DER SCHUTZ KRITISCHER INFRASTRUKTUREN

UNTER BESONDERER BERÜCKSICHTIGUNG VON KRITISCHEN INFORMATIONSINFRASTRUKTUREN

JAN KUHN

Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle

Institute for Peace Research and Security Policy at the University of Hamburg
Falkenstein 1, 22587 Hamburg
Tel: +49 40 866 077-0 - Fax: +49 40 866 36 15

GRUPPENPROFIL

Die „Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle (IFAR)“ beschäftigt sich mit dem komplexen Zusammenspiel von rüstungsdynamischen Faktoren, dem potenziellen Waffeneinsatz, der Strategiedebatte sowie den Möglichkeiten von Rüstungskontrolle und Abrüstung als sicherheitspolitische Instrumente. Der Schwerpunkt der Arbeit liegt dabei auf folgenden Forschungslinien:

- Grundlagen, Möglichkeiten und Formen von Rüstungskontrolle, Abrüstung und Nonproliferation nach dem Ende des Ost-West-Konfliktes sowie die Entwicklung von anwendungsbezogenen Konzepten präventiver Rüstungskontrolle

- „Monitoring“ der fortschreitenden Rüstungsdynamik und Rüstungskontrollpolitik in Europa und weltweit mit Fokus auf moderne Technologien

- Technische Möglichkeiten existierender und zukünftiger (Waffen-) Entwicklungen, besonders im Bereich Raketenabwehr und Weltraumbewaffnung

Der steigenden Komplexität solcher Fragestellungen wird in Form einer interdisziplinär arbeitenden Forschungsgruppe Rechnung getragen. Die Arbeitsweise zeichnet sich durch die Kombination von natur- und sozialwissenschaftlichen Methoden und Expertisen aus. Durch die intensiven Kooperationen mit anderen Institutionen unterschiedlicher Disziplinen wird insbesondere Grundlagenforschung im Bereich der naturwissenschaftlich-technischen Dimension von Rüstungskontrolle geleistet. Darüber hinaus beteiligt sich IFAR auch an einer Reihe von Expertennetzwerken, die Expertisen aus Forschung und Praxis zusammenführen und Forschungsanstrengungen bündeln.

Die Arbeitsgruppe hat eine langjährige Expertise in den Bereichen kooperative Rüstungssteuerung und Rüstungstechnologien sowie verschiedene wissenschaftlichen Kernkompetenzen aufgebaut. Diese flossen in die international vielbeachteten Beiträge des IFSH zur Rüstungskontrolle ein, so das Konzept der 'kooperativen Rüstungssteuerung' sowie Studien zur konventionellen und nuklearen Rüstung und Abrüstung, zur Bewertung technologischer Rüstungsprozesse, zur strategischen Stabilität, zur strukturellen Angriffs-unfähigkeit sowie zur Vertrauensbildung und europäischen Sicherheit.

IFAR bietet verschiedene Formen der Nachwuchsförderung an. Neben Lehrtätigkeiten gemeinsam mit der Universität Hamburg und im Studiengang 'Master of Peace and Security Studies' können auch Praktika in der Arbeitsgruppe absolviert werden.

Die Arbeitsgruppe kooperiert mit einer Vielzahl von nationalen und internationalen Organisationen.

Kontakt:
Götz Neuneck
Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle IFAR

Institute for Peace Research and Security Policy at the University of Hamburg
Falkenstein 1, 22587 Hamburg
Tel: +49 40 866 077-0 Fax: +49 40 866 36 15
ifar@ifsh.de www.ifsh.de
Webpage zur Rüstungskontrolle: www.armscontrol.de

DER SCHUTZ KRITISCHER INFRASTRUKTUREN

UNTER BESONDERER BERÜCKSICHTIGUNG VON KRITISCHEN INFORMATIONSINFRASTRUKTUREN

Einleitung

> „Critical infrastructures underpin the security of our national wealth, our defense capability, the economic prosperity of the people, and, above all, the maintenance of the system of human rights and individual freedoms for which the United States was founded and has stood since 1776."
>
> *Presidential Commission on Critical Infrastructure Protection*[1]

> „ [...] a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees ."
>
> *Global Organized Crime Project*[2]

Zitate wie das der *Presidential Commission on Critical Infrastructure Protection (PCCIP)* machen deutlich, welche Bedeutung bestimmte, besonders wichtige Infrastrukturen für die Funktionsfähigkeit eines Staates haben können. Die Argumentation des „*Global Organized Crime Project*" weist ferner darauf hin, das Fortschritte der Computertechnologie als Waffe eingesetzt werden könnten. Für einen erfolgreichen Angriff auf die Supermacht USA bräuchte ein Angreifer keine riesige Militärmaschinerie mehr, sondern nur noch ein paar Computer-Spezialisten und ein paar PCs, welche problemlos auf dem freien Markt zu erhalten sind. Diese Angriffe werden durch die überragende Bedeutung bestimmter Infrastrukturen möglich. Die ehemalige Sicherheitsberaterin und jetzige US-Außenministerin Condoleezza Rice brachte es auf den Punkt: „Corrupt those Networks and you disrupt the nation."[3]

Obwohl die Relevanz des Themas in den letzten Jahren zu genommen hat, ist in Deutschland bisher keine öffentliche Diskussion zur Problematik festzustellen. Zwar ist es 1997 zur Gründung der Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS)[4] gekommen, gleichwohl sind spätere Bemühungen nur spärlich. Es gibt zwar am Bundesamt für Sicherheit in der Informationstechnik (BSI) und am Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Referate bzw. Abteilungen, die sich mit dem Schutz Kritischer Infrastrukturen beschäftigen. Gleichwohl sind diese Abteilungen sehr klein (im Falle des BSI unter 10 Personen). Nicht zu verschweigen ist ferner, dass es einige andere Abteilungen in anderen staatlichen Institutionen gibt, die sich aber nur unter anderem mit dem Schutz von Kritischen Infrastrukturen auseinander setzen.[5]

---

1 Presidential Commission on Critical Infrastructure Protection (1997): *Critical Foundations -Protecting America's Infrastructures*, http://www.tsa.gov/public/interweb/assetlibrary/Infrastructure.pdf (08.06.2004).

2 Global Organized Crime Project (1998): *Cybercrime.. cyberterrorism.. cyberwarfare.. : averting an electronic Waterloo*, Washington, D.C., : CSIS Press, S. 2.

3 Rice, Condolezza (2001): *National Security Advisor on Rice on protecting U.S. Infrastructure*, http://www.usembassy.it/file2001_03/alia/a1032210.htm (22.06.2005).

4 Bei der AG KRITIS handelt es sich um eine interministerielle Arbeitsgruppe, welche von der Bundesregierung auf Initiative des Bundesministerium des Inneren gegründet wurde. Ihre Aufgabe besteht im Aufzeigen eventueller Bedrohungsszenarien sowie von Schwachstellen im Bereichen von Infrastrukturen ausfindig zu machen und Lösungsvorschläge zu erarbeiten.

5 Der Entsprechende IT-Stab am Bundesinnenministerium umfasst 50 Leute, aber nur wenige sind dem Schutz Kritischer Infrastrukturen zugeordnet.

Das vorliegende Papier gibt einen Einblick in die Problematik der Kritischen Infrastrukturen unter besonderer Berücksichtigung der so genannten Kritischen Informationsinfrastrukturen (KII) – d.h. Telekommunikations- und Informationsnetzen. Dazu wird zuerst gezeigt, was unter dem Begriff Kritische Infrastrukturen zu verstehen ist. Im **zweiten Kapitel** wird die Situation Kritischer Infrastrukturen anhand der Kritischen Informationsinfrastrukturen dargelegt. Dabei wird darauf verwiesen, dass viele Infrastrukturen, so auch die Informations- und Kommunikations-(IuK)-Netze nicht unter besonderen Sicherheitsaspekten entwickelt worden und ihre jetzige Form eher „natürlich" gewachsen ist. Dieser Mangel an strategischer Planung wirft dadurch unterschiedliche Probleme auf, welche zur Verwundbarkeit entsprechender Infrastrukturen führen. Am Ende des Kapitels wird daher auf die Bedrohungslage und mögliche Akteure eingegangen werden. Der **dritte Abschnitt** gibt einen Ausblick auf staatliche Programme und Dokumente im Bereich des Schutzes von Kritischen Infrastrukturen anhand der USA und Deutschland. Die Staaten wurden ausgewählt, da die USA führend bei dem Schutzes Kritischer Infrastrukturen ist und Deutschland schon alleine aufgrund der sehr verschlossenen Informationspraxis (man denke an das lange versprochene Informationsfreiheitsgesetz) ein interessantes Kontrastland darstellt. Darüber hinaus ist Deutschland zwar ähnlich hoch technisiert, hat aber gleichzeitig einige Entwicklungen der USA, wie die Privatisierung von Infrastrukturen, erst sehr viel später eingeleitet.

1. Definition Kritischer Infrastrukturen

Das Wort „Infrastruktur" stammt eigentlich aus dem Sprachgebrauch der französischen Eisenbahn und bezeichnet dort erdverbundene Einrichtungen mit langer Lebensdauer, wie z.B. Tunnel oder Brücken. In die deutsche (wirtschafts-)wissenschaftliche Diskussion wurde es aus dem Wortschatz der NATO übernommen, in dem es ortsfeste Einrichtungen beschreibt , wie Kasernen oder Tanklager.[6] Im alltäglichen Gebrauch und in der Debatte um Kritische Infrastrukturen ist mit dem Begriff Infrastruktur entgegen der wirtschaftswissenschaftlichen[7] Beschreibungen nicht die gesamte Infrastruktur gemeint, sondern nur bestimmte Teilbereiche. Beispielsweise ist das Verkehrswesen eine Infrastruktur – auch wenn sie nach der oben genannten Definition eigentlich nur ein Teil der Infrastruktur eines Staates ist.

Kritisch wird eine Infrastruktur, wenn ihre Bedeutung für den Staat oder die darin lebende Gesellschaft so weit gestiegen ist, dass der Staat im Falle ihrer Störung nicht mehr funktionieren kann, bzw. wenn durch den Ausfall ein deutlicher Wohlstandsverlust für die Bürger des Staates eintreten würde. Die Definition gibt vor, dass beispielsweise das gesamte Straßensystem als Infrastruktur bezeichnet wird. Es ist allerdings unklar, ob immer eine vollständige Infrastruktur als kritisch bezeichnet werden kann, oder ob auch einzelne Teile derselben eine solche Bedeutung haben, dass ihr Zusammenbruch zu einem Kollabieren oder sehr starken Funktionsstörungen des gesamten Systems Staat führen kann. So kann beispielsweise für die Infrastruktur „Transportwesen" gezeigt werden, dass nur einige wenige Straßen

[6] Frey, René L. (1988): *Infrastruktur*, in: Willie, Albers et al.: Handwörterbuch der Wirtschaftswissenschaft, Albers, Willie et al (Hrsg.), Stuttgart, S. 201.

[7] Wirtschaftswissenschaftlich bezeichnet der Begriff heute den Unterbau oder das Fundament, auf dem wirtschaftliche Transaktionen und Interaktionen zwischen den einzelne Wirtschaftssubjekten stattfinden (Schlag, Carsten-Henning (1999): *Die Bedeutung öffentlicher Infrastruktur für das Wachstum der Wirtschaft in Deutschland*, Frankfurt am Main, S. 15). Eine Definition könnte demnach sein: „...die Gesamtheit aller materiellen, institutionellen und personalen Anlagen, Einrichtungen und Gegebenheiten, die den Wirtschaftseinheiten im Rahmen einer arbeitsteiligen Wirtschaft zur Verfügung stehen" (Joachimsen 1966, zitiert nach Ebd.). Die materiellen Einrichtungen sind mit dem Begriff ‚physische Infrastruktur' gleichzusetzen, die wiederum in zwei Untereinheiten geteilt ist, nämlich die haushaltsbezogene und die wirtschaftsbezogene Infrastruktur. Letztere umfasst die Bereiche Verkehrs- und Nachrichtenwesen, Wasser und Energieversorgung sowie die Abwasserentsorgung (Ebd.: 17).

oder Schienenverbindungen so wichtig sind, dass sie nicht oder nur unzureichend von anderen Wegen oder Knoten ersetzt werden können.[8]

Seit einiger Zeit gibt es bei verschiedenen Regierungen die Bemühung die wahrgenommenen Probleme, welche durch Kritische Infrastrukturen entstehen können, zu beseitigen oder zumindest einzudämmen. Erstaunlicherweise hat Schweden bei der Analyse und Problematisierung von KI eine Vorreiterrolle eingenommen.[9] Dort wurde schon 1979 eine Untersuchung zum Thema „Die Verletzlichkeit der computerisierten Gesellschaft" durchgeführt.[10] Nichts desto trotz sind die USA seit Mitte der 1990er Jahre Vorreiter beim Schutz Kritischer Infrastrukturen. So ist beispielsweise die deutsche Kommission, die sich mit dem Schutz Kritischer Infrastrukturen auseinander setzt, unter anderem als Reaktion auf ihren US-Pendant gegründet worden.[11]

Seit der verstärkten internationalen Beachtung des Schutzes Kritischer Infrastrukturen ist es zu einer erheblichen Ausweitung des Begriffes gekommen.[12] So definierte die Clinton-Administration in der *Executive Order* (EO) 13010:

> „*Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."*[13]

Infrastrukturen, deren Beeinträchtigung einen solchen Effekt haben könnten, wurden in den Bereichen Telekommunikation, Elektrizitätssysteme, Gas- und Öl-Transport und -Lagerung, Banken und Finanzdienstleistungen, Transportsysteme, Wasserversorgung, Rettungsdienste und in der Kontinuität der Regierungsfunktionen gesehen.[14] Unter der aktuellen US-amerikanischen Bush-Regierung werden inzwischen auch die medizinische Versorgung, die Landwirtschaft oder auch nationale Monumente[15] als kritisch für das Überleben der USA bezeichnet.

In Deutschland ist ein Referat des BSI mit dem Schutz der KII beschäftigt, während sich eine Abteilung des BBK mit dem physischen Schutz Kritischer Infrastrukturen auseinander setzt. Das BSI bezeichnet die Infrastrukturen als kritisch, die von Clinton Mitte der 1990er Jahre hervorgehoben wurden, erweitert um die Gesundheits- und Lebensmittelversorgung. Interessant ist, dass die äußere Sicherheit bei der deutschen Definition eher im Hintergrund steht:

> **„Kritische Infrastrukturen** sind Organisationen oder Einrichtungen mit (lebens-) wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Störung für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten. [...]

---

8 Moteff, John / Copeland, Claudia / Fischer, John (2002): *Critical Infrastructures: What Makes an Infrastructure Critical?*, CRS Report to Congress RL 31556, http://www.fas.org/irp/crs/RL31556.pdf (04.06.2004), S. 12.

9 Dunn, Myriam / Wigert, Isabelle 2004: *Sweden*, in: Wenger, Andreas / Metzger, Jan (Hrsg.) (2004): *International CIIP Handbook 2004. An Inventory and Analysis of Protection Policies in Fourteen Countries*, Center for Security Studies, Zürich, S. 157-170, S. 159

10 KRITIS (1999*): Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland*, http://userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html (15.12.2004)

11 Stein, Willi / Ritter, Stefan (2003): *Schutz Kritischer Infrastrukturen – Aktivitäten in Deutschland*, in: <kes> Die Zeitschrift für Informations-Sicherheit, Nr., S. 41-44.

12 Moteff et al., Ciritical Infrastructures, S. 11.

13 Presidential Executive Order 13010 vom 15 Juli 1996, Federal Register Vol. 61, No. 138

14 Ebd.

15 Bush, George W. (2002): *The Department of Homeland Security*, http://www.whitehouse.gov/deptofhomeland/toc.html (22.06.2005), S. 15

> Sind einzelne solcher Infrastrukturen von gezielten Störungen (Information Warfare, terroristische Angriffe etc.) bzw. Ausfällen ihrer Informationstechnik betroffen, könnte dadurch eine Kettenreaktion von Störungen auch in anderen Bereichen ausgelöst werden. Auswirkungen auf die innere Sicherheit und in einigen Fällen sogar die äußere Sicherheit Deutschlands könnten die Folge sein."[16]

Hinter dem Begriff der Kettenreaktion steht die Annahme, dass alle Kritischen Infrastrukturen mehr oder weniger voneinander abhängig sind. Beispielhaft sei die Abhängigkeit der unterschiedlichen Infrastrukturen von IuK-Netzen, sowie der Energieversorgung aufgeführt: Ein Krankenhaus braucht als Teil der Gesundheitsversorgung sowohl Energie für die Versorgung der unterschiedlichen Geräte als auch Kommunikationswege, um Medikamente zu bestellen, Krankenwagen zu koordinieren, etc. Ersichtlich wurde die Abhängigkeit von Kommunikationsmitteln durch den kurzzeitigen Verlust des Kommunikationssatelliten PanAmSat Galaxy IV im Mai 1998. Durch den Ausfall konnten beinah 80% der US-Amerikanischen digitalen Pager nicht mehr erreicht werden, wodurch Bankautomaten nicht funktionierten, aber auch Ärzte und andere Notfalldienste nicht mehr gerufen werden konnten.[17]

Die Informations- und Telekommunikationsinfrastruktur ist dabei offensichtlich von der Energieversorgung abhängig: beispielsweise wird Strom in den Vermittlungsstellen benötigt oder bei der Verstärkung der Lichtwellen in den Langstreckenleitungen. Genauso ist die Energieinfrastruktur von der Kommunikationstechnologie abhängig. Besonders deutlich wurde das während des weiträumigen Stromausfalls in den USA im Sommer 2003. Obwohl der Ausfall nicht durch ein Kommunikationssystem ausgelöst wurde, ermöglichte die Vernetzung der Kontrollstellen eine Kettenreaktion und dadurch zum großflächigen Ausfall erheblich beitrug.[18]

Generell ist es äußerst schwierig über ein Gewichtung in der Bedeutung von einzelnen Infrastrukturen zu urteilen. Beispielhaft wird eine Abwägung hier für die Kommunikations- und die Energieinfrastruktur angeführt: Auf der einen Seite lässt sich argumentieren, dass Energie für einen, wenn auch kurzen, Zeitraum zwischengespeichert werden kann, man denke nur an Notstromversorgungen. Bei Informations- und Kommunikationsverbindungen ist das nicht ohne weiteres möglich.[19] Gleichzeitig ist aber auch anzunehmen, dass Kommunikationsverbindungen zumindest kurzfristig bei den Rettungsdiensten umgangen werden können. Feuerwehren könnten beispielsweise Streife fahren, um Brände zu sichten, falls die Kommunikationsverbindungen ausfallen, wie etwa in der Silvesternacht zum Jahreswechsel 2000 in Berlin. Krankenhäuser könnten sicherlich für kurze Zeit ohne Kommunikationsverbindungen funktionieren, gleichwohl ist allerdings ein bedeutender Effizienzverlust zu vermuten, d.h. es können weniger Kranke versorgt werden oder weniger Brände gelöscht werden, da die Rettungsdienste nicht schnell und zielgenau zur Stelle sein könnenDas der Schutz Kritischer Infrastrukturen Mitte der 1990er Jahre ein so hohe Aufmerksamkeit erfahren hat ist mit der immer stärker werdenden Verbreitung von Computernetzen zu erklären. So waren Infrastrukturen wie das Schienennetz auch schon vor dieser Zeit leicht zu unterbrechen, die inzwischen erreichte Vernetzung wurde erst durch den Einsatz von Computern und den sie verbindenden Kommunikationsnetzen möglich.[20] Aufgrund ihres Charakters erlauben Informationsinfrastrukturen großflächigen elektronischen Angriff auf wichti-

---

16 Definition auf der Internetseite des BSI zum Thema Kritische Infrastrukturen, Hervorhebung im Original; http://www.bsi.de/fachthem/kritis/kritis.htm (06.02.2004)

17 Michel-Kerja, Erwann (2003): *New Challenges in Critical Infrastructures: A US Perspective*, in: Journal of Contingencies and Crisis Management, Jg. 11, Nr. 3: 132-141, S. 134

18 BSI (2004): *Einführung in den Schutz Kritischer Infrastrukturen*, http://www.bsi.bund.de/-fachthem/kritis/kritis_kurz.pdf (15.12.2004), S. 7

19 Westrin, Peter (2001): *Critical Information Infrastructure Protection (CIIP)*, in: Information & Security Bd. 7: S. 67-79, http://www.isn.ethz.ch/researchpub/publihouse/infosecurity/volume_7/b1/B1_index.htm (23.06.2005).

