

10. EUROPÄISCHER POLIZEIKONGRESS

Jörg Ziercke, Präsident des Bundeskriminalamts

„Aktuelle Entwicklungen bei der Terrorismusbekämpfung aus polizeilicher Sicht“

Es gilt das gesprochene Wort!

Meine sehr verehrten Damen und Herren,

vor einem Jahr habe ich an dieser Stelle über „Neue Allianzen gegen Terrorismus und Extremismus“ referiert. Ich habe über die hohe Bedeutung der präventiven Maßnahmen gegen Extremismus und Terrorismus gesprochen und die Rolle des BKA bei der Vorbereitung der Fußball-WM 2006 skizziert. Nun können wir auf dieses „Sommermärchen“ gelassen zurück blicken. Auch wenn wir nicht Fußballweltmeister geworden sind, hat die deutsche Polizei eine der größten Herausforderungen, die sie je zu bewältigen hatte, mit vereinten Kräften – auch aus anderen EU-Staaten – hervorragend gemeistert.

2006 war aber nicht nur durch dieses sportliche Highlight geprägt. 2006 steht auch für eine Reihe von Anschlägen, die uns das hohe Gefahren- und Schadenspotential des internationalen Terrorismus auch in Deutschland erneut vor Augen geführt haben.

Ganz allgemein sind es nicht mehr staatliche Konflikte, sondern transnationale Bedrohungsfaktoren, die heute dominieren. Wie zum Beispiel Globalisierungsrisiken, illegale Migration und Integrationsprobleme, Proliferation, Regionalkonflikte, Organisierte Kriminalität, Störungen Kritischer Infrastrukturen – um nur einige zu nennen. Die Trennung von innerer und äußerer Sicherheit ist obsolet geworden. Die Handlungsfähigkeit der Nationalstaaten ist dadurch zunehmend eingeschränkt. Die neuen Verwundbarkeiten moderner Industriegesellschaften haben die

Sicherheitsumgebung verändert. Von einem erweiterten Sicherheitsbegriff ist die Rede.

Vor diesem Hintergrund hat sich an meiner Einschätzung zur Bedrohung durch den internationalen islamistischen Terrorismus seit dem vergangenen Jahr im Grunde nichts geändert. Trotz zahlreicher polizeilicher Erfolge kann es keine Entwarnung geben. Die Strukturen des islamistischen Terrorismus sind weiterhin funktionsfähig und Terroristen trotz aller polizeilichen Erfolge in der Lage, Anschläge durchzuführen. Die Bundesrepublik Deutschland ist dabei nach wie vor Teil eines weltweiten Gefahrenraumes, auch wenn uns derzeit keine konkreten Erkenntnisse für einen bevorstehenden Anschlag vorliegen. Die Bekämpfung des internationalen Terrorismus bleibt eine der größten Herausforderungen für die Sicherheitsbehörden weltweit. Dass diese Aufgabe unsere Aufmerksamkeit auf hohem Niveau erfordert, zeigte sich im vergangenen Sommer insbesondere an zwei Ereignissen.

Meine Damen und Herren,

sicher sind viele von Ihnen mit dem Flugzeug nach Berlin angereist. Seit August des vergangenen Jahres müssen wir uns an neue Bestimmungen zum Handgepäck halten, was gerade für Vielflieger nicht immer einfach ist. Der Grund dafür ist bekannt: Am 10. August 2006 wurden in Großbritannien 24 Personen festgenommen. Sie stehen im Verdacht, einen Terroranschlag geplant zu haben, von dem vermutlich mehrere Passagierflugzeuge betroffen gewesen wären. Die Tatverdächtigen befanden sich bereits im Stadium einer fortgeschrittenen Anschlagplanung.

Auch in Deutschland sind wir im vergangenen Sommer nur knapp einem terroristischen Anschlag entgangen. In zwei Regionalzügen Richtung Hamm und Koblenz wurden am 31. Juli 2006 zur Mittagszeit zeitgleich zwei unkonventionelle Sprengvorrichtungen in Koffern mittels eines Zeit-Zündmechanismus gezündet. Aufgrund eines Konstruktionsfehlers detonierten die Bomben trotz Zündauslösung nicht. Eine Detonation der explosionsfähigen Sprengvorrichtung hätte in beiden Fällen zu einer erheblichen Druckwelle verbunden mit einem Feuerball geführt. Das

steht nach Sprengversuchen der Bundesanstalt für Materialforschung und -prüfung fest.

