.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Inan, Alev (2007):

E-Dschihad. Der „Heilige Krieg“ und das Internet

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 53-61.

doi: 10.7396/2007_1_E

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Inan, Alev (2007). E-Dschihad. Der „Heilige Krieg“ und das Internet SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 53-61, Online: http://dx.doi.org/10.7396/2007_1_E.

Hinweis: Die gedruckte Ausgabe des Artikels ist in der Print-Version des SIAK-Journals im Verlag NWV (http://nwv.at) erschienen.

Online publiziert: 4/2014

E-Dschihad

DER "HEILIGE KRIEG" UND DAS INTERNET

ALEV INAN, MAG. DIPL.,
seit März 2006 Wissenschaftliche Mitarbeiterin am Lehrstuhl für Bürgerliches Recht an der Friedrich-Alexander Universität Erlangen-Nürnberg, Deutschland

Während Mitte der Neunziger Jahre die Anzahl der Websites islamistischer Terroristen auf knapp 100 Seiten geschätzt wurde, ist mittlerweile die Anzahl der Seiten, die sich dem "Heiligen Krieg" im Internet verschrieben haben, auf ca. 5.000 angestiegen. Davon werden wiederum die Inhalte von rund 100 Websites als sehr gefährlich eingestuft. Für diesen sprunghaften Anstieg geben Experten als einen der Gründe den Irakkrieg an. Das Internet ist für islamistische Terroristen zu einem viel genutzten Medium geworden. Der "E-Dschihad", der "Heilige Krieg" im Internet, hat viele Facetten. Meist wird das Internet zu Propagandazwecken verwendet, indem die religiös motivierten Terroristen Gewaltanwendung als legitimes Mittel gegen die Unterdrückung durch den Westen darstellen und um "Märtyrer" werben. Als psychologische Kriegsführung sind die Berichte, Fotos und Videos von den Enthauptungen "westlicher" Feinde zu bewerten, die vor allem Angst in der Bevölkerung auslösen sollen. Die neue Generation von "E-Dschihadisten" ist lokal ungebunden, weil sie nicht extra in Trainingslager in Afghanistan fahren müssen, sondern im Internet Handbücher zur Herstellung von Bomben und Giften vorfinden, um sich das nötige Wissen anzueignen. Der wohl wichtigste und gefährlichste Aspekt des "E-Dschihad" ist, dass terroristische Organisationen wie die al-Qa'ida das Internet intensiv als Kommunikationsmittel zur Koordination von Anschlägen genutzt haben und dies immer noch tun. Mit Hacker-Angriffen auf feindliche Websites versuchen radikal-islamische Aktivisten, die Medienaufmerksamkeit auf sich zu ziehen. Zu den größten Bedrohungen in der Zukunft gehört der Cyberterrorismus. Wenn islamistische Terroristen das nötige technische Wissen haben, dann sind computergesteuerte Anschläge auf Infrastruktur, Transportmittel und Kommunikationssysteme denkbar. Staatliche Sicherheitsmaßnahmen stehen vor der Aufgabe, die Gefahren durch Terroristen zu beheben und gleichzeitig ein Höchstmaß an Freiheiten, die das Internet bietet, für die Bürger in offenen Gesellschaften beizubehalten. Die Fülle und Bandbreite, wie das Internet für den "Heiligen Krieg" eingesetzt wird, gilt es zu analysieren und Möglichkeiten und Grenzen staatlicher Sicherheitsmaßnahmen zu diskutieren.

Das arabische Wort "Dschihad" bedeutet "sich bemühen" oder "sich anstrengen". Es wird im Islam unterschieden zwischen einem inneren (oder großen) "Dschihad" und einem äußeren (oder kleinen) "Dschihad". Der innere "Dschihad" bein-