20 Presidental Commission, Critical Foundations, S. 4.

ge Strukturen eines Staates, sowohl von innerhalb des Staatsgebiets als auch von außerhalb, da, zumindest theoretisch, nur einen Telefonanschluss, ein Modem und einen Computer[21] braucht, um Infrastrukturen anzugreifen. Dadurch verschwimmen die Grenzen innerer und äußerer Sicherheit.[22] Aufgrund ihrer spezifischen Eigenschaften[23] und der davon ausgehenden Gefahren beschäftigen sich die staatlichen Studien der 1990er Jahre in der Hauptsache mit Cyberangriffen auf Kritische Infrastrukturen, auch wenn andere Gefahren unter Umständen als ähnlich problematisch für die Funktionsfähigkeit, wenn nicht sogar gefährlicher, zu bewerten sind. Beispiele hierfür sind die Stromausfälle aus dem Jahr 2003 in den USA und Italien. Der wirtschaftliche Schaden war immens. Allerdings wurden die Ausfälle nicht durch Cyberangriffe, sondern durch umstürzenden bzw. zu hohe Bäume ausgelöst.

2. Situationsbeschreibung

Die folgende Analyse der KI beschränkt sich auf die beiden Infrastrukturen *IuK-Netze* und die *Energieversorgung*. Eine Konzentration erfolgt auf diese Infrastrukturen, da sie bei der Funktionsfähigkeit der anderen Infrastrukturen eine herausragende Rolle haben und sich besonders für großflächige Störungen des öffentlichen Lebens eignen. Obwohl Angriffe auf Computersysteme sehr häufig sind und inzwischen auch in der Tagespresse über Computerwurm-Epidemien und ähnliche Vorfälle berichtet wird, sind diese Vorfälle zum größten Teil nicht mit einem Angriff auf Kritische Infrastrukturen in einen Zusammenhang zu bringen. Computerwürmer greifen andere Rechner an und haben zur Zeit noch keine Mechanismen, die KI gefährden könnten.

2.1 Technische Grundlagen

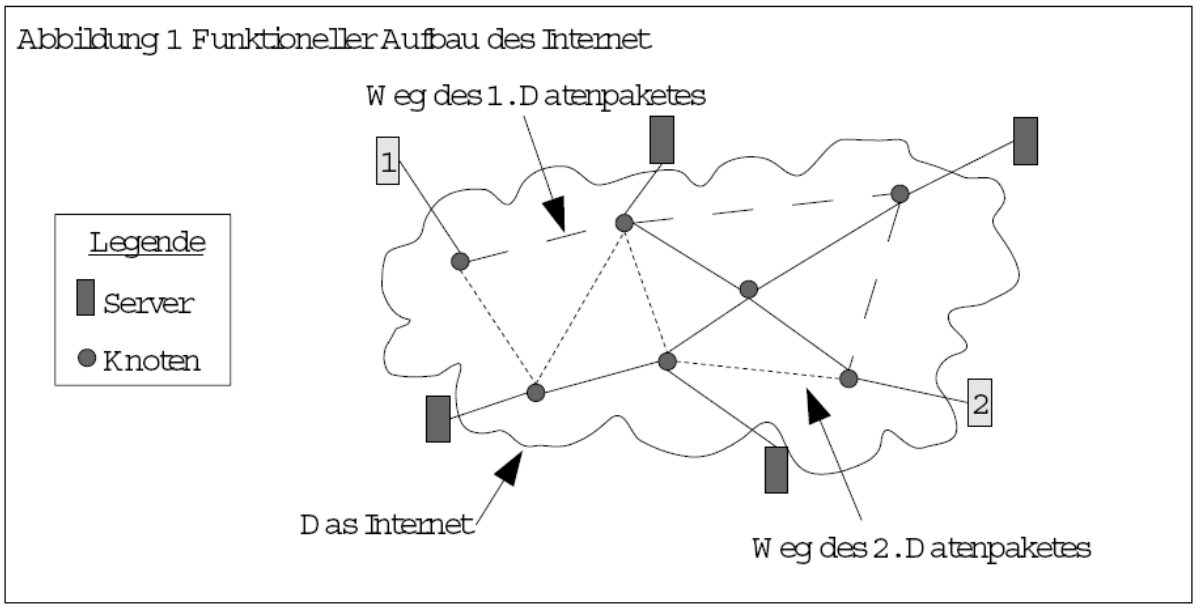
Der Vorläufer des Internets ist in den 1960er Jahren in den USA unter Regie der DARPA[24] entstanden. Über die Gründe für die Entwicklung gibt es unterschiedliche Meinungen: Am häufigsten ist die Argumentation vertreten, dass es zum Schutz von Informationen und Kommunikationsverbindungen bei einem Angriff mit Nuklearwaffen entwickelt wurde. Die Schutzfunktion bestände in der Dezentralisierung von Daten, Datenleitungen und Netzknoten. Das Netz (siehe Abbildung 1) ist so aufgebaut, dass trotz Ausfall einzelner Verbindungen die Daten immer noch ihr Ziel erreichen können. Beim Verschicken werden die Daten dazu in kleine Pakete aufgeteilt, die unterschiedliche Wege durch das Netz nehmen können.

[21] Die Idee ist hier, dass ein potentieller „Angreifer“ sich an seinen Computer setzt und sich mit Hilfe des Telefonnetzes beispielsweise in eine KI einwählt um ihr Schaden zuzufügen.

[22] Odentahl, Hans W. (2003): *Der Schutz kritischer Infrastrukturen*, in: Hirschmann, Kai / Leggemann, Christian (Hrsg.) (2003): *Der Kampf gegen den Terrorismus: Strategien und Handlungserfordernisse in Deutschland*, Berliner Wiss.-Verl., Berlin, S. 292.

[23] Eine Eigenschaft ist die hohe Vernetzung von Strukturen, die wiederum Abhängigkeiten hervorruft.

[24] DARPA steht für „Defense Advanced Research Projects Agency“. Die Organisation ist die zentrale Forschungs- und Entwicklungseinheit des US-amerikanischen Verteidigungsministeriums.



Kommuniziert beispielsweise Server 1 mit Server 2, kann ein Datenpaket über mindestens fünf verschiedene Verbindungen übertragen werden. Noch dazu kann ein erstes Datenpaket über einen anderen Weg übertragen werden als das zweite. Es gibt also keine direkte Verbindung zwischen zwei Teilnehmern wie etwa bei Telefonnetzen. Gerade durch diese Art der Übermittlung in Form von Paketen kann nur sehr schwer festgestellt werden, woher die Daten kommen, die teilweise durch mehrere Staaten übertragen werden, bis sie ihr Ziel erreichen. Diese Redundanz des Übertragungsweges ist die wesentliche Stärke des Internet, da es ein gewisses Maß Sicherheit vor physikalischen Angriffen oder auch Ausfällen bietet.

Ein inhärenter Schwachpunkt der zugrunde liegenden Technik ist, dass sie für Umgebungen entwickelt wurde in denen allen Nutzern getraut werden konnte, da das Netz nur vom Militär und der Wissenschaft genutzt wurde.[25] Die Protokolle, die heute immer noch für die Übertragung der Pakete sorgen, stammen aus eben jenen Tagen und sind aus diesem Grunde zwar auf die eben angesprochene Robustheit, aber nicht auf andere sicherheitstechnische Aspekte ausgelegt.

Das hat mehrere Implikationen: Zum einen ist nicht garantiert, dass der Absender, welcher in dem Datenpaket steht, auch wirklich der Absender ist. Zweitens ist die Integrität der Daten nicht gewährleistet. Ein Angreifer kann ein Datenpakete abfangen und seinen Inhalt ändern, wodurch ggf. andere Informationen bei dem intendierten Empfänger ankommen. Drittens ist keine Vertraulichkeit der Daten gegeben. Jeder, der die Fähigkeiten dazu hat, kann die Datenpakete für sich kopieren und somit an ihre Inhalte gelangen. Viertens kann der Absender im Nachhinein die Authentizität der Daten bestreiten, da die Daten oder die Absenderangabe möglicherweise verfälscht wurde.

Für Angriffe auf IuK-Netze bedeutet das, dass ein System nicht erkennen kann, ob die ankommenden Befehle wirklich vom angegebenen Absender kommen. Hinter den Befehlen kann entweder ein Techniker stehen, der das betroffene System warten soll, oder ein Akteur, der eigentlich keinen autorisierten Zugang zu dem System hat. Werden Passwörter zu dem zu steuernden System übertragen, kann jemand versuchen, diese mitzulesen und sich dann später selber zu dem System Zugang gewähren. Dadurch, dass die Integrität der Daten nicht gewährleistet ist, kann ein Akteur die Datenpakete abfangen und deren Inhalt verändern – es können so andere Steuerungsbefehle bei dem System ankommen als gedacht. Allerdings müssen dazu

[25] Charney, Scott (2000): *The Internet, Law Enforcement and Security*, Papier in der Serie „Birefing the President", Internet Policy Institute, http://www.first.org/events/progconf/2002/d5-01-charney-paper.pdf (03.06.2004), S. 1.

alle Pakete abgefangen werden, da die Informationen über mehrere Datenpakete verteilt sein können und eine Integritätsüberprüfung[26] der Daten sonst scheitern könnte.

2.2. Verwundbarkeit

Wenn über die Sicherheit von Kritischen Infrastrukturen und Kritischen Informationsinfrastrukturen gesprochen wird, dreht sich die Argumentation meist nur um die Verwundbarkeit von Rechnersystemen. Diese sind verwundbar, da es keine „Security Policies“[27], nicht genügend Sicherheitstraining für Systemadministratoren und fehlerhafte Software gibt.[28] Es wird nur selten explizit ein Zusammenhang zwischen derartigen, allgemeinen Sicherheitsproblemen und Sicherheitslücken der KII hergestellt. Deshalb ist unklar, ob die bekannten Verwundbarkeiten von Rechnersystemen einen Einfluss auf die Verwundbarkeit von Kritischen (Informations-) Infrastrukturen haben.

2.2.1. Planspiele & Simulationen

In unterschiedlichen Staaten hat es Planspiele und Simulationen gegeben, welche Auskünfte über die Verwundbarkeit Kritischer Infrastrukturen liefern sollten. Zuerst ist hier die Übung „Eligible Receiver“ zu nennen, die 1997 vom US-amerikanischen Verteidigungsministerium durchgeführt wurde. Angestellte der *National Security Agency* (NSA) betätigten sich dabei als Hacker und griffen mit Software, welche frei über das Internet verfügbar ist, Rechnernetzwerke des Verteidigungsministeriums, aber auch das Stromnetz über das Internet an. Die genauen Ergebnisse der Übung sind nicht bekannt, allerdings sind immer wieder bruchstückhaft Teilergebnisse an die Öffentlichkeit gelangt. So sagte beispielsweise der US Senator Kyl in einem Interview 1998:

> „ [...] "Eligible Receiver," demonstrated in real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by, literally, hackers – people using conventional equipment, no "spook" stuff in other words. Just that which is available can disrupt key aspects of our information infrastructure. Now, in this case, they disrupted parts of the electric grid, the transportation system, the financial systems.”[29]

Eines der Teilergebnisse von „Eligible Receiver“ ist, dass nur ein Bruchteil der Administratoren der angegriffenen Systeme den Vorfall meldete, der Rest schien gar nicht bemerkt zu haben, dass Angreifer in ihr Netzwerk eingedrungen waren. Während der Übung gelang es den NSA-Mitarbeitern nach Aussage von Mitarbeitern des Verteidigungsministeriums, in das Stromsystem der Vereinigten Staaten einzudringen. Sie hätten danach theoretisch überall in den USA den Strom ausschalten können:

> „The attacks were not actually run against the infrastructure components because we don't want to do things like shut down the power grid, but the referees were shown

[26] Dabei geht es wohlgemerkt nicht darum zu prüfen, ob die Daten, die bei dem Empfänger ankommen die gleichen sind, die beim Sender verschickt wurden. Vielmehr müssen die Pakete logisch zueinander passen.

[27] Eine Security Policy ist ein Dokument eines Unternehmens, in dem die Verfahrensweisen und Regeln in Bezug auf die Rechnersicherheit des Unternehmens festgelegt werden.

[28] Wilson, Clay (2003) *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues*, CRS Report to Congress RL 32114, URL: http://www.fas.org/irp/crs/RL32114.pdf (04.06.2004), S. 5

[29] Interview mit Senator John Kyl, *information warfare threat demands more attention on all sides*, in: U.S. Foreign Policy Agenda, USIA Electronic Journal, Vol. 3, Nr. 4, November 1998, http://www.fas.org/irp/threat/cyber/docs/usia/pj48kyle.htm (23.06.2005).

> the attacks and shown the structure of the power-grid control, and they agreed, yeah, this attack would have shut down the power grid."[30]

Solchen Aussagen ist mit Vorsicht zu begegnen, da keine Belege seitens des Pentagon vorgebracht wurden (Smith 1998: 5/6). Auf der einen Seite mag eine Nichtveröffentlichung von Verwundbarkeiten aus Gründen der Sicherheit richtig sein. Auf der anderen Seite können die Behauptungen dadurch nicht einer wissenschaftlichen Untersuchung unterzogen werden. Somit ist nicht eindeutig festzustellen, ob es wirklich möglich ist, das US-amerikanische Stromnetz auszuschalten, oder ob es einfach im Interesse des Verteidigungsministeriums ist, Angst zu verbreiten, um mehr Gelder für den „Schutz" des Landes zu erhalten.[31]

Das eigentliche Ziel der NSA-Hacker war angeblich das US-amerikanische Pazifische Kommando. Sie hatten den Auftrag, einen Truppenaufmarsch der USA gegen Nord-Korea zu verhindern. Die Aufgabe konnte innerhalb von zwei Wochen ausgeführt werden, indem die Kommando- und Kontrollfähigkeiten der USA praktisch lahm gelegt wurden. Nach einem Bericht der Washington Times erfolgten Angriffe dabei nur gegen nicht klassifizierte Systeme des Pentagon, die einen erstaunlich niedrigen Sicherheitsstandard zu haben schienen. So war das Passwort, um Zugang zu den Systemen zu erlangen, manchmal einfach „password".[32]

Nimmt man ungeachtet der Fragwürdigkeit der vorliegenden Informationen an, dass ein Angriff auf die Energieversorgung möglich ist, kann dennoch nicht automatisch geschlossen werden, dass jeder ohne spezielle Kenntnisse dazu in der Lage wäre, auch wenn Senator Kye sagt, dass bei der Übung nur normale Software eingesetzt wurde. So ist die NSA für die Sicherheit der US-amerikanischen Regierungskommunikation sowie für die Entschlüsselung der Kommunikation fremder Regierungen zuständig. Die Hacker, welche bei der Übung eingesetzt wurden, mögen also keinen „spook stuff"[33] genutzt haben, es ist aber davon auszugehen, dass sie auf ihrem Gebiet exzellent ausgebildete Spezialisten sind, wodurch sie sowohl die Schwachstellen von unterschiedlichster Software kennen als auch die normalen Fehler, die ein Administrator begehen kann. Nimmt man weiter an, dass Administratoren nicht immer die bestbezahlten Mitglieder einer IT-Abteilung sind[34] und dass weiterhin die Regierung traditionell in Konkurrenz mit der freien Wirtschaft um die besten Leute zu kämpfen hat[35], treffen zwei unterschiedliche Extreme aufeinander: sehr gut ausgebildete Personen auf der einen Seite und mögliche Schwächen auf der anderen Seite. Ein normaler Angreifer kann die Schwächen auf Seite der Netzwerkadministratoren natürlich auch ausnutzen, wobei inzwischen zumindest die Passwörter etwas besser geworden sein dürften. Es ist aber zumindest zu hinterfragen, ob er immer das gleiche Know-How hat wie die NSA-Angestellten. Deshalb kann nicht davon ausgegangen werden, dass es besonders kostengünstig und einfach ist, das US-amerikanische Stromnetz über das Internet auszuschalten.

Eine Übung mit einem ähnlichen Ziel wie „Eligible Receiver" hat auch in Deutschland 2001 unter dem Namen CYTEX (Cyber Terror Exercise) stattgefunden. Unter der Schirmherrschaft der Industrieanlagen- und Betriebsgesellschaft (IABG) wurde ein Planspiel unter

---

30 zitiert nach Gertz, Bill (1998): *Computer hackers could disable military*, in: Washington Times, 16. April 1998, http://www.newdimensions.net/headlines/m02.htm (07.05.2004).

31 Man könnte sich auch Vorstellen, das Eligible Receiver eine Art Verschwörungsgeschichte ist, welche nur aufzeigt, dass die Medien sehr unkritisch im Bereich der Bedrohung von Kritischen Informationsinfrastrukturen recherchieren, wodurch es den Verteidigungsministerien sehr viel einfacher fallen würde, die KII als Vorwand für Kompetenzausweitung verwenden. Siehe hierzu auch Crypt Newsletter der Northern Illinois University: http://www.soci.niu.edu/~crypt/other/eligib.htm (09.06.2004).

32 Gertz, Computer hackers could disable military.

33 Der von Kyl benutzte umgangssprachliche Ausdruck „spook stuff" bedeutet sinngemäß übersetzt etwas ähnliches wie „Dinge, die von Spionen benutzt werden".

34 Nelson, Bill / Choi, Rodney / Iacobucci, Michael et all (1999): *Cyberterror Prospects and Implications, White Paper*, Center for the Study of Terrorism and irregular Warfare, Naval Postgradute School, http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf (04.06.2004), S. 98.

