ERICH SCHWEIGHOFER[1]

Konflikt im Cyberspace: Wo bleibt das Völkerrecht?

Die Informationsgesellschaft bringt auch eine neue Konfliktform: die informationelle Kriegsführung (*Information Warfare*).[2] Grundlage der informationellen Kriegsführung ist die unbestreitbare Tatsache, daß Information und Informationstechnologien zunehmend bedeutend für die nationale Sicherheit im allgemeinen und für Kriegsführung im besonderen sind. Jene Staaten, die die Techniken der informationellen Kriegsführung beherrschen, haben einen wesentlichen Vorteil über Staaten, die hier im Hindertreffen sind.

Die zentrale Bedeutung von Information in der Kriegsführung ist allgemein anerkannt. Die weitgehende Steuerung von kriegerischen Handlungen sowie zivilen Versorgungssystemen durch Informationssysteme hat jedoch das Potential exponentiell erweitert. Die digitale Informationsstruktur eines Staates kann durch militärische Hacker lahmgelegt werden: Elementare Bereiche wie Telekommunikation, Verkehr, Wirtschaft (insbes Banken und Versicherungen) und staatliche Verwaltung funktionieren dann nicht mehr oder nur sehr ineffizient. Staaten können ohne merkliche Zerstörung lahmgelegt und nach erfolger Kapitulation sofort wieder *in Betrieb* genommen werden.

Die informationelle Kriegsführung wird als Summe der Maßnahmen zur Erzielung von Informationsüberlegenheit zum Zwecke der Unterstützung nationaler Sicherheitsstrategien gesehen.[3] Gegnerische Informationssysteme sollen lahmgelegt, eigene Informationssysteme bestmöglichst geschützt werden. Informationelle Kriegsführung betrifft die Chancen und Risiken, die in der steigenden Abhängigkeit von Information liegen.

Für die Vereinigten Staaten als der vorherrschenden Informationsgesellschaft dieser Erde stellt sich die Herausforderung, die militärische Vorherrschaft auszubauen oder eine beträchtliche Schwächung trotz der Stärke in anderen militärischen Sektoren zu erleiden.

Auch ein Kleinstaat wie Österreich muß sich dieser Frage stellen, um zu wissen, inwieweit die eigene militärische Stärke ausgebaut bzw eine Verwundbarkeit gegenüber informationeller Kriegsführung gegeben ist.

---

[1] Universitätsdozent, Institut für Völkerrecht und Internationale Beziehungen, Universität Wien; Leiter der dortigen Arbeitsgruppe Rechtsinformatik. Da der Zweck dieses Beitrag eine kurze Einführung in die Problematik ist, wurden die Fußnoten auf ein Minimum beschränkt.

[2] Eine umfassende Information mit Stand Juli 1996 über die informationelle Kriegsführung bietet die Homepage des INSTITUTE FOR THE ADVANCED STUDY OF INFORMATION WARFARE (IASIW): http://www.psycom.net/iwar.1.html. Der Zweck des IASIW (einer virtuellen nicht-zwischenstaatlichen Internationalen Organisation) *"is to facilitate an understanding of information warfare with reference to both military and civilian life"*.

Eine gute Einführung mit Berücksichtigung der rechtlichen Problematik bieten: J. J. Arquilla und D. F. Ronfeldt, Cyber War is Coming, in: Comparative Strategy, Vol 12 (1993), 141-165 (Ein Auszug ist verfügbar über: http://www.rand.org/publications/RRR/RRR.fall95/cyber/cyberwar.html), N. Barrett, Digital Crime, Policing the Cybernation, 1997: Kapitel 6: From digital crime to digital conflict, 167-188, S. E. Goodman, War, Information Technologies, and International Asymmetries, in: Communications of the ACM, Vol. 39, No. 12 (1996), 11-15, M. Libicki, What is Information Warfare?, Institute for National Strategic Studies, http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html.

Einen Einstieg bieten auch die Beiträge im Time Magazine, 21.8.95 (verfügbar über: http://ei.cs.vt.edu/~cs3604/fall.95/Hacking/Cyberwar.html) sowie im The Economist, 13.1.1996, 83-84.

