Inhaltsverzeichnis

Terror - Hacker lassen Flugzeuge aufeinanderprallen

Tausende Flüge fallen täglich wegen des Vertrauensverlusts der Passagiere aus. Gibt es noch eine Zukunft für die Fluggesellschaften?

Nach dem Terroranschlag vor drei Wochen, bei dem unbekannte Hacker zwei Flugzeuge über San Francisco aufeinanderprallen und 200 Passagiere umkommen ließen, dauern noch immer intensive Ermittlungen an. Bisher ist noch nicht klar, wie die unbekannten Täter die Steuerung über eines der Flugzeuge übernehmen konnten. Der FBI-Chef James Comey hat bei der gestrigen Pressekonferenz erneut nur Vermutungen über den Cyberanschlag äußern können. Es ist nicht einmal klar, ob die Angreifer selbst an Bord waren oder ob sie die Kontrolle vom Boden übernommen haben. Eine Möglichkeit ist, dass sich die Hacker in der Passagierkabine durch eigene Geräte mit den Schnittstellen unterhalb der Sitze verbunden haben und so in die Computersysteme des Flugzeugs eingedrungen waren. Eine andere Möglichkeit ist, dass sie einen Schadcode auf einem Passagier-Gerät in das Flugzeug schmuggeln und sich so mit dem Flugzeug-Netzwerk durch WLAN verbinden konnten. Fraglos ist nur, dass sie in das Steuerungssystem eingedrungen sind und die Leistung der Triebwerke und dadurch den Kurs des Flugzeugs manipuliert haben. Das Fluggeschäft in den USA ist fast am Boden. Wie werden die US-Amerikaner noch einen Angriff wie den 9/11 vor 20 Jahren verkraften können?[1]

Könnte in der nahen Zukunft ein solcher Tageszeitungsartikel tatsächlich erscheinen? Im Jahre 2015 würden EU-Bürgerinnen und EU-Bürger dieses Ereignis noch immer eher in einen Science-Fiction-Roman einordnen, als es als eine Möglichkeit unserer digitalen Realität anzuerkennen. Die Voraussetzungen für einen Flugzeug-Terroranschlag, der für die Wirtschaft und viele andere Bereiche (z.B. wegen Einleitung neuer Terrorismusbekämpfungsmaßnahmen vonseiten der Regierungen) schwere Folgen haben würde, sind jedoch schon gegeben. In einem aktuellen Bericht[2] des US-Rechnungshofs GAO (Government Accountability Office) der US-Luftfahrtbehörde FAA (Federal Aviation Administration) wird vor dem hohen potenziellen Risiko der derzeit eingesetzten Systeme in den USA gewarnt. Da bei Flügen in den USA häufig WLAN angeboten wird, sind Flugzeuge Angriffen ausgesetzt, die sich von Hackerangriffen am Boden nicht viel unterscheiden[3]. Das Internet Protokoll

> wird dabei nicht nur für die Bereitstellung von Drahtlos-Internet für Passagiere eingesetzt, sondern findet mitunter auch Verwendung beim Entertainment-System des Flugzeugs, beim Cockpit-Kommunikationssystem sowie beim Next Generation Air Transportation System – ein für 2025 geplantes, neues System für das Flugverkehrsmanagement. Im Bericht des GAO heißt es: „IP-Netzwerke erlauben einem Angreifer, Avionik-Systeme übernehmen zu können.[4]

---

[1] Vgl. *Flugzeuge über Inflight-Wi-Fi kapern und fremdsteuern*, o.S.
[2] Abzurufen unter http://www.gao.gov/assets/670/669627.pdf
[3] Vgl. Nguyen, o.S.
[4] Nguyen, o.S.

Das Risiko geht dabei einerseits von mitreisenden Kriminellen sowie von Hackern von außerhalb aus.[5] Ein Cyberangriff auf fliegende Flugzeuge ist also keine Science-Fiction mehr.

