Hans G. Zeger[1],

Konstruktion und Dekonstruktion eines Terroristen?

Mit dem "Terroristenprozess" wurde ein Verfahren in erster Instanz beendet, das eine völlig neuartige Mischung aus Gesinnungs- und Propagandaverfahren, Kommunikationsüberwachung und Internet-Sachbeweisen darstellte - die Ermittlungsorgane (BVT, SEO) trugen große Datenmengen zusammen, die einer nüchternen Beurteilung nicht stand halten - die Sicherheitsbehörden haben eine große Chance vertan, Sinnhaftigkeit und Effizienz von Internetüberwachung zu beweisen - wer in das Visier derartiger Ermittlungsmethoden kommt dürfte es sehr schwer haben, seine Unschuld zu beweisen - auf die Eigentümlichkeiten des Medienraums Internet ist die demokratische Gesellschaft nicht ausreichend vorbereitet

Besonderheiten des Verfahrens

Erstmals standen in Österreich terroristische Hilfsaktivitäten unter Anklage, die weder direkte Tatbeteiligung, Vorbereitungshandlungen, noch deren Finanzierung betrafen, sondern die ideologisch-propagandistische Weiterverbreitung von Ideen. Mit vier Jahren bzw. 22 Monaten vielen die - noch nicht rechtskräftigen - Urteile ziemlich deutlich aus.

Im Verfahren stand die Gesinnung des Angeklagten zur Beurteilung (so Richter Gerstberger am letzten Prozesstag). Damit wurden wesentliche Teile der Europäischen Menschenrechtskonvention, insbesondere Art. 8 (Privatsphäre) und Art. 10 (Meinungsfreiheit) umfassend relativiert, es ging um die Bewertung von Ideologien und oppositioneller Medienarbeit. Weiters wurden reine Internetdelikte verhandelt, bei denen abgesehen von den Angeklagten nicht erkennbar war, wer sonst noch beteiligt ist. Für das Vorhandensein einer terroristischen Vereinigung, als unternehmensartige Struktur wäre jedoch das Vorhandensein von mehr als zwei Personen zwingend vorgesehen.

Mit diesem Verfahren begibt sich eine demokratische Gesellschaft in ein äußerst gefährliches Fahrwasser: Meinungsäußerung, oppositionelle Kritik, Propaganda und Infomation werden unter polizeilichem und sicherheitspolitischem Blickwinkel betrachtet. Das erinnert an Metternichsche Zensur, aber auch an totalitäre Meinungsprozesse. Ein Schritt in Richtung Meinungskontrolle wurde jedenfalls getan.

Im Laufe der Prozesstage drängte sich auch die Frage auf, wie soll sich ein Muslim verhalten, der fundamentale Kritik an den Vorgängen im IRAK und in Afghanistan üben möchte? Würde nicht jede Äußerung als Propaganda terroristischer Gruppen angesehen werden?

Ergebnisse der technischen Überwachung

Wenn Menge Inhalt als Beweismittel ersetzt, dann stehen uns problematische Zeiten bevor. Wenn ein Richter tausende Seiten elektronischer Überwachung als unverständlich kommentiert und meint, dieses Material sollen die Geschworenen eben "der freien Beweiswürdigung unterziehen", sollte der Gesetzgeber mehr als hellhörig werden. Wie soll etwas frei gewürdigt werden, wenn es sogar vom Berufsrichter nicht verstanden wird?

---

1 Der Autor ist Lektor an der Universität Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Obmann der "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (http://www.zeger.at)

Die ermittelten Daten und technischen Informationen wurden daher in Folge gar nicht an sich bewertet, wie dies als Sachbeweis zu erwarten gewesen wäre, sondern dienten als Unterfutter dafür, dass sich die Polizeibeamten bei der Ermittlungsarbeit bemüht haben und dass deren Aussagen und Schlussfolgerungen daher glaubwürdig seien.

