Humanistische Union

Der Bundestrojaner - ein notwendiges Übel?

I. Einleitung

Nachdem Bundespräsident Horst Köhler über die Weihnachtsfeiertage das über Monate hinweg umstrittene BKA-Gesetz unterschrieb, stehen dem Bundeskriminalamt mit 1. Januar 2009 neben weit reichenden Erweiterungen seiner Kompetenzen im Kampf gegen den Terrorismus auch eine in der breiten Öffentlichkeit als "Bundestrojaner" bekannte Maßnahme zum "verdeckten Eingriff in informationstechnische Systeme" zur Verfügung. Sollte dieses Gesetz auch vor dem Bundesverfassungsgericht in Karlsruhe bestehen, würde damit dem BKA ein Instrument zur Verfügung gestellt, das ihm erlaubt, direkten Zugriff auf Computer von Verdächtigen zu erlangen, um damit terroristische Aktivitäten beobachten und potentielle Anschläge bereits im Vorfeld verhindern zu können.

Es stellt sich aber die Frage, wie effektiv eine solche Maßnahme zur Terrorismusbekämpfung überhaupt sein kann? Ist der Zugriff auf Computer durch Sicherheitsbehörden wirklich unerlässlich, um gegen den transnationalen Terrorismus vorzugehen oder gefährdet diese Maßnahme vielmehr Bürger- und Freiheitsrechte in nicht begründbarer Weise? Um diese Fragen zu beantworten wird zunächst geklärt, wie und zu welchem Zweck Terroristen das Internet nutzen. Aufbauend darauf soll erläutert werden, wie der "Bundestrojaner" funktioniert und wie dieser die terroristische Nutzung des Internets beeinflussen kann. In einem dritten Schritt wird dargelegt, wie potentielle Terroristen auf die Einführung dieses Untersuchungsmittels mit hoher Wahrscheinlichkeit reagieren werden und abgeleitet davon wird analysiert, wie effektiv der verdeckte Eingriff in informationstechnische Systeme überhaupt sein kann.

Dieser Beitrag kommt zu dem Ergebnis, dass der "Bundestrojaner" ein unerlässliches Mittel zur Bekämpfung terroristischer Bedrohungen ist. Dieser Befund wird jedoch eingeschränkt durch die Erkenntnis, dass diese Überwachungsmethode aller Voraussicht nach nur in seltenen Fällen wirklich zum Einsatz kommen kann und dass eine große Zahl potentieller Terroristen Mittel und Wege finden wird, um sich der digitalen Überwachung zu entziehen. Es muss daher Ziel des Gesetzgebers sein, den Schutz vor missbräuchlicher Verwendung dieses Instruments so hoch wie möglich anzusetzen.

II. Terrorismus und Internet

Über die Nutzung des Internets durch Terroristen wurde bereits viel geschrieben[1]. Es lässt sich festhalten, dass al-Qaida und ähnliche Gruppierungen das Internet "lieben".[2] Um diese Nutzung zu kategorisieren kann zwischen fünf konkreten Anwendungsbereichen unterschieden werden: (1) Cyber-Terrorismus, (2) Propaganda, (3) Ressourcenallokation, (4) Informationsgewinnung und (5) Aufbau von Führungs-, Kommunikations- und Kontrollstrukturen.

Die Angst, das Internet könnte für Cyber-Terrorismus missbraucht werden, stellt eine immer wiederkehrende Sorge dar. Ähnlich wie "gewöhnliche" Hacker oder staatliche Einrichtungen, die sich auf den "Krieg im Cyberspace" konzentrieren, könnten Terroristen versuchen, über das Internet Daten zu stehlen, diese zu manipulieren oder durch gezielte Attacken auf ausgesuchte Seiten des Wirtschaftslebens, der Medien oder Politik das immer mehr vom World Wide Web geprägte Leben massiv zu stören. Solche Szenarien können nicht ausgeschlossen werden, es gibt jedoch bis heute keine ernsthaften Anzeichen dafür, dass potentielle Terroristen diese Art der Nutzung des Internets bevorzugen. Darüber hinaus scheinen die

Sicherheitsvorkehrungen gegen Cyber-Terrorismus besser zu sein als vielerorts befürchtet.[3]

