Uwe Nerlich

Strategische Dimensionen der Informationskriegführung

Informationskriegführung ist so alt wie die Kriegskunst selbst. Vor 2.500 Jahren rechnete Sun Tzu Informationskriegführung schon zu den Elementen militärischer Strategie. Mit den technischen Entwicklungen, die die Kriegskunst immer neu verändert haben, haben sich pari passu auch die Möglichkeiten der Informationskriegführung verändert. Dabei gab es - wie in anderen Dimensionen der Kriegführung - immer wieder auch zeitweilige taktische, operative oder sogar strategische, also kriegsentscheidende Vorteile für den, der technische Möglichkeiten zuerst umgesetzt hat.

Solche Vorteile wurden durchweg, ganz im Sinne von Sun Tzu, im Zusammenhang einer Strategie wirksam. Sun Tzu hatte bereits die optimale Strategie formuliert, von der die heutigen Protagonisten der strategischen Informationskriegführung sprechen: daß derjenige, der wirksame Vorbereitungen getroffen hat, gewinnen könne, ohne überhaupt kämpfen zu müssen. Allerdings wird heute eine solche "Entscheidung ohne einen Schuß" als Folge wirksamer Anwendung von Informationstechnologie und u. U. entsprechender organisatorischer Vorkehrungen, weniger als Resultat einer militärischen Strategie gesehen.

1. Die Debatte in den USA

In den USA hat das Thema der Informationskriegführung (IKF) in den letzten Jahren eine zunehmend zentrale Bedeutung erlangt. Dabei stehen neben der Analyse der technisch möglichen Angriffsoptionen vor allem Fragen der Verwundbarkeit nationaler ziviler wie militärischer Infrastrukturen gegenüber IKF-Angriffen im Vordergrund. Ende Oktober 1997 wurde der Bericht der vom amerikanischen Präsidenten eingesetzten "Kommission zum Schutz kritischer Infrastrukturen" vorgelegt.[1] Die Kommission hat fünf Sektoren untersucht: 1. Information und Kommunikation, 2. Banken und Finanzen, 3. Energie einschließlich Strom, Öl und Gas, 4. Verteilungssysteme (Transport usw.) sowie 5. vitale Hilfsdienste. Dabei wurde die Verwundbarkeit gegenüber einem breiten Spektrum von Störungen berücksichtigt: von Hackern bis zu strategischen Informationsoperationen. Das Fazit der Kommission: Es gibt gegenwärtig noch keine Anzeichen für Störungen mit dem Ausmaß einer nationalen Katastrophe (trotz einer ständig steigenden Zahl von Störungen). Aber die Verwundbarkeiten nehmen stetig zu, während die Kosten für wirksame Angriffe sich laufend verringern. Es sei also nötig, die kritischen Infrastrukturen zu schützen, "bevor der Sturm angekommen ist, nicht hinterher. Die Katastrophe abzuwarten ist ebenso kostspielig wie unverantwortlich."[2] In diesem Sinne hat die amerikanische Administration neue Grundlagen geschaffen: mit der Entscheidung (und dem Weißbuch) zum Schutz kritischer Infrastrukturen und darauf basierenden organisatorischen Neuerungen und Budgetzuweisungen.[3]

---

1 Critical Foundations. Protecting America's Infrastructure. The Report of the President's Commission on Critical Infrastructure Protection, Washington, DC, October 1997.

2 R. Tom Marsh (Chairman der Presidential Commission).

3 Siehe die Presidential Decision Directive PDD 63. Dieses Dokument hat einen inneren Zusammenhang mit der PDD 62, die den Schutz vor Angriffen mit B- und C-Kampfmitteln stärken soll. Aggressive Informationsoperationen haben mit B- und C-Angriffen in einer erheblichen Einsatzbreite gemein, daß sie (u.U. strategische) Lähmungs- statt Zerstörungsoptionen darstellen. Sie eignen sich deshalb besonders zu terroristischen Aktionen im großen Maßstab.

2. Die fehlende Debatte in Europa

In Europa sind die möglichen Gefährdungen nationaler Infrastrukturen und der Auswirkungen auf die militärische Sicherheit bisher noch wenig ins politische Bewußtsein getreten. Die Abhängigkeit dieser Infrastrukturen von zunehmend verwundbaren bzw. schutzbedürftigen Informationssystemen wird in Europa etwas langsamer voranschreiten als in den USA. Aber sie wird ohne Frage zunehmen, und anders als in den USA gibt es bisher kaum systematische Anstrengungen zum Schutz dieser Infrastrukturen.[4] Ebenso wenig wird bisher in der politischen Öffentlichkeit Europas der zunehmend engere Zusammenhang zwischen dem Schutz der nationalen Infrastrukturen und der militärischen Sicherheit erkannt.

Die Informationstechnologie wird in Europa militärisch zur Kampfkraftverbesserung der heutigen Systeme eingesetzt, aber ein Ansatz wie in den USA, sie in Verbindung mit anderen Technologien zur Bereitstellung neuartiger Fähigkeiten für militärische Aufgaben des 21. Jahrhunderts einzusetzen, fehlt bisher. Entsprechend nimmt auch die Verwundbarkeit militärischer Systeme gegenüber IKF-Angriffen in europäischen Streitkräften langsamer zu, allerdings um einen Preis: ihre Zukunftsfähigkeit wird insgesamt geringer bzw. eine spätere Nachholanstrengung wird um so größer und kostspieliger sein, wenn die Bündnis- und Koalitionsfähigkeit - vor allem mit den USA - in den ersten Jahrzehnten des 21. Jahrhunderts erhalten bzw. neu gestaltet werden soll.