Nach dieser Logik und vermutlich mit gleichem Prozessergebnis hätten sich die Beamten hinstellen können und erklären können, dass auf Grund ihrer Erfahrungen, nach gründlicher Befragung des Angeklagten, nach Studium der GIMF-Webseiten ("Globale Islamische Medienfront") und nach Einschätzung der privaten SITE-Organisation (http://www.SITEInstitute.com), die übersetzte Terrorbotschaften kommerziell vermarktet, der Terrorismustatbestand eindeutig belegt sei. Die gesamte problematische technische Überwachung hätte man sich ersparen können.

In jedem banalen Indizienprozess, in dem etwa ein Messer als Tatwaffe zentrale Bedeutung hat, wären Länge und Breite der Klinge, Breite des Messerrückens, Einstichrichtung, Tiefe der Wunde, Blutspuren am Messer und usw. Gegenstand gründlicher Sachverständigengutachten. Kein Geschworener gäbe sich mit Plausibilitätsaussagen nach dem Motto zufrieden: das Opfer wurde mit einem Messer erstochen, der Angeklagte besitzt ein Messer und kennt das Opfer, irgendwas wird schon zusammen passen. Der Grund liegt wohl in der Tatsache, dass sich jeder unter einer Tat mit einem Messer etwas sehr konkretes vorstellen kann und die Unterschiede verschiedener Messertypen und Tatabläufe erkennen und beurteilen kann.

Resümee der Überwachungsergebnisse: Trotz gigantischem Aufwand, aufgeboten wurde das gesamte denkbare Lauscharsenal (akustische- und optische Überwachung, Telefon- und Internet-Überwachung, Computerüberwachung), zum Teil - folgt man dem Verfassungsexperten Funk - jenseits der Legalität, wurden bloß lückenhafte Datentrümmer zusammen getragen, die nur in der Masse, nicht aber im Inhalt beeindrucken und einer nüchternen Beurteilung nicht stand halten.

Wobei die geringen IT-Kenntnisse des Angeklagten den Überwachern entgegen kamen. Wären tatsächlich unternehmensartige Strukturen tätig, die auch grundlegende IT-Kenntnisse hätten, dann wäre das Ergebnis wohl noch bescheidener ausgefallen.

Geschaffen wurden Plausibilitätsketten, wie etwa folgende: Im Drohvideo werden Bilder verwendet, die auf einer regierungsamtlichen Seite vorhanden sind. Auf diese Seite wurde ein Monat vor der Videoveröffentlichung über einen malaysischen Proxyserver zugegriffen und der Angeklagte hatte auch irgendwann diesen Server benutzt. Also muss der Angeklagte, so der kurze Schluss, etwas mit dem Drohvideo zu tun haben.

Es wurde nicht einmal versucht die zeitlichen Abläufe genauer darzustellen und so zumindest die Faktenlage zu verbessern. Von wem und in welchem Ausmaß der malaysische Server tatsächlich genutzt wurde, wurde gar nicht versucht darzustellen. Wenn ein malaysischer Server von BVT-Mitarbeitern als Indiz für besondere Konspirativität vorgeführt wird, wird offenbar mit fehlenden Internetkenntnissen der Richter und Geschworenen spekuliert. Die transkontinentale Lokalisierung von Servern ist typisch für das Internet, ohne dass dadurch automatisch Illegalität abzuleiten wäre. So führt die Spur von www.gimf.org oder www.gimf.net direkt in die USA, von www.gimf.info nach Singapur, ohne dass damit sinnvolles über Inhalt und Betreiber gesagt werden kann.

Nicht unerwähnt soll bleiben, dass mittlerweile für eine Reihe von Internet-Recherchen die Nutzung internationaler Proxyserver zwingend notwendig ist. Immer mehr Anbieter, allen voran die Suchmaschine Google, gehen dazu über ihre Websites und darauf dargestellte Informationen länderspezifisch zu filtern. Zur Filterung wird die IP-Adresse des Benutzers herangezogen. Möchte man

herausfinden, welche Information in einem anderen Land verbreitet werden, muss man zwangsläufig über einen dort beheimateten Proxyserver gehen.

Eine Fülle anklagerelevanter Fragen zu der Videobotschaft blieb offen. Wer tatsächlich der Verleser der Videobotschaft ist, wer hinter der Kamera stand, wo und wie die Produktion erfolgte, wurde nicht einmal andeutungsweise aufgeklärt.

