Schöne neue Welt? Visionen einer vernetzten Zukunft

Von Professor Dr. Peter Glotz, Direktor am Institut für Medien- und Kommunikationsmanagement der Universität St. Gallen

Kurzstatement zum Vortrag vor dem Bundeskriminalamt
am 2. Dezember 2003 in Wiesbaden

Kein Zweifel, es entsteht eine neue Welt. Aber wie entkommt man den korrupten Hochrechnungen, mit denen die Public-Relations-Agenten der börsennotierten Unternehmen die Welt verrückt machen wollen? Zwischen 1995 und 2000 entstanden eine ganze Reihe von Start-up-Unternehmen, die plötzlich einen höheren Börsenwert hatten als einige der grössten Airlines der Welt. Wer mit Ankündigungen Millionen gemacht hat, wird bei seinen Zukunftsprognosen nicht zu skrupulöser Genauigkeit neigen. Realismus ist in dieser Atmosphäre eine Sünde; schlimmer: eine Dummheit. Ich habe schon 1999 geschrieben: "Deswegen sind viele schwungvolle Bilder der Online-Gesellschaft des 21. Jahrhunderts übertrieben, verlogen, falsch."

Das gilt sowohl für die positiven wie die negativen Utopien, sowohl für den süsslieben wie für den sauren Kitsch. Wie arbeitet man sich aus dem mausgrauen Heer der Empiriker und Spezialisten heraus? Durch eleganten Radikalismus oder tragische Dunkelheit. Daraus entstehen dann Visionen vom "gläsernen Menschen" oder vom "smart home", in dem 50 Videokameras installiert sind. Beide Visionen einer vernetzten Zukunft sind falsch.

Informations- und Kommunikationskriminalität
Lage, Bedrohungsszenarien und Handlungsbedarf

Max-Peter Ratzel, Abteilungsleiter Organisierte und Allgemeine Kriminalität (OA) im BKA

Globale Vernetzung und Kommunikation mittels digitaler Daten wie die elektronische Verbreitung von Informationen sind heute essentieller Bestandteil aller Bereiche des öffentlichen und privaten Lebens. Die Vorteile dieser Entwicklung für alle Gesellschaften sind unbestritten. Naturgemäß nutzen aber auch Straftäter die Möglichkeiten der Nutzung von Informations- und Kommunikationstechnik zur Begehung von Straftaten. Verbrechen können schneller oder geschickter begangen und besser camoufliert werden. Darüber hinaus stellen die weltweiten Datennetze - insbesondere für politisch motivierte Täter - Angriffsziele mit enormem Schadenspotenzial dar.

In der IuK-Kriminalität sind aktuell zwei gegenläufige Entwicklungen erkennbar. Einerseits ist nach Jahren kontinuierlich steigender Zahlen im Jahr 2002 erstmals eine insgesamt rückläufige Tendenz zu verzeichnen. Dem gegenüber steht aber ein Anstieg des Fallaufkommens um mehr als 50% bei einzelnen IuK-Delikten mit einer besonderen Qualität.

Das Bundeskriminalamt nimmt in der Bekämpfung der IuK-Kriminalität präventive wie auch repressive Aufgaben wahr.

So ist das Bundeskriminalamt für die Strafverfolgung in Fällen der Computersabotage zuständig, wenn sie sich gegen "kritische Infrastrukturen" richtet. Daneben wertet das Bundeskriminalamt als Zentralstelle relevante Informationen zur IuK-Kriminalität aus und stellt die Ergebnisse den Polizeien des Bundes und der Länder zur Verfügung.

Im übrigen tauscht das BKA solche Erkenntnisse auch mit den Zentralstellen anderer Staaten sowie im Rahmen multilateraler Arbeitsgremien aus.

Das BKA unternimmt große Anstrengungen, um die Strafverfolgung von Hackingangriffen zu gewährleisten, sei es bei der Sicherung und Auswertung von beschlagnahmten Datenträgern, sei es bei der Beschaffung notwendiger Informationen im In- und Ausland oder in eigenen Ermittlungsverfahren. Das BKA bemüht sich insbesondere um eine effektive Fallbearbeitung auf dem Gebiet „Hacking kritischer Infrastrukturen".
Ein neuer Schwerpunkt in der Wahrnehmung der Zentralstellenfunktion des BKA ist die Bekämpfung der missbräuchlichen Verwendung von Telekommunikations-Anlagen. Diese Art des Computerbetruges wird als "Phreaking" (Phone break in) bezeichnet. Dahinter verbirgt sich ein modus operandi, bei dem Personen unberechtigt auf Telefonanlagen von Firmen zugreifen und durch intensive Nutzung, z.B. von Überseeverbindungen, hohe Kosten verursachen. Auch der missbräuchlichen Verwendung von 0190er Dialerprogrammen gebührt eine besondere Beachtung.

