Nichtöffentliches Expertengespräch der Enquete-Kommission Internet und digitale Gesellschaft, Projektgruppe Zugang, Struktur und Sicherheit im Netz, am 05.03.2012

Oberstaatsanwalt Rainer Franosch
Leitung der hessischen Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT)
Generalstaatsanwaltschaft Frankfurt am Main

Frage 1
Inwieweit reicht die bestehende Cybercrime Convention für eine verstärkte internationale Zusammenarbeit gegen Kriminalität im Internet aus? Wie bewerten Sie in diesem Zusammenhang die derzeitigen bilateralen Rechtshilfeabkommen in diesem Bereich? Wo besteht noch Verbesserungsbedarf (z.B. bei der Zusammenarbeit mit ausländischen Providern)?

Die Grenzenlosigkeit des Internets verursacht eine steigende Notwendigkeit grenzüberschreitender Ermittlungen. Die damit verbundenen Probleme – erforderliche Strafverfolgungsmaßnahmen berühren die Hoheitsrechte anderer Staaten und bedingen Rechtshilfemaßnahmen – sind den Tätern wohlbekannt und werden gezielt ausgenutzt (siehe Antwort zu Frage 4). Das Übereinkommen über Computerkriminalität (Convention on Cybercrime, ETS No.185, auch „Budapester Konvention gegen Datennetzkriminalität“ genannt) vom 23.11.2001 ist das weltweit erste multilaterale Übereinkommen über Datennetz- und Computerkriminalität. Die Vertragsstaaten haben sich zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen verpflichtet, bestimmte materielle Straftatbestände im Bereich der Computerkriminalität sowie bestimmte Befugnisse für Ermittlungsverfahren einzuführen. Deutschland hat die Cybercrime Convention (nachfolgend: CC) am 09.03.2009 ratifiziert und am 01.07.2009 in Kraft gesetzt. Das Vertragswerk enthält in Kapitel III (Art. 23 bis 35) Vorschriften zur internationalen Zusammenarbeit und Rechtshilfe, insbesondere, sofern Beweise in elektronischer Form erhoben werden sollen. Geregelt werden die Behandlung von Rechtshilfeersuchen bei Vorliegen von anwendbaren völkerrechtlichen Übereinkünften sowie solche ohne. Darüber hinaus sind Vorschriften enthalten zum grenzüberschreitenden Zugriff auf gespeicherte Daten ohne Rechtshilfeersuchen und zur Errichtung eines 24 (Stunden) /7 (Tage) Netzwerkes für eine schnelle wechselseitige Hilfeleistung.

Die getroffenen Regelungen sind angesichts der durch die Internationalität der Datennetzkriminalität entstehenden Schwierigkeiten und Hindernisse (vgl. Antwort zu Frage 4) hilfreich. Besonders hervorzuheben ist dabei die Möglichkeit einer beschleunigten zwischenstaatlichen Rechtshilfe zur umgehenden Sicherung von beweiserheblichen Computerdaten nach Art. 29 CC i.V.m. Art. 16 und 17 CC. Hierfür genügt ein formloses Ersuchen an den ausländischen Vertragsstaat zur Vorabsicherung der beweisrelevanten Daten, das inhaltlich den Anforderungen des Art. 29 Abs. 2 CC entsprechen muss. Durch die Verpflichtung zur Sicherung der Daten, insbesondere gegen die automatische Löschung, begründet die Maßnahme im Unterschied zur klassischen Durchsuchung und Beschlagnahme, die nur mit einer Duldungspflicht einhergehen, eine aktive Mitwirkungspflicht der betroffenen Provider. Nach Eingang des Ersuchens hat der Vertragsstaat gem. Art. 29 Abs. 3 S. 1 CC geeignete Maßnahmen zur umgehenden Sicherung der Daten zu treffen, wobei die beiderseitige Strafbarkeit keine Voraussetzung für die Vornahme der Sicherung ist (Art. 29 Abs. 3 S. 2 CC). Durch diese vorläufige Maßnahme lässt sich damit eine Aufbewahrung der beweisrelevanten Daten erreichen, die viel schneller

und effektiver als traditionelle Rechtshilfehandlungen ist. Art. 29 Abs. 7 CC sieht vor, dass die gesicherten Daten für mindestens 60 Tage aufbewahrt werden sollen, um der ersuchenden Vertragspartei ein förmliches Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff bzw. Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu ermöglichen.

Art. 35 CC verpflichtet die Vertragsparteien zur Einrichtung einer Kontaktstelle, die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für eilige Ermittlungshandlungen oder für die Erhebung von Beweismaterial in elektronischer Form unverzüglich für Unterstützung zu sorgen. Diese Unterstützung umfasst unter anderem die jederzeitige transnationale Übermittlung der Vorabsicherungsersuchen nach Art. 29 CC. Die Aufgabe des Art. 35 CC übernimmt das auf polizeilicher Ebene eingerichtete G8 24/7 High Tech Crime Network (HTCN). Die deutschte Kontaktstelle ist das Bundeskriminalamt, Referat SO 43.

Im Unterschied zur CC dienen die derzeitigen bilateralen Rechtshilfeabkommen nicht primär der verbesserten Bekämpfung von Datennetzkriminalität. Sie gehen – phänomenbereichsspezifisch – regelmäßig nicht über die Regelungen der CC hinaus. Gleichwohl sind auch hier z.T. Instrumente enthalten, die besonders bei der Bekämpfung von Cybercrime nützlich sein können. Beispielhaft ist das deutsch-amerikanische Rechtshilfeübereinkommen (von 2003, mit Ergänzungen aus 2006, BGBl. II, 2007, S. 1618) zu nennen. Art. 12 dieses Abkommens ermöglicht jeder Vertragspartei auf Ersuchen der anderen Vertragspartei – im Rahmen ihrer Möglichkeiten und unter den nach ihrem innerstaatlichen Recht geltenden Bedingungen – die notwendigen Schritte für die Überwachung der Telekommunikation einzuleiten. Zudem wird die Vornahme strafrechtlicher Ermittlungen durch unter verdeckter oder falscher Identität handelnder Strafverfolgungsbeamter der anderen Vertragspartei im eigenen Hoheitsgebiet gestattet. Ferner ermöglicht Art. 5 des Zusatzvertrages die Einrichtung gemeinsamer Ermittlungsgruppen auf dem Hoheitsgebiet beider Staaten, die transnational arbeiten können.