Von den Ermittlungsbeamten wurden dutzende Alias- und Nicknames und Mailadressen präsentiert, wie sie üblicherweise in Foren und Chats verwendet werden. Auch eine Fülle von Dialogen und Beiträgen wurden aufgezeichnet. Hinter diesen Beiträgen stehen zahllose IP-Adressen. Wenn die GIMF tatsächlich eine unternehmensartige Organisation wäre, dann müssten auf Grund dieser IP-Adressen auch Personen identifizierbar sein, die hinter diesen Adressen stehen und die Kontakt mit den Angeklagten hatten. Eine Ausforschung der Personen der zumindest in den USA und EU-Europa lokalisierten IP-Adressen wäre machbar, umso mehr, als das BVT ("Bundesamt für Verfassung und Terrorismusbekämpfung") intensiv mit US-Diensten und dem deutschen Geheimdienst zusammen arbeitete. Tatsächlich führen die BVT-Unterlagen, laut Verlesung der Unterlagen in der Hauptverhandlung aus, dass die Identitäten der Kommunikationspartner des Angeklagten nicht geklärt werden konnten.

Rolle und Funktion elektronischer Kommunikation nicht aufgearbeitet

An seine Grenzen kam das Verfahren auch, als es um die Beurteilung der Internetkommunikation ging. Die verschiedensten Kommunikationsformen wurden vermischt und unterschiedslos nebeneinander gestellt.

Persönliche bzw. private Kommunikation mittels eMail und Chat wurden Veröffentlichungen in Foren und auf Webseiten gleichgestellt, lokale Computernotizen wurde öffentlicher Propaganda gleichgesetzt. Selbst zwischen Uploads und Downloads wurde nicht ordentlich unterschieden, es macht jedoch einen wesentlichen Unterschied, ob jemand eine Information aus dem Internet konsumiert (download) oder verbreitet (upload).

Es entstand damit ein diffuser Daten- und Informationsnebel privater und veröffentlichter Vorstellungen, eigener und bloß wiedergegebener Positionen, der letztlich ausschlaggebend für die Verurteilung war.

Damit wurde einem technischen Werkzeug per se eine besondere deliktische Bedeutung zugewiesen. Das dahinter auch ein ordentliches Maß an Technikfeindlichkeit steckt, sei nur am Rande bemerkt.

Die grundsätzliche Frage, was denn der Unterschied sei, zwischen jemandem der im Hinterzimmer oder am Stammtisch mit Gleichgesinnten und in einer sehr beschränkten Öffentlichkeit über Politiker schimpft oder seinen Vorurteilen und Wut auch in drastischen Formulierungen Ausdruck verleiht und jemandem, der es mittels des technischen Instruments Computer gegenüber einer einzelnen Person oder einer beschränkten Gruppe im Rahmen eines Chats oder eines persönlichen eMails tut, wurde tunlichst vermieden.

Die leichtere Überwachbarkeit des Computers gegenüber den unzähligen alpenländischen Stammtischen kann wohl nicht ein ausreichendes Unterscheidungsmerkmal sein.

Auch die spezifischen Eigenheiten des Medienraums Internet, der nicht mit den klassischen Medienbegriffen beschrieben werden kann, wurden nicht beachtet. Während Printmedien, aber auch Fernsehanstalten lokal verortet sind und damit lokalen Gesetzen und Offenlegungspflichten unterliegen, entfällt dies im

Internet weitgehend. Informations- bzw. Propagandaplattformen können unter Ausnutzung nationaler Rechtsdifferenzen weitgehend anonym betrieben werden (Offshore-Plattformen) und sind auch keinerlei Objektivitätsgebot verpflichtet. Die Mehrzahl der Internetplattformen sind Propaganda- oder Gesinnungsinstrumente, einseitige Informationspolitik ist dabei in der Regel ein bewusster Gegenpol zu anderen existierenden Seiten, weil - so die Logik der Betreiber - es nicht notwendig ist objektiv zu berichten, da sich ja der Internetnutzer durch das Nebeneinander verschiedenster Propagandaplattformen sein eigenes Weltbild zusammenb(r)auen kann.