[3] Diese Definition stammt von E. Paige, dem Director of Information Warfare des UN-Verteidigungsministeriums (zitiert in Barrett, aaO, 168). Das IASIW bietet folgende Definition: *"Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy, an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."*

Kaum Beachtung hat bisher die völkerrechtliche Seite der informationellen Kriegsführung erhalten. Da die humanste Form der informationellen Kriegsführung, die Simulation des Krieges, (leider) keine Aussicht auf Verwirklichung hat, werden in diesem Beitrag Vorüberlegungungen hiezu angestellt, wie die informationelle Kriegsführung in das System des Völkerrechts einzuordnen ist.

Arten der informationellen Kriegsführung

Für die weitere Untersuchung ist es hilfreich, die Ausprägungen der informationellen Kriegsführung näher zu klassifizieren.

Die sehr umfassende Untersuchung von Libicki[4] zählt sieben Arten der informationellen Kriegsführung auf: Kriegsführung gegen Kommando und Kontrolle der Streitkräfte *(Command and Control Warfare, C2 Warfare, Kopf* und Informationsstränge des Gegners sollen lahmgelegt werden), Aufklärungskriegsführung (Design, Schutz oder Zerstörung von Systemen, mit denen die notwendige Information zur Dominanz des Kampfplatzes erlangt wird), elektronische Kriegsführung (elektronische oder kryptographische Techniken), psychologische Kriegsführung (Versuch der Beeinflussung von Freunden, Feinden und Neutralen mit Information), Hackerkriegsführung (Einbruch im fremde Computersysteme mit Datendiebstahl, Datenmanipulation oder Datenlöschung, Einsatz von Computerviren, *digitalen Bomben*, trojanischen Pferden oder *Schnüfflern*[5]), Wirtschaftsinformationskriegsführung (Blockierung oder Kanalisierung von Information zur Erzielung wirtschaftlicher Dominanz) und die futuristischen Szenarien der Kriegsführung im Cyberspace.

Gemeinsam ist allen diesen Ausprägungen, das sie in irgendeiner Weise mit Information zu tun haben. Ansonsten sind die verschiedenen Formen sehr unterschiedlich.

Szenarien der informationellen Kriegsführung

Der Szenarien gibt es viele. In diesem Beitrag sollen vor allem jene Szenarien vorgestellt werden, die für die völkerrechtliche Beurteilung wichtig sind.

Szenario 1: Der digitale Angriff

Von einem sicheren Bunker der Supermacht wird der Krieg gegen einen Tyrannen eines fremden Staates ausgetragen. Keine Truppen, keine Kriegsschiffe und keine Luftstreitkräfte werden eingesetzt. Stattdessen werden die moderen Kampfmittel eingesetzt, die der Welt der Mäuse, Monitoren und Tastaturen entstammen.

Computerviren werden in das Telefonsystem des Gegners eingeschleust, womit dieses zusammenbricht. *Digitale Bomben* zerstören zu vorbestimmten Zeiten die Kontrollsysteme von Eisenbahnen und militärischen Konvois. Durch den Einbruch in das Computersystem des Verteidungsministeriums erhalten kommandierende Offiziere gefälschte Befehle, womit deren Truppen ineffektiv werden. Über Rundfunk- und Fernsehsendungen wird massive Propaganda gegen den Gegner ausgeübt. Die Bevölkerung lehnt sich gegen den Tyrannen auf, der das Land verlassen muß. Beim Versuch, die für solche Fälle sichergestellten Millionen auf einem

---

[4] M. Libicki, What is Information Warfare?, aaO.

[5] In allen Fällen handelt es sich im Computerprogramme. Computerviren “befallen” fremde Programme und manipulieren diese. Dies kann von harmlosen Geräuschen bis zur Systemzerstörung gehen. Digitale Bomben zerstören Computerprogramme und Daten. Trojanische Pferde legen Abwehrmaßnahmen lahm. *Schnüffler* sitzen in einem fremden Netzwerk und sammeln Paßwörter und andere wichtige Informationen.

schweizerischen Bankkonto zu kassieren, muß der Ex-Diktator feststellen, daß das Bankkonto bereits geleert wurde.[6]

Kein militärischer Gewalteinsatz, ineffektive, aber nicht zerstörte Informationssysteme, aber trotzdem ein Gegner, der zu keinem Widerstand mehr fähig ist. Auf dem ersten Blick eine hervorragende Chance für eine Supermacht der informationellen Kriegsführung, Staaten beliebig ohne Risiken für eigene Truppen lahmzulegen.