Im Hinblick auf die Wirksamkeit des in der Cybercrime Convention vorgesehenen Instrumentariums sind vor allem die nachfolgenden Punkte als grundsätzlich verbesserungsgeeignet anzusehen:

- Art. 32 CC regelt den unmittelbaren grenzüberschreitenden Datenzugriff durch Strafverfolgungsbehörden. Danach ist eine Sicherung ausländischer Daten immer dann ohne Rückgriff auf ein Rechtshilfeersuchen möglich, wenn die gesuchten Dateien frei zugänglich sind (z.B. Abruf einer Internetseite). Gleiches gilt, wenn eine rechtmäßige und freiwillige Zustimmung der zur Datenübermittlung berechtigten Person vorliegt, so dass unter diesen Voraussetzungen etwa auch ein Zugriff auf E-Mail-Konten auf ausländischen Servern oder auf Daten in Betracht kommt, die sich im Ausland befinden. Die seit 2001 eingetretenen technischen Veränderungen haben bewirkt, dass diese Vorschrift den Anforderungen an moderne Strafverfolgung nicht mehr genügt. Im Rahmen des „Cloud Computing“ werden beweiserhebliche Daten nicht mehr statisch, sondern dynamisch automatisiert auf Computersystemen weltweit abgespeichert und dabei ohne Zutun sowohl des Dateninhabers, als auch des Hostproviders, von Serverstandort zu Serverstandort grenzüberschreitend verlagert. Damit befinden sich die Daten nicht nur an Orten in anderen Rechtsordnungen als derjenigen des physischen Standorts des Beschuldigten oder seines Computers. Zudem ist den Strafverfolgungsbehörden nunmehr häufig die genaue Position der Daten in der "Wolke" unbekannt und auch nicht ohne weiteres feststellbar. Die Entwicklung hin zu Cloud Computing erschwert somit die Sicherung elektronischer Beweise in einer

Weise, wie sie 2001 nicht absehbar war, ohne dass ein Vorgehen nach Art. 29 CC Abhilfe schaffen könnte.

Zudem unterhalten globale Telemediendienste wie Google, facebook, Microsoft oder Apple nicht in allen Ländern, in denen sie geschäftliche Aktivitäten entfalten, Niederlassungen, an die die nationalen Strafverfolgungsbehörden Auskunftsersuchen nach Kundendaten richten könnten. Angesichts der herausgehobenen Bedeutung weltumspannender Internetkonzerne für die Strafverfolgung ist die Notwendigkeit, in jedem Einzelfall Rechtshilfeersuchen stellen zu müssen, obwohl die abgefragten Kundendaten regelmäßig ausschließlich Bezug zu Bürgern des ersuchenden Staates haben, wegen der eintretenden Verzögerung und des trotz Art. 29 CC bestehenden Risikos des Datenverlustes unbefriedigend. Die CC enthält keine dem Art. 52 des Schengener Durchführungsabkommens vergleichbare Regelung, wonach Direktanfragen an ausländische Provider nach Kundendaten mit ausschließlich inländischem Bezug möglich wären.

Das Konventionskomitee (Convention Comittee on Cybercrime, C-TY) hat den Änderungsbedarf von Art. 32 CC erkannt. Art. 46 CC regelt die Konsultationen der Vertragsparteien. Diese konsultieren einander bei Bedarf in regelmäßigen Abständen, um Überlegungen über eine etwaige Ergänzung oder Änderung des Übereinkommens zu treffen. Anlässlich des Treffens im November 2011 in Straßburg wurde eine Ad-hoc-Untergruppe (ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows, Az. T-CY (2011) 5 E) eingerichtet, die die Probleme beim Rückgriff auf Artikel 32 CC untersuchen soll. Ferner soll der Einsatz von grenzüberschreitenden Ermittlungsmaßnahmen im Internet unter geltendem internationalen Recht, mit Blick auf die gerichtliche Zuständigkeit und auf die staatliche Souveränität geprüft werden. Es bleiben die Ergebnisse der Untersuchungen abzuwarten, aus Sicht der Strafverfolgungspraxis erscheint es aber naheliegend, dass seitens der T-CY-Untergruppe eine Ausweitung von Art. 32 CC empfohlen werden könnte.

- Weiterhin ist festzustellen, dass Deutschland derzeit ausländischen Ersuchen gemäß Art. 29 nicht in der Weise nachkommen kann, wie es die Konvention eigentlich vorsieht. Die in Art. 17 i. V. m. Art. 16 Abs. 1 des Übereinkommens geforderte beschleunigte Sicherung von Verkehrsdaten ist bislang nicht ausdrücklich in nationales Recht umgesetzt worden. Zum Zweck der Umsetzung war zunächst erwogen worden, in § 100g StPO die zur Beauskunftung Verpflichteten auch zu verpflichten, die von ihnen erhobenen Verkehrsdaten aufgrund einer polizeilichen oder staatsanwaltschaftlichen Anordnung für die Dauer von einer Woche bereitzuhalten, wenn die Strafverfolgungsbehörden die Beantragung einer gerichtlichen Anordnung zur Erhebung der Daten ankündigen. Man ging jedoch dann davon aus, dass die Umsetzung der Richtlinie 2006/24/ EG über die Vorratsspeicherung von Verkehrsdaten dies entbehrlich machen würde (BR-Drucksache 16/5846, S. 27). Durch den Wegfall der Vorratsdatenspeicherung besteht insoweit ein für die Strafverfolgungsbehörden spürbares Umsetzungsdefizit, das sich immer dann bemerkbar macht, wenn andere Vertragsstaaten entsprechende Ersuchen auf beschleunigte Vorabsicherung von Daten an die zuständige deutsche Kontaktstelle (BKA, Referat SO 43) richten und diese oft nicht in erforderlicher Weise erledigt werden können. Mangels einer Verpflichtung der Provider (in der Praxis sind zumeist Hostserviceprovider betroffen), auf polizeiliche oder staatsanwaltschaftliche Anordnung beschleunigt Daten vor einer Löschung zu bewahren, kann hier derzeit

regelmäßig nur der herkömmliche und deutlich langsamere Weg über §§ 94 Abs. 1 Nr. 1 i.V.m. 67 Abs. 1, Abs. 2 und 66 Abs. 1 Nr. 1, Abs. 2 Nr. 1 IRG beschritten werden.

Eine weitere Möglichkeit ist für den Fall gegeben, dass sich aus dem ausländischen Ersuchen ein Anfangsverdacht für eine auch in Deutschland verfolgbare Tat ergibt (etwa, weil sich unter den Tätern oder Opfern der betreffenden Straftat deutsche Staatsangehörige befinden). Bei dieser Sachlage kann umgehend ein „Spiegelverfahren" bei einer deutschen Staatsanwaltschaft eingeleitet und die erforderliche Datensicherung nach den entsprechenden deutschen Ermächtigungsgrundlagen (zumeist gemäß §§ 94 ff. StPO) durchgeführt werden. Auch dieser Weg ist jedoch oft langwieriger als eine Direktverpflichtung der Provider, auf polizeiliche Anordnung unmittelbar nach Eingang des ausländischen Ersuchens eine Datensicherung durchzuführen.