35 Smith, George (1998): *An Electronic Pearl Harbor? Not Likely,* in: Issues in Science and Technology Online, Herbst 1998, http://205.130.85.236/issues/15.1/smith.htm (12.11.2003).

Beteiligung von staatlichen Organisationen und privaten Unternehmen durchgeführt.[36] In der Übung wurde ein IT-Angriff von Globalisierungsgegnern auf die KI im Raum Berlin simuliert. Dort sollte, so das Szenario des Planspieles, eine internationale Konferenz unter Leitung der Bundesregierung, stattfinden. Mit den Angriffen sollte erreicht werden, dass das öffentliche Leben in Berlin zusammenbricht, wodurch die Konferenz erzwungenermaßen abgebrochen werden müsste. Außerdem sollte laut Szenariobeschreibung die Regierung erpresst werden, inhaftierte Mitglieder der angreifenden Gruppe aus ihrer Haft zu entlassen.[37]

Ähnlich wie im Falle „Eligible Receiver" sind nur Ergebnisse veröffentlicht, die Unterlagen des Planspieles selbst stehen unter Verschluss. Deshalb kann man bei der Sichtung der Veröffentlichungen zu dem Planspiel zu unterschiedlichen Schlüssen kommen. Rainhard Hutter, Mitarbeiter der IABG, kommt beispielsweise zu folgendem Ergebnis:

> „Durch Informationsangriffe lassen sich die gesamte Infrastruktur und damit das öffentliche Leben, die Funktionsfähigkeit der betroffenen Wirtschaftszweige und die politische Handlungsfähigkeit massiv in die Knie zwingen. Nach und nach brechen Telefonverkehr, Transaktionsfähigkeit von Banken, Energie, Straßen-, Schienen- und Luftverkehr zusammen. Großveranstaltungen müssen abgesagt werden, es kommt zu Panikreaktionen und erheblichen wirtschaftlichen Schäden – und – es gab keine Zweifel, dass ein derartiges Szenario machbar ist und so oder ähnlich real eintreten kann."[38]

Durch solche Äußerungen wird suggeriert, dass auch die Kritischen Infrastrukturen in Deutschland verwundbar sind und dass die Verwundbarkeit ausgenutzt werden kann, um die Sicherheit Deutschlands massiv zu gefährden. Zu einem ganz anderen Schluss gelangt man, wenn unterstellt wird, dass die in der Übung vorgenommenen IT-Angriffe als erfolgreich vorgegeben waren und daher nur die Auswirkungen solcher Angriffe auf Entscheidungsträger und Infrastrukturen simuliert wurde.[39] Die Schlussfolgerung aus der Übung ist dann nicht, dass die Verletzlichkeit von Kritischen Infrastrukturen gegeben ist, sondern dass unter der Voraussetzung, dass sie gegeben ist und dass sie durch einen Akteur ausgenutzt werden kann, die unterschiedlichen Krisenstäbe noch nicht optimal zusammen arbeiten können und dass in diesem Bereich Nachholbedarf besteht. Des Weiteren ist darauf hinzuweisen, dass die Panikreaktionen in der Übung angenommen wurden. Betrachtet man allerdings Erfahrungen mit den Stromausfällen im Sommer 2003 in den USA, Italien und Dänemark, wird deutlich, dass die Ausnutzung einer Verwundbarkeit, die zu bestimmten Ereignissen (dem Ausfallen des Stroms) führen könnte, nicht unbedingt die in der Übung angenommenen Auswirkungen – eine Panikreaktion der Bevölkerung – haben muss.

Beide Übungen, „Eligibe Receiver" und „CYTEX", sollen der Öffentlichkeit glaubhaft machen, dass die Kritischen Infrastrukturen des Landes angreifbar sind und dass ein Angreifer dieses ausnutzen kann, um entweder den Strom im ganzen Lande abzuschalten oder öffentliche Panik zu verursachen. Die Abschaltung des Stroms würde dazu führen, dass kein System der modernen „Informationsgesellschaft" mehr funktioniere. Obwohl es verständlich ist, dass nicht veröffentlicht werden kann, wie die Angriffe ausgeführt wurden, führt die Ge-

---

[36] Folgende Institutionen waren beteiligt: das BSI, das Bundesministeriums für Wirtschaft, das Bundesverteidigungsministeriums, die Bundesakademie für Sicherheitspolitik, die Telekom, die Deutschen Flugsicherung, die Deutschen Bahn Verkehr, die Polizei, die Bundesanstalt Technisches Hilfswerk, ein Energieversorger, der Technische Überwachungsverein und Vertreter der Großindustrie. Vgl. Hutter, Reinhard (2002): *Cyber Terror – eine realistische Gefahr*, In: Das Parlament, 8. März 2002, http://www.aksis.de/Hutter-Cyber-Terror.pdf (04.06.2004), S. 14.

[37] Hess, Sigurd (2003): *Informationssicherheit und Schutz kritischer Infrastrukturen*, http://www.dmkn.de/1779/technologie.nsf/D9F02C2A100B89D7C1256CD80037695B/$File/itsicherheit.pdf (03.06.2004), S. 7.

[38] Hutter, Cyber Terror, S. 15.

[39] Hess, Informationssicherheit, S. 7.

heimhaltung dazu, dass die behaupteten Ergebnisse nicht überprüfbar sind. Im Rahmen von CYTEX wird deutlich, dass bestimmte Vorbedingungen, wie z.B. dass die Cyberangriffe erfolgreich waren, nicht genannt werden, wodurch wiederum die Verwundbarkeit nicht richtig dargestellt wird. Aus den Informationen, die verfügbar sind, lässt sich nur schließen, dass eine Verwundbarkeit nicht bewiesen ist oder dass sie, falls es sie wirklich gibt, erst einmal nur von hoch spezialisierten Experten ausgenutzt werden kann.

Diese Überlegungen werden von einem anderen US-amerikanischen Planspiel mit Namen „Electronic Pearl Harbor", welches 2002 durchgeführt wurde, bestätigt. In der vom US Naval War College zusammen mit der Gartner Group veranstalteten dreitägigen Übung testeten Spezialisten Rechnerangriffe auf KI. Das Ergebnis war, dass Angriffe sehr wahrscheinlich wenig erfolgreich sind, da sie beispielsweise dann, wenn sie gegen SCADA-Systeme von Energieversorgern gerichtet sind, meist nur zu kurzen Unterbrechungen der Stromversorgung führen würden. Darüber hinaus würde ein großer Angriff 200 Millionen US-Dollar kosten und eine Vorbereitungsphase von mehreren Jahren benötigen.[40] Wiederum sind keine genauen Einzelheiten zu diesem Planspiel bekannt. Allerdings widerspricht sie der Grundthese von leicht durchzuführenden, kostengünstigen Angriffen mit katastrophalen Konsequenzen vollständig.

2.2.2. Reale Vorfälle

Neben gezielten Übungen werden Schwachstellen in der mit Rechnersystemen vernetzen KI durch Rechnerwürmer deutlich. Während medienwirksame Ereignisse wie der „I Love You"-Wurm oder „Mellissa" „nur" wirtschaftlichen Schaden angerichtet haben, verbreiteten sich im Jahr 2003 Würmer im Internet, die Auswirkungen auf Elemente der KI hatten.

Der W32/SQLSlammer.worm (auch bekannt unter dem Namen W32/Sapphire.worm) begann sich am 25. Januar 2003 um 5:30 Uhr (UTC) zu verbreiten. Im Gegensatz zu vorangegangenen Würmern schaffte er es, das gesamte Internet innerhalb von wenigen Minuten in Mitleidenschaft zu ziehen. Dabei nutzte er eine Schwachstelle in dem von der Firma Microsoft hergestellten SQL Datenbankserver aus. Diese Schwachstelle war auch in der in anderen Programmen eingebetteten Version vorhanden und wurde dementsprechend auch dort angegriffen. Dadurch waren nicht nur Serversysteme, sondern auch Arbeitsplatzrechner vom Wurm betroffen.[41] Seine hohe Ausbreitungsgeschwindigkeit erreichte er, da er nur durch die Bandbreite des Netzwerkanschlusses der infizierten Rechner begrenzt wurde. Des Weiteren war der Wurm so klein, dass er in ein einziges Datenpaket passte, wodurch jedes vom Rechner ausgesandte Paket eine andere Adresse enthalten konnte. An sich war der Wurm nicht gefährlich, da er keinerlei Schadroutinen enthielt und durch einfaches Neustarten des betroffenen Rechners entfernt werden konnte (er war nur im Speicher der betroffenen Rechner vorhanden und nicht als Datei auf der Festplatte). Was den Wurm problematisch machte, war die Tatsache, dass er die gesamte Netzwerkbandbreite von Organisationen aufbrauchte und sämtlichen anderen Netzwerkverkehr damit unterband. Des Weiteren ist es wichtig anzumerken, dass der Wurm ein nicht sehr weit verbreitetes Programm als Ziel nutzte und es dennoch schaffte, Teile des Internets komplett zu blockieren. Hätte er ein „wichtigeres" Dienstprogramm angegriffen, wäre es schwieriger gewesen den Wurm zu stoppen. Zwar hätte durch eine einfache Zugriffssperre auf den Dienst sich der Wurm nicht mehr weiterverbreiten können, allerdings der Dienst auch nicht mehr genutzt werden können, wodurch ggf. schwerwiegendere Folgen aufgetreten wären. So hätte ein Angriff auf den Dienst (HTTP), der Internet-

[40] Wilson, Computer Attack and Cyber Terrorism, S. 9.

[41] Es muss angemerkt werden, dass der SQL-Datenbankdienst nicht zu den Diensten gehört, die immer von außen erreichbar sein müssen. Für das Gros der Anwendungsfälle muss nur intern auf den Dienst zugegriffen werden. Außerdem ist er im Vergleich zu Diensten wie http (zur Auslieferung von Internetseiten), ftp (zur Auslieferung von Dateien) und smtp (für den Versand von E-Mail) nicht sehr weit verbreitet.

seiten ausliefert, dazu geführt, dass unter anderem Firmen keine Geschäfte über Internetportale hätten abwickeln können.[42]

Die Auswirkungen auf Komponenten Kritischer Infrastrukturen bestanden darin, dass einige Kontrollen oder Dienste nicht mehr wahrgenommen oder angeboten werden konnten, da sie über die überlastet Netzwerke hatten abgewickelt werden müssen. Eine solche Überlastung betraf das US-Kernkraftwerk „Davis Besse". Der Wurm konnte in das Rechnernetzwerk eindringen, welches für die Kontrolle des Kraftwerkes genutzt wurde, wodurch das Sicherheits-Parameter-Anzeige-System (SPDC) für fünf Stunden nicht mehr nutzbar war.[43] Nach einiger Zeit fiel noch ein zweites System aus, welches allerdings nicht so kritisch ist wie dass SPDC. Das Kraftwerk war seit 2002 nicht mehr in Betrieb, so dass es zu keinen problematischen Auswirkungen kam. Außerdem fiel zwar das rechnergesteuerte System aus, die analogen Systeme funktionierten aber weiterhin, so dass auch bei aktiver Nutzung des Kraftwerkes keine schwerwiegenden Schäden zu erwarten gewesen wären. Der Ausfall hatte nur zur Folge, dass die Arbeit der Operatoren erschwert wurde.[44]

Der SQLSlammer Wurm konnte in das Kraftwerk eindringen, da neben dem aufgrund von Sicherheitsaspekten problematischen Zugang zum administrativen Netzwerk noch ein weiterer Zugang zum Kontrollsystem des Kraftwerkes bestand, welcher nicht durch Schutzvorkehrungen gesichert war. Dieser bestand über einen nicht genannten Zulieferer des Kraftwerkes. Er wurde nicht beobachtet und das Wissen über ihn war anscheinend nur bei einigen und nicht bei allen Mitarbeitern der IuK-Sicherheitsabteilung vorhanden.[45]

Neben dem Kraftwerk ist 2003 auch bekannt geworden, dass Geldautomaten durch Würmer bedroht sind. So führte W32/SQLSlammer.worm dazu, dass 13.000 Geldautomaten der „Bank of America" durch den Wurm für einige Stunden nicht betrieben werden konnten.[46] Außerdem werden in Geldautomaten inzwischen Windows-Betriebssysteme installiert, um dem Benutzer mehr Komfort zu bieten. Dieses hat aber zur Folge, dass die Automaten durch die gleichen Angriffe verwundbar sind wie normale PCs. Ein weiteres Beispiel sind die Geldautomaten der Firma Diebold, welche im August 2003 von einem zu der Zeit grassierenden Wurm befallen und der Wurm durchsuchten danach, von den Geldautomaten ausgehend, das Netzwerk, in das sie eingebunden waren, nach anderen Rechnern, die verwundbar gewesen wären. Der erzeugte Verkehr löste eine Schutzmaßnahme aus, wodurch die Geldautomaten automatisch vom Netz getrennt wurden – und damit auch nicht mehr benutzt werden konnten. Von dem Vorfall waren zwei unterschiedliche Bankinstitute betroffen.[47] Dass sich ein Ausfall oder zumindest eine drastische Verlangsamung von Abläufen auch ohne einen erfolgten Angriff eines Wurmes ereignen kann, hat sich bei der deutschen Postbank in der Woche nach dem 1. Mai 2004 gezeigt. Aus Angst vor dem Wurm „Sasser" wurden die Firewallregeln verschärft, wodurch die Filialen nicht mehr mit der Zentrale kommunizieren konnten.

Die Beispiele zeigen drei unterschiedliche Teilaspekte der Verwundbarkeit von Kritischen Informationsinfrastrukturen und Kritischen Infrastrukturen, welche von IuK-Netzen abhängen: *Erstens* gibt es Verbindungen zwischen unterschiedlichen Netzen, die auf der einen Seite nicht erwartbar sind und die auf der anderen Seite nur relativ wenigen Menschen be-

---

42 Moore, David / Vern Paxson / Stefan Savage / Colleen Shannon / Stuart Staniford / Nicholas Weaver (2003): *The Spread of the Sapphire/Slammer Worm*, http://www.cs.berkeley.edu/~nweaver/sapphire/ (05.06.2004); Graham, Robert (2003): *Advisory: SQL slammer*, http://www.robertgraham.com/journal/ 030126-sqlslammer.html (05.06.2004).

43 Busch, C. / Wolthusen, S. D. (2003): *Information Warfare: Threats to Critical Infrastructures*, in: Proceedings of the XV International Amaldi Conference of Academies of Science and National Scientific Societies on Problems of Global Security (Helsinki, Finland, Sept. 2003), http://www.wolthusen.com/publications/Amaldi2003.pdf (03.06.2004), S. 2.

44 Poulsen, Kevin (2003): *Slammer worm crashed Ohio nuke plant network*, in: SecurityFocus, 19. August 2003, http://www.securityfocus.com/news/6767 (05.06.2004).

45 Ebd.

46 Krebs, Brian (2003): *Internet Worm Hits Airline, Banks*, in: Washington Post, 26. Januar 2003, http://www.washingtonpost.com/ac2/wp-dyn/A46928-2003Jan26 (05.06.2004).

47 Poulsen, Kevin (2003b): *Nachi worm infects Diebold ATMs*, in: SecurityFocus, 24. November 2003, http://www.securityfocus.com/news/7517 (25.11.2003).

kannt sind. Solche Verbindungen vom Internet sind auch zu sicherheitsrelevanten Netzen vorhanden, zumindest in den USA. Durch sie wäre es für einen Angreifer möglich, Kontrolle über bestimmte, kritische Funktionen zu erhalten und wichtige Dienste ggf. abzuschalten. Dazu benötigt ein Angreifer neben sehr einfach zu beschaffender Hardware, wie zum Beispiel einem Rechner und einem Modem, vor allem Wissen. Zwar mag es erschreckend sein, dass ein Wurm, welcher keine intelligente Funktionen in seinen Programmroutinen hat, in das Steuerungsnetzwerk eines Atomkraftwerkes gelangen kann oder Zugriff auf Geldautomaten erhält. Daraus zu schließen, dass solche Angriffe einfach wäre, ist aber nicht ganz unproblematisch. Wie oben angeführt hat SQLSlammer innerhalb kürzester Zeit das gesamte Internet gescannt. Die Geschwindigkeit basierte unter anderem darauf, dass er sich nicht darum „kümmerte“, ob eine Antwort vom abgefragten Ziel kam. Ein menschlicher Angreifer, der gezielt in den Steuerungsrechner des Atomkraftwerks hätte einbrechen wollen, dürfte es sehr viel schwerer haben, in solche „interessanten“ Netze einzudringen, da er sie erst einmal finden müsste. *Zweitens* muss ein Angreifer gar nicht in ein System wirklich eindringen, um bestimmte Funktionen der Infrastruktur außer Kraft zu setzen. Gelingt es, die Verbindungswege beispielsweise mit Datenschrott zu überfluten, können reguläre Dienste nicht mehr erreicht werden, was dazu führen kann, dass Informationen von entfernten Stellen nicht mehr ausgelesen werden können, wodurch wiederum keine Steuerungsmöglichkeiten mehr bestehen. Um einen solchen Effekt zu erzielen, muss allerdings zumindest das gesamte anzugreifende Netz überflutet werden oder das komplette Internet. *Drittens* wird anscheinend immer häufiger das sehr weit verbreitete Windows-Betriebssystem auch in wichtigen Komponenten von KI genutzt. Obwohl „Patches“[48] für bekannte Sicherheitslücken in Systemen zum Teil schnell bereit gestellt werden können, werden sie nicht immer schnell genug eingespielt, wodurch sich weit verbreitete Sicherheitslücken auch in diesen Komponenten auftun.

