erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Ingo Ruhmann

Cyber-Krieg oder Cyber-Sicherheit –

wächst aus Abhängigkeiten auch die Einsicht?

Cyber-Kriegsführung als militärisch-geheimdienstlich motivierte Manipulation von Computern bedroht die Sicherheit der IT-Systeme, von deren Funktionieren mittlerweile die meisten sozialen und politischen Systeme auf diesem Globus abhängig sind. Cyber-Kriegsführung als kleiner Teil der Informationskriegsführung verändert zugleich militärische Organisationen und Operationsformen grundlegend.

Cyber-Kriegsführung – der Einsatz von Schadsoftware gegen Computer und Netzwerke durch staatliche Akteure – war für viele IT-Sicherheitsexperten lange Jahre ein schein-riesenhaftes Szenario: Es wurde überschaubarer, je intensiver man sich damit auseinandersetzte. Diese Bewertung wird mittlerweile jedoch nicht mehr geteilt.

Ein Grund dafür sind die Beispiele ernst zu nehmende Cyber-Kriegsaktionen. 2007 störte eine Serie von Cyberattacken die digitalen Infrastrukturen Estlands. Im August 2008 begann der kurze Krieg zwischen Georgien und Russland mit gezielten Cyber-Kriegshandlungen, wie ein Jahr später die private U.S. Cyber Consequences Unit (CCU) in einer detaillierten Untersuchung darlegte[1]. Die CCU belegte, dass die Angreifer im Cyberspace Zivilisten ohne direkte Beteiligung russischer Behörden oder Militärs waren, die allerdings im Voraus über russische Militäraktionen informiert waren. Das wichtigste Ergebnis dieser detaillierten Untersuchung war jedoch, dass eine Analyse von IT-Sicherheitsvorfällen heute in sehr ähnlicher Weise möglich ist, wie eine Untersuchung der Auslöser und des Verlaufs eines konventionellen Konflikts durch herkömmliche Militärbeobachter. 2010 schließlich wurde mit Stuxnet ein Computerwurm identifiziert, der hochspezifisch für die Kompromittierung eines Anlagensteuerungssystem der Firma Siemens entwickelt wurde. Die Umstände seines Auftretens im Zusammenhang mit Anlagen des iranischen Atomprogramms, der primäre offline-Verbreitungsweg und der extrem hohe Aufwand zur Programmierung des Wurms legen den Schluss nahe, dass durch die Schadsoftware eine gezielte Sabotage des iranischen Atomprogramms durch staatliche Stellen beabsichtigt war.

Cyberwar – Infowar

Cyber-Kriegsführung ist eine gezielte Manipulation von Computern und Rechnernetzen mit Mitteln der Informatik und richtet sich daher gegen eine Infrastruktur von militärischer Relevanz. Militärs nutzen Computer aber weit umfassender zu ihren Zwecken: Sie sammeln Daten, übermitteln Kommandos, koordinieren ihre Aktionen mit vielen Beteiligten. Gegen alle Aspekte dieser Art der Informationsverarbeitung durch das Militär als Organisation richtet sich die „Informationskriegsführung“ in einer „Informationsumgebung“, die aus Sicht der Militärs nur ein Teil der militärischen Operationsumgebung ist.

Zur „Informationsumgebung“ gehören die eigenen und gegnerischen militärischen Informationsinfrastrukturen – eigene Computer und abgeschottete Netzwerke – genauso wie das offene

Internet, die Medien und die Akteure, die Informationen in diesen Kanälen verbreiten.

In der 1996 veröffentlichten Informationskriegsführungs-Doktrin der U.S. Army, dem Field Manual 100-6, wurden erstmals Information Operations definiert. 2003 wurde das Manual 100-6 ersetzt durch das Field Manual 3-13[2]. Darin heißt es:

> *„Information operations is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking."*[3]

Die Mittel für Informationskriegsführung lassen sich entsprechend ihrer Intensität und Abfolge in einer Hierarchie ordnen, die eine Abfolge von Eskalationsschritten sichtbar macht. Die niedrigste Eskalationsstufe ist die Beeinflussung von Medien vor einem bewaffneten Konflikt, es folgt das Ausspähen von Daten über potentielle gegnerische Akteure – im Kern: Spionage oder mit dem neutralen Begriff: Aufklärung – und geht über in einen Schadsoftware-Einsatz – also eine Cyber-Kriegsführung. Eine eindeutig militärische Ebene ist die Zerstörung von Infrastrukturen durch „physische Destruktion", die als letzte Stufe bis zum Einsatz von Atomwaffen zur Erzeugung eines elektromagnetischen Impulses reicht, durch den elektronische Geräte in großem Umkreis überlastet und zerstört werden.

