

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

Band: 83 (2010)

Heft: 9

Vorwort: Cyberwar, der lautlose Krieg

Autor: Haudenschild, Roland

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: 19.11.2024

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

Cyberwar, der lautlose Krieg

Cyberwar ist eine Wortkombination aus den englischen Wörtern Cyberspace und War; sie bedeutet im engeren Sinn die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. In einem weiteren Sinn sind damit die hochtechnisierten Formen des Krieges im Informationszeitalter gemeint, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basieren.

Der Begriff soll erstmals 1993 in einer Studie *Cyberwar is coming!* Für die RAND Corporation verwendet worden sein, welche eng mit dem US-Verteidigungsministerium zusammenarbeitet.

Welche Methoden und üblichen Verfahren umfasst Cyberwar:

- Spionage: Das Eindringen in fremde Computersysteme zum Zwecke der Informationsgewinnung
- Defacement: Veränderung am Inhalt einer Webseite, um u.a. Propaganda zu schalten
- Diverse Formen von Social Engineering
- Einschleusen von kompromittierter Hardware, die bewusst fehlerhaft arbeitet oder Fremdsteuerung erlaubt
- Denial-of-Service-Attacken, um feindliche Dienste zu stören oder vollständig zu unterdrücken
- Materielle Angriffe (Zerstören, Sabotage, Ausschalten) von Hardware (z.B. Kabel-, Antennen- und Satellitenverbindungen).

Die Kriegführung hat sich unaufhaltsam gewandelt; wurde früher mit grossen Armeen gekämpft, schwere Waffen eingesetzt und verlustreiche Schlachten geschlagen, befassen sich heute ausgewählte Spezialisten mit „virtuellen“ Waffen und das Kampfgebiet ist elektronisch und unsichtbar. Der Cyberspace als Schlachtfeld der Zukunft umfasst nicht nur einige Computer und Server, sondern fast die ganze Infrastruktur einer modernen Gesellschaft.

Jedermann kann heute mit der umfassenden Vernetzung über das Internet kommunizieren; ein Vorgang welcher grosse Vorteile aber auch akute Gefahren beinhaltet.

Ein landesweiter Stromausfall kann auf die gesamte Volkswirtschaft westlicher Staaten verheerende Folgen haben. Innerhalb Minuten bricht der gesamte Verkehr zusammen, die Industrieunternehmen stehen still, das System der Dienstleistungen funktioniert nicht mehr und die Grundversorgung der Bevölkerung ist nicht mehr gewährleistet.

Für dieses Szenario ist keine kriegerische Handlung notwendig, sondern ein Computer reicht völlig aus. Die weltweite Vernetzung über das Internet führt zu neuen Schlachtfeldern. Die Computer Network Operations sind ein Teil des globalen Cyberwar, einer kriegerischen Auseinandersetzung mittels Manipulation und Kontrolle gegnerischer Computernetze.

Die Schweiz hat diese Bedrohung erkannt. Der Sicherheitspolitische Bericht vom 23. Juni 2010 erwähnt unter den sicherheitspolitischen Trends die Anwendung von Machtpolitik; dazu gehört aber nicht nur der Einsatz militärischer Mittel: «es gibt auch andere, subtilere Mittel: so die Manipulation der Energieversorgung, um andere Staaten unter Druck zu setzen, oder Cyber-Angriffe zur Blockierung der Informatik-Infrastruktur oder zur Aushorchung von Ministerien, Armeen und Unternehmen.»

Unter den direkten Bedrohungen und Gefahren sind im Bericht u.a. die Angriffe auf die Informatik- und Kommunikationsinfrastruktur enthalten: «Information ist ein immer wichtiger werdendes Gut. ... Angriffe auf Informatik- und Kommunikationsstrukturen sind attraktiv, weil Angreifer aus weiter Distanz, mit kleinem Aufwand und geringem Erkennungsrisiko Schaden anrichten können. Diese Infrastrukturen sind deshalb jederzeit ... Bedrohungen und Risiken ausgesetzt. Die Schweiz verfügt über keine übergreifenden Massnahmen zur Abwehr von Angriffen auf Informatik- und Kommunikationsinfrastrukturen. ...»

Der Bundesrat misst dem Schutz der Informatik-Infrastrukturen hohe Bedeutung zu und wird eine Strategie zur Bekämpfung von derartigen Angriffen ausarbeiten, die effiziente und wirksame Massnahmen gegen Spionage, unbefugte Beschaffung und Missbrauch von Daten sowie Angriffe auf eigene Netze umfasst.»

Cyberwar, der lautlose Krieg ist allgegenwärtig; seine Gefahren sind erkannt; Massnahmen sind vorgesehen.

Roland Haudenschild

Herausgegriffen

Wasserproblematik 2

Im Blickpunkt

Finnlandreise der SOLOG 3

Hintergrund

Die Militäretik der Schweizer Armee 10

SOLOG / SSOLOG

Agenda und Einladung zum Herbstanlass 13

SFV / ASF

Agenden und Rückblick auf Anlässe 15

Hommage à Gaston Durussel 18

VSMK / ASCCM / ASCM

Rückblicke 21



Titelbild

«Flagge von Finnland, Emblem der finnischen Verteidigungskräfte und Territoriale Aufteilung der Landesverteidigung».