Eine hohe Bedeutung für die Verwundbarkeit Kritischer Infrastrukturen gegenüber Computersystemen wird den so genannten „Supervisory Control and Data Acquisition” (SCADA)-Systemen zugeschrieben. Die Systeme (siehe Abbildung 2) werden sowohl im Bereich der Elektrizitätserzeugung und Kontrolle genutzt, als auch bei der Wasserversorgung oder im Telekommunikationssektor. Diese kleinen Rechner werden verwendet, um Informationen über bestimmte Einheiten innerhalb einer Fabrik oder eines weit verbreiteten Versorgungsnetzes zu erhalten oder bestimmte Abläufe zu steuern, sei es das Öffnen eines Ventils oder das Starten einer Pumpe.[49] Ein Beispiel für die Einschätzung der Bedeutung von SCADA-Systemen liefert der US-amerikanische Senator Adam Putnam, Vorsitzender des „Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census“ nach einer Anhörung im Frühjahr 2004:

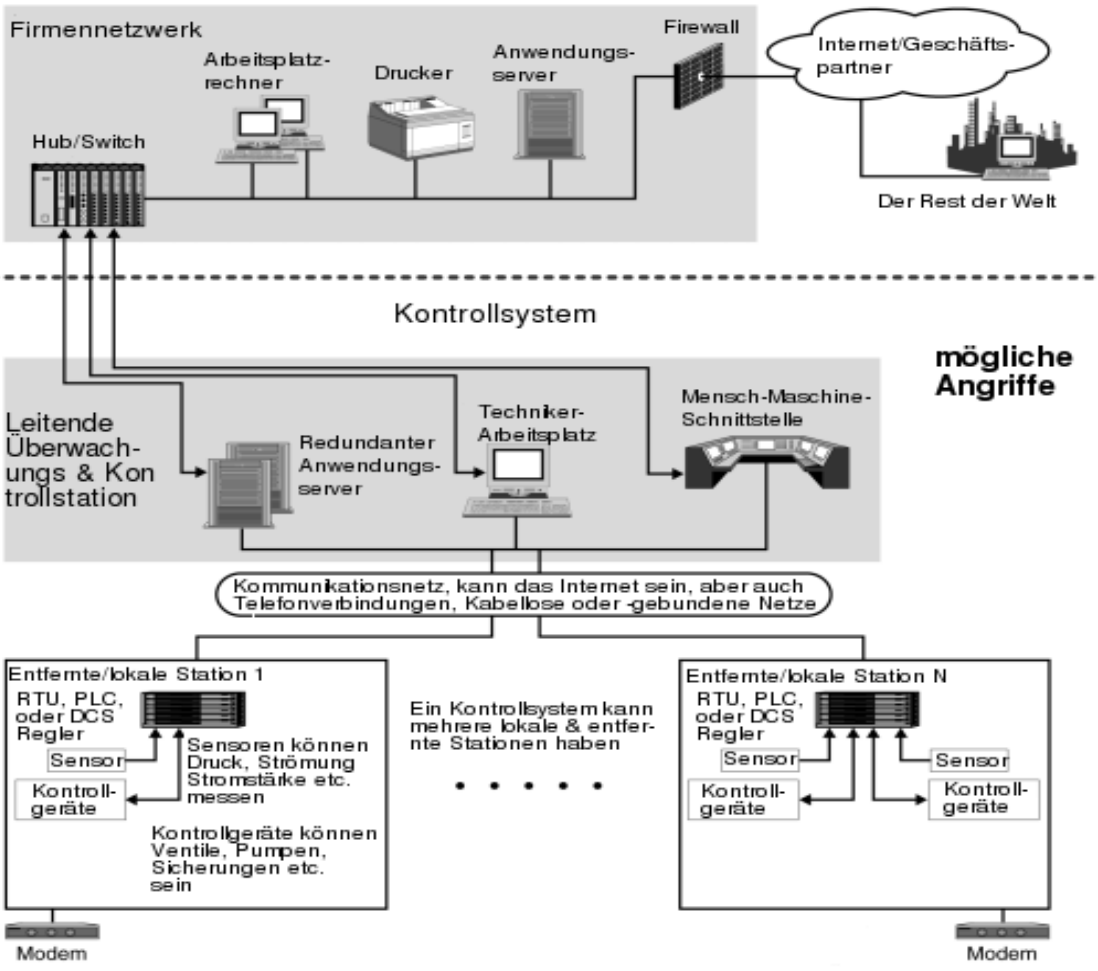
> „The more I've learned [about the lack of SCADA system security], the more concerned I've become. I've learned that today's SCADA systems have been designed with little or no attention to computer security. Data are often sent as clear text; protocols for accepting commands are open, with no authentication required; and communications channels are often wireless, leased lines or the internet.”[50]

[48] Ein „patch“ ist kleines Stück Programmcode, welches in existierende Programme eingefügt werden kann, um Sicherheitslücken oder andere, erst nach Veröffentlichung der Software bekannt gewordene Probleme, auszubessern.

[49] Shea, Dana A (2003): *Critical Infrastructure: Control Systems and the Terrorist Threat*, CRS Report for Congress RL31534, http://www.fas.org/irp/crs/RL31534.pdf (04.06.2004), S. 2.

[50] zitiert nach Verton, Dan (2004): *Industrial Control Systems Seen as 'Undeniably Vulnerable'*, in: ComputerWorld, 31. März 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,91790,00.html (07.06.2004)

Abbildung 2: SCADA Systeme



Nach GAO 2003[51]

Ob SCADA-Systeme sich eignen, als Ziel von Angriffen auf Kritische Infrastrukturen zu dienen, gilt als umstritten.[52] Während gerade von Rechnerexperten mit der technischen Verwundbarkeit argumentiert wird, vergleichen andere die Debatte mit der Diskussion, wie sie Anfang des 20. Jahrhunderts über Luftkriegsführung schon einmal geführt wurde.[53] Im Folgenden wird nur auf die technischen Aspekte eingegangen, da durch sie die Verwundbarkeit von KII erst entstehen.

Technisch begründet sich die Verwundbarkeit solcher Systeme damit, dass sie in großem Umfang eingesetzt werden, meist über Rechnernetze oder zumindest Einwahlzugänge gesteuert sind und über relativ niedrige Sicherheitsvorkehrungen verfügen. Prinzipiell lassen sich zwei unterschiedliche Kategorien bilden (Stamp et al 2003: 9):

---

51 GAO (2003): *Critical Infrastructure Protection - Challenges in Securing Control Systems*, http://www.gao.gov/cgi-bin/getrpt?GAO-04-140T (08.06.2004).

52 PBS (2003): *Cyberwar! Frontlines, vulnerabilites*, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/scada.html (09.05.2004).

53 In den 1920er Jahren fand die Idee großen Anklang, dass man alleine mit strategischen Bombardement gegen militärische und zivile Ziele den Gegner zur Aufgabe zwingen könnte (vgl. Garden, Timothy (2003): *Air Power: Theory and Practice*, in: Baylis, John et al. (Hrsg.) (2003): *Strategy in the Contemporary World – an Introduction to Strategic Studies*, Oxford, S. 137-160, S. 143).

1. Systeme, die schon sehr lange eingesetzt werden und über proprietäre[54] Software verfügen: Sie haben den Vorteil, dass Wissen über Lücken in den Systemen nicht weit verbreitet ist und gleichzeitig die Benutzung nicht mit normalen Rechnern zu vergleichen ist. Der Nachteil ist, dass in ihnen keine oder nur sehr geringe Sicherheitsmaßnahmen implementiert, d. h., sie können nicht sicher gemacht werden.

2. Systeme neueren Herstellungsdatums, die sehr viel sicherer gemacht werden, da sie über wesentlich mehr Funktionen verfügen. Allerdings haben sie bekanntere Schwächen und werden meist im Auslieferungszustand belassen, d. h., die bekannten Sicherheitsmaßnahmen werden nicht genutzt.

Anfänglich waren SCADA-Systeme nach außen abgeschlossene Netzwerke. Die Hersteller gingen davon aus, dass sie nur physikalisch geschützt werden müssten. War ein solcher Schutz einmal gewährleistet, wurde angenommen, dass nur berechtigte Nutzer auf die einzelnen Komponenten zugreifen könnten.[55] Eine solche Vorstellung ist jedoch veraltet; inzwischen sind SCADA-Systeme mit dem Rechnernetzwerk der betreibenden Organisation eng verbunden. Dadurch bauen sie zum einen auf den KII auf und zum anderen sind sie über die KII angreifbar. Drei Arten der Verbindung sind bekannt, wodurch sich unterschiedliche Schwachstellen ergeben: Erstens werden SCADA-Systeme mit Hilfe von gemieteten Telefonleitungen kontrolliert. Eine zweite Methode ist die Steuerung über „Virtual Private Networks“ (VPN)[56] und als drittes werden Funkverbindungen eingesetzt[57] (Abbildung 2). Letztere werden hier nicht betrachtet werden, da die Verwundbarkeit nicht mit Hilfe der KII ausgenutzt werden kann, sondern eine Anwesenheit vor Ort voraussetzt.

Auch wenn kein direkter Zugriff auf die gemieteten Telefonleitungen besteht, ergibt sich durch die Verbindung zwischen SCADA-System und dem Firmennetzwerk eine Angriffsmöglichkeit.[58] Gelingt es einem Angreifer in das Firmennetz einzudringen, kann er sehr leicht SCADA-Systeme abhören und ggf. mit eigenen Kommandos steuern, da sie selber nur sehr schwache Schutzmechanismen eingebaut haben bzw. nicht alle vorhandenen Schutzmechanismen aktiviert sind (s.o.). Selbst wenn sie per Passwort vor dem direkten Zugriff geschützt sind, braucht ein Angreifer nur den Netzverkehr zu protokollieren: Nach einer gewissen Zeit wird sich ein Techniker in eine SCADA-Komponente einwählen und dadurch das Passwort verraten. Da meist aus Bequemlichkeitsgründen die Passwörter für alle Elemente gleich sind, hat der Angreifer nun die Möglichkeit direkten Zugriff auf jede oder zumindest fast jede Kontrollkomponente im SCADA-Netz zu erhalten.[59] Obwohl sehr häufig nur niedrige Sicherheitsstandards zu existieren scheinen, z.B. aufgrund der Überlegung, dass die Sicherheit der Produktion vor der Sicherheit des IT-Systems steht, gibt es auch Anlagen, die relativ sicher vor Angriffen sind. So beschreibt Berinato[60] in seinem Artikel „Debunking the Threat to Water Utilities“ das SCADA-System der „Massachusetts Water Resource Authority“. Zu dem System gebe es nur zwei Zugänge. Einer bestehe über ein Modem, welches normalerweise ausgeschaltet sei und nur durch einen Mitarbeiter mit einer bestimmten Sicherheitseinstufung angeschaltet werden könne. Der zweite Zugang erfolge wie auch bei den oben

54 Eigens für diesen Zweck programmierte Software, die so nicht im normalen Umlauf ist.

55 Brown, Alan S. (2002): *SCADA vs. The hacker. Can freebie software and a can of Pringles bring down the U.S. power grid?*, in: mechanical engineering, Dezember 2002, http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html (10.05.2004).

56 Ein virtuelles privates Netz bezeichnet eine Netzverbindung zwischen zwei Rechnernetzen, welche über ein drittes, unsicheres Netz erfolgt. Dabei ist die Verbindung über das dritte Netz (meist das Internet) verschlüsselt. Diese Verbindungen werden verstärkt genutzt, da sie günstiger sind als solche über Telefonleitungen.

57 Internet Security Systems (ISS) (2003): *Assessment and Remediation of Vulnerabilities in SCADA and Process Control Systems*, http://documents.iss.net/whitepapers/SCADA.pdf (01.06.2004), S. 3.

58 Ebd., S. 5.

59 Lemos, Robert (2002): *Cyberterrorism: The real risks*, in: ZDNet News UK, 27. August 2002, http://news.zdnet.co.uk/internet/0,39020369,2121358,00.html (15.11.2003).

60 Berinato, Scott (2002b): *Debunking the Threat to Water Utilities*, in: CIO Magazine, 15. März 2002, http://www.cio.com/archive/031502/truth_sidebar2.html (12.11.2004).

beschriebenen Systemen vom normalen Rechnernetzwerk, wobei nur lesender Zugriff auf die Daten gestattet sei. Es zeigt sich hier aber wiederum, dass eine Verbindung (die vielleicht wirklich nötig ist) besteht. Dadurch ist es nicht ausgeschlossen, dass ein Angreifer mit genügend Wissen die Verbindung so abändert, dass er Daten nicht nur lesen, sondern auch schreiben kann – allerdings scheint das eher eine theoretische Möglichkeit zu sein.

Gegen eine gefährliche Verwundbarkeit von SCADA-Systemen spricht, dass bis heute immer noch Menschen die Kontrollfunktion wahrnehmen. Ein Angreifer müsste also gleichzeitig das System angreifen und die ausgegeben Kontrolldaten verändern.[61] Allerdings gibt es schon länger die Entwicklung, dass SCADA-Systeme Menschen vollständig ersetzen. Das bedeutet wiederum, dass ein Rechner alle Vorgänge automatisch kontrolliert. Wird nun dieser Rechner angegriffen und manipuliert, kann er nicht mehr kontrollieren, ob die Ergebnisse der einzelnen Subkomponenten innerhalb der Betriebsspezifikationen der kontrollierten Anlage liegen.

Trotz der genannten möglichen Verwundbarkeit von SCADA-Systemen und trotz der wichtigen Aufgaben, die die Systeme wahrnehmen, ist ein Angriff auf sie bis jetzt nur theoretischer Natur. Es hat – soweit bekannt – bisher nur einen erfolgreichen Angriff auf SCADA-Systeme gegeben.[62] Dieser erfolgte aber nicht über ein Rechnernetz, sondern durch einen Zugriff über drahtlose Verbindungen: Ein entlassener Australier, der vorher bei der Stadtverwaltung von „Maroochy Shire“, Queensland, angestellt war, hat, nach seiner Entlassung hat er einen Laptop und eine Antenne genutzt, um damit in das Funk-Kontrollsystem des städtischen Wassersystems einzubrechen. Dieses gelang ihm nach über 40 fehlgeschlagenen Versuchen, wodurch er die Kontrolle über das System erhielt, welches er dann so manipulierte, das Abwasser in das Wasserwegesystem der Gemeinde zu leiten. Der Schaden war hauptsächlich ökologischer Natur und verursachte keine Personenschäden.[63] Ein weitere publizierter Fall ist äußerst umstritten: Es gibt einen dokumentierten Einbruch in das Rechnernetzwerk von „California Independent System Operator“, einer Organisation, welche große Teile des Stromnetzes in Kalifornien mit Hilfe von SCADA-Systemen überwacht.[64] Allerdings gibt es keine Hinweise, dass die SCADA-System erfolgreich Angriffen wurden. Zwar gelangten die Angreifer in das normale Rechnernetz, nicht aber in das SCADA-System-Netz.[65]

2.2.3. Theoretische Angriffsmöglichkeiten

Die beschriebenen Verwundbarkeiten ergeben sich daraus, dass Angreifer über Verbindungen von IuK-Netzen zu Kritischen Infrastrukturen in Systeme eindringen. Darüber hinaus gibt es unterschiedliche theoretische Verwundbarkeiten der IuK-Netze selber. Würde sie ausfallen, könnten Dienste der Kritischen Infrastrukturen, die auf das Internet angewiesen sind, nicht mehr miteinander kommunizieren, wodurch ein Kontroll- und Steuerungsverlust entstände, welcher wiederum in den Ausfall der KI münden könnte.

Theoretisch ist es relativ einfach, das gesamte Internet lahm zu legen. Diese Tatsache wird in Zukunft noch problematischer, da durch die Verlagerung von Telefonverbindungen aus den geschalteten Verbindungen „in das Internet“ sämtliche drahtgebundene Kommunikation verhindert werden könnte. Um einen Ausfall zu erreichen, müsste ein Wurm, die Angriffswaffe, sich so schnell verbreiten, dass keine Gegenmaßnahmen seitens der Betreiber von

---

61 Ebd.

62 Avancha, S. / Undercoffer, J. / Joshi, A. und Pinkston J. (2004): *Security for Wireless Sensor Networks*, in: Raghavendra, C.S. et al (Hrsg.) (2004): *Wireless Sensor Networks*, Kluwer, S. 253-275, S. 254.

63 Garrison, Linda / Grand, Martin (2002): *National Infrastracture Protection Center – Highlights*, Ausgabe 3, 15. Juni 2002, http://www.iwar.org.uk/infocon/nipc-highlights/2002/highlight02-03.pdf (03.06.2004), S. 5.

64 Verton, Dan (2001): *California hack points to possible IT surveillance threat*, in: ComputerWorld, 12 Juni 2001, http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html (10.05.2004).

65 Stamp, Jason / Dillinger, John / Young, William (2003): *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandina National Labs, http://www.ea.doe.gov/pdfs/vulnerabilities.pdf (31.05.2004), S. 6.

Servern und anderen Infrastrukturen mehr möglich sind. Sind eine genügend große Anzahl von Servern befallen, könnten diese Datenmüll in alle Welt senden, es käme zu einer Überlastung der Netze und damit zu einem Totalausfall. Rechnerwürmer, die so etwas können, werden seit 2001 in der Informatik diskutiert und sind unter den Namen Warhol-Worm[66] oder Flash-Worm[67] bekannt. Ersterer benötigt schätzungsweise 15 Minuten, um das komplette Internet zu befallen, und ist deswegen nach der Theorie von Andy Warhol benannt, das jeder Mensch 15 Minuten Ruhm erhält. Der zweite Wurm schafft die gleiche Aufgabe in ein paar Sekunden.

Der Großteil der Würmer, die in den letzten Jahren bekannt wurden, verbreiteten sich per E-Mail und erforderten daher eine menschliche Aktion. Ein Anwender muss den Anhang seiner Mail öffnen, um seinen Rechner zu infizieren und dem Wurm somit eine Weiterverbreitung zu erlauben. Die Ausbreitung solcher Würmer ist durch diesen Nachteil nicht sehr schnell und kann sich über mehrere Tage hinziehen. Anders liegt der Fall bei automatischen Würmern, wie z.B. Code Red (I und II), Sasser oder SQLSlammer. Sie nutzen eine Schwäche in einem Serverdienst und können sich ohne menschliche Hilfe weiterverbreiten, wodurch eine sehr viel schnellere Ausbreitung möglich ist. Ihre Verbreitung wird dadurch begrenzt, dass sie andere Rechner finden müssen, die sie infizieren können. Dabei ist gerade die Anfangsphase der Verbreitung sehr relevant. Werden nicht genügend andere Rechner gefunden, die die richtige Schwachstelle aufweisen, „stirbt“ der Wurm. Um infizierbare Gegenstellen zu finden, durchsucht ein Wurm einen Adressraum automatisch, wobei unterschiedliche Methoden eingesetzt werden können – beispielsweise indem „nahe“ Adressen bevorzugt werden.

Der Warhol-Wurm ist wesentlich schneller als bisher aufgetretene Würmer, da er als Basis eine Liste mitgegeben bekommt, die mögliche Ziele verzeichnet – er muss seine ersten Ziele nicht finden, wie konventionelle Würmer. Eine solche Liste soll zwischen 10.000 und 50.000 mögliche Adressen umfassen. Wenn der Wurm einen anderen Rechner infiziert, übergibt er seinem „Kind“ die Hälfte der Listen und muss nun einen geringeren Teil abarbeiten. Durch das Übergeben wird die Liste für jeden Wurm schnell kleiner. Weaver hat in einer Simulation herausgefunden, dass ein Netz mit 1 Millionen Maschinen innerhalb von 8 Minuten komplett infiziert werden kann. Nachdem die Liste abgearbeitet ist, sucht der Wurm noch nach weiteren infizierbaren Rechnern. Er gewinnt seine Geschwindigkeit also daraus, dass er eine relativ große Basis hat im Gegensatz zu bekannten Würmern, die sich diese Basis erst suchen müssen.

