

USA

Schweiß schnuppern

Pentagon-Offiziere planen den Krieg der Zukunft. Er wird am Computer entschieden – unblutig.

In einem abhörsicheren Raum, den die Führungsstelle für Aufklärung und Sicherheit bei der US-Armee im Norden von Virginia für geheime Besprechungen benutzt, zeichnet Oberst Mike Tanksley die Umrisse eines neuen Armageddons nach.

Sollte der Beherrscher irgendeines modernen Babylon (Bagdad, Teheran oder Tripolis etwa) in nächster Zukunft einen US-Verbündeten bedrohen (Riad vielleicht, Kairo oder Jerusalem), würden die Vereinigten Staaten nicht wieder sofort ganze Heerscharen in Bewegung setzen wie 1990 gegen Saddam Hussein. Statt dessen würde der Präsident die Aggressoren mit einem zeitgemäßen Äquivalent biblischer Plagen bestrafen.

Schon bald wird solches Unheil allerdings mit Hilfe von PC-Mäusen, Computerkeyboards und Bildschirmen entfesselt: Da wird zunächst ein Computervirus in die Schaltzentralen des gegnerischen Telefonsystems eingespeist, um alle Fernsprecheinrichtungen lahmzulegen. Heimtückische Software-Programme, die sogenannten Trojanischen Pferde des Datenzeitalters, zerstören die Rechenzentralen des Eisenbahnnetzes. Sind auf diese Weise erst einmal die Stellwerke ausgeschaltet, bricht der Nachschub zusammen.

An der Front befolgen die feindlichen Offiziere zwar noch Befehle, die sie über Sprechfunk erhalten. Aber was die Kommandeure nicht wissen: Ihre Orders sind gefälscht, die Truppen verlaufen sich alsbald in der Wüste. US-Flugzeuge stören derweil die Fernsehsender des Gegners und strahlen eigene Propaganda aus, um die Bevölkerung gegen den Tyrannen aufzuwiegeln.

All das geschieht, ohne daß auch nur ein Schuß gefallen ist. Auf diese Weise, hofft Oberst Tanksley stolz, ließe sich ein „Krieg beenden, bevor er überhaupt begonnen hat“.

„Information warfare“, Krieg der Computer, heißt das neueste Konzept des Pentagon. Die Cyber-Krieger am Potomac hoffen, künftige Schlachten genauso grundlegend zu verändern, wie es Maschinengewehre im Ersten und Panzer im Zweiten Weltkrieg getan haben. Die Strategen wollen die technologi-

schen Wunder des späten 20. Jahrhunderts so nutzen, daß sie künftig blitzschnelle, unsichtbare und vernichtende Angriffe auf das Militär und die zivile Infrastruktur des Gegners führen können. Admiral William Owens, stellvertretender Vorsitzender der Vereinigten Stabschefs: „Das ist Amerikas Beitrag zur modernen Kriegführung.“

Schon beim letzten Waffengang der USA waren Anfänge eines Computerkriegs zu erkennen. Am ersten Tag des Golfkriegs machten die Präzisionswaffen amerikanischer Tarnkappenbomber den irakischen Diktator reaktionsunfähig, indem sie das Telefonsystem und Bagdads Elektrizitätswerke zerstörten.

Doch das war erst der Anfang. An der Entwicklung des Computerkriegs arbeiten bereits Expertenteams aller Waffengattungen mit Hochdruck. Professoren der National Defense University in Washington haben in aller Stille die ersten 16 Abschlußdiplome an Cyber-Kampf-Spezialisten ausgegeben. Die sollen nun Verteidigungsstrategien gegen Angriffe auf US-Computer entwickeln oder über den Einsatz von virtueller Realität bei Manövern nachdenken.

Noch in diesem Jahr wollen Offiziere im Verteidigungsministerium die Resultate von mehr als einem Dutzend geheimer Computerkriegssimulationen auswerten, die in den vergangenen zwei Jahren stattfanden. Die Planer werden darüber entscheiden, wie militärische Taktik künftig auszusehen hat.

