



US-Soldaten bei digitalem Manöver, jugoslawische Flugabwehr gegen Nato-Luftangriffe: Mit unsichtbaren Waffensystemen wird eine Nation

MILITÄRTECHNIK

„Die Fronten sind überall“

Im Kosovo-Krieg gelang es US-Militärs offenbar, fiktive Flugzeuge in die Zielcomputer der serbischen Flugabwehr zu zaubern – ein Vorspiel zum Krieg der Zukunft? Die weltweiten Datennetze könnten zum Schlachtfeld werden. Mit Hilfe von Computer-Viren und geheimen Zugangscodes lässt sich die digital gesteuerte Infrastruktur des Gegners attackieren.

Elf Wochen feuerte die serbische Flugabwehr. Doch die Raketen explodierten meist im Leeren. Nur zwei Flugzeuge – einen Tarnkappenjet vom Typ F-117A und einen F-16-Jagdbomber – verlor die Nato im Kosovo-Krieg durch Abschuss.

Eine der Ursachen für die erstaunlich geringe Trefferzahl der jugoslawischen Abwehr wird nun deutlich: Im Krieg auf dem Balkan wurde offenbar erstmals eine Waffe eingesetzt, welche die künftige Kriegsführung total umkrempeln dürfte.

Viele der serbischen Raketen trafen durchaus ihr Ziel – doch dieses erwies sich als Phantom. Denn US-Elektronikexperten hatten die Computer der jugoslawischen Flugabwehrsysteme manipuliert: Die Radaroffiziere sahen auf ihren Monitoren feindliche Flugzeuge aufblitzen, wo in Wahrheit nur leerer Himmel war.

Die Einspeisung der virtuellen Ziele, so berichtet das US-Fachblatt „Aviation Week

& Space Technology“, sei einfach gewesen. Auch hätten die USA im Kosovo-Krieg „mit Hilfe ihrer Computernetze die Stromversorgung und die Kommunikationswege“ des Gegners lahm legen können, behauptet einer der Experten, die im US-Verteidigungsministerium derzeit unter strenger Geheimhaltung den jüngsten Balkan-Krieg analysieren.

Er wird, so viel scheint sicher, als eine Art Vorspiel einer neuen Kriegsführung in die Geschichte eingehen, die unter den Strategen RMA genannt wird. Das Kürzel steht für „Revolution in Military Affairs“. Mit der Umwälzung streben die Militärs einen Krieg an, der ohne Sprengstoff und Bomben („War by other means“ – WBO) ausgefochten wird, wenn möglich ohne Tote („zero death“). Zum unblutigen Schlachtfeld werden die weltweit gespannten Datennetze mit all ihren Verzweigungsästen.

Sieger der neuartigen Waffengänge ist, wer sich die Kontrolle über möglichst viele Informationen verschafft. Der Verlierer ist der Informationsüberlegenheit seines Gegners ausgeliefert.

Die Vorbereitungen auf den Cyber-Krieg laufen auf Hochtouren. Das Tempo wird, anders als zu Zeiten des Kalten Krieges, nicht von den Militärs und deren Waffenarman vorgegeben. Die Informationskrieger hecheln hinter der Hard- und Software her, die im letzten Jahrzehnt von den Experten in den Computerfirmen, Halbleiterlabors und Denkfabriken der freien Wirtschaft ausgetüftelt wurden.

Der amerikanische Auslandsgeheimdienst CIA hat in seinem Hauptquartier in Langley (Virginia) vor drei Jahren eine Stabsstelle eingerichtet, deren Mitarbeiter sich ausschließlich um den Informationskrieg („Information Warfare“ – IW) kümmern. Auch die supergeheime National Se-



und so eine Wirtschaft kollabieren lassen können. Das Elektron als kleinster Baustein der Datenverarbeitung, sagt John Deutch, ehemals Direktor der CIA, „ist die ultimative Präzisionswaffe“.

Angreifen und manipulieren lassen sich die elektronischen Telekommunikationssysteme vielfach heute schon, so etwa durch:

- ▶ Viren – Programm-Codes, die Datensätze manipulieren und sich selbständig vermehren; bekannt sind derzeit knapp 17 000 Viren, fünf Prozent von ihnen gelten als potenziell gefährlich;
- ▶ Würmer – Programme, die geheime Daten wie Passwörter oder Codes ausspähen und dem Absender melden;
- ▶ Logische Bomben – Software, die unter bestimmten Konstellationen zum Beispiel große Datensätze zerstört;
- ▶ Falltüren – in Software eingebaute Geheimzugänge, die ein Eindringen in das System unter Umgehung gängiger Sicherheitsvorkehrungen erlauben;
- ▶ Elektromagnetische Pulse (EMP) – energiestarke, sehr kurzweilige Strahlung, die elektronische Anlagen in Bruchteilen von Sekunden zerstören kann, selbst wenn diese ausgeschaltet sind.