- Eine weitere Schwierigkeit liegt schließlich darin, dass der Wirkungsbereich der Cybercrime Convention bislang zu gering ist. Nur ein Teil der für den Phänomenbereich „Datennetzkriminalität" relevanten Länder haben die Cybercrime Convention unterzeichnet, ratifiziert und in nationales Recht umgesetzt. Unter den Nicht-EU-Staaten sind dies bisher nur die USA. Auch insoweit ist der Handlungsbedarf erkannt worden und das T-CY hat einen Plan zur Verbesserung der Situation vorgelegt (T-CY: The way forward, T-CY (2011) 4 E rev.).

Frage 2
Wie bewerten Sie den Austausch über Ermittlungsmethoden / forensische Informatik innerhalb Deutschlands und weltweit? Sehen Sie Verbesserungsmöglichkeiten bei der Ausbildung und in der Forschung?

Die hohe technische Komplexität moderner Datenverarbeitung und Telekommunikation ist eine wesentliche Schwierigkeit bei der Bekämpfung von Cybercrime (vgl. Antwort zu Frage 4). Eine entsprechende Aus- und Weiterbildung der in der Strafverfolgung tätigen Personen ist daher notwendig. Dabei geht es auf polizeilicher Seite primär um die Beherrschung der erforderlichen Ermittlungsmethoden und, im Bereich der Auswertung von Beweismitteln, der forensischen Auswerte- und Ermittlungssoftware. Innerhalb der Justiz – Staatsanwaltschaften und Gerichte – ist ein Verständnis der technischen Zusammenhänge wichtig, um prozessuale und materiellrechtliche Normen zutreffend subsumieren zu können. Den staatlichen Stellen stehen dabei im Rahmen der gesetzlichen Möglichkeiten (vgl. z.B. §§ 72 ff. StPO) privatrechtliche Personen als Sachverständige zur Seite.

Der Austausch und die Aus- und Fortbildung von Ermittlungsbehörden werden durch ein entsprechendes Tagungsangebot auf Länder- oder Bundesebene gefördert. So finden ständig an zahlreichen polizeilichen Ausbildungseinrichtungen Lehrgänge statt. Das BKA führt deutschlandweite Fortbildungsveranstaltungen durch. Die Justizministerien der Länder richten Internettagungen aus, auch das Tagungsprogramm der Deutschen Richterakademie enthält jedes Jahr mehrere solche Veranstaltungen. Das BSI schult EDV-Forensiker von Strafverfolgungsbehörden des Bundes und der Länder auf hohem Niveau. Auch international gibt es ein breites Aus- und Fortbildungsprogramm für den Bereich Cybercrimebekämpfung, gerichtet an Justiz und Polizei (Ausrichter u.a. Interpol, Europol, Academy of European Law – ERA, EU – Cybercrime Centres of Excellence Network for Training Research and Education etc.)

Ausgehend von dieser durchaus soliden Basis ist aber nicht zu verkennen, dass die Wahrnehmung von Aus- und Fortbildungsangeboten häufig Eigeninitiative der Fortbildungsinteressierten voraussetzt. Zudem ist die hohe tägliche Arbeitsbelastung bei Justiz und Polizei oft ein Hindernis bei der Anmeldung zu Lehrgängen oder Tagungen, sofern eine Teilnahme nicht, was jedenfalls bei der Justiz die Ausnahme darstellt, verpflichtend ist.

Seitens der Justiz wurden daher bereits im Mai 2010 konkrete Schritte unternommen, um die Situation zu verbessern. Es wurde im Rahmen der Arbeitstagung der Generalstaatsanwältinnen und Generalstaatsanwälte mit der Generalbundesanwältin und Vertretern oberster Staatsanwaltschaften aus den europäischen Nachbarländern in Rostock die „Arbeitsgruppe zur Bekämpfung der Informations- und Kommunikationskriminalität“ ins Leben gerufen, die unter der Federführung Hessens steht und seit Juni 2011 als ständige Einrichtung etabliert worden ist. Sie hat Vorschläge unterbreitet, wie aus Sicht der Justiz die Bekämpfung der IuK-Kriminalität verbessert werden kann. Zur Verbesserung der Aus- und Fortbildung der Justiz wurde angeregt:

- Ausbildung von „IuK-Ansprechpartnern“ für die landgerichtlichen Staatsanwaltschaften durch mehrmonatige Hospitation oder einer längerfristigen Vor-Ort-Schulung in Ausbildungs- oder Ermittlungseinheiten (Aus- und Fortbildungszentren der Länder, Zentralstelle/n oder Schwerpunkt-Staatsanwaltschaften) anhand umfangreicher und/oder komplexer Ermittlungsverfahren.
- Schaffung praxisorientierter Arbeitsunterlagen zur Bewältigung wiederkehrender Ermittlungssachverhalte.
- Ein- oder mehrtägige Vor-Ort-Schulungen der Dezernenten in den landgerichtlichen Staatsanwaltschaften durch qualifiziertes Personal (soweit bereit vorhanden: durch IuK-Ansprechpartner oder die zentrale Ausbildungsstelle des Landes).
- Wissenstransfer durch interne Weiterbildungsmaßnahmen der landgerichtlichen Staatsanwaltschaften.
- Einrichtung eines Online-Portals, auf dem zeitnah aufbereitete Informationen über aktuelle und praxisrelevante Rechtsprechung aus den Bereichen des Telekommunikations- und des Jugendmedienschutzrechtes sowie Unterlagen zur Aus- und Weiterbildung im Selbststudium zur Verfügung gestellt werden.
- Vorrangige Möglichkeit der Teilnahme an Fortbildungsveranstaltungen.
- Durchführung interdisziplinärer Fortbildungsveranstaltungen (EDV-Technik und Recht).

Zur Verbesserung des Informationsaustauschs innerhalb der Strafverfolgungsbehörden hat die Arbeitsgruppe die Schaffung einer gemeinsamen Informationsplattform für Justiz und Polizei vorgeschlagen. In Form eines Online-Lexikons (Wikipedia-Prinzip) soll IuK-relevantes Wissen für die Strafverfolgungsbehörden verfügbar gemacht werden. Zudem soll darin ein Forum zum Zweck der Kommunikation über rechtliche und technische Fragen eingerichtet werden, damit der Informationsfluss nicht lediglich von der Redaktion zu den Nutzern verläuft, sondern auch zwischen den Nutzern, um Informationen sehr schnell verfügbar zu machen. Vorbild ist insoweit das polizeiliche Extranet „Extrapol“. Hauptziele des Forums sind:

- Direkter Zusammenfluss polizeilicher und justizieller Informationen.
- Schnellstmögliche Information über aktuelle rechtliche und technische Entwicklungen (Fortbildungsfunktion).

- Schnellstmögliche Information und Koordinierung bezüglich aktueller krimineller Entwicklungen (neue modi operandi) zwecks frühzeitiger Erkennung von Gemeinsamkeiten und ggf. Bildung von Sammelverfahren.