Die Anleitungen zum Bau der Bomben fanden die Täter im Internet, ebenso wie die Fatwa, ein islamisches „Rechtsgutachten“, mit dem sie ihre Taten gerechtfertigt glaubten.

Was wäre geschehen, wenn die Täter ihren Plan umgesetzt hätten? Ausgebrannte Waggon, entgleiste Züge, Tote und Schwerverletzte wären die mögliche Folge gewesen. Und eine öffentliche Diskussion in Deutschland, die die derzeitige Kritik an der Online-Durchsuchung mit Erstaunen zur Kenntnis genommen hätte. Doch dazu später. Welche Konsequenzen ziehen wir aus diesen Ereignissen? Inwiefern gibt es neue Entwicklungen im Hinblick auf Erscheinungsformen, die Motivation und den Modus Operandi des internationalen Terrorismus?

Anders als am 11. September 2001 hatten wir es bei den jüngsten Anschlägen nicht mehr mit Tätern zu tun, die eine direkte Verbindung zu Al-Qaida haben. Sie waren allenfalls von der durch Al-Qaida verkörperten Ideologie inspiriert.

Die operative Basis von Al-Qaida wurde nach dem Einmarsch der alliierten Truppen in Afghanistan im Oktober 2001 und dem Sturz des dortigen Taliban-Regimes weitgehend zerstört. Dadurch wurde auch – ebenso wie durch die zahlreichen Festnahmen der vergangenen Jahre – die Organisationsstruktur von Al-Qaida weitgehend zerschlagen. Eine hierarchisch gegliederte Neuformierung ist derzeit nicht erkennbar.

Andere regional nicht mehr eingrenzbar Erscheinungen des Terrorismus haben ihre Ideologie aber übernommen. Zum Beispiel so genannte non aligned mudschahidin, selbsternannte „Gotteskrieger“, die unabhängig von Al-Qaida agieren, wie in Madrid. Autonome Zelle, wie die jungen Libanesen in Deutschland. Fanatisierte Einzeltäter, wie der Mord an van Gogh in den Niederlanden. Suizidtäter, wie in London. Mit den Anschlägen von London im Juli 2005 verlor auch Westeuropa seinen Status als eine der letzten Regionen weltweit, in der das terroristische Mittel des Suizidattentäters bislang nicht zur Anwendung kam. Oder – homegrown-networks, wie in Großbritannien, mit dem wesentlichen Merkmal, dass eine Radikalisierung im Westen erfolgte und dass es sich typischerweise um Einwanderer der zweiten und

nachfolgenden Generationen handelt, die wenige bis gar keine Verbindungen zu bekannten islamistisch terroristischen Netzwerken aufweisen.

Das Phänomen der homegrown-networks war in Deutschland bislang nicht bekannt. Dies änderte sich im August des vergangenen Jahres. Am 26. August verdichteten sich Hinweise auf einen unmittelbar bevorstehenden Anschlag während einer Konzertveranstaltung der Sängerin Nena in Gelsenkirchen. Zur Gefahrenabwehr wurden am Tag des Konzerts insgesamt acht Personen durch die Polizei in Gewahrsam genommen und deren Wohnungen durchsucht. Es handelt sich um mutmaßliche Mitglieder eines Netzwerks, das sich überwiegend aus türkischstämmigen Islamisten zusammensetzt. Sie alle leben seit längerer Zeit in Deutschland. Die Generalbundesanwaltschaft hat ein Ermittlungsverfahren eingeleitet.

Mit Blick auf die verschiedenen Erscheinungsformen des internationalen Terrorismus kann vor allem eines gesagt werden: Ein festes Raster gibt es nicht – die Tätergruppierungen sind überaus heterogen.

Zur Motivation der Täter: Bei der Motivation der Täter hat das Internet – zumindest bezogen auf das auslösende Moment – eine wichtige Bedeutung. So wurde der Tatentschluss der beiden Libanesen nach derzeitigem Ermittlungsstand durch islamistische Propaganda begünstigt, die im Internet verbreitet wurde. Sie bezog sich auf die Veröffentlichung der Mohammed-Karikaturen in Dänemark und den Tod des Al-Qaida-Terroristen Al-Sarkawi im Irak. Auffällig ist dabei, dass zwischen diesen beiden Ereignissen und dem Tag der geplanten Anschläge nur wenige Monate lagen. Von der Rekrutierung, der Fanatisierung bis zum Tatentschluss ist eine Verkürzung des Zeitablaufs eingetreten.