Dass die Vereinigten Staaten als derzeit einzige militärische Supermacht und technisch fortgeschrittenste Nation zugleich auch besonders verwundbar ist, zeigte ein Kriegsspiel, das Amerikas höchste Militärs vorletzten Sommer anberaumten.

Aufgabe eines feindlichen „Red Team“ war es, im Verlaufe des Unternehmens mit dem Codenamen „Eligible Receiver“ (Befugter Empfänger) die Fähigkeit der US-Streitkräfte und der politischen Führung zu testen, einem massiven „Cyber-Angriff“ zu widerstehen.

Die roten Hacker waren gehalten, nur solche Techniken und Informationen zu nutzen, die öffentlich zugänglich waren, etwa im Internet von jedermann abrufbar. Nach drei Monaten hatten die Hacker es geschafft: Amerikas Fähigkeit zur Führung eines Krieges war lahm gelegt.

Offenbar geschockt vom Ausmaß der eigenen Verwundbarkeit, verfügten die

paralysiert, ohne dass ein einziger Soldat ins Feld geschickt werden muss

curity Agency (NSA), die Amerikas Abhöreinrichtungen in aller Welt betreibt, mischt auf diesem Gebiet mit.

In einem 1996 erschienenen Report werden die Aufgaben der Geheimdienste definiert: Sie sollen den Vereinigten Staaten „die globale Informationsüberlegenheit“ verschaffen. Hilfe dabei erhalten die CIA- und NSA-Trupps durch Kollegen in neuen Sonderabteilungen, die inzwischen bei allen Waffengattungen der US-Streitkräfte und auch bei der Bundespolizeibehörde FBI ihren Dienst aufgenommen haben.

Vor einigen Jahren noch, sagt der amerikanische Experte für Informationstechnik, Howard Frank, habe „niemand die Möglichkeiten und Auswirkungen eines Informationskrieges ernst genommen“. Nun sind tausende von Info-Spezialisten damit beschäftigt, die USA für einen digitalen Waffengang zu rüsten, aber auch Frühwarnsysteme und Abwehrmechanismen gegen IW-Angreifer zu entwickeln.

Regelmäßig testet die neue Kaste der Cyber-Krieger in Simulationsübungen und Kriegsspielen ihre Kenntnisse. Nur gelegentlich sickern Einzelheiten über den Verlauf der im Computer ausgefochtenen „War Games“ an die Öffentlichkeit.

Zu den Quellen zählen etwa Studien, die der US-Kongress von unabhängigen Gremien oder angesehenen Denkfabriken durchführen lässt. Auch eine Reihe von Büchern über das neue Kapitel der Militärgeschichte ist inzwischen erschienen. Es geht darin um stumme und unsichtbare Waffensysteme, die eine ganze Nation para-

lysiert, ohne dass ein einziger Soldat an die Front geschickt werden muss.

Was sich wie Science-Fiction-Thriller liest, ist häufig schon Realität, wie der amerikanische Militär- und Geheimdienstjournalist John Adams in seinem neuesten Buch „The Next World War“ deutlich macht. In diesem fiktiven Großkrieg sind laut Untertitel „die Computer die Waffen“ und „die Fronten überall“.

Die Voraussetzungen für eine neue Form von Krieg sind bereits vorhanden: Dieselben Netze, durch die sich Banküberweisungen, persönliche E-Mails, Einsatzpläne für Vertreterkolonnen oder Hotelreservierungen befördern lassen, eignen sich auch zum Versand von Desinformationen sowie von Daten, die Kraftwerke, Flugkontrolle oder Bankenverkehr lahm legen



US-Verteidigungsministerium: „80 bis 100 Hacker-Angriffe pro Tag“

Kriegsspielstrategen die höchste Geheimhaltungsstufe über die Ergebnisse der Niederlage. Aus Sorge, dass die aufgezeigten Schwachstellen nicht behoben würden, ließen einige Mitspieler Einzelheiten durchsickern.

„Mit bemerkenswerter Leichtigkeit“, so berichtet Buchautor Adams, gelang es den Hackern, „die gesamte Logistik durcheinander zu wirbeln“: Eine Jet-Staffel hatte Raketen angefordert – die Hacker klinkten sich ins Nachschubnetz ein und änderten den Bestellzettel; Folge: Statt der bestellten Luft-Boden-Raketen wären im Ernstfall Scheinwerfer angeliefert worden.

In einer anderen Spielsituation warteten hunderte von Soldaten stundenlang auf einem Flugplatz, von dem aus sie mit Zivilflugzeugen ins Einsatzgebiet geflogen werden sollten. Die Transportanforderung war ordnungsgemäß erteilt, doch die vom roten Hackerteam umgeleiteten Jets waren längst zu einem anderen Einsatzort unterwegs.