Wissenschaftlicher Diskurs

In der Tagespresse lesen wir ständig, dass täglich tausende Cyberangriffe auf unterschiedliche Ziele ausgeübt werden: auf Webseiten der Regierungen (z.B. Datennetz des Deutschen Bundestags, 2015), Medienhäuser (die französische Fernsehgruppe TV5 Monde, 2015), Finanzinstitute (JP Morgan, 2014) oder Energieunternehmen (Energieversorger in Norwegen, 2014). Forscher warnen, dass unter diesen Angriffen insbesondere die auf die sogenannten Kritischen Infrastrukturen ernst zu nehmen sind. Nach dem Bericht des Bundesministerium des Inneren *Die Lage der IT-Sicherheit in Deutschland* von 2014 werden unter Kritischen Infrastrukturen (KRITIS) Institutionen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen verstanden, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Neun Sektoren gelten in Deutschland derzeit als Kritische Infrastrukturen: Transport und Verkehr, Energie, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Staat und Verwaltung, Ernährung, Wasser, Gesundheit, Medien und Kultur[6]. Cyberangriffe, die für die öffentliche Sicherheit gefährlich (und so für Cyberterroristen attraktiv) wären, würden sich also auf diese Ziele richten:

- Stromversorgung
- Versorgung mir Erdöl, Erdgas, Heizöl, Treibstoffen, Kraftstoffen, Schmierstoffen etc.
- Nationale Kommunikationsnetze (Telefon-Netze, GSM, Funknetze, BOS-Funk)
- Vernetzung der Banken, Geldautomaten, EC-Kartensysteme, Kreditkarten etc.
- Smart-Meter in Haushalten
- Steuerungssysteme in intelligenten Häusern (Smart Homes)
- vernetzte Computersysteme (das ominöse „Internet“)
- Industriesteuerungsanlagen (SCADA)
- Satelliten
- Geo-Positionssysteme (GPS, Glonass, Galileo)
- Steuerungsanlagen in der Luft- und Raumfahrt, Drohnensteuerung[7]

Wie ernst die Gefahr vor Angriffen auf die KRITIS ist, zeigt auch die Tatsache, dass der Deutsche Bundestag in Juni 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) verabschiedet hat, dessen Zweck es u.a. ist, Kritische Infrastrukturen vor Cyberangriffen zu schützen. Wie wahrscheinlich ist es aber, dass ein Cyberangriff von Terroristen

[5] Vgl. Nguyen, o.S.
[6] Vgl. Bundesamt für Sicherheit und Informationstechnik, S. 41
[7] Vgl. Schumacher, S. 169

durchgeführt wird? Die Frage ist umstritten und die Meinungsverschiedenheiten unter Forschern und Wissenschaftlern hängen vor allem mit dem Begriff und der Definition des Terrorismus zusammen. Es geht darum, ob die traditionellen Definitionen des Terrorismus auf die Angriffe in der Cyberwelt anwendbar sind.

Geschäftsführender Direktor des Magdeburger Instituts für Sicherheitsforschung und Herausgeber des Magdeburger Journals zur Sicherheitsforschung, Stefan Schumacher, stützt sich in seinem Beitrag zum Jahrbuch Terrorismus 2013/2014 *Cyber Terrorismus – Reale Bedrohung oder Mythos?* auf die folgende Definition:

> Im Allgemeinen lässt sich unter Terrorismus die systematisch vorbereitete Planung und Durchführung illegaler Gewaltakte durch temporär oder dauerhaft zusammengesetzte Gruppen, die in der Regel konspirativ und subversiv, national und international mit der Zielsetzung kooperieren, eigene oder im Auftrag zu erfüllende politische Ziele zu erreichen. […] Das wesentliche Ziel des politischen Terrors ist die Abschaffung bestehender Herrschaftsverhältnisse, die Beseitigung bestehender Herrschaftseliten und die Etablierung radikaler Alternativen unter Zuhilfenahme von Gewalt, Schrecken und Terror. Zugleich soll aber auch in Teilen der Bevölkerung Sympathie und Unterstützungsbereitschaft erzielt werden.[8]