Auch die Geheimdienste untersuchen derzeit, ob mit Hilfe von Computerhak-

kern ein Krieg zu führen ist. Zusammen mit den Nachrichtendiensten der Armee, der Marine und der Luftwaffe hat die National Security Agency (NSA) erforscht, wie besonders bösartige Computerviren in die Rechner eines feindlichen Landes eingespeist werden können.

Geschickt platzierte „Trojanische Pferde“ würden bis zu einem bestimmten Zeitpunkt untätig bleiben, bevor sie beginnen, Daten des Gegners zu zerstören. Die elektronischen Killer könnten eingesetzt werden, um etwa die wichtigsten Computer der Luftabwehr oder der Zentralbank des Gegners auszuschalten.

Die CIA verfügt über ein Programm, mit dem zerstörerische Computerchips in Waffensysteme eingebaut werden könnten, die ein ausländischer Hersteller in ein möglicherweise feindliches Land exportiert. „Wenn das Waffensystem dann im Ernstfall gegen uns eingesetzt werden soll“, erklärt ein CIA-Experte, „explodiert der Sprengkopf nicht.“

Daß es im Krieg von Bits und Bytes bereits exotischere Waffen als Computerviren gibt, enthüllt der Rüstungsexperte des Nachrichtenmagazins *Time*, Douglas Waller. Wissenschaftler des National Laboratory von Los Alamos in New Mexico haben ein koffergroßes Gerät entwickelt, das einen starken elektromagnetischen Impuls (EMP) erzeugt. Eine Spezialeinheit der Streitkräfte könnte damit in die Hauptstadt eines gegnerischen Landes vordringen, den EMP-Koffer im Zentrum abstellen und das Gerät einschalten. Der Impuls würde dann alle

Lautlose Attacke Methoden und Angriffsziele im Computerkrieg

Störung aus dem Äther

Von Spezialflugzeugen ausgestrahlte Desinformation verwirrt die Abläufe im feindlichen Militärapparat; durch TV- und Radiopropaganda wird die Bevölkerung beeinflusst.

Elektromagnetische Impulse (EMP)

Eine aktienkoffergroße EMP-Bombe, die von Spezialeinheiten in der Nähe von elektronischen Kommunikationssystemen platziert wird, detoniert und friert sämtliche Datenströme ein.

Computerviren

werden von Spezialisten in die Netze eingeschleust. Sie legen den Telefonverkehr und das Transportsystem lahm.

Trojanische Pferde

01011001

Software-Programme mit Zeitzündung lösen zu einem genau berechneten Zeitpunkt Fehlfunktionen in Computern aus; denkbare Ziele: Banken, Elektrizitätswerke.

DER SPIEGEL



Zukunftskrieger, Ausrüstung: „Vor der wirklichen Schlacht werden Staatenlenker virtuelle Kriege ausfechten“

elektronischen Geräte der Umgebung zerstören.

Andere Entwicklungen kombinieren biologische und elektronische Waffen. Im Auftrag des Pentagon wollen Wissenschaftler Mikroben züchten, die das Isoliermaterial und andere Bauteile des Computers auffressen können.

Auch die Feindaufklärung wird sich durch den Cyber-Krieg grundlegend verändern: Im Massachusetts Institute of Technology arbeiten Wissenschaftler an einem Flugobjekt von der Größe einer Zigaretenschachtel. Der Miniflieger soll Bilder von gegnerischen Truppenbewegungen liefern.

Kleinstsensoren werden den Feind künftig sogar riechen. Aus Flugzeugen heraus könnten Aerosole über gegnerische Truppen versprüht werden, Biosensoren würden anschließend aus der Luft jede ihrer Bewegungen melden. Thomas Baines vom Argonne National Laboratory in Illinois sagt: „Wir können Ortsveränderungen am Atem oder am Schweiß der Soldaten erschnuppern.“

Experten der Johns-Hopkins-Universität testen derzeit ein höchst komplexes Computersystem, das Radarsignale in ein dreidimensionales Monitorbild verwandelt. Statt verwirrender Symbole bekommt beispielsweise der kommandierende Admiral einer Flugzeugträgergruppe grafische Darstellungen gegnerischer und eigener Flugzeuge zu sehen. Mit seiner PC-Maus kann er die Bedrohungslage aus jeder Perspektive studieren.