Neben diesen Phänomenen, die im Wesentlichen nur zu materiellen Schäden führen, gibt es aber weitaus bedrohlichere Szenarien, bei denen ein Angriff auf die Verfügbarkeit und Performanz des Internet selbst durchgeführt wird.
Beispiele zeigen, welche Gefahrenpotenziale für kritische Infrastrukturen bei destruktiven Angriffen bis hin zum möglichen "Cyberterrorismus" bestehen.
Es wird nachvollziehbar, welche Schäden entstehen können, auf der anderen Seite wird aber auch deutlich, dass nach wie vor eine vermeidbare Leichtfertigkeit im Umgang mit IuK-Systemen weit verbreitet ist.
Präventive Maßnahmen zur Steigerung des Sicherheitsbewusstseins sind daher eine wesentliche Option zur Gefahrenminimierung.
Die Strafverfolgungsbehörden müssen neben den notwendigen Maßnahmen im nationalen Bereich - Organisation, Aus- und Fortbildung, Rechtsfortentwicklung und Ausstattung mit ausreichenden und modernen Ressourcen - vor allem die Zusammenarbeit im internationalen Bereich betrachten.
Das BKA ist mit der Einrichtung des Technischen Servicezentrums Informations- und Kommunikationstechnologien (TeSIT) zum Jahresbeginn 2002 in Vorleistung getreten.
Die Anforderungen an Polizei und Justiz zur kompetenten Bekämpfung der IuK-Kriminalität müssen aber schon in der Aus- und Fortbildung ansetzen. Die Umsetzung des polizeilichen Konzeptes zur angemessenen Aus- und Fortbildung im Bereich IuK wird weiter forciert.
Der Bedarf an einem schnellen und gut funktionierenden internationalen Informationsaustausch erfordert neue Wege. Die Einrichtung der so genannten High Tech Points of Contact im Rahmen eines 24/7-Netzwerkes sind erste positive Schritte in dieser Richtung.

Große Probleme bereitet die Flüchtigkeit von Daten. Die aktuelle Rechtslage lässt nur ein zeitlich begrenztes Vorrätighalten der Daten zu Zwecken der Rechnungsstellung zu. Die polizeiliche Praxis zeigt aber, dass Verdachtsmomente in Hinblick auf IuK-Straftaten erst mit zeitlicher Verzögerung bekannt oder ermittelt werden.

Einziger erfolgversprechender Ermittlungsansatz zur Ermittlung der Verantwortlichen sind die bei den Providern gespeicherten Daten. Daher ist die Wichtigkeit der Einführung von angemessenen Mindestspeicherfristen zu betonen.

Darüber hinaus müssen alle gesellschaftlichen Kräfte für ein Umdenken im Umgang mit der noch jungen Technik sorgen. Bei allen Bürgern muss ein Unrechtsbewusstsein auch bei bestimmten Formen der Nutzung des Internet, wie z.B. dem Herunterladen von Software, Musik- und Filmtiteln, geweckt werden.

Ebenso müssen wir schon bei der Entwicklung wie beim Betreiben von IT-Systemen standardmäßig Schutzmechanismen vorsehen, um uns vor kriminellen Angriffen zu schützen. Firewalls und Virenschutzprogramme sollten auf jedem PC installiert sein und regelmäßig aktualisiert werden. Dazu sind verstärkte Zusammenarbeitsformen zwischen Industrie, Handel und Strafverfolgungsbehörden notwendig, um dem Aspekt der Datensicherheit einen höheren Stellenwert zu verschaffen.

Deshalb sollten im Rahmen von public-private-partnerships öffentliche und private Organisationen und Institutionen Lösungsstrategien entwickeln und anbieten.

Es bedarf besonderer, aber auch besonnener, Aktivitäten der Strafverfolgungsbehörden, um permanent auch auf die Risiken hinzuweisen. Nicht die Verteufelung der IuK-Technologien ist angesagt, sondern eine rationale und soweit möglich auf empirisch belegbaren Daten entwickelten Kriminalpolitik, die den Gefahrenpotenzialen der neuen Technologien angemessene Grenzen setzt.

Belange der IT-Sicherheit brauchen einen höheren Stellenwert. Sie sind daher bereits in der Planung zu berücksichtigen. Angriffe oder Schäden durch Missbrauch der IuK-Technologie müssen offensiv den Strafverfolgungsbehörden mitgeteilt werden.

Gemeinsame Anstrengungen aller Beteiligten oder Betroffenen sind der beste Weg im Umgang mit den Chancen und Risiken der "schönen neuen Welt".

Max-Peter Ratzel

„E-Commerce – eine erste Bewertung"

Jörg Rheinboldt, Geschäftsführer Sicherheit und Vertrauen, eBay GmbH

Die Möglichkeiten des Internets, einerseits unabhängig von Zeit und Ort jederzeit mit Menschen in der ganzen Welt zu kommunizieren und andererseits völlig neue Absatz- und Beschaffungsmärkte zu erschließen, haben dazu geführt, dass sich Online-Marktplätze wie eBay etablieren konnten. Mittlerweile kaufen und verkaufen weltweit über 75 Millionen registrierte Nutzer bei eBay Waren und Dienstleistungen. In der ersten Hälfte des Jahres 2003 wurden bei eBay weltweit Waren und Dienstleistungen im Wert von 10,95 Mrd. US-Dollar gehandelt. eBay ist mittlerweile in 27 internationalen Märkten präsent.

Anders als bei traditionellen Handelsformen, bei denen sich i.d.R. die Marktbeteiligten physisch begegnen, finden Transaktionen bei eBay auf einem virtuellen Marktplatz statt. Das Vertrauen seiner Mitglieder in die Sicherheit der Plattform ist für einen Marktplatz wie eBay daher von fundamentaler Bedeutung. Dies betrifft nicht nur die infrastrukturelle Systemsicherheit im technischen Sinne, die der Marktplatzbetreiber sicherzustellen hat, sondern auch und insbesondere die Sicherheit, dass die Transaktionen zwischen Käufer und Verkäufer strukturiert und nach bestimmten Regeln erfolgen. Viele der im Offline-Handel erlernten Handlungsmuster, wie z.B. das Vertrauen der Verbraucher in die Präsenz und Qualität der Einzel-, Fach- und Großhändler vor Ort, müssen für die Online-Welt in veränderter Form neu „erlernt" werden. Als Marktplatzbetreiber sieht eBay es als seine Verpflichtung an, diese Handelskompetenz jedes Einzelnen zu ermöglichen und zu fördern.