Die Integration von Informationskriegsführung in reguläre militärische Operationen zeigt, dass Information Operations – geordnet nach ihrer Gewaltintensität – als Eskalationshierarchie begriffen werden muss, bei der die Grenzen zwischen Krieg und Frieden zusehends verschwimmen.

Trotz dieser umfassenden Sicht nutzen Information Operations nur eine begrenzte Zahl neuer Elemente. Für IT-Systeme, militärische Organisationen sowie Medien und Öffentlichkeit als Ziele von Information Operations wird im Wesentlichen auf bekannte Operationsformen zurückgegriffen. Eingesetzt werden sie

- gegen IT-Systeme: Mittel des *electronic warfare*, Destruktion mit herkömmlichen Waffen sowie neuartigen EMP-Generatoren,
- gegen militärische Organisationen: das Tarnen und Täuschen gegen jede Form der Aufklärung und Spionage, die Störung der Kommunikation durch Mittel der elektronischen Kriegführung sowie psychologische Mittel,
- gegen Medien und Öffentlichkeit: Mittel der psychologischen Kriegsführung, aber auch direkte Gewalt, beispielsweise gegen Journalisten und deren Kommunikationssysteme.

Psychologische Kriegsführung, Spionage, elektronische Kriegsführung und die Destruktion von Kommunikationsknotenpunkten sind schon weit über 60 Jahre im militärischen Einsatz. Schon seit den 80er Jahren wurde über erste Erfahrungen mit dem Einbruch in gegnerische Computernetze berichtet, mangels Vernetzung vielfach jedoch noch durch Einbruch und Einspielen vor Ort[4]. Neu bei diesen Mitteln sind nur technologische Entwicklungen wie nicht-atomare EMP-Generatoren und die systematische Nutzung von Computerviren gegen vernetzte IT-Systeme bei der Cyber-Kriegsführung.

Einher ging mit der Formulierung von Operationen der Informationskriegsführung eine deutliche Ausdifferenzierung von Gefahren, Operationsformen und potentiellen Gegnern[5], deren Ursache vor allem in der Cyber-Kriegsführung liegt. Dank der im Internet inhärent vorhandenen Manipulationsmöglichkeiten mit erheblichem Schadenspotential ist die Vielfalt potentieller Gegner bei einer Cyber-Kriegsführung kaum mehr begrenzt. Aufgezählt als Beteiligte werden neben den Regierungen von potentiellen Gegnern daher die Medien, Industrie und Non-Government Organisations (NGOs). Da als potentielle Schadensverursacher in Computernetzen auch unautorisierte Nutzer, „Insider" und „Nonstate Activists" aufgeführt werden, ist im militärischen Verständnis letztlich jeder Internetnutzer potentieller Gegner in militärischen Informationsoperationen.

Eine relativ überschaubare Zahl neuer militärischer Mittel der Informationskriegsführung und die damit verbundene Sichtweise hat also zu einer ganz erheblichen Ausweitung der „Kampfzone" und der potentiellen Gegner geführt.

Infowar – eine internationale Entwicklung

Diese Entwicklung wurde zwar in den USA intensiv vorangetrieben, von anderen Ländern aber in ähnlicher Weise adaptiert. Die USA sehen sich daher einer ganzen Reihe von Staaten gegenüber, deren Infrastruktur – also die „Informationsumgebung" – weniger auf vernetzte IT-Systeme angewiesen ist, die aber über ausreichende Fähigkeiten und Ressourcen für Manipulationen an IT-Systemen, also eine Cyber-Kriegsführung, verfügen. Hinzu kommt, dass sich Cyber-Kriegsführung durch militärische oder geheimdienstliche Organisationen ebenso wie Spionage nicht nur gegen militärische Gegner, sondern auch gegen Bündnispartner richten kann.

