

Denkbar, aber noch nicht Realität



Der Begriff Cyberterrorismus meint, dass Terroristen für ihre Ziele Computersysteme nutzen. Dabei ist ganz besonders zwischen zwei Anwendungen zu unterscheiden. Erstens Terroristen, welche die Computertechnologie als Logistik- und Agitationsmittel für ihre Ziele nutzen. Und zweitens Akteure, die mit einem Computer einen virtuellen terroristischen Angriff auf beispielsweise Kernkraftwerke, Stromversorgungen oder ähnliche Strukturen durchführen.

Die meisten heutigen illegalen Anwendungen gehören in den Bereich der Cyberkriminalität. Bild: shutterstock

VON HANS-ULRICH HELFER

Obschon eine gewaltige Zunahme von Computerangriffen in privaten, wirtschaftlichen und staatlichen Bereichen zu verzeichnen ist, sind heute insgesamt nur wenige Prozente den Terroristen zuzurechnen. Die meisten illegalen Anwendungen gehören in den Be-



Hans-Ulrich Helfer

ist Geschäftsführer der Presdok AG Zürich; im Besonderen Berater von staatlichen Institutionen, Firmen, Anwaltskanzleien

sowie namhaften Persönlichkeiten. Am Jubiläumsanlass der Vereinigung Kriminaldienst Österreich von Ende November 2010 hielt er ein Referat zum Thema «Terrorismus: Lage und Trends». Kontakt: www.presdok.ch

reich Cyberkriminalität und nicht Cyberterrorismus. Aber auch die Anzahl der politisch motivierten Angriffe durch Hacker und Cracker ist gestiegen. Diese Aktionen als Cyberterrorismus zu bezeichnen, zielt eindeutig am Problem vorbei und verschleiern sogar die tatsächliche Bedrohung. Cyberterrorismus als Logistik- und Agitationsmittel umfasst beispielsweise folgende Erscheinungsformen:

Interne Kommunikation: Seien es die klassischen nationalen Terrororganisationen oder weltumspannende wie die al-Qaida, alle nutzen heute das Internet für ihre Kommunikation. Benutzt wird nicht nur die bekannte E-Mail, sondern auch Websites, Twitter, Blogger und SMS. Die Vielzahl der Möglichkeiten und Systeme sowie Sprachen verunmöglicht eine stetige Kontrolle durch die Behörden.

Propaganda: Mittels E-Mail-Massenversand und Websites in fast allen Sprachen propagieren die nationalen wie internationalen Terroristenorganisationen ihre Ziele. Sie stellen auf Download-Servern Material kostenlos zur Verfügung.

Rekrutierung: Die Rekrutierung über das Internet erfolgt indirekt, da die Terrororganisationen Einschleusungen von Beamten befürchten. Potenzielle Bewerber werden vorerst über Chatrooms angesprochen. Dabei wird alleine schon durch die Sprache eine wichtige Selektion vorgenommen. Ein Blick in die wichtigen Chats zeigt die unzähligen kaum kontrollierbaren Möglichkeiten.

Online-Ausbildung: Die ideologische und theoretische Grundausbildung geschieht grösstenteils nicht mehr in Trainingslagern irgendwo im Hinterland un-

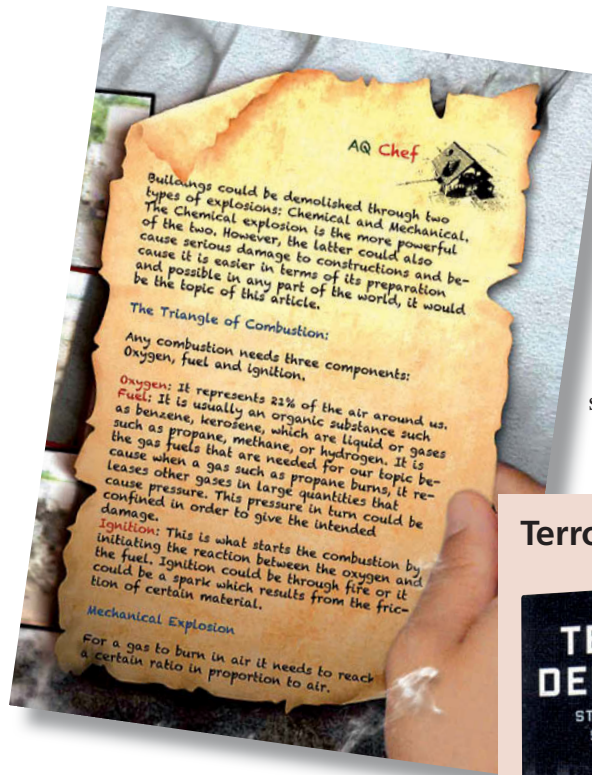
ter der Satellitenbeobachtung westlicher Staaten, sondern über das Netzwerk des so gehassten Feindes. Unter dem Slogan «Open Source Jihad» kursieren unzählige Anweisungen und Handbücher in etlichen Sprachen im Internet. Die Terroristen nutzen für die Online-Ausbildung modernste Technologie aller Art.

Geldbeschaffung: Online-Geldsammlaktionen für undurchsichtige Wohltätigkeitsorganisationen jeder Art gibt es unzählige. Seit den Kontensperrungen der Behörden sind die Terroristen vorsichtiger geworden und benutzen für ihre Belange auch bekannte Hilfswerke. Die Beschaffung geschieht auch über den Verkauf von Propagandamaterial wie Filmen, Musik und Flyern.