Szenario 2: Angriff auch mit informationeller Kriegsführung

In einem Konflikt wird die Kriegsführung gegen Kommando und Kontrolle der Streitkräfte forsiert. Die gegnerischen Computer werden von Hackern geknackt und die notwendigen Programme und Daten zur strategischen wie taktischen Armeeführung gelöscht. Weiters werden die Kommunikationsleitungen zwischen Zentrale und Truppenverbänden gekappt. *Kopf* und *Nervenzentrum* des Gegners ist nunmehr lahmgelegt. Die militärischen Verbände können weitgehend ungehindert vorrücken, weil die Aufklärung ebenfalls vollkommen versagt.

Szenario 3: Terror mit informationeller Kriegsführung

Der Bunker steht nicht im Kommandozentrum der Supermacht, sondern in einem schäbigen Keller. Ein begabter Hacker *knackt* lebenswichtige Computersysteme eines Staates. Nach einiger Zeit beschließt er, dieses Wissen praktisch zu nutzen. Um seine Fähigkeiten zu demonstrieren, werden in einem Zeitraum von drei Monaten wichtige Computersysteme für einige Tage lahmgelegt. Danach möchte der Hacker auch Geld verdienen. Er stellt an die Regierung das Ultimatum mit sehr hoher Lösegeldforderung. Falls dies nicht geschehe, werde die Informationsinfrastruktur sofort lahmgelegt. Da der Staat nicht zahlt, werden nach kurzer Zeit alle wichtigen Computer stillgelegt. Der Terrorist hat die erste Runde im Cyberwar gewonnen.

Vorbemerkungen zur völkerrechtlichen Relevanz des Cyberwars

Aus der Sicht des Völkerrechts sind folgende Punkte besonders interessant:

- Voraussetzungen des Cyberwars sind eine globale Vernetzung sowie weitgehend ungehindete grenzüberschreitende Datenflüsse. Diese stehen unter einem Souveränitätsvorbehalt der Staaten, und zwar sowohl hinsichtlich der Aufrechterhaltung der Netzstruktur als auch des Menschenrechts auf freie Meinungsäußerung.
- Das Kampfmittel der Daten ist unscheinbar und ohne Einwirkung auf Computersysteme ungefährlich. Da Daten vornehmlich Informationen zum Meinungsaustausch sind, werden diese durch das Recht auf freie Meinungsäußerung geschützt.
- Die Zuordnung eines digitalen Angriffs zu einem Staat wird wesentlich erschwert, weil neben dem Staat auch Aufständige, Terroristen oder Saboteure in Frage kommen. Bei der zunehmenden Vernetzung spielt der Ausgangsort nur eine geringe Rolle. Dieser kann im Dschungel, in der Sahara oder in der Nachbarschaft des Angriffsziels liegen.
- Die Satzung der Vereinten Nationen (SVN) ist eher zurückhaltend in der Anerkennung neuer Formen des bewaffneten Angriffs.
- Im Humanitätsrecht sind Telekommunikationseinrichtungen nicht besonders geschützt, sondern werden als legitimes Kampfziel angesehen.

---

[6] Dieses Beispiel wurde folgendem Beitrag im Time Magazine vom 21.8.95, aaO, entnommen: D. W. Washington, Onword Cyber Soldiers, The U.S. may soon wage war by mouse, keyboard and computer virus. But it is vulnerable to the same attacks.

Daten: Unsichtbare Kampfmittel im Heuhaufen

Die Kampfmittel sind Daten und als solche nur dadurch gefährlich, weil sie potentionell als Programme andere Programme zur Steuerung vielfältiger Aufgaben lahmlegen oder zerstören können. Daten wirken als Kampfmittel nur indirekt, niemals direkt. Die Unterscheidung zwischen harmlosem Datentransport und *digitaler Bomben* ist äußerst schwierig. Die Entdeckung ist bei der zunehmenden Vernetzung sowie dem steigenden Datenaustausch zwischen den Staaten fast unmöglich.