Zum Modus Operandi: Auch bei der Tatplanung spielt das Internet heute eine wichtige Rolle. So haben u. a. die jeweiligen Täter bei den Anschlägen in den USA, auf Bali, in Istanbul und Madrid das Internet nachweislich sehr intensiv genutzt. Es wird von den Tätern oftmals zur Selbstradikalisierung genutzt. Das gilt auch für die Attentäter von London. Al-Qaida verfolgt ein Konzept der Indoktrinierung über die

modernen Medien, das leider aufzugehen scheint. Sie profitiert dabei offensichtlich auch von der Evolution des Internet. Potenzielle Attentäter suchen im Internet jedoch nicht nur nach islamistischem Gedankengut, sondern auch nach Informationen über gegebenenfalls zu attackierende Zielobjekte.

Auch bei der Zielauswahl stellen wir Veränderungen fest. Bei früheren Anschlägen wählten die Attentäter Ziele mit einer wichtigen Symbolik, wie etwa World-Trade-Center und Pentagon aus. Bei den jüngsten Anschlägen scheint Rache für ein vermeintlich erlittenes Unrecht im Vordergrund zu stehen. So sind nun vermehrt weiche, d. h. ungesicherte Ziele in den Fokus geraten. Symbolische Einrichtungen, wie z. B. Synagogen auf Djerba und in Istanbul werden heute seltener ausgewählt. Beispiele für weiche Ziele sind die Anschläge auf Hotels oder Gaststätten, z. B. in Casablanca oder auf Bali. Im Gegensatz zu besonders geschützten Botschaften oder Konsulaten gewähren sie in der Regel freien Zugang.

Eine Eskalation in Bezug auf weiche Ziele stellen die Anschläge in Madrid im März 2004 und in London im Juli 2005 dar. Sie zeichneten sich durch keinen besonderen Symbolwert aus und hatten die Vernichtung möglichst vieler Menschenleben und die Verbreitung von Furcht und Schrecken zum Ziel.

Ein weiterer Aspekt bei der Nutzung des Internet im Zuge der Tatplanung ist inzwischen allgemein bekannt. Im Internet gibt es einen schier unerschöpflichen Fundus an Anleitungen zum Bau unkonventioneller Sprengvorrichtungen. Für islamistische Attentäter ist es ein Leichtes, sich diese herunterzuladen. Im Einzelhandel besorgt man sich die wesentlichen Zutaten – kostengünstig und völlig legal.

Insgesamt kann man bzgl. des logistischen und finanziellen Aufwandes und damit des gesamten Modus Operandi eine Entwicklung zur Vereinfachung feststellen. So war mit den Anschlägen vom 11. September 2001 nicht nur ein sehr hoher finanzieller Aufwand verbunden. Ihnen gingen auch mehrjährige Planungen und Vorbereitungen voraus.

Die jüngsten Anschlagversuche in Europa zeichnen ein anderes Bild: Tatmittel waren selbst gebaute Sprengsätze, z. B. Selbstelaborate wie in London oder manipulierte Gasflaschen und Kraftstoff wie bei den Anschlagversuchen in Deutschland. Die Kosten der Anschlagversuche auf die Regionalzüge nach Koblenz und Hamm lagen vermutlich unter 200 Euro.

Meine sehr verehrten Damen und Herren,

Aus den Entwicklungen der vergangenen Monate konnten wir neue Schlüsse für unsere Bekämpfungsstrategien ziehen. Zugleich wurden wir aber auch darin bestätigt, den bisher verfolgten ganzheitlichen Ansatz weiter konsequent umzusetzen.

Auf den Punkt gebracht bedeutet das: Wir müssen den Netzwerken des Terrorismus ein Netzwerk an Informationen entgegensetzen. Hier spielt das Gemeinsame Terrorismusabwehrzentrum in Berlin – kurz GTAZ – weiterhin eine zentrale Rolle. Im Dezember 2004 als neues Kooperationsforum der Sicherheitsbehörden gegründet, um die Zusammenarbeit der im Phänomenbereich islamistischer Terrorismus zuständigen Ämter sowohl auf der konzeptionell-analytischen Ebene als auch im operativen Bereich zu verbessern, hat es sich in der Zwischenzeit vielfach bewährt.