Der Zugang zur Plattform soll nur registrierten Benutzern aus Justiz und Polizei offenstehen. Um Datenschutzprobleme zu vermeiden, darf das Portal keine personenbezogenen Daten i.S.v. § 3 Abs. 1 BDSG enthalten, d.h. es soll nicht der Fahndung o.ä. dienen und stellt keine Datensammlung (Datei) im Rechtssinne dar. Dies ist auch nicht notwendig, denn wenn sich anhand von über die Plattform eingestellten und ausgetauschten Informationen der Bedarf für den verfahrensbezogenen Datenaustausch ergibt, kann dieser auf herkömmlichem Weg erfolgen.

Speziell für die Verbesserung der forensischen Informatik erscheint es wünschenswert, die Zahl der ausgebildeten Informatiker im Bereich der Strafverfolgung zu erhöhen. Erst nach und nach werden auf der Ebene der Polizei Informatiker (ohne und mit Polizeiausbildung) eingestellt. Durch das Zusammenwirken von Polizeibeamten und Informatikern kann die Strafverfolgung im Bereich von Cybercrime effektiviert werden.

Schließlich ist die grenzüberschreitende polizeiliche Zusammenarbeit, die in den letzten Jahren in formeller und informeller Weise stark zugenommen hat, zu begrüßen und zu fördern. In gleicher Weise, in der hier ein nahezu weltweites Netzwerk von polizeilichen Spezialisten entstanden ist, erscheint es erstrebenswert, eine derartige Entwicklung speziell für den Bereich Cybercrime auch auf justizieller Ebene anzustoßen. Zu diesem Zweck existieren bereits Strukturen (z.B. The Global Prosecutors Ecrime Network (GPEN), vgl. http://www.iap-association.org), die nutzbar gemacht werden können.

Frage 3
Wie verlaufen kriminelle Karrieren? Gibt es Verbindungen zu bestehenden Strukturen klassischer Organisierter Kriminalität (OK) oder haben sich bzw. bilden sich neue Strukturen heraus?

Die Entwicklung krimineller Karrieren hat sich durch das Internet teilweise gewandelt. Dies liegt zum einen daran, dass das Internet eine Anonymität bietet, die bei der Begehung von herkömmlichen Straftaten nicht gegeben ist. Die sich offensichtlich bietende Möglichkeit, über Internet vollständig unerkannt handeln zu können, fördert das Interesse an der Begehung von Straftaten. Auf der anderen Seite haben im Internet dank eines ständig wachsenden Angebots von kriminellen Dienstleistungen auch technisch ungeschulte Personen die Möglichkeit zu weitreichenden kriminellen Aktivitäten. Die Fähigkeit zu programmieren o.ä. ist zur Begehung von Delikten im Internet nicht nötig. Aufgrund des frei verfügbaren umfassenden Angebots der sog. „Underground Economy“ (= Globaler, virtueller Marktplatz, über den kriminelle Anbieter und Käufer ihre Geschäfte rund um die digitale Welt tätigen, wie z. B. der Verkauf gestohlener digitaler Identitäten oder auch kompletter krimineller Infrastrukturen) besteht auch eine Anreiz für Personen, die bis dato nicht tatgeneigt waren.

Es gibt im Phänomenbereich Internetkriminalität den klassischen, langjährig auffälligen Täter, der früher offline-Betrug begangen hat und nunmehr online dasselbe unternimmt, nur besser vor der Entdeckung geschützt. Es gibt aber auch netz-affine Täter, die offline niemals Straftaten begehen und nur die Möglichkeiten des Netzes nutzen. Darunter befinden sich zunehmend junge Täter, gut ausgebildet, oft mit EDV-Ausbildung oder in EDV-Berufen tätig,

die ein echtes Doppelleben führen. Neben der bürgerlichen Existenz verdienen sie sich ein Zubrot als Straftäter im Netz.

Die Datennetzkriminalität weist zudem immer engere Verbindungen zur existierenden, klassischen Organisierten Kriminalität (OK) auf. Diese Beobachtung aus der Praxis der ZIT findet sich auch im EU Organised Crime Threat Assessment 2011 (OCTA) wieder (ebda., S. 6).
Ganz deutlich wird dies beim Handel mit illegalen Substanzen wie Drogen oder verschreibungspflichtigen Arzneimitteln sowie mit Waffen. Sowohl Drogen als auch Waffen werden über die anonymen Foren der Underground Economy gehandelt und über die Kanäle der klassischen OK dorthin eingespeist.

Weiterhin gibt es Anzeichen dafür, dass das Internet auch beim Menschenhandel eine zunehmende Rolle spielt. Immer wieder werden Gelegenheiten zur (Kinder-)Prostitution in einschlägigen Internetforen angeboten.

Eine Verbindung von Strukturen herkömmlicher OK und Internet zeigt sich auch bei der Geldwäsche. Es ist im Internet eine große Zahl von Portalen anonymer Offshore-Banken entstanden, die ihre Dienste weltweit anbieten und Schnittstellen zum legalen Geldkreislauf bereithalten.

Gleichzeitig bilden sich neue, netzspezifische OK-Strukturen heraus, die, wie oben bereits erwähnt, üblicherweise als Underground Economy bezeichnet werden. Die im Phänomenbereich aktiven Täter haben heute nach den bisherigen Erfahrungen in einer Vielzahl der Fälle als Einzelpersonen oder in Kleingruppen weder das vollständige zur Tatbegehung technische und soziale Wissen / Erfahrung, noch die zur Tatbegehung notwendige (technische und finanzielle) Infrastruktur. Allerdings hat sich in den vergangenen Jahren ein globaler Markt entwickelt, auf dem sowohl die zur Tatbegehung notwendige Infrastruktur angekauft oder angemietet, als auch Ergebnisse kriminellen Aktivitäten (z. B. ausgespähte Daten) wieder in monetäre Vorteile gewandelt werden können. In der Welt der Cybercrime hat sich ein Parallelmarkt entwickelt, auf dem Daten, Waren, Geschäftsmodelle und Infrastruktur gehandelt werden. Dieser Markt orientiert sich dabei, wie „normale“ Märkte auch, an den Kundenbedürfnissen, und damit vor allem an der Nachfragesituation. Hier werden Wissen und Ressourcen gehandelt, mit digitalen Währungen wie Bitcoins, UKash oder Webmoney bezahlt und durch Umsatz- und Gewinnbeteiligungen abgegolten. Die einzelnen Beteiligten kennen sich dabei in aller Regel nicht – man bleibt auch gegenüber seinem „Partner“ anonym – was die Ermittlungschancen der Strafverfolgung gleichfalls negativ beeinflusst.