Grafik: www.palestine-info.info/arabic/hamas

Inoffizielle Hompage der Hamas

haltet die individuelle Bemühung um den Glauben bzw die Anstrengung, ein islamkonformes Leben zu führen. Der äußere "Dschihad" ist ein Verteidigungskrieg oder ein offensiver Kampf zur Ausbreitung des Islam in nicht-muslimische Gebiete. In der Moderne zählt das Konzept des "Dschihad" zur Rhetorik radikaler islamistischer Bewegungen bei der Abgrenzung vom Westen (Elger 2004, 146). Die Entdeckung des Mediums Internet seitens islamistischer Terroristen für den "Dschihad" wurde mit verschiedenen Bezeichnungen versehen: "Digital Jihad" (Kirchner 1996), "Cyber-Jihad" (Lohlker 2002) oder "E-Jihad" (Bunt 2003). Michael Whine (1999) nennt fünf Gründe, warum das Internet für islamistische Terroristen eine so attraktive Option für ihre Aktivitäten darstellt: Erstens können sie sich über das Internet zusammenschließen und vernetzen. Zweitens bietet das neue Medium grundlegend Anonymität, wobei zusätzlich noch die Möglichkeit besteht, Websites durch Passwörter für andere unzugänglich zu machen. Drittens ist das Internet ein äußerst kostengünstiges Medium. Viertens ist das Internet als Multiplikator des Einflussbereichs nützlich. Und fünftens dient das Internet dazu, eine bestimmte Zielgruppe – speziell junge und gebildete Muslime – zu erreichen.

Welche islamistisch-terroristischen Gruppen nutzen nun das Internet? Einige der wichtigsten Gruppierungen sind, allen voran: al-Qa'ida, Ansar al-Islam ("Helfer des Islam"), al-Aqsa Märtyrer Brigaden, Palästinensischer Islamischer Dschihad, Islami Büyükdogu Akincilar Cephesi (IBDA-C) ("Front der Kämpfer für den Islamischen Großen Osten"), Hizb-ul Mujahideen, Hamas ("Islamische Widerstandsbewegung"), Hisbollah ("Partei Gottes"), etc.

Zudem fungieren auch Betreiber anderer Websites in der Rolle als Unterstützer und Helfer der Terroristen, indem sie zB Propagandamaterial von al-Qa'ida auf ihre Seiten stellen oder zu ihren Seiten verlinken (Weimann 2006, 72, 245 ff). Um nicht entdeckt zu werden, wechseln die "E-Jihad"-Seiten immer wieder ihre Internetadressen und/oder operieren aus Ländern, in denen sich die Terroristen in Sicherheit vor einer Strafverfolgung wähnen. Allerdings wurde im Oktober 2005 auch in Düsseldorf ein al-Qa'ida-Server entdeckt. Eine IT-Sicherheitsfirma fand heraus, dass radikal-islamistische Extremisten von diesem Server aus Material der terroristischen Vereinigung in türkischer Sprache verbreitet hatten (Schink 2005). Nachfolgende Ausführungen sollen aufzeigen, auf wie viele verschiedene Weisen das Internet für religiös motivierte terroristische Aktivitäten genutzt wird. Behandelt werden diese ausgewählten Aspekte: Propaganda und Rekrutierung, Psychologische Kriegsführung, Online-Ausbildung, Kommunikationsmittel zur Koordination von Anschlägen, Defacements (Hacker-Angriffe auf Websites) und Cyberterrorismus.

PROPAGANDA UND REKRUTIERUNG

Eine Art der Internetnutzung durch Extremisten ist die Verbreitung ihrer "Dschihad"-Ideologie. Dabei kann man drei rhetorische Strategien bei terroristischen Websites feststellen, um die eigene Anwendung von Gewalt zu rechtfertigen: Als erstes fällt auf, dass die Terroristen das Argument anführen, dass sie gar keine andere Wahl haben als Gewalt anzuwenden, da sie selbst Opfer der Repressionen ihrer Feinde sind. Auf den Webseiten werden die eigenen Gewalthandlungen heroisiert und als legitimer Widerstand dargestellt, während diejenigen des "Feindes" mit emotionalisierenden Worten wie "Abschlachten", "Mord" oder "Genozid" bezeichnet werden. Es soll dadurch der Eindruck erweckt werden, dass die eigene Gruppe die Unterlegenen des repressiven Staates oder des vermeintlichen Feindes seien. Eng verbunden damit ist die zweite Strategie, im Rahmen derer die Terroristen sich selbst als Freiheitskämpfer stilisieren, die eigentlich gegen ihren Willen dazu gezwungen sind, Gewalt anzuwenden, um die "Würde" ihrer Landsleute oder Glaubensbrüder zu schützen. Die Verantwortung für terroristische Gewaltanwendung ist somit nicht bei den Terroristen selbst zu suchen, sondern sie wird dem Feind übertragen. Zur Propaganda gehören auch die zahlreichen Berichterstattungen über die muslimischen Opfer aus Krisenregionen wie zB Tschetschenien, Afghanistan, Palästina und dem Irak. Die Fotos von blutüberströmten Kindern, Frauen und alten Menschen haben je nach Zielgruppe eine andere Funktion.