3. Zwei Sichtweisen

In der Betrachtung strategischer Informationskriegführung herrschen gegenwärtig *zwei Sichtweisen* vor. Die *eine* geht vom klassischen Kriegsbild aus und sieht in den möglichen Wirkungen strategischer IKF teils kontinuierliche Kampfkraftverbesserungen, teils exotische Risiken, die man im Rahmen der herkömmlichen Aufgaben für wahrnehmbar oder vernachlässigbar hält, z.B. im Sinne zusätzlicher Spezialaufgaben.

In dieser Sicht ist es schwierig, IKF konzeptionell in die strategische Orientierung einer Nation einzuordnen. Die Lehren aus Pearl Harbour lassen sich hier, in den Worten Tom Schellings, auf das mögliche "elektronische Pearl Harbour" beziehen: "Es gibt eine Tendenz in unserer Planung, das Ungewohnte mit dem Unwahrscheinlichen zu verwechseln. Der Fall, den wir nicht betrachtet haben, erscheint fremd; was fremd erscheint, gilt als unwahrscheinlich; was unwahrscheinlich ist, muß nicht ernsthaft in Betracht gezogen werden... Überraschung ist alles, was im Versagen einer Regierung (oder eines Bündnisses), wirksam zu antizipieren, involviert ist. Die Gefahr liegt in der Armut der Erwartungen - einer Routineobsession mit einigen Gefährdungen, die gewohnt, aber wenig wahrscheinlich sein mögen."[5]

Der konzeptionelle Charakter des Problems wird wiederum an Pearl Harbor deutlich. Die USA verfügten über ein "intelligence"-Bild wie vor kaum einem zweiten großen Überraschungsangriff und hatten dennoch kein Bild der japanischen Absichten, das entsprechende politische und militärische Maßnahmen ausgelöst hätte.[6] Was im Fall eines klassischen Überraschungsangriffs schon schwierig war, ist es vollends bei einem IKF-Angriff mit strategischer Qualität: Er findet innerhalb der herkömmlichen Streitkräfteeinsatzplanung keinen Ort und hat ihn in den meisten großen Nationen auch außerhalb nicht. Die Ausnahme sind die USA.

---

4 Ansätze entwickeln sich in erster Linie in Deutschland, Großbritannien, Frankreich, Schweden und Italien.

5 Thomas C. Schelling: Vorwort zu Roberta Wohlstetters Klassiker: Pearl Harbour. Warning and Decision. Stanford, Cal., 1962, p.viif.

6 Wohlstetter, a.a.O., p. 382.

Die *zweite* Sichtweise ist heute vor allem in den USA verbreitet: Sie ist weniger am gegebenen Zustand von Streitkräften als an längerfristigen Streitkräfteentwicklungen orientiert, die insgesamt vor allem durch Umsetzung von Informations- und Kommunikationstechnologien vorangetrieben wird. Damit entsteht eine zunehmende IT-Abhängigkeit, die sich als Verwundbarkeit darstellt, soweit keine vorbeugenden Schutzmaßnahmen ergriffen werden bzw. werden können.

Angesichts der damit möglichen wechselseitigen Optionen von Opponenten zur Nutzung solcher Verwundbarkeiten hat sich ein *Paradigma des Informationskrieges* herausgebildet, das sich verkürzt wie folgt darstellen läßt: Es gibt eine Gesamtheit relevanter Informationen, deren volle Verfügbarkeit strategisch nutzbare Transparenz bedeutet. Im Krisen- und Konfliktfall ist die zeit- und situationsgerechte Verfügbarkeit relevanter Informationen entscheidend, wobei sich mit fortschreitender Anwendung von IT die Entscheidungshierarchien abflachen, ohne daß die strategische Entscheidungskompetenz damit ihren Ort hätte: Abläufe nehmen einen quasi automatisierten Charakter an. Die wechselseitige Interferenz mit Informations- und Kommunikationsvorgängen der anderen Seite mit IT-Mitteln macht in diesem Verständnis den Informationskrieg aus. Sofern er potentiell kriegsentscheidende Wirkungen hat, gilt er als strategischer Informationskrieg (IW).

Die Relevanz von Informationen kann sich, wenn es nicht nur um Zieldaten und andere taktische Informationen u. ä. geht, je nach der Art der strategischen Konzeption sehr unterschiedlich darstellen. Im übrigen gilt auch hier, was Clausewitz über die Nachrichten im Kriege gesagt hat: "Ein großer Teil der Nachrichten, die man im Kriege bekommt, ist widersprechend, ein noch größerer ist falsch, und bei weitem der größte einer ziemlichen Ungewißheit unterworfen."[7] Das wird auch eine überlegene Kenntnis der Gefechtsfeldlage nicht grundsätzlich verändern, solange es um herkömmliche Einsatzformen von Streitkräften geht, und auch in militärischen Konfrontationen künftiger Jahrzehnte wird es Informationen geben, deren Relevanz sich aus strategischen Zielsetzungen und entsprechender Führungsfähigkeit herleitet.

Das Fazit eines der großen Informationskrieger der neueren Geschichte, R. V. Jones, der für Churchill den „Wizard War“ führte, dürfte auch im Informationszeitalter relevant bleiben: „In a time of crisis you will find that a tendency to lose one’s head is apt to appear at any level of administration."[8] Diese Sichtweise erinnert an die frühen Modelle nuklearer Kriegführung, in denen Interaktionen ebenfalls weitgehend unabhängig vom militärischen Gesamtgeschehen abliefen und die strategischen Zielsetzungen der Konfliktpartner praktisch außer Betracht blieben.

