Reinhard Hutter

„Cyber-Terror“: Risiken im Informationszeitalter

I. Sicherheitspolitische Relevanz der Informationstechnik

Nicht erst seit dem 11. September 2001, sondern spätestens seit der „Ölkrise“ der siebziger Jahre ist klar, dass essentielle Bedrohungen von Gesellschaften und Staaten nicht primär militärischer Natur sein müssen. Feindlich gesinnte Kräfte – seien es gegnerische Staaten, terroristische Gruppen, die von außen oder innen agieren können, oder die Organisierte Kriminalität – werden auch in Zukunft ihr Verhalten grundsätzlich an folgenden Zielparametern ausrichten:

- Sie werden *Schwachstellen* identifizieren und das schwächste Glied in der Kette des anzugreifenden oder zu schädigenden Systems zu nutzen versuchen.
- Sie werden ihren *Aufwand* – sowohl für die Erzeugung ihres Angriffspotenzials als auch für die Durchführung ihrer Operationen – so niedrig wie möglich halten.
- Sie werden ihre *Wirkung* und damit den Schaden des Anzugreifenden ihrer Zielsetzung entsprechend so groß und nachhaltig wie möglich gestalten wollen.
- Sie werden sich selbst, so weit es geht, *schützen* – sowohl vor Entdeckung als auch vor Gegenmaßnahmen des Angegriffenen. (Diese Feststellung gilt nicht oder nur eingeschränkt für Selbstmordattentäter.)
- Sie werden sich, so weit wie möglich, modernster verfügbarer *Verfahren* und *Technologien* bedienen.

Die Wiederholungsgefahr gleichartiger Szenarien hängt ab von der Sichtbarkeit und Glaubwürdigkeit der Gegenmaßnahmen. Es ist daher anzunehmen, dass der Terrorismus sich wechselnder Formen von Angriffen bedient. Im Prinzip kommen alle „Optionen“ von Bedrohungen – die konventionelle, die biologische, die chemische und unter gewissen Voraussetzungen auch die atomare – in Betracht (s. Abb. 1).

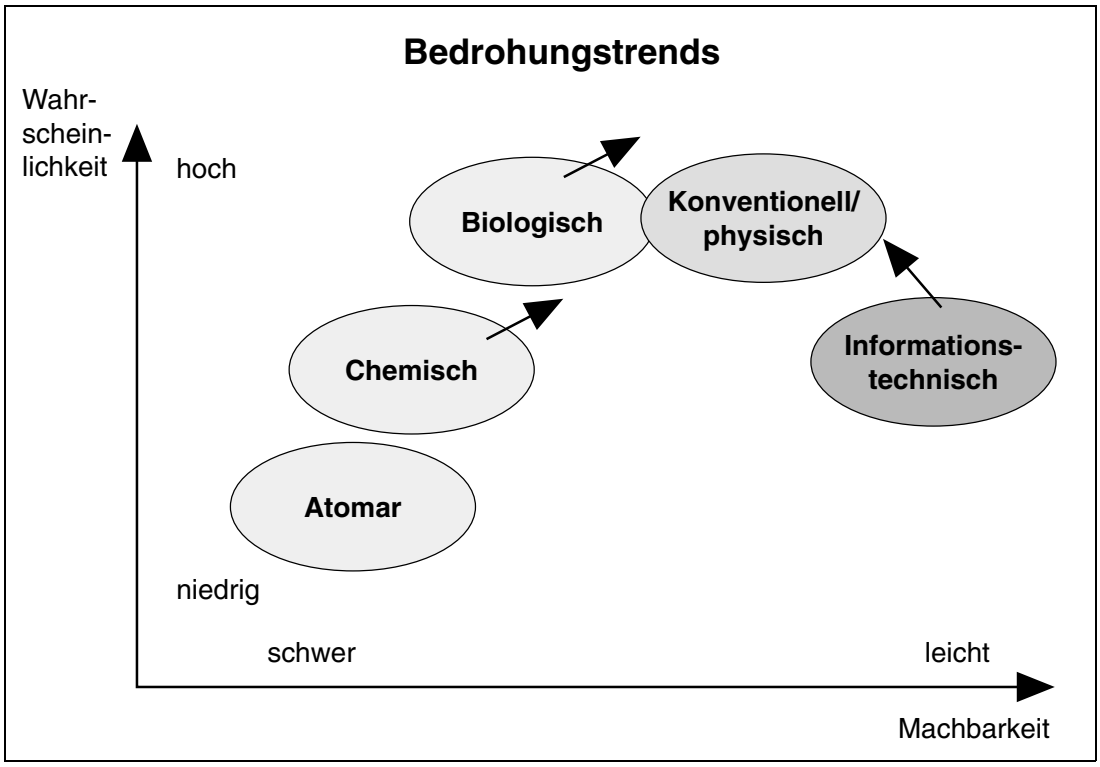
Allerdings sollten wir uns von den klassischen, aus dem Militärischen bekannten Bedrohungsanalysen verabschieden. Zumindest für ideologisch und religiös motivierte Terrorkräfte ist eine nach westlich-rationalen Kriterien abgeschätzte Eintrittswahrscheinlichkeit nicht brauchbar. Wir müssen damit rechnen, dass das Machbare auch eingesetzt wird. Somit ergibt sich für die Informationstechnik (IT) sowohl als Ziel wie auch als Waffe eine zunehmende Bedeutung. IT im Sinne dieser Abhandlung beinhaltet u. a. Computerhardware, Betriebssysteme, Anwendersoftware, Netze, Dienste, Administration, Verfahren und Organisation von Systemen der Informationsverarbeitung, -übertragung und -nutzung.