Der Flash-Worm ist schneller, da ein Urheber schon vorher alle möglichen verwundbaren Rechner herausgefunden haben kann – er muss, nach dem Abarbeiten der Liste keine weiteren Ziele mehr suchen, sondern kann vor dort ausgehend sofort das Internet mit Datenpaketen überschwemmen. Je nach Internet-Verbindung dauert diese Phase zwischen zwei Stunden und ein paar Tagen. Die erste Phase kann rein passiv durchgeführt werden – dadurch wird nicht ersichtlich, dass ein Rechnerwurm in Zukunft ausgesetzt werden soll. Hat er oder sie eine komplette Liste erstellt, wird sie dem ersten Wurm mitgegeben. Anfänglich ist die Liste sehr groß (48 Megabyte), wird aber nach kurzer Zeit äußerst schnell deutlich kleiner. Dadurch, dass der Wurm keine neuen Ziele finden muss, kann er sich ganz auf die Verbreitung konzentrieren und hat innerhalb kürzester Zeit das ganze Internet infiziert.

Gegen das Konzept der beiden Würmer gibt es zur Zeit keinen Schutz im Internet. Die weiter voranschreitende Monopolisierung der Rechnerlandschaft durch Microsoft macht das System sogar noch anfälliger für solche Art von Attacken. Obwohl die Konzepte seit ca. drei Jahren veröffentlicht sind, scheint die Programmierung solcher Würmer die Kenntnisse von Hackern zu übersteigen oder ihr Gewissen hindert sie an einem solchen Einsatz, da bis heute

[66] Weaver, Nicholas C. (2001): *Warhol Worms: The Potential for Very Fast Internet Plagues*, http://www.cs.berkeley.edu/~nweaver/warhol.htm (07.06.2004).

[67] Staniford, Stuart / Grim, Gary / Jonkman, Roelof (2001) *Flash Worms: Thirty Seconds to Infect the Internet, Silicon Defense*, http://richie.idc.ul.ie/eoin/SILICON%20DEFENSE%20-%20Flash%20Worm%20Analysis.htm (12.05.2004).

kein Wurm bekannt ist, der auch nur annähernd die Geschwindigkeit des Warhol- oder Flash-Wurmes erreicht. Es gibt also eine prinzipielle Verwundbarkeit des Internets, die aber noch nicht ausgenutzt werden kann oder zumindest wird. Noch ist sie deshalb nur eine Verwundbarkeit, aber keine Bedrohung.

2.3. Bedrohung

Nachdem im vorangegangenen Kapitel Überlegungen zur Verwundbarkeit angestellt wurden, soll im Folgenden geklärt werden, welche Bedrohungen für Kritische Infrastrukturen im Allgemeinen und Kritische Informationsinfrastrukturen im Besonderen bestehen. Dieser Schritt ist wichtig, da aus einer Verwundbarkeit zwar ein gedachtes Sicherheitsproblem entstehen kann, es aber einer Bedrohung bedarf, um die Verwundbarkeit relevant zu machen. Besteht eine solche Bedrohung nicht oder ist nur entfernt vorhanden, bleibt ggf. genügend Zeit, um die Verwundbarkeit mit technischen und/oder regulären politischen Mitteln zu schließen oder zumindest einzugrenzen. Erst wenn es Akteure gibt, welche die Verwundbarkeit ausnutzen können, besteht eine deutliche Gefahr für die Sicherheit von KI oder KII.

2.3.1. Staatliche Akteure

Es hat – soweit bekannt – noch keinen Vorfall gegeben, in dem ein Staat die KII eines anderen Staates angegriffen hat. Darüber hinaus ist nicht bekannt, welcher Staat überhaupt Fähigkeiten hat, einen Cyberwar[68] zu führen. Es gilt jedoch als relativ sicher, dass die USA mit hohem personellem und technischem Aufwand solche Fähigkeiten entwickeln. Allerdings wird angenommen, dass die USA diese Fähigkeiten noch nicht vollständig beherrschen.[69] Nach Richard Clarke, ehemaliger Berater des US-Präsident George W. Bush zum Thema „Sicherheit von Informationsnetzen“, soll China offen zugegeben haben, dass es an einer Cyberwar-Doktrin arbeite.[70] Auch werden andere Staaten, wie z.B. Russland, Großbritannien, Frankreich, Japan und Deutschland, in der Diskussion erwähnt[71], wobei nicht klar zu sein scheint, ob die genannten Staaten ein rein defensives Cyberwar-Programm haben oder ob sie darüber hinaus an offensiven Fähigkeiten arbeiten. Außerdem ist beachtenswert, dass vier der fünf Staaten zur NATO gehören und es zumindest unwahrscheinlich ist, dass sie ihre Fähigkeiten, soweit sie denn welche haben, gegen Bündnispartnereinsetzen werden.[72] Weiterhin werden nach einem Report des US-Marine-Geheimdienstes außerdem Nord-Korea, Libyen, Iran, Irak, Kuba und Syrien verdächtigt, entsprechende Programme zu unterhalten oder unter-

---

[68] Der englische Begriff Cyberwar ist hier ganz bewusst gewählt worden, da der deutsche Begriff „Informationskrieg“, der unter anderem mit dem massenhaften Auftreten von Computern auch auf dem Schlachtfeld, unpassend ist. Informationen waren in allen Kriegen wichtig, wodurch der Begriff „Informationskrieg“ eine unscharfe Kategorie ist. Der Begriff Cyberwar wird im folgenden benutzt, um die Kriegsführung von Nationalstaaten gegen anderen Nationalstaaten mit Hilfe von Rechnern, die gegen andere rechnergestützte Systeme eingesetzt werden, zu benennen. Es sei darauf hingewiesen, dass andere Autoren, hauptsächlich Journalisten, den Begriff Cyberwar benutzen, um Kämpfe zwischen verschiedenen Hackergruppen zu benennen (z. B. Delio, Michelle (2001) *It's (Cyber) War: China vs. US*, in: Wired, 30. April 2001, http://www.wired.com/news/politics/0,1283,43437,00.html (23. Juni 2005)).

[69] Antes, Manfred (2002): *Sicherheitspolitische Herausforderungen moderner Informationstechnologie* , http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/friedenspolitik/cyberwar.pdf (03.06.2004), S. 4.

[70] Thieme Richard (2003): *CyberSecurity Czar - An Interview with Richard Clarke*, auf onlinesecurity.com, http://www.onlinesecurity.com/forum/article276.php (22.06.2005).

[71] Hildreth, Steven (2001): *Cyberwarfare*. CRS Report RL30735, http://policy.house.gov/assets/def-cyberwarfare.pdf (04.06.2004), S. 2

[72] Auch wenn Neo-Realisten argumentieren, dass man nie wissen könne, ob sich ein Verbündeter nicht letztendlich doch gegen die eigene Staatengruppe stellen werde, ist z. B. ein Angriff von Deutschland auf Frankreich eher unwahrscheinlich.

halten zu haben.[73] Über die Fähigkeiten dieser Staaten sind aber keine anderen Quellen zu finden.

Ein Grund für die Befürchtung durch andere Staaten bedroht zu werden, ist der, dass kleinere Staaten Cyberwar-Fähigkeiten als Mittel der asymmetrischen Kriegsführung gegen größere Staaten einsetzen könnten, um somit deren militärisches Potential, welches konventionell nicht zu schlagen wäre, zu umgehen. Gerade der erste Golfkrieg 1991 habe gezeigt, dass dies die einzige Möglichkeit für manche Staaten sei, gegen die USA und ihre Verbündete zu bestehen.[74] Des Weiteren wurde in einer Studie der RAND Corporation aus dem Jahr 1996 angenommen, dass die Einstiegskosten zur Entwicklung eines Cyberwar-Potentials gering seien.[75] Dabei werden zu den Kosten nur der Anschaffungskosten von Hardware gerechnet, welche seit „Erfindung" des Computers in den 1940er Jahren rapide gesunken ist, sowie die Möglichkeit, sich über das Internet oder andere Netzwerke mit Datenbanken und anderen Infrastruktureinrichtungen zu verbinden. Außerdem würden immer mehr Menschen sich mit Rechnern auskennen, was zu einer Vergrößerung der Masse derjenigen führen würde, die fähig wären, Cyberwar-Aktionen gegen andere Staaten durchzuführen.[76] Dass der Preis für Cyberwarfähigkeiten gering sei, wird heute immer noch propagiert. So schreibt Reinhard Hutter, Leiter des Geschäftsbereichs „Führung, Information und Kommunikation" der IABG, dass früher Waffensysteme zwei bis dreistellige Millionenbeträge gekostet hätten und Schäden in dieser Höhe hervorrufen könnten. Dagegen würde die Entwicklung von Rechnerviren einen Bruchteil kosten und ähnlich teure Schäden hervorrufen.[77]

Dagegen ist einzuwenden, dass das schlichte Betrachten des Anschaffungspreises von einzelnen Rechnern, der Kosten für Kommunikation und des Aufwandes für die Virenprogrammierung nicht ausreicht, um die Kosten für ein Cyberwar-Potential zu beziffern. So ist beispielsweise ein Rechnervirus oder ein -wurm erst einmal eine ungenaue wie ungelenkte Waffe. Staaten werden bei einem Angriff mit Cyberwarwaffen aber das Ziel haben, den Schaden sehr genau im Voraus bestimmen zu können. Darüber hinaus werden sie bestimmte Systeme angreifen wollen und nicht auf den Zufall vertrauen, auf den es bei der erfolgreichen Verbreitung von Viren oder Würmern ankommt.[78] Entsprechend müsste eine optimale ‚Cybertruppe' aus hochspezialisierten Fachleuten bestehen, die sowohl die Lücken in Standardsoftware als auch die möglichen Fehler, die Systemadministratoren normalerweise machen, kennen. Die Truppe müsste entsprechend eng mit dem Geheimdienst zusammenarbeiten, der Passwörter liefern oder Agenten in die „gegnerischen" Strukturen einschleusen könnte, um einen Angriff von innen vorzubereiten. Darüber hinaus müsste eine solche Truppe das gegnerische System nachbauen, um ein „Übungsobjekt" zu haben und den hervorgebrachten Schaden zu evaluieren.[79] Die Kosten lägen wahrscheinlich unter denen „normaler" Waffensysteme. Trotzdem verlangt das Vorgehen einen sehr hohen Ausbildungsstand der beteiligten Personen und im optimalen Fall einen sehr guten Geheimdienst, welcher die nötigen Informationen liefert. Beides ist nicht so kostengünstig, wie es die RAND-Corporation, möglicherweise aus eigenen Interessen, glaubhaft machen will.

Die Kosten eines Cyberwarprogramm werden am Beispiel der Volksrepublik China deutlich. So soll es dort eine Reserveeinheit von Experten geben, die für einen Cyberwar-Einsatz an unterschiedlichen Universitäten, Akademien und anderen Trainingszentren ausge-

---

73 Hildreth, Cyberwarfare, S. 4.

74 Shimeall, Timothy / Williams, Phil / Dunlevy, Casey (2001): *Countering Cyberwar*, in: NATO Review (Web edition), Jg. 49, Nr. 4, S. 16-18, http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf (31.05.2004).

75 Molander, Roger C. / Riddle, Andrew S. / Wilsor, Peter A. (1996): *Strategic Information Warfare – A New Face of War*, RAND Cooperation, S. 17.

76 Ebd.

77 Hutter, Reinhard (2001): *Risiken im Informationszeitalter*, in: Bundesakademie für Sicherheitspolitik (Hrsg.): *Sicherheitspolitik in neuen Dimensionen – Kompendium zum erweiterten Sicherheitsbegriff*, Hamburg: 483-500, S. 485.

78 Smith, An Electronic Pearl Harbor?

79 Berkowitz, Bruce (2000): *Information Warfare: Time to Prepare,* in: Issues in Science and Technology Online, Winter 2000, http://www.issues.org/issues/17.2/berkowitz.htm (12.11.2003).

bildet werde- Außerdem gebe es seit 1997 Übungen zur Führung von Cyberwar.[80] Eine neuere Quelle zitiert einen geheimen CIA-Report, nach dem die chinesische Volksarmee noch nicht dazu fähig sei, Rechnerattacken gegen die USA oder andere Staaten durchzuführen, auch wenn dies angestrebt werde.[81] Zum einen wird hier wieder deutlich, dass die Diskussion über die Bedrohung durch den am häufigsten genannten Staat – China – unübersichtlich ist und sich hauptsächlich auf geheime Dokumente stützt, welche nicht nachzuprüfen sind. Außerdem scheint es auch für Staaten nicht einfach zu sein, Cyberwar-Fähigkeiten zu entwickeln. Wenn selbst sehr große, ressourcenreiche Staaten wie China die Fähigkeiten noch nicht entwickelt haben, wie sollen dann kleinere Staaten schon weiter sein?

Cyberwarführung wird vor allem in einem strategischen Kontext gesehen. Deutlich wird dies z.B. in Titeln wie „Strategic Information Warfare“[82], „Strategic Warefare Rising“[83] oder „Strategic warfare in cyberspace“.[84] Dabei wird angenommen, dass ein Krieg schon geführt werde und Cyberwar-Methoden als neue Waffe eingesetzt würden. Der Erfolg eines solchen Einsatzes wird aber aufgrund der Erfahrungen in der Vergangenheit bestritten, da strategische Bombardierung sowohl im Zeiten Weltkrieg als auch im Vietnam-Krieg erstens wenig erfolgreich gewesen sei und zweitens eine kontinuierliche Schädigung der Infrastrukturen hervorgerufen werden müsste, um Wirkung zu erzielen. Eine dauerhafte oder immer wiederkehrende Schädigung sei bei Rechnersystemen nicht möglich, da die Angriffspunkte schnell geschlossen werden könnten, wodurch ein erneuter Angriff am selben Punkt unmöglich sei. Auch würden viele normale Ausfälle erfolgen, so dass ein Angriff über die regulären Ereignisse hinausragen müsste um einen strategisch relevanten Schaden anzurichten.

Diese Überlegungen können allerdings nicht vollständig überzeugen. Auf der einen Seite ist es nicht angemessen mit Kriegen aus der Mitte des letzten Jahrhunderts zu argumentieren, da es zu der Zeit noch keine so enge Vernetzung von Infrastrukturen gegeben hat, die durch den Ausfall einer wichtigen Schlüsselinfrastruktur große Teile eines Landes hätte effektiv stören können. Beispielsweise waren Angriffe der Alliierten auf Kugellagerfabriken in Schweinfurt insoweit erfolgreich, als die Produktion von Kugellagern auf 30% zurückfiel. Die Anlagen konnten erst im Laufe eines Jahres wieder vollständig repariert werden. Auf der anderen Seite hatte das 3. Reich einen so großen Vorrat an Kugellagern, dass der Produktionsrückgang keine nennenswerte Wirkung hatte.[85] Im Gegensatz zu Kugellagern können Informationen und Informationsverbindungen nicht „gelagert“ werden, sondern müssen wiederhergestellt werden. Deshalb ist ein Vergleich mit den Erfahrungen aus dem Zweiten Weltkrieg nur sehr begrenzt sinnvoll – heute könnten Angriffe auf Informationsknoten, wie z.B. den für Deutschland wichtigen DECIX[86] Knoten in Frankfurt, nicht durch die Lagerung von Informationen ausgeglichen werden. Gleichzeitig können durch die zugrunde liegende Technik des Internet aber relative einfach Redundanzen geschaffen werden, beispielsweise in der Einrichtung von Übergangsknoten. Dies erscheint zumindest kostengünstiger, als die entsprechende Produktion auf das gesamte Land zu verteilen und dadurch hohe Transport- und Logistikkosten in Kauf zu nehmen.

Betrachtet man Cyberwar-Angriffe nicht als Kriegs- sondern als Drohmittel, dass vor einem bewaffneten Konflikt eingesetzt werden könnte, dann könnten sie keine Wirkung ent-

---

80 Hildreth, Cyberwarfare, S. 12.

81 Lichtblau, Eric (2002): *CIA Warns of Chinese Plans for Cyber-Attacks on U.S*, Los Angeles Times, 25. April 2002, http://archive.infopeace.de/msg01294.html (22.06.2005).

82 Molander et al., Strategic Information Warfare.

83 Molander, Roger C. / Wilson, Peter A / Mussington, David A. et al (1998): *Strategic Information Warfare Rising*, RAND Cooperation.

84 Rattray, Greg (2001): *Strategic warfare in cyberspace*, Cambridge.

85 United States Bombing Survey – European War 1945 S.5 URL: http://www.anesi.com/ussbs02.htm (08.06.2004)

86 Der DECIX Knoten ist der wichtigste Knoten im „deutschen Internet“, da er das nationale Netz mit anderen Netzen verbindet und so beispielsweise einen Datenübergang in die USA, aber auch zum restlichen Europa herstellt. Neben ihm gibt es noch drei weitere Übergänge, die aber bei weitem nicht so leistungsfähig und gut angebunden sind.

falten. Richard Clarke erklärte dieses Argument in einem Interview: Im Jahre 2000 kam es zu Auseinandersetzungen zwischen China und Taiwan, die zu eskalieren drohten. Um die Position der USA klar zu machen, die keinen Krieg zu dulden gedachte, entsandte der damalige US-Präsident Clinton zwei Flugzeugträger in die Straße von Taiwan. Hätte China zu der Zeit schon über ein funktionierendes Cyberwar Potential verfügt, hätte es beispielsweise in Kalifornien einen Stromausfall hervorrufen können. Dieser hätte gar nicht lange andauern müssen und er wäre wahrscheinlich nicht auf China zurückzuführen gewesen. Dennoch hätte er eine gewisse Symbolik gehabt oder eine ähnliche Botschaft wie die zwei US- Flugzeugträger sein können.[87] Ein solcher Angriff hätte ein Sicherheitsproblem dargestellt, da die US Regierung in ihren Handlungsoptionen auf eine sehr ähnliche Weise eingeschränkt gewesen wäre, wie sie die chinesischen Regierung eingeschränkt hat. Es ergibt sich allerdings die Frage, ob ein paar Stunden Stromausfall in Kalifornien nicht ein ganz normales Ereignis gewesen wäre, wodurch die Botschaftsfunktion keinerlei Wirkung entfaltet hätte. Zwei Flugzeugträger unter US-Flagge wiederum sind unübersehbar. Cyberattacken können hingegen relativ unbemerkt erfolgen – und in alltäglichen „Routine"-Problemen, wie kurzfristigen Stromausfällen, untergehen und damit ihre Botschaftsfunktion verlieren.

2.3.2. Substaatliche Akteure

Terroristen gelten, gerade nach den Anschlägen des 11. Septembers, als Bedrohung für die Sicherheit westlicher Industrienationen. Von unterschiedlichen Autoren[88] wird angenommen, dass ‚Cyberterror' ein sehr weit verbreitetes Phänomen sei. Dabei wird schon die Veränderungen von Internetseiten als Terrorismus gewertet. Ein solches Verständnis hat allerdings zur Folge, dass die Bedrohung sehr viel größer gemacht wird, als sie ist – die Veränderung von Internetseiten mag zwar ein Unannehmlichkeit darstellen, ein Problem für die Sicherheit eines Staates ist sie gewiss nicht. Außerdem haben solche als unwichtig einzustufenden Vorfälle keine Bedeutung für die Funktionsfähigkeit von Kritischen Infrastrukturen.

