

RÜSTUNG

Den Laptop im Tornister

Militär-Strategen planen für den Krieg im 21. Jahrhundert: Elektronische Attacken auf lebenswichtige Datennetze des Feindes sollen an die Stelle blutiger Kämpfe treten. Mit gewaltigem Aufwand rüstet die U. S. Army schon für den Info-Krieg auf.

Seit Menschengedenken träumen Soldaten vom Siegen. Nun aber dürfen die Militärs von Schlachten schwelgen, die sie schon gewonnen haben, bevor der erste Schuß fällt.

Fredi Büntemeyer zum Beispiel, Major beim „Amt für Studien und Übungen der Bundeswehr“ in Waldbröl, erwartet vom Info-Krieg der Zukunft vor allem Attacken, die nicht mehr auf die „Rüstung“ des Gegners zielen, auf Panzer und Truppen, sondern auf sein „Nervensystem“, die Computer der Führungsstäbe.

Ein „Verbund“ moderner Informationstechnologien, glaubt auch Luftwaffeninspekteur Bernhard Mende, könne eine ganz „neue Dimension“ der Abschreckung erzeugen und dem „möglichen Gegner“ jegliche Art von „Aggression verwehren“.

Schöne neue Welt des Krieges? Wird es im 21. Jahrhundert keine blutgetränkten Schlachtfelder mehr geben?

Über Sieg oder Niederlage im Informationszeitalter, so die jüngsten Zukunftsvisionen der Militärs und ihrer Rüstungslobby, entscheiden nicht mehr Soldaten,

Panzer und Geschütze, sondern raffinierte Computer, clevere Programmierer und ein flinker Datentransfer in digitalen Netzen.

Damit dies die deutschen Soldaten lernen, verbreiten sich Bundeswehr-Blätter wie INFORMATION FÜR DIE TRUPPE oder SOLDAT UND TECHNIK neuerdings über Schlachten-Bilder der Zukunft. Helmut Kohls Armee entdeckt den „Information war“ – den Info-Krieg.

Schon preisen die Konzerne von Daimler-Benz Aerospace (Dasa) bis Siemens im Lobby-Organ WEHRTECHNIK ihre High-Tech-Produkte für das „digitale Gefechtsfeld“ an. Spionage- und Fernmeldesatelliten, unbemannte Kleinflugzeuge, die Aufklärungsbilder in „Echtzeit“ liefern, digitale Funknetze zum Transfer der Daten in die Laptops der Kampftruppe – das alles verheißt den Militärs bessere Übersicht, schnellere „Reaktionsfähigkeit“ und mehr Kampfkraft.

Stören und täuschen lautet die Devise für den digitalen Angriff. In die Computersysteme des Feindes einzudringen, sie

auszuspähen und zu manipulieren: das ist das Ziel.

Per Internet eingeschleuste Computerviren könnten Aufmarschpläne oder Nachschubbefehle löschen, Störprogramme könnten falsche Ziele auf die Radarschirme der Flugabwehr zaubern, Hacker-Attacken ganze Computernetzwerke lahmlegen – und damit die Befehlsgeber mitsamt ihren Truppen.

Was den einen das schöne Bild vom unblutigen Sieg, ist den anderen die Horrorvision der elektronisch erzeugten Blindheit und Lähmung. Und was für die martialische Welt der Militärs gilt, läßt sich auf die gesamte Industriegesellschaft übertragen.

Moderne Daten- und Telekommunikationssysteme, warnt der Autor Sidney Dean in INFORMATION FÜR DIE TRUPPE, seien die neue Achillesferse: „Vermutlich der schwächste Punkt sowohl der wirtschaftlichen wie der militärischen Infrastruktur der Industrieländer“.

Saboteure und Spione, Terroristen oder Mafiosi könnten „mit geringer Ent-



Computergesteuertes Manöver im US-Gefechtszentrum Hohenfels: Angriff per Modem

Schöne neue Kriegsspiele

Beispiele für computergesteuerte Militäroperationen

In den Kommandozentralen werden Computer ständig mit detaillierten Lagebildern gefüttert und simulieren im Vorwege den Ablauf der Militäroperation.



Navigations-, Spionage- und Nachrichtensatelliten übertragen die Datenflut der vernetzten Armee.



„Awacs“-Frühwarnflugzeuge überwachen den feindlichen Luftraum aus großer Entfernung.



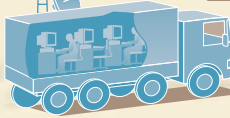
Jagdbomber navigieren satellitengestützt im Zielgebiet. Lasergesteuerte Raketen finden ihre Ziele mit höchster Präzision.



Panzerverbände werden fortwährend mit den neuesten Zielkoordinaten versorgt.



Mobile Rechenzentralen verarbeiten blitzschnell eintreffende Informationen über das Kampfgeschehen und koordinieren Abwehr- und Angriffsoperationen.