Weitaus wichtiger scheint der Einsatz des Internets für Propagandazwecke zu sein. Wie Yariv Tsfati und Gabriel Weimann zeigen, versuchen Terroristen über Internetseiten vor allem Unterstützer und Sympathisanten zu erreichen und nutzen solche Webseiten daher primär für Propagandazwecke.[4] Michael Whine geht sogar soweit zu behaupten, dass der Propagandazweck des Internets jenen für Kommunikation und Führungsaufgaben übertrifft.[5] Es kann jedoch festgehalten werden, dass Terroristen durch das Internet nicht mehr nur auf traditionelle Medien wie Zeitungen und dem Fernsehen angewiesen sind. Während der internationale Terrorismus in den 1960er, 1970er und 1980er Jahren darauf angewiesen war, dass dessen Aktionen im Fernsehen übertragen und Botschaften durch Zeitungen Weiterverbreitung fanden, können die Terroristen von heute durch die Entwicklungen des Internets (Stichwort Web 2.0) ihre eigenen Inhalte relativ einfach und schnell selber erstellen und sie über diverse Homepages oder Videoportale nahezu der gesamten Welt zur Verfügung stellen. Das Internet wird damit zu einem Propagandainstrument, mit dem Unterstützer mobilisiert und rekrutiert werden können und das zur Radikalisierung einer bereits extremistischen Sympathisantenschaft beitragen kann.

Eng damit verbunden ist das Einwerben von finanziellen Mitteln, um terroristische Aktivitäten und Netzwerke zu finanzieren. Vergleichbar mit Präsidentschaftskandidaten in den USA, versuchen Terroristen durch Spendenaufrufe im Internet Mittel zu lukrieren, sei dies nun direkt an das eigene Netzwerk oder über den Umweg von Wohltätigkeitsorganisationen, die sowohl wissentlich als auch in manchen Fällen unwissentlich dieses Geld diskret an die betreffenden Stellen weiterleiten. Darüber hinaus scheint die kriminelle Nutzung des Internets, durch Kreditkarten-, Onlinebanking oder Online-Auktionsbetrug (zum Beispiel dem Verkauf hochpreisiger Produkte via Ebay, ohne diese dann auch wirklich zu versenden) immer wichtiger zu werden. Daneben bieten Online-Banksysteme oder Online-Finanzservices wie PayPal die Möglichkeit, Gelder diskret und ohne viel Spuren zu verschieben.[6]

Das Internet gibt Terroristen aber nicht nur die Möglichkeit zur vereinfachten Ressourcenallokation. Suchmaschinen wie Google oder Yahoo, Satellitenbilder über Google Earth oder Microsoft Virtual Earth, Webseiten von Regierungseinrichtungen und Polizeistellen dienen heutzutage nicht mehr nur dazu, um Bilder des Hotels für den nächsten Tunesienurlaub zu finden. Solche Hilfsmittel werden von Terroristen vor allem dazu verwendet, um Informationen zu sammeln und Anschläge oft aus weiter Entfernung zu planen. Das Internet gibt diesen Akteuren somit eine Art nachrichtendienstliches Aufklärungsinstrument, das in früheren Zeiten nur Staaten vorbehalten war, in die Hand. Das Ausmaß an Informationen, die frei über das Internet für solche Zwecke gewonnen werden können, kann laut Aussagen des früheren US Verteidigungsministers Rumsfeld ungefähr 80 Prozent der vorhandenen Informationen umfassen.[7] Die Rolle, die das Internet in diesem Bereich spielt, kann daher nicht hoch genug eingeschätzt werden.

Schließlich und endlich erleichtert das Internet die Kommunikation zwischen den und die Führung von Zellen und Akteuren eines oder unterschiedlicher Netzwerke. Dieser Umstand ist besonders seit der Zerschlagung der ursprünglichen Strukturen al-Qaidas nach dem 11. September 2001 wichtig, galt es seitdem, die oft nur lose verbundene Zellen und Sympathisanten miteinander zu verknüpfen. Das Internet nimmt hier einen nicht mehr wegzudenkenden Stellenwert ein. Es hilft diese unterschiedlichen Akteure miteinander zu verbinden, bietet ihnen eine Plattform, um Informationen untereinander auszutauschen (zum Beispiel durch das Bereitstellen von Handbüchern wie der "Enzyklopädie des Jihad") und erleichtert Kommunikations-, Koordinations- und Planungsaktivitäten. Besonders wichtig ist in diesem Zusammenhang die Möglichkeit, Kommunikation mittels Verfahren wie dem Verstecken von Nachrichten in Bildern, der Verschlüsselung von Emails (zum Beispiel mittels PGP[8]) oder dem Telefonieren via Internet (zum Beispiel durch eine AES-256 Verschlüsselung via Skype) vor der staatlichen Kontrolle geheim zu halten und

damit den Erfolg geplanter Operationen zu sichern.