Selbst wenn man also keine „Nonstate Activists" berücksichtigt, so kommen als Beteiligte in Informationskriegen neben den Hochtechnologie-Staaten auch zahlreiche Schwellenländer in Betracht:

- Russland setzt weniger auf Computer als auf die Intensivierung konventioneller Methoden, vor allem der psychologischen und elektronischen Kriegführung[6], verfügt aber zumindest im Privatsektor eindeutig über eine ausreichende Basis an Technik und Kompetenzen zu moderner Cyber-Kriegsführung;
- China reklamiert nicht nur die Erfindung des Begriffs „Information Warfare" für sich, sondern verfügt über ähnlich umfassende Konzepte wie die US-Militärs[7] und setzt auf einen „Volksinformationskrieg"[8];
- Taiwan nutzt die Stärken in der Elektronikbranche und setzt auf den Einsatz von Computerviren und ähnlichen Manipulationsmitteln[9];

- Indien beginnt nach der Adaption amerikanischer Ideen mittlerweile damit, differenzierte und auf die eigenen Fähigkeiten im IT-Bereich zugeschnittene Ansätze der Cyber-Kriegsführung zu entwickeln[10].

In Deutschland hat sich die Bundeswehr seit Mitte der 90er Jahre dem Schutz vor Information Warfare-Attacken gewidmet und entwickelte Ansätze zu Information Operations als Planungsinstrument[11]. Unterschiedliche Teilaktivitäten im Rahmen von Informationskriegsführung werden von der Bundeswehr in unterschiedlichen Truppenteilen und Einrichtungen verfolgt. 2002 wurden die ersten organisatorischen Grundlagen gelegt, die 2007 um weitere Aufgaben ergänzt wurden.

Die Erhebung aus verschiedenen offenen Quellen war Aufgabe von zwei mittlerweile umstrukturierten Einrichtungen. Die Feldnachrichtenkräfte in der Bundeswehr sind für Personenbefragungen und Beobachtung zuständig, das Feldnachrichtenzentrum in Dietz wurde jedoch 2008 aufgelöst. Das Zentrum für Nachrichtenwesen der Bundeswehr in Gelsdorf betrieb die Aufklärung und Lagebewertung aus offenen Quellen. Es wurde 2007 aufgelöst und teilweise dem Bundesnachrichtendienst (BND) zugeschlagen.

Der Psychologischen Kriegsführung entstammt das Zentrum Operative Information in Mayen, das Psychologische Verteidigung („langfristige Einstellungs- und Verhaltensänderung erreichen") betreibt und mit dem Radio Andernach als Truppensender und Video-Trupps in Einsatzgebieten auf Sendung geht. Für Aufklärung und Informationsbeschaffung zuständig ist außerdem der Militärische Abschirmdienst (MAD), der mit dem BND Daten austauscht.

In der Bundeswehr ist das 2002 gegründete Kommando Strategische Aufklärung (KSA) der Truppenteil, dem bei Aufklärung, Psychologischer Kriegsführung und Computer-Netzwerkoperationen der größte Teil des Spektrums von Informationskriegsaufgaben zugewiesen wurde. Im KSA wurden alle bisher in den Teilstreitkräften der Bundeswehr vorhandenen Kräfte und Mittel der elektronischen Kriegsführung, also der ortsfesten und mobilen so genannten Fernmelde-/Elektronischen Aufklärung (Fm/EloAufkl), die des Elektronischen Kampfes des Heeres (EloKa) sowie der Satellitengestützten Abbildenden Aufklärung (SGA für SAR-Lupe) im KSA in Gelsdorf und anderen Orten zusammengeführt. Damit wurden im KSA zur Gründung 6.300 Militärs und 700 Zivilbeschäftigte zusammengefasst. 2007 wurde das KSA umstrukturiert, es wurden Standorte aufgegeben. 2009 kam dann die Abteilung „Informations- und Computernetzwerkoperationen" in Rheinbach zum KSA neu hinzu. Im Mai 2010 wurde die „Gruppe Informationsoperationen", die mit der Produktion von Medieninhalten betraut ist, dem Zentrum Operative Information (ZOpInfo) in Mayen zugeordnet[12].