High-Tech-Infanteristen empfangen ihre Befehle über Kopfhörer oder den mitgeführten Laptop. Daten über Lage und Bewegung feindlicher Streitkräfte werden ins Helmvisier eingespiegelt.



Unbemannte Flugkörper übermitteln laufend digitalisierte Aufklärungsbilder.



DER SPIEGEL

deckungsgefahr“ und aus „bequemer Ferne“ per Modem die globalen Netzwerke internationaler Konzerne ebenso attackieren wie die Computer staatlicher Behörden oder der Streitkräfte. Werde diesem Risiko nicht bald – durch teure Vorkehrungen zum Schutz der Daten – vorgebeugt, so Deans Horror-Szenario, „könnten Industrieländer in wenigen Jahren per Fernbedienung abgeschaltet werden“.

In dieser hässlichen neuen Welt des Cyber-war gibt es keine Grenze mehr zwischen Zivilem und Militär. In Hunderten von Planspielen haben US-Experten vor-exerziert, wie feindliche Kräfte mit Computerviren oder elektro-magnetischem Puls (EMP) Telefonnetze, Kraftwerke und Banken außer Betrieb setzen – und damit direkt ins Herz der amerikanischen Gesellschaft vorstoßen könnten.

„Das Elektron ist die ultimative Präzisionswaffe“, warnt der ehemalige CIA-Chef John Deutch seine Landsleute. US-Spezialisten hätten bereits eine Vielzahl von Staaten identifiziert, die „Doktrin, Strategie und Werkzeuge einer Info-Attacke“ entwickelten.

Auch international operierende Terror-Gruppen wie die libanesische Hisb Allah, erklärte Deutch voriges Jahr bei einer Anhörung vor einem Senatsausschuß, verfügten „mit Sicherheit über die Fähigkeit“, die Informations-Infrastruktur der USA anzugreifen. Das könne „die nationale und ökonomische Sicherheit“ des Landes „ernsthaft gefährden“.

Die Stützpunkte der Militärs sind in den USA – wie in Deutschland auch – an das öffentliche Telefonnetz angeschlossen. So lassen sich mehr als 150 000 Militär-Computer über das Internet anwählen. Mit geringem Aufwand könnte enormer militärischer Schaden angerichtet werden.

Vor einem Vierteljahrhundert von Pentagon-Militärs noch als absolut störsicheres Kommunikationsmittel für den Atomkrieg aufgebaut, eignet sich das Netz durch sei-

ne Öffnung für zivile Nutzer inzwischen bestens für alle Zwecke der Cyber-Krieger – Mißbrauch inklusive.

Eine Test-Attacke der „Defense Information Systems Agency“ auf das Pentagon führte den Strategen ihre neue Verwundbarkeit vor Augen: Die staatlich besoldeten Hacker schlichen sich in 88 Prozent der Rechner ein – gerade mal vier Prozent der Angriffe wurden von den Computeroperatoren im Verteidigungsministerium überhaupt entdeckt.

Die potentielle Bedrohung ist eklatant: Wenn es einem Gegner gelinge, die zivilen Strom- und Datennetze außer Funktion zu setzen, analysiert die WASHINGTON POST, „werden auch die US-Streitkräfte nicht

mehr essen, sprechen, sich bewegen oder schießen können“. Das Pentagon treibe deshalb ein neuer Alptraum um – die Angst vor einem „elektronischen Pearl Harbor“.

Um sich gegen derartige Überraschungen zu wappnen, gibt Washington schon heute viele Milliarden Dollar für den Zukunftskampf mit den Info-Kriegern aus. Erforscht werden soll ein wirksamer Schutz vor Computerattacken, etwa durch neue Verschlüsselungstechniken.

Die Informationstechnologie, so spekulieren die US-Militärs, werde die Kämpfe der Zukunft ähnlich verändern wie die Ankunft der Panzer im Ersten Weltkrieg, die den Grabenkrieg zum beweglichen



Digitale Kampfausrüstung: Computerdaten ins Visier gespiegelt

PENTAGON

Gefecht wandelten, und damit die Kriegsführung revolutionieren. Und Amerika als einzig verbliebene Weltmacht müsse sich auf diesem Feld die totale Überlegenheit sichern.

Bereits im Juni 1995 graduierten an der „National Defense University“ in Washington die ersten 16 Info-Krieg-Offiziere. Zu ihren Spezialitäten zählen die elektronische Schlachten-Simulation sowie der Einsatz von EMP-Waffen gegen feindliche Computer.

Schon der Golfkrieg gab 1991 den Blick frei auf die Möglichkeiten künftiger Technologie. Tarnkappenbomber zerstörten mit lasergesteuerten Waffen Telefonzentralen und Elektrizitätswerke im Land des irakischen Diktators Saddam Hussein. Vom Boden aus brachten mobile Störsender (Codename „Sandkrebs“) der U. S. Army alle Langwellen-Verbindungen des Iraks durcheinander.