Die Informationstechnik, ihre Verbreitung und Vernetzung in industrialisierten Gesellschaften, bietet in allen genannten aggressiven Verhaltenskategorien nahezu ideale Voraussetzungen für feindliche Handlungen. Die Informationstechnologie ist daher ein Risikofaktor ersten Ranges, dessen sicherheitspolitische Relevanz für die innere und äußere Sicherheit anderen Faktoren wie militärisches Potenzial oder Energie-, Lebensmittelbzw. der Rohstoffversorgung in nichts nachsteht. Unser tägliches Leben hängt hochgradig von der IT ab. Der Welthandel ist in der heutigen Form ohne IT nicht möglich. Verwaltung und staatliches Handeln sind ohne IT undenkbar. Die Schätzungen der Abhängigkeit von IT bei uns liegen für wichtige Bereiche zwichen 90 und 99 Prozent. Es gibt allerdings auch Regionen auf unserem Globus, da ist sie nahezu null.

Die Abhängigkeit der so genannten „Kritischen Infrastrukturen“ – lebenswichtiger Bereiche unseres Gemeinwesens – von der IT hat sich so schnell und z. T. so subtil entwickelt, dass das politische Bewusstsein und Handeln mit den damit herangewachsenen Gefahren nicht Schritt gehalten hat. Die Denkzyklen zur Analyse neuartiger Bedrohungspotenziale und zur Einleitung von Schutz- und Gegenmaßnahmen im Bereich Kritischer Infrastrukturen bewegten sich bisher in Zeiträumen von Jahren und teilweise sogar kontraproduktiv (z. B. der Katastrophenschutz). Sie haben sich nun mit dem 11. September 2001 schlagartig verkürzt. Es bleibt zu hoffen, dass diese Einsicht in die dramatischen Veränderungen auch anhält.[1]

1 Vgl. zu den diversen Problembereichen u. a. den umfangreichen Sammelband „Sicherheitspolitik in neuen Dimensionen. Kompendium zum erweiterten Sicherheitsbegriff,

Abbildung 1



Quelle: Industrie- und Betriebsanlagengesellschaft (IABG).

II. Die zehn Risikofaktoren der Informationstechnologie

Warum wird die Informationstechnik zunehmend zu einem ernsten Risikoelement von sicherheitspolitischer Bedeutung?[2]

1. Durch die *weltweite IT-Vernetzung* können Angriffe mit u. U. verheerenden Folgen weitgehend unerkannt aus jedem Winkel der Erde gestartet werden. Die Urheber spektakulärer Angriffe befanden sich z. B. auf den Philippinen oder in Petersburg und verursachten Schäden im zweistelligen Milliardenbereich. Die buchstäblich grenzenlose Vernetzung macht eine Lokalisierung, Identifizierung, Rückverfolgung und Haftbarmachung von Tätern weitgehend unmöglich. Vernetzte Strukturen für Telearbeit oder Fernwartung stellen weitere Risikoquellen dar.

2. Die „Nervenstränge und Gehirne" – also die Netze und datenverarbeitenden Einrichtungen von Industriegesellschaften – sind heute fast sträflich abhängig von wenigen Großlieferanten, sowohl bezüglich wichtiger Bauelemente wie Prozessoren und Speicherchips als auch hinsichtlich der Betriebssysteme, der Standardsoftwaresysteme und der dahinter stehenden Dienste. Daraus folgt nicht nur eine *Abhängigkeit* bezüglich *Versorgung* und *Verfügbarkeit* von Hard- und Software-Komponenten. Es ist ein offenes Geheimnis, dass es enge Verbindungen zwischen der IT-Großindustrie und den nationalen Sicherheitsbehörden, z. B. in den USA, gibt. Es bedarf keiner besonderen Phantasie, dass hier ein Macht- und Einflusspotenzial existiert, welches aufgrund der Komplexität der Systeme nicht mehr transparent ist und das sowohl für Wettbewerbsvorteile der Wirtschaft als auch im Falle von Spannungen oder gar Krisen massiv genutzt werden kann.[3] Heute ist weitgehend nicht

hrsg. von der Bundesakademie für Sicherheitspolitik, Hamburg 2001.

2 Zum Folgenden vgl. Reinhard Hutter, Risiken im Informationszeitalter, in: ebd., S. 483 ff.

3 Vgl. Assessment of the Technologies of Political Control, STOA Report, European Parliament, Straßburg 1998, sowie zahlreiche Veröffentlichungen zu ECHELON, insbesondere im Internet (Stichwortsuche empfohlen).

mehr nachvollziehbar, was alles in ein Softwaresystem „eingebaut“ ist oder eingebaut werden kann. Grundsätzlich ist eine *Monokultur* leichter angreifbar und birgt ein höheres Schadenspotenzial als eine heterogene Vielfalt. *Outsourcing* bzw. *Privatisierung* von kompletten IT-Großsystemen und deren Diensten reduzieren darüber hinaus die Möglichkeit der Kontrolle und Überwachung durch den Staat.

3. Ein stetes Dilemma schaffen die extrem schnellen *Innovationszyklen* der IT-Systeme. Sie wirklich sicher zu machen, dauert häufig länger als die Entwicklung der IT-Nachfolgegeneration selbst, sodass der erstrebte Sicherheitsstandard nie erreicht wird. Wir müssen uns auch schon jetzt auf weitere, völlig neue Formen des Eindringens der IT in unsere Gesellschaft vorbereiten: Intelligente Roboter im Alltag, direkte Schnittstellen zwischen Elektronik und Nervensystemen, Leistungen der künstlichen Intelligenz, welche die des menschlichen Gehirns zumindest in Teilbereichen weit übersteigen. Wenn sich die Visionen von Zukunftsforschern auch nur zu Bruchteilen bewahrheiten, werden IT und Elektronik zum integralen Bestandteil aller Belange des täglichen Lebens und des Menschen selbst.