Es geht also um die Art und Weise, wie Anschläge geplant und zu welchem Zweck sie durchgeführt werden. Schumacher kommentiert die problematischen Stellen in dieser Definition, die auf die digitale Welt schwer übertragbar sind. Erstens sei es unklar, ob es „Gewaltakte" gegen Computer- oder Netzwerksysteme geben kann. Er bezieht sich jedoch darauf, dass § 303 StGB den Vorgang als Sachbeschädigung, bzw. präziser §§ 303a und 303 StGB als Datenveränderung und Computersabotage bezeichnet. Man könne diese Vorkommnisse als Gewalt gegen Sachen betrachten. Außerdem bestehe immer die Möglichkeit, durch Datenveränderung und Computersabotage IT-Systeme derart zu manipulieren, dass Menschen in ihrer körperlichen Unversehrtheit eingeschränkt werden[9]. Ein anderer kritischer Punkt in der Definition, den Schumacher anspricht, ist der Bezug auf das Ziel eines Terroraktes: „Es ist zumindest bisher nicht möglich, durch Angriffe im Internet bestehende Herrschaftsverhältnisse abzuschaffen und bestehende Herrschaftseliten zu beseitigen"[10]. Schumacher behauptet folglich, dass aus diesem Grund der Cyberterrorismus als neue, andere Form des Terrorismus *sui generis* nicht existiert.

Andere Forscher sind ähnlicher Meinung. Zu ihnen gehört der schwedische Sicherheitsexperte Roland Heickerö, der in seiner Publikation *Cyberterrorismus: der elektronische Jihad, eine Strategieanalyse* (*Cyber Terrorism: Electronic Jihad, Strategic Analysis*) über die Logik des Terrorismus schreibt. Sie basiere auf der Angst vor unvorhersehbaren Angriffen, die zu jedem Zeitpunkt ausgeführt werden

[8] Meier et al. zitiert in Schumacher, S. 59
[9] Vgl. Schumacher, S. 166-167
[10] Schumacher, S. 173

können, auf leicht angreifbare Ziele ausgerichtet sind und bei denen es die Täter nicht interessiert, wer ihre Opfer sind. Für Heickerö liegt das Wesen des Terrorismus im Gefühl des Terrors. Es gehe darum, Menschen zu schockieren und sich machtlos fühlen zu lassen, wobei bei ihnen auch Misstrauen darüber ausgelöst werden sollte, dass die Regierungsstrukturen über Kapazitäten verfügen, ihren Bürgern Sicherheit zu gewährleisten. Neben diesen Eigenschaften zeichnen einen Terroranschlag außerdem menschliche Verluste und folglich ein großes Aufsehen in den Medien aus. Die Aufmerksamkeit soll dafür sorgen, dass die politischen Ziele der Terrorgruppe der Öffentlichkeit offenbart und ihre Stärke gezeigt wird.[11] Bei dem Versuch, diese Eigenschaften auf Cyberterrorismus anzuwenden, unterstützt Heickerö die Definition der US-amerikanischen Forscherin zu IT-Sicherheit, Dorothy Dennings: Damit ein Cyberangriff als Terrortat bezeichnet werden kann, muss seine Absicht sein, schwere menschliche und wirtschaftliche Verluste herbeizuführen und der Bevölkerung Schreck und Terror einzujagen. Die Absicht der Angreifer ist also die Eigenschaft, die bestimmt, ob ein Cyberangriff Terroristen zugeschrieben werden kann[12]. Juristen Sigmar Stadlmeier und Walter J. Unger gehen in ihrer Arbeit *Cyber-War und Cyber-Terrorismus aus völkerrechtlicher Sicht* in eine ähnliche Richtung und lassen den Aspekt der menschlichen Verluste eines traditionellen Terrorangriffes aus der Definition des Cyberterrorismus aus: „Cyber-Terrorismus (CT) sind computergestützte kriminelle Akte zur Beeinträchtigung von Informationen, Informationssystemen und informationsgestützten Prozessen, mit denen Unsicherheit, Verwirrung, Angst/Panik etc. hervorgerufen werden sollen, um eigene politisch-strategische Ziele durchzusetzen bzw. Regierungen zu einem bestimmten Handeln zu veranlassen“[13]. Wieder liegt der Schwerpunkt auf Angst und Terror. Dazu argumentiert Heickerö, dass die Spieler in der digitalen Arena die gleichen politischen, ideologischen und religiösen Ziele wie die „traditionellen“ Terroristen haben, aber dass sie sich anders benehmen und mit anderen Mitteln arbeiten. Sie sind keine Selbstmordattentäter und das Aufsehen in den Medien ist kein Zweck in sich selbst. Stattdessen versuchen die digitalen Terroristen, ihre Spuren im Internet so gut wie möglich zu verstecken. Auch der Unterschied, den manche zwischen Cyberterroristen und Terroristen, die Internet nur als Mittel für z.B. Propaganda oder Training nutzen, wird immer verschwommener. Der „richtige“ Cyberterrorist versteckt sich, zumindest solange bis der Anschlag im voll geplanten Umfang durchgeführt wird[14]. Dieser Logik entsprechend könnte Cyberterrorismus einen obligatorischen Aspekt des traditionellen Terrorismus verloren haben – Blutvergießen (was nicht heiß, dass es immer ausfällt). Cyberterrorismus ist also eine Erscheinungsform, die sich aus dem traditionellen Terrorismus entwickelt hat. Er bedient sich anderer Mittel, wird aber wegen ähnlicher politischer und ideologischer Ziele ausgeführt.