Einen isoliert betrachteten Informationskrieg, in dem die Anwendung von IKF-Mitteln quasi „ohne einen Schuß" kriegsentscheidend wirken kann, wird es in naher Zukunft noch nicht geben. Das IW-Paradigma kann - ähnlich wie die frühen Nuklearkriegsmodelle - dazu dienen, spezifische Wirkungen und Schutzerfordernisse zu erkennen. Aber es muß in einen weiteren konzeptionellen Rahmen integriert werden, der strategische Zielsetzungen, strategische Lage, Entscheidungsträger, Wechselwirkungen verschiedener Streitkräftekomponenten einschließlich der IKF-Fähigkeiten, Wechselwirkungen zwischen Auswirkungen auf militärische Fähigkeiten und Strukturen und zivilen Infrastrukturen, Rekonstitutionsfähigkeit usw. umfaßt.

---

[7] Vom Kriege, Erstes Buch, Sechstes Kapitel.

[8] R.V. Jones: The Wizard War. British Scientific Intelligence 1939 - 1945. New York 1978 (US Ausgabe), S. 533.

Beide Sichtweisen sind unzureichend. Die klassische unterschätzt tendenziell, in welchem Umfang und Tempo sich mit der Anwendung fortgeschrittener Technologien und namentlich der IT-Technologien die Art der Bedrohung, die militärischen Aufgaben, die Fähigkeiten und die Strukturen und Einsatzkonzepte verändern werden. Im IW-Paradigma wird umgekehrt unzureichend gesehen, daß - abgesehen von einem vielfältigen neuartigen Störpotential und neuartiger strategischer Asymmetrien - auf Seiten aller größeren Staaten militärische Fähigkeiten verfügbar bleiben werden, in deren Verbund IKF-Fähigkeiten wirksam werden. Entsprechend sind die tendenziellen Fehlurteile in den beiden Sichtweisen: Im klassischen Paradigma werden die Mittel der IKF eher als bescheidene Möglichkeiten der Kampfkraftverbesserung gesehen, im IW-Paradigma entsteht der Eindruck, als seien IKF-Optionen schon heute ein strategisches Mittel nationaler Macht.[9]

4. Entwicklungen von IKF-Fähigkeiten im Rahmen der Gesamtentwicklung militärischer Fähigkeiten

Für ein angemessenes Verständnis der strategischen Dimensionen der IKF ist ein Entwicklungsmodell erforderlich, das die Veränderungen im Bedrohungsspektrum, die national unterschiedlichen Entwicklungsmöglichkeiten und -tendenzen von Streitkräften und die zunehmend IT-abhängigen Rahmenbedingungen militärischen Handelns im Zusammenhang (und auf gleiche Entwicklungsstufen bezogen) betrachtet.

Dabei ist besonders hervorzuheben, daß eine fortschreitende Streitkräftemodernisierung - das macht der Ansatz der amerikanischen "Joint Vision 2010" deutlich - vor allem durch Umsetzung von Informations- und Kommunikationstechnologien erfolgt, und zwar in allen Bereichen operativen Handelns. Damit wird operative oder sogar strategische Informationsdominanz angestrebt, was der offensiven IKF zunehmend Wirkungschancen einräumt.

Die Kehrseite ist, daß mit zunehmender IT-Abhängigkeit die Anfälligkeit für IKF-Angriffe zunimmt. Mit der IT-gestützten Modernisierung nimmt also ein neuartiges Schutzerfordernis zu. Da die USA in ihrer Entwicklung weit voraus sind, gibt es in den USA eine technologische Dominanz/Schutz-Konkurrenz (ähnlich wie in früheren Jahrzehnten zwischen offensiven und defensiven ballistischen Fähigkeiten). In den USA laufen rund 95% der militärischen Informationen über zivile Kanäle. Deshalb ist dieses Schutzerfordernis nur in enger Zusammenarbeit mit der Industrie zu erfüllen.

Eine weitere Konsequenz ist, daß eine IT-abhängige Streitkräftemodernisierung auf umfassende Dominanz abzielen muß. Andererseits nimmt mit der IT-Abhängigkeit der Streitkräfte auch die ziviler nationaler Infrastrukturen zu, und zwar zum Teil sogar rascher, weil der Treiber der IT-Abhängigkeit inzwischen in den zivilen Bereichen liegt. Das heißt für die am weitesten fortgeschrittenen Nationen weiten sich auch die offensiven strategischen IKF-Optionen gegen zivile Infrastrukturen aus. Im Maße der Ausbreitung von IKF-Fähigkeiten nimmt damit also auch das strategische Schutzerfordernis zu. D.h. je fortgeschrittener ein Industriestaat in der Anwendung von IT-Technologien in den volkswirtschaftlichen und gesellschaftlich wichtigen Sektoren - Kommunikation, Verkehr, Energie, Finanzwesen, vitale Hilfsdienste usw. - ist, um so anfälliger ist er für aggressive Informationsoperationen. Dies wird zunehmend auch Aggressoren erlauben, einen Staat entscheidend zu lähmen, ohne daß dessen Streitkräfte dies abwehren können. Da der Urheber u.U. nicht oder nur viel später identifizierbar sein kann, kann sogar die Vergeltungs- und damit Abschreckungsrolle von Streitkräften stark eingeschränkt werden. Solche Wirkungen werden besonders kritisch, wenn

---

[9] Vgl. Jeffrey Cooper: Understanding Information Warfare: Another View, in John Arquilla and David Ronfeldt (eds),: Society and Security in the Information Age; Johns Hopkins University Press, 1997.

zwischen wichtigen Sektoren Wechselwirkungen auftreten, etwa zwischen Energie und Verkehr.