Auch Bosnien dient den US-Militärs als Testgebiet für High-Tech-Gerät. Unbemannte Flugkörper vom Typ „Predator“ kurven über der Krisenregion und liefern Aufklärungsbilder mit einer Schärfe, die selbst einzelne Soldaten in ihren Stellungen sichtbar macht. Erstmals erproben die US-Truppen auch ein „geheimes Internet“, aus dem sie Karten, Luftbilder, Logistik-Daten und Geheimdienst-Informationen abrufen können.

Das alles ist freilich nur eine Vorstufe zum total „digitalisierten Kriegsschauplatz“, von dem amerikanische Militärs und Rüstungslobby schwärmen: Da bekommen etwa Kommandeure in Bunkern fernab des Kriegsgebiets in Echtzeit Lagebilder auf die Monitore projiziert. Computer simulieren daraufhin den Schlachtverlauf – lange bevor ein Schuß fällt.

In solchen Visionen wird auch der gemeine Infanterist zum High-Tech-Krieger. Die Befehle erhält er nicht mehr per Feldtelefon, sondern per Satellit. Sein Helm verfügt über Mikrofon, Kopfhörer und Nachtsichtgerät. Ins Visier können Computerdaten eingespiegelt werden, die ihn allzeit über Ort und Lage, Feindbewegungen und neue Befehle informieren.

Erste Prototypen des Super-Helms, entwickelt vom Elektronik-Konzern Motorola, sind bereits im Test. Die U. S. Army will schließlich jedes Waffensystem und jeden Soldaten – Laptop im Tornister – elektronisch vernetzen. Geschätzte Kosten bis Ende des Jahrtausends: zwei Milliarden Dollar.

Ob der neue Soldaten-Typ die hochgepannten Erwartungen erfüllen kann, bleibt indes ungewiß. Die mit fast 20 Kilogramm Zusatzgepäck zum Info-Krieger aufgerüsteten GIs erzielten in ersten Tests keinen nennenswerten Zuwachs an Kampfkraft.

Und so betrachten die Generäle auf der Bonner Hardthöhe das Tempo, das der große Verbündete vorlegt, mit ge-

mischten Gefühlen. Sie fürchten, die finanziell klammen Streitkräfte der Europäer könnten technologisch abgehängt und später genötigt werden, teuer bei der amerikanischen Rüstungsindustrie einzukaufen.

Vorerst trösten sich europäische Spitzenmilitärs allerdings damit, daß die High-Tech-Spielerei den Amerikanern wenig nützt, wenn in Bosnien ein Soldat auf eine primitive Mine tritt oder ein Hecken-schütze den Fahrer eines Lastwagens ins Visier nimmt.

Auch seien die Verhältnisse in Europa, das schon viele Kriege durchlitten hat, anders als in den USA: Die Amerikaner hielten sich bisher für unangreifbar – vom Krieg mit Atomraketen einmal abgesehen – und erlebten jetzt als Trauma, daß Freaks

Hohe Offiziere werden regelmäßig mit E-Mail-Botschaften traktiert

aus der Ferne in ihre heimischen Computer eindringen können.

Die Militärs in Bonn warten deshalb erst einmal ab: Im „Amt für Studien und Übungen der Bundeswehr“ beschränken sich die Experten darauf, Fachliteratur auszuwerten, Dokumente zu sammeln und die Ergebnisse routinemäßig in Studien zusammenzufassen. Im Verteidigungsministerium beschäftigen sich mit dem Konzept des Info-Krieges zwei Stabsoffiziere des Referats „Militärstrategie“ – im Hardthöhen-Jargon als „die Wolkenschieber“ verspottet.

Heeresinspekteur Helmut Willmann hat seinen Fachleuten für elektronische Kampfführung zwar die Parole „we must win the information war“ vorgegeben. In der Praxis ist er aber von seinem US-Kameraden Dennis Reimer noch weit entfernt: Der Stabschef der U. S. Army drückt jedem Obristen bei der Beförderung zum Brigadegeneral einen Laptop in die Hand. Um zu testen, ob die hohen Offiziere mit dem Computer umgehen können, traktiert er sie danach regelmäßig mit E-Mail-Botschaften.

Willmanns Luftwaffen-Kamerad Mende erkennt zwar an, daß „die Beherrschung der Informationstechnologie einen strategischen und operativen Vorteil“ bringen könnte. Aber, so der Luftwaffenchef skeptisch: „Begriffe wie ‚Cyber-war‘ erwecken in mir zumindest ein unbehagliches Zweifeln.“

Einen Vorgeschmack auf die potentielle Wirkung einer Info-Attacke hat Mendes Luftwaffe indes schon bekommen: Bei einem Tornado-Geschwader stürzte ein simples Netz aus einigen Computern ab, mit dessen Hilfe die Wartung der Kampffjets koordiniert wird. Techniker mußten plötzlich die bürokratischen Prozeduren handschriftlich erledigen. Und so vergingen drei Tage, bis der erste Tornado wieder starten konnte. ♦