Heickerö ist der Meinung, dass es nur logisch ist, dass die Terroristen versuchen werden, die Abhängigkeit der modernen Gesellschaft von Computernetzwerken und der mobilen Kommunikation

[11] Vgl. Heickerö, S. 554
[12] Vgl. Heickerö, S. 555
[13] Unger et al. zitiert in Stadlmeier et al., S. 63
[14] Vgl. Heickerö, S. 555

auszunutzen[15]. Ein wachsendes Problem seien die Versuche von Terroristen, in Datenbanken einzudringen, um empfindliche Informationen über verschiedene Objekte, deren Datenstrukturen und Informationen zu Sicherheitsniveaus zu sammeln. Es sei anzunehmen, dass Gruppen wie Cyberterroristen ein Interesse daran haben, wichtige Infrastrukturen und Ziele, die eingegriffen werden können, zu studieren. Eine weitere Gefahr gehe davon aus, dass in einer schützenswerten Datenbank absichtlich Informationen verändert werden können, wie, z.B., die in den Steuerungssystemen von Flugzeugen[16]. Ähnlich wie bei traditionellen terroristischen Angriffen, planen auch Cyberterroristen ihre Attacken und Cybereinsätze sorgfältig und mit einer klaren Absicht. Obwohl für einen Angriff nicht mehr als ein paar Täter nötig sind, kann er verheerende Folgen haben. Ein solcher Angriff wird eher auf zivile als militärische Ziele ausgeübt, da sie viel verwundbarer und die gesellschaftlichen Folgen größer sind. Überdies erregen zivile Ziele eine größere Sensation in den Medien. Heickerö meint, dass der Trend des Cyberterrorismus Mitte des ersten Jahrzehnts dieses Jahrhunderts angefangen hat, als Terroristen ihre Ziele und *modus operandi* zu ändern/erweitern begannen. Sie sind von generell einfachen Methoden zum rationalen, ausgedachten Handeln mit einem bestimmten Zweck übergegangen. Heickerö nennt auch mehrere Inzidente, die unter Verdacht stehen, dass sie von Cyberterroristen begangen wurden, z.B. die Einsätze einer Reihe von Computerviren in den frühen 2000ern wie Nimda, Code Red, Love Bug und später Melissa. Es ist in den meisten Fällen noch unbekannt, wer hinter den Angriffen steht und unklar, welche die endgültigen Ziele waren und warum die Angriffe durchgeführt wurden - das Internet ermöglicht Anonymität, vorausgesetzt, dass man technische Kenntnisse besitzt, und weiß, wie die digitalen Spüren verwischt werden können. Die Auswirkungen dieser Attacken waren limitiert und entsprachen nicht der gewöhnlichen Logik des Terrorismus: Sie waren unspektakulär und brachten keine Todesopfer hervor. Bis heute ist keine Cyberattacke bekannt, bei der Menschen gestorben sind. Heickerö beschreibt zwar einen Verdachtsfall, bei dem es aber nicht klar ist, wer ihn begangen hat: 2008 ist auf dem Flughafen Madrid-Barajas ein Flugzeug beim Starten verunglückt. Vor dem Unglück hat das Flugzeug wegen drei technischer Probleme ein Notsignal ausgesendet. Der zentrale Computer der Fluggesellschaft Spanair hat aber keinen Notfallalarm ausgelöst, weil ihn ein auf ihn installierter Trojaner daran gehindert hat. Die Folgen waren desaströs – das Flugzeug ist abgestürzt und 154 Menschen sind umgekommen. Es konnte nicht entdeckt werden, wie der Trojaner installiert wurde und zu welchem Zweck. Es gibt auch keine Belege, dass es sich um einen Terroranschlag gehandelt hat. Nichtsdestotrotz zeigt dieser Vorfall, welche die Risiken und Folgen eines Cyber-Angriffs sein können. Solche Fälle können Unruhe und Misstrauen bei der Bevölkerung auslösen, denn es entsteht die Wahrnehmung, dass wichtige Systeme von ihren Betreibern (Staat oder Unternehmen) nicht genügend geschützt werden. Es wirft sich die Frage auf: Verfügen die Unternehmen und Staaten über die nötigen Kapazitäten, mit den Risiken, dem