Schließlich ist festzustellen, dass sich im Bereich der Verbreitung kinderpornographischer Bild- und Videodateien im Internet organisierte Strukturen neuer Qualität herausgebildet haben. In umfangreichen Ermittlungen in diesem Phänomenbereich seit 2009 konnte nicht nur festgestellt werden, dass es festgefügte, abgeschottete und hierarchisch aufgebaute geschlossene Benutzerkreise zum Austausch von Kinderpornographie gibt, sondern auch exklusive Bereiche, in denen der reale sexuelle Missbrauch von Kindern und die Weitergabe des so selbst produzierten Materials als Zugangsvoraussetzung dienen. Das Motto eines Bereiches in einem Pädophilen-Forum lautete: „Don’t ask for membership if you haven’t got your own daughter to share”. Das Umfangsverfahren “Geisterwald” erbrachte folgende Erkenntnisse:

- Es handelte sich um einen bandenmäßig strukturierten Internetring zum Tausch von kinderpornographischen Bild- und Videodateien.
- Der Austausch erfolgte über geschlossene Internetforen, sog. Boards und Chaträume.
- Der streng nach außen abgeschottete Ring umfasste weltweit ca. 500 Personen mit Schwerpunkt im deutschsprachigen Raum (Deutschland, Schweiz, Österreich).
- Die Mitglieder tauschten sowohl umfangreiches Bild- und Videomaterial als auch ihre eigenen Erfahrungen beim sexuellen Missbrauch von Kindern aus.
- 29.9.2009: 121 Durchsuchungen in BRD, 15 im Ausland, 800 eingesetzte Polizeibeamte
- Sichergestellte Beweismittel: rund 220 Computer und mehr als 17.000 digitale Speichermedien
- 9 Haftbefehle gegen ermittelte Administratoren
- Weltweit bislang insgesamt rund 160 Personen als Mitglieder identifiziert.
- März 2010: Anklage gegen neun Männer im Alter zwischen 30 und 58 Jahren wegen bandenmäßiger Drittbesitzverschaffung von kinderpornographischem Material im Internet und gegen zwei der Männer darüber hinaus wegen teils schweren sexuellen Missbrauchs von Kindern in 33 Fällen.
- Hauptverhandlung vor dem LG Darmstadt von September 2010 bis April 2011
- Ergebnisse: Freiheitsstrafen zwischen 2 Jahren und 8 Jahren 6 Monaten mit anschließender Sicherungsverwahrung für die 9 Administratoren.
- Gegen rund 25% (!) der identifizierten Mitglieder wurden Ermittlungsverfahren wegen Verdachts des sexuellen Missbrauchs eingeleitet.

Der entgeltliche Vertrieb von Kinderpornographie wird ebenfalls überwiegend in organisierter Form betrieben, wie immer wieder anhand von Ermittlungsverfahren festgestellt wird. So wurden 2008 drei Entwickler und Betreiber eines Internet-Zahlungssystems in Weißrussland festgenommen. Das System war dazu benutzt worden, die Zahlungen im Zusammenhang mit über 270 kostenpflichtigen kinderpornographischen Webseiten abzuwickeln. Die sichergestellte Datenbank umfasste über 60.000 verschiedene Kundenkonten aus 146 Ländern. Der jährliche Gewinn der Täter betrug ca. vier Millionen US-Dollar. Ca. 1700 Kreditkartennummern waren Deutschen zuzuordnen.

Frage 4
Welches sind die fünf größten Schwierigkeiten, vor denen Ermittlungsverfahren im Bereich Internetkriminalität regelmäßig stehen?

1. Anonymität im Netz

Grundsätzlich ist die Möglichkeit, sich im Internet unerkannt zu bewegen, ein zwingendes Gebot des Grundrechts auf informationelle Selbstbestimmung. Anonymität im Netz reduziert zudem die Angreifbarkeit durch Kriminelle oder durch professionelle Datensammler aller Art. Schließlich fördert Anonymität die Bereitschaft zum aktiven Diskurs, zur Meinungsäußerung und zur Wahrnehmung des Grundrechts auf Meinungsfreiheit. In Ländern mit diktatorischer Staatsform sind Anonymisierungstechniken oft der einzige Schutz vor staatlicher Repression. Die diesbezügliche Bedeutung des Internets haben nicht zuletzt die Ereignisse des arabischen Frühlings gezeigt.

Es liegt auf der Hand, dass der Einsatz von Anonymisierungstechniken wie TOR (The Onion Router) anderseits Probleme für die Strafverfolgung aufwirft. Das Internet bietet z.B. im Bereich der digitalen Schutzgelderpressung (siehe näher dazu unten) die technische

Möglichkeiten zur Begehung der perfekten Straftat. Der Täter kann dabei von einem beliebigen Ort aus innerhalb kürzester Zeit eine Vielzahl von Geschädigten in beliebiger Entfernung mit Schäden bedrohen, seine Drohungen in die Tat umsetzen sowie die geforderten Geldbeträge erhalten und weitertransferieren, ohne sich auch nur einmal von seinem PC wegbewegen zu müssen. Benutzt der Täter dabei Anonymisierungstechniken, ist er nicht ermittelbar.

Die Möglichkeit, ohne jeden Ermittlungsansatz Vermögensdelikte erheblichen Ausmaßes zu begehen, ist nur im Internet gegeben.

Die Flüchtigkeit der beweiserheblichen Daten u.a. aufgrund fehlender Vorratsdatenspeicherung ist, neben der Benutzung von Anonymisierungstechniken, eine weitere Möglichkeit für Täter, anonym zu bleiben. Die Flüchtigkeit von Daten wird gefördert durch die fehlende Verpflichtung von Internet-Providern, eine 24/7-Bereitschaft für behördliche Auskunftsersuchen sicherzustellen.

2. Internationalität des Netzes, Notwendigkeit für grenzüberschreitende Ermittlungen

Bereits bei der Beantwortung von Frage 1 ist dieses Verfolgungshemmnis angesprochen worden. Zu ergänzen ist, dass die Täter die Probleme der Strafverfolgung kennen. Sie reagieren entsprechend zum Beispiel durch folgende Verhaltensweisen:

- Programmierung der Malware dort, wo dies nicht unter Strafe steht.
- Einrichtung von digitaler Geldwäsche-Infrastruktur dort, wo dies aufgrund von Regelungslücken nur schwer verfolgt werden kann.
- Verteilen des Hostings und der durch sie genutzten Infrastruktur über unterschiedliche Staaten, um Rechtshilfe zu erzwingen.
- Kommunikationsserver in Staaten, mit denen formelle justizielle Rechtshilfe erfolgen muss.
- Konzentration des Hostings auf Staaten, die in keinem Vertrauensverhältnis zu den primären Opferstaaten stehen, um Rechtshilfe zu erzwingen.
- Keine Angriffe auf Institutionen aus Staaten, die geographischer Standort von Teilen der kriminellen Infrastruktur sind, um dort keine strafprozessualen Maßnahmen zu provozieren.