Grenzüberschreitende Datenflüsse und staatliche Souveränität

Im Rahmen des ITU-Vertragswerks[7] gestehen die Mitglieder jedermann das Recht zu, die öffentlichen internationalen Telekommunikationsdienste zu nutzen.[8] Die Staaten haben jedoch einen Souveränitätsvorbehalt. Kommunikation kann untersagt werden, wenn sie gegen die Gesetze, die öffentliche Ordnung oder die guten Sitten verstößt. Dieser Souveränitätsvorbehalt ist beim derzeitigen Stand der Vernetzung und des Umfangs des grenzüberschreitenden Datenverkehrs praktisch illusorisch. Die Diskussion um die erlaubte Verschlüsselung im Internet beweist die Grenzen staatlicher Einwirkungsmöglichkeit sowie die zunehmende staatliche Sensibilität für diese Problematik.

Andererseits wird das Recht auf grenzüberschreitenden Datenaustausch als Ausprägung des Rechts auf freie Meinungsäußerung und somit als Menschenrecht gesehen, das aber auch hier unter Souveränitätsvorbehalt steht. Der Staat kann aus Gründen des Schutzes der nationalen Sicherheit, der öffentlichen Ordnung (ordre public), der Volksgesundheit oder der öffentlichen Sittlichkeit[9] (Art 19 UN-Menschenrechtspakt II, BGBl 1978/591, Art 10 EMRK, BGBl 1958/210 idgF) gegen den grenzüberschreitenden Datenaustausch vergehen.

Werden *digitale Bomben* und Computerviren für Störaktionen gegen die Informationsinfrastruktur eines Staates eingesetzt, ist eine Verletzung der staatlichen Souveränität sowie des Interventionsverbots gegeben.[10] Hiefür ist aber eine Zurechnung zu einem Staat erforderlich, was praktisch oft nur sehr schwer nachzuweisen ist.

"Nur Cyberwar" oder Cyberwar als Begleiterscheinung des bewaffneten Konflikts

Bei der völkerrechtlichen Beurteilung muß unterschieden werden, ob der Angriff nur mit den neuen Formen der informationellen Kriegsführung erfolgt oder nicht. Diese Formen werden unter dem Begriff des Cyberwars zusammengefaßt. Obwohl dieser Begriff etwas unscharf ist, wird er wegen dessen bildlicher Aussagekraft beibehalten. Als Formen dieser Kriegsführung kommen insbes der Hackerkrieg sowie der Wirtschaftsinformationskrieg in Betracht. Wesentliches Merkmal ist die Absicht, die digitale Informationsinfrastruktur eines Landes zu schädigen oder auszuschalten. Einbruch in fremde Computersysteme, Viren, *digitale Bomben* und Desinformation sind die Werkzeuge dieser Form der Kriegsführung. Diese Form entspricht

---

[7] Letzte Fassung: Internationaler Fernmeldevertrag (Genf 1992), mit Änderungen der Konferenz der Regierungsbevollmächtigten (Kyoto 1994). Informationen und Materalien zur ITU sind verfügbar: http://www.itu.int. Internationaler Fernmeldevertrag (Nairobi 1982): BGBl 1989/593.

[8] Vgl dazu grundlegend J. Frowein, Das Problem des grenzüberschreitenden Informationsflusses und des "domaine réservé", in: Berichte der Deutschen Gesellschaft für Völkerrecht, Heft 19, Karlsruhe 1979, 3-38.

[9] Diese Beschreibung wurde dem UN-Menschenrechtspakt II entnommen, weil sie knapper die Einschränkungsmöglichkeit umschreibt als Art 10 Abs 2 EMRK.

[10] Vgl dazu A. Verdross und B. Simma, Universelles Völkerrecht, Theorie und Praxis, Dritte Auflage, Berlin 1984, Rz 456 ff und 490 ff, H. Neuhold, Die Grundregeln der zwischenstaatlichen Beziehungen, in: H. Neuhold, W. Hummer und Ch. Schreuer, Österreichisches Handbuch des Völkerrechts, Band 1: Textteil, 2. Aufl, Wien 1991, Rz 1636 ff.

weitgehend den Szenarien 1 (wenn es der Staat selbst macht) und 3 (wenn es Privatpersonen machen).

