Georg Schöfbänker

Vom Cyberwar zum INFOWAR
Computer und Telekommunikation für den "realen" und "virtuellen" Krieg

Was "Krieg", was ein "Computer" und was "real", was "virtuell", und schließlich was "Kommunikation" ist, scheint alltagssprachlich allgemein bekannt und einleuchtend zu sein. Dennoch ist dies nicht der Fall. Eine begriffliche Analyse auch mit einer Klarstellung der Substanz der verwendeten Termini scheint erforderlich. "Cyberwar", "InfoWar", "Netwar" sind neue Begrifflichkeiten, die scheinbar einen Paradigmenwechsel vom generellen politischen und militärischen Konzept des Krieges verkünden und in der strategischen Versuchsanstalt des experimentellen Weltuntergangs und seiner gleichzeitigen Verhinderung durch Gegenmaßnahmen, der US-amerikanischen RAND-Corporation, in den frühen neunziger Jahren entwickelt wurden. Diese Begriffe "Cyberwar", "InfoWar", "Netwar" finden sich bis heute noch in keinem Wörterbuch oder einem etymologischen Lexikon. Es sind nicht nur sprachliche, sondern auch kontextuelle und konstruktivistische Neuschöpfungen. In einer ersten Annäherung können diese Begriffe als "kybernetischer Krieg", "Informationskrieg" und "Krieg innerhalb von Computer-Netzwerken" übersetzt werden.

Der "reale" "Krieg" war im 19. und 20. Jahrhundert auf der nördlichen Halbkugel der Welt die Fortsetzung von nationalstaatlicher Machtpolitik mit Mitteln bewaffneter Auseinandersetzung zwischen diesen Nationalstaaten nach Maßgabe ihrer phantasierten territorialen, wirtschaftlichen und imperialen Reichsansprüche im Clausewitz’schen Sinn. Dies ist der Standpunkt des "politischen Realismus" der internationalen Beziehungen. Gleichzeitig waren kriegerische Auseinandersetzungen ein bis heute nicht vollständig dokumentiertes und aufgearbeitetes Kapitel der Unterwerfung und Ausbeutung der Peripherie im Weltsystem, des "Südens" und der "Kolonien", sowohl durch die industrialisiert-kapitalistische als auch durch die industrialisiert-kommunistische Welt.

"Krieg" zwischen Staaten der entwickelten Welt ist heutzutage unwahrscheinlich geworden, so heißt es. Sehr gewalttätige und mörderische Konflikte die etliche hunderttausend Menschenleben kosteten, haben dennoch in den letzten Jahren nicht aufgehört. Man denke nur an die Genozide in Afrika oder an die Konflikte in den Zerfallsprodukten von Jugoslawien oder der Sowjetunion. Die Konfliktursachen werden als "ethnische Konflikte" oder "neuer Tribalismus" zwischen "Warlords" oder gar als "Kampf der Kulturen" bezeichnet. Dies scheinen jedoch eher untaugliche intellektuelle Versuche zu sein, die dahinterstehenden Konfliktursachen zu beschreiben und zu erklären. Zum zusätzlichen Verstehen wären aber andere, weiterführende Schritte erforderlich. Mörderische Konflikte finden aber nach wie vor statt, auch wenn die Lehre des Völkerrechts und die Sprachregelung der internationalen Staatengemeinschaft andere Begrifflichkeiten dafür gefunden haben und der "Krieg" im klassischen Sinn, zumindest im "reichen Norden", ausgedient haben mag.

Das Konzept des Krieges hat sich in der Logik der militärischen Planungen bisher nicht verändert. "Si vis pax, para bellum" — "Wenn Du den Frieden willst, so rüste für den Krieg" lautet noch immer das schon aus den Antike stammende Motto aus der Sicht und Logik der militärischen Eliten. Die daraus resultierenden intellektuellen Dilemmata sind hinlänglich bekannt: Aus Rüstung und wahrgenommener Bedrohung erfolgt Gegenrüstung und gespiegelte Bedrohungswahrnehmung. Die Begrifflichkeit und Logik des Krieges hat sich durch die neuen Informations- und Kommunikations-technologien gleich entscheidend und bedeutend verändert, wie durch die Entwicklung und Einführung von nuklearen Waffen in der Mitte dieses Jahrhunderts.