eBay bietet dazu eine Vielzahl von Sicherheitsleistungen an, die es jedem eBay-Nutzer ermöglichen, sicher auf dem Online-Marktplatz zu handeln. Dazu gehören z.B. die Verifizierung der Anmeldeinformationen, die eBay in Kooperation mit der Schufa durchführt, die Möglichkeit, sich über das Post-Ident-Verfahren als „geprüftes Mitglied" registrieren zu las-

sen, das Bewertungsforum, in dem sich Käufer und Verkäufer gegenseitig nach erfolgter Transaktion bewerten und Treuhanddienste zur sicheren Abwicklung des Kaufvertrages. Wie sicher der Handel letztlich abläuft, hängt allerdings nicht nur von den von eBay angebotenen Sicherheitsleistungen ab. Entscheidend ist, dass jeder Einzelne eigenverantwortlich dazu beiträgt, den Umgang mit diesen Leistungen zu beherrschen und sie in Anspruch zu nehmen um damit seinen Beitrag für die Sicherheit im Online-Handel zu leisten.

Zusätzlich zu den angebotenen Services und Funktionen für die eBay-Nutzer übernimmt eBay eine aktive Rolle bei der Bereitstellung des sicheren Marktplatzes: Durch die Zusammenarbeit mit Behörden und Organisationen werden permanent die Regeln zum Handel bei eBay verbessert und die Mitglieder darüber aufgeklärt, was sie wie handeln können. Mitarbeiter von eBay gehen Hinweisen nach, überprüfen stichprobenartig die angebotenen Artikel und entfernen diese vom Marktplatz, sobald sie Kenntnis von Missbrauch erlangen. eBay arbeitet seit langem weltweit erfolgreich mit Ermittlungsbehörden zusammen, um Missbrauch des Marktplatzes zu verfolgen.

Jörg Rheinboldt

Bekämpfung der High-Tech-Kriminalität im Vereinigten Königreich

DCS Len Hynds, Leiter National Hi-Tech Crime Unit

Die National Hi-Tech Crime Unit wurde 2001 zur Bekämpfung der nationalen und transnationalen organisierten High-Tech-Kriminalität ins Leben gerufen.

In Zusammenarbeit mit Regierung, Wirtschaft und weiteren Strafverfolgungsbehörden bekämpft die National Hi-Tech Crime Unit die Internetkriminalität wie bspw. Viren und Hakking, Erpressung, Kindesmissbrauch über das Internet und illegalen Handel mit harten Drogen.

Tatsache ist, dass Kriminalität in allen Bereichen menschlichen Handelns entsteht. Da sich der Cyberspace als neues Kommunikationsmedium etabliert hat, treten dort nun auch kriminelle Aktivitäten auf. Dies erfordert Polizeiarbeit, und wie alle Arten der Polizeiarbeit in einer demokratischen Gesellschaft muss diese alle Beteiligten einbinden.

Was ist also über die Gefährdung bekannt? Auch im Cyberspace existiert dieselbe Vielfalt an Delikten wie in der realen Welt. Genau betrachtet ist die Komplexität und häufig unbestimmte Art des Phänomens nur eine der Facetten, die es anzugehen gilt.

Daher ist klar, dass Internetkriminalität ein globales Problem darstellt und als solches eine globale Lösung erfordert.

Die High-Tech-Kriminalität ist getrennt von der Kriminalität der realen Welt zu sehen. Wir versuchen oft, Kriminalität einzuteilen in "alte oder traditionelle Straftaten", die heute über ein neues Medium und durch den Einsatz neuer Hilfsmittel begangen werden, einerseits und

durch die neuen Medien auftretende neue Straftaten, wie Hacking, Cracking und das Programmieren von Viren, andererseits. Im Wesentlichen ist jedoch nur das Medium ein anderes, stellt das Medium die Herausforderung dar, ist das Medium daher der Faktor, an den wir uns bei der Entwicklung von Strategien zur Bekämpfung der Cyberkriminalität anpassen müssen.

Die Strafverfolgung hat der Wirtschaft viel zu bieten. Die Beziehung zwischen Strafverfolgungsbehörden und Wirtschaft muss für beide Seiten von Nutzen sein. Erkenntnisse, die von Unternehmen erlangt werden, müssen unter Berücksichtigung der verschiedenen Wirtschaftszweige und weiterer Erkenntnisquellen analysiert, zusammengeführt und verglichen werden. Tendenzen werden vor dem Hintergrund von Umweltanalysen dargestellt und betrachtet, um eine Gefährdungsbewertung zu erhalten, die für die Wirtschaft einen effektiven Nutzen darstellt. Dieser Nutzen ist natürlich, dass die Gefährdungsanalyse dem Risikomanagement eine weitere Dimension eröffnet – eine vollkommen unabhängige und alternative Sicht auf die Welt.

In ähnlicher Weise wollen wir vorausschauend fundiert und kompetent beraten und die Weitergabe von bewährten Verfahrensweisen fördern. Der virtuelle Markt befindet sich noch im Aufbau, und Strafverfolgung kann und muss dabei eine Rolle spielen.
Die Strafverfolgungsbehörden müssen eine Plattform für den Erfahrungsaustausch zur Verfügung stellen; sie müssen außerdem jedes einzelne Unternehmen, das zur Gestaltung des virtuellen Marktes beiträgt, einbinden, damit einem Missbrauch für kriminelle Zwecke vorgebeugt wird.