Solche Spiele werden vor realem Hintergrund erdacht: Die Anzahl der Versuche von Hackern, in die Datenbanken des US-Verteidigungsministeriums einzudringen, belaufe sich, so der stellvertretende US-Verteidigungsminister John Hamre, auf „80 bis 100 pro Tag“.

Für Surfveternanen sind die Computer im Fünfeckbau am Ufer des Potomac eine beliebte Spielwiese. 95 Prozent der „nicht geheimen“ militärischen Kommunikation laufen über öffentliche Datennetze. Zu großen Teilen besteht die Welt im Pentagon mittlerweile aus marktgängiger Hard- und Software.

Die Modernisierung wurde so rasch betrieben, dass die Spezialisten für den Schutz gegen unbefugte Zugriffe nicht mithalten konnten. Ergebnis: „Die amerikanischen Verteidigungssysteme wurden gegen Cyber-Angriffe zunehmend verwundbar“, so das Fazit einer Studie, die das National Research Council im Auftrag des US-Kongresses erstellte. Seit einigen Monaten steht der 298 Seiten umfassende Report im Internet.



Jet-Start von Flugzeugträger: Scheinwerfer statt Raketen

Im Gegensatz zu den Militärs, denen beigebracht wird, das Unkalkulierbare zu erwarten und sich darauf einzustellen, haben Amerikas Unternehmer und Politiker häufig Schwierigkeiten, die unsichtbaren Angriffe auf die Computer der Nation ernst zu nehmen.

Wenn Richard Clarke, von Clinton berufener Terrorismus-Experte im Weißen Haus, amerikanischen Konzernbossen die Gefahr eines Cyberwars erläutert, „dann glauben die, ich würde von einem 14-jährigen Hacker reden, der ihnen ihre Web-Seite kaputt macht“. Dabei gehe es ihm um „Leute, die in einer Stadt das Licht aus-

knipsen, die das Telefonnetz ausschalten und das Verkehrssystem lahm legen“, bezieht Clarke. Jeder Angriff auf den „amerikanischen Cyberspace“ sei ein Angriff auf die Vereinigten Staaten, „so als landeten Soldaten an der Küste von New Jersey“.

Doch noch ist die Gefahr von Attacken aus dem Ausland gering. Denn gegenüber potenziellen Gegnern wie etwa der darniederliegenden Ex-Weltmacht Russland und der aufstrebenden Regionalmacht China genießen die Computer-Nationen des Westens und ihre asiatischen Zuarbeiter wie Japan, Taiwan oder Indien eine gewaltige Info-Übermacht.

Als Russland beispielsweise bei IBM und Siemens 100 Großrechner für den zivilen Einsatz bestellte, machte die CIA schnell als tatsächlichen Empfänger das Moskauer Verteidigungsministerium aus. Die Software wurde daraufhin mit allerlei Fallen, Viren und Logischen Bomben gespickt und ausgeliefert.

Vor dem Einsatz nahmen Experten des russischen Geheimdienstes FAPSI, Pendant zur amerikanischen NSA, die Großlieferung aus dem Westen unter die Lupe. Ob es ihnen gelang, alle unerwünschte digitale Fracht zu tilgen, ist ungewiss.

Nachhaltig prägte dieser Betrug die russische Haltung gegenüber Amerikas InfoKriegern, die aus Moskaus Sicht gegen Ende der neunziger Jahre damit begannen, die russische Kommunikationstechnik unter ihre Kontrolle zu bringen – mal im Zuge der Privatisierung russischer Hightech-Firmen mit westlichen Krediten, mal durch die Lieferung weiterer Großrechner und Server, vor allem aber durch die verstärkte Lieferung von Personalcomputern.

Im Januar 1995 war jeder vierte der 1,2 Millionen russischen Computer in Russland hergestellt; ein Jahr später waren vier Millionen Computer in Betrieb, von denen fast keiner mehr aus russischen Fabriken stammte. „Sämtliche Geräte, die wir inzwischen für unsere Infrastruktur einsetzen“, sagt der russische Sicherheitsexperte Witalij Zygitshko, „sind westlichen Ursprungs. Und niemand weiß, was in ihnen wirklich verborgen ist.“

Sie könnten die Grundlage jener „Informationswaffen“ bilden, mit denen die russischen „Informations- und Telekommunikations-Systeme penetriert werden können, um Informationen zu stehlen, zu deformieren oder zu zerstören“, heißt es in einem 60 Seiten umfassenden Dokument, das dem amerikanischen Autor Adams vom FAPSI übersandt wurde.