C4I — "Command, Control, Communication, Computer und Intelligence" lautet ein militärisches Kürzel, das die Tragweite des Einsatzes von konventionellen Waffen auf einem "realen Schlachtfeld" des Krieges treffend auf den Punkt bringt. Von "Kampfwertsteigerung" ist dabei die Rede, womit der punktgenaue Einsatz von "intelligenter Munition", die ihr Ziel durch elektronische Leitsysteme selbständig finden kann, gemeint ist. War dieser Begriff von "Cyberwar" zunächst als Metapher gemeint, so ist daraus inzwischen ein operatives Konzept für den Einsatz auf einem Kriegsschauplatz entstanden. Der Golfkrieg der Alliierten gegen den Irak 1991 dient als Studienobjekt. "Cyberwar" ist gleichzeitig ein Sammelbegriff für die experimentelle Versuchsanstalt des neuen individuellen Soldaten in einer informationstechnisch verbundenen Kampfeinheit und auf Echtzeitkommunikation basierenden Soldaten, deren Kampfanzug einen Computer enthält und deren Waffen durch Datenfernübertragung ins Ziel gesteuert werden. "Cyberwar" wird mit den Vorteilen von "Blitzkrieg" gleichgesetzt, mit der Möglichkeit durch Datenfernübertragung und dem Einsatz von rechnergesteuerten Waffen einen "Vernichtungsvorteil" zu erzielen. "Gegenwärtig ist das US-Militär weltweit führend in der Planung und Vorbereitung des Cyberwar, sowohl offensiv als auch defensiv. […] Die USA sind das einzige Land der Welt, dem ein breites Arsenal zur Verfügung steht, um Cyberwar als eine attraktive und durchführbare Option erscheinen zu lassen", schreiben die beiden RAND-Autoren John Arquilla und David Ronfeldt.

"InfoWar" schließlich geht weit über das Konzept der Steuerung von Waffen in ihr Ziel hinaus. Dieser Begriff wird auch als "Strategic Information Warfare" beschrieben. Gemeint ist der Einsatz aller Mittel und Möglichkeiten der Informations- und Kommunikationstechnologien für Sabotage und Desinformation. So etwa die Manipulation des Bank- und Finanzwesen, fernmeldetechnischer Einrichtungen, Behörden der öffentlichen Verwaltung und natürlich des Militärs. Stellt man erst einmal die These auf, daß das moderne Leben im 20. Jahrhundert ohne den Einsatz von Computern und Telekommunikation nicht mehr möglich wäre, so ist es nur ein kleiner Schritt, um die "Verwundbarkeit" dieser Systeme durch gezielte Angriffe zu behaupten und dies als eminente Bedrohung darzustellen. Diese Bedrohung erscheint jedoch in Ermangelung anderer Bedrohungsbilder teilweise erfunden oder hysterisch hochgespielt zu sein. Heutzutage werden Bedrohungsbilder bereits extraterristisch ausgewählt — der mögliche Einschlag eines Asteroiden auf der Erde in ca. 30 Jahren — um damit die weitere Entwicklung von Kernwaffen, die zu dessen Sprengung im Weltall erforderlich wären, plausibel erscheinen zu lassen, ein Konzept, das auf das "Krieg-Der-Sterne-Projekt" der achtziger Jahre zurückgreift.

Der Einsatz von Computern für militärische Zwecke ist damit aber noch immer nicht voll erfaßt. Gegenwärtig betreiben die USA das sog. "Stockpile Stewardship Program", für das das US-Energieministerium am 3. Februar 1998 einen Auftrag an IBM vergeben hat, um die weltschnellsten Supercomputer (100 Teraflops) zu entwickeln. Diese werden von den US-Kernwaffenentwicklungslabors betrieben und können möglicherweise zur Weiterentwicklung oder gar zur Neuentwicklung von Kernwaffen verwendet werden, ohne daß dazu dann ein vollständiger Kernwaffentest erforderlich wäre, der nach dem gegenwärtigen "Vollständigen Teststopp-Vertrag" nicht mehr erlaubt wäre. Die militärischen Wurzeln der Computer-Technik-Entwicklung finden sich überall im militärischen Bereich: Der ENIAC, einer der ersten primitiven elektronischen Rechner wurde für die Berechnung der ersten Thermonuklearwaffen entwickelt, die Dezentralisierung des Internet, wie wir es heute kennen, basiert auf den Anforderungen des US-Militärs, auch nach einem Kernwaffenschlag gegen ihr Territorium dezentrale "überlebensfähige" Kommunikationseinrichtungen zur Verfügung zu haben. Womit sich der Kreis wieder schließt und man sowohl für die Entwicklung der Rechenleistung von Computern als auch für die Meilensteine des Internet Brechts Ausspruch, der Krieg sei der Vater aller Dinge, zustimmen muß.

So verwundert es zu guter Letzt nicht, wenn "der Cyberspace", jener für viele der politischen und militärischen Eilten der Welt unbekannte Raum der modernen Informationsgesellschaft, generell als Bedrohung wahrgenommen wird und aus diesem Raum auch militärische Angriffe auf die Informationsinfrastruktur erwartet werden. Wieviel dies mehr mit "Science", mit "Fiction" oder mit guter Public Relation zu tun hat, wird ein zentraler Gegenstand des diesjährigen Ars Electronica Festivals sein.