[15] Vgl. Heickerö, S. 564
[16] Vgl. Heickerö, S. 556-557

Schadenpotenzial und den Krisen eines Cyberangriffs umzugehen? Dies könnte langfristig politische Folgen haben[17].

Dass Terroristen über Cyberangriffe nachdenken, zeigen nach Heickerö die Funde einer Polizeirazzia bei der islamischen Organisation al-Muhajiroun und deren Anführer Omar Bakri Muhammad, die 2005 in London durchgeführt wurde. In einem beschlagnahmten Dokument stand, dass es nicht überraschen würde, wenn in absehbarer Zukunft ein wirtschaftlicher Kollaps wegen einer Attacke auf wichtige technische Systeme großer Unternehmen zustande kommen würde[18].

In der politischen und akademischen Diskussion über Cyberterrorismus sind vorwiegend zwei Positionen vertreten. Die Staaten und IT-Sicherheitsunternehmen sind in erster Linie der Meinung, dass die Gefahr real und groß ist. Wissenschaftler, Analysten und Forschungsinstitute vertreten dagegen die Sichtweise, dass diese Gefahr nicht oder nur im begrenzten Maße existiert und dass es keine oder sehr wenige bekannte Fälle der cyberterroristischen Anschläge gibt. Sie behaupten, dass die Gefahr vor Cyberangriffen überschätzt wird und dass die Sicherheitssysteme generell gut funktionieren. Es liege im Interesse der IT-Sicherheitsunternehmen, die Unruhe über potenzielle Cyberangriffe zu steigern, weil das für sie finanziell gewinnbringend ist. Ein anderes Kontraargument ist, dass Cyberterrorismus teurer als der „traditionelle“ ist. Er sei nicht wirtschaftlich rational: Es ist billiger, einen Rucksack mit einer Bombe auf ein paar Selbstmordattentäter aufzuhängen, wobei auch das Sensationspotenzial größer ist.[19]

Argumentation

Die genannte Meinungsverschiedenheit haben Lee Jarvis, Stuart Macdonald und Lella Nouri in der Studie *Die Gefahr vor Cyberterrorismus: Resultate einer Umfrage von Forschern* (*The Cyberterrorism Threat: Findings from a Survey of Researchers*) untersucht, die in Form einer Umfrage durchgeführt wurde. An der Umfrage nahmen 118 Forscher aus 24 Ländern teil. Die Resultate zeigen, dass 35 Prozent der Befragten Cyberterrorismus für eine reale Gefahr halten, während 29 Prozent in ihm keine Bedrohung sehen. Von dem Rest der Befragten halten ihn 15 Prozent für möglich, fünf Prozent waren sich unsicher und 16 Prozent haben sich zur Frage nicht geäußert[20].