Getrennt von diesen operativen Einheiten der Bundeswehr ist das ebenfalls im November 2002 nach zweijähriger Planung eingerichtete Computer Emergency Response Team der Bundeswehr, CERTBw, das beim IT-Amt der Bundeswehr in Euskirchen untergebracht ist. Das CERTBw hat – wie andere derartige Teams auch – die Aufgabe, Angriffe auf die IT-Infrastrukturen der Bundeswehr zu erkennen und Schutzmaßnahmen zu treffen. Zur Philosophie des CERTBw gehört, sich mit zivilen CERTs auszutauschen, und organisatorisch und konzeptionell eine konventionelle defensive Aufgabe zu verfolgen. Das CERTBw ist daher auch Mitglied im CERT-Verbund[13] und stellt seine Arbeit auch bei zivilen Veranstaltungen zur IT-Sicherheit dar[14].

Kritische Infrastrukturen: Militarisierung der IT-Sicherheit?

Militärs, die in einem Informationskrieg gegnerische militärische Systeme mit Störsendern der elektronischen Kriegsführung oder anderen Mitteln angreifen, sind eine leider nur zu alltägliche Erscheinung. Mit Angriffen auf Computersysteme verändern sich die Gewichte. Die sicherheitsrelevanten militärischen Kommandonetze waren bislang vom Internet abgeschottet; Einzelheiten über Manipulationen an diesen Netzen gelangen nur selten an die Öffentlichkeit.

Zunehmend sind jedoch auch rein militärische Netze mit dem Internet vernetzt. Zum einen, um das Internet für die Informationsbeschaffung zu nutzen, vielfach aber auch, um weniger sensitive Daten zu übermitteln. Durch diese Vermischung von zivilen und militärischen IT-Netzwerken und die Abhängigkeit der Militärs von zivilen logistischen und organisatorischen Infrastrukturen gewinnt die Bedrohung an Bedeutung, dass sich potentiell gegnerische Militäreinheiten oder „Cyberterroristen" an zivilen IT-Infrastrukturen zu schaffen machen. Da „Cyberterroristen" im Normalfall keinen Zugang zu abgeschotteten militärischen Netzwerken haben, sind ihre Ziele jene offen verfügbaren Infrastrukturen, von deren störungsfreiem Funktionieren die zivile Informationsgesellschaft vital abhängig ist. Diese Abhängigkeit macht solche IT-Infrastrukturen zu „kritischen Infrastrukturen". Als kritisch werden Infrastruktursysteme definiert, deren Ausfall in einer technisierten Gesellschaft zu erheblichen Problemen führt. Diese sind Informations- und Kommunikationssysteme, die Energieversorgung und fossile Brennstoffe, das Banken- und Finanzsystem, Verkehr, Wasserversorgung, Notfall- und Rettungsdienste und Regierungsdienste.

Aus dieser Abhängigkeit erwächst der Anspruch, kritische zivile Infrastrukturen mit Mitteln der IT-Sicherheit in militärischer Hand zu schützen. Auch das CERTBw ist in dieser Sichtweise eine an zivilen Kooperationsstrukturen ausgerichtete Spezialistentruppe zu genau diesem Zweck.

Das führt zu der Frage, ob es nun möglich und denkbar ist, dass bei einer Manipulation von zivilen IT-Infrastrukturen schnell erkannt wird, wer die Urheber sind, um dann ebenso schnell zu entscheiden, zivile oder militärische Einrichtungen mit Gegenmaßnahmen zu beauftragen? Bisher gibt es jedenfalls noch keinen Beleg dafür, dass bei Cyber-Attacken so schnell und eindeutig bewertet und gehandelt wurde. Statt dessen wurden Attacken oft jugendlicher Hacker[15] vorschnell als gefährliche Cyber-Angriffe und „Cyberterrorismus" bezeichnet.