Ein- und Angriffe auf „automatisierte oder kritische Technologien“, befürchten die Geheimdienstler, könnten schließlich „Russlands wirtschaftlichen, politischen,



Kommandozone des Energiekonzerns Gazprom in Moskau: Mit Leichtigkeit lahm legen?

technischen und ökologischen Interessen schweren Schaden zufügen“.

Was können die Info-Krieger wirklich? Das im Unklaren zu lassen, ist schon Teil der Schlacht um die Informationshoheit. Die NSA betrachtet jedes Bit auf der Welt als ihr Operationsgebiet. Auf jede Datei sucht sie sich das Zugriffsrecht zu sichern.

Strenge Exportrichtlinien verbieten amerikanischen Softwarefirmen, wirkungsvolle Verschlüsselungsprogramme auf den Weltmarkt zu bringen.

Ohne viel Aufhebens haben sich die großen Softwarekonzerne mit den Begehrlichkeiten der Infowar-Strategen arrangiert. So baut die Firma Lotus in die Exportversion ihrer „Notes“-Software, die in vielen Konzernen den internen E-Mail-Austausch verwaltet, eine Art Sollbruchstelle in den Code ein.

Der Schlüssel, der Firmengeheimnisse vor neugierigen Blicken schützen soll, ist zweigeteilt: Fremde Eindringlinge müssten einen PC jahrzehntelang knobeln lassen, um eine verschlüsselte Nachricht zu entziffern; die NSA jedoch kennt einen Teil des Schlüssels, und den exportgenehmigten Rest, so vermuten Kryptologen, können ihre Spezialrechner innerhalb von Minuten oder Sekunden knacken.

Vorletzte Woche geriet auch Microsoft ins Zwielficht. Als ein Sicherheitsspezialist die neueste Version des Betriebssystems „Windows NT“ unter die Lupe nahm, das auf Millionen von Rechnern weltweit den Datenverkehr regelt, stieß er auf das verdächtige Kürzel „NSAKEY“ in einem Programmteil, der für die Einbindung von Verschlüsselungstechnik in das Betriebssystem verantwortlich ist.

Wozu der bis vor kurzem unbekannt Zweitschlüssel mit dem verdächtigen Namen dient, konnte der Konzern nur gewunden erläutern. Es handele sich um einen Reserveschlüssel für den Fall des „Verlusts des Primärschlüssels“, sei aber unter Microsofts Kontrolle und „zu keinem Zeitpunkt Institutionen oder Behörden bekannt gegeben“ worden.

Kryptologen zweifeln an dieser Lesart. Heftig tobt im Internet die Diskussion über die Tragweite der Entdeckung. Wäre der „NSAKEY“ doch im Besitz des Supergeheimdienstes – so meinen einige –, könnten die NSA-Experten womöglich manipulierte Software als Microsoftprodukt ausgeben und so den Geheimnisschutz nach Belieben aushebeln.

„Haltlose Spekulationen“, erklärt der Gates-Konzern. „Microsofts Erklärungen sind weder logisch noch befriedigend“, findet dagegen SPD-Technologiexperte Jörg Tauss. Schriftlich forderte er die Minister für Inneres, Wirtschaft, Forschung und Justiz auf, zu prüfen, ob man es angesichts der undurchsichtigen Lage beantworten könne, in „sicherheitsrelevanten Bereichen noch Microsoft-Systeme einzusetzen.“ RAINER PAUL, JÜRGEN SCRIBA

TIERE

Lächelnde Killer

TV-Star, verspielter Menschenfreund und Lebensretter – der Delfin gilt als Publikums- liebbling unter den Wildtieren. Jetzt gerät das Bild ins Wanken.

Alles begann mit dem Fund der Mordopfer. Tierärzte und Biologen hatten tote Schweinswale gefunden, gestrandet im Moray Firth, einer Bucht im Nordosten Schottlands.

Ben Wilson, Meeresbiologe an der Universität von Aberdeen, untersuchte die Ka-



Getöteter Schweinswal, „Delfintherapie“ für

daver. Die Tiere hatten gebrochene Rippen, innere Blutungen und Prellungen am ganzen Leib. Bei einigen hatten die Rippen die Lungenflügel zerfetzt. Alles deutete auf äußere Gewalteinwirkung hin.

Waren die Wale mit Fischerbooten kollidiert oder in Netze geraten? Dazu, so fanden die Forscher schnell heraus, passte das Verletzungsmuster nicht.

Verräterisch schienen ihnen vor allem charakteristische, dreieckige Wunden in der Haut einiger Opfer. Sie lagen auf einer Linie und gingen in parallel verlaufende, oberflächliche Kratzer über. Wilson tippte auf Biss-Spuren und vermaß den Abstand der Wunden.

Das Ergebnis erlaubte kaum einen Zweifel: Den passenden Kiefer hat einzig der Große Tümmler, bekannt als Hauptdarsteller der Kinder-Serie „Flipper“. Im