4. Die *Komplexität* der Systeme hat zu einem hohen Grad der *Unüberschaubarkeit* und *Nicht-Beherrschbarkeit* in Störfällen geführt. Sie nimmt weiter zu. Jeder von uns wundert sich schon über die Unmöglichkeit, bestimmte Abläufe bei der Handhabung eines Systems wie *Windows* zu verstehen oder gar zu reproduzieren. Komplexe Systeme wie Betriebssysteme oder Netzsteuerungen führen zunehmend ein „Eigenleben“, das immer schwerer zu beherrschen ist.

5. IT ist *allgemein verbreitet* und *verfügbar*, IT-Systeme sind üblicherweise leicht zugänglich, sowohl IT-technisch als auch physisch. Jeder „Angreifer“ kann heute schon über einen enormen Fundus verfügen: von der Kabelzange bis hin zur Bauanleitung von schädlichen Codes im Internet. Eine eigene Art der „Proliferation“ hat bei der IT bereits stattgefunden und wird sich weiter fortsetzen. Digitale Waffen lassen sich ohne Aufwand beliebig vermehren und transportieren.

6. Gleichzeitig hat diese Verbreitung dazu geführt, dass die meisten unserer so genannten „Kritischen Infrastrukturen“ elementar von der Verfügbarkeit und Funktionsfähigkeit der Informationstechnik abhängen. Mit geringem Aufwand können daher extrem hohe Schäden verursacht werden. Ein Hochleistungs-Waffensystem kostet einen zwei- bis dreistelligen Millionenbetrag pro Einheit (Systempreis), und es kann im Einsatz Schäden in vergleichbarer Größenordnung verursachen. Dagegen können heute Milliardenschäden durch einen einzelnen Hacker oder Virus produziert werden, wie der „I Love You-“ oder andere Viren gezeigt haben. Dieses zunehmende Ungleichgewicht zwischen Mittel und Wirkung zählt zu dem so genannten *asymmetrischen Verhalten* in künftigen Konflikten, welches vor allem typisch ist für substaatliche Organisationen und Terrorgruppen.

7. Das *Spektrum der Verwundbarkeit* der IT ist sehr groß und im ständigen, schnellen Wechsel begriffen. Hackerangriffe gehören heute bereits zum Alltag. Was kaum Beachtung findet, ist die Tatsache, dass auch täglich neue Angriffswerkzeuge entstehen und neue Lücken in Betriebssystemen, Browsern oder Chips identifiziert werden. Am „Lebensgang“ eines IT-Systems sind bis zu 50 verschiedene „Parteien“ beteiligt: Das reicht von der Forschung über Entwicklung, Fertigung, über Handel, Betrieb und Nutzung bis hin zur Wartung. Jede dieser Parteien ist ein potenzieller Risikofaktor.

8. Das *Spektrum der Angreifer*, ihrer Motive und Angriffsoptionen ist somit weit gespannt und reicht vom verärgerten Mitarbeiter als Innentäter über den Fanatiker, Terroreinheiten, Industriespionage, organisiertes Verbrechen bis hin zu feindlichen Staaten. Das *Spektrum der Angriffsoptionen* reicht vom heute schon fast „normalen“ Hackerangriff bis zur gezielten Störung oder Zerstörung eines zivilen oder militärischen Lagezentrums durch eine EMP-Bombe oder HERF-Sender (EMP = Elektro-Magnetic-Pulse; HERF = High Energy Radio Frequency).

9. Die *Rechts- und Gesetzeslage* sowie darauf basierende Gegen- bzw. Abschreckungsmittel stehen noch auf juristisch wie organisatorisch sehr unsicherem Boden, wenn es sich um „Cyber-Vergehen“ handelt. So hat z. B. das Verbot rechtsradikaler Darstellungen im Internet dazu geführt, dass die deutsche Szene einfach auf ausländische Provider ausweicht. Die Legislative und Exekutive sind weitgehend machtlos bzw. auf freiwillige Vereinbarung mit Providern angewiesen. Die internationale Abstimmung von Rechtsnormen steckt ebenfalls noch in den Kinderschuhen, das gilt auch für die Kooperationsverfahren bei Ermittlung und Strafverfolgung von „Informationstätern“.

10. Die *Verantwortlichkeiten* und *Zuständigkeiten* für den Schutz unserer Infrastrukturen insbesondere gegen terroristische Angriffe auf Netze und Computer sind ebenfalls unklar. Bundeswehr und NATO haben begonnen, die Aufgabe „Informati-

onsoperationen“ konzeptionell zu gestalten.[4] Konkrete Umsetzungsmaßnahmen sind vor allem in den USA erkennbar.[5] Doch welche Aufgaben hat z. B. die Polizei, wie wird sie ausgerüstet und wie arbeitet sie mit Wirtschaftsunternehmen und weiteren Sicherheitsdiensten, insbesondere mit Behörden und Organisationen mit Sicherheitsaufgaben (BOS), etwa Feuerwehr, Polizei, Rettungs- und Hilfsdienste, zusammen, wenn diese massiven Informationsangriffen ausgesetzt sind? Wo sind die Notfallpläne für einen IT-Angriff? Wo ist die Grenze zwischen innerer und äußerer Sicherheit; muss sie neu definiert werden oder löst sie sich auf? Brauchen wir eine IT-Aufsicht? Wird sich ein neuer Regulierungsbedarf entwickeln? Wird es einen „Cyber War“ geben – wie ist er definiert, wer wird ihn austragen? Die Diskussion über neue Aufgaben der Bundeswehr wird bei stärkerer Bewusstwerdung von Szenarien mit Informationsoperationen fortgeführt werden müssen.

III. Das Bedrohungs- und Risikopotenzial

Es gibt im Prinzip drei Arten der kriminellen, subversiven oder aggressiven Gefährdungen durch IT (vgl. Abb. 2):[6]

- Die Informationsnutzung durch entsprechende Kräfte;
- das sogenannte Hacking und
- den Cyber-Terrorismus bis hin zum Cyber War.