Der Terrorismus über die Grenze (Szenario 3) ist von den Staaten im Rahmen ihrer Jurisdiktion zu bekämpfen. Das gleiche gilt für Hacker im Staatsgebiet des Staates selbst. Da die Bestrafung nur möglich ist, wenn man dem Täter auch habhaft werden kann, muß für die Zukunft überlegt werden, die Ahndung durch international vereinheitlichte Straftatbestände zu erleichtern sowie eine Auslieferung oder Aburteilung vorzusehen.

Die anderen Formen der informationellen Kriegsführung (Szenario 2) sind nicht neu, werden aber in ihrer Bedeutung durch die Möglichkeiten der Informationsgesellschaft wesentlich verstärkt. Hiebei handelt es sich um Kriegsführung gegen Kommando und Kontrolle, Kriegsführung gegen die Aufklärung, elektronische Kriegsführung und psychologische Kriegsführung. Diese Formen der Kriegsführung werden vornehmlich in einem bestehenden bewaffneten Konflikt eingesetzt, womit bei Vornahme der notwendigen begrifflichen Anpassungen eine ausreichende Regelung im gegenwärtigen Kriegs- und Humanitätsrecht gegeben ist.

Ist der Cyberwar als bewaffneter Konflikt anzusehen?

Unter die Eingliederung als bewaffneter Konflikt knüpft das Völkerrecht eine Reihe von Folgen: Anwendbarkeit des Gewaltverbots (Art 2 Z 4 der Satzung der Vereinten Nationen [SVN]), Zulässigkeit des Selbstverteidigungsrechts (Art 51 SVN) sowie die notwendige Beachtung des Humanitätsrechts: Genfer Abkommen 1949 (BGBl 1953/155) sowie Zusatzprotokolle 1977 (BGBl 1982/527).[11]

Neben dem bewaffneten Konflikt mit militärischen Machtmitteln gibt es unterhalb die sog *kleine Gewalt*[12] wie Grenzzwischenfälle oder Einflüge durch Militärluftfahrzeuge. Diese Gewaltakte unterliegen vornehmlich der Jurisdiktion des jeweiligen Staates. Militärische Abwehrmaßnahmen gegen diese sog *kleine Gewalt* sind zulässig, wenn keine andere Möglichkeit der Abwehr besteht und die Maßnahmen verhältnismäßig bleiben. Die Maßnahmen hiezu sind vornehmlich jene zur Sicherung der Datensicherheit, dh defensiver Art. Das Abschalten der Telekommunikationsleitungen kommt bei deren Bedeutung in der Informationsgesellschaft nur im echten Konfliktfall in Frage, wobei beim derzeitigen Stand der Vernetzung kaum alle Leitungen mehr gekappt werden können. Gegen Hacker im Staatsgebiet hilft diese Maßnahme wiederum nicht. Gegenmaßnahmen gegen Hacker sind zulässig, wenn das Gebot der Verhältnismäßigkeit eingehalten wird, wodurch letztendlich nur gleichartige Maßnahmen gegen dessen Computersystem zulässig sind.

Die Einordnung von Computerviren oder *digitalen Bomben* als Kampfmittel macht gewisse Schwierigkeiten. Bites und Bytes sind vorerst harmlos und wirkungslos. Erst in Verbindung mit einer Hardware und Software entfalten sie ihre mögliche zerstörerische Wirkung wie zum Beispiel eine fehlgeleitete Steuerung eines Staudammes oder eine Lahmlegung wichtiger

---

[11] Vgl zum Gewaltverbot und zur Selbstverteidung: Verdross und Simma, aaO, Rz 467 ff, Neuhold in H. Neuhold, W. Hummer und Ch. Schreuer, aaO, Rz 1560 ff.