III. Der Bundestrojaner und seine Wirkungsweise

Es stellt sich also die Frage, wie gegen die soeben beschriebene terroristische Nutzung des Internets effektiv vorgegangen werden kann? Das neue BKA-Gesetz versucht diese Frage zu beantworten, indem es den Zugriff der Behörde auf Computer von potentiellen Terroristen ermöglicht. Eine solche Neuregulierung wurde notwendig, nachdem der Bundesverfassungsgerichtshof im Februar 2008 das Vorgehen des nordrhein-westfälischen Verfassungsschutzes bei der Online-Durchsuchung von Computern als verfassungswidrig bezeichnete. Obwohl Karlsruhe das Mittel der Online-Durchsuchung nicht prinzipiell ausschloss, wurde das nordrhein-westfälische Vorgehen als eine Verletzung des durch das Grundgesetz gesicherten Persönlichkeitsrechts angesehen, da weder Vertraulichkeit noch Integrität informationstechnischer Systeme geschützt seien.[9]

Der vom Innenministerium im Juni 2008 vorgelegte Entwurf über die Adaptierung des BKA-Gesetzes glaubte diesem Urteil Rechnung zu tragen und versuchte mit §20k des neuen BKA-Gesetzes die Erkenntnis des Bundesverfassungsgerichts umzusetzen und damit die Verwendung von Online-Durchsuchungen zur Terrorismusbekämpfung auf ein gesetzlich sicheres Fundament zu stellen. Obwohl das Gesetz zunächst im Bundestag eine breite Mehrheit von CDU/CSU und SPD erhielt, scheiterte es im ersten Anlauf am Widerstand des Bundesrates, da neben den Bundesländern, in denen FDP, Grüne und die Linke mitregieren auch die SPD-mitregierten Bundesländer dem Gesetz ihre Zustimmung versagten. Erst nach Einberufung des Vermittlungsausschusses und substantiellen Nachbesserungen in wichtigen Passagen zum Schutz der Bürger- und Freiheitsrechte, erhielt das Gesetz eine knappe Mehrheit von 35 zu 34 Stimmen.

Kernstück des Gesetzes ist der Paragraph 20k mit der Bezeichnung "Verdeckte Eingriffe in informationstechnische Systeme": Online-Durchsuchung ist nur dann gestattet, wenn es einen konkreten Hinweis darauf gibt, dass die Freiheit oder das Leben von Menschen oder die Grundlagen des Staatswesen gefährdet sind. Die Maßnahme dient somit ausschließlich der Abwehr schwerwiegender Gefahren und nicht zur Strafverfolgung per se. Angewandt kann diese Maßnahme nur werden, nachdem der Präsident des BKA oder sein Stellvertreter dies bei einem unabhängigen Gericht beantragt hat. Während im zunächst vom Bundesrat abgelehnten Gesetz noch die Möglichkeit vorhanden war, dass in seltenen Ausnahmefällen, wenn unmittelbar Gefahr droht, die Zustimmung durch ein Gericht auch im Nachhinein (spätestens drei Tage nach Anwendung) erlaubt werden soll, ist im beschlossenen Gesetz die Genehmigung ausschließlich an eine zuvor eingeholte richterlicher Erlaubnis gebunden. Eine Änderung im Vermittlungsausschuss ergab sich auch bezüglich der Überprüfung des verfassungsrechtlich gebotenen Schutzes des Kernbereichs privater Lebensgestaltung. Während diese ursprünglich von zwei weisungsgebundenen Beamten des BKA hätte erfolgen sollen, wurde dies mittlerweile auch einem Richter übertragen. Im Kommentar zur Gesetzesvorlage werden zudem die technischen Besonderheiten der Maßnahme detaillierter erläutert. Ziel des "Bundestrojaner" ist es, mittels spezieller Überwachungsprogramme, die auf den fremden Rechnern zuvor installiert werden müssen, Zugriff auf die Festplatten von Computern potentieller Terroristen zu erhalten und mit Hilfe von so genannten "key-loggers" Tastatureingaben auszulesen. Explizit verboten ist dabei aber der Zugriff auf Webcams und Mikrophone, die an den Computer angeschlossen sind. Kurz zusammengefasst, dient dieses Programm also dazu, die auf der Festplatte Fremder gespeicherten Inhalte den Sicherheitsbehörden zugänglich zu machen und Eingaben in die Tastatur am Computer auszulesen, ohne dass diese vorher verschlüsselt werden können.