Cyberterrorismus

Wer den Begriff Cyberterrorismus ausloten will, sollte sich zuerst vor Augen halten, dass „Terrorismus" schon in seiner konventionellen Bedeutung ein stark politisch geprägtes Etikett ist, das von Politikern äußerst willkürlich vergeben wird, aber auch von

den Strafverfolgungsbehörden wenig präzise verwendet wird. Der Vergleich von Strafermittlungen und Strafverfahren zum zentralen Terrorismus-Paragraphen, dem 129a, ergab: „So kam es lediglich in 5 % der vom Generalbundesanwalt geführten § 129a StGB-Verfahren und gegen 8 % der Beschuldigten überhaupt zu einer Anklage“[16], da kein Tatverdacht gegeben war.

Wenn schon konventioneller Terrorismus bei 90 % der Verdächtigten zu unrecht unterstellt wird, dürfte „Cyberterrorismus“ – bei dem man der verdächtigen Personen so gut wie nie habhaft wird oder politisch unbedarfte Jugendliche ermittelt – ein analytisch recht sinnloser Begriff sein, von dem sich manche Akteure allenfalls Nutzen als Aufmerksamkeit erheischender Domainname erhoffen[17]. Auch Sicht von IT-Sicherheitsfachleuten führt der Begriff vor allem zu „fundamentalen Missverständnissen“[18]: Es kann zwar sein, dass konventionelle Terroristen über Kenntnisse der Manipulation von Computern verfügen und für ihre Zwecke einsetzen. Die psychologischen und medialen Effekte aber, auf die bei asymmentrischer Kriegsführung und Terrorismus abgezielt wird, lassen sich durch „Cyberterrorismus“ kaum erreichen, da es medial bisher nicht gelungen ist, Manipulation an IT-Systemen überhaupt mit politischen oder anderen Zielen in Verbindung zu bringen.

„Cyberterrorismus“, dessen Bekämpfung sich Militärs zusätzlich zuwenden, ist damit in jeder Hinsicht eine äußerst vage Begründung für eine neue Verteilung von Aufgaben zwischen staatlichen Einrichtungen zum Schutz der IT-Sicherheit.

Cyberterrorismus – und die Strafverfolgung

Cyberterrorismus wirft also die Frage auf, wer im Rahmen einer Cyber-Kriegsführung für deren Abwehr zuständig sein und für diese Aufgabe erweiterte Ressourcen – Personal und Finanzmittel – erhalten sollte: zivile oder militärische Organisationen. Nun ist die Terrorismusbekämpfung keine Aufgabe von Militärs, sondern der Strafverfolgungsbehörden. In der Bundesrepublik gibt es außerdem seit 1986 Straftatbestände für die Manipulation an und das Ausspähen von Computern, wenngleich die Zahl der damit juristisch verfolgten Straftaten jedoch nur ein verschwindend geringer Teil der tatsächlichen Fälle waren und sind. Zur exemplarischen Beantwortung der Frage für Deutschland ist es daher notwendig, den schon genannten militärischen IT-Einrichtungen ihre zivilen Pendants gegenüber zu stellen.

Als Bündelung von Fachkompetenz erfolgte 2007 die Einrichtung des Gemeinsamen Internetzentrum beim Gemeinsamen Terrorismusabwehrzentrum (GTAZ), in dem ein großer Teil der IT-Kompetenzen der Strafverfolger und zivilen IT-Sicherheitsbehörden von Bund und Ländern zusammen arbeiten.

Soweit es die dürre Datenlage hergibt, sind bei den Polizeibehörden von Bund und Ländern insgesamt etwa 350 Beamte mit der Überwachung des offenen Internets beschäftigt[19]. Überwiegendes Einsatzgebiet sind Delikte im Bereich der Kinderpornografie. Laut Bundesinnenministerium waren im GTAZ zumindest zu Beginn 190 Personen in der Terrorbekämpfung beschäftigt[20]. Es handelt sich um Experten aus dem BKA, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, den Kriminal- und Verfassungsschutzämtern der Länder, der Bundespolizei, dem Zollkriminalamt, dem Militärischen Abschirmdienst, dem Bundesamt für Migration und Flüchtlinge und dem Generalbundesanwalt. Das GTAZ bindet also ca. 100 der 350 bekannten und mit der Internetfahndung betrauten Polizisten der Republik. Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sind derzeit insgesamt ca. 400 Mitarbeiter beschäftigt, aber nur ein kleiner Teil davon mit der Analyse von IT-Sicherheitsfragen. Das 2011 gestartete Internet-Sicherheitszentrum beim BSI nahm seine Arbeite mit 10 Mitarbeitern auf[21]. Seit Juni 2011 wirken auch der Bundesnachrichtendienst (BND) sowie die Bundeswehr als assoziierte Behörden mit[22]. Bei der Bundeswehr ist die Zahl hoch spezialisierter IT-Sicherheitsexperten beim CERTBw nicht größer, die Gruppe „Informations- und Computernetzwerkoperationen“ des KSA sollte zu Beginn 76 Mitarbeiter umfassen[23].