Vgl zum Humanitätsrecht: M. Bothe, K. J. Partsch und W. A. Solf, New Rules for Victimes of Armed Conflicts, Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949, The Hague 1982, E. Chadwick, Self-determination, Terrorism and the International Humanitarian Law of Armed Conflict, The Hague 1996, E. David, Principes de droit des conflits armés, Bruxelles 1994, I. Detter De Lupis, The Law of War, Cambridge 1987, Fleck, Handbuch des humanitären Völkerrechts in bewaffneten Konflikten, München 1994, K. Zemanek, Das Kriegs- und Humanitätsrecht, in: H. Neuhold, W. Hummer und Ch. Schreuer, aaO, Rz 2403 ff.

[12] Verdross und Simma, aaO, Rz 472.

Verkehrsleitsysteme. Sehr wichtig ist es auch sich vor Augen zu halten, daß zunehmend Computerprogramme Aufgaben übernehmen, die früher von Personen oder mit mechanisch-elektrischen Hilfsmitteln gelöst worden sind. Die Wirkung einer Löschung oder Störung der Software ist die gleiche, wie wenn die Personen getötet oder die Anlagen zerstört werden.

Das Humanitätsrecht kennt keine Begriffserklärung des bewaffneten Konflikts. Einigkeit besteht aber über zwei wesentliche Kriterien: Das Vorliegen von Gewaltakten sowie eine ausreichende Intensität dieser.[13] Militärische Kampfmittel sind im Humanitätsrecht keineswegs definiert, sondern nur nach bestimmten Kriterien verboten. Daher können Kampfmittel mit indirekter Wirkung darunter subsumiert werden, weil mit ihnen die gleichen Konfliktziele erreicht werden können. Es macht keinen Unterschied, ob der Computer physisch zerstört oder durch die Löschung der Software unbrauchbar gemacht wird. Die Nutzung der Anlage wird für bestimmte Zeit oder auf Dauer verhindert. Das Argument der rascheren Wiederherstellung ist nicht wirklich überzeugend, weil dies ja auch bei physischen Sachen der Fall sein kann, aber trotzdem von Gewaltanwendung gesprochen wird.

Zur Frage der notwendigen Intensität des Einsatzes von Waffengewalt sind nur Anhaltspunkte aufgrund der Praxis zu geben. So reicht beispielsweise der Abschuß eines Militärflugzeuges nicht für die Entstehung eines bewaffneten Konflikts aus, sondern die Kampfhandlungen müssen eine Intensität erreichen, die die isolierter Zwischenfälle übersteigt. Für den Cyberwar bedeutet dies, daß kleine Störaktionen *nur* eine Verletzung der territorialen Souveränität sowie des Interventionsverbots darstellen, nicht aber das Gewaltverbot der SVN verletzen. Mögliche Abwehrmaßnahmen sind Datensicherheit sowie reziproke Handlungen gegen das Computersystem des Angreifers unter Beachtung der Proportionalität.

Überschreiten die Störaktionen diese Schwelle (Szenario 1), so liegt eine Verletzung des Gewaltverbots vor. Die wirtschaftliche und militärische Macht eines Staates wird fortlaufend durch Störaktionen von einem anderen Staat gestört. Neben der Intensität der Gewaltakte ist insbes auch auf die Intention des Angreifers abzustellen. Weiters ist zu beachten , daß diese Akte in der Regel Prolog einer militärischen Aktion sein werden. Die Problematik ähnelt jener der Verteidigung gegen einen unmittelbar bevorstehenden Angriff[14], hat aber den wichtigen Unterschied, daß bereits Kampfmittel in Form von Computerviren oder *digitalen Bomben* eingesetzt werden.

Ein weiteres wichtiges Problem ist die Zuordnung der Angriffe. Digitale Angriffe können von Staaten, Aufständigen, Terroristen oder von Hackern im Staatsgebiet des jeweiligen Staates durchgeführt werden. Die “Kombattanten” tragen keine Abzeichen und Waffen, sondern operieren anonym. Die Zuordnung kann erst nach umfangreicher Recherche erfolgen. Das macht die Anwendung des Gewaltverbots schwierig, weil nicht leicht ein Staat als Angreifer festgestellt werden kann. Eine Zurechnung der Hacker zum Staat wegen Verletzung einer Verhinderungspflicht findet keine Grundlage im Völkerrecht.