Mit der Einrichtung des GTAZ wurde die behördenübergreifende Zusammenarbeit zwischen dem BKA, dem Bundesamt für Verfassungsschutz (BfV), dem Bundesnachrichtendienst (BND), den Kriminal- und Verfassungsschutzämtern der Länder, dem Militärischen Abschirmdienst (MAD), der Bundespolizei sowie dem Zollkriminalamt (ZKA) auf eine neue Grundlage gestellt. Wichtigstes Ziel ist das frühzeitige Erkennen möglicher Bedrohungsszenarien. Aktuell vorliegende Erkenntnisse aller im GTAZ vertretenen Behörden werden einer abgestimmten Erstbewertung unterzogen.

Zentrales Element dieses Informationsverbundes sind tägliche gemeinsame Lagebesprechungen aller eingebundenen Behörden. Dabei werden tagesaktuell polizeiliche und nachrichtendienstliche Erkenntnisse ausgetauscht und anlassbezogen Erstbewertungen erstellt. Darüber hinaus werden Gefährdungs- und Fallauswertungen vorgenommen, operative Informationen ausgetauscht und

Strukturanalysen erstellt. Trotz dieses intensiven Informationsaustauschs zwischen Polizei und Nachrichtendiensten, bleibt das Trennungsgebot gewahrt.

Nicht zuletzt die Erfahrungen aus dem GTAZ haben uns vor Augen geführt, dass der Austausch von Informationen in Echtzeit für die Verhinderung von Anschlägen und für die Verfolgung islamistischer terroristischer Straftäter unerlässlich ist.

In Zukunft steht uns hierfür mit der Antiterrordatei (ATD) ein weiterer Baustein im sicherheitsbehördlichen Netzwerk zur Verfügung. Mit Hilfe der ATD können wir den Austausch der Erkenntnisse der Sicherheitsbehörden von Bund und Ländern weiter optimieren. Es handelt sich um eine zentrale Datei, deren Daten schon in anderen Ablagen gespeichert werden. Daten werden zum einen von den Nachrichtendiensten (BND, BfV, LfVs und MAD) und zum anderen von den Polizeien (BKA, Bundespolizei, LKÄ und ZKA) geliefert.

In der ATD wird insbesondere aus Gründen des Quellenschutzes zwischen offen und verdeckt gespeicherten Daten unterschieden. Zwar kann nach allen Daten recherchiert werden, angezeigt werden aber nur die Treffer des offenen, nicht des verdeckten Bestandes. Der Besitzer der verdeckt gespeicherten Daten wird automatisch über die Anfrage informiert und entscheidet selbst, ob er antwortet.

Ein Treffer im offenen Bestand gibt nur Auskunft über die Grunddaten und zieht immer eine konventionelle Anfrage bei der datenbesitzenden Behörde auf Grundlage der bisherigen rechtlichen Möglichkeiten nach sich. Auf der Basis dieser Anfrage werden die so genannten erweiterten Grunddaten übermittelt. Lediglich in ausdrücklichen Eilfällen kann eine Behörde ausnahmsweise auf die erweiterten Grunddaten zugreifen. Diese Fälle müssen jedoch von den Behördenleitern genehmigt werden.

Durch dieses komplexe System kann gewährleistet werden, dass das Trennungsgebot, der Datenschutz und der Quellenschutz gewahrt werden.

Als weitere Konsequenz aus den Ereignissen des vergangenen Jahres konzentrieren wir uns noch mehr als zuvor auf das Internet. Ich habe bereits betont: Als Verbreitungsmedium für extremistische Propaganda, als Forum für potentielle islamistische Terroristen und als Tatmittel zur Rekrutierung junger Menschen zum

Jihad ist das Internet das entscheidende Kommunikationsmittel des islamistischen Terrorismus.

Um es gleich vorweg zu sagen: Deutschland soll kein Überwachungsstaat werden und wir wollen keineswegs alle Internet-Nutzer unter Generalverdacht stellen. Die Sicherheitsbehörden müssen aber auf die rasante Geschwindigkeit, mit der sich die Kommunikationsmuster unserer Gesellschaft entwickeln, reagieren können.