Sektoral sind bei entsprechenden Anstrengungen Schutzmöglichkeiten gegeben. Kritische Wechselwirkungen erfordern ein nationales Konzept für das Zusammenwirken von Regierung, Industrie, Banken, Streitkräften u.a., das über eine bloße Koordinierung verfügbarer Mittel hinausgeht. Die Lähmung kritischer Sektoren oder im nationalen Maßstab greift im übrigen natürlich auch auf die Handlungsfähigkeit von Streitkräften über. D.h. es können Lagen eintreten, in denen Streitkräfte keine Abwehroption bieten und selbst handlungsunfähig werden.

Umgekehrt besitzt der Staat, der einen ausreichenden Schutz kritischer Infrastrukturen bieten kann, auch entsprechende offensive Optionen: je fortgeschrittener er in der Informationsabsicherung ist, um so leichter ist er auch zu eigenen offensiven Informationsoperationen fähig. Man muß aber auch die Möglichkeit einräumen, daß es spezialisierte Akteure gibt, die in der IKF (ähnlich wie bei B- und/oder C-Waffeneinsätzen) ein Mittel zum Ausgleich militärischer Überlegenheit, also zu asymmetrischer Kriegführung sehen.

5. Zeitliche Horizonte der Veränderung: Das Dreistufen-Modell

Ein Entwicklungsmodell, das diese kovarianten Entwicklungen in Zeitstufen erfaßt, existiert nicht. Insbesondere gilt, daß die IKF-Potentiale sich zwar am klarsten am Beispiel der am weitesten fortgeschrittenen Entwicklung, also an der amerikanischen, ablesen lassen, daß man aber die amerikanische Entwicklung, die sich selbst noch in einem Zwischenstadium befindet, nicht einfach verallgemeinern kann. Es gibt zwischen den USA und europäischen Verbündeten ein Gefälle der Leistungsfähigkeit, unterschiedliche Streitkräfteaufgaben und -modernisierungsziele usw. Es wird hier teils langsamere nachholende Entwicklungen, teils hingenommene zunehmende Abstände und Qualitätsunterschiede in den militärischen Fähigkeiten geben, die wiederum neuartige Probleme der Einsetzbarkeit und Koalitions- bzw. Bündnisfähigkeit von Streitkräften auslösen.

In den USA wird diese Entwicklung rein national bzw. unter dem Proliferationsgesichtspunkt untersucht. Hier sollte eine koordinierte Anstrengung der potenten Verbündeten der USA in Europa und Ostasien einsetzen, um zu einer umfassenderen Einschätzung zu gelangen. Gerade weil es sich bei der IKF um eine sektorale Entwicklung im Zuge des aufkommenden Informationszeitalters handelt, können die Erfahrungen aus vorausgegangenen umwälzenden technologischen Neuerungen in der Informations- und Kommunikationstechnologie einen ersten Schlüssel bieten, wenngleich daraus noch kein Entwicklungsmodell resultiert.

Man hat in diesem Sinne die Auswirkungen der Einführung von Fernschreiber, Telefon, Radio und Fernsehen untersucht und dabei das von Thomas Malone entwickelte Modell der Auswirkungen technologischer Umwälzungen benutzt.[10] In diesem Modell werden solche erster, zweiter, dritter Ordnung unterschieden (siehe Schaubild 1). Auswirkungen erster Ordnung bestehen in der Ersetzung älterer Technologien bzw. Systeme durch neuere. Solche zweiter Ordnung zeigen sich in der zunehmenden Nutzung der neuen Mittel für ein wachsendes Aufgabenspektrum. Auswirkungen dritter Ordnung schließlich resultieren in neuen Verhaltensformen in Abhängigkeit von den neuen Technologien. Diese drei Stufen zeigen eine typische zeitliche Progression. Im Falle des Radios hat es fast 50 Jahre seit der

[10] Thomas W. Malone and John F. Rockart, Computers, Networks and the Corporation, in Scientific American 265.3, Sept. 1996, S. 128-136.

Einführung gedauert, bis im Zweiten Weltkrieg militärische Auswirkungen dritter Ordnung wirksam wurden.[11]

Es ist erkenntnisfördernd, die Entwicklung von IKF-Fähigkeiten entsprechend auf einer Zeitachse abzubilden. Danach befinden die USA sich zunehmend in der zweiten Phase, während mit den längerfristigen Planungszielen, wie sie etwa in der Joint Vision 2010 formuliert sind, klar die dritte Phase angestrebt wird. Wichtige europäische Partner der USA befinden sich eher in der ersten Phase mit der Tendenz zur zweiten. Dabei ist diese Entwicklungsform für verschiedene Nationen und für einzelne Sektoren wie den militärischen nicht zwangsläufig: Nationen können über das Maß und die Folgen relativer Rückständigkeit selbst entscheiden, nicht aber über die Auswirkungen aus dem Umfeld.

Das Beispiel des amerikanischen Quadrennial Defense Review (QDR) zeigt mit seinen drei „Pfaden", wie wichtig in der gegenwärtigen Übergangsphase die Organisation des Modernisierungsprozesses ist. Es gibt eine kritische Abwägung zwischen der Einführung neuer Technologien und der strategischen Konzeptentwicklung: Eine frühzeitige Einführung neuer Technologien erlaubt einen größeren Zeitraum für die Konzeptentwicklung. Diese kann sich jedoch u.U. an unausgereiften Technologien orientieren. Umgekehrt kann ein Ausreifenlassen von Technologien zweckmäßig sein, aber eine entsprechend verzögerte Konzeptentwicklung kann u.U. die Handlungsfähigkeit stark beeinträchtigen. Es gibt große Beispiele für beides. Erforderlich ist ein ausgewogenes Vorgehen, das sich allerdings nicht nur an nationalen Vorgaben ausrichten kann, sondern das Tempo in der Entstehung von Bedrohungen und in der Veränderung von Bündnisstrukturen berücksichtigen muß.