Auch die Vermehrung von Organisationen in den letzten Jahren hat somit zu keiner nennenswert größeren Zahl von Personal bei staatlichen Stellen für genuine IT-Sicherheitsaufgaben geführt. Statt dessen kooperieren alle bisher bestehenden Zentren nun in neuen Formen miteinander. Dass dieselben IT-Sicherheits-Fachleute deutscher Behörden nun einen größeren Teil ihrer Arbeitszeit für den gegenseitigen Austausch und für die Abstimmung aufwenden, mag Doppelarbeit vermeiden helfen und der Verdichtung von Problemlagen dienen. Der eigentlichen zu leistenden fachlichen Arbeit hilft dies jedoch weniger. Es ist daher eine Frage der erst noch zu leistenden zukünftigen Evaluation der Ergebnisse, ob dieses Pooling von Ressourcen einen positiven Effekt hat.

Begrenzung von Informationskriegsführung

Informationskriegsführung sieht das Internet als Kampfraum. Cyber-Kriegsführung bedient sich der Manipulation von Computersystemen als Kampfmittel. Die gegen Industrie-Steuerungsanlagen programmierte Stuxnet-Schadsoftware belegt, dass nicht nur die mit dem Internet vernetzten Computer Ziele

Ingo Ruhmann

Ingo Ruhmann, Informatiker, wissenschaftlicher Referent und Lehrbeauftragter, Gründungsmitglied und ehemaliges Vorstandsmitglied im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Arbeiten zu Datenschutz, IT-Sicherheit, sowie Informatik und Militär.

von Angriffen sind, sondern auch solche in abgeschotteten Industrieanlagen, sofern dasselbe Computermodell zufälligerweise auch in irgend einer strategisch wichtigen Industrieanlage genutzt wird.

Cyber-Kriegsführung durch Militärs und Geheimdienste – nicht „Cyberterrorismus" – bedroht die zivilen Infrastrukturen der Informationsgesellschaft. Der „Virtual Criminology Report" des IT-Sicherheitsunternehmens McAfee beschäftigte sich 2009 erstmals nicht mit allgemeinen IT-Sicherheitsproblemen und deren kriminellen Verursachern, sondern mit staatlichen Stellen und den Bedrohungen durch die „so gut wie eingeläutete" Cyber-Kriegsführung[24]. McAfee fordert eine offene Debatte über die Gefahren von Cyber-Kriegen. Es gehe darum, die weitgehend hinter verschlossenen Türen stattfindende Diskussion über Cyber-Kriegsführung, die gravierende Folgen für die Allgemeinheit haben werde, auch in der Öffentlichkeit zu diskutieren.

Immerhin haben die Aktionen der letzten Jahre zu der Einsicht geführt, dieses sicherheitspolitische Thema nicht allein aus militärischem Blickwinkel zu sehen, sondern auch zum Gegenstand einer politischen Abstimmung zu machen. Am 13. Dezember 2009 meldete die New York Times, dass die USA Verhandlungen mit Russland aufgenommen habe, um eine „Verbesserung der Internet-Sicherheit und eine Begrenzung der militärischen Nutzung des Internet"[25] zu erreichen. Weitere Gespräche seien 2010 in New York und Garmisch-Partenkirchen terminiert.