Meine sehr verehrten Damen und Herren,

wie auch das Bundesverfassungsgericht bei seiner Entscheidung zur Wohnraumüberwachung gesagt hat, muss die Polizei in die Lage versetzt werden, in den Bereichen Terrorismus, Schwerstkriminalität und bei der besonders sozialschädlichen Kriminalität mit dem technischen Fortschritt Schritt halten zu können.

Am 1. Januar 2007 nahm das Gemeinsame Internetzentrum (GIZ) der Bundessicherheitsbehörden den Betrieb auf. Diese behördenübergreifende Internet-Monitoring- und Analysestelle soll zur Verbesserung der Erkenntnislage zu extremistischen und terroristischen Aktivitäten im Internet beitragen. Dort arbeiten Beschäftigte des BKA mit Mitarbeitern des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes unter Federführung des Bundesamtes für Verfassungsschutz zusammen. Sie sichten und analysieren Webseiten von Einzelpersonen oder Organisationen, Newsgroups, Foren und Chatrooms. So sollen extremistische und terroristische Aktivitäten im Internet frühzeitig erkannt werden.

Auch im Rahmen der Deutschen EU-Ratspräsidentschaft wollen wir eine vertiefte Zusammenarbeit beim Beobachten und Analysieren von Internetauftritten terroristischer Strukturen erreichen. Diese Initiative steht unter dem Motto „check the web“. Dabei soll die Abstimmung zwischen den Mitgliedstaaten unter Berücksichtigung der besonderen Sprach- und Sachkompetenz ihrer Sicherheitsbehörden intensiviert werden. Bei Europol wird ein Portal eingerichtet, über das die Mitgliedstaaten Informationen austauschen können.

Außerdem setzt sich die deutsche EU-Ratspräsidentschaft dafür ein, den 2005 zwischen sieben Mitgliedstaaten geschlossenen Vertrag von Prüm in den

europäischen Rechtsrahmen zu überführen. Damit soll die Kooperation aller 27 EU-Mitgliedstaaten bei der Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration verbessert werden. Straftäter dürfen keine Chance haben, sich durch Überschreiten der Grenze ihrer Verfolgung zu entziehen. Wir wollen einen polizeilichen Informationsverbund aufbauen, um europaweit wirksam gegen Schwerkriminelle vorzugehen. Dabei ist es uns ein besonderes Anliegen, dass ein europaweiter Austausch personenbezogener Informationen über terroristische Gefährder stattfindet, an dem sich alle Mitgliedstaaten beteiligen. Der DNA-Datenabgleich mit Österreich hat bislang zu 1.500 Treffern geführt, die wir zur Zeit auswerten.

Als weiteres operatives Instrument im Kampf gegen den Terrorismus müssen wir die bestehenden Fahndungsinstrumente wie die Überwachung der Telekommunikation stärken.

Meine Damen und Herren,

ohne das Mittel der Telekommunikationsüberwachung ist eine effektive Bekämpfung des internationalen Terrorismus nicht möglich. Gleiches gilt im Übrigen für die Bekämpfung der Organisierten Kriminalität. Es ist mir sehr wichtig zu betonen, dass wir diese Maßnahmen nur sehr gezielt zur Aufklärung schwerer Straftaten einsetzen. 99,9 Prozent aller in Deutschland lebenden Menschen sind davon nicht betroffen. Eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht belegt den zurückhaltenden Gebrauch der TKÜ durch die Strafverfolgungsbehörden. Niemand braucht in der Bundesrepublik „Orwell’sche“ Verhältnisse zu befürchten. Niemand will das – auch die Polizei nicht!

Was aber die Rechtsprechung des Bundesverfassungsgerichts, die ich respektiere, in der Praxis für Folgen haben kann, belegt das Beispiel der Wohnraumüberwachung, die für verfassungsgemäß – unter bestimmten Bedingungen – erklärt worden ist.