6. IT-abhängige Verwundbarkeiten nationaler Infrastrukturen

Das Dreistufenmodell ist hilfreich, um die gegenwärtig noch babylonisch verwirrte Diskussionslage übersichtlich zu machen: Man kann angeben, bei welchem Staat man von welcher Entwicklungsstufe spricht. Damit lösen sich etliche Scheinkontroversen auf.

Dies gilt auch für die Betrachtung IT-bedingter Verwundbarkeiten ziviler nationaler Infrastrukturen. Es gibt hier zwei ganz unterschiedliche Ausgangspunkte für die Analyse und Diskussion. Der eine besteht in der rapide zunehmenden Zahl der Zugänge, Wirkungsverfahren und potentiellen Akteure in beliebigen Distanzen für Angriffe auf Informationssysteme und -operationen. Der andere ist mit der Verwundbarkeit der nationalen Infrastrukturen gegeben: In den Worten des Vorsitzenden der Commission on Critical Infrastructure Protection: „With our increased reliance on IT throughout the economy, increased interdependence of infrastructures, we are on the road to catastrophe."[12] Risiken und Schutzaufgaben lassen sich wiederum auf der Zeitachse abbilden.

Einzelangriffe sind bereits in großer Zahl Tatsache. Sie werden sogar zu Schutzzwecken als selbstinitiierte Experimente durchgeführt: Die US Defense Information Agency hat 1996 rund 38.000 on-line-Angriffe auf Departement of Defence-Computer unternommen, um deren Sicherheit zu testen; nur 4% wurden identifiziert, und von diesen wurden nur 27% regelrecht gemeldet.[13] Im Sommer 1997 hat das amerikanische Verteidigungsministerium ein großangelegtes Experiment durchgeführt, das Projekt "Eligible Receiver", bei dem durch

---

[11] Siehe die SAIC Fallstudie von Christopher Burton: The Radio Revolution, McLean, Virginia, January 1997.

[12] R. Tom / Marsh, in: Workshop on Protecting and Assuring National Infrastructure. July 1997, Stanford University, S. 7.

[13] Siehe den Bericht über die Untersuchungen des zuständigen Unterausschusses des US Senate Government Committees, Defense News.

Angriffe auf nichtklassifizierte Computer das gesamte U.S. Pacific Command gelähmt wurde. Das nachfolgende Experiment "Solar Sunrise" diente mit ähnlichen Ergebnissen Angriffen auf Hochleistungscomputer.[14] Im Zuge der Verlegung von militärischem Personal und Ausrüstung im Februar 1998 wurden elektronische Angriffe auf mindestens 11 amerikanische militärische Computersysteme festgestellt, der bisher am besten organisierte und systematischste Angriff, den amerikanische Behörden bisher registriert haben (John Hamre, Stellvertr. Verteidigungsminister).[15] Andererseits ist das Fazit der "Presidential Commission", daß es noch keine unmittelbaren Gefahren mit der möglichen Konsequenz einer nationalen Katastrophe gebe. Aber die zunehmenden Risiken bei sinkenden Kosten eines wirksamen Angriffs machen den Schutz nationaler Infrastrukturen zu einer vorrangigen Aufgabe. Sie ist unverhältnismäßig schwieriger und aufwendiger als der Schutz vor Einzelangriffen. Er erfordert eine relativ lange Vorlaufzeit. Es ist also keine Zeit zu verlieren. Dies gilt verstärkt angesichts der Möglichkeit, daß nationale Infrastrukturen im Rahmen einer aggressiven Strategie gegen den Staat angegriffen werden.

Die US Defense Intelligence Agency hat die in verschiedenen Zeiträumen möglichen Angriffe auf amerikanische Ziele von nationaler Bedeutung systematisiert und gewichtet (siehe Schaubild 2). Dazu sind einige qualifizierende Feststellungen nötig:

Eine Verwundbarkeit gegenüber Informationsangriffen erfordert Schutzmaßnahmen. Sie ist aber nicht mit akuter Gefahr gleichzusetzen. Dazu zwei Vergleichsbeispiele: Seit den siebziger Jahren wird die von Amateuren gebastelte nukleare "Bombe im Keller" als technisch möglich angesehen. Dennoch ist der nukleare Terrorismus bisher noch nicht zur akuten Gefahr geworden, wenngleich das Risiko seit dem Zerfall der UdSSR zunimmt. Die "Presidential Commission" hat auf die extreme Verwundbarkeit ziviler Infrastrukturen gegenüber nuklearen EMP- (Elektromagnetischer Puls) Angriffen hingewiesen, nicht-staatliche EMP-Angriffe aber angesichts einfacherer Mittel und hoher Anforderungen zugleich als besonders unwahrscheinlich bezeichnet.[16]