Len Hynds

--

Kritische Infrastrukturen – Präventionsmaßnahmen aus Sicht des BSI

Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Bonn

Auf dem Weg ins Informationszeitalter entstehen durch den zunehmenden Einsatz von Informationstechnologien (IT) zwangsläufig neue Verwundbarkeiten und Abhängigkeiten. Wenn Staat, Wirtschaft und Gesellschaft sich bei der Erfüllung ihrer Aufgaben immer mehr in die Abhängigkeit von IT begeben, dann sind immer mehr Bereiche nur arbeitsfähig, wenn Informations- und Kommunikationstechnik (IuK) zuverlässig und sicher funktioniert. Technisches Versagen, menschliches Fehlverhalten, vorsätzliches Handeln (Sabotage) von Einzeltätern oder Tätergruppen sowie Naturereignisse können jederzeit zum Ausfall von Informations- und Kommunikationsinfrastrukturen und damit auch von Produktionsprozessen führen. Eine massive Beeinträchtigung von Staat, Wirtschaft und Gesellschaft kann die Folge sein - auch über den ursprünglich betroffenen Staat hinaus.

Mit dem BSI-Programm „Schutz Kritischer Infrastrukturen" (KRITIS) wird dieses neue Problemfeld analysiert. Es werden praktikable und bezahlbare Lösungsmöglichkeiten aufgezeigt. KRITIS ist mehr als rein technische IT-Sicherheit. Die Aufgabe bezieht nicht nur die technikorientierte Sichtweise ein, sondern beleuchtet gesamtstaatliche und gesamtgesellschaftliche Risiken und bezieht ein allgemeines staatenübergreifendes Sicherheitsverständnis mit ein.

Betroffen von diesen neuen IuK-Abhängigkeiten und den daraus resultierenden Gefährdungen ist nicht nur die Wirtschaft. Auch behördliche Dienstleister wie BOS (Behörden und Organisationen mit Sicherheitsaufgaben) sind insbesondere in Gefahren- und Katastrophenlagen auf das reibungslose Funktionieren ihrer IuK angewiesen. Gerade in diesen Situationen sind Einschränkungen der Leistungsfähigkeit der IuK zumindest denkbar, wenn nicht sogar wahrscheinlich.

Wir müssen uns auf solche besonderen Lagen vorbereiten – und zwar auf drei Ebenen:

- Die Technik muss mit angemessenen und aktuellen Schutzmaßnahmen versehen sein, ggf. sind auch Redundanzen vorzuhalten.
- Die Mitarbeiter sollten geschult sein, sowohl um durch besonnenes Handeln Vorfälle und Schäden zu vermeiden, aber auch um im Fall des Falles richtig reagieren zu können.
- Durch geeignete Organisationsformen kann sichergestellt werden, dass Ausfälle der IuK weniger wahrscheinlich werden, im Falle des Ausfalles aber auch zügig und koordiniert der Normalbetrieb wiederhergestellt werden kann.

Das BSI bietet eine Vielzahl von Kompetenzen und Hilfestellungen für Maßnahmen auf allen oben angesprochenen Ebenen an. Hierzu zählen u.a. das CERT-Bund, das IT-Penetrationszentrum, die IT-Sicherheitsberatung und das IT-Grundschutzhandbuch sowie die Bereiche Abhörsicherheit, Kryptographie und Internetsicherheit.

Dr. Udo Helmbrecht

E-Commerce, eine erste Bewertung

Helke Heidemann-Peuser; Referatsleiterin Wirtschaftsrecht im Bundesverband der Verbraucherzentralen und Verbraucherverbände, Verbraucherzentrale Bundesverband e.V.; Berlin

Durch den elektronischen Handel wurde in den letzten Jahren für Verbraucher eine völlig neue Einkaufsmöglichkeit eröffnet. Das Internet erlaubt – außerhalb jeglicher Ladenöffnungszeiten - den Zugang zu Dienstleistungs- und Warenangeboten weltweit. Bis dahin nicht bekannte Vertriebsformen, wie etwa die Internet-Auktion, sind entstanden. Bankgeschäfte können von zu Hause aus erledigt, ebenso können Reisen vom eigenen PC aus verbindlich gebucht werden. Die Verbraucher können dabei zum Teil von besonders günstigen Konditionen profitieren. Allerdings werfen die neuen Möglichkeiten des Konsums auch neue Sicherheits- und Rechtsfragen auf, deren Lösung Politik und Justiz vor schwierige Aufgaben stellt. In der Rechtsberatung der Verbraucherzentralen spielt E-Commerce bereits seit Jahren eine wichtige Rolle.

Gesetzliche Grundlagen

- Der europäische Gesetzgeber hat durch die Richtlinie 2000/31/EG über den elektronischen Rechtsverkehr vom 17.07.2000 (E-Commerce-Richtlinie) Vorgaben zum Vertragsabschluss gemacht. Die Richtlinie regelt im Wesentlichen Informationspflichten des Unternehmers sowie Modalitäten des Vertragsabschlusses. Sie wurde in Deutschland im Wesentlichen durch das Schuldrechtsmodernisierungsgesetz mit Wirkung vom 02. Januar 2002 umgesetzt.
- Ferner sind für Vertragsabschlüsse unter Verwendung von Fernkommunikationsmitteln die Vorschriften der Fernabsatzrichtlinie aus dem Jahr 1997, bei uns umgesetzt durch das seit dem 30.06.2000 geltende Fernabsatzgesetz, das durch die Schuldrechtsmodernisierung in das BGB integriert wurde.

- Zu erwähnen ist darüber hinaus das zur Umsetzung der E-Commerce-Richtlinie dienende Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14.12.2001, mit dem außer bei Verträgen mit Verbrauchern das Herkunftslandprinzip eingeführt wurde. Für Verbraucherverträge bleiben Artikel 29, 29a EGBGB maßgebend.

Rechtsanwendung und Kontrolle

Die gesetzlichen Vorgaben werden nicht in ausreichendem Maße eingehalten:

- Eine Untersuchung von über 500 Internetangeboten, die der vzbv in der Zeit von Oktober 2002 bis Februar 2003 durchgeführt hat, ergab, dass 71 Prozent der Internetangebote gegen die gesetzlichen Informationspflichten verstießen, lediglich 29 Prozent der Anbieterseiten waren nicht zu beanstanden. Die Verstöße zogen sich quer durch alle Branchen.