In der Studie wurden die Forscher auch gefragt, ihre Einstellung zu begründen. Diejenigen, die Cyberterrorismus als eine relativ geringe Gefahr eingeschätzt haben, begründen das damit, dass Cyberattacken im Vergleich zu traditionellen Angriffen aus mehreren Gründen für Terroristen unattraktiv sind: Ihnen fehle an Theatralizität und die traditionellen terroristischen Methoden und Waffen bleiben effektiver, wenn es darum geht, mehrere Menschen zu töten, wodurch sie auch als ein

[17] Vgl. Heickerö, S. 556
[18] Vgl. Heickerö, S. 556 ff.
[19] Vgl. Heickerö, S. 555
[20] Jarvis et al., S. 76

besseres Mittel für Erregung der politischen Aufmerksamkeit dienen. Das heiße nicht, dass man das Internet als ein Werkzeug der Terroristen unterschätzen soll: Das Netz wird für Anwerbung neuer Terroristen, Finanzierung, Netzwerken, Datenerhebung und Datenbanken genutzt, wodurch die Leistungsfähigkeit und Reichweite der Terroristengruppen erhöht wird.[21] Die drei Hauptgründe, die in der Studie von den Forschern angegeben wurden, die die Gefahr vor Cyberterrorismus nicht ernst nehmen, sind:

- Bis jetzt hat es noch keine Fälle von Cyberterrorismus gegeben - es fehlt an einem Präzedenzfall und an Maßstäben, an denen die reale Gefahr von Cyberterrorismus eingeschätzt werden kann. Es gibt nur hypothetische Szenarios und keine empirischen Beweise, die auf die Gefahr hinweisen würden.
- Terroristenorganisationen verfügen über kein Potenzial für einen Angriff auf Kritische Infrastrukturen und andere wichtige Ziele.
- Dem Cyberterrorismus fehlt der Heroismus, d.h., es werden keine Selbstmordattentate ausgeübt. Jarvis et al. formulieren es so: „Ich glaube, dass das Selbstbild [von Terroristen] ein sehr wichtiger Faktor im Radikalisierungsprozess ist. Im Unterschied zu anderen Formen des Terrorismus erfüllen die Angriffe der Cyberterroristen nicht diese Anforderung“[22] – sie nehmen sich selbst weniger als Helden wahr.[23]

Inwieweit sind diese Begründungen plausibel und was sagt die andere Seite dazu? Widmen wir uns jetzt den Argumenten von Forschern, die denken, dass die Gefahr vor Cyberterrorismus nicht unterschätzt werden darf. Der israelitische Forscher Gabriel Weimann gibt in seinem Forschungsartikel *Cyberterrorismus: Die Summe aller Ängste?* (*Cyberterrorism: The Sum of All Fears?*) fünf Gründe an, die den oben genannten komplett widersprechen:

- Cyberterrorismus ist billiger als die traditionellen terroristischen Methoden. Alles, was ein Terrorist braucht, ist ein PC und ein Internetanschluss. Er muss kein Geld für Waffen wie Gewehre und Explosivstoffe ausgeben - er kann Computerviren schreiben und sie durch Telefonverbindung, Kabel oder WLAN verbreiten.
- Cyberterrorismus bietet im Unterschied zu traditionellen terroristischen Methoden Anonymität. Wie viele andere Internetnutzer können auch Terroristen Spitzwörter (*screen names*) benutzen oder sich als Gast auf Internetseiten einloggen. Dadurch erschweren sie es der Polizei und den Sicherheitsbehörden, ihre wahre Identität herauszufinden. Außerdem gibt es im Cyberspace keine physischen Barrieren wie Kontrollstellen, Grenzübergänge oder Zölle.