Für politisch motivierte Angriffe wird man also (wie beim Nuklearterrorismus) Zielsetzungen, Strategien, alternative Einsatzmittel und die Haltbarkeit erreichter Ziele in Rechnung stellen müssen, was das Spektrum realer Bedrohungen einschränkt und das Setzen von Prioritäten erlaubt. Entsprechende Analysen fehlen aber noch weitgehend. Nationale Sicherheit kann auch durch nicht gegen den Staat gerichtete Angriffe verletzt und gefährdet werden, und es kann auch gegenüber nicht-staatlichen Adressaten Zielsetzungen, Strategien, eine Wahl der Einsatzmittel und ein Erfordernis der Absicherung erreichter Ziele geben. Solche Angriffe können im übrigen eine Schwächung relativ zu Dritten bewirken, die nur indirekt oder gar nicht beteiligt sind.

s ist nicht nur schwierig, konzeptionell zwischen nicht-politischen Störungen bzw. Angriffen und solchen Angriffen zu unterscheiden, die auf die Handlungsfähigkeit des betroffenen Staates zielen. Es kann auch zu verdeckten Angriffen vor allem in der Vorlauf- und Anfangsphase eines Krieges kommen, ohne daß klar ist, ob es sich um eine Kriegshandlung handelt oder nicht. Im weiteren Verlauf würde die strategische Natur des Angriffs zwar erkennbar werden, aber bis dahin können potentiell entscheidende Nachteile eingetreten sein. Dabei entstehen auch rechtliche Probleme: Solange nicht erwiesen ist, ob

---

[14] Washington Post, 26.2.1998.

[15] Siehe Washington Post 16.4.1998 sowie die Anhörung von George Tenet, Director für Central Intelligence und Generalleutnant Kenneth Minihan (U.S. Air Force Director, NSA) am 24.6.1998 vor dem Senatsausschuß für Regierungsangelegenheiten.

[16] AW&ST, 30.06.97, S.51.

eine Aggression vorliegt, ist auch das Recht auf Selbstverteidigung, noch mehr aber eine Beistandspflicht strittig.[17]

Nichtmilitärische nationale Infrastrukturen befinden sich überwiegend im privaten Besitz und der militärische Informationsfluß verläuft in den USA, wie gesagt, zu rund 95% über private Kanäle. Damit kommt der Industrie in Fragen der nationalen Sicherheit eine ganz neuartige Rolle von maßgebender Bedeutung zu. Dies erfordert neue Formen der Zusammenarbeit zwischen Regierung, Streitkräften und Industrie, die entsprechende organisatorische Vorkehrungen vor allem innerhalb der Regierung erfordert. Seitens der Industrie gibt es - abgesehen von der Frage staatlicher Anreize für Schutzmaßnahmen - einmal das Problem, daß zunehmende IT-Abhängigkeit die Konkurrenzfähigkeit am Markt erhöhen soll, was übergreifenden Lösungen im Wege stehen kann. Zum anderen geht es vor allem um große Unternehmen, die multinational organisiert sind, was wiederum der Kooperation mit Regierung und Streitkräften Grenzen setzt. Es ist hier bemerkenswert, daß von den 100 größten Ökonomien der Welt 51 Unternehmen und 49 Staaten sind.

Da Schutzmaßnahmen auf offensive Optionen bezogen sind, ist auch die Zusammenarbeit mit anderen Staaten und deren Streitkräften nur begrenzt opportun, und die USA verhalten sich hier bisher auch tatsächlich sehr zurückhaltend. Das gilt natürlich verstärkt für internationale Organisationen wie die WTO, die ITU (International Telecommunications Union), die UNO, die OECD, die G-7/8 (führende Wirtschaftsmächte USA, Großbritannien, Frankreich, Deutschland, Japan, Kanada und Italien plus Rußland), die World International Property Organization u.a., die sämtlich im Prinzip für Zusammenarbeit bei Schutzvorbereitungen gegenüber Informationsangriffen in Betracht kommen. Vor allem aber: keine internationale Organisation wird etwas ausrichten, wenn die nationalen Instanzen nicht zunächst die materiellen, organisatorischen und konzeptionellen Grundlagen geschaffen haben.

7. Die absehbaren Verschiebungen im Konfliktspektrum: Frieden/Krise/Krieg unter IKF-Bedingungen

Mit den zeitlichen Perspektiven und der Verwundbarkeit nationaler Infrastrukturen verändern sich die Schutzaufgaben von Staaten. Um diese zu erfassen, ist es erforderlich, nicht nur die Auswirkungen möglicher IT-Angriffe, sondern auch deren politische Qualität zu erfassen und zu kategorisieren. Hier betritt man Neuland. Diese Staatsaufgabe wird zusätzlich dadurch erschwert, daß die Wahrscheinlichkeit von IT-Angriffen mit nationalen Konsequenzen, die Zuständigkeiten, die Voraussetzungen für eine Zusammenarbeit mit Industrie und gesellschaftlichen Organisationen, die Aufgaben der Streitkräfte und damit die nationalen Strategien sich von Staat zu Staat unterscheiden.

Es gibt bisher keine allgemein akzeptierte Kategorisierung der Auswirkungen nach ihrer politischen Qualität. Genauer, es gibt überhaupt erst erste Ansätze dazu. Dies wird letztlich auch nur mit einer gewissen Interpretationsbreite möglich sein. Trotz der dominierenden Rolle der nuklearen Abschreckung während mehrerer Jahrzehnte war dies in der nuklearen Ära nicht anders.