Der "Bundestrojaner" versucht daher vor allem zwei Kategorien der terroristischen Nutzung des Internets zu bekämpfen - nämlich die Sammlung von Informationen und den Aufbau von Kontroll-, Führungs- und Kommunikationsstrukturen zur Anschlagsplanung. Er kann aber auch eingesetzt werden, um sowohl Cyber-

Terrorismus als auch Propaganda und finanzielle Ressourcenallokation zu observieren und zu bekämpfen.

IV. Rationalität der Terroristen und Effektivität des "Trojaners"

Um die Effektivität des "Bundestrojaners" bewerten zu können, muss zunächst geklärt werden, wie Terroristen allgemein auf Gegenmaßnahmen reagieren. Den in weiterer Folge beschriebenen Ansatz zur Erklärung terroristischen Verhaltens bezeichne ich als die "Notwendigkeit des Erfolges".

Dieser Ansatz geht zunächst von der Annahme aus, dass es sich bei Terroristen nicht um Verrückte handelt, deren Verhalten auf erratische oder psychische Faktoren zurückgeführt werden kann. Eine Vielzahl von AutorInnen hat sich mit diesem Thema beschäftigt und es kann mittlerweile als gesichert angesehen werden, dass Terroristen rationalen Entscheidungsprozessen folgen und dass Terrorismus willentlich zur Erreichung politischer oder strategischer Ziele angewandt wird. Terrorismus ist sozusagen das Ergebnis einer kaltblütigen Abwägung von Kosten und Nutzen - solange die Durchführung eines Attentats die Mittel wert sind und die Wahrscheinlichkeit eines Erfolges gegeben ist, besteht eine hohe Wahrscheinlichkeit, dass es auch durchgeführt wird.[10] Sogar im Falle der extremsten Form terroristischer Anschläge - dem Selbstmordattentat - kann die Entscheidung auf den Rückgriff terroristischer Vorgehensweise durch strategische Logik und nicht durch psychische Faktoren erklärt werden - Terrorismus wird angewandt, weil er sich aus Sicht der Terroristen bezahlt macht.[11] Diese Sichtweise wird unter anderem durch Studien von Marc Sageman, einem Terrorismusexperten und Psychiater, belegt, der nach dem Studium der Biographien von über 130 Terroristen zum Ergebnis kommt, dass diese durch ihre "Normalität" bezüglich ihrer mentalen Gesundheit (im Vergleich zum Bevölkerungsdurchschnitt) gekennzeichnet sind.[12]

Andrew H. Kydd und Barbara F. Walter haben darüber hinaus gezeigt, wie diese Form der kalkulierten Gewalt dazu verwendet wird, um Strategien zu entwickeln und Ziele zu erreichen.[13] Auch wenn Max Abrahams bestreitet, dass Terrorismus das Ergebnis einer strategischen Überlegung sei, um politische Ziele zu erreichen, sondern Terroristen als "social solidarity seekers" bezeichnet, unterstreicht er die Annahme, dass diese Akteure rational handeln und von einer Kosten-Nutzen-Abwägung geleitet werden.[14] Dieser rationalistische Ansatz wird zudem noch durch Studien wie jener von Lisa M. Cartan verfestigt, die zeigt, dass Terroristen Anschlagziele meiden, die zu gut bewacht sind und deren Erfolg daher in Frage gestellt wird.[15]

Darüber hinaus können es sich Terroristen nicht erlauben, über einen längeren Zeitraum hinweg keine Attentate durchzuführen, wollen sie nicht in Vergessenheit geraten. Terroristen sind daher gezwungen, ein Minimum an Präsenz zu zeigen, um effektiv bleiben zu können.16 Dies erfolgt jedoch immer nur unter Berücksichtigung des zuvor erwähnten Arguments, dass Anschläge nicht um jeden Preis durchgeführt werden, sondern Terrorismus von einer Kosten-Nutzen-Abwägung geleitet wird.