Meinungsäußerung im Internet tendiert generell zu Radikalisierung und Einseitigkeit, zum einen weil sie sehr oft von Laien und nicht Berufsredakteuren erfolgt, zum Anderen weil die nicht ganz unlogische Vorstellung besteht, da ja jeder seine Meinung äußern könne, müsse man sich nicht um Ausgewogenheit im Einzelfall kümmern. Auch der Schutz der Anonymität begünstigt radikale und extremistische Positionen.

Dies unterscheidet das Internet mit seiner Vielzahl von interaktiven Websites, Blogs- und Communityplattformen, die auch Privatpersonen weltweite Medienpräsenz ermöglichen, fundamental von Fernseh- oder Radio-Berichterstattung, in der der Einzelne keine Möglichkeiten einer Meinungs- und Medienpräsenz hat. Eine ausgewogenere Berichterstattung soll somit den Gegenpol zur beschränkten Verbreitungsmöglichkeit darstellen.

Auch diese grundsätzlichen medienpolitischen und medienkritischen Fragestellungen wurden im Prozess tunlichst vermieden. Dies führte einerseits zu wiederholten hilflosen Versuchen des Angeklagten, seine in unterschiedlichen Formen getätigten Äußerungen zum Teil als private Meinungsäußerung, zum Teil als bloße Weitergabe von bestehenden, veröffentlichten Meinungen und zum Teil als propagandistisches Gegengewicht zu anderen Informationen darzustellen. Andererseits waren Berufs- und Laienrichter mit einem nicht aufbereiteten und unverdaulichen Datengebräu konfrontiert, dass geradezu zwangsläufig höchste Ablehnung und Skepsis hervorrufen musste.

Ist eine demokratische Gesellschaft auf einen Medienraum vorbereitet, in dem jeder jede nur denkbare einseitige Meinung propagieren kann? Die ernüchternde Antwort nach rund 15 Jahren öffentlich zugänglichem Internet lautet NEIN.

GROSSE CHANCE VERTAN

Insgesamt wurde eine große Chance für die technische Kommunikations-Überwachung vertan. SEO ("Sondereinheit für Observation") und BVT hätten auf Grund der weitreichenden Überwachungsbefugnisse die Möglichkeit gehabt, durch objektiv nachvollziehbare Indizienketten zu beweisen, dass eine Internetüberwachung sinnvoll ist und Täter überführen kann.

Dazu wäre es aber notwendig gewesen einerseits alle technischen Zweifel an der Richtigkeit und Vollständigkeit der Aufzeichnungen zu beseitigen und andererseits die Sachbeweise so verständlich aufzubereiten, dass sie auch objektiv und ohne Kommentar der BVT-Beamten für Berufs- und Laienrichter aussagekräftig sind.

Statt ordentliche Indizienketten zu präsentieren wurde die Beurteilung der Überwachungsdaten den Laienrichtern zur "freien Beweiswürdigung" übertragen. Ohne den Laienrichtern nahe treten zu wollen, hatten diese kaum das technische Detailwissen, um tatsächlich die Aussagekraft der Aufzeichnungen beurteilen zu können. Und wenn sie es hätten, dann hätten sie jede Menge von Zusatzfragen zu stellen gehabt. Unter ftp://ftp.freenet.at/pri/fragestellungen-gutachter-terrorprozess.pdf sind einige Fragen zusammengestellt, die sich ein technisch interessierter Prozessbeobachter

unwillkürlich stellt. Damit wurde die Beweisführung auf die Glaubensfrage reduziert, ob den BVT-Beamten oder dem Angeklagten mehr geglaubt wird.

Tatsächlich entstand der Eindruck, dass tunlichst vermieden werden sollte in die Details der Kommunikationsüberwachung zu gehen, das Ergebnis hätte sowohl eine Belastung, als auch eine Entlastung des Angeklagten sein können. Die Vorgangsweise von Gericht und Sicherheitsbehörden ist umso ärgerlicher, als es natürlich technisch möglich gewesen wäre, zu qualitativ wesentlich besseren Sachbeweisen zu gelangen.