- Die Allgemeinen Geschäftsbedingungen der Anbieter im Internet halten zum Teil einer AGB-rechtlichen Inhaltskontrolle nicht stand. Ende des Jahre 2002 hat der vzbv in 20 Fällen Unterlassungsverfahren nach § 1 Unterlassungsklagengesetz (UklaG) i. V. m. §§ 307 bis 309 BGB eingeleitet.

Aktivitäten gegen Spamming

Ein besonderes Ärgernis aus der Sicht der Verbraucher stellen unverlangte Werbemails dar. TACD (Transatlantic Consumer Dialogue), ein Forum für 65 europäische und amerikanische Verbraucherorganisationen, führt zur Zeit eine Online-Befragung von Verbrauchern nach ihren Erfahrungen durch, deren Ergebnis im Februar 2004 der OECD sowie der internationalen Presse vorgestellt werden soll.

Die Datenschutzrichtlinie für elektronische Kommunikation vom 12. Juli 2002 schreibt vor, dass elektronische Post für die Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer gestattet werden darf. Die Richtlinie wird voraussichtlich im Frühjahr 2004 durch die Novelle des Gesetzes gegen den unlauteren Wettbewerb (UWG) umgesetzt werden.

Helke Heidemann-Peuser

**Der Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht**

LAND BRANDENBURG
LDA
Schutz der
- *Persönlichkeitsrechte*
- *Informationsfreiheit*

Dr. Alexander Dix

Thesen

zum Thema „Freiheit braucht Sicherheit – Sicherheit braucht Freiheit"

bei der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003
Informations- und Kommunikationskriminalität

1. Das Telekommunikationsgeheimnis ist das zentrale Menschenrecht (die „Grundfreiheit") in der Informationsgesellschaft. Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass die Nutzung von Kommunikationsmedien „in allem" (also sowohl hinsichtlich des Inhalts als auch hinsichtlich der Umstände) vertraulich möglich sein soll. Auf diese Weise sollen die Bedingungen einer freien Telekommunikation überhaupt aufrecht erhalten werden.

2. Wie das Grundrecht auf Datenschutz schützt auch das Telekommunikationsgeheimnis nicht lediglich ein Individualinteresse, sondern zugleich das Gemeinwohl. Jede heimliche Überwachung des Fernmeldeverkehrs betrifft die Kommunikation der Gesellschaft insgesamt und gefährdet ihre Qualität (so zuletzt BVerfG, Urteil vom 12.3.1003, NJW 2003, 1787, 1793). Diese Feststellung hat auch angesichts der Bedrohung durch den internationalen Terrorismus nichts von ihrer Berechtigung verloren.

3. Die Freiheit der vertraulichen Telekommunikation gilt allerdings nicht uneingeschränkt. Einschränkungen sind zulässig, wenn sie dem legitimen öffentlichen Zweck der Aufklärung und Verfolgung schwerer Straftaten dienen, wobei die Liste dieser schweren Straftaten ständig wächst und bisher noch keiner kritischen Überprüfung unterzogen worden ist. Außerdem sind Einschränkungen des Telekommunikationsgeheimnisses nicht schon dann verfassungskonform, wenn sie allgemein der Strafverfolgung dienen. Vielmehr muss ein konkreter Tatverdacht für eine Straftat von erheblicher Bedeutung vorliegen und es müssen hinreichend sichere Tatsachen für die Annahme sprechen, dass die überwachte Person, wenn sie nicht mit dem Beschuldigten identisch ist, für ihn als Nachrichtenmittler auftritt.

4. Aus dieser Aussage des Bundesverfassungsgerichts ergibt sich zwingend, dass eine anlassunabhängige, verdachtslose Überwachung des Telekommunikationsverkehrs auf Vorrat (sog. Verdachtsgewinnungseingriff) verfassungswidrig ist. Das gilt auch für den jüngsten Vorschlag des Rechtsausschusses des Bundesrates zum Entwurf des Telekommunikationsgesetzes, nach dem Provider zur Speicherung aller Verkehrsdaten für ein halbes Jahr verpflichtet werden sollen. Bereits die Speicherung der Daten über den für die Rechnungslegung erforderlichen Zeitraum hinaus ist ein unverhältnismäßiger Eingriff in das Telekommunikationsgeheimnis.

5. Immer mehr Lebensäußerungen finden in Telekommunikationsnetzen statt. Diese Entwicklung wird durch „ubiquitous computing" bzw. „ambient intelligence" noch erheblich zunehmen. Dies erfordert eine Neubestimmung der Balance zwischen Freiheit (Schutz der Privatsphäre) und Sicherheit. Dabei wird zunehmend deutlich, dass dem Schutz der Privatsphäre und dem Recht auf vertrauliche Kommunikation wieder mehr Bedeutung zukommen wird.

6. Telekommunikationsnetze sind keine rechtsfreien Räume. Deshalb muss Kriminalitätsbekämpfung auch in weltweiten Netzen möglich sein. Sie muss sich aber strikt am Grundsatz der Verhältnismäßigkeit orientieren. Eine flächendeckende Überwachung aller Bewegungen und Lebensäußerungen scheidet von Verfassungs wegen selbst dann aus, wenn sie technisch möglich sein/werden sollte. Kommunikationsnetze würden ihren Charakter grundlegend negativ verändern, wenn sie zu Plattformen der Verdachtsschöpfung würden.