1. Informationsnutzung

Elektronische Information wird in zunehmendem Maße für Zwecke ökonomisch-protektionistischer oder totalitärer Politik, aber auch durch terroristische und kriminelle Kräfte genutzt oder manipuliert. Dies schließt gesteuerte Zugangskontrolle, gezielte Informationsfilterung und Propagada ein.

Beispiele:

- Die Blockierung so genannter subversiver Web-Sites durch die chinesische Regierung.
- Unwahre, hetzerische Darstellungen; z. B. Propaganda und Gegenpropaganda im Kosovo-Krieg.
- Verbreitung rechtsradikalen oder islamisch-fundamentalistischen Gedankenguts im Internet.
- Die Hizbollah propagiert ihre Angriffe auf israelische Ziele auf ihrer Web-Site.
- Die USA überwachen den weltweiten Telefonverkehr mit ECHELON.
- Virtuelle Organisationen, Versammlungen, Verschwörungen: Sog. Globalisierungsgegner rufen auf zum koordinierten Vorgehen u. a. gegen Finanzdienstleister und Energieversorger durch Märsche, Demonstrationen und durch Hacking.

Im Prinzip sind das alles keine neuen Phänomene, jedoch verleiht das Internet diesen Maßnahmen aufgrund von Geschwindigkeit, Verbreitungs-Reichweite und Anonymität eine völlig neue Qualität von Bedrohung und Gefährdung.

2. Hacking

Hacking ist eine Form des aktiven Eindringens in Computersoftware und Datenbestände. Die gefährlicheren Varianten haben zum Ziel, Informationen zu erlangen, zu manipulieren oder zu zerstören bis hin zum Funktionszusammenbruch von Großsystemen.

Beispiele:

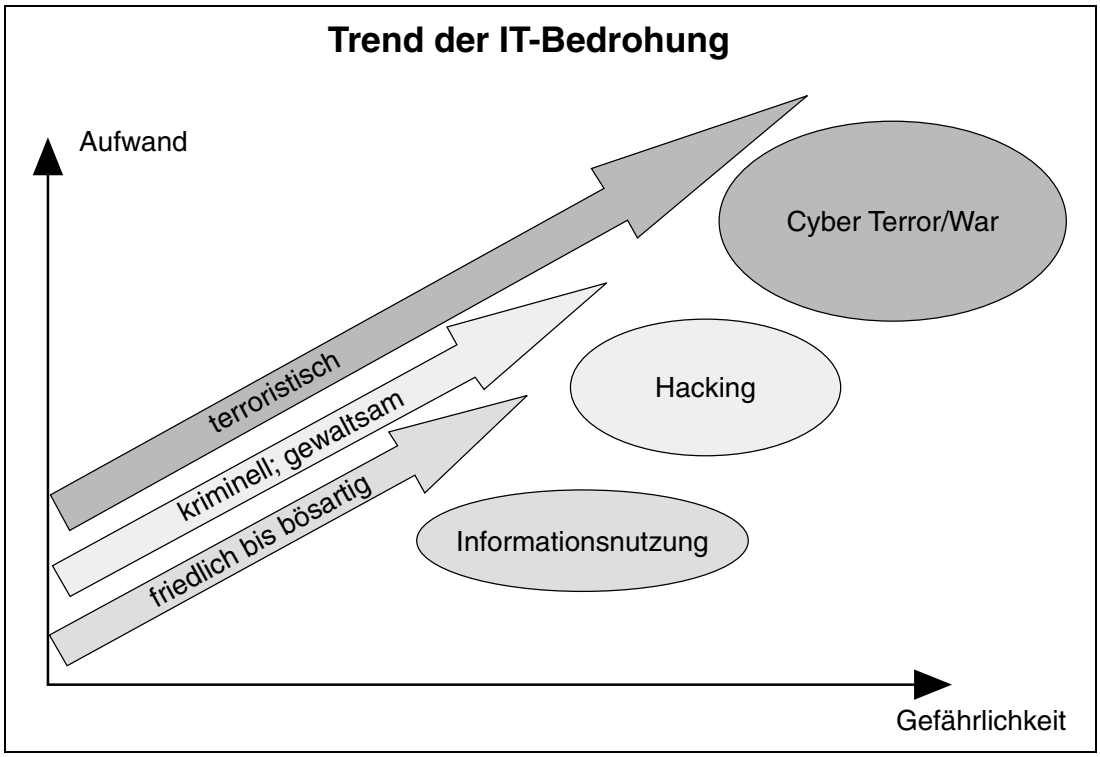
- Virtuelle „Sit Ins“ z. B. in Form von Blockaden, so genannte *Denial of Service*-Attacken wie etwa auf die Server von *Yahoo* oder *Ebay.*
- Italienische Zapatista-Sympathisanten versuchten, in die Web-Sites des mexikanischen Staatspräsidenten Zedillo und von Bill Clinton einzudringen.
- Tamilische Rebellen überschwemmen weltweit die Botschaften Sri Lankas durch sog. *e-mail bombing.*
- Die ETA erpresst einen Internet Serviceprovider (IGC) ebenfalls durch elektronisches Bombardement, um zu erzwingen, dass ihr unerwünschte Publikationen zurückgezogen werden.

4 Vgl. Reinhard Hutter, Critical Infrastructures – What is new and what needs to be done, in: Armed Forces Communication and Electronic Association (AFCEA), München 1999; NATO-RTO Meeting, Proceedings 27: „Protecting NATO Information Systems in the 21st Century“, publ. May 2000.

5 Vgl. Clarence A. Robinson, Jr., Information Operations Sweep Across Milieu of Peace and War, in: Signal, September 1999.

6 Vgl. Dorothy Denning, Activism, Hacktivism, and Cyberterrorism: Information axioms-papers, 1999. The Internet as a Tool for Influencing Foreign Policy, http://www.terrorism.com/documents/denning-infoterrorism.html

Abbildung 2



Quelle: IABG.

