

Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 86 (2011)
Heft: 3

Artikel: Der Krieg von morgen
Autor: Schlüer, Ulrich
DOI: <https://doi.org/10.5169/seals-715414>

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: 15.03.2025

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

Der Krieg von morgen

Verspätet wurde bekannt, dass ums Jahresende 2009 mehrere Fahrzeuge im Gotthard-Strassentunnel urplötzlich Wendemanöver vorgenommen hatten. Teilweise äusserst gefährliche Situationen waren die Folge.

NATIONALRAT ULRICH SCHLÜER, FLAACH

Offensichtlich wendeten nur ausländische Fahrzeuge. Einige der danach angehaltenen Lenker sagten übereinstimmend, ihr GPS-Navigationssystem habe ihnen den Befehl zum Wenden gegeben. Weiter ergab sich, dass auch Schweizer Fahrzeuge diesen GPS-Befehl erhalten hatten.

Die Lenker befolgten ihn im Tunnel aber nicht. Sie wussten, dass vor allem ältere GPS-Geräte bei Tunneldurchfahrten manchmal «spuken» – verwirrt durch Strassen, die über dem Tunnel die Tunnelroute kreuzen. Von Gotthard-Passanten wurden zuvor allerdings nie Routenverwechslungen ihres Geräts bekannt. Die Gründe für die plötzlichen Wendemanöver im Gotthard wurden nicht genauer eruiert.

Angriff aufs EDA

Sicherheit besteht aber, dass das Schweizer Aussendepartement EDA Ziel eines schweren Hacker-Angriffs wurde. Offizielle Nachrichten dazu sind spärlich. Betroffene bezeichnen den Angriff aber als schwerwiegend.

Die im gespeicherten Wissen des EDA angerichteten Schäden seien längst nicht behoben, die gestohlenen Informationen seien brisant. Weil ähnliche Angriffe schon

das Computer-Netzwerk der deutschen Regierung, insbesondere jenes der deutschen Bundeswehr, getroffen haben, wofür als Urheber China identifiziert werden konnte, mutmasste man auch bezüglich des Angriffs aufs EDA auf chinesische Urheberschaft.

Schliesslich verfügt China über eine Spezialisten-Truppe für Computerangriffe. Cyber War heisst diese neue Kriegsform – die längst nicht nur auf Armeen zielt.

Wer war der Urheber?

In Bern ist inzwischen durchgesichert, dass der Angriff aufs EDA keineswegs china-relevanten Daten galt. Vielmehr sei wichtiges gespeichertes Wissen zur Nahost-Diplomatie geraubt worden. Bern tappt bezüglich Täterschaft völlig im Dunkeln. Obwohl auch Bern weiss, dass Cyber War eine Realität und äusserst gefährlich ist. Wer in sensible Netze eindringen kann, entscheidet über das Funktionieren des Transportwesens, des Zahlungsverkehrs, des Rechnungswesens. Er entscheidet, ob Kampfflugzeuge im entscheidenden Moment überhaupt starten können.

Er kann bewirken, dass Verkehrsflugzeuge beim Landen neben die Pisten geraten. Ob auch der Fall «Wendemanöver Gotthard» auf einen Cyber-Angriff zurück-



Wachsam bleiben: Auto wird durchsucht.

geht, wurde bisher nicht untersucht. Die Schweiz wäre gut beraten, dies rasch nachzuholen. Vorbereitung auf Cyber War gibt es in der Schweiz bisher nicht.

Obwohl auch die 4450 angeblich identifizierten UBS-Konten von behaupteten Steuerbetrüggern (woher haben die USA nur diese Zahl?) das Ergebnis eines Einbruchs ins Computernetzwerk der UBS sein könnten – zwecks Ausschaltung des erfolgreichen Finanzplatz-Konkurrenten Schweiz.

Es ist höchste Zeit, dass sich Bern endlich mit den modernen, äusserst gefährlichen Bedrohungsformen befasst. +

Meldestelle MELANI: Aktivitäten von Cyberkriminellen nehmen zu

Systeme zur Überwachung, Kontrolle und Steuerung von Industrie- und Versorgungsanlagen sind zunehmend im Visier von Cyberkriminellen. Ebenfalls zeichnet sich eine Verlagerung der Angriffe mittels E-Mails mit Anhang oder Links hin zu Webseiteninfektionen, mittels so genannten Drive-By Infektionen ab. Dies sind zwei der Hauptthemen des neunten Halbjahresberichtes der Melde- und Analysestelle Informationssicherung (MELANI).

Nebst den aktuellen Gefahren wie der Trojaner Gozi, der Missbrauch von Schweizer E-Mail-Konten oder dem gezielten Versenden von E-Mails mit Mal-

ware an Kaderpersonen, widmet sich der Bericht der zunehmenden Bedrohung von SCADA-Systemen und der Zunahme von Drive-By-Infektionen.

Sogenannte SCADA-Systeme (Supervisory Control and Data Acquisition) werden zur Überwachung, Kontrolle und Steuerung von Industrieanlagen oder von Infrastrukturen zur Verteilung lebenswichtiger Güter wie Strom, Wasser, Brennstoffe oder im Bereich des Transports und Verkehrs eingesetzt. Ohne Informations- und Kommunikationstechnologie (IKT) ist deren Einsatz undenkbar. Heutige SCADA-Systeme benutzen vermehrt In-

ternettechnologien, um mit dem Zentralrechner zu kommunizieren. Dies bringt mit sich, dass SCADA-Systeme denselben Bedrohungen ausgesetzt sind, wie sie vom Internet her bekannt sind. Schadsoftware und Hacker halten Einzug.

Die Sicherheit dieser Systeme, die für das Funktionieren unserer Gesellschaft zentral sind, muss erhöht werden. Dabei geht es aber nicht nur um das Erschweren von Hacker-Angriffen, sondern auch um das Minimieren möglicher technischer Störungen, die den Ausfall wichtiger Systeme zur Folge haben können.

Aus einem Bericht MELANI