Geht man von der Vielfalt möglicher IT-Einzelangriffe aus, so kann der Staat durch Setzen rechtlicher Rahmenbedingungen, Anreize, organisatorische Vorkehrungen, Forschungs- und Entwicklungsprogramme, Aufklärung usw., wichtige Teilaufgaben übernehmen, die sich nur

---

[17] Siehe dazu im Rahmen des Stanford-Projekts Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo: Old Law for a New World? The Applicability of International Law to Information Warfare. Stanford, Februar 1997; sowie den Bericht zum zweiten Workshop on Protecting and Assuring Critical National Infrastructure, a.a.O.

teilweise im Rahmen der bestehenden Regierungsorganisation ausreichend wahrnehmen lassen. In Deutschland etwa wäre z.B. ein Ausbau der Struktur des Bundessicherheitsrates und dessen systematische Nutzung wichtig. Da, wo der Staat selbst Ziel von IT-Einzelangriffen ist, die Zuständigkeit also entsprechend eindeutig ist, erweitert sich diese Aufgabe. Doch bleibt der Staat auf Zusammenarbeit mit der Industrie angewiesen.

Staatliche Schutzaufgaben hoher Priorität entstehen, wenn

- nationale Infrastrukturen gefährdet sind,
- eine Interferenz von IT-Angriffen mit anderen (z.B. militärischen) staatlichen Schutzaufgaben erfolgt,
- Massenterrorismus (national oder transnational) mit IT-Mitteln stattfindet,
- zwischenstaatliche Konflikte bzw. IT-Angriffe auf den Staat durch nicht-staatliche strategische Akteure wesentlich defensiv und/oder offensiv in starkem Maße durch IKF bestimmt sind.

Bei staatlichen Schutzaufgaben hoher Priorität ist die Bekämpfung von IT-Angriffen naturgemäß noch schwieriger als bei taktischen Einzelangriffen. Mit solchen Angriffen ist eher mittelfristig zu rechnen. Aber die Vorbereitung - technologisch, organisatorisch, doktrinal, in bezug auf Management der Öffentlichkeit usw. - erfordert auch einen erheblich größeren Aufwand und einen längeren Vorlauf. Man kann hier nicht auf auslösende Schocks, auf einen "reality check“ warten.

Andererseits ist bei Angriffen mit politischer Qualität bzw. durch strategische Akteure die Entdeckbarkeit quantitativ anders zu sehen als bei einzelnen Störangriffen: IKF ist hier nicht isoliert zu sehen, sondern im Kontext von Konfliktlagen, Interessen und Zielen einer Strategie zur Beeinflussung der betroffenen Bevölkerung usw. Strategische Ziele sind nicht ohne politische Öffentlichkeit verfolgbar. Insofern läßt sich bei Angriffen von nationaler Relevanz nicht einfach durch Verallgemeinerung der möglichen Anonymität von IT-Einzelangriffen folgern, daß es strategische IKF ohne Kenntnis des Aggressors geben kann. Am ehesten läßt sich dies noch für IT-bedingten Massenterrorismus absehen. Natürlich kann es im Vorlauf zu umfangreichen politisch-strategischen Konflikten größere IKF-Angriffe ohne erkennbaren Akteur geben, die den nachfolgenden Konfliktverlauf zum Nachteil des Angegriffenen beeinflussen. Dies erfordert Vorkehrungen besonderer Priorität. Dazu gehört vor allem eine defensive Strategie, die Vorkehrungen und Abwehrverhalten leitet. Diese Sachlage verändert sich erst dann, wenn es strategische IKF-Angriffspotentiale gibt, die sich isoliert mit kriegsentscheidender Wirkung einsetzen lassen. Aber auch hier wird das Problem weniger das der Anonymität des Aggressors als das der Gefahr eines "Entwaffnungsschlages" nach dem Modell eines nuklearen Entwaffnungschlages sein.

In diesem Zusammenhang ist im übrigen hervorzuheben, daß die kritischen nationalen Infrastrukturen sich in unterschiedlichem Maße als Ziele für strategische IKF-Angriffe eignen. So würde ein Angriff auf den Geldverkehr internationale bzw. globale Auswirkungen haben, die mit einem Angriff auf einen Staat X nicht erwünscht sein dürften oder sogar die Interessen des Angreifers selbst verletzen können. Hier liegt dann zwar eine staatliche Mitverantwortung für den Schutz vor, aber die strategische Qualität ist anders einzuschätzen als bei einem Angriff auf das Informations- und Kommunikationssystem oder die Energieversorgung. Das besondere Schutzbedürfnis von Finanzinstitutionen macht den Schutz im übrigen besonders schwierig.

Eine Kategorisierung der Auswirkungen von IT-Angriffen nach ihrer politischen Qualität sollte also zweckmäßigerweise in strategischer und das heißt in langfristiger Perspektive

vorgenommen werden. Ein solcher "top-down-approach" wird allerdings dadurch erschwert, daß in einem Zeitraum, in dem derartige strategische Veränderungen zu erwarten sind, die aus den vergangenen Jahrhunderten vertrauten Definitionen des Krieges und der Kriegführung selbst grundlegenden Veränderungen ausgesetzt sein werden.

Globale militärische Konflikte sind in den nächsten Jahrzehnten kaum zu erwarten, da ein globaler Rivale für die USA fehlt, und die Entwicklungen in diesem Zeitraum werden von der amerikanischen Streitkräfteentwicklung als Treiber bestimmt sein. Es wird auch kaum noch zu klassischen zwischenstaatlichen Kriegen zwischen Industriestaaten kommen. Die Streitkräfte moderner Industriestaaten werden sich zudem, wie gesagt, vor allem durch Umsetzung von Informations- und Kommunikationstechnologien verändern. Die Verschiebungen und Erweiterungen im internationalen Konfliktspektrum sind aber nur teilweise das Resultat technologischer Dynamik. Sie werden ebenso durch veränderte Rollen der Nationalstaaten, einen zunehmenden strategischen Vorrang ökonomischer Interessen, eine insgesamt veränderte geostrategische Lage sowie durch High-Tech-Modernisierung erzeugte, veränderte logistische und operative Erfordernisse bestimmt.