Wenn Terroristen sich also bestimmten Gegenmaßnahmen durch Staaten gegenübersehen und diese Gegenmaßnahmen analysieren, haben sie prinzipiell zwei Möglichkeiten, darauf zu reagieren - entweder mit dem Terrorismus aufzuhören oder Mittel und Wege zu finden, um diese Gegenmaßnahmen zu umgehen. Der erste Weg ist aus Sicht der Terroristen nicht wirklich realistisch, solange sie Terroristen bleiben wollen. Daher muss es ihnen gelingen, trotz der Gegenmaßnahmen erfolgreich zu sein. Terroristen sind folglich dazu gezwungen, neue Anschlagsmethoden zu entwickeln, neue Waffen zu finden, ihre Ziele von stärker bewachten Zielen auf weniger stark geschützte Ziele umzulenken oder neue Kommunikationsmittel und -kanäle zu finden, um Anschläge in aller Ruhe vorbereiten und durchführen zu können.[17] Solche Innovationen, die auch als "Substitutionseffekt" bezeichnet werden, sind notwendig, weil der höhere Preis eines bestimmten Anschlages durch die Konzentration auf ein neues, weniger stark geschütztes Ziel umgeleitet wird, um die Kosten geringer zu halten.[18] Dieser Befund wird durch Studien wie jene von Brynjar Lia und Thomas Hegghammer bestärkt, die argumentieren, dass es so etwas wie strategische Studien

bei Terroristen gibt. Ihnen zur Folge werden unterschiedliche wissenschaftliche Analysemethoden unter Jihadisten benutzt, um politische Konstellationen zu analysieren, Schwachpunkte der Gegenmaßnahmen aufzudecken und dadurch die Effektivität von Operationen zu steigern.[19]

Es muss daher davon ausgegangen werden, dass Terroristen staatliche Gegenmaßnahmen als solche identifizieren und über kurz oder lang Mittel und Wege finden werden, diese zu umgehen. Dies bedeutet nicht, dass Staaten im Kampf gegen den transnationalen Terrorismus chancenlos sind, weil es Terroristen immer gelingen wird Gegenmaßnahmen zu antizipieren und zu analysieren und entsprechend dagegen vorzugehen. Es wird immer wieder Fälle geben, wo dies nicht der Fall ist. Trotzdem müssen Staaten über die Auswirkungen ihres Handelns genauer Bescheid wissen und etwaige Konsequenzen mit bedenken.

V. Auswirkungen des "Bundestrojaners"

Welche Konsequenzen hat nun die Einführung des "Bundestrojaners"? Es lässt sich zunächst zeigen, dass Terroristen, ohne die Anwendung solcher Maßnahmen, einen großen Vorteil bei der Planung von Anschlägen und bei der Kommunikation untereinander haben. Solange sie es vermeiden in Räumlichkeiten, die von Sicherheitsbehörden durch das Verwanzen unter Beobachtung stehen, über Anschlagspläne zu sprechen und solche zu organisieren und wenn sie darüber hinaus auch noch Verschlüsselungstechniken benutzen, um ihren Internetverkehr unlesbar zu machen, haben staatliche Institutionen kaum Möglichkeiten, solche Aktivitäten umfangreich aufzudecken und dadurch mögliche Anschläge zu verhindern. Aus dieser Sicht ist der Einsatz des "Bundestrojaners" unabdingbar. Es darf Terroristen nicht ermöglicht werden, dass durch neue technische Entwicklungen wie dem Internet plötzlich Optionen offen stehen, die im Ernstfall der staatlichen Kontrolle entzogen sind.