Zusammenfassend kann gesagt werden, daß bei derzeitigem Stand des Völkerrechts dem Selbstschutz der Informationssysteme des Staates höchste Priorität bekommen muß. Der Schutz der territorialen Integrität, das Interventionsverbot und das Gewaltverbot schaffen zwar eine Völkerrechtsverletzung. Dazu muß aber dem Staat entsprechendes Handeln nachgewiesen werden, was praktisch sehr schwierig sein kann. Da der Staat im Cyberwar mit privaten Hackern und Terroristen Waffengleichheit besitzt, können auch Private hier ihren Krieg führen. Gegenmaßnahmen gegen Hacker sind zulässig, wenn das Gebot der Verhältnismäßigkeit

---

[13] Detter De Lupius, aaO, 24, E. David, aaO, 94, Ch. Greenwood, Anwendungsbereich des humanitären Völkerrechts, in: D. Fleck, aaO, 35 ff.

[14] Vgl zu dieser alten Streitfrage des Völkerrechts Verdross und Simma, aaO, Rz 470 f.

eingehalten wird, wodurch letztendlich nur gleichartige Maßnahmen gegen dessen Computersystem zulässig sind. Das Abschalten der Telekommunikationsleitungen ist unzweckmäßig und hilft nicht gegen Hacker im Staatsgebiet selbst. Staatliche Eingriffsakte wie Beschlagnahme der Computerausrüstung, Abschaltung der Telekommunikationsleitung des Hackers, Inhaftnahme etc bedürfen der Zustimmung des jeweiligen Gebietsstaates. Kommandoaktionen auf fremden Staatsgebiet gegen Hacker sind unzulässig.

Zum Abschluß muß noch auf einen interessanten Punkt aufmerksam gemacht werden. Der Schutz des Staates erfolgt hier nicht mehr an der Grenze, sondern beim Zugang zum jeweiligen Computersystem. Diese Verlagerung ist typisch für die vernetzte Struktur der heutigen Staatengemeinschaft und ist eine notwendige Voraussetzung, um Privatpersonen die weitgehend ungehinderte Nutzung dieses Mediums über die Staatsgrenze zu ermöglichen.

Humanitätsrecht

Im Cyberwar mit ausreichender Intensität findet das Humanitätsrecht Anwendung.

Zentrale Regel des Kriegs- und Humanitätsrechts ist, daß die Parteien eines bewaffneten Konflitks kein unbeschränktes Recht in der Wahl der Mittel (Art 22 Landkriegordnung) und Methoden (Art 35 Abs 1 I. Zusatzprotokoll zu den Genfer Abkommen) haben.

Der Cyberwar kann sehr weitreichende Auswirkungen auf Kombattanten, militärische Ziele, Zivilpersonen, zivile Objekte und die Umwelt haben. Die Kampfmittel – Daten – wirken nur indirekt. Die Zerstörung von Computersystemen durch *digitale Bomben* kann bedeuten, daß Züge entgleisen oder im schlimmsten Fall Kernkraftwerke explodieren. Nach dem Humanitätsrecht dürfen weder überflüssige Verletzungen oder unnötige Leiden hervorgerufen (Art 23 lit e Landkriegsordnung, Art 35 Abs 2 I. Zusatzprotokoll), ausgedehnte, langanhaltende und schwere Schäden der natürlichen Umwelt verursacht (Art 35 Abs 3 und 55 Abs 1 I. Zusatzprotokoll, ENMOD-Konvention), militärische Ziele und Zivilpersonen oder zivile Objekte unterschiedlos geschädigt (Art 51 Abs 4 und 5 I. Zusatzprotokoll) oder Einrichtungen, die gefährliche Kräfte enthalten, angegriffen werden (Art 56 I. Zusatzprotokoll).[15]

Unstreitig ist, daß Computersysteme zur Kontrolle von Staudämmen, Deichen oder Kernkraftwerken nicht angegriffen werden dürfen (Art 56 I. Zusatzprotokoll). Angriffe gegen Computersysteme des Zivilschutzes, der Feuerwehr, der Rettung oder von Krankenhäusern sind ebenfalls untersagt.