7. Die Ergebnisse der parallelen Untersuchungen des Max-Planck-Instituts für internationales Strafrecht und der Universität Bielefeld zwingen zu Veränderungen im System der staatlichen Kommunikationsüberwachung. Die Steigerung der Zahl der Ermittlungsverfahren, in denen eine Telekommunikationsüberwachung angeordnet worden ist, zwischen 1990 und 2000 um das Sechsfache kann nicht allein mit dem Wachstum der Mobilkommunikation erklärt werden. Die Telekommunikationsüberwachung wird immer mehr zur standardmäßigen Ermittlungsmaßnahme („prima ratio" statt „ultima ratio"). Nur in 17% der Fälle brachte die Überwachungsmaßnahme einen Ermittlungserfolg, der sich direkt auf den die Telefonüberwachung begründenden Verdacht bezog. 73% der betroffenen Anschlussinhaberinnen und –inhaber wurden nicht über die Maßnahme unterrichtet.

8. Eine Revision der Telekommunikationsüberwachung sollte deshalb folgende Punkte berücksichtigen:

- die Transparenz muss erhöht und die wissenschaftliche Evaluation muss fortgeführt und erweitert werden; der Gesetzgeber sollte die gesetzlichen Regelungen den Ergebnissen der Evaluation anpassen;

- der Richtervorbehalt darf nicht gelockert, sondern er muss im Gegenteil gestärkt werden;

- die Ergebnisse von Eilanordnungen der StA dürfen nur nach richterlicher Überprüfung verwertet werden;

- die Qualität der richterlichen Entscheidungen sollte verbessert werden, indem erhebliche Begründungsmängel zu Beweisverwertungsverboten führen;

- die Aufgaben der Ermittlungsrichter sollten auf wenige Personen konzentriert werden;

- der Straftatenkatalog des § 100a StPO ist kritisch zu überprüfen und gegebenenfalls zu reduzieren;

- die Pflicht zur Benachrichtigung aller bekannten Gesprächsteilnehmer ist zu präzisieren und abzusichern; die Benachrichtigung sollte längerfristig nur mit richterlicher Zustimmung zurückgestellt werden dürfen;

- abgehörte Gespräche zwischen Beschuldigten und Zeugnisverweigerungsberechtigten sollten grundsätzlich nicht verwertet werden dürfen;

- Daten aus Telekommunikationsüberwachungsmaßnahmen müssen gekennzeichnet werden;

- die Höchstdauer der Telekommunikationsüberwachung sollte auf zwei Monate reduziert werden;

- PINs und PUKs unterliegen dem Telekommunikationsgeheimnis, auf sie darf deshalb nur unter den gleichen Voraussetzungen zugegriffen werden wie auf Gesprächsinhalte;

- eine Zwangsidentifizierung beim Erwerb von prepaid-Handys ist abzulehnen.

9. Für die Schaffung präventiv-polizeilicher Befugnisse zur Telekommunikationsüberwachung (geltendes Recht bereits in Thüringen, Gesetzentwürfe in Rheinland-Pfalz, Niedersachsen und Bayern) ist ein Bedarf bisher nicht überzeugend dargelegt worden. Dadurch würde zudem der Anfangsverdacht als Eingriffsvoraussetzung aufgegeben und die Befugnis zu derart schweren Grundrechtseingriffen noch weiter in das Vorfeld verlagert, ohne dass ein Richtervorbehalt angesichts der verwendeten Blankettbegriffe für eine effektive Kontrolle sorgen könnte.

10. Eine routinemäßige, verdachtsunabhängige Speicherung sämtlicher Verkehrsdaten, um eine mögliche Strafverfolgung in der Zukunft zu erleichtern, wäre nicht nur verfassungswidrig (s.o. These 4), sondern sie wäre auch unvereinbar mit der Europäischen Menschenrechtskonvention (Art. 8). Danach setzen Einschränkungen des Rechts auf Privatsphäre und des Telekommunikationsgeheimnisses ein „zwingendes gesellschaftliches Bedürfnis" voraus und müssen verhältnismäßig sein. Die abstrakte Möglichkeit, dass der Zugriff auf massenhaft gespeicherte Verkehrsdaten in der Zukunft die Strafverfolgung erleichtern könnte, reicht dafür nicht aus. Denkbar wäre dagegen ein anlassbezogenes Einfrieren vorhandener Verkehrsdaten im Einzelfall bis zu einer richterlichen Entscheidung über die Verwertung nach dem Prinzip „fast freeze – quick thaw", wie es auch die Cybercrime-Konvention vorsieht.

11. Angriffe auf Netze, Infrastrukturen und Computer (Computer-Kriminalität) können und müssen sehr viel effektiver als bisher durch eine Erhöhung der Technik-Sicherheit (Produkte, Verfahren) abgewehrt oder erschwert werden. Dazu unternimmt die Europäische Union verstärkte Anstrengungen (Gründung einer Europäischen Agentur für Netzsicherheit).

12. In einem freiheitlichen Rechtsstaat muss der Schutz der Grundrechte, also auch des Rechts auf vertrauliche Kommunikation die Regel und ihre Einschränkung die begründungsbedürftige Ausnahme im Einzelfall bleiben. Der Staat darf nicht allein die Tatsache, dass jemand Kommunikationsnetze nutzt, zum Anlass dafür nehmen, seine Bewegungen und Äußerungen umfassend zu registrieren, und so jeden, der – aus legitimen Gründen - unbeobachtet kommunizieren will, zur Technikabstinenz zwingen. Der Verlust an Freiheit wäre zugleich ein Verlust an Sicherheit.