Auch die Umstände, wie man dem Angeklagten auf die Spur kam sind unbefriedigend. Der eigentlich amtsbekannte Angeklagte wurde nicht durch eigene Ermittlungen des BVT aufgefunden, sondern durch Hinweise Dritter (US-Dienste, deutscher Verfassungsschutz, Fernsehinterviews). Damit vermag das Verfahren auch sicherheitspolitisch nicht zu überzeugen.

Gefahr der Beweislastumkehr

Für jeden, der ins Visier derartiger Überwachungsmaßnahmen und Datenaufzeichnungen kommt, dürfte es sehr schwer werden seine Unschuld zu beweisen. Was soll er tausenden Seiten von Aufzeichnungen entgegen halten, die, wie die BVT-Beamten behaupten, bestimmte plausible Erklärungen nahelegen, die für sich genommen - laut Richter - jedoch unverständlich sind und zu denen Anträge nach Alternativgutachten abgewiesen werden.

Den Erklärungsversuchen eines Beschuldigten, der in vielen Fällen gar nicht mehr alle Details Jahre zurückliegender Kommunikation und Computeraktivitäten präsent hat und dadurch auch widersprüchliche Erklärungen abgibt, kommt sowieso eine geringere Glaubwürdigkeit zu.

Macht diese Vorgangsweise Schule, wird man in Zukunft mit einer Häufung von Internetverfahren mit unscharfen Verdachtslagen und Gesinnungstaten rechnen müssen.

Propaganda als Delikt?

Nun kann man auf dem Standpunkt stehen, dass die Verbreitung der Reden führender Al Quida-Mitglieder auf deutsch gefährliche Propaganda sei, die zwar niemandem direkt schadet, aber labile Menschen motivieren könnte derartige Texte und Aussagen zum Anlass zu nehmen, selbst aktiv zu werden und Straftaten zu begehen. Daher muss die Verbreitung derartiger Gedanken unterbunden werden.

Folgt man dieser Logik, kommt man rasch in Bereiche der selektiven Meinungs- und Gedankenkontrolle.

Einerseits sei auf die unzähligen Südtirol-Bumser-Verherrlichungen verwiesen, die - selbstverständlich(?) - ungeahndet blieben, an die Verharmlosung nationalsozialistischer und ständestaatlicher Aktionen durch Österreicher, die tausenden Menschen unmittelbar das Leben kosteten und die selbst 2008 bei Gedenkfeiern im Nationalrat ungeahndet verbreitet werden können. Auch die eigentümlichen Kontakte und Beschönigungen österreichischer Politiker für die Aktionen früherer irakischer Diktatoren fallen in diese Gruppe. Extremistische Meinungen und Vorurteile über bestimmte Volks- und Ausländergruppen, nichtchristliche Religionen und Religionsführer, die geeignet sind, labile Charaktere zu Gewalttaten hinzureißen, finden sich sonder Zahl.

Andererseits begünstigen Gesinnungs- und Meinungsverbote immer auch Mythenbildungen. Eine entwickelte demokratische Gesellschaft sollte imstande

sein, auf abseitige Propaganda effektiver als mit Verbotsgesetzen darauf zu reagieren.

Im Übrigen sollte insgesamt das Verhältnis zwischen freier Meinungsäußerung und Gesetzen, die bestimmte Geschichtsleugnungen unter Strafe stellen, neu hinterfragt werden. Bestimmungen, die die Leugnung von Völkermord oder Holocaust unter Strafe stellen sind höchst problematisch und könnten langfristig eine demokratische Gesellschaft schwer belasten. Gerade im Zusammenhang mit Nationalsozialismus und Holocaust schwindet die Zahl der Zeit- und Augenzeugen, der Zeitpunkt ist absehbar, zu dem der letzte Zeuge verstirbt. Anschließend sind nur mehr Schriften, Bild- und Tondokumente vorhanden. Es ist eine Tatsache, dass auch eine Vielzahl gefälschter Dokumente im Umlauf sind. Damit muss befürchtet werden, dass in Zukunft verstärkt Gruppen auftreten werden, die mit Hinweis auf diese Materialien die Vorgänge der NS-Zeit verharmlosen und darauf verweisen werden "dass an der Sache ja irgend etwas nicht stimmt, denn sonst hätte man ja nicht Denkverbotsgesetze" erlassen.