Die Entscheidung des Bundesverfassungsgerichts zum Schutz der Privatsphäre vom 3. März 2004 wirft aus polizeilicher Sicht aber schier unlösbare Probleme auf. Darin forderte der Erste Senat einen absoluten Schutz des Verhaltens in Privaträumen. Daher dürfe die Polizei Gespräche, die den Kernbereich privater Lebensgestaltung

beträfen, weder mithören noch aufzeichnen. Derartige polizeiliche Überwachungsmaßnahmen sind seither praktisch nicht mehr durchsetzbar, da die Prognose einer möglichen Betroffenheit des grundrechtlich geschützten Kernbereichs in der Praxis äußerst schwierig festzustellen ist. Diese Schwierigkeiten betreffen insbesondere den Zeitpunkt für Beendigung und Wiederaufnahme der Überwachung. Um vorherzusehen, wann ein Gespräch mit Vertrauten beendet ist und die Wiederaufnahme der Überwachung möglich wäre, müssten die Polizeibeamten über geradezu hellseherische Fähigkeiten verfügen. So ist die Wohnraumüberwachung heute logistisch kaum noch umsetzbar. Darüber hinaus ist nur mit bruchstückhaften, keinesfalls zielführenden Ergebnissen zu rechnen. Daher wurde die Wohnraumüberwachung als Instrument der Strafverfolgung seit der Entscheidung des Bundesverfassungsgerichts praktisch unbrauchbar. Das BKA hat seit der Entscheidung des Bundesverfassungsgerichts keine Wohnraumüberwachung mehr durchgeführt. Bisher war dies ein durchaus erfolgreiches Instrument in der Bekämpfung des internationalen Terrorismus. Dies bestätigen uns auch unsere ausländischen Kollegen. Aus vielen Bundesländern wird Ähnliches berichtet.

Meine Damen und Herren,

Sie haben die Diskussion um die Zulässigkeit der so genannten Online-Durchsuchung verfolgt. Es handelt sich um eine Maßnahme, mit der ganz gezielt schwere Straftaten aufgedeckt werden sollen. Wir müssen darauf reagieren, dass sich die Täter – und das gilt längst nicht nur für den Bereich des Terrorismus – zunehmend des PCs als Tatmittel bedienen. Sie ziehen ihre PCs bei der Tatvorbereitung heran und tauschen ihre Informationen immer öfter rechnergestützt aus. Die Polizei muss mit diesem technischen Fortschritt der Täter Schritt halten und darf nicht zulassen, dass diese den „Cyberspace“ als geschützten Raum für sich in Anspruch nehmen. Wir brauchen dieses Instrument vor allem zur Aufdeckung krimineller Netzwerke in den Bereichen Terrorismus, Organisierte Kriminalität, Kinderpornografie, Wirtschaftskriminalität, Menschenhandel und Waffenhandel.

Die positiven Seiten des Internet sind Ihnen allen bekannt. Einige Zahlen zu seiner negativen Seite: Von 2005 auf 2006 stieg die Zahl der Straftaten, bei denen das Internet als Tatmittel genutzt wurde, um 115% auf 118.000 Fälle. Im Mai 2006

wurden ca. 12.000 neue Phishing-Seiten registriert, im Monat November allein 37.000, und das mit steigender Tendenz. In einem Jahr sind weltweit ca. 1,2 Millionen Bankkunden durch Phishing-Angriffe geschädigt worden. Die Angriffe mit Bot-Netzen, um Spam-Mails zu transportieren, explodieren in Millionenhöhe – wenn zum Beispiel in einem Fall ca. 40.000 Rechner weltweit von Internet-Kriminellen gekapert werden, und der Einsatz von Trojanern, die auch über Spam-Mails verschickt werden, sich vervierfacht. Der tägliche Mailverkehr besteht inzwischen zu 60 bis 90 Prozent aus Spam-Mails. 2,5 Millionen Hacking-Angriffe gab es laut BSI im Jahr 2005 auf den Informationsverbund der Behörden zwischen Berlin und Bonn. 2006 sind über 20.000 neue Schadprogramme entdeckt worden. Wirtschaftsspionage, Kinderpornografie und Rechtsextremismus – die Kriminalität im Internet kennt keine Grenzen. Vor allem – Internet-Kriminelle müssen den Opfern nicht Auge in Auge entgegentreten, sie haben keine psychologischen Hemmungen. Auf Knopfdruck produzieren sie Tausende von Opfern.

Für den internationalen islamistischen Terrorismus ist das Internet mit ca. 5.000 Seiten eine unverzichtbare Propaganda-Plattform. Der virtuelle globale Jihad. Über das Internet werden junge Menschen radikalisiert, als Suizidtäter angeworben, Bombenbauanleitungen angeboten, Anschlagpläne geschmiedet. Internet-Täter nutzen moderne Technologien. Die Polizei kann dem nur Einhalt gebieten, wenn sie auf Augenhöhe mit diesen Kriminellen agieren kann. Anders kann man keine Strukturen erkennen, um vor die Lage zu kommen, um Anschläge zu verhindern!