Zur Zusammenarbeit der Strafverfolgung mit Service-Providern

Thomas Königshofen, Deutsche Telekom, Bonn

Die effiziente Verbrechensbekämpfung und die Verfolgung und Überführung von Straftätern ist eine Aufgabe des Staates im Interesse des Schutzes seiner Bürger. Deswegen ist es im Grundsatz selbstverständlich, dass die Unternehmen, die Dienstleistungen im Telekommunikations- und Multimediabereich anbieten (Service-Provider), die Strafverfolgungsbehörden bei diesem Ziel unterstützen. Diese grundsätzliche Bereitschaft zur Zusammenarbeit hat aber auch genauso selbstverständlich ihre Grenzen, wo gesetzliche Regelungen konkrete Formen der Zusammenarbeit im Interesse der Freiheits- und Persönlichkeitsrechte der Bürger untersagen.

In der Praxis spielt dies insbesondere dort eine Rolle, wo die Service-Provider Informationen über ihre Kunden auf Grund ihrer vertraglichen Beziehung zu diesen Kunden vorhalten bzw. beschaffen könnten, weil die Beschaffung dieser Informationen bzw. ihre Bekanntgabe an Dritte (auch an Strafverfolgungsbehörden) datenschutzrechtlichen Grenzen unterliegt. So verlangen das die Service-Provider verpflichtende Telekommunikationsgeheimnis (Fernmeldegeheimnis) nach § 85 des Telekommunikationsgesetzes (TKG) und die einschlägigen Datenschutzgesetze (Bundesdatenschutzgesetz, Teledienstedatenschutzgesetz, Telekommunikationsgesetz und Telekommunikations-Datenschutz-verordnung) sowohl für die Beschaffung von Daten (Erhebung) als auch für deren Weitergabe an Dritte (Übermittlung) entweder das Einverständnis der Betroffenen, also der Personen, auf die sich diese Daten beziehen, oder aber eine gesetzliche Grundlage.

Die wichtigste gesetzliche Grundlage für die im Interesse der Strafverfolgungsbehörden durchzuführende Informationsbeschaffung mit Hilfe der Service-Provider findet sich im § 100a Strafprozessordnung, auf dessen Basis die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung angeordnet werden kann. Dem korrespondiert § 88 des Telekommunikationsgesetzes, der die Service-Provider generell verpflichtet, den Strafverfolgungsbehörden die für die Telekommunikationsüberwachung erforderlichen Netzzugänge zur Verfügung zu stellen. Die Vorschriften der §§ 100g und h der Strafprozessordnung und § 89 Abs. 6 des Telekommunikationsgesetzes regeln die wesentlichen gesetzlichen Pflichten der Service-Provider zur Übermittlung von Kundendaten an die Strafverfolgungsbehörden.

Mit diesen grundsätzlichen gesetzlichen Pflichten sind aber auch die gesetzlichen Voraussetzungen beschrieben, die erfüllt sein müssen, damit die Service-Provider überhaupt in rechtlich zulässiger Weise die Informationen über ihre Kunden beschaffen bzw. weitergeben dürfen. Die genaue Auslegung dieser Voraussetzungen war und ist häufig rechtlich umstritten, was sich dann auch auf die Praxis der Zusammenarbeit der Service-Provider mit den Strafverfolgungsbehörden niederschlägt. Im Referat werden diese Konfliktfelder an Hand von Beispielen aus der Praxis näher erläutert.

Ein weiteres Konfliktfeld ergibt sich daraus, dass die Zuarbeit für die Strafverfolgungsbehörden organisatorische, personelle und sachliche Mittel erfordert, die nach den derzeitigen gesetzlichen Bestimmungen bzw. nach der herrschenden Auslegung der einschlägigen Bestimmungen durch die Gerichte auch nicht annähernd durch einen Kostenersatz von Seiten staatlicher Stellen ausgeglichen wird. Auch hierauf wird im Referat mit Hilfe von konkreten Beispielen näher eingegangen. Insofern gilt es, mit gegenseitigem Respekt und Verständnis für die jeweilige Interessenlage zu tragbaren und verhältnismäßigen Lösungen zu kommen, die eine effektive Strafverfolgung ermöglichen, ohne die betrieblichen und wirtschaftlichen Belange der Service-Provider zu vernachlässigen. Insoweit bietet sich ein stärkerer regelmäßiger Informationsaustausch und Dialog an, zu dem sich die Deutsche Telekom mehrfach bereit erklärt hat.

Thomas Königshofen

Streitgespräch: „Rechtsfreie Räume zulassen – die Anarchie im Netz akzeptieren

Franz-Hellmut Schürholz, Präsident des Landeskriminalamt Baden-Württemberg, Stuttgart

Eine Bestandsaufnahme der aktuellen Kriminalitätslage zeigt, dass das Internet zunehmend von Straftätern zur Tatausführung benutzt wird. Dabei handelt es sich um Verfahren in den verschiedensten Deliktsgruppen. Die Straftaten erstrecken sich von Urheberrechtsverletzungen über Betrugsstraftaten bis hin zum Extremismus und der Verbreitung kinderpornografischer Schriften. Während in Baden-Württemberg im Jahr 2001 noch 2.724 Straftaten verübt wurden, bei denen das Internet als Tatmittel eingesetzt wurde, so waren es im Jahr 2002 bereits 4.321 Straftaten. Dies entspricht einem Anstieg von rund 60 Prozent. Mit der erweiterten und vermehrten Nutzung des Internets steigt auch die Vielfalt der begangenen Taten und der modi operandi der Täter. So sind im vergangen Jahr die Delikte des Warenbetruges vermehrt mit Hilfe so genannter Auktionsplattformen im Internet begangen worden. Erfahrungen aus den einzelnen Ermittlungsverfahren zeigen, dass nicht nur der Umfang sondern auch die Qualität der Straftaten zunimmt. Diese Dynamik verläuft analog zur ansteigenden Verbreitung des Internets in Deutschland.