[21] Vgl. Jarvis et al., S. 71
[22] Jarvis et al., S. 76
[23] Vgl. Jarvis et al., S.76

- Die Vielfalt und die Auswahl der Ziele sind enorm. Cyberterroristen könnten Computer und Computernetzwerke der Regierungen, Individuen, öffentlichen Versorgungseinrichtungen, privaten Fluggesellschaften u.Ä. angreifen. Bloß die Anzahl und Komplexität der potenziellen Ziele garantiert, dass die Terroristen Lücken und Schwachstellen finden und sie ausnutzen können. Mehrere Studien haben gezeigt, dass Kritische Infrastrukturen wie Energieversorgungsnetze oder Notdienste gefährdet sind, weil ihre Infrastruktur zu komplex ist, als dass alle Schwachstellen eliminiert werden können.
- Cyberterrorismus kann durch Fernsteuerung durchgeführt werden – eine Charakteristik, die eine besondere Anziehungskraft für Terroristen haben sollte. Die Vorteile sind weniger Investitionen in körperliche und mentale Ausdauer, geringeres Todesrisiko und weniger Reiseaufwand als konventionelle Terrorismusformen. Das alles erleichtert den Terroristen, neue Anhänger zu rekrutieren und alte beizubehalten.
- Cyberterrorismus hat ein größeres Potenzial als die traditionellen terroristischen Methoden größeren Mengen von Menschen Schaden zuzufügen. Dadurch wird auch ein größeres Aufsehen in den Medien erreicht, was das ultimative Ziel der Terroristen ist.[24]

Auf Basis der genannten Argumente definiert Weimann den Cyberterrorismus als das Verwenden von Werkzeugen der Computernetzwerke, um Kritische Infrastrukturen (wie Energie oder Transport) zu beschädigen oder sie außer Betrieb zu setzen. Die wichtigste Voraussetzung dafür ist schon in Kraft: das Funktionieren von nationalen und Kritischen Infrastrukturen ist abhängig von Computernetzwerken und deren Infrastruktur schon so komplex, dass ständig neue Schwachstellen entstehen. Diese Vernetzung ist „eine große elektronische Achillesferse“[25]. Das macht Cyberterrorismus zu einer attraktiven Alternative für moderne Terroristen, die sein Potenzial für Zufügung massiver Schäden, die durch ihn ermöglichte Anonymität, seine psychologischen Wirkungen und seine Attraktivität für die Medien zu schätzen wissen.[26]

Fazit

Trotz aller genannten Vorteile und trotz der Möglichkeit, Millionen Menschenleben zu bedrohen, haben die Forscher, die den Cyberterrorismus nicht fürchten, in einem Recht: Es gibt nicht genügend Beweise, dass wir einen bekannten Vorfall mit Sicherheit als terroristischen Cyberanschlag bezeichnen können. Das heißt aber nicht, dass Terroristenorganisationen die Vorteile des Cyberterrorismus nicht ausnutzen werden. Dafür haben sie einfach ein zu großes Potenzial. Die wachsende Abhängigkeit unserer Gesellschaft von der Informationstechnologie kreiert neues Schadenpotenzial und eröffnet den Terroristen Zugang zu Zielen, die ihnen ansonsten unerreichbar wären (Verteidigungssysteme von

[24] Vgl. Weimann, S. 137
[25] Lewis zitiert in Weimann, S. 130
[26] Vgl. Weimann, S. 130

Regierungen oder Verkehrskontrollsysteme). Je entwickelter die Technologie eines Landes oder Unternehmens ist, desto ausgesetzter sind ihre Infrastrukturen den Cyberangriffen. Die Terroristen können, zumindest in Theorie, in staatliche und private Computersysteme eindringen und den Militär-, Finanz- und Dienstleistungssektor lahmlegen[27].

Um die Gefahr vor Cyberterrorismus einschätzen zu können, sollen nach Dennings zwei Fragen gestellt werden:

- Gibt es Ziele, die Cyberangriffen ausgesetzt sind?
- Gibt es Täter, die in der Lage sind und genug Motivation haben, solche Angriffe auszuüben?