3. Professionalität der Täter

Insbesondere im Bereich der organisierten Internetkriminalität agieren die Täter auf technisch hohem Niveau. Neue Schutzlücken werden sofort erkannt und ausgenutzt, ehe Gegenmaßnahmen ergriffen werden können (zero-day-exploits).

4. Schwierigkeit der Materie / Komplexität technischer Abläufe

Wie bereits zu Frage 2 ausgeführt, bedingen die hohe technische Komplexität moderner Datenverarbeitung und Telekommunikation ständigen Fortbildungsbedarf bei Justiz und Polizei sowie eine zeitgemäße technische Ausstattung. Dies erschwert die Strafverfolgung.

5. Mangelnde Anzeigebereitschaft von Geschädigten

Die mangelnde oder zu späte Erstattung von Strafanzeigen führt dazu, dass Zusammenhänge oft zu spät erkannt werden oder Spuren kalt sind, d.h. Datenverlust eingetreten ist.

Frage 5
In welchen Bereichen findet Kriminalität im Internet statt? Wissen Sie, in welchem Umfang diese Delikte auftreten? Können Sie Größenordnungen verschiedener Delikte darlegen?
Frage 6
Findet in diesem Zusammenhang eine „Verschiebung" der Deliktsbegehung von der analogen in die digitale Welt statt? Konnten Sie insgesamt eine Zunahme von Delikten feststellen?

Internetkriminalität umfasst zahlreiche Straftatbestände. Diese reichen von der Beleidigung in Internetforen über Betrugshandlungen bei Internethandel bis hin zur Infizierung fremder Rechner mittels Trojanern, um sensible Daten (z. B. im Online-Banking) auszuspähen. Bedeutend ist dabei der Anteil des Betruges im Internet und hier insbesondere der Waren- bzw. Warenkreditbetrug. Gängige Methode ist die Nutzung von Online-Plattformen für betrügerische Angebote. Ferner ist hier das „Carding" zu nennen, also der Betrug mittels fremder Kreditkartendaten.
Daneben ist der Kernbereich der Internetkriminalität, wie beispielsweise Angriffe auf Computersysteme, das Ausspähen sensibler Daten und die Manipulation von solchen oder Computern zu nennen. Ein Phänomen, welches nach wie vor eine große Rolle spielt, ist das Ausspähen von Zugangsdaten für Online-Banking und andere Dienste im Internet wie Internetshops oder soziale Netzwerke. Dabei werden mit Schadprogrammen (Trojanern) infizierte Rechner ausgespäht und die Daten anschließend für Geldtransfers und andere kriminelle Aktivitäten genutzt. Unter dem Begriff Phishing gewinnt dieses Phänomen zunehmend an Bedeutung und ist momentan eine der Bedrohungen für die heimische IT-Infrastruktur. Allerdings dürfte der Begriff des „Phishing", ein Kunstwort aus „Password" und „Fishing", nicht geeignet sein, die tatsächliche Bedeutung der dahinterstehenden Straftat für das Opfer abzubilden. Letztlich geht es um nicht weniger als den Diebstahl der digitalen Identität des Opfers.

Ausgespähte Daten werden sodann von den Tätern oft auf den Marktplätzen der Underground Economy verkauft (Datenhehlerei).

Das Phänomen der digitalen Erpressung gewinnt ebenfalls an Bedeutung. Digitale Erpressung umfasst:

- Digitales Schutzgeld: Geld wird verlangt von den Betreibern von Internetshops zur Abwendung von Distributed Denial of Service (DDoS) – Angriffen (angegriffene Server sind aufgrund einer Überlastung mittels sinnloser, durch infizierte PCs generierter Anfragen nicht mehr in der Lage, die auf ihnen abgelegten Inhalte im Internet bereit zu stellen).
- Digitales Lösegeld: Ein mit einem Trojaner infizierter Rechner wird von den Tätern zugangsgesperrt und erst nach Zahlung des Lösegeldes wieder freigegeben (oder auch nicht).
- Rückkauf kompromittierter Daten: Wichtige Daten werden ausgespäht, kopiert und beim Eigentümer gelöscht und die Kopie der Datensätze nur zurückgegeben, wenn vom Opfer dafür gezahlt wird.
- Schweigegeldforderung: Sensible Daten werden ausgespäht, also kopiert, und nur dann nicht im Internet veröffentlicht, wenn vom Opfer dafür gezahlt wird.

Wesentlicher Deliktsbereich der Internetkriminalität ist weiterhin die Verbreitung von Kinderpornographie sowie von gewaltverherrlichenden oder politisch oder religiös extremistischen Schriften, Bildern und Videos.

Schließlich werden strafbare Verstöße gegen das Urheberrecht mittels Internet begangen, wobei aus Sicht der Strafverfolgungspraxis besonders der unmittelbar oder mittelbar (Stichwort "kino.to") entgeltliche Vertrieb von raubkopierter Software, Film- und Musikwerken relevant ist.

Angesichts der Tatsache, dass die Justiz keine eigenen phänomenspezifischen Statistiken führt, kann bei der Beantwortung der Frage nach Umfang und Größenordnung von Straftaten im Internet lediglich die polizeiliche Kriminalstatistik (PKS) helfen, wobei diese Statistik bekanntermaßen systemimmanente Schwächen aufweist, die nicht vernachlässigt werden dürfen. Einzelne bzw. besonders relevante Phänomene der echten Cybercrime (= IuK-Kriminalität, umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden, nicht zu verwechseln mit „Straften unter Verwendung des Tatmittels Internet", dazu näher unten), wie z. B. Phishing im Bereich Onlinebanking oder auch Straftaten im Zusammenhang mit gezielten DDoS-Attacken auf Server eines Unternehmens oder einer Behörde, werden in der PKS nicht unter dem Begriff Cybercrime erfasst. Vielmehr erfolgt eine statistische Erfassung dieser Delikte unter den PKS-Schlüsseln der einzelnen Tathandlungen. Dies führt dazu, dass keine auf zuverlässigen Daten basierenden Aussagen zum tatsächlichen Ausmaß gerade in diesen von den Strafverfolgungsbehörden als relevant wahrgenommenen Feldern des Bereichs Cybercrime möglich sind. Zusätzlich ist, insbesondere bei den Deliktsfeldern Computersabotage und Datenveränderung, von einem großen Dunkelfeld auszugehen. Dies ist unter anderem darauf zurückzuführen, dass Straftaten häufig durch den Geschädigten gar nicht erkannt werden (die Infektion des Computers bleibt unentdeckt) oder □der Geschädigte (häufig ein Unternehmen) die erkannte Straftat nicht anzeigt, um beispielsweise im Kundenkreis die Reputation als „sicherer und zuverlässiger Partner" nicht zu verlieren.