Der verdeckte Eingriff in informationstechnische Systeme erschwert daher nachvollziehbar die Nutzung des Internets für terroristische Zwecke, da die Wahrscheinlichkeit, bei dieser Nutzung observiert zu werden, steigt. Damit Terroristen durch diesen Eingriff ungestört weiterplanen und agieren können - und von diesem Wunsch muss ausgegangen werden - müssen sie Mittel und Wege finden, um der Kontrolle durch die Sicherheitsbehörden zu entkommen. Die Anwendung von Verschlüsselungsprogrammen scheint hier ein viel versprechender Weg zu sein, da vor allem mit steigender Verschlüsselungsrate die Dechiffrierung nahezu unmöglich gemacht wird. Der Einsatz der zuvor erwähnten "key-logger" durch den "Bundestrojaner", die Kommunikation bereits vor der Verschlüsselung direkt nach Eingabe an der Tastatur abfangen, soll genau diesem Problem begegnen. Das explizite Verbot, mit dem Webcams und Mikrophone von der Überwachung ausgeschlossen werden, verwundert aber. Hier glaubt man aller Voraussicht nach, durch bereits bestehende Methoden wie das Verwanzen der betreffenden Räumlichkeiten zum gleichen Ergebnis zu kommen. Dies mag zwar bei Computern gelten, die immer am selben Standort stehen. Sobald ein potentieller Terrorist dies aber über ein Notebook an unterschiedlichen Orten tut, ist es nicht nachvollziehbar, warum zwar die Kommunikation über die Tastatur, nicht aber jene über Webcam und Mikrophon "abgehört" werden soll. Gewichtiger wird dieser Umstand noch dadurch, dass Terroristen auf öffentlich zugängliche Computer wie zum Beispiel in Bibliotheken der Überwachung ausweichen können. Es ist nicht anzunehmen und gesetzlich auch nicht gedeckt, dass das BKA präventiv alle frei zugänglichen Rechner in der Bundesrepublik mit diesem Überwachungsprogramm versieht.

Das größte Problem besteht jedoch darin, dass der "Bundestrojaner" erst in solchen Fällen zum Einsatz kommen wird, wo es bereits einen Verdacht auf die missbräuchliche Nutzung des Internets für terroristische Zwecke gibt. Dies soll jedoch nicht bedeuten, dass diese Maßnahme aufgeweicht und präventiv auf sämtlichen Computer angewendet werden soll, wie es die britische Regierung plant. Es soll nur verdeutlicht werden, dass der "Bundestrojaner" in begrenzten Fällen durchaus nützlich sein kann, aber in einer Vielzahl der Fälle keine Wirkung zeigen wird, weil er eben nicht angewendet (weil potentielle Terroristen nicht unter Beobachtung stehen) oder umgangen werden kann (durch Ausweichen auf andere Rechner). Wann immer es

potentiellen Terroristen gelingt, das Augenmerk staatlicher Institutionen im Vorfeld eines Anschlages nicht auf sich zu lenken, und sie gleichzeitig bei der Nutzung des Internets ein gewisses Maß an Vorsicht walten lassen (nämlich durch die Nutzung von Verschlüsselungsprogrammen etc.) oder auf öffentliche Rechner ausweichen, wird der "Bundestrojaner" ein zahnloses Instrument bleiben.

VI. Resümee und Ausblick

Der "Bundestrojaner" bietet gegenüber traditionellen Überwachungsmethoden Vorteile, die von Seiten der Terroristen mit Hilfe von modernen und einfach anwendbaren Verschlüsselungsprogrammen umgangen werden können. Er wird in vielen Situationen keine Wirkung zeigen, weil nicht unter Beobachtung stehende potentielle Terroristen einfach nicht erfasst werden. Darüber hinaus ist anzunehmen, dass die Wirkung dieses Überwachungsinstruments durch die Nutzung frei zugänglicher Computer ausgehebelt wird. Deshalb wird der "Bundestrojaner" nur in seltenen Fällen wirklich zum Einsatz kommen können.

Es bedarf daher einer kritischen Auseinandersetzung mit diesem Instrument. Das Bundesverfassungsgericht hat mit seinem Urteil vom Februar 2008 hier erste Maßstäbe zum Schutz der Persönlichkeitsrechte gesetzt, die im Gesetz großteils auch ihre Widerspiegelung fanden. Vor allem die Betonung, dass der Einsatz dieses Instruments nur in Ausnahmefällen und nur mit richterlicher Genehmigung erfolgen kann sind wichtige Punkte. Gerade hier zeigte sich, wie produktiv sich das politische System der Bundesrepublik auf die Nachbesserung von Schwachstellen im Gesetz ausgewirkt hat. Während im Entwurf des Bundesinnenministers noch die Möglichkeit bestand, den Einsatz der Online-Durchsuchung vorübergehend auch ohne richterliche Genehmigung durchzuführen und die Überprüfung einer möglichen Verletzung der persönlichen Integrität von zwei weisungsgebundenen BKA-Beamten erfolgen sollte, wurden diese Passagen auf Druck kritischer Stimmen im Bundesrat abgeändert. Die beschlossene Version des Gesetzes gewährt somit den wohl höchstmöglichen Schutz an Bürger- und Freiheitsrechten, ohne gleichzeitig die begrenzte Effektivität dieses Instruments zu untergraben.