– Aus dem Entwicklungssystem von Microsoft wird Software Code entwendet, zumindest eingesehen.
– China bricht in ausländische Server von Falun-Gong-Anhängern ein.
– Ein Aufruf zur „Internet-Demonstration" gegen die Lufthansa wegen ihrer Beteiligung an Abschiebungen von illegal eingereisten Ausländern brachte 1,3 Mio. Anfragen von 12 000 IP-Adressen.

3. Cyber-Terrorismus und Information War

Hierbei handelt es sich um gezielte, politisch motivierte Angriffe mit Hilfe der IT und/oder auf die IT mit gewaltgleichen Auswirkungen auf Leben und Gesundheit der Bevölkerung oder die wirtschaftliche und/oder die politische Handlungsfähigkeit von Staaten – dies nicht notwendigerweise, aber auch unter Einbeziehung von Streitkräften. Spionage, Aufklärung, Täuschung, elektronische Kampfführung, physische Zerstörung (von IT-Systemen) oder sonstige Angriffe auf die Information sind alles Elemente künftiger offensiver und defensiver Informationsoperationen eines möglichen „Cyber-Krieges" oder auch künftiger bewaffneter Auseinandersetzungen. Dabei sind diese Elemente selbst im Prinzip nicht neu. Neu ist die zunehmende Bedeutung dieser Art von Operationen in künftigen Auseinandersetzungen.

Der Charakter von Informationsoperationen trägt auch dazu bei, dass die Grenzen zwischen innerer und äußerer Sicherheit, zwischen Aufgaben der Streitkräfte und jenen der Kräfte für die innere Sicherheit mehr und mehr verschwinden. Hier werden neue Aufgabendefinitionen und Aufgabenverteilungen erforderlich. Es gibt zahlreiche Diskussionen, die inzwischen die Information gleichwertig neben die Parameter Kräfte, Raum und Zeit der klassischen Kriegsführung stellen. Insbesondere Angriffe auf so genannte „Kritische Infrastrukturen" gelten mit dem Heranwachsen der nächsten Terroristen-Generation als immer wahrscheinlicher. Es gibt offensichtlich nachrichtendienstliche Erkenntnisse, wonach Bin-Laden-Anhänger in Deutschland die Fähigkeit besitzen, einen Anschlag auf die Internet-Infrastruktur zu verüben. Eine pakistanische Hackergruppe („G-Force") griff eine US-Verwaltung an und drohte, geheime

Regierungsdaten an Bin Laden zu liefern, falls die Angriffe auf Afghanistan nicht eingestellt würden.

4. Die Einschätzung nach dem 11. September 2001

Die klassische Vorstellung, die vor allem in der militärischen Konfliktforschung vorherrscht, man könne Bedrohungen mit Eintrittswahrscheinlichkeiten bewerten, hat sich als trügerisch erwiesen. Die NATO hat den Bündnisfall nach Artikel 5 erstmals in ihrer Geschichte festgestellt, ausgerechnet für ein Szenario, auf das sie sich 52 Jahre lang *nicht* vorbereitet hat. Für die USA lag das größte Gefahrenspotenzial lange bei den ballistischen Flugkörpern von „Rouge States", „Schurkenstaaten". Dass ein vollgetanktes Linienflugzeug zu einem ebenso gefährlichen „Flugkörper" umfunktioniert werden könnte, stand nicht in den Bedrohungsszenarien. Daher muss die „Informationstechnische Option" eines Angreifers bzw. feindlich gesinnter Kräfte ebenso ernst genommen werden wie jede andere. Und mit weiterschreitender Vernetzung und Verbreitung der IT einerseits sowie den sich entwickelnden Fähigkeiten von Streitkräften, Terrorgruppen oder der Großkriminalität andererseits wachsen auch die Möglichkeiten, dass Informationsoperationen konkret eingesetzt werden, ggf. auch im Verbund mit konventionellen, biologischen u. a. Mitteln.

IV. Die Lagebeurteilung

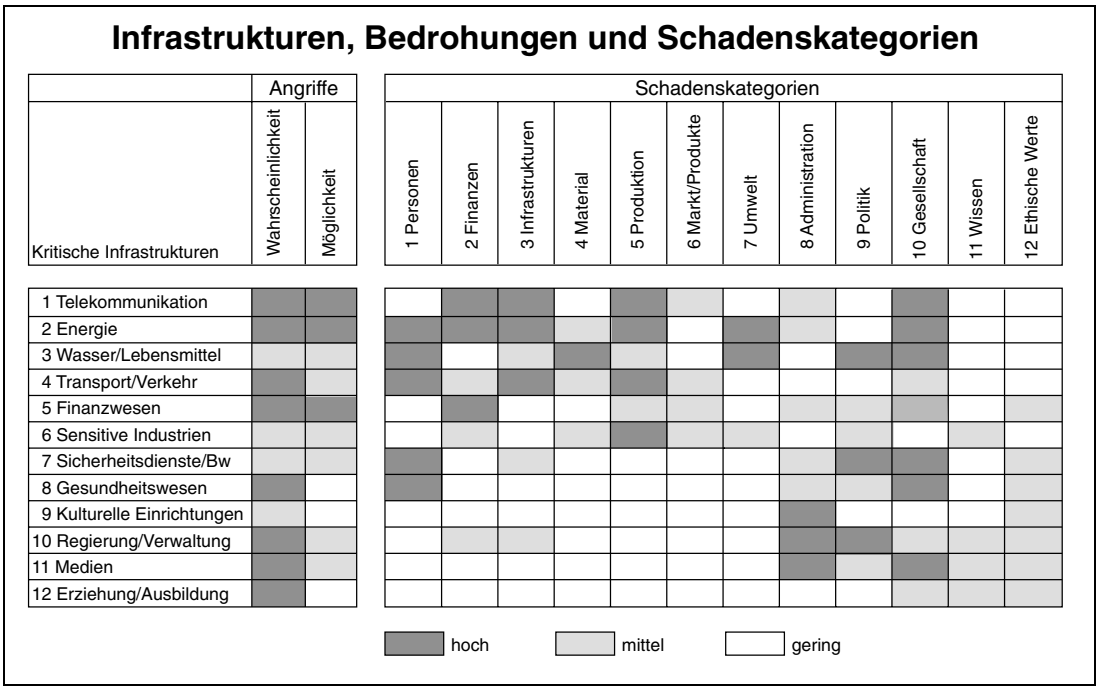
Die meisten z. T. lebenswichtigen Infrastrukturen – ob Schienen-, Straßen-, Luftverkehr oder Sprach- und Datennetze, Energieversorgung oder Rettungsdienste, Banken oder Krankenhäuser – sind heute ohne Informationstechnik und Vernetzung nicht mehr funktionsfähig. In vielen Bereichen sind bereits hochgradig automatisierte, ja sogar selbst entscheidende IT-Systeme im Einsatz. Die damit verbundenen Risiken werden immer unüberschaubarer. Sie können sich für Wirtschaftsunternehmen, für die Politik oder ganze Bevölkerungsgruppen existenzbedrohend entwickeln. Deshalb müssen sie sowohl transparent als auch kalkulierbar gemacht werden.