Im Gegensatz zu einer Definition von Terrorismus scheint es bei der Definition von Cyberterrorismus eine gewisse Einigkeit zu geben. Die am häufigsten genutzte Definition von Cyberterrorismus ist die von Denning, welche sie vor einem Unterausschuss des US-Amerikanischen Kongresses äußerte:

> „Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[89]

[87] Thieme, CyberSecurity Czar.

[88] Vatis, Michael A. (2001): *Cyber attacks during the war on terrorism: a predictive analysis*, Institute For Security Technology Studies at Dartmouth College, http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf (03.06.2004).

[89] Denning, Dorothy E. (2001): *Is Cyber Terror Next? In Social Science Research Council: After September 11,* http://www.ssrc.org/sept11/essays/denning.htm (26.04.2004), S. 1.

Die Autoren der unten zitierten Studie der *Naval Postgraduate School* definieren Cyberterrorismus sehr ähnlich, wobei sie eine Unterscheidung zwischen unterstützenden Cyberattacken und reinen Cyberattacken machen. Reiner Cyberterrorismus ist nach Nelson et al:

> „...the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological."[90]

Beide Definitionen sollen deutlich machen, dass Cyberterrorismus dazu führen soll, dass eine Regierung oder Bevölkerung zu einer bestimmten Handlung gezwungen werden soll, was wiederum zu einer Einschränkung der möglichen Handlungsalternativen führt. Dabei führt Denning explizit Angriffe auf KI als mögliche Form von Cyberterrorismus auf.

Die 1999 an der „Naval Postgraduate School" in den USA entstandene Studie „Cyberterror Prospects and Implications" (NPS-Studie) analysiert, welche verschiedenen Hindernisse terroristische Organisationen überwinden müssen, um bestimmte Arten von Angriffen im virtuellen Raum durchführen zu können. In ihr werden drei verschiedene Stufen von Cyberterror eingeführt, die Rückschlüsse erlauben, wie wahrscheinlich eine Bedrohung durch Cyberterror zur Zeit ist.

Die erste Stufe, „e*infach-unstrukturierter*" Cyberterror, ist relativ problemlos zu erreichen. Terrorgruppen, welche sich Fähigkeiten der ersten Stufe aneignen wollen, benötigen nur einen Rechner und einen Internet Zugang. Im Internet können sie dann entsprechende Hackerwerkzeuge finden, um erste Angriffe zu verüben.[91] Dabei werden die Werkzeuge nicht weiter verändert. Um die Werkzeuge für terroristische Aktionen einzusetzen, kann eine Wissensaneignungsphase von etwa sechs Monaten angenommen werden, sollte die Terrororganisation ohne Vorkenntnisse beginnen.

Die Aussage vieler anderer Autoren[92], dass Cyberterror eine sehr akute Bedrohung sei, weil terroristische Aktionen mit Hilfe des Internet günstig seien und das Wissen hierzu relativ leicht zugänglich sei, trifft eigentlich nur auf diese erste Stufe zu. Gleichzeitig ist die Stufe aber für die Sicherheit eines Staates bzw. die Sicherheit von Kritischen Informationsinfrastrukturen relativ unbedeutend, weil die Schäden, welche durch nicht unmodifizierte Programme hervorgerufen werden können, nicht bedeutsam sind. Ein weiterer Virus oder eine weitere DoS-Attacke wird im allgemeinen Rauschen der „normalen" Aktivitäten im Internet nicht auffallen.[93]

Die zweite Stufe: „*fortgeschritten-strukturiert"* Ist eher als Bedrohung zu betrachten. Terrorgruppen, die die zweite Stufe erreicht haben, können Angriffe gegen unterschiedliche Rechnersysteme oder gar einzelne Netzwerke durchführen. Dabei haben sie gewisse Fähigkeiten, ihre Ziele zu analysieren. Außerdem haben sie wichtige Änderungen in ihrer Organisationsstruktur vorgenommen, die für Cyberterrorismus erforderlich sind. Darunter fallen die Fähigkeit, neues Personal für diese Art von Terrorismus auszubilden, und gewisse Kommando- und Kontrollfähigkeiten.[94]

Es sind größere Investitionen erforderlich, um die zweite Stufe zu erreichen. Beispielsweise muss ein Mitglied der Gruppe eine Ausbildung im Bereich Informatik haben, um der Gruppe zu den gewünschten Fähigkeiten zu verhelfen.[95] Hat die Gruppe keinerlei Erfahrung mit Rechnern, dauert das Erlangen der entsprechenden Fähigkeiten ca. zwei bis vier Jah-

---

90 Nelson et al, Cyberterror Prospects and Implications , S. 9)
91 Ebd., S. 14
92 Wie z.B. Blattner-Zimmermann, Marit (2001): *Kritische Infrastrukturen im Zeitalter der Informationstechnik, Vortrag gehalten auf dem Internationales Symposium Information Warfare*, Luzern, November 2001, http://www.bsi.de/fachthem/kritis/d_iwsymp.pdf (26.04.2004), S. 2.
93 Nelson et al., Cyberterror Prospects and Implications, S. 80
94 Ebd.
95 Ebd., S. 82.

re. Außerdem sind Spannungen innerhalb der Gruppe zu erwarten, da anfänglich Kosten entstehen, die nicht sichtbar in Erfolge gewandelt werden können.[96] Daneben kann nicht garantiert werden, dass ein Angriff auf ein Informationssystem erfolgreich ist. Wird Cyberterror als Unterstützung zu konventionellen Anschlägen genutzt, die gewünschten Effekte, wie den Ausfall der Funkverbindungen von Sicherheitskräften, aber nicht hervorgerufen, könnten entsprechende Operationen als Ganzes gefährdet werden. Passiert so etwas, sind Spannungen zwischen den unterschiedlichen Zellen (der „normalen" Terrorgruppe und der unterstützenden Cyberterror-Zelle) der Organisation zu erwarten, welche letztendlich zur Auflösung der Cyberterror-Zelle führen könnten.[97]

Die dritte Stufe, „*komplex und koordiniert"*, ist eine wirkliche Bedrohung für Kritische Infrastrukturen, da eine Gruppe auf dieser Stufe die Fähigkeit hat, konventionelle Formen des Terrorismus komplett durch Cyberterror zu ersetzten. Das bedeutet, dass die Terrororganisation fähig ist, koordinierte Attacken gegen heterogene Netzwerke durchzuführen, wodurch massive Störungen auftreten. Dabei können sogar Verschlüsselungen erfolgreich gebrochen werden. Die Gruppe hat auf dieser Stufe weitreichende Fähigkeiten zur Zielanalyse und kann ihre eigenen Werkzeuge (Programme) erstellen, die speziell auf ein oder mehrere Ziele angepasst sind.[98] Von dieser Stufe dürften derzeit noch alle Terrororganisationen weit entfernt sein. Das wird daraus ersichtlich, dass selbst die USA trotz eines massiven Aufwandes an Personal und Ressourcen immer noch Probleme haben, Angriffe gegen Infrastrukturen zu handhaben.[99] Der Kosten- und Personalaufwand für die komplex-koordinierte Stufe wurde in der oben beschriebenen Übung „Electronic Pearl Harbor" deutlich. Ein Ergebnis war, dass mehr oder weniger erfolgreiche Angriffe Kosten für den Angreifer in Höhe von mehreren 100 Millionen US-Dollar verursachen würden. Es stellt sich die Frage, ob unter diesen Gesichtspunkten die sich nun stellt, ist, ob eine Terrororganisation dieses Geld nicht lieber für sicherere Erfolge einsetzt als für langwierige Operationen, deren Erfolg mehr als unsicher ist.

In der NPS-Studie wird nach verschiedenen Terrororganisationstypen unterschieden und versucht einzuordnen, welcher Typ welche Stufe anstreben wollen würde. Die Unterteilung erfolgt in fünf Gruppen: Religiöse, ethno-nationalistische/separatistische, revolutionäre, rechtsextreme und „New Age".[100] Von den identifizierten Gruppen könnten nach Meinung der Autoren nur die religiösen Gruppen ein Interesse daran haben, die komplex-strukturierte Stufe zu erlangen. Alle anderen würden sich mit der zweiten oder gar ersten Stufe (Rechtsextremisten) zufrieden geben.[101]

Gerade die zweite und dritte Stufe der Fähigkeitsskala verlangt von der Terrororganisation nicht nur Geld für die entsprechenden Geräte und die Ausbildung der Mitglieder, sondern auch Zeit. Die Autoren der NPS-Studie diskutieren deshalb unter anderem auch das Auslagern (outsourcing) der Fähigkeiten. So könnte beispielsweise ein Hacker oder eine Hackergruppe engagiert werden, die die geforderten Angriffe ausführt.[102] Ein solches Vorgehen hätte für Terroristen den Vorteil, dass relativ schnell gefährliche Angriffe auf Kritische Infrastrukturen durchgeführt werden könnten. Das Reservoir an möglichen Hackern, die unter Umständen auch für Terroristen arbeiten würden, wurde, zumindest Ende der 1990er Jahre, als relativ groß beurteilt. Zu den verfügbaren Spezialisten wurden unter anderem ehemalige Mitarbeiter von osteuropäischen Geheimdiensten, die nach dem Fall des Eisernen Vorhanges von ihrem alten Arbeitgebern entlassen wurden, gezählt. Ihnen wurde nachgesagt, dass sie über sehr

96 Ebd., S. 67.
97 Ebd., S. 69.
98 Ebd., S. 88.
99 Antes, Sicherheitspolitische Herausforderungen , S. 5.
100 „New-Age" Gruppen sind solche, die sich auf einen einzigen Sachverhalt konzentrieren. Sie sind nur in den westlichen Industrienationen zu finden und kämpfen beispielsweise für die Rechte von Tieren (Animal Liberation Front) usw.
101 Nelson et al., Cyberterror Prospects and Implications, S. 72ff.
102 Ebd., S. 99ff.

großes Wissen in Bezug auf die KII und KI der westlichen Staaten verfügen.[103] Es ist bis heute aber nicht bekannt geworden, dass ein ehemaliger Geheimdienstangestellter für eine Terrororganisation Cyberanschläge durchgeführt hat. Deshalb ist die Befürchtung – zumindest aus jetziger Sicht – unbegründet.

Es ergeben sich durch das Auslagern von Know-how aber Nachteile. So besteht zum einen für die Terrororganisation die Gefahr, dass sie von Sicherheitsdiensten unterwandert werden könnte. Da ein professioneller Hacker eher für Geld als aus ideologischen Gründen arbeitet, ist die Gefahr sehr viel größer, dass er die Seiten wechselt und mit Sicherheitsdiensten zusammenarbeitet.[104] Darüber hinaus hat sich gezeigt, dass die Zusammenarbeit zwischen Terroristen und Hackern für beide Gruppen nicht einfach ist. So wurde auf einer Konferenz, welche ebenso von der NPS durchgeführt wurde, eine Simulation mit „Praktikern" durchgeführt. Die Gruppe der Praktiker setzte sich aus Mitgliedern von Terrororganisationen wie der ETA oder der FARC sowie einem Hacker zusammen.[105] Bei der Zusammenarbeit zwischen den „Terroristen" und dem Hacker kam es zu Spannungen, und zwar einerseits aufgrund von Anerkennungsproblemen seitens der „Terroristen"[106] und andererseits aufgrund der unterschiedlichen „Organisationsstrukturen". Während terroristische Gruppen eher hierarchisch organisiert seien und klare Befehlsstrukturen hätten, arbeiteten Hacker eher in losen Formationen und hätten andere Denkweisen.[107] Die daraus resultierenden Gegensätze führten zu einem Zusammenbrechen der Funktionsweise der Gruppe.[108] Eine Zusammenarbeit zwischen Terroristen und Hackern ist aus diesem Blickwinkel nicht sehr wahrscheinlich. Demgegenüber steht die Annahme unterschiedlicher RAND-Studien über „Netwar"[109], die besagen, das in Zukunft Terrororganisationen netzwerkartige Organisationsstrukturen aufbauen würden.[110] Ebenso weist die Organisationsstruktur der Selbstmordattentäter des 11. September 2001 eher auf eine Netzstruktur, welche die Technologie des Internet nutzt, hin.[111] Diese Entwicklungen deuten darauf hin, dass in Zukunft die Zusammenarbeit zwischen Hackern und Terroristen leichter möglich sein könnte.

Schon 1998 behauptete Clark L. Staten, verantwortlicher Direktor des „*Emergency Response & Research Institute*" in Chicago, vor dem „Subcommittee on Technology, Terrorism and Government Information" des „U.S. Senate Judiciary Committee":

> „It is also believed that members of some Islamic extremist organizations have been attempting to develop a "hacker network" to support their computer activities and even engage in offensive information warfare attacks in the future."[112]

---

103 Rathmell, Andrew / Overill, Richard / Valeri, Lorenzo et all (1997): *The IW Threat from Sub-State Groups: an Interdisciplinary Approach*, Papier präsentiert auf de dritten internationalen Symposium über „Command and Control" Forschung und Technologie, Institute for National Strategic Studies - National Defense University, 17-20 Juni 1997, http://www.kcl.ac.uk/orgs/icsa/Old/terrori.html (03.06.2004).

104 Ebd.

105 Tucker, David (2000): *The Future of Armed Resistance: Cyberterror? Mass Destruction?* Endbericht einer Konferenz vom 15 - 17 Mai 2000 an der Navy Postgradute School, http://www.nps.navy.mil/ctiw/files/substate_conflict_dynamics.pdf (03.06.2004), S. 2.

106 Auf der Konferenz schienen die Mitglieder von Terrororganisationen die Ansicht zu vertreten, dass sie sehr viel erfahrener und weiser seien, da sie direkt in der Krisenregion gearbeitet hätten und somit ihr Leben aufs Spiel gesetzt hätten. Ein Hacker hingegen würde aus der Ferne operieren und nur Einsen und Nullen manipulieren (Tucker, The Future of Armed Resistance, S. 15).

107 Nelson et al., Cyberterror Prospects and Implications, S. 59

108 Tucker, The Future of Armed Resistance, S. 14.

109 Netwar wird in der Studie eher als Beschreibung des Organisationsprinzips der beteiligten Gruppen verstanden den als Art der Durchführung von Kriegsführung.

110 Arquilla, John/Ronfeld, David F. (1996) The Advent of Netwar, RAND Corporation, S. 67f.; Arquilla, John/Ronfeldt, David/Zanini, Michele (1999) "Networks, Netwar and Information-Age Terrorism, in: Lesser, Ian O. et al. (Hrsg.) Countering the New Terrorism, RAND Corporation.

111 Conway, Maura (2002): *Reality Bytes: Cyberterrorism ans Terrorist `Use` of the Internet*, in: firstmonday, Jg. 7, Nr. 11, http://www.firstmonday.org/issues/issue7_11/conway/index.html (10.06.2004).

112 Staten, Clark L. (1998): Foreign Terrorism in the United States: Five years After the World Trade Center, Testimony of Clark L. Staten, Executive Director and Senior Analyst, Emergency Response & Research Institute, Chicago, IL Before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee**,** February 24, 1998, http://www.emergency.com/senate98.htm (23.06.2005).

Sollte dem so sein, dann sollten Terrororganisationen die komplex-koordinierte Stufe der NPS-Studie inzwischen erreicht haben und es wären ernsthafte Angriffe sowohl auf Systeme wie auch KI und KII zu befürchten. Bisher gibt es jedoch nach wie vor keine bekannten Vorkommnisse solcher Attacken. In den letzen Jahren wurde immer wieder geschrieben, dass Terrorgruppen zumindest die zweite Stufe der Cyberterror-Fähigkeitenskala erreicht hätten. So würden Mitglieder von Al Kaida Verschlüsselungen einsetzen, um Angriffspläne zu schützen[113], was für ein höheres Verständnis von Rechnersystemen sprechen würde. Darüber hinaus gebe es die schon 1998 von Staaten angesprochene Verbindungen zwischen Hackergruppen und Terrororganisationen, was für den Eintritt in die dritte Stufe spräche. Als Gruppen werden „Muslim online Syndicate", „GForce Pakistan" und andere genannt.[114] Diese Gruppen sind in der Vergangenheit jedoch nicht durch gezielte Cyberanschläge aufgefallen, sondern durch das Verunstalten von Internetseiten.[115] Das mag zwar dienlich sein, um Nachrichten und Informationen zu verbreiten[116], jedoch waren es weder Angriffe, die Kritischen Infrastrukturen gefährlich werden könnten, noch Anzeichen für das Erreichen der zweiten oder gar dritten Stufe.

Neben Angriffen auf bestehende Systeme bietet sich für Terroristen noch die Möglichkeit, selbst an der Softwareentwicklung beteiligt zu sein und Schwachstellen in bestimmte Produkte einzubauen, die dann zu einem späteren Zeitpunkt ausgenutzt werden könnten, um Angriffe durchzuführen. Ansatzpunkte würden sich beispielsweise dadurch ergeben, dass eine Terrororganisation als Subunternehmer für Cisco-Systems arbeiten würde. Cisco stellt einen großen Teil der für das Internet benötigten Hardware, wie zum Beispiel Router[117], her. Würde eine Terrororganisation Schwächen in Router einbauen, könnten sie Teile des Internets und damit der KII außer Funktion setzen. Allerdings würde ein solches Vorgehen auch wieder zumindest das Erlangen der zweiten Stufe erfordern, wohl eher aber der dritten, da die Organisation fähig sein müsste, Software selbst zu entwickeln oder zumindest fähige Softwareentwickler zu rekrutieren.

Als Beispiel für solch ein Vorgehen dient die japanische Aum Shinryko-Sekte, welche für die Giftgas-Anschläge in der U-Bahn von Tokio 1995 verantwortlich ist. Sie entwickelte eine Software, welche dann von der japanischen Polizei gekauft wurde. Diese Software sollte dazu dienen, 150 Polizeifahrzeuge, auch nicht markierte, zu verfolgen. Als die Verbindung aufgedeckt wurde, hatte die Sekte schon geheime Daten von 115 Fahrzeugen gesammelt. Darüber hinaus wurde herausgefunden, dass die Sekte Software für mindestens 80 japanische Firmen und zehn Regierungsbehörden entwickelt hat. Allerdings wurden keine Angriffe bekannt, welche durch diese Tätigkeit hätten stattfinden können.[118] Ein mutmaßliches Mitglied von Al Kaida, Mohammad Razzak, behauptete zudem nach seiner Festnahme, dass Al Kaida Mitglieder in die Firma Microsoft eingeschleust habe, welche Hintertüren in das zu der Zeit gerade erschienene Windows XP eingebaut hätten.[119] Die Behauptung wurde natürlich von einem Microsoft-Sprecher zurückgewiesen. Aus heutiger Sicht erscheint die Behauptung als unwahrscheinlich, da außer den üblichen Problemen, die jede komplexe Software hat, keinerlei ungewöhnliche Angriffe gegen das Betriebssystem bekannt geworden sind.