Eine offensive Auseinandersetzung mit ideologisch Abseitigem wäre wohl die beste Immunisierung gegen Geschichtsverfälschung.

Das Überwachungsniveau der BVT

Tiefe Einblicke erlaubte der Prozess auch in die Überwachungsmethoden des BVT und deren Effizienz. Wenngleich die informierten Zeugen des BVT und der SEO Auskünfte über die Überwachungsmethoden unter Hinweis auf Ermittlungsschutz verweigerten, ließen sich doch für Experten ausreichend klare Hinweise auf die Methoden finden.

Positiv für die Ermittler war, dass der Angeklagte technisch nur sehr oberflächliche Informatikkenntnisse hatte und neben dem Standard-Betriebssystem "Microsoft Windows XP", auch den "Microsoft Internet Explorer" und "MSN Messenger" verwendete. Für diese Systeme existieren die meisten Überwachungswerkzeuge. Auch dass der Angeklagte "vergessen" hatte, die Verschlüsselung im Messengerdienst zu aktivieren, erleichterte die Überwachung, so ein BVT-Mitarbeiter. Insgesamt dürfte der Angeklagte seinen eigenen Computer nicht ausreichend unter Kontrolle gehabt haben.

Dass bei der forensischen Datensicherung bloß das Disk-Sicherungsprogramm Encase verwendet wurde, das sich etwa zur Integritätssicherung der beschlagnahmten Daten mit dem Hashverfahren MD5 zufrieden gibt, ein Verfahren das seit etwa zehn Jahren als nicht mehr sicher eingestuft wird, ließe Raum für Spekulationen und begründete Vorwürfe, dass Datenmaterial nachträglich manipuliert wurde. Selbstverständlich existieren modernere Integritätssicherungsverfahren, die als nicht manipulierbar gelten. Man hätte gerade bei derartig schweren Vorwürfen erwarten können, dass jeder, auch noch so geringe Manipulationsverdacht von vornherein ausgeschalten wird.

Weiters wurden keine Maßnahmen gesetzt, die zuverlässige zeitliche Zuordnungen der einzelnen überwachten Daten erlauben würden. Dazu wären jedoch technische Mittel, sogenannte Zeitstempeldienste, verfügbar, die eine eindeutige zeitliche Einordnung erlauben. Wenn diese Zeitstempeldienste von Dritten in Anspruch genommen werden, wäre jeder Manipulationsverdacht ausschaltbar gewesen.

Die Überwachung des Internetverkehrs erfolgte beim Provider Chello durch ein dem tcpdump vergleichbares Filterprogramm, das die Internet-Datenpakete von und zum Angeklagten kopierte. Die Verwendung einer Virtual Private Network - Software (VPN) wie sie als Freeeware in dutzenden Versionen verfügbar ist (der Angeklagte verwendete OpenVPN, http://openvpn.net/) und von SSL-/TLS-Serververbindungen reichten jedoch, um diese Aufzeichnungen für die Ermittlungsbeamten weitgehend wertlos zu machen.

Doch wie formulierte es ein BVT-Beamter in verblüffend naiver Logik: "OpenVPN und Proxyserver, welche Privatperson verwendet das schon, so jemand muss doch was zu verbergen haben!" ... und wer etwas verbirgt, muss ja auch ein Täter sein, ist man versucht zu ergänzen. Damit stehen etwa 5-10.000 Menschen in Österreich unter Generalverdacht, so groß dürfte mittlerweile die Community der notorischen VPN-Nutzer sein.

Die Überwachung der eMail-Kommunikation wurde schlicht dadurch unterlaufen dass ein eMail-Account gemeinsam genutzt wurde. Mails wurden nicht verschickt sondern auf einem Mailserver als Mail-Entwurf hinterlegt. Der Kommunikationspartner rief dann den Entwurf über ein Webmail-Interface über denselben Account ab, trug seine eigenen Nachrichten ein usw. usf. Eine simple Maßnahme, die auch die geplante Vorratsdatenspeicherung unterlaufen würde. Mails, die nie verschickt werden, werden nicht protokolliert, die Nutzung bzw. der Aufruf von Webseiten wird von der Vorratsdatenspeicherung nicht erfasst.