Eine erste Befragung unter Vertretern von sog. Kritischen Infrastrukturbranchen ergab ein großes Spektrum an möglichen Schadenskategorien bei Angriffen auf IT-abhängige Infrastrukturen. Potenzielle Schäden umfassen Personen- und wirtschaftliche Schäden, Handlungsunfähigkeit von Verwaltung und Politik, den Raub von Wissen oder die Beeinflussung gesellschaftlichen Verhaltens mit Folgen wie Panik oder Verweigerungshaltung. Es handelt sich hier um beispielhafte Schadenspotenziale in einem schon lange vor dem 11. Septemer 2001 gedachten Bedrohungsszenarium für Deutschland (vgl. Abb. 3). Diese Faktoren müssen kontinuierlich beobachtet werden und in eine entsprechende Lagebeurteilung einfließen.

Trotz der Gefahrenpotenziale ist es müßig, die weitere Entwicklung und Verbreitung der IT in Frage zu stellen. Verstärkt durch die Globalisierung von Wirtschaft und Finanzwesen, ferner durch die zunehmende Privatisierung öffentlicher Infrastrukturen und von Aufgaben, die früher als hoheitlich betrachtet wurden, wird jedoch die IT zur sicherheitspolitischen Größe. Ulrich Beck spricht mittlerweile von der „Weltrisikogesellschaft" und fordert eine „Weltinnenpolitik". Inzwischen haben sich auch Innenminister und Bundeskanzler dieser Begriffe bedient. Es liegt auf der Hand, dass hierzu auch eine nationale wie internationale Komponente gehört, die sich mit Risiken, Gefährdungen und dem Schutz von Infrastrukturen unter dem besonderen Aspekt der Informationstechnik und Vernetzung auseinandersetzt. Risiken und Gefahren erwachsen aus den unterschiedlichsten Ursachen und Motivationen. Dabei leisten ebenfalls sehr unterschiedliche Trends der potenziellen Gefährdung gleichermaßen Vorschub:

In weiten Teilen der öffentlichen Diskussion werden „Cyber"-Gefahren zu eng gesehen. Im Bewusstsein vieler sind sie auf die Begriffe Internet, Hacking und Viren reduziert. Die von bewusstem Missbrauch herrührenden Gefahren sind grenzenlos, und die quasianarchische Struktur des Internets verschließt sich staatlich regulativen Kontrollen, Überwachungsmaßnahmen und Eingriffen. Allerdings wird dabei übersehen, dass gerade eine dezentrale Architektur wie die des Internet gegen Ausfälle hochgradig redundant und damit auch widerstandsfähig gegen Angriffe ist. Innerhalb weniger Stunden nach den Angriffen auf das World Trade Center war die Funktionsfähigkeit des Internet im Wesentlichen wiederhergestellt. Gleichwohl war ein wichtiger Grund für den Niedergang des sog. Neuen Marktes an den Börsen die mangelhafte Sicherheit des Internets. Ebenso übersehen wird in einer auf das Internet fokussierten Diskussion das große Spektrum an Verwundbarkeiten durch schädliche Codes und vor allem durch Manipulationen, die durch Innentäter verursacht werden können. Am anderen Ende der Skala von Gefährdungsmöglichkeiten liegen Monopole oder monopolistische Bestrebungen im IT-Sektor, wie die frühere Kryptopolitik der USA oder die

Abbildung 3



Quelle: IABG.

weltweite Abhängigkeit von Microsoft. Sie erhöhen naturgemäß – und schlimmstenfalls auch gewollt – die Risiken und Verwundbarkeiten unserer Infrastrukturen. Dabei hätte uns nicht erst der 11. September 2001 aufzurütteln brauchen: Es gab bereits unzählige Studien, Expertisen, Warnungen, auch konkrete Programme in den USA seit Mitte der neunziger Jahre. John Arquilla z. B. hatte schon 1998 ein umfassendes, global organisiertes Angriffsszenario auf die USA verfasst.[7] Entsprechend diesen Erkenntnissen wird das FBI massiv mit IT-Spezialisten ausgestattet.

V. Ein denkbares Szenario

Die Bedrohung im Sinne eines strategisch angelegten Cyber-Wars ist „virtuell". Mögliche Akteure lassen sich nicht so leicht lokalisieren wie Raketenbasen oder Chemiefabriken. Unklar bleibt auch bis auf weiteres, was in einem Cyber-Szenario öffentliche, was private Zuständigkeit ist. Ferner: Wie ist innere und äußere Sicherheit definiert, müssen die Aufgaben des Staates und ihr Zusammenwirken mit dem Privaten Sektor neu geregelt werden? Die völkerrechtlichen Normen und Definitionen müssen für den vorhersehbaren Informationskrieg uminterpretiert werden.[8] Viele Fragen, auf die es heute noch keine Anworten gibt.