Die Bekämpfung des Terrorismus und der OK erfordert vor allem den Einsatz verdeckter Maßnahmen. Nur dann sind wir in der Lage, über den erkannten Einzeltäter hinaus die dahinter stehenden Netzwerke zu erkennen. Offene Maßnahmen, z. B. Wohnungsdurchsuchungen, finden in diesen Verfahren deshalb relativ spät statt, da es um mehr geht als um wenige erkannte Tatverdächtige. Die klassische Hausdurchsuchung würde die Täter im Netzwerk warnen. Vor allem aber bringt die Beschlagnahme des PCs einschließlich Festplatte bei diesen hochprofessionellen Tätern nicht den gewünschten Erfolg. Festplatten, die verschlüsselt/kryptiert sind, können kaum entschlüsselt werden. Jeder Informatiker kann die Grenzen beschreiben, die durch die Verschlüsselungstechniken im heutigen Internet – übrigens kostenfrei herunterzuladen – für die Entschlüsselung bestehen.

Für eine erfolgreiche Beweisführung müssen wir also vor oder nach der Verschlüsselung durch den Täter auf den PC zugreifen können. Ferner nutzen Internetprofis das World Wide Web, um auf virtuellen Laufwerken irgendwo auf der Welt ihre Daten sicher zu speichern. Das heißt, das World Wide Web wird zum universellen Datenspeicher und nicht der heimische PC mit Festplatte. Beweissicherstellung ist nur möglich, wenn der Internet-Kriminelle seine Daten auf den häuslichen PC herunterlädt. Den Zugang zu World Wide Web-Datenspeichern kryptiert er selbstverständlich! Nur wenn wir online zugreifen können, haben wir eine Chance. Passwörter und Schlüssel speichert der Profi natürlich nicht auf seinem PC. Diese bewahrt er außerhalb auf, was ich übrigens jedem Internetnutzer auch nur dringend empfehlen kann. Nur wenn wir online zugreifen können, haben wir eine Chance, in den Besitz dieser Passwörter oder Schlüssel zu kommen.

Meine sehr verehrten Damen und Herren,

der Staat wird dadurch nicht zum kriminellen Hacker! Man sollte die Dinge nicht auf den Kopf stellen. Niemand würde einen Polizeibeamten, der auf richterlichen Beschluss in eine Wohnung eindringt, durchsucht und Sachen beschlagnahmt, als Einbrecher bezeichnen. Mit dubioser Hacker-Software oder mit Trojanern, die Schadsoftware darstellen, operieren wir nicht. Unsere mögliche Strategie lautet: gezielter Einsatz von spezieller Software nur im Einzelfall und nach gründlicher Umfeldanalyse des Tatverdächtigen, kontrolliert und hochprofessionell. Ein flächendeckender Einsatz ist nicht das Ziel, insbesondere keine verdachtsunabhängige Online-Durchsuchung und keine Schleppnetzfahndung im Internet. 99,99% der Menschen in Deutschland werden davon niemals betroffen sein. Unerlässliche Voraussetzungen sind eine gesetzliche Eingriffsgrundlage, nur mit richterlicher Zustimmung und mit einer Software, die auch mit speziellen Suchbegriffen arbeitet, um den Kernbereich der Persönlichkeitsrechte zu schützen. Es ist auch vorstellbar, dass nur ein qualifizierter Richter die Ergebnisse der Online-Durchsuchung sichten darf. Er entscheidet dann, was für die Beweisführung verwendet werden darf und was nicht. Der Staatsanwalt überwacht die ausführende Polizei, der Datenschützer kontrolliert sie zusätzlich!

Meine Damen und Herren,

am 05.02.2007 entschied der Bundesgerichtshof, dass verdeckte Online-Durchsuchungen auf der Grundlage der derzeitigen rechtlichen Lage unzulässig seien. Der BGH sagte damit aber nicht, dass eine Online-Durchsuchung verfassungsrechtlichen Bedenken begegnet.