Bei der Wandlung der Gesellschaft hin zur Informationsgesellschaft spielt das Internet eine zentrale Rolle. Es hat mittlerweile maßgeblichen Einfluss auf die Wirtschaft (E-Commerce, Kommunikation, Geldfluss), den Staat (eGovernment, IT-Infrastruktur, Kommunikation der Behörden, Internet als kriminogener Faktor), die Wissenschaft (Austausch von Informationen, Arbeitsteilung bei Projekten) und den einzelnen Bürger (Homebanking, Kommunikation, eCommerce). Die virtuelle Welt bildet fast alle Lebensbereiche der „realen" Welt ab und macht sie für jedermann nutzbar.

Vor dem Hintergrund einer immer noch zunehmenden Bedeutung der Datennetze für die Gesellschaft und den Einzelnen darf das Internet kein rechtsfreier Raum sein. Die Gesellschaft hat sich Regeln gegeben, die ein geordnetes Zusammenleben auf der Grundlage

eines Rechts- und Wertesystems ermöglichen. Dies bedeutet, dass der einzelne Bürger, die Unternehmen und die Allgemeinheit erwarten können, vor Rechtsverletzungen geschützt zu werden und ein Anrecht auf die Durchsetzung ihrer Individualrechte haben.

Der virtuelle Raum des Internets ist ein sozialer Raum wie andere auch. Und wie in den anderen sozialen Räumen beansprucht das Recht dort Geltung. Dass auch hier ein Spannungsfeld zwischen den Freiheitsrechten des Einzelnen und dem Strafverfolgungs-anspruch des Staates besteht, steht außer Frage. Es wäre jedoch nicht hinnehmbar, dass einem Bürger oder einem Unternehmen Rechtsschutz versagt bliebe, nur weil ein Kommunikations- oder Geschäftsprozess über das Internet abgewickelt wurde. Dem Rechtsgüterschutz muss also auch in Datennetzen zur Geltung verholfen werden. Dabei soll nicht, wie vielfach behauptet, der virtuelle Überwachungsstaat geschaffen werden. Es geht nur darum, Mechanismen zu implementieren, die eine Durchsetzung des geltenden Rechts im virtuellen Raum ermöglichen. Polizei und Justiz allein können dies nicht bewerkstelligen.
Insbesondere im präventiven Bereich sind die Gesellschaft, jeder Einzelne und natürlich auch die Anbieter, die die Plattform für die Nutzung bereitstellen, gefordert.

Die Europäische Union hat sich das Ziel gesetzt, zu einem Raum der Freiheit, der Sicherheit und des Rechts zu werden. Auch für den virtuellen Raum des Internets wäre das ein gutes Ziel. Ihm näher zu kommen, erfordert allerdings noch große Anstrengungen – auf nationaler wie internationaler Ebene und im Schulterschluss aller, die hierzu beitragen können.

- Polizei und Justiz müssen in der Verfolgung von Straftaten unter Missbrauch des Internets ebenso wie in der Verfolgung von Straftaten gegen die Integrität der Internetkommunikation effektiver und effizienter werden. Das erfordert eine Fortbildungs- und Ausstattungsoffensive sowie die Bereitschaft, die so genannten „anlassunabhängigen" Recherchen im Internet, also das „Streife gehen" dort, auf einer viel breiteren Grundlage zu betreiben und intelligent arbeitsteilig zu organisieren. Zur Unterstützung der Internet-Ermittlungen vor Ort bedarf es in allen Ländern der Schaffung von Kompetenzzentren mit technischen, taktischen und rechtlichen Serviceangeboten.
- Die internationale Zusammenarbeit der Strafverfolgungsbehörden muss schneller und direkter werden. Es müssen gemeinsame Strategien und Standards für die Bekämpfung von Datennetz-Kriminalität entwickelt und umgesetzt werden.

- Die Provider müssen verpflichtet werden, den ihnen möglichen und zumutbaren Beitrag zur Rückverfolgung der digitalen Spuren von Tatverdächtigen im Netz zu leisten. Dazu sollen sie künftig in der Lage sein, auf Anforderung der Strafverfolgungsbehörden entsprechende Verbindungsdaten über einen längerfristigen Zeitraum bereitzustellen.
- Der verständliche und berechtigte Einsatz von Verschlüsselungstechnik in der Internetkommunikation darf den justitiellen Nachweis von Verbrechensverabredungen über das Internet nicht unmöglich machen. Deshalb müssen die technischen wie rechtlichen Voraussetzungen für die Überwachung auch der kryptierten Kommunikation über das Internet schnellstmöglich geschaffen werden.
- Auch in der Verhütung von Straftaten im Zusammenhang mit dem Internet stehen wir noch am Anfang der Möglichkeiten. Das gilt für den Erwerb von Medienkompetenz durch Kinder, Jugendliche, Lehrer und Eltern als einem der wirksamsten Instrumente des Opferschutzes. Das gilt aber auch für die die Bereitschaft der Provider, sich im Rahmen des technisch Machbaren und wirtschaftlich Zumutbaren selbst für die möglichen kriminellen Nutzungen der von ihnen bereitgestellten Kommunikationsplattformen zu interessieren. Überall dort, wo sie entdecken, dass es Räume oder Seiten gibt, in denen eklatant gegen geltendes Recht verstoßen wird, sind diese zu sperren, auch ohne dass es hierzu eines behördlichen oder gerichtlichen Verfahrens bedarf.

Ich weiß um die Bemühungen des „Programms Polizeiliche Kriminalprävention", mit einem Provider zu gemeinsam getragenen Präventionsaktionen zu kommen. Das könnte der Auftakt für eine kriminalpräventive Partnerschaft mit der gesamten Internetwirtschaft werden. Die Wirkungsperspektiven einer solchen Partnerschaft wären enorm.

Franz-Hellmut Schürholz