Der „Arbeitskreis Schutz von Infrastrukturen" veranstaltete vom 12. bis 14. November 2001 bei der Industrie- und Betriebsanlagengesellschaft (IABG) in Ottobrunn ein „Cyber Terror Exercise" (CYTEX) unter Beteiligung von Vertretern verschiedener Ministerien und Behörden sowie u. a. der Bundesakademie für Sicherheitspolitik, der Telekom, der DB, der Polizei, des THW, eines Energieversorgers, des TÜV und Vertretern der Großindustrie. Das Szenario bestand aus einer konzertierten Serie von Attacken von innen und außen auf die IT-Systeme dieser vertretenen Branchen sowie von Großbanken im Raum Berlin mit dem Ziel einer massiven politischen Erpressung. Neben vielen Detailergebnissen führte diese Planübung zu folgenden Erkenntnissen:

– Durch Informationsangriffe lassen sich die gesamte Infrastruktur und damit das öffentli-

7 John Arquilla, The Great Cyber War of 2002, in: WIRED Archive, Februar 1998.

8 Vgl. Torsten Stein/Thilo Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, Studie erstellt im Auftrag der IABG, München März 1999.

che Leben, die Funktionsfähigkeit der betroffenen Wirtschaftszweige und die politische Handlungsfähigkeit massiv in die Knie zwingen.

– Nach und nach brechen der Telefonverkehr, die Transaktionsfähigkeit von Banken, die Energieversorgung sowie der Straßen-, Schienen- und Luftverkehr zusammen. Großveranstaltungen müssen abgesagt werden, es kommt zu Panikreaktionen und erheblichen wirtschaftlichen Schäden.

– Es gab keine Zweifel, dass ein derartiges Szenario realistisch ist und so oder ähnlich eintreten kann. Es hat sich vor allem aber auch gezeigt, dass ein hoher Kooperationsgrad zwischen diesen Infrastrukturen zur Beherrschung des Szenarios unabdingbar ist.

VI. Schutz- und Abwehrmaßnahmen

Im internationalen Umfeld sind hier die USA mit ihren militärischen und zivilen Programmen am weitesten.[9] Tausende von Mitarbeitern mit Milliardenbeträgen sind damit beschäftigt, die Gefahren des „Cyber"-Terrorismus zu analysieren, zu bewerten und Maßnahmen vorzubereiten und umzusetzen.[10] Zahlreiche Organisationen entwickeln Formen der staatlich-privaten Kooperation mit unterschiedlichen Erfolgen. In Europa sind vor allem die Schweiz, Großbritannien, Schweden und die Niederlande relativ aktiv. Die EU-Kommission hat begonnen, sich damit auseinander zu setzen. Die NATO hat bisher lediglich Konzeptpapiere.

Allen Initiativen gemeinsam ist die Anlage eines Kooperationsprogramms, welches möglichst viele verantwortlich Zuständige und ggf. Betroffene zusammenführt – staatliche Organe und Sicherheitsdienste auf der einen sowie Infrastrukturbetreiber und -nutzer auf der anderen Seite. Naturgemäß ähneln sich diese Programme sehr. Sie beinhalten durchweg:

– Maßnahmen zum vertrauensvollen Austausch von Informationen;

– Kapazitäten und Methoden zur Analyse, Bewertung und Prognose von Entwicklungen;

– die Einrichtung gemeinsamer Lagezentren mit Aufgaben der Beobachtung, Lagebewertung, Frühwarnung, Alarmierung und Reaktion;

– Maßnahmen zur Schulung und Ausbildung, Zusammenarbeit mit der Forschung;

– Vorschläge zum Umgang mit Medien sowie zur Sensibilisierung der Öffentlichkeit und der Führung in Wirtschaft und Politik;

– Maßnahmen zur Überprüfung und Anpassung der Rechtsnormen und Abstimmung im internationalen Rahmen.

Die Inhalte eines solchen Programms wurden an anderer Stelle bereits beschrieben.[11] In Deutschland haben nun die Ereignisse des 11. September 2001 dazu geführt, dass im Rahmen des Anti-Terror-Pakets der Bundesregierung der Schutz von Kritischen Infrastrukturen einen höheren Stellenwert einnimmt.

Dagegen hat sich die Bundeswehr bereits seit Mitte der neunziger Jahre zumindest theoretisch mit den Gefahren des *Information-Warfare* und den Möglichkeiten von Informationsoperationen intensiv auseinandergesetzt. Eigenständige militärische Systeme für Führung, Nachrichtengewinnung und Aufklärung sowie für den Waffeneinsatz lassen sich vergleichsweise leichter schützen als die zivile IT-Infrastruktur, auf die auch die Bundeswehr zunehmend angewiesen ist. Grundsätzlich wird das Risiko der Bundeswehr in diesem Sektor verstärkt durch Pläne, weite Teile ihrer IT-Struktur – Weitverkehrsnetze, Liegenschaftsausstattung, Rechenzentren und Verwaltungsverfahren – in die privatwirtschaftliche Verantwortung zu übertragen.