Bei westlichen Besuchern von "Dschihad"-Seiten kann es aufgrund der emotionalen Eindrücke zu Schuldgefühlen in den eigenen Reihen kommen und dadurch zu einem Wandel der öffentlichen Meinung (Weimann 2004a). Die Betreiber von diesen Webseiten intendieren bei der eigenen Gruppe, dass die Fotos starke Betroffenheit auslösen und zur Stärkung des Wir-Gefühls führen. Die Solidarisierung mit den muslimischen Opfern geschieht sowohl in der muslimischen Welt, als auch im Westen. Nicht selten finden sich auf diesen radikal-islamistischen Seiten dann auch Aufrufe zur Rekrutierung freiwilliger Kämpfer für den "Heiligen Krieg". Für die Radikalisierung junger Männer sehen Experten die mediale Propaganda als hauptsächlichen Grund an. Dazu sagt Johannes Schmalzl, Präsident des baden-württembergischen Landesamtes für Verfassungsschutz: "Ein 17 Jahre alter Mann kann sich innerhalb von wenigen Wochen in einen Selbstmordattentäter verwandeln, da spielen die Medien eine Rolle" (Soldt 2006). Die Legitimation für Selbstmordattentate entnehmen die "heiligen Krieger" dem Islam selbst, indem sie selektiv Koransuren, Hadithe und Rechtswerke anführen (Whine 1999). Der Internetforscher Manuell Castells stellt fest, dass es ein typisches Anzeichen für religiöse Extremisten ist, selektive Vorgehensweisen anzuwenden (Castells 2003, 15). Beim Vorgang der Rekrutierung an sich kommen vor allem die interaktiven (Chats, Foren) und multimedialen (Audio, Video) Funktionen des Internets zum Einsatz, da dadurch Informationen und Details auf diskretem Wege weitergegeben werden können.

PSYCHOLOGISCHE KRIEGSFÜHRUNG

Neben den beschriebenen Aspekten dient das Internet den islamistischen Terroristen auch dazu, dem Feind durch besonders barbarische Taten wie zB Exekutionen, die als Videos ins Internet gestellt werden, Angst einzuflößen. Diese Vorgehensweise ist entgegengesetzt zu derjenigen, die im vorherigen Punkt behandelt wurde, bei der die eigene Gewaltanwendung bewusst

nicht erwähnt wird. Eine psychologische Kriegsführung hat den Sinn, dass nicht nur auf das direkte Opfer der Gewalttat abgezielt wird, sondern auch auf die Betrachter aus dem feindlichen Lager. Eine wichtige Rolle kommt dabei auch den Massenmedien zu, da durch wiederholtes Ausstrahlen der brutalen Taten Panik bei den Zuschauern hervorgerufen wird. Die dadurch erzeugte Angst in der Bevölkerung kommt den Terroristen zugute, da sie es schaffen, das Individuum unter anderem in seinem Glauben an die Werte der eigenen Gemeinschaft und das richtige Handeln der eigenen Regierung zu erschüttern (Weimann 2006, 37).

Der mittlerweile getötete Abu Mussab al-Sarkawi, Anführer der al-Qa'ida im Irak, hat wie kein anderer von brutalen medienwirksamen Inszenierungen Gebrauch gemacht. Nur ein Beispiel ist die Enthauptung der amerikanischen Geisel Nick Berg (Eben 2006). Aber auch die zahlreichen anderen al-Qa'ida-Webseiten bieten Videos, CD-ROMs, DVDs, Fotos etc mit brutalen Inhalten an. Hamas und Hisbollah verwenden das Internet, um

Foto: www.palestine-info.co.uk

Verletzter palästinensischer Junge auf www.palestine-info.co.uk

sozusagen eine "Buchführung" über Tote zu machen, indem sie aktuelle Statistiken auf ihrer Website zu den Kategorien "Märtyrer", "Israelis" und "Kollaborateure" erstellen (Weimann 2004a).