Die Antwort auf die erste Frage ist positiv: Kritische Infrastrukturen sind komplex und haben deshalb auch Schwachstellen, die ausgenutzt werden können. Sogar Systeme, die von äußerer Manipulation als abgesichert wirken, sind Insidern, die alleine oder mit Terroristen handeln, erreichbar[28]. Was ist aber mit der zweiten Frage? Obwohl es bis jetzt keine konkreten terroristischen Cyberangriffe gab, könnten in der Zukunft Terroristen mehr das Potenzial des Cyberterrorismus nutzen. Die neuen Generationen von Terroristen wachsen in einer digitalen Welt auf, in der Hackerwerkzeuge ständig mächtiger, einfacher und zugänglicher werden. Cyberterrorismus wird insbesondere attraktiver werden, weil sich die virtuelle und reale Welt immer mehr verzweigen. Eine Terroristengruppe könnte so, z.B., gleichzeitig eine Bombe auf einem Bahnhof explodieren lassen und einen Cyberangriff auf die Kommunikationsinfrastruktur starten, um so die Folgen des Angriffes zu stärken. Wenn diese Systeme nicht ausreichend gesichert werden, könnte in der nahen Zukunft eine online Aktion mit physischem Schaden genauso leicht auszuführen sein, wie heute eine Webseite zu hacken. Das Paradox ist, dass der Krieg gegen den traditionellen Terror, die Terroristen zu unkonventionellen Mitteln wie Cyberterrorismus wenden könnte. Die richtige Herausforderung ist, einzuschätzen, wie mit dieser Ambiguität umzugehen ist, ohne gleichzeitig die reale Bedeutung des Cyberterrorismus aufzublasen und dadurch die Manipulation durch Angst zu erleichtern[29].

[27] Vgl. Weimann, S. 144
[28] Vgl. Weimann, S. 144
[29] Vgl. Weimann, S. 146

Literaturverzeichnis

- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2014): Die Lage der IT-Sicherheit in Deutschland 2014. PDF.
- Heickerö, Roland (2014): *Cyber Terrorism: Electronic Jihad.* In: Strategic Analysis. Band 38, Nr. 4, S. 554–565
- Jarvis, Lee / Macdonald, Stuart / Nouri, Lella (2014): *The Cyberterrorism Threat: Findings from a Survey of Researchers*. In: Studies in Conflict & Terrorism. Band 37, Nr. 1, S. 68 – 90
- Nguyen, The-Khoa: *In-Flight-WLAN stellt ernsthaftes Sicherheitsrisiko dar*. In: PC Magazin. Stand: 16.04.2015. URL: http://www.pc-magazin.de/news/wlan-flugzeug-internet-in-flight-an-bord-sicherheit-risiko-gao-faa-bericht-3013934.html (letzter Abruf am 24.07.2015)
- o. V.: *Flugzeuge über Inflight-Wi-Fi kapern und fremdsteuern*. In: www.heise.de. Stand: 16.04.2015. URL: http://www.heise.de/security/meldung/Flugzeuge-ueber-Inflight-Wi-Fi-kapern-und-fremdsteuern-2609663.html (letzter Abruf am 24.07.2015)
- Schumacher, Stefan (2014): *Cyber Terrorismus – Reale Bedrohung oder Mythos?* In: Jahrbuch Terrorismus. Band 6. 2013/14/ Hrsg. vom Institut für Sicherheitspolitik an der Universität Kiel, S. 159-180
- Stadlmeier, Sigmar/ Unger, Walter J. (2012): *Cyber-War und Cyber-Terrorismus aus völkerrechtlicher Sicht*. In: Aktuelle Herausforderungen des Völkerrechts: Beiträge zum 36. Österreichischen Völkerrechtstag 2011. Frankfurt am Main [u.a.], S. 63 – 80
- Weimann, Gabriel (2005): Cyberterrorism: The Sum of All Fears? In: Studies in Conflict & Terrorism. Band 28, Nr. 2, S. 129-149