dass dabei die Verbindung gestört wird. In einem Netz ergibt sich daraus – aus einem für alle Verbindungen identischen ersten Schlüssel für jede Strecke – ein individueller Schlüssel. Somit kann auch die Verteilung einer grossen Anzahl verschiedener Schlüssel vermieden werden. ■

Bücher und Autoren:

Die deutsche Luftwaffe im Afrika-Feldzug 1941/1943

Von Werner Held und Ernst Obermaier. 237 Seiten, über 500 Fotos und Abbildungen, Motorbuch-Verlag, Stuttgart 1979, DM 39,-.

Aus der Sicht der deutschen Führung zuerst als «Nebenkriegsschauplatz» betrachtet, hat der Krieg in Nordafrika trotz Klima- und Versorgungsproblemen rasch Dimensionen angenommen, die eine immer umfangreichere deutsche Beteiligung erzwangen. Dem tapferen Einsatz der deutschen Flieger in diesem im Grunde hoffnungslosen Kampf gegen einen zunehmend überlegener werdenden alliierten Gegner ist der vorliegende Band aus der Reihe «Bildreport Weltkrieg II» gewidmet. Die grosse Zahl unveröffentlichter Fotos, meist aus Privatarchiven, und ein leichtfasslicher, prägnanter Text machen dieses Buch für alle interessant, die sich in irgendeiner Form mit diesem Abschnitt der Weltgeschichte befassen. FS

Die Seeschlacht von Coronel und Falkland

Von Geoffrey Bennett. Heyne Taschenbuch Verlag, München 1980.

Spannend und lehrreich zugleich sind die mit zahlreichen durch den deutschen Übersetzer fachkundig ergänzten Schilderungen über die für die Royal Navy wenig ruhmreiche Schlacht von Coronel. Dort – vor der chilenischen Küste – hatten die briti-

schen Schiffe («Good Hope», «Glasgow», usw.) gegen ein deutsches Geschwader («Scharnhorst», «Gneisenau», usw.) unter dem berühmten Admiral Graf Spee eine empfindliche Niederlage erlitten. Erstmals seit über 100 Jahren hatte ein deutsches Geschwader einen Sieg über die Royal Navy errungen. Im gleichen Jahre – im Dezember 1914 – revanchierte sich die britische Marine in der Schlacht von Falkland. Das kräftemässig unterlegene, deutsche Geschwader verlor bei diesem Gefecht auch den Chef des ursprünglich in ostasiatischen Gewässern operierenden Kreuzergeschwaders. Die Wiedergabe vieler Zitate aus Originaldokumenten verleiht dem Taschenbuch eine gewisse Lebendigkeit. Es lässt sich entsprechend leicht lesen. J. K.

Die Besatzer und die Deutschen: Amerikanische Zone 1945–1948

Von Klaus-Jörg Ruhl. 200 Seiten, 169 Abbildungen. Droste-Verlag, Düsseldorf 1980. DM 46,-.

Die deutsche Geschichte von 1945 bis 1948 – der Zeit, in der das Land zwischen Briten, Franzosen, Amerikanern und Russen in vier Besatzungszonen aufgeteilt war – dürfte denjenigen, die diese Jahre nicht selber miterlebt haben, eher unbekannt sein. Der vorliegende Text/Bild-Band über das Leben im amerikanisch besetzten Teil ist ein Beitrag, um diese Lücke zu schliessen. Zudem darf er wohl als Ergänzung der im gleichen Verlag erschienenen Text/Bild-Bände über die französische und die britische Zone verstanden werden.

In sechs Kapiteln schildert der Autor den Einmarsch der Amerikaner und ihre Versu-

che, die Deutschen zu entnazifizieren und zur Demokratie umzuerziehen. Er beschreibt aber auch die Existenzbedingungen in diesem in Trümmern liegenden Deutschland der ersten Nachkriegsjahre, die Not und Verzweiflung der Menschen, die sich wohl anfänglich über ihre Befreiung freuten, jedoch kurze Zeit später unter Hunger, Kälte und Wohnungsnot litten. Zahlreiche Abbildungen, Quellentexte von alliierter und deutscher Seite sowie Augenzeugen- und Erlebnisberichte ergänzen den Text. D. Heuberger

Militärgerichtsbarkeit in der DDR

Von Regina Rühmland. J.-Schweitzer-Verlag, BRD 1980.

Über die Militärgerichtsbarkeit in einem kommunistischen Staat gibt es auffallend wenig seriöse Literatur. Im Osten werden die mit diesem Fragenkomplex zusammenfallenden Probleme unter Ausschluss der Öffentlichkeit behandelt. Nicht einmal vollgestreckte Todesurteile an Soldaten, die in den Volksarmeen auch in Friedenszeiten keine Seltenheit sind, werden publik gemacht! So ist es nur zu begrüssen, wenn Frau Rühmland in ihrer knapp gehaltenen, aber das Wesentliche aufzeigenden Abhandlung die Militärgerichtsbarkeit in der DDR zusammenfasst. Sie schreibt dabei sowohl über die Militärgerichte als auch über die Rechtspflege in den DDR-Streitkräften und schildert die Zusammenstellung der Militärgerichte sowie ihre Zuständigkeit. Auch die Institution der Militärstaatsanwaltschaft gehört zum Inhalt der Abhandlung, deren Fortsetzung, wenn möglich, umfangreicher nur wünschenswert wäre! PG