Ansonsten ist eine schwierige Abwägung hinsichtlich des Verbots der unterschiedslosen Kampfführung vorzunehmen. Computersysteme und Telekommunikationseinrichtungen sind einerseits Wirtschaftsziele, weil sie wirksam zu militärischen Handlungen beitragen.[16] Nach einer Liste des IKRK von 1956 wurden darunter unter anderem Telefon- und Telegraphenverbindungen angeführt, womit bei systemimmanter Interpretation das gesamte Informations- und Telekommunikationssystem umfaßt wird. Die Praxis der Kuwaitaktion 1991 beweist, daß Telekommunikationsnetze eindeutig ein militärisches Ziel darstellen, weil für eine Lahmlegung der Führungs- und Kommunikationsstruktur der gegnerischen Streitkräfte eine Totalzerstörung der Telekommunikationsnetze notwendig ist. Andererseits ist die nationale Informationsinfrastruktur von elementarer Bedeutung für die Zivilbevölkerung. Die heutige Informationsgesellschaft kann nicht von heute auf morgen auf moderne Kommunikationseinrichtungen verzichten. Daher sollte überlegt werden, ob das Verbot der unterschiedslosen Kampfführung nicht auch auf die grundlegende Informationsinfrastruktur der Zivilbevölkerung Anwendung

---

[15] St. Oeter, Kampfmittel und Kampfmethoden, 89 ff, in: D. Fleck, aaO, 126 ff, David, aaO, 232 ff, M. Bothe, K. J. Partsch und W. A. Solf, aaO, 296 ff, I. Detter de Lupis, aaO, 241 ff.

[16] St. Oeter, Kampfmittel und Kampfmethoden, in: D. Fleck, aaO, 126 ff (132).

finden soll. Derzeit werden eher nur Maßnahmen umfaßt, die dem Schonungsgebot der Zivilbevölkerung zuwiderlaufen. Ein Beispiel hiefür wäre ein Eindringen in das U-Bahn-Leitsystem, um Züge entgleisen oder zusammenstoßen zu lassen. Für eine Ausweitung des Begriffs spricht, daß eine Lahmlegung der nationalen Informationsinfrastruktur unterschiedslos gegen militärische Ziele und Zivilpersonen oder zivile Objekte wirkt.

Für die Zukunft wäre es zweckmäßig, hier eine Klarstellung in Form einer eigenen Konvention nach dem Vorbild der ENMOD-Konvention zu schaffen. Hiemit sollte sichergestellt werden, daß zumindest der Kern des zivilen Informationssystems nicht als legitimes Kampfziel anzusehen werden darf.

Schlußfolgerungen und Ausblick

Bei derzeitigen Stand des Völkerrechts kann das Gebot an die Staaten nur lauten: Datensicherheit ist unbedingt notwendig, um sich gegen die Angriffe von Computerviren oder *digitalen Bomben* zu schützen. Der Angreifer können Staaten, Aufständige, Terroristen oder Saboteure sein, wobei die Zuordnung schwierig ist. Der Einstieg in diesem Cyberwar ist von den Kosten her sehr gering und stellt eine weitere Gefahr dar.

Die Satzung der Vereinten Nationen sowie das Humanitätsrechts sind in interpretativer Hinsicht anzupassen. Computerviren und *digitale Bomben* sind Kampfmittel, weil ihre Wirkung genauso verherrend sein kann wie die von konventionellen Bomben. Hier ist ein Umdenkprozeß notwendig, weil nunmehr viele Dinge genauso effizient mit Hard- und Software durchgeführt werden, wie dies früher Menschen oder Maschinen gemacht haben.

Die Zielsetzung müßte sein, daß die grundlegende nationale Informationsinfrastruktur eines Staates kein militärisches Ziel sein darf, soweit sie insbes auch zivilen Zwecken dient. Neben einer begrifflichen Klarstellung im Humanitätsrecht sollte die Ausarbeitung einer Konvention wie der ENMOD überlegt werden, um die notwendige Einschränkung der militärischen Ziele hinsichtlich der nationalen Informationsinfrastruktur vorzunehmen.