Der Computer empfiehlt Angriffsziele und beobachtet sogar den Himmel für den Kommandeur, wenn der einen Augenblick lang den Gefechtsstand verlas-

sen hat. Entdeckt der Computer eine Gefahr, sendet er ein Alarmsignal für den Offizier vom Dienst.

Bis zum Jahre 2010, so hofft die U.S. Army, werde „das Schlachtfeld der Zukunft vollkommen digitalisiert sein“. Alle Soldaten und Waffensysteme wären dann miteinander vernetzt.

Ein Forscherteam des Elektronikonzerns Motorola will gemeinsam mit Experten der Streitkräfte im nächsten Jahr den Prototyp einer Ausrüstung für den „Krieger des 21. Jahrhunderts“ vorstellen. Dessen Helm verfügt über ein eingebautes Mikrofon und Kopfhörer. Nachtsichtgeräte und Wärmebildsensoren, mit denen der Soldat auch in der Dunkelheit sehen kann, sind ebenfalls integriert. Ein durchsichtiges Gelände-Display, das wie ein Visier vor seine Augen geklappt wird, zeigt dem GI, wo er sich gerade befindet. Über diesen Bildschirm wird er ständig mit neuesten Aufklärungsdaten versorgt.

So soll sich der Krieg von morgen den Science-fiction-Vorstellungen von heute immer weiter annähern. „Eines Tages werden Staatenlenker virtuelle Kriege ausfechten, bevor sie sich entscheiden, wirklich in die Schlacht zu ziehen“, sagt Generalleutnant Jay Garner, der Armee-Chef für Weltraumfragen.

Einige Zukunftsforscher glauben sogar, daß Nationen ihre Kriege künftig nur noch im Computer simulieren und auf blutige Gefechte auf dem Schlachtfeld vollständig verzichten könnten – was für Militärs von heute allerdings unvorstellbar ist. Garner: „Ich glaube nicht, daß der Krieg zum schmerzlosen Videospiel wird.“

Skeptiker innerhalb und außerhalb des Pentagon halten die angeblichen Vorzüge des Computerkriegs denn auch für maßlos übertrieben. „Die Leute in Bosnien bringen sich gegenseitig mit Küchenmessern um“, sagt etwa der Verteidigungsexperte William Arkin. „Computerviren werden solche Konflikte nicht beenden.“

Erfahrene Pentagon-Offiziere befürchten außerdem, daß mögliche Feinde Computerwaffen ebenso leicht gegen die USA verwenden könnten. Die dafür benötigte Technologie ist nicht besonders teuer, schon Computer und Modem reichen aus. „Elektronische Kriegführung ist der große Gleichmacher“, sagt der Futurologe Alvin Toffler. „Niemand muß groß und reich sein, um bei einem solchen Krieg mitzumischen.“

Die Gefahr ist durchaus real. Computerhacker könnten die neuen Söldner sein, die sich gegen Höchstgebot jedem Diktator zur Verfügung stellen. Pentagon-Mitarbeiter berichten, daß eine Gruppe holländischer Cyber-Freaks während des Golfkriegs Irak anbot, für eine Million Dollar den US-Aufmarsch im Nahen Osten elektronisch zu stören. Doch Saddam lehnte das Angebot ab.

Auch außerhalb des Pentagon und seiner militärischen Installationen könnte ein elektronischer Angriff auf die USA katastrophale Folgen haben. Die NSA ist besorgt, daß die heute vorhandenen Computer der Banken, der großen US-Börsen und der Flugleitstellen verhältnismäßig einfach lahmgelegt werden könnten. „Wir sind die verwundbarste Nation der Erde“, fürchtet NSA-Chef John McConnell. □