Die psychologische Kriegsführung wird gezielt und bewusst von den terroristischen Organisationen eingesetzt.

Die Hisbollah macht aus diesen Absichten kein Geheimnis. Der eigene Fernsehsender al-Manar ist extra dazu geschaffen worden, und auf der Homepage www.manartv.com.lb heißt es in einer Selbstbeschreibung: "al-Manar ist die erste arabische Anstalt, die eine effektive psychologische Kriegsführung gegen den zionistischen Feind führt" (Weimann 2006, 36).

Zum medialen Krieg gehören auch die zahlreichen Bekennerschreiben, die nach erfolgter Tat ins Netz gestellt werden. Mittlerweile sind jedoch nicht einmal Arabischkenntnisse nötig, da Sympathisanten in einem Weblog die Dokumente ins Deutsche übersetzen. Die Rede ist hier von der Seite "Globale Islamische Medienfront" (GIMF), die sich als Sprachrohr der irakischen al-Qa'ida versteht (Musharbash 2006).

Grafik: www.albasrah.net

Website "www.albasrah.net"

DIE ONLINE-AUSBILDUNG

Eine eher "praktische" Komponente des Internets ist die Brauchbarkeit als virtuelle Ausbildungsstätte. Die jüngsten Ereignisse – wie die vereitelten Flugzeuganschläge in England oder die verhinderten Anschläge der Kofferbomber in Deutschland im Sommer 2006 – zeigen, mit welcher Leichtigkeit die Täter die nötigen Informationen zum Bombenbasteln bekommen. Man braucht nur zu "googeln" (Frasch/ Koch 2006). Im World Wide Web gibt es zahlreiche Handbücher mit detaillierten Anleitungen, wie Gifte oder Bomben hergestellt werden können. Bert Weingarten von der IT-Firma PAN AMP antwortet auf die Frage, wie viele Bombenbauanleitungen im Internet kursieren: "Wir gehen weltweit von einer siebenstelligen Zahl aus. Allein in Deutschland kommen pro Quartal 3.000 neue Pläne hinzu" (Pabst 2006). Bekannte Beispiele für den Bombenbau sind "The Terrorist's Handbook" und "The Anarchist Cookbook".

Das von Abdel-Aziz 1996 verfasste "Mujahadeen Poisons Handbook" wurde auf der offiziellen Homepage der Hamas veröffentlicht.

Auf 23 Seiten erhält der "Dschihadist" das nötige Wissen darüber, wie man selbst verschiedene Gifte und gefährliche Gase für terroristische Anschläge herstellt. "The Encyclopedia of Jihad" der al-Qa'ida wiederum instruiert auf fast 1.000 Seiten, wie man eine Untergrundorganisation gründet und Anschläge ausführt (Weimann 2004a).

Wenn Schwierigkeiten bei der "Do-it-yourself"-Herstellung von Giften oder Bomben auftreten sollten, können sich die Zöglinge Hilfestellung von ihren erfahreneren Glaubensbrüdern in Chatrooms holen. Bezeichnend ist, dass sich Terroristen diese Option bewusst zu eigen machen. Al-Qa'ida preist die neuen Möglichkeiten in dieser Weise an: "Oh Mujaheddin-Bruder, du musst nicht mehr weit reisen, um in unsere großartigen Ausbildungslager zu kommen. Das Trainingsprogramm kannst du auch allein oder mit anderen Brüdern absolvieren" (Thamm 2006). Die Konsequenzen der Online-Ausbildung sind jedoch, dass die Generation der E-Terroristen, weil sie nicht mehr die "klassische" Schulung erhält, über weniger fundierte Kenntnisse verfügt. Allerdings hat diese Methode aus Sicht der Terrorgruppen den "Vorteil", dass schnelle Operationen durchgeführt werden können. Der kurze Zeitraum von der Rekrutierung bis zum tatsächlichen Anschlag gewährleistet den Terroristen mit hoher Wahrscheinlichkeit unerkannt zu bleiben, da sie noch nicht von Sicherheitsbehörden beobachtet werden (Thamm 2006).