Unabhängig von der Entwicklung der reinen Fall- bzw. Schadenszahlen, die aufgrund des vermuteten Dunkelfeldes ohnehin nur eine sehr begrenzte Aussagekraft besitzen, haben die Intensität der kriminellen Aktivitäten im Bereich Cybercrime und das für jeden Internetnutzer bestehende Gefährdungspotenzial weiter zugenommen. Diese Entwicklung lässt sich nicht zuletzt an der gestiegenen Professionalität der eingesetzten Schadsoftware sowie der festgestellten zunehmenden Spezialisierung und Professionalisierung der Täter ablesen. Darüber hinaus hat sich mittlerweile im Bereich der Underground Economy auch in Deutschland eine breite Szene etabliert, die sich zuvor überwiegend in englisch- oder russischsprachigen Foren und Plattformen betätigte.

Betrachtet man nun – unter Berücksichtigung ihrer beschränkten Aussagekraft – die PKS, so ergibt sich, dass die Anzahl der Taten unter Verwendung des Tatmittels Internet seit dem Jahr 2008 stetig angestiegen ist. Der Erfassungsmerker „Tatmittel Internet" wird durch die jeweiligen polizeilichen Datenerfasser – welche nicht immer mit dem Sachbearbeiter des Verfahrens identisch sein müssen – gesetzt, wenn das Internet im Verfahren in beliebiger Weise relevant wurde, also auch dann, wenn lediglich über das Internet kommuniziert wurde. Dies erklärt, warum beispielsweise in der Statistik für das Jahr 2010 auch 31 Fälle des „Diebstahls von Fahrrädern unter erschwerenden Umständen" als Internetkriminalität erfasst wurden.

Die Entwicklung der so entstandenen Zahlen belief sich von

167.451 Taten im Jahr 2008 über
206.909 Taten im Jahr 2009 auf schließlich
223.642 Taten im Jahr 2010.

Dies ergibt einen Anstieg um 23,6 Prozent von 2008 auf 2009 und von 2009 auf 2010 einen Anstieg um 8,1 Prozent. Dabei ist zu berücksichtigen, dass die Erfassung nur 15 Bundesländer berücksichtigt. Im Jahr 2010 wurde das 16. Bundesland – das bis dahin die Kategorie „Tatmittel Internet“ nicht aufgenommen hatte – eingefügt, wodurch sich eine Gesamtzahl für 16 Bundesländer von 246.607 Taten ergibt.

Dem gegenüber wurden im Jahr 2008 insgesamt, also in allen Deliktsfeldern, 6.114.128 Taten, in 2009 6.054.330 Taten und in 2010 5.933.278 Taten erfasst. Die Anzahl an Straftaten ist in der Gesamtschau – legt man die PKS zugrunde – also rückläufig und zwar um 1% zwischen 2008 und 2009 und um 2% zwischen 2009 und 2010. Die Aufklärungsquoten insgesamt betragen 2008 54,8%, in 2009 55,6% und in 2010 56%.

Bei vier Fünftel der Fälle mit Tatmittel Internet handelt es sich im Jahre 2010 um Betrugsdelikte (80,6 %). Besonders hervorzuheben ist hierbei der Warenbetrug, auf den allein der größte Anteil (29,0 %) aller Fälle entfielen. Beachtenswert ist auch der Anteil von 14,5 % bei sonstigem Warenkreditbetrug. Beim Waren-, Computer- und Leistungsbetrug, aber auch bei der Verbreitung pornographischer Schriften (Erzeugnisse) diente das Internet in mehr als der Hälfte der Fälle als Tatmittel.

In manchen Bereichen – ohne dies jedoch näher quantifizieren zu können – ist eine nahezu vollständige Verschiebung der Straftaten in das Internet zu beobachten, wie zum Beispiel bei der Verbreitung kinderpornographischer Schriften. Auch betrügerische Warenbestellungen werden in immer größer werdendem Umfang im Internet vorgenommen. Hinzu kommt, dass bestimmte Deliktsarten, wie zum Beispiel Phishing oder auch Warenkreditbetrug mittels gephishter Kreditkartendaten (ohne die Herstellung und Nutzung gefälschter Karten) zu ihrer Umsetzung auf das Tatmittel Internet angewiesen sind.

Für Hessen liegen bereits die Zahlen für das Jahr 2011 vor, aus denen sich eine Zunahme von registrierten Fällen der Internetkriminalität um 282 Fälle auf insgesamt 17.951 Fälle ergibt. Dabei ist jedoch seit 2007 eine deutlich steigende Tendenz bei den Straftaten des Computerbetruges und des Ausspähens von Daten zu erkennen, was dem Bundestrend entspricht. Die Entwicklung in Hessen verläuft für die Straftat des Computerbetruges von 586 registrierten Fällen im Jahr 2007 auf 1.059 Fälle im Jahr 2011 bezüglich des Ausspähens von Daten stieg die Fallzahl von 358 Fällen in 2007 auf 945 Fälle im Jahr 2011 an.
Prozentual sind verschiedene Fälle der Internetkriminalität ausweislich der PKS Hessen für das Jahr 2011 wie folgt verteilt: An der Spitze stehen Waren- und Warenkreditbetrugstaten mit 39,1%, dicht gefolgt von sonstigen Straftaten mit 38,5%, die zum Beispiel Beleidigungen, aber auch Betrug mit Zugangsberechtigungen umfassen. Computerbetrugstaten wurden mit einem Anteil von 5,9% erfasst, Ausspähen von Daten mit 5,3%, Leistungskreditbetrug mit 3,7%, Leistungsbetrug mit 3,5%, Verbreitung pornographischer Schriften mit 2,4% und Urheberrechtsverletzungen mit 1,7%.

Im Hinblick auf Wirtschaftsstraftaten mit dem Tatmittel Internet wurde durch die KPMG International Cooperative eine repräsentative Befragung 300 mittelständischer und großer Unternehmen durchgeführt. Während für das Jahr 2003 nur 19% der befragten Unternehmen

angaben, Opfer von „E-Kriminalität“ geworden zu sein, stieg dies in 2006 bereits auf 23% und in 2010 auf 53% der befragten Unternehmen.
Ob die Definition von „E-Kriminalität“ sich mit der polizeilichen Definition zu 100% deckt, kann indes nicht gesagt werden.

Die Gesamtaufklärungsquote für alle Straftaten im Jahr 2009 von 55,6% und im Jahr 2010 von 56% steht den Aufklärungsquoten bei der IuK-Kriminalität im engeren Sinne von 35,2% im Jahr 2009 und 33% im Jahr 2010 gegenüber. Beim Tatmittel Internet liegen Zahlen bei 75,7% im Jahr 2009 (ohne Bayern) und bei 71,0 % für 2010 (mit Bayern, ohne Bayern: 72,3%).