---

113 Weimann, Gabriel (2004): *www.terror.net – How modern Terrorism uses the Internet*, United States Institut of Peace, Special Report 116, http://www.usip.org/pubs/specialreports/sr116.pdf (04.06.2004), S. 10.

114 Lawson, Shannon M. (2002): Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure SANS Institute http://www.sans.org/rr/papers/29/821.pdf (15.09.03), S. 4.

115 Denning, Doroty (2002): *Presentation zum Thema Terrorists & the Internet*, SRI Cyber Adversary Workshop, 13 –14 August, http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt (23.04.2004), S. 16.

116 Lawson, Information Warfare, S. 4.

117 Router sind die Geräte, die die unterschiedlichen Rechnernetze, aus denen das Internet besteht,.

118 Denning, Is Cyber Terror Next?, S. 2

119 McWilliams, Brian (2001): *Suspect Claims Al Qaeda Hacked Microsoft – Expert*, in: newsbyte, 17. Dezember, http://www.mail-archive.com/hydro@topica.com/msg00406.html (22.06.2005).

3. Staatliche Reaktionen

Der Schutz Kritischer Infrastrukturen stellt für Staaten eine paradoxe Situation dar. Während den „Gefahren" des Kalten Krieges durch rein staatliche Mittel begegnet werden konnte, ist das bei Kritischen Infrastrukturen nicht mehr der Fall. Diese sind, seit den verschiedenen Privatisierungsvorgängen nicht mehr unter staatlicher Kontrolle, sondern befinden sich in den Händen der Wirtschaft. Während beispielsweise der Bedrohung durch sowjetischen Bomber mittels Luftabwehr von Staaten alleine organisiert werden konnte, bedarf es nun der Zusammenarbeit mit der Wirtschaft. Deshalb sind Public-Private-Partnerships (PPP) für den Schutz Kritischer Infrastrukturen äußerst beliebt. Trotz des Kontrollverlusts ist die Sicherheit der Bürger noch immer die Kernaufgabe von Staaten. Gleichwohl stehen in der Wirtschaft Sicherheitsinteresse meist hinter anderen Interessen. Der Staat muss, um seinem Schutzauftrag nachzukommen, die Wirtschaft deswegen überzeugen in Sicherheitsaspekte zu investieren, entweder durch Kooperation oder durch Zwang. Im Folgenden wird ein Überblick über die Dokumente zum Schutz von KI in den USA und Deutschland gegeben.

3.1. USA

Für die USA sind sechs unterschiedliche Dokumente relevant, die die andauernden Bemühungen zum Schutz Kritischer Infrastrukturen deutlich machen. Als erstes ist die bereits eingangs erwähnte *Executive Order 13010* zu nennen, die eine erste Definition des Begriffs Kritische Infrastrukturen vornimmt und die schon eingangs erwähnte *Presidential Commission on Critical Infrastructure Protection* (PCCIP) ins Leben rief. Die Kommission legte 1997 ihren Endbericht, *Critical Foundations: Protecting America's Infrastructures* vor, der wiederum Grundlage der *Presidential Decision Directive (PDD) 63*[120] wurde. 2000 erschien der *National Plan for Information Systems Protection Version 1.0*[121], der nach eigenen Angaben den ersten Versuch eines Staates darstellt, einen konsistenten Plan zur „Verteidigung des Cyberspace" zu entwickeln. Das vorläufige Ende markieren die beiden, unter Präsident Bush jr. 2003 erstellten Dokumente *National Strategy to Secure Cyberspace*[122] und die *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*[123]

Anfang der 1990er Jahre, nach den Erfahrungen des Golfkrieges 1991, sahen Angehörige des Militärs die Möglichkeiten von Computern in der Kriegsführung hauptsächlich in einem positiven Licht.[124] Computer sollten helfen, effektiver und effizienter gegen Feinde vorgehen zu können und dabei die eigenen Truppen zu schützen. Ein Umschwung zeichnete sich in der Mitte der 1990er Jahre ab. Kritische Infrastrukturen wurden nicht mehr nur als das Ziel der eigenen Cyberwar-Fähigkeiten, sondern vom Militär auch als „Achillesferse" des eigenen Staates gesehen. Präsident Clinton rief mit der EO *13010* im Juli 1996 die PCCIP ins Leben, die sich verstärkt mit Cyber-Angriffen auf KI beschäftigten sollte. Die EO definierte auf der einen Seite, welche Infrastrukturen als „kritisch" zu betrachten sind und auf der anderen Seite die Ministerien, die an der Kommission zu beteiligen wären. Darüber hinaus forderte die EO, dass bis zu zehn Experten aus dem privaten Sektor zu den Beratungen hinzugezo-

[120] White House (2000): *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidental Decision Directive 63.* White Paper, 22. Mai 1998, http://www.iwar.org.uk/cip/resources/pdd63.pdf (22.06.2005).

[121] White House (2000): *National Plan for Information Systems Protection. Version 1.0. An Invitation to Dialogue*, http://www.iwar.org.uk/cip/resources/national_plan%20_final.pdf (22.06.2005).

[122] White House (2003): *The National Strategy to Secure Cyberspace*, http://www.whitehouse.gov/pcipb/ (22.06.2005).

[123] White House (2003): The National Strategy For Physical Protection of Critical Infrastructures and Key Assets., http://www.whitehouse.gov/pcipb/physical.html (22.06.2005).

[124] Bendrath, Ralf (2002): *Computerkriminalität: Zivile Politik trotz militärischer Rhetorik*, in: Daase, Christopher / Feske, Susanne / Peters, Ingo (Hrsg.) (2002): *Internationale Risikopolitik*, Baden-Baden, S. 143-166, S. 146.

gen werden sollten. Anzumerken ist, dass zehn Behörden und Ministerien an der Kommission beteiligt wurden, dass gleichzeitig aber der Anteil der „Sicherheitsbehörden“ sehr hoch war und das Gelder hauptsächlich vom Verteidigungsministerium bereit gestellt werden sollten.

Die PCCIP legte 1997 ihren Abschlussbericht vor. In dem Bericht analysierte sie nur die vom Präsidenten vorgegebenen Infrastrukturen, wies aber darauf hin, dass es erforderlich sei, andere Infrastrukturen mit in ein Schutzkonzept einzubeziehen. Die Konzentration auf die vorgegebenen Infrastrukturen erfolgte, da nicht genügend Zeit und Ressourcen zur Verfügung stand, um alle relevante Bereiche zu bearbeiten. Der Bericht legte vor allem den Zeitdruck offen, unter dem jegliche Planung stände: „Waiting for desaster is a dangerous strategy. Now is the time to act to protect our future“.[125] Zu dem Schluss kommt die Kommission, nachdem sie eine deutliche Bedrohungskulisse aufgebaut hat. So wird zuerst argumentiert, dass durch die Vernetzung von Infrastrukturen jedwede Form des Angriffes Auswirkung auf sehr große Gebiete haben könnte[126], wobei dieses praktisch eine Fortsetzung der Erfahrungen der USA ist, die durch die Sowjetischen Bomber und Raketen lernen musste, dass auch ihr Staatsgebiet nicht mehr unverwundbar ist.[127] Die neue Technologie führe nun dazu, dass es auf der einen Seite eine gleichzeitige Bedrohung von privaten Akteuren (sowohl Individuen als auch Unternehmen) und staatlichen Akteuren gibt und dass darüber hinaus ein Angriff sehr einfach und vor allem kostengünstig durchgeführt werden könnte[128], gerade weil sich ein Angreifer nun nicht mehr zuerst mit dem Militär der USA konfrontiert sähe (PCCIP 1997: 8) (siehe Abbildung 3):

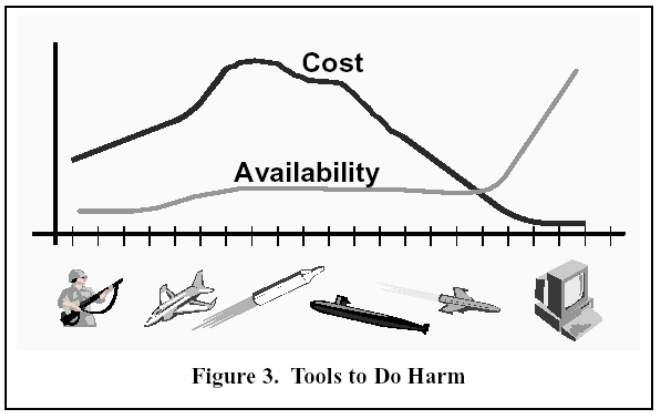


Figure 3. Tools to Do Harm

Quelle: PCCIP 1997: 18

Obwohl die PCCIP fordert, dass die USA KI mit allen Mitteln, d.h. auch mit diplomatischen und militärischen, verteidigen soll, sind die vorgeschlagenen Programme in ihre Auslegung nur geringfügig aggressiv. Von den insgesamt acht vorgeschlagenen Programmen beschäftigt sich fast die Hälfte mit dem Aufbau und der Funktionsfähigkeit einer Partnerschaft zwischen Staat und Industrie. Die anderen Programme hingegen fordern eine Erhöhung des Situationsbewusstseins der Verwundbarkeit Kritischer Infrastrukturen, eine Erhöhung der Forschungsausgaben oder die Führung durch beispielhaftes verhalten.

Als Reaktion auf den Abschlussbericht der PCCIP erließ Präsident Clinton 1997 die PDD-63, die auf der einen Seite einige neue Institutionen erschafft und auf der anderen Seite das Ziel für den Schutz Kritischer Infrastrukturen formuliert:

„Any interruption or manipulation of these critical functions must be brief,

[125] Presidental Commission, S. 6.
[126] Ebd., S. 5.
[127] Ebd., S. 6.
[128] Ebd., S. 18.

> infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[129]

Um diesen Schutz zu erreichen wurden durch die PDD das Amt des *National Coordinator for Security, Infrastructure Protection and Counter-Terrorism* geschaffen. Der Koordinator ist beim Nationalen Sicherheitsrat angesiedelt und hat hauptsächlich die Aufgabe, zwischen den unterschiedlichen Behörden zu vermitteln und die entsprechenden Schutzmechanismen in Krisenfällen zu beurteilen. Als weiteres wurde das *Critical Infrastructure Assurance Office* (CIAO) gegründet, welches dem Nationalen Koordinator zuarbeiten soll. Schlussendlich entstand beim FBI das *National Infrastructure Protection Center* (NCIP), dass neben FBI-Mitarbeitern auch Angestellte anderer Dienste, wie der CIA oder der NSA, aber auch aus dem Verteidigungsministerium, beschäftigt.[130]

Der 2000 veröffentlichte *National Plan for Information Systems Protection* liefert zuerst einmal eine Bedrohungsdarstellung. So wird angenommen, dass sowohl Staaten als auch Terroristen und Einzeltäter die Kritischen Infrastrukturen der USA angreifen können und auch die Intention haben dieses zu tun. Darüber hinaus wird geschrieben, dass schon jetzt die Computersysteme der USA permanent Angriffen ausgesetzt seien, die zum Teil sogar erfolgreich wären. Um die Verwundbarkeit der KI durch Angriffe auf Computersysteme zu verringern, soll der Plan Wege aufzeigen, die das in der PDD-63 formulierte Ziel bis Mai 2003 erreichbar machen. Diese Wege sind in zehn unterschiedliche Programme aufgeteilt, die sich wiederum in drei Kategorien einteilen lassen:

1. Vorbereitung und Prävention
2. Entdeckung und Reaktion
3. Erschaffung stabilere Grundlagen

Im ersten Teilbereich ist nur ein Programm verzeichnet, bei dem es primär darum geht, zuerst einmal eine Verwundbarkeitsanalyse zu erstellen. In deren Rahmen sollen staatliche und private Infrastrukturen identifiziert werden, die von hoher Bedeutung für den Staat sind. Die identifizierten Verwundbarkeiten sollen anschließend vermindert werden. Die zweite Kategorie ist mit insgesamt vier Programmen schon etwas umfangreicher und erklärungsbedürftiger. So erscheint es erst einmal einfach, Computerangriffe zu entdecken, so dass ein Programm extra für diesen Zweck eher unsinnig erscheinen. Dieses ist aber nicht der Fall: Gerade wenn ein Angriff auf Computersysteme nicht in der Störung von Kommunikation besteht, sondern in der Installation von Hintertüren oder dem Stehlen von Informationen, ist er äußerst schwierig festzustellen. Deshalb müssen Detektoren entwickelt werden, die einen solchen Einbruch überhaupt erst einmal sichtbar machen.[131] Obwohl das Wort Reaktion vielleicht im ersten Augenblick an aktive Gegenwehrmaßnahmen denken lässt, werden im National Plan nur passive genannt. Diese erstrecken sich von der Ausbildung entsprechender Strafverfolgungskapazitäten bis hin zur Bereithaltung von speziellen, restriktiveren Firewall-Regeln[132] oder einer Notfallplanung, die einen minimalen Informationsfluss garantieren soll. Die Schaffung stabiler Grundlagen soll zum einen durch Ausbildung entsprechender Computersicherheitsexper-

[129] Presidental Decision Directive.
[130] Vatis, Michael A. (2000): *Statement for the Record of Michael A. Vatis Director, National Infrastructure Protection Center Federal Bureau of Investigation before the Senate Judiciary Committee Subcommittee on Technology and Terrorism*, Washington, 8. März 2000, URL: http://commerce.senate.gov/hearings/0308vat.pdf (23.06.2005).
[131] Es sei hier auf die nicht bemerkten/gemeldeten Einbrüche bei „Eligibe Receiver" verwiesen.
[132] Ein Firewall ist ein spezieller Computer der zwischen Computernetze oder -teilnetze geschaltet wird und den Fluss von Daten begrenzen oder steuern kann.

ten und zum anderen durch die Information der Bevölkerung erreicht werden. Hierbei hat gerade letzteres inzwischen eine höhere Bedeutung als noch vor fünf Jahren. So haben immer mehr Menschen einen Breitbandzugang. Die Rechner der meisten Nutzer sind gegenüber Angriffen ungeschützt, so dass die Rechner schnell zu „Drohnen“ oder „Zombies“ gemacht werden können. Die kumulierte Bandbreite reicht dann aus, um eine DDoS[133] Attacke auch gegen gut angebundene Server oder gar Netze durchzuführen.

Neben den Programmen hebt der National Plan das große Problem des Schutzes von KI hervor: Der Staat kontrolliert nur einen sehr kleinen Teil der Rechnernetze. Zum Schutz der KI ist es aber notwendig, dass alle, auch private, Netze sicherer gemacht werden müssen. Gleichwohl könne (und wolle) der Staat jedoch keine kontrollierenden Eingriffe in die privatwirtschaftlich organisierten Netze vornehmen und sei deswegen auf den guten Willen der privaten Betreiber angewiesen.

Als neustes Dokument des Schutzes von IuK-Netzen ist die *National Strategy to Secure Cyberspce* (NSSC) zu nennen, das 2003 veröffentlicht wurde. Die Strategie wurde in mehreren so genannten „Town Hall Meetings“ zur Diskussion gestellt und soll einen Konsens zwischen der Regierung und beteiligten Industrieunternehmen darstellen. Diese Konsensfindung hat aber nach Meinung unterschiedlicher Beobachter dazu geführt, dass die NSSC äußerst schwammig und damit nicht praktikabel umsetzbar ist. An sich ist die NSSC ähnlich aufgebaut wie der National Plan, nur die Etiketten wurden leicht geändert. Wo im National Plan von Kategorien gesprochen wurde, ist nun von Prioritäten die Rede. Programme heißen nun „Actions“ und ihre Zahl hat deutlich zugenommen. Gleichwohl ist die Richtung gleich geblieben. Es wird immer noch dazu aufgerufen, Analysen über die Bedrohung und die Verwundbarkeit aufzustellen, die Nutzer auf allen Ebenen zu informieren und ihren Teil dazu beitragen, et cetera. Neu ist ein größerer Fokus auf den Regierungsteil des „Cyberspace“. Die Konzentration wird damit erklärt, dass der Staat zwar nur einen kleinen Teil des Cyberspace kontrolliert, gleichzeitig aber der kleine Teil eine sehr hohe Bedeutung hat. Darüber hinaus soll der Staat mit seinen Anstrengungen ein Beispiel für andere geben und dazu noch den Markt für Sicherheitstechnologie verbessern. Außerdem beinhaltet die NSSC erste Ansätze zu einer „aktiveren“ Gegenwehr bei Angriffen auf den US-amerikanischen Cyberspace. Diese Gegenwehr wird dadurch ersichtlich, dass es eine Aktion gibt, die zum Ziel hat, die Ursprünge von Angriffen besser zu identifizieren. Kennt man diese Ursprünge wäre es sicherlich leichter, mit traditionellen Methoden zu reagieren.

Neben den verschiedenen Strategischen Zielen liefert die NSSC sowohl eine oberflächliche Bedrohungsanalyse, als auch eine Verwundbarkeitsanalyse. Dabei wird zuerst darauf aufmerksam gemacht, welche Rolle der „Cyberspace“, d.h. die IuK-Netze, für andere Kritische Infrastrukturen der USA spielen: „Cyberspace is the nervous system of these infrastructures—the control system of our country.“[134] Daneben wird, wie schon im National Plan, eine sehr weite Bedrohung identifiziert, die von Einzeltätern über Kriminelle oder terroristische Vereinigungen bis hin zu anderen Nationalstaaten reicht. Gleichwohl wird eingeschränkt, dass ein Angriff auf KI mit Hilfe von Computern komplexer sei, als man anfänglich gedacht habe, da es bis jetzt noch nicht zu Vorfällen gekommen sei. Allerdings könne und werde sich dieser Zustand in der Zukunft ändern, so dass man sich schon jetzt darauf vorbereiten müsste. In der Darstellung der Verwundbarkeit wird darauf verwiesen, dass nicht nur die großen Netze gefährdet seien, sondern dass es insbesondere kleinere, wenig beachtete Netze gäbe, die angreifbar wären. Aufgrund des Vernetzungscharakters würde „der“ Cyber-

[133] Distibuted Denial of Service: Der anzugreifende Rechner wird von mehreren anderen Rechnern mit Datenschrott überlastet. Im Gegensatz zu einer DoS-Attacke hat dieses Vorgehen für den Angreifer den Vorteil, dass er keinen Rechner unter Kontrolle haben muss, der die gleiche Bandbreite (d.h. Anbindung an das Internet) wie der anzugreifende Rechner hat. Vielmehr kann er viele Rechner, die jeweils eine geringe Bandbreite haben, nutzen, um einen Rechner mit einer sehr guten Anbindung an das Internet zu überlasten.

[134] White House, The National Strategy to secure cyberspace, S. 1.

space der USA, bzw. ihre Kritischen Infrastrukturen gerade durch die unscheinbaren, kleine Netze gefährdet.