8. Bündnisfähigkeit unter IKF-Bedingungen

Für eine Ausrichtung auf klassische zwischenstaatliche Kriege zwischen Industriestaaten mag es auf absehbare Zeit noch politische Rechtfertigungen geben. Die militärischen Konfliktlagen, auf die industrielle Kernstaaten in kommenden Jahrzehnten vorbereitet sein müssen, sind

- Expeditionskriege ("power projection"),
- mögliche Konflikte als Resultat der Rekonstitution einer Fähigkeit zu großangelegten Invasionen,
- Mitwirkung an ungleichen Koalitionen (z.B. bei besonderer Exponiertheit einiger Partner der USA),
- zwischenstaatliche Konflikte mit den Fähigkeiten, Organisationsformen und strategisch/operativen Konzepten, wie sie in der Entwicklungsperspektive der USA liegen (mit zeitlicher Verzögerung und begrenzteren Möglichkeiten werden China, Rußland und einige westeuropäische Bündnispartner zunehmend der amerikanischen Richtung folgen).

Die USA sind bisher in der strategischen Konzeptentwicklung weit voraus. Aber in dieser Perspektive gibt es kaum noch Raum für ausgewogene militärische Partnerschaft. Koalitionspartner bleiben aus politischen Gründen relevant. Für die wichtigen Partner der USA ist es zunächst wichtig, diese Entwicklung in der USA in ihren Auswirkungen - nicht zuletzt auf Bündnisse und Koalitionen - zu verstehen. Dabei wird aus der Sicht der USA ein Spannungsverhältnis von "interoperability" und "safety" entstehen, das schwieriger zu gestalten sein wird als in vergangenen Jahrzehnten im nuklearen Bereich.

Es gibt in den USA eine Reihe von Vorstellungen für eine militärische Zusammenarbeit unter strategischen IKF-Bedingungen, z.B.

- selektives "sharing" (Adm. Owen, bis 1996 stellvertretender Vorsitzender der Joint Chiefs of Staff, einer der maßgebenden Urheber der heutigen amerikanischen Zielvorstellung für Streitkräftemodernisierung - Joint Vision 2010)
- amerikanischer "IKF-Schirm" für Verbündete Nye/Owen (Nye: Dean der John F. Kennedy School of Government der Harvard Universität, ehemaliger Vorsitzender des National

Intelligence Council und ehemaliger Undersecretary of Defense for International Security Affairs)

- virtuelle Bündnisse bzw. "plug-and-play-coalitions" (Libicki: Mitarbeiter der RAND Corp, vormals an der National Defense University).

Keiner dieser Ansätze reicht als Basis für künftige Bündnisbeziehungen. Jeder tendiert zu einer Vergrößerung des militärischen Leistungsgefälles zwischen den USA und Dritten.

Es müßte das vitale Interesse gerade der europäischen Kernstaaten sein, nicht nur die konzeptionellen Grundlagen zu schaffen und die erforderlichen nationalen Maßnahmen zu ergreifen. Es wird auch zukunftsentscheidend sein, ob zwischen diesen Kernstaaten ein gemeinsamer Ansatz gefunden werden kann, der in den kommenden Jahrzehnten eine militärisch-politische Partnerschaft mit den USA ermöglicht. Dafür fehlt bisher auf Seiten der USA eine ausreichende Bereitschaft. In Europa beginnt man erst, die Dimensionen des Problems zu verstehen.

Es mag nützlich sein, daran zu erinnern, daß in einer vergleichbaren Situation Anfang der fünfziger Jahre europäische konzeptionelle Angebote (in diesem Fall hauptsächlich britische) dazu geführt haben, daß nukleare Abschreckung zu einem bündnisfähigen Konzept wurde.

NERLICH Uwe, Dr.h.c.
Direktor des Zentrums für europäische Strategieforschung, Ottobrunn.

Schaubild 1

IT-AUSWIRKUNGEN	**DIMENSION DER VERÄNDERUNG**			
	Objekte der Veränderung	Handlungs-ebenen	Art der Veränderung	Ziele für IT-Angriffe
1. Ebene kurzfristig: 1. Ordnung	Systeme	taktisch	Militärisch-technische Revolution (MTR)	kleine Einheiten
2. Ebene mittelfristig: 2. Ordnung	Operationen (Kriegführung)	operativ	Revolution in/of Military Affairs (RMA)	größere Einheiten
3. Ebene langfristig: 3. Ordnung	Krieg	strategisch	Revolution in Security Affairs (RSA)	Staaten global

Schaubild 2

An 'Electronic Pearl Harbour' – Potential Threats of Information Attack on Us National Security

Source	**Validated existence***	**Existence likely (but not validated)**	**Likely by 2005**	**Beyond 2005**
Incompetent Amateur	W	-	-	-
Hacker	W	-	-	-
Disgruntled employee	W	-	-	-
Criminal	W	-	-	-
Organized crime	L	-	W	-
Political dissident	-	W	-	-
Terrorist group	-	L	W	-
Foreign espionage	L	-	W	-
Tactical countermeasures	-	W	-	-
Orchestrated tactical IW	-	-	L	W
Major strategic disruption of US	W	-	-	L

* Validated by the US Defense Intelligence Agency; **W** = widespread, **L** = limited
Source: From a Defense Science Board (US Department of Defense) Task Force report on 'Information Warfare-Defense'.