Allein die Existenz dieser Gespräche stellte eine deutliche Abkehr von einer jahrelangen Abwehr gegen Verhandlungen über dieses Thema dar. Ein nahe liegender Maßstab für die Bedeutung dieser Gespräche ist der Vergleich mit dem heute zur Informationskriegsführung zählenden elektronischen Kriegsführung. Dabei geht es um das Ausspähen elektronischer Signale und Kommunikation und entsprechende Schutzmaßnahmen. Der seit dem zweiten Weltkrieg ununterbrochen andauernde Einsatz der elektronischen Kriegsführung ist gekennzeichnet durch einen ganz speziellen Rüstungswettlauf. Dazu gehören nicht nur elektronische Gegenmaßnahmen, sondern auch elektronische Gegen-Gegenmaßnahmen, wie das Abstrahlen von Störsignalen oder das Aussenden hochenergetischer Strahlung, die elektronisches Gerät zeitweilig oder dauerhaft lahmlegt. Ein Ende dieses Wettlaufes ist nicht abzusehen. Die Schäden durch diese, meist auf militärische Systeme angewandte Form der Informationskriegsführung sind jedoch begrenzt.

Für Cyber-Kriege mit Computerviren und Netzattacken gilt diese Begrenztheit nicht. Es wäre daher für alle Seiten vernünftig, Schäden zu vermeiden und eine internationale Verständigung zu erreichen[26]. Nicht ganz so überraschend war aber nach den ersten Gesprächen zur Kontrolle von Cyber-Kriegsführung, dass im Wesentlichen über Differenzen berichtet wurde, die nur begrenzte Fortschritte erhoffen lassen. Ein Ansatz dafür könnte die von US-Präsident Obama im Mai 2011 vorgestellte globale Cyberspace-Strategie sein, die schon als kurzfristige Maßnahme vorsieht, ein „internationales Cybersecurity-Politik-Rahmenwerk" zu entwickeln, um gemeinsam mit anderen Staaten die Sicherheit im Internet zu verbessern[27].

Fazit

Fest steht, dass IT-Systeme unsicher und offen für Manipulationen sind. Zusätzlich zur grundlegend verbesserten Sicherheit von IT-Systemen sind Organisationen wie CERTs und deren Kooperation nötig zum Schutz gegen Manipulationen. Ohne zusätzliche Fachleute in diesen spezialisierten Organisationen wird die Verbesserung des Niveaus der IT-Sicherheit jedoch nicht erreichbar sein.

Wenn zwischenstaatliche Konflikthintergründe bei IT-Sicherheitsproblemen an Bedeutung gewinnen, wird die unweigerliche Folge eine weitere sicherheitspolitische Destabilisierung bei Bedrohungen der IT-Sicherheit sein. Durch ein stärkeres militärisches Engagement und einen damit einhergehenden Rüstungswettlauf analog zur elektronischen Kriegsführung kann aber weder eine höhere Effektivität in Sachen IT-Sicherheit erwartet werden noch eine Stärkung der Strafverfolgung.

Internationale Übereinkünfte zur Verbesserung der IT-Sicherheit – zusätzlich zu stärkeren Investitionen in die zugehörige Technik – und Begrenzung von Information Warfare[28] sind daher der einzige Weg zu einer zivil nutzbaren verlässlichen IT-Infrastruktur. Die politische Einsicht in die Notwendigkeit scheint vorhanden. Die Zukunft wird zeigen, ob sie ohne größere IT-Katastrophen auch zu einem tragfähigen Ergebnis führt.

Anmerkungen

1 *US-CCU Special Report: Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008; August 2009; http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf*

2 *U.S. Department of the Army: FM 3-13 (FM 100-6) Information Operations: Doctrine, Tactics, Techniques, and Procedures, November 2003, URL: http://www.carlisle.army.mil/DIME/documents/FM%203-13%20-%20Info%20Opns%20Doc,%20Tactics,%20Tech,%20and%20Proced%5B1%5D.pdf*

3 *FM 3-13, ebd., S. 1-13*

4 *Jay Peterzell: Spying and Sabotage by Computer; in: Time, March 20, 1989, S. 41; Oberstleutnant Erhard Haak: Computerviren – ein Kampfmittel der Zukunft?; in: Soldat und Technik, Nr. 1, 1989, S. 34-35.*

5 *FM 3-13, ebd., S. 1-2ff*

6 *Igor Panarin: InfoWar und Autorität; in: G. Stocker, C. Schöpf (Hg.): Information.Macht.Krieg; Wien 1998, S. 105-110*

7 *Shen Weiguang: Der Informationskrieg – eine neue Herausforderung; in: G. Stocker, C. Schöpf (Hg.): Information.Macht.Krieg; Wien 1998, S. 67-91*