Das Vorgehen der USA beinhaltet mehrere Auffälligkeiten. So werden Strategien und Programme meist in enger Zusammenarbeit mit der Industrie entwickelt. Ersichtlich wird das schon in der Zusammensetzung der PCCIP, die zum Teil aus Industrievertretern oder Experten verstand. Die sehr viel neuere NSSC wiederum wurde sogar in Abstimmung mit der Industrie entwickelt. Daneben ist der National Plan mit dem Untertitel „*An Invitation to a Dialogue*“ versehen und innerhalb des Plans wird darauf aufmerksam gemacht, dass er eine erste Version und die Regierung dankbar für Verbesserungsvorschläge sei. Trotz der Dialogangebote sind ein paar grundsätzliche Schwächen festzustellen: Der Schutz Kritischer Infrastrukturen und das Hauptziel, das von Clinton formuliert wurde (Störungen sollen schnell behoben und geografisch beschränkt sein) ist immer noch nicht erreicht, obwohl der National Plan das Jahr 2003 (dem Erscheinungsjahr der NSSC) als Jahr proklamiert hatte, indem die Forderung Clintons erfüllt werden sein sollte. Darüber hinaus ist eine gewisse Radikalisierung der Maßnahmen festzustellen. So werden als mögliche Angreifer in allen Dokumenten andere Staaten identifiziert. Während der National Plan aber als Gegenwehr passive Maßnahmen – den Schutz der Strukturen und unter Umständen eine Stärkung von Strafverfolgungsbehörden vorschlägt, geht die NSSC einen Schritt weiter und lässt anklingen, dass man sich nicht auf die Strafverfolgung von Angriffen beschränken wolle und daher auch andere, traditionelle Sicherheitsinstrumente, gedenke einzusetzen:

> „When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution.”[135]

Eine solche Entwicklung ist als sehr problematisch einzuschätzen. Noch immer kann nicht genau bestimmt werden, woher ein „Angriff“ erfolgt ist und ob er durch die Regierung des als Ursprung lokalisierten Staates gebilligt wurde. Letztendlich besteht deshalb eine sehr hohe Gefahr, dass der „falsche“ Staat dafür verantwortlich gemacht wird und unter Umständen gar auf traditionellem, militärischem Wege angegriffen wird.[136] Selbst wenn dieses Problem gelöst sein sollte, stellen sich diverse rechtliche Fragen, die bei „Cyber-Angriffen“ zu klären sind, wie z.B. ab wann ein „Cyber-Angriff“ als eine Anwendung von Gewalt interpretiert werden kann. Nur dann wäre eine Gegenwehr mit militärischen Mitteln nach Artikel 42 der UN Charter zulässig.[137] Hier wird abzuwarten sein, wie sich die Doktrinen der USA in Zukunft entwickeln werden. Vor allem unter dem Gesichtspunkt, dass Angriffe auf Kritische

---

[135] White House, The National Strategy to Secure Cyberspace, S. 50.

[136] Deutlich wurde das Problem der Zuordnung von Angriffen im Februar 1998 während des Aufmarsches von US-amerikanischen und britischen Truppen am persischen Golf. Genau zur selben Zeit ist ein unbekannter Akteur in die Rechner des US-amerikanischen Verteidigungsministeriums eingebrochen. Der oder die Einbrecher verschafften sich durch bekannte Schwächen in dem Solaris-Betriebssystem Zugang zu Administrationskonten (d. h., sie konnten die Rechner kontrollieren) und luden Passwortdateien auf andere Rechner herunter. Die betroffenen Rechner waren keine Systeme, die als klassifiziert galten, was bedeutete, dass sie über das Internet erreicht werden konnten und keine starken Sicherheitsmaßnahmen zu überwinden waren (GlobalSecurity (2002): *Solar Sunrise*, http://www.globalsecurity.org/military/ops/solar-sunrise.htm (28.04.2004)). Anfänglich wurde angenommen, dass die Angriffe von Seiten des Iraks erfolgten, da der Datenverkehr in den Nahen Osten zurück verfolgt werden konnte (Clarke, Richard (1998): *America's Fight against Terrorism: At Home and Abroad*, Rede auf der Policy Konferenz im Lansdown Conference Center am 16 Oktober 1998, http://www.washingtoninstitute.org/templateC07.php?CID=78 (23.06.2004)). Allerdings schienen manche Aktionen ihren Ursprung in Taiwan oder Deutschland zu haben. Das Verteidigungsministerium und das Justizministerium arbeiteten zusammen, um die Angriffe aufzuklären; diese Zusammenarbeit wurde unter dem Namen „Solar Sunrise“ bekannt. Erst nach einigen Tagen stellte sich heraus, dass die Angreifer nicht aus dem Irak stammten, sondern zwei Teenager aus Kalifornien sowie ein Teenager aus Israel waren (Rötzer, Florian (2001): *Glimpflicher Ausgang einer Crackerkarriere*, in: Telepolis ,18. Juni 2001, http://www.heise.de/tp/deutsch/special/info/7910/1.html (28.04.2004)).

[137] Grove, Gregory D. / Goodman, Seymour E. / Lukasik, Stephen J. (2000): *Cyber-attacks and International Law*, in: Survival, Jg. 42, Nr. 3, S. 89-103, S. 93.

Infrastrukturen mit Hilfe von Computern zur Zeit noch als unwahrscheinlich zu betrachten sind.

3.2. Deutschland

Im Gegensatz zu den USA gibt es in Deutschland keine Gesetze oder offizielle Strategien, die sich direkt mit Kritischen Infrastrukturen befassen. Das einzige Dokument, welches sich ausschließlich mit dem Schutz Kritischer Infrastrukturen beschäftigt ist der Vorabbericht der Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS); *Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland der AG KRITIS*. Daneben wird der Schutz von KI im „Zweite Gefahrenbericht der Schutzkommission beim Bundesministerium des Inneren“ und im vierten Zwischenbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ andiskutiert. In beiden ist der Schutz aber nur ein Randaspekt, der auf wenigen Seiten abgehandelt wird. Darüber hinaus scheint es eine Studie des Auswärtigen Amtes zu geben, welche sich mit dem Schutz Kritischer Infrastrukturen auseinander setzt. Die Studie ist allerdings nicht veröffentlich worden und wurde nur im Spiegel zitiert.[138]

Die AG KRITIS, unter Federführung des Bundesministerium des Inneren, wurde unter anderem als Reaktion auf die Entwicklungen in den USA eingesetzt. Sie hatte als erste Aufgabe einen Bericht zu erstellen, der das Ziel hatte, Bedrohungsszenarien zu entwerfen, Schwachstellen der über Informationssysteme angreifbaren Systeme zu ermitteln, Möglichkeiten zur Behebung der Schwachstellen oder zumindest einer Minderung der zu erwartenden Schäden auszuarbeiten sowie Vorschläge zu einem Frühwarn- oder Analysesystem zu entwickeln (KRITIS 1999: 7/24). Die Endversion des Berichtes ist nicht veröffentlich worden, allerdings kursiert im Internet ein Vorabbericht.[139]

Der Vorabbericht der AG stellt eher eine Situationsbeschreibung dar, denn eine wirkliche Strategie, wie mit dem Schutz Kritischer Infrastrukturen umzugehen ist. Im Bericht wird argumentiert, dass man weder die Erfahrungen aus den USA übernehmen könne, noch annehmen müsse, dass die Gefahr von Angriffen auf KI sonderlich hoch sei. Gleichzeitig will die AG nicht ausschließen, dass die Bedrohungsanalyse in der Zukunft anders aussehen könnte, sprich, das sich die Bedrohung sehr schnell ändern könne. Daneben wird ganz deutlich, im Gegensatz zu den Empfehlungen in den USA, für defensive Maßnamen plädiert. Um defensive Maßnamen optimal durchzuführen sie zuerst einmal eine Schwachstellenanlyse nötig und außerdem sollten angepasste Schutzstrategien für Hochverfügbarkeitssysteme entwickelt werden.

Der „Zweite Gefahrenbericht der Schutzkommission beim Bundesministerium des Inneren“[140] enthält ein Teilkapitel zum Schutz Kritischer Infrastrukturen. Dabei stehen auch hier wieder Verteidigungsmaßnahmen deutlich im Vordergrund. So wird analysiert, wie es möglich ist, die Vertraulichkeit, Echtheit und Verbindlichkeit von Daten zu gewährleisten. Erst in einem letzten Schritt wird darauf eingegangen, dass die Verfügbarkeit von Informationsdiensten gestört werden könnte. Die Autoren gehen dabei von zwei unterschiedlichen Arten des Verlustes der Verfügbarkeit aus: Auf der einen Seite könnte es Angriffe auf die Verfügbarkeit geben, indem ein Akteur versuchen könnte, in ein System einzudringen. Ein Schutz hiergegen sei mit wirkungsvollen Zugangskontrollmechanismen, wie sicheren Authentisierungsverfahren und Ähnlichem, möglich. Gegen Angriffe auf die Verfügbarkeit, die mit Hilfe von Über-

[138] Beste, Ralf (2002): Terrorismus – Neuralgische Punkte, in: Der Spiegel, Nr. 2/2002, S. 31.
[139] KRITIS, Informationstechnische Bedrohungen.
[140] Bundesministerium das Inneren (2001): *Zweite Gefahrenbericht der Schutzkommission beim Bundesministerium des Inneren. Bericht über mögliche Gefahren für die Bevölkerung durch Großkatastrophen und im Verteidigungsfall*, Berlin, http://www.bzs.bund.de/bzsinfo/broschur/zsforschung/gefahrenbericht_2.pdf (28.04.2004).

flutung mit Informationen durchgeführt würden (die so genannten DoS-, oder DDoS-Attacken), sei kein Schutz möglich:

> „Jedes System, das sich der Umwelt gegenüber nicht völlig verschließt (und somit wertlos wird), setzt sich der Bedrohung aus, so mit Informationen zugeschüttet zu werden, dass es zu einer normalen Reaktion nicht mehr fähig ist.“[141]

Im Unterschied zu US-amerikanischen Dokumenten werden keine „gegnerischen Akteure“ genannt und die vorgeschlagenen Maßnahmen zum Schutz von KI sind rein defensiv. So wird zu einer Sensibilisierung der Bevölkerung und der Anwender sowie zur Schaffung von rechtlichen Rahmenbedingungen und zum Schutz der Kritischen Infrastrukturen aufgerufen. Eine „aktive Abwehr“ durch Drohungen auch mit militärischen Mitteln wird nicht als Option genannt.

In Artikel im Spiegel[142] zitierte nach den Terroranschlägen des 11. September 2001 eine vertrauliche gemeinsame Studie des Auswärtigen Amtes und des Bundesministeriums für Verteidigung zum Thema Sicherheit von Kritischen Informationsinfrastrukturen. Die Studie scheint den KII eine wichtige Bedeutung in Bezug auf die Sicherheit von Deutschland zuzuschreiben:

> „Mit gezielten Angriffen an besonders neuralgischen Punkten [ließen sich] gegenseitig aufschaukelnde Ausfallerscheinungen hervor rufen, die das gesellschaftliche Leben buchstäblich lahm legen.“[143]

Das 16-seitige Papier identifiziert als einziges bekanntes staatliches Dokument mögliche Angreifer. Diese seien aber weniger in Nord-Korea oder dem Irak zu finden. Nur die USA hätte die technologischen Fähigkeiten, Kritische Infrastrukturen wirkungsvoll anzugreifen. Vielleicht deshalb wird in der Studie gefordert, dass sich Deutschland um ein nationales Computersicherheits- und Kryptografieprogramm kümmern müsse, da es bei der Nutzung ausländischer Programme gewisse Risiken gäbe. Darüber hinaus wird die Schaffung einer eigenen Behörde gefordert, die sich speziell mit der Sicherheit von Computernetzen auseinander zu setzen habe. Die von Innenminister Otto Schily im Jahr 2000 eingesetzte „Task Force `Sicherheit im Internet´“ reiche nicht aus.[144]

Im Vergleich zu den USA zeigen sich in Deutschland deutliche Unterschiede auf. Während in den USA die Bedrohung auch von anderen Nationalstaaten sehr prominent erwähnt wird, kommt die Bedrohung nach deutsche Sicht eher von unorganisierten Hackern oder unter Umständen noch Terroristen. Das führt zu einer unterschiedlichen Einordnung: Während in den USA der Schutz Kritischer Infrastrukturen auch durch das Verteidigungsministerium bearbeitet wird, werden der Großteil der Aufgaben in Deutschland durch Abteilungen des Innenministeriums durchgeführt. Daneben ist festzustellen, dass der Schutz von KI in Deutschland keinen so hohen Stellenwert zu haben scheint, betrachtet man die produzierten Dokumente oder auch Initiativen. Es gibt zwar eine gewisse Zusammenarbeit mit der Industrie, doch ist diese eher rudimentär, beispielsweise durch den Arbeitskreis Schutz Kritischer Infrastrukturen (AKSIS). Zusätzlich ist das Personalaufgebot in Deutschland äußerst gering; wo in den USA ein eigenes Zentrum zum Schutz von KI geschaffen wurde, das nun dem Ministerium für Heimatverteidigung angeschlossen ist, beschäftigen sich in Deutschland einige wenige Mitarbeiter des BSI sowie einige weitere Unterabteilungen im Innenministerium und im neu geschaffenen Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mit dem

141 Ebd., S. 44.
142 Beste, Terrorismus.
143 Zitierte nach Ebd.
144 Ebd.

Problem. Letztendlich ergibt sich aber für jeden Wissenschaftler das Problem, dass der Schutz Kritischer Infrastrukturen in Deutschland zum größtenteils äußerst undurchsichtig und vor allem nicht öffentlich ist.[145]

4. Fazit & Ausblick

Der Schutz Kritischer Infrastrukturen wird in Zukunft weiter an Bedeutung gewinnen, da es zu einer immer engeren Kopplung von Abläufen innerhalb der Gesellschaft kommt, welches wiederum zu einer größeren Abhängigkeit von Infrastrukturleistungen führt. Gleichzeitig ist zu erwarten, dass Computernetze eine noch höhere Bedeutung gewinnen werden, beispielsweise indem in zunehmenden Maße andere Strukturen an diese Netze angeschlossen werden. Netze oder Metanetze wie das Internet basieren zur Zeit allerdings noch auf der Technologie des letzten Jahrhunderts und sind nicht für die Aufgaben ausgelegt, für die sie heute genutzt werden. Gerade im Bereich der Computersicherheit kann das zu verheerenden Folgen führen.

Gleichwohl ist noch nicht geklärt, ob sich die Schwächen wirklich zu großflächigen Angriffen eignen. Dieses wird auch schwer heraus zu finden sein. So ergibt ein Atombombentest beispielsweise ein relativ genaues Bild über deren Zerstörungskraft. Angriffe auf Kritische Infrastrukturen lassen sich nur äußerst schwierig simulieren, da die Vernetzungen zwischen den Strukturen teilweise gar nicht bekannt sind. Dieses trifft gerade auf großflächige Auswirkungen zu. Daneben kann zur Zeit keine Aussage darüber getroffen werden, wie die Bürger eines Staates auf einen Ausfall reagieren würden, welcher Schaden entstehen würde und ähnliches. Gerade im Feld der Computervorfälle ist eine Kostenabschätzung sehr schwierig. So kommt es zwar immer wieder zu Ausfällen von Computersystemen. Der Schaden, der dadurch entsteht, kann aber bis heute nicht annähernd zuverlässig gemessen werden. Die Kosten, die genannt werden, basieren meist auf Schätzungen des Möglichen Verlustes, müssen deswegen aber nichts mit der Wirklichkeit zu tun haben. Neben den grundsätzlichen Überlegungen zur Verwundbarkeit ist die Bedrohungslage vollkommen undurchsichtig. Es kann beispielsweise nicht vollständig nachgewiesen werden, welche Staaten Cyberwar-Fähigkeiten haben, welchen zwecken diese dienen und wie weit die Fähigkeiten Fortgeschritten sind. Gleichzeitig sind solche Aussagen für substaatliche Akteure noch weniger möglich – gerade weil es keinerlei bekannte Vorfälle gibt.

Beim Vergleich zwischen den USA und Deutschland fällt auf, dass die USA sehr viel deutlicher und offener mit dem Schutz Kritischer Infrastrukturen umgehen. In Deutschland hingegen ist keine öffentliche Debatte festzustellen. Dies führt zu unterschiedlichen Fragen. Beispielsweise wird zu klären sein, welche Unterschiede zwischen Deutschland und den USA im Bereich der KI bestehen. Während in den USA offensichtlich eine äußerst geringe Redundanz im Stromnetz besteht und viele Vorgänge über öffentliche Netze gesteuerte werden, muss dies in Deutschland nicht der Fall sein. Hinweise auf diese Vermutung sind während der Stromausfälle vom Sommer 2003 zu finden, als deutsche Stromerzeuger aussagten, dass ein Stromausfall in Deutschland in diesem Maße nicht möglich sei, da es einer sehr viel höhere Vermaschung des Netzes gäbe.[146] Eine weitere Frage ist, welche Auswirkungen die Privatisierung von KI auf Schutzbestrebungen haben. Durch die Privatisierung stehen die Infrastrukturen nicht mehr unter Kontrolle des Staates, was dazu führt, dass der Staat nur noch indirekt auf den Schutz einwirken kann. Darüber hinaus ist zu erwarten, dass ein privates Unternehmen die Strukturen sehr viel effizienter führen will als ein Staat. Der Wunsch nach Effizienz hat aber zur Folge, dass die Infrastrukturen sehr viel anfälliger für Störungen werden können,

[145] Ritter, Stefan / Weber, Joachim (2003): *Critical Infrastructure Protection: Survey of world-wide Activities, Vortrag gehalten auf der Cyber Security and Contingency Planning - Threats and Infrastructure Protection*, University of Zürich-Irchel, Zürich, 25 – 27 September, Organised by the Governments of Switzerland and Germany, http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/pubonl.html (23. Juni 2005).

[146] Siehe hierzu beispielsweise FAZ vom 15. August 2003: „Das deutsche Netz ist stabiler“

da Redundanzen entfernt werden. Hier ist ein Vergleich zwischen der Auswirkung von Privatisierung zwischen den USA und Deutschland äußerst angebracht, da beispielsweise das Stromnetz in den USA in den 1980er Jahren privatisiert wurde, in Deutschland aber erst Mitte der 1990er Jahre. Ähnliches lässt sich auch über die Wasserversorgung sagen.

Working Paper von IFAR:

WORKING PAPER #1:
Präventive Rüstungskontrolle

WORKING PAPER #2:
Die Raketenprogramme Chinas, Indiens und Pakistans sowie Nordkoreas – Das Erbe der V-2 in Asien

WORKING PAPER #3:
Weapons of Mass Destruction in the Near and Middle East - After the Iraq War 2003

WORKING PAPER #4:
Streitkräftemodernisierung und ihre Auswirkungen auf militärische Bündnispartner

WORKING PAPER #5:
Der Schutz Kritischer Infrastrukturen

Kontakt:
Götz Neuneck
Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle IFAR

Institute for Peace Research and Security Policy at the University of Hamburg
Falkenstein 1, 22587 Hamburg
Tel: +49 40 866 077-0 Fax: +49 40 866 36 15
ifar@ifsh.de www.ifsh.de
Webpage zur Rüstungskontrolle: www.armscontrol.de