Um die Onlineüberwachung durchführen zu können, wurde in die Räume des Angeklagten eingebrochen und vor Ort ein Spyware-Programm am Computer des Angeklagten installiert. Das Programm entspricht, auch wenn das BVT keine Angaben dazu machen möchte, dem bekannten Orvell-Programm der ProtectCom GmbH. Das Programm erlangte vor einigen Jahren eine gewisse Berühmtheit, als sich herausstellte, dass mehrere Ministerien damit experimentierten.

Genutzt wurden die typischen Funktionalitäten wie Screenshots und Keylogging (Aufzeichnung der Tasteneingaben). Auch dieser Lauschangriff wäre mit Standardmitteln leicht zu umgehen.

Insgesamt ergibt sich folgendes Bild: Jemand, der etwas zu verbergen hat oder dem bloß seine Privatsphäre wichtig ist, müsste folgende Maßnahmen zur Abwehr eines Überwachungsangriffs setzen:

- Verschlüsselung seiner Festplatte (damit kann weder der Festplatteninhalt ausgespäht werden, noch ist es möglich ein Spyware-Programm ohne Zerstörung der Festplattendaten zu installieren)
- Hochfahren / Booten des Computers über eine CD (wer ganz sicher sein will, kann auch einen signierten und verschlüsselten USB-Stick verwenden)
- laufendes Entfernen temporärer Dateien, Beobachtung des Internettraffics
- laufende Kontrolle des Rechners mittels Anti-Spyware-Programme
- Nutzung von VPN-Software, SSL-/TLS-gesicherte Webserver, etwa für Forums- oder eMail-Nutzung und Verschlüsselung im Chat- oder eMail-Verkehr

Die Computernutzung wäre mit diesen Maßnahmen schon unter den Microsoft-Betriebssystemen sicher. Will der Benutzer zusätzliche Sicherheit, ist er gut beraten, auf Linux umzusteigen. Dafür existiert zwar auch Angriffs- und Überwachungssoftware, gleichzeitig gibt es aber zusätzliche Monitoring-Produkte, die es auch dem privaten Nutzer erlauben "verdächtigen" Datenverkehr über seinen Computer leichter zu erkennen und zu unterbinden.

Installationsaufwand für einen derartigen BVT-sicheren Computer: rund vier Stunden, Zusatzkosten: unter hundert Euro. Nach erfolgter Installation ist die Nutzung des Computers nicht wesentlich umständlicher als ein ungesicherter Computer.

Insbesondere die Verschlüsselung der Festplatte und das externe Booten sind ein Gebot der Stunde für jeden sorgsamen Computerbenutzer, bleibt doch damit auch im Fall eines Verlustes oder Diebstahls die Vertraulichkeit der Daten gewahrt.

Auf offensive Schutzmaßnahmen, wie zu den Produkten TOR, JAP, freenet oder Psiphon vergleichbare Anonymisierungsdienste, die aktiv Benutzerspuren im Internet verwischen, wird dabei noch gar nicht eingegangen.

DISCLAMER

Diese Ausführungen können keine Rechtfertigung oder gar Identifizierung mit den Handlungen und Absichten von Mohamed M. darstellen. Dies schlicht schon allein deswegen nicht, weil die Absichten nicht wirklich bekannt sind. Weder die Verantwortung des Angeklagten, noch die Behauptungen der Anklage, beide im jeweiligen Sinn gefärbt - was im Rahmen eines Strafverfahrens völlig legitim ist - konnten bei nüchterner Betrachtung ein lückenlos nachvollziehbares Bild der Ziele liefern.

Wenn die immer wieder wechselnde Verantwortung zu den Beweggründen für die Beteiligung an der GIMF-Propaganda stellenweise befremdlich und wenig glaubwürdig erscheint, muss auch zu Bedenken gegeben werden, dass es in einem Strafverfahren nicht so sehr auf die Glaubwürdigkeit des Angeklagten ankommt, sondern um die Glaubwürdigkeit der Anklage und deren Beweisführung geht. Hier blieben Lücken und Fragen offen.