KOMMUNIKATIONSMITTEL ZUR KOORDINATION VON ANSCHLÄGEN

Das Internet wird von terroristischen Gruppen darüber hinaus als Kommunikationsmittel zur Koordination von Anschlägen genutzt. Interaktive Funktionen wie das Chat und vor allem E-Mails sind in diesem Zusammenhang von Bedeutung. Die Schwierigkeit für Sicherheitsbehörden, die sich bei der Beobachtung von Chats mit vermuteten terroristischen Aktivitäten ergibt, ist offensichtlich. Eine allumfassende Überwachung ist schlichtweg nicht durchführbar.

Die Möglichkeiten im World Wide Web sind zu vielfältig, sodass keine hundertprozentige Kontrolle des Internets gewährleistet werden kann.

Beobachtungen seitens Sicherheitsbehörden können lediglich selektiv vorge-

nommen werden.

Die Probleme, die beim Observieren der Kommunikation via E-Mail auftreten, sind ähnlich gelagert. Mit Hilfe von Verschlüsselungsprogrammen gelingt es islamistischen Terroristen Informationen auszutauschen. Die palästinensische Terrororganisation Hamas beispielsweise – die Anfang 2006 durch demokratische Wahlen zur politischen Führungspartei gewählt wurde – verwendete diese Methode, um sich verschlüsselte Botschaften mit Lageplänen, Adressen, technischen Details etc für anstehende Operationen zukommen zu lassen (Bunt 2003, 57). Auch al-Qa'ida hat für die Vorbereitung und Koordination der Anschläge vom 11. September 2001 das Internet intensiv genutzt (Vertigans/Sutton 2001). Nachdem der Planungschef Bin Ladens, Abu Zubayda, festgenommen wurde, konnten auf seinem Computer tausende verschlüsselte Nachrichten gefunden werden. Um nicht entdeckt zu werden, hatten die al-Qa'ida-Terroristen auch darauf geachtet, ihre Nachrichten von öffentlichen Plätzen und E-Mail Accounts zu verschicken (Weimann 2004a).

Die Bemühungen seitens der Sicherheitsbehörden, verschlüsselte Nachrichten zu entschlüsseln, erscheinen beinahe aussichtslos, da es zu viele mögliche Kombinationen gibt.

Das Verschlüsselungspropramm "Advanced Encryption Standard" (AES) bietet beispielsweise Codeschlüssel an, bei denen einer Zahl 77 Nullen folgen. Das ergibt eine Ziffer, die man mit der Gesamtzahl aller Atome im Universum vergleichen könnte (Jolish 2002). Geradezu paradox erscheint die Tatsache, dass Verschlüsselungsprogramme ganz einfach im Internet bezogen werden können. Ein Beispiel wäre hier die Verschlüsselungssoftware ShyFile, die man sich als Probeversion kostenlos herunterladen kann. Dieses Computerprogramm enthält auch einen File Shredder, der die Originaldokumente unwiderruflich zerstört.

Eine der neuesten Varianten, wie islamistische Terroristen ihre elektronischen Nachrichten schützen, ist, dass sie die E-Mails erst gar nicht verschicken. Stattdessen werden die Nachrichten als Entwürfe im E-Mail Account abgespeichert. Alle, die das Passwort für diesen E-Mail Account kennen, haben somit die Möglichkeit, die Botschaften zu lesen (Eben 2006).

DEFACEMENTS: HACKER-ANGRIFFE AUF WEBSITES

Auf virtueller Ebene findet sich eine besondere Variante der Internetnutzung durch religiöse Extremisten: "Hacken im Namen Gottes". Islamistische Gruppierungen oder Einzelpersonen greifen dabei Webseiten ihrer Feinde an. Als Beispiel können hier die World's Fantabulous Defacers (WFD) angeführt werden. Die Gruppe besteht hauptsächlich aus pakistanischen Hackern und hat sich auf Anschläge israelischer Ziele spezialisiert. Das englische Wort "deface" bedeutet "entstellen" oder "verunstalten".

Der Name der World's Fantabulous Defacers (WFD) ist gleichzeitig ihr Programm: Internetauftritte des Feindes werden "verunstaltet".