8 *Wei Jincheng: Der Volksinformationskrieg; in: G. Stocker, C. Schöpf (Hg.): Information.Macht.Krieg; Wien 1998, S. 92-104*

9 *Florian Rötzer: Taiwans Militär probt Angriffe mit Computerviren; in: Telepolis, 8.8.2000, http://www.heise.de/tp/deutsch/special/info/6955/1.html.*

10 *C. Uday Bhaskar: Trends in Warfare: A Conceptual Overview; in: Strategic Analysis, Dec. 2000, S. 1577-1589, vgl auch: Ajai K. Rai: Media at War: Issues and Limitations, Strategic Analysis, Dec. 2000, S. 1681-1694; sowie: Vinod Anand: An Integrated and Joint Approach Towards Defence Intelligence; in: Strategic Analysis, Nov. 2000, S. 397-1410.*

11 *Ralf Bendrath: Informationstechnologie in der Bundeswehr; in: Telepolis, 25.7.2000, http://www.heise.de/tp/deutsch/special/info/6933/1.html.*

12 *Informationsprofis arbeiten enger zusammen; Bundeswehr-Pressemeldung vom 29.06.2010; http://www.opinfo.bundeswehr.de/portal/a/opinfo/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uykPyCzLy0fL3SvOLUotT4HL0qqACIyC_QK01NSi1KT0xK1S_IdlQEAJFZpok!/*
13 *http://www.cert-verbund.de/*
14 *Vgl. u.a. den Vortrag an der Uni Koblenz: http://www.uni-koblenz-landau.de/koblenz/fb4/institute/iwvi/egov-network/egov-day/historie/egov-day-2007/Vortrag_Rohde.pdf*
15 *Vgl. dazu den Fall von jugendlichen Hackern, die vom FBI als internationale Verschwörung bezeichnet wurden, vgl.: Armin Medosch: FBI deckt internationale Verschwörung von Cyber-Terroristen auf; in: Telepolis, 17.1.2001, http://www.heise.de/tp/deutsch/special/info/4701/1.html*
16 *Staatsschutzkriminalität, Lexikon Kriminologie des Lehrstuhls für Kriminologie und Polizeiwissenschaft der Ruhr-Universität Bochum, http://vmrz0183.vm.ruhr-uni-bochum.de/krimlex/artikel.php?BUCHSTABE=S&KL_ID=177*
17 *wie etwa: www.cyberterrorism.org*
18 *Sarah Gordon, Richard Ford: Cyberterrorism? Symantec Whitepaper, Cupertino, 2003, http://www.symantec.com/avcenter/reference/cyberterrorism.pdf*
19 *Virtuelle Front; in: Der Spiegel, Nr. 30, 2007, S. 26 – 27, S. 27*
20 *http://www.bmi.bund.de/cln_028/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Gemeinsames__Terrorismusabwehrzentrum__de.html*
21 *Nationales Cyber-Abwehrzentrum nimmt Arbeit auf, BSI-Pressemitteilung vom 1.04.2011, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Cyber-Abwehrzentrum_01042011.html*
22 *Bundesinnenminister Dr. Hans-Peter Friedrich eröffnet das Nationale Cyber-Abwehrzentrum, BSI-Pressemitteilung vom 16.06.2011, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Eroeffnung-Nationales-Cyber-Abwehrzentrum_16062011.html*
23 *Der Spiegel: Bundeswehr baut geheime Cyberwar-Truppe auf, 07.02.2009, http://www.spiegel.de/spiegel/vorab/0,1518,606095,00.html*
24 *McAfee: Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare, Santa Clara, 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF*
25 *John Markoff; Andrew E. Kramer: In Shift, U.S. Talks to Russia on Internet Security; http://www.nytimes.com/2009/12/13/science/13cyber.html*
26 *Committee on Deterring Cyberattacks: Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for U.S. Policy; National Academy Press, Washington 2010*
27 *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, S. vi, Mai 2011, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*
28 *Ingo Ruhmann: Rüstungskontrolle gegen den Cyberkrieg? In: Telepolis, 4.01.2010, http://www.heise.de/tp/artikel/31/31797/1.html*