Psychologischer Krieg: Mit dem Internet haben terroristische Organisationen erstmals die Möglichkeit gefunden, mit den grossen staatlichen oder privaten Massenmedien gleichzuziehen. Sie agieren schnell und gekonnt und schocken nicht selten den Bürger und die verantwortlichen Beamten mit Folter und Enthauptungen auf Videos, die sie übers Internet verbreiten.

Politische Agitation: Nach dem Masterplan der zweiten Al-Qaida-Generation befinden wir uns gegenwärtig in der vierten Phase, welche dem Untergang der verhassten arabischen Regime dient, was der momentane Brandherd Nordafrika/Arabien deutlich zeigt. In dieser Phase, die bis etwa 2013 dauert, sollen auch Öllieferanten sowie die westliche Wirtschaft durch Cyberterrorismus angegriffen werden. In seinem soeben erschienenen Buch «Terrorziel Deutschland» beschreibt der Autor Berndt Georg Thamm, wie al-Qaida

er lediglich über seinen Laptop ein Verkehrsflugzeug in ein Hochhaus oder Kernkraftwerk rasen oder eine Stadt in den Fluten eines Staudamms versinken lassen. In dem Sinne ist der in den Massenmedien dargestellte Cyberterrorismus noch Panikmache, niemand weiss, wann er Tatsache in der Gegenwart sein wird. Vielleicht schon heute!



Ausbildungsanleitung aus dem Internet zur Zerstörung eines Gebäudes.

zu «@Qaida» wurde und welches Gefahrenpotenzial dahintersteckt.

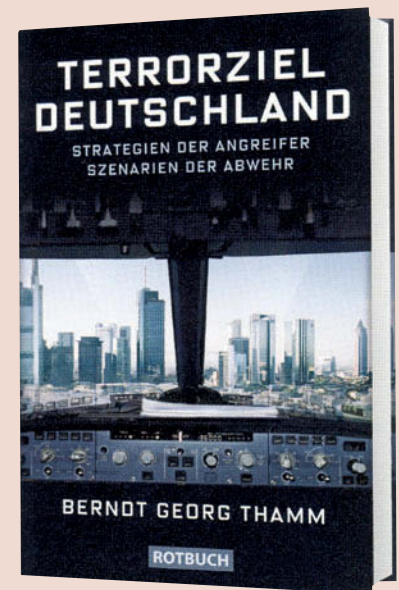
Wann kommt der «echte» Cyberterrorismus?

Terroristen suchen immer nach neuen Anschlagsmöglichkeiten und effizienteren Waffen. Wenn es Terroristen also möglich ist, den Computer als eigentliche Waffe einzusetzen, so werden sie dies auch tun. Aus diesen Überlegungen ergeben sich tatsächlich Schreckensszenarien, denn die westlichen Gesellschaften nutzen in einem äusserst starken Ausmass die Systeme, die mit einem Laptop online angreifbar sind.

Dies führt dazu, dass immer wieder angeblich stattgefundene oder geheim gehaltene Angriffe von Cyberterrorismus kolportiert werden. Reine cyberterroristische Angriffe auf nationale Logistiknetzwerke wie Kernkraftwerke, Flugleitsysteme, Bankzentren, Wasserwerke, Satellitenkommunikation, Raketenbasen, Städte-Notfallsysteme und Militärstützpunkte sind gegenwärtig noch Fantasien und Visionen der Massenmedien. Bis heute ist kein einziger Fall von «echtem» Cyberterrorismus bekannt oder öffentlich belegt. Ebenso sind wir erst am Beginn des so von vielen Armeen gefürchteten Cyber-War.

Allerdings ist zu beachten, dass alles, was denkbar ist, auch eines Tages ausgeführt wird. Osama bin Laden würde wohl keine Sekunde zaudern, könnte

Terrorziel Deutschland



Berndt Georg Thamm, geboren 1946, beschäftigt sich seit Jahrzehnten mit den Themen Terrorismus und Organisierte Kriminalität. Von 1985 bis 1995 war er in der Politikberatung mit Schwerpunkt Innere Sicherheit/Drogen tätig, seit 1979 arbeitet er ausserdem als Referent für die Polizei.

Die Anschläge des 11. September 2001 jähren sich zum zehnten Mal. In seinem neuesten Buch analysiert Thamm die Strukturen von al-Qaida anhand ihrer bisherigen terroristischen Aktivitäten und dokumentiert die neue Vielfältigkeit der Angriffsstrategien des Djihad-Terrorismus. Er schildert den Fall der «Sauerland-Gruppe» von 2007 und die damals gerade noch verhinderte Katastrophe, nennt gleichzeitig die gegenwärtige Gefährdung durch die stets steigende Anzahl konvertierter deutscher Märtyrer. Thamm zeigt, wie al-Qaida zu «@Qaida» wurde und welches Gefahrenpotenzial dahintersteckt. Fundiert gibt er einen Vorgeschmack auf das, was uns in den kommenden Jahren erwarten könnte.

Berndt Georg Thamm, *Terrorziel Deutschland, Strategien der Angreifer Szenarien der Abwehr*, 280 Seiten, ISBN 978-3-86789-130-1



Inspire ist das Magazin der Terrororganisation al-Qaida. In der Ausgabe vom November 2010 geben die Verfasser die Online-Kommunikation bekannt.