Es bleibt abzuwarten, wie sich der Einsatz des "Bundestrojaners" nun wirklich auswirken wird.

Die von mir vorgebrachten Argumente deuten aber darauf hin, dass der erhoffte Effekt vielerorts ausbleiben wird. Eine mögliche Ausweitung auf unbeteiligte Computer oder der präventive Einsatz auf Rechnern in öffentlichen Räumen, wie in Großbritannien gefordert, sollte aber auf jeden Fall verhindert werden.

[1] Siehe u.a. Thomas, Al Qaeda and the Internet: The Danger of Cyberplanning, in: Parameters, 33/Spring 2003, S. 112-123, Weimann, www.terror.net: How Modern Terrorism Uses the Internet, Special Report, Washington, DC March 2004.

[2] Thomas, a.a.O., hier S. 112.

[3] Siehe Weimann, Cyberterrorism: The Sum of All Fears? in: Studies in Conflict & Terrorism, 28/2/2005, S. 129-149.

[4] Siehe Tsfati und Weimann, www.terrorism.com: Terror on the Internet, in: "Ebenda 25/5/2002, S. 317-332.

[5] Whine, Islamist organizations on the Internet, in: Terrorism and Political Violence, 11/1/1999, S. 123-132 hier S. 123.

[6] Siehe Hinnen, The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet, in: The

Columbia Science and Technology Law Review, V/2004, S. 1-42.

[7] Zitiert nach Thomas, a.a.O., hier S. 118.

[8] Unter PGP (Pretty Good Privacy) versteht man ein spezielles Verschlüsselungsprogramm. BVerfG, 1 BvR 370/07, 27.02 2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

[9] Siehe Crenshaw, The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice, in: Howard und Sawyer (Hg.), Terrorism and counterterrorism: Understanding the new security environment, Readings & interpretations, Dubuque 2006, S. 54-66, Lake, Rational Extremism: Understanding Terrorism in the Twenty-first Century, in: Dialog-IO, 1/1/Spring 2002, S. 15-28.

[10] Siehe Pape, The Strategic Logic of Suicide Terrorism, in: American Political Science Review, 97/3/August 2003, S. 343-361.

[11] Siehe Sageman, Understanding terror networks, Philadelphia 2004, Sageman, Leaderless Jihad: Terror networks in the twenty-first century, Philadelphia. 2008.

[13] Siehe Kydd und Walter, The Strategies of Terrorism, in: International Security, 31/1/2006, S. 49-80.

[14] Siehe Abrahms, What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy, in: Ebenda 32/4/2008, S. 78-105.

[15] Siehe McCartan, Masselli, Rey und Rusnak, The Logic of Terrorist Target Choice: An Examination of Chechen Rebels Bombings from 1997-2003, in: Studies in Conflict & Terrorism, 31/1/2008, S. 60-79.

[16] Siehe McCormick, Terrorist Decision Making, in: Annual Review of Political Science, 1/6/2003, S. 473-507 hier S. 496.

[17] Siehe Faria, Terrorist Innovations and Anti-Terrorist Policies, in: Terrorism and Political Violence, 18/1/2006, S. 47-56 hier S. 48.

[18] Siehe Jenkins, Defense Against Terrorism, in: Political Science Quarterly, 101/5/1986, S. 773-786 hier S. 777, Enders und Sandler, The Effectiveness of Antiterrorism Policies: A Vector-Autoregression-Intervention Analysis, in: "American Political Science Review", 87/4/December 1993, S. 829-844 hier S. 831, Cauley und Im, Intervention Policy Analysis of Skyjackings and Other Terrorist Incidents, in: American Economic Review, 78/2/May 1998, S. 27-31 hier S. 27.

[19] Siehe Lia und Hegghammer, Jihadi Strategic Studies: The Alleged Al Qaida Policy Study Preceding the Madrid Bombings, in: Studies in Conflict & Terrorism, 27/5/2004, S. 355-375.