Im Jahre 2001 hackte die WFD zB die Website der Wahlkampagne von Ariel Sharon. Die Hacker behielten das originale Format bei, veränderten jedoch Bilder und Texte auf der Seite. Als Foto war unter anderem ein schwer verletztes Kind vor

einem Haus zu sehen, das von israelischen Siedlern niedergebrannt worden war. Als Text waren von den Hackern auf Ariel Sharons Wahlkampfseite folgende Parolen platziert worden: "Long live Hizballah! Long live Palestina! Long live Chechnya, Kashmir, Kosovo and Bosnia!" Die Motivation für derlei Hackerangriffe ist es, möglichst viel Aufsehen in der Öffentlichkeit zu erregen (Bunt 2003, 55). Das Wissen um diese Art von virtuellen Angriffen ist einer der Gründe, warum die Angst vor strategischen Anschlägen, wie sie dem Cyberterrorismus eigen sind, so groß ist.

CYBERTERRORISMUS

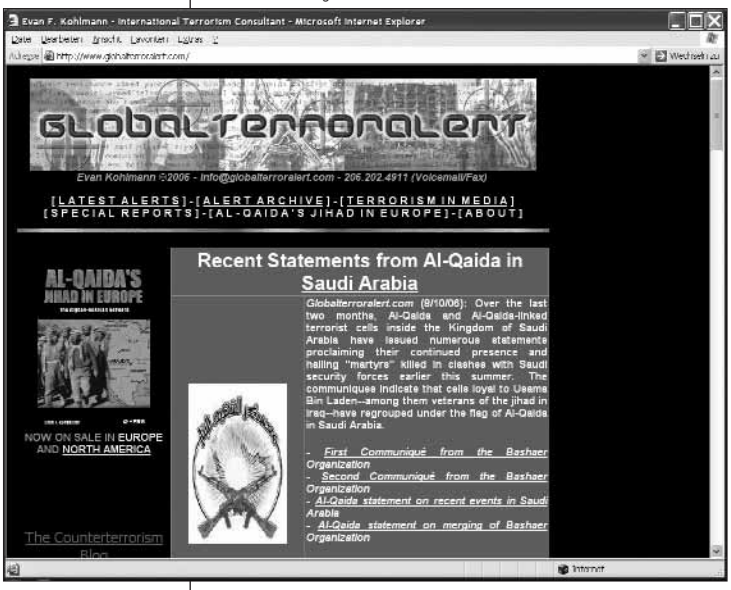
Der wesentliche Unterschied zwischen den oben genannten Hacker-Angriffen und dem Cyberterrorismus ist, dass der "Austragungsort" der Anschläge unterschiedlich ist. Während sich diese Hacker-Attacken auf virtuellem Raum abspielen, wird unter Cyberterrorismus der computergesteuerte Angriff auf reale Ziele verstanden. Islamistische Terroristen könnten den Computer in Zukunft als Waffe einsetzen. Besonders gefährdete Objekte wären: Transportverbindungen, Energieunternehmen, Kernkraftwerke, Dämme, Militärcomputer etc. Der zu erwartende Schaden des Cyberterrorismus wäre immens, denn in westlichen Gesellschaften werden Rechnersysteme immer unentbehrlicher – sei es im Finanzwesen, im Transportwesen oder in der Energieversorgung. Die hohe Abhängigkeit von Computern könnte zur Zielscheibe für eine neue Generation von Terroristen werden, die über das nötige technische Wissen verfügen, um einen Anschlag verüben zu können (Weimann 2005).

Paradox an der Situation ist, dass Informationen für mögliche Angriffsziele der Terroristen aus dem Internet stammen.

Verton weist zwar darauf hin, dass Militär- und Sicherheitsbehörden schon vor dem 11. September 2001 Anweisung hatten, sensitive Daten wie Abbildungen von Steuerungs- und Kontrollknotenpunkten, Informationen zur Computer- und Kommunikationsstruktur, Telefonnummern der einzelnen Abteilungen, Berichte über technische Innovationen, Karten und geographische Daten etc nicht auf ihren Webseiten zu veröffentlichen (Verton 2003, 117). Aber anscheinend sind die bestehenden Vorsichtsmaßnahmen noch nicht ausreichend bzw scheint der Erkenntnisgewinn für die Terroristen sich nicht nur auf die Seiten von Militär- und Sicherheitsbehörden zu beschränken. Denn das amerikanische Verteidigungsministerium hat im Jahre 2003 erneut bekannt gegeben, dass das Internet die Hauptinformationsquelle für Terroristen ist. Ein in Afghanistan entdecktes Trainingshandbuch der al-Qa'ida enthält den Hinweis, dass man 80% der Informationen über den "Feind" aus öffentlich zugänglichen Quellen erhalten könne (Thomas 2003).