Wir benötigen möglichst bald eine neue, spezielle Rechtsgrundlage. Auf das Instrument der Online-Durchsuchung können wir angesichts der dynamischen Entwicklungen beim Kommunikationsverhalten der Täter bereits jetzt und in Zukunft nicht verzichten. Niemand sollte die Wirkungen der Internetkriminalität unterschätzen. Wir wollen den Menschen das Vertrauen in e-Commerce und e-Banking erhalten und es stärken.

Meine Damen und Herren,

die nachhaltige Bekämpfung des internationalen islamistischen Terrorismus setzt voraus, möglichst umfangreiche Kenntnisse auch über dessen Ursachen zu erlangen: Das Verstehen ist Grundlage für das Handeln; wissen, warum jemand zum islamistischen Extremisten oder Terroristen wird und welche Aspekte für solche Entwicklungen maßgeblich sind.

Zur Ursachenforschung in den Bereichen Extremismus und Terrorismus haben wir vor drei Jahren die Forschungsstelle Terrorismus / Extremismus (FTE) eingerichtet. Sie hat sich zum Ziel gesetzt, die Grundlagen und Entwicklungsströmungen im Phänomenbereich Terrorismus/Extremismus zu erforschen. Das hier verfolgte Konzept lässt sich mit dem Schlagwort: „Der Zukunft auf der Spur“ am besten beschreiben. Auf der Grundlage fundierter Ursachenanalysen soll ein phänomenadäquates Monitoringsystem auf den Weg gebracht werden, um künftige Entwicklungen im Bereich des Terrorismus zu antizipieren. Dabei geht es nicht um die Vorhersehbarkeit konkreter Straftaten oder Anschläge, sondern um die Beobachtung allgemeiner Entwicklungen. Erst wenn wir das soziale Umfeld, die Täter und ihre Ideologie genau betrachten, lassen sich Entwicklungen voraussagen und möglicherweise verhindern. Dies wird auch ein Thema der deutschen EU-Ratspräsidentschaft sein.

Meine sehr verehrten Damen und Herren,

nach meiner Überzeugung muss Kriminalitätsbekämpfung – viel intensiver als bisher – als gesamtgesellschaftliche Aufgabe begriffen werden. Das gilt im besonderen Maße für die Bekämpfung des islamistischen Extremismus.

In diesem Kontext steht auch der Dialog der Sicherheitsbehörden mit muslimischen Verbänden in Deutschland. Dessen Ziel ist es, extremistische Bestrebungen und Gefährdungen möglichst frühzeitig aufzudecken und dagegen vorzugehen. Dafür muss zunächst Vertrauen zwischen den Dialogpartnern aufgebaut werden. In diesem Sinne wurden konkrete vertrauensbildende Maßnahmen zwischen den Sicherheitsbehörden und den beiden islamischen Verbänden DITIB und ZMD vereinbart. Diese umfassen die Benennung fester "Ansprechpartner zur Förderung des Vertrauens" und die Organisation und Durchführung von regionalen Vortrags- und Informationsveranstaltungen. Letztere sollen einen unmittelbaren Dialog zwischen interessierten Muslimen und Mitarbeitern der Sicherheitsbehörden über ihre jeweiligen Anliegen ermöglichen. Hervorzuheben ist in diesem Zusammenhang, dass die Diskussion um den Gewaltbegriff bzw. eine Rechtfertigung von Gewalt in bestimmten Situationen in die Vereinbarung mündete, dass Imame und Gemeindevorsitzende beider Dachverbände weiterhin deutlich Stellung gegen die Anwendung von Gewalt und die Zerstörung jeglichen Lebens beziehen. Verantwortung ist nicht teilbar! Alle, die friedlich in Deutschland leben wollen, müssen sich dieser Verantwortung stellen.

Meine sehr verehrten Damen und Herren,

zum Schluss möchte ich noch einmal betonen, dass wir das Wissen und die Handlungsoptionen der Sicherheitsbehörden auf eine breite Basis stellen müssen. Die Bekämpfung des internationalen Terrorismus erfordert die Bündelung aller gesellschaftlichen Kräfte. Wir verfolgen einen ganzheitlichen Ansatz und gehen davon aus, dass der Kampf gegen Extremismus und Terrorismus nach Möglichkeit im Vorfeld möglicher Straftaten zu führen ist und daher nicht allein Aufgabe der Polizeibehörden sein kann.