Auch andere Infrastrukturbetreiber und -nutzer schaffen sich sukzessive eigene technische und organisatorische Sicherheitsmaßnahmen. Niemandem kann man Verantwortungslosigkeit unterstellen. Dennoch werden diese Einzelmaßnahmen nicht ausreichen, um gegen massive und konzertierte Cyber-Attacken mit kriegerischer bzw. terroristischer Absicht gewappnet zu sein. Ähnlich wie in den USA und beginnend auch in anderen Ländern müssen alle staatlichen, militärischen und zivilen Kräfte sowie die Privatwirtschaft in einer „Public Private Partnership" zusammengeführt werden. Am Anfang muss eine Sicherheitsbewertung des „Infrastruktursystems Deutschland" stehen. Die neuralgischen Punkte bzgl. Abhängigkeit und Verwundbarkeit sind zu ermitteln, zu bewerten und kontinuierlich fortzuschreiben. Der Einsatz von Computermodellen und Simulationswerk-

9 Vgl. Critical Foundations – Protecting America's Infrastructure, www.pccip.gov. Oct. 1977.

10 Vgl. National Plan for Information Systems Protection, Version 1, The White House, Washington 2000.

11 Vgl. Reinhard Hutter, Angriffe auf Informationstechnik und Infrastrukturen – Realität oder Science Fiction?, in: Aus Politik und Zeitgeschichte, B 41–42/2000, S. 31 ff., sowie ders. (Anm. 2).

zeugen ist, auch unter Kosten-Effizienz-Kriterien, zu prüfen.[12] Die Zusammenarbeit kann und darf nicht durch staatliche Regularien dominiert oder gar erzwungen werden. Vielmehr muss die Motivation von der Einsicht aller getragen sein, dass hier eine Gemeinschaftsaufgabe ansteht, die nur in Kooperation und nicht von Einzelnen, auch nicht vom Staat alleine bewältigt werden kann. Auf die unterschiedlichen Interessenslagen und Aufgaben von staatlichen Organen im Vergleich zur Privatwirtschaft wird einzugehen sein. Erfolge werden nur zu erzielen sein, wenn eine „Win-Win"-Strategie gefunden wird, bei der einerseits die Aufgaben des Staates durch Mitwirkung der Privatwirtschaft optimiert werden sowie andererseits die Privatwirtschaft durch staatliche Anreize und Standortverbesserung von einem solchen Programm profitiert.

Schutz und Abwehr sind jedoch nur eine Seite der Medaille: Wir haben uns zu sehr daran gewöhnt, dass Verbreitung und Abhängigkeit von Informationstechnik selbstverständlich sind und sich weiter beschleunigen. Es muss möglich sein – und es wird notwendig werden –, sich zunehmend auch mit Rückfallpositionen und Minimallösungen für den Ernstfall auseinander zu setzen: Welche Infrastrukturen sind lebenswichtig, wie sind sie unter Sicherheitsaspekten auszurüsten und welche minimale Funktionsfähigkeit ist im Ernstfall aufrecht zu erhalten – notfalls auch ohne moderne Informationstechnik? So genannte „robuste Lösungen" bestehen aus sog. redundanten Systemen, alternativen Systemen oder unempfindlichen Strukturen, wie dies auch aus dem Militärischen bekannte Lösungsstrategien sind. Am anderen Ende der Bewertungsskala steht der Umgang mit Restrisiken, deren Beseitigung wirtschaftlich nicht mehr vertretbar ist, die aber transparent und im Einzelfall entweder bewusst hingenommen oder anderweitig – z. B. über Versicherungen oder über politische/diplomatische Handlungsoptionen – abgedeckt sein müssen.

VII. Internationale Zusammenarbeit

Sowohl die IT-Bedrohung als auch die Möglichkeiten von Angreifern, sich auf entsprechende Netze abzustützen, sind internationale Phänomene. Entsprechend muss auch die Gefahrenerkennung und -abwehr international organisiert werden, zumindest benötigt sie eine starke internationale Komponente. Nationale Beobachtungs- und Frühwarnsysteme – z. Z. entstehen z. B. in Deutschland mehrere CERT-Netzwerke (Computer Emergency Response Teams) – müssen auch international vernetzt sein. Hierzu bedarf es geeigneter Absprachen, Regularien und Meldewege – Voraussetzungen, die heute noch nicht existieren. Die EU-Kommission hat sich inzwischen des Themas angenommen, ist aber über erste Studien noch nicht hinaus gekommen. Anders verhält es sich im Bereich der Ermittlung und Strafverfolgung. Hierzu wurde immerhin die *Cybercrime Convention* durch den Europarat verabschiedet. Die Ratifizierung und Umsetzung in nationales Recht wird jedoch noch geraume Zeit in Anspruch nehmen, insbesondere gilt dies für die Harmonisierung von Rechtsnormen in sensiblen Feldern wie die Feststellung von Straftatbeständen, für On-line-Durchsuchungen oder die Datenaufzeichnungen durch Service-Provider.

Noch weniger konkret fassbar sind Maßnahmen im Bereich der Prävention. Vereinzelt werden Stimmen laut, die eine internationale „Cyber-Politik" fordern, die sich mit verbindlichen Regeln im Umgang mit der Informationstechnik befasst, welche z. B. die Nutzung des Internets für internationale Auseinandersetzungen wie Wirtschaftskriege ächten sowie internationale Sicherheitsstandards und allgemeingültige Verhaltensregeln für den Einsatz des Internets in Konflikten festlegen. Ein solcher „Code of Conduct" müsste sich vor allem auch an humanitären Normen orientieren wie etwa dem Schutz lebenswichtiger Basis-Infrastrukturen, u. a. der Wasser- und Energieversorgung und des Gesundheitswesens, auch vor „Cyber-Attacken".

Nationale wie internationale Programme bedürfen aber vor allem zweierlei: einer langfristigen Strategie mit einem entsprechenden politischen Willen zur Umsetzung sowie der Möglichkeit, schnell und flexibel auf Veränderungen in der „Cyber-Welt" reagieren zu können.[13]

12 Vgl. Roger Smitt, Modelling and Simulation Adds Insight on Terrorism, in: Signal, Dezember 2001.

13 Vgl. u. a. Bruce Hoffmann, Terrorismus. Der unerklärte Krieg. Neue Gefahren politischer Gewalt, Frankfurt/M. 2001, S. 281 – 285.