Doch wie wahrscheinlich ist es, dass es tatsächlich zu einem Anschlag durch Cyberterroristen kommt? Umfragen unter Computerexperten nach dem 11. September 2001 haben ergeben, dass sie dies für die größte Bedrohung unserer Zeit halten. Auch das besondere Augenmerk seitens Regierungen, die immense Summen für Sicherheitsmaßnahmen im IT-Bereich investieren, ist bezeichnend. Allerdings weist Weimann darauf hin, dass bis zum heutigen Tage kein einziger Anschlag à la Cyberterrorismus verübt worden ist. Als Grund für das Ausbleiben vermutet er,

Grafik: www.globalterroralert.com



Homepage des Internetbeobachters Evan Kohlmann: www.globalterroralert.com

dass Terroristen das technische Know-how noch nicht haben. Mit der zukünftigen Generation von Terroristen, die bereits mit Computern aufwächst, werden Anschläge per Computer wahrscheinlicher als heute sein (Weimann 2004b).

MÖGLICHKEITEN UND GRENZEN STAATLICHER SICHERHEITSMAßNAHMEN

Wie können angesichts dieser Bedrohung aus verschiedenen Facetten des "E-Jihads" Gegenmaßnahmen aussehen? Yael Shahar vom "Institute for Counter Terrorism" (ICT) schlug auf der "Euroscience Open Forum" (Esof) 2006 in München vor, dass man die Nutzung des Internets als Waffe behindern müsse. Das Sicherheitsgefühl, in dem die Terroristen sich wähnen, müsse grundlegend erschüttert werden. Zu den Vorschlägen zur Bekämpfung der E-Terroristen zählen: Ausspähen der PCs von Terroristen, Lahmlegen der PCs mit Hilfe von Viren, Überwachen von Chatrooms (Grosse 2006). An dieser Stelle sei auf die verschiedenen "Internet watchdogs" wie www.haganah.org.il oder www.globalterroralert.com hingewiesen, die sich auf die Beobachtung von radikal-islamistischen Seiten spezialisiert haben und ihre Dienste unter anderem Regierungen zur Verfügung stellen.

Polizeibehörden sind seit Jahren in der Terrorfahndung im Internet tätig.

In Deutschland ist für die Beamten eine entsprechende Ausbildung angestrebt, damit sie die Ergebnisse aus dem Web besser verwerten können.

Als Schwachstelle wird konstatiert, dass man bestehende Programme aus der freien Wirtschaft nicht für die Recherche und zum Ausfindigmachen der Server, die terroristische Inhalte verbreiten, nutzen würde. Im Polizeibereich versuche man eher eigene Lösungen und Strategien zu entwickeln anstatt vorhandene Tools zu kaufen (Prevezanos 2006).

Einigkeit herrscht bei den Experten, die sich mit der Thematik beschäftigen darüber, dass es ineffektiv ist, islamistisch-terroristische Websites sofort nach ihrer Entdeckung zu schließen, denn dadurch beraubt man sich gleichzeitig auch wertvoller Informationen, um Anschläge verhindern zu können. Das Abstellen der Seiten sei ohnehin immer nur eine kurzfristige Lösung. Viel wichtiger ist es, die Webmaster der Terroristenseiten zu stoppen (Eben 2006; Thamm 2006; Weimann 2004a). Neben dem Aspekt, dass Sicherheitsbehörden die Informationen im Internet über die Terroristen nutzen könnten, spricht sich Weimann noch aus einem anderen Grund gegen drakonische Mittel aus. Das Internet gilt als Inbegriff demokratischer Werte in Form von Meinungsfreiheit und offener Kommunikationsform. Autoritäre Staaten wie China sind dafür bekannt, dass

sie unliebsame Inhalte zensieren. Aber auch westliche Demokratien bedienen sich im Zuge der Anti-Terror-Bekämpfung Mittel, die Freiheiten im Internet zu beschneiden. Bei all diesen Überlegungen hat die Sicherheit der Menschen oberste Priorität und es besteht die Notwendigkeit wirksam gegen den "E-Jihad" vorzugehen. Die Kunst wird es sein, eine Ausgewogenheit zwischen der Sicherheit und den Freiheiten offener Gesellschaften herzustellen (Weimann 2006, 203).

Quellenangaben

Bunt, G. R. (2003). Islam in the Digital Age. E-Jihad, Online Fatwas and Cyber Islamic Environments, London, Sterling.

Castells, M. (2003). Die Macht der Identität. Teil 2 der Trilogie: Das Informationszeitalter, Opladen.

Eben K. (2006). Terrorists and the Internet, http://www.cfr.org/publication/10005/, 12.05.2006.

Elger, R. (Hg) (2004). Kleines Islam-Lexikon. Geschichte – Alltag – Kultur, Bonn.

Frasch, T./Koch, B. (2006). Die Bombe aus dem Netz, in: Frankfurter Allgemeine Zeitung, 03.08.2006.

Grosse, A. (2006). Attentäter im Netz aufspüren, http://www.abendblatt.de/daten/2006/07/18/587667.html, 18.07.2006.

Jolish, B. (2002). The encrypted jihad, http://www.salon.com/tech/feature/2002/02/04/terror_encryption/print.html, 07.07.2005.

Kirchner, H. (1996). Digital Jihad. Islam im Internet, in: Der Überblick (32, 4), 19.

Lohlker, R. (2002). Cyberjihad. Das Internet als Feld der Agitation, in: Orient (43, 4), 510.

Musharbash, Y. (2006). Al-Qaidas deutsche Lautsprecher, http://www.spiegel.de/politik/deutschland/0,1518,434203,00.html, 29.08.2006.

Pabst, S. (2006). Internet-Fahnder suchen Bomben-Bauanleitungen, in: Hamburger Abendblatt, 14.08.2006.

Prevezanos, K. (2006). Terrorgefahr aus dem Internet,http://www.dw-world.de/dw/article/0,2144,2149341,00.html, 29.08.2006.

Schink, P. (2005). Al-Qaeda-Server in Düsseldorf entdeckt, http://www.netzeitung.de/internet/362272.html,17.10.2005.

Soldt, R. (2006). Die virtuelle Welt des Terrorismus, in: Frankfurter Allgemeine Zeitung, 24.08.2006.

Thamm, B. G. (2006). Der Heilige Krieg ist Internet-gesteuert, http://www.sicherheit-heute.de/politik,205,Der_Heilige_Krieg_ist_Internet-gesteuert.htm,14.05.2006.

Thomas, T. L. (2003). Al Qaeda and the Internet: The Danger of "Cyberplanning". http:///fmso.leavenworth.army.mil/documents/alqaedainternet.HTM, 20.06.2005.

Vertigans, S./Sutton, P. (2001). Back to the future: Islamic terrorism and interpretations of past and present, http://www.socresonline.org.uk/6/3/vertigans.html, 17.06.2005.

Verton, D. (2003). Black Ice: The Invisible Threat of Cyber-Terrorism, New York.

Weimann, G. (2004). www.terror.net: How Modern Terrorism Uses the Internet, http://www.usip.org/pubs/specialreports/sr116. pdf,01.04.2006 (zitiert a).

Weimann, G. (2004). Cyberterrorism: How Real Is the Threat?, http://www.usip.org/pubs/specialreports/sr119.pdf, 01.04.2006 (zitiert b).

Weimann, G. (2005). Cyberterrorismus ist eine große, schwarze Wolke am Horizont, http://www.sicherheitheute.de/technik,177,Cyberterrorismus_ist_eine_schwarze_Wolke_am_Horizont. htm, 01.05.2006.

Weimann, G. (2006). Terror on the Internet. The New Arena, the New Challenges, Washington, DC.

Whine, M. (1999). Cyberspace. A New Medium for Communication, Command, and Control by Extremists, http://www.ict.org.il/articles/cyberspace.htm,17.06.2005.