Bei den registrierten Schäden im Bereich Cybercrime ist in 2010 ein Anstieg um mehr als 66% gegenüber dem Jahr 2009 zu verzeichnen. So beläuft sich der im Jahr 2010 registrierte Schaden aller in der PKS mit Schadenssumme erfassten Delikte aus dem Bereich Cybercrime (Erfassung der Schadenssumme erfolgt lediglich bei den Delikten Computerbetrug und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten) auf insgesamt rund 61,5 Mio. Euro (2009: 36,9 Mio. Euro), wobei rund 47 Mio. Euro auf den Bereich Computerbetrug und 14,5 Mio. Euro auf den Bereich Betrug mit Zugangsdaten zu Kommunikationsdiensten entfallen.

Frage 7
Was sind die Möglichkeiten der Strafverfolgung und welche verfassungskonformen Mittel erachten Sie als zielführend?

Die Strafverfolgungsbehörden reagieren auf die wachsende Bedrohung durch Datennetzkriminalität mit verbesserter Aus- und Fortbildung, besserer Vernetzung und der Bildung von spezialisierten Ermittlungseinheiten. Dieser Weg erscheint sinnvoll und sollte konsequent weiter beschritten werden.

Die StPO enthält zudem brauchbare Instrumente zur Täterermittlung. Neben den Maßnahmen zur Telekommunikationsüberwachung und Observation (z.B. §§ 100a, 100g, h StPO) als verdeckte technische Ermittlungsmethoden sind hier besonders verdeckte personale Internetermittlungen zu nennen, namentlich der Einsatz verdeckter Ermittler gemäß § 110a StPO oder von nicht offen ermittelnden Polizeibeamten auf Grundlage der Ermittlungsgeneralklausel des § 163 StPO. Angesichts der Möglichkeiten der Anonymisierung stoßen technische Ermittlungsmethoden allein häufig an Grenzen. Daher werden verdeckte personale Internetermittlungen zukünftig an Bedeutung gewinnen.

Soziale Netzwerke dürften sich zukünftig im verstärkten Maße für Öffentlichkeitsfahndungen anbieten.

Auf internationaler Ebene dürfte der verstärkte Einsatz von gemeinsamen Ermittlungsgruppen eine erfolgversprechende Maßnahme sein, um grenzüberschreitende Ermittlungen zu vereinfachen.

In Bezug auf die aufgrund der durch den Beschluss des BVerfG, 1 BvR 1299/05, vom 24.01.2012 erforderlich gewordene Neuregelung der Abfrage dynamischer IP-Adressen durch die Ermittlungsbehörden erscheint es aus Sicht der staatsanwaltschaftlichen Praxis ratsam, die bisherigen Voraussetzungen hierfür in verfassungskonformer Umsetzung der Gerichtsentscheidung beizubehalten. Das heißt konkret, die neu zu schaffende

Ermächtigungsgrundlage sollte – aus Praktikersicht – vorsehen, dass die Polizei die Bestandsdaten zu dynamischen IP-Adressen auch weiterhin bei einfachem Anfangsverdacht, ohne einen begrenzenden Straftatenkatalog und ohne Richtervorbehalt bei den Providern abfragen kann. Das BVerfG lässt dies bereits in der Entscheidung zur Vorratsdatenspeicherung vom 02.03.2010 ausdrücklich zu (vgl. 1 BVR 256/08 Rn. 254-256, 289), was durch die neue Entscheidung nicht in Frage gestellt, sondern fortgeführt wird.

Frage 8
Bestehen Regelungslücken im Zusammenhang mit der Strafverfolgung? Welche praktischen Strafverfolgungsprobleme bestehen aus Ihrer Sicht?

Bei der Beantwortung dieser Frage sind materielles und prozessuales Recht zu unterscheiden.

In materiell-rechtlicher Hinsicht erscheint der strafrechtliche Schutz von persönlichen Daten nicht genügend zu sein. Insbesondere die Weitergabe rechtswidrig erlangter persönlicher Daten im oder über Internet durch einen Täter, der von den Daten selbst keinen Gebrauch macht, ist nur in seltenen Konstellationen nach den sehr engen Strafbestimmungen des Bundesdatenschutzgesetzes (BDSG) verfolgbar, in der Regel aber vollständig straflos. Deswegen hat Hessen zu Beginn seines Vorsitzes der Justizministerkonferenz im Januar dieses Jahres eine Initiative gestartet, die Datenhehlerei unter Strafe zu stellen.

In diesem Zusammenhang könnte man auch darüber nachdenken, ob die Ausgestaltung der Strafbestimmung des § 44 BDSG als absolutes Antragsdelikt (mit einer Möglichkeit der Antragstellung für den Bundesdatenschutzbeauftragten) sinnvoll ist oder ob es nicht ratsam sein kann, hier nicht nur dem Bundesbeauftragten für den Datenschutz, sondern auch den Staatsanwaltschaften die Möglichkeit einzuräumen, bei Vorliegen eines besonderen öffentlichen Interesses die Strafverfolgung einzuleiten.

Bei der Schaffung oder Reform von strafprozessualen Ermächtigungsgrundlagen im Bereich von Telekommunikationsermittlungen sollte daneben generell bedacht werden, dass die Einführung begrenzender Straftatenkataloge im Bereich der Netzkriminalität mangels anderweitiger Ermittlungsansätze verfolgungsfreie Räume schaffen kann. Sinnvoll erscheint insoweit die Regelung des § 100g StPO, wonach bei Straftaten mittels Telekommunikation auf die Beschränkung der erheblichen Bedeutung der aufzuklärenden Tat verzichtet wird, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Hinsichtlich der Probleme der Strafverfolgung nehme ich auf die Ausführungen zu Frage 1 und 4 Bezug.

Frage 9
Wie erfolgreich gestaltet sich der Kampf der Staatsanwaltschaften gegen diese Art von Kriminalität? Wo stoßen die Staatsanwaltschaften an ihre Grenzen?

Hinsichtlich der Grenzen der Strafverfolgung darf ich wiederum auf meine Antwort zu Frage 1 und 4 verweisen.

Trotz aller Schwierigkeiten können die Strafverfolgungsbehörden immer wieder teils auch gute Erfolge bei der Bekämpfung von Internetkriminalität erzielen. Besonders das Zusammenwirken von verdeckten technischen und personalen Internetermittlungen führt, gepaart mit gründlicher Nutzung aller zugänglichen Datenquellen, nicht selten zum Erfolg.

Beispielhaft kann hier – neben den oben schon genannten Fällen in Bezug auf die Verbreitung von Kinderpornographie – auf ein Verfahren wegen digitaler Schutzgelderpressung verwiesen werden. Sachverhalt:

- Im Sommer 2010 blockierten die Täter bundesweit wiederholt die Erreichbarkeit von Internetseiten verschiedenster Onlineshops durch DDoS-Attacken auf deren Servern.
- Die Täter forderten im Anschluss per E-Mail von den Betroffenen die Zahlung von dreistelligen Euro-Beträgen über anonyme Zahlungsdienste wie „UKash“ oder „Paysafecard“.
- Die ZIT bildete ein bundesweites Sammelverfahren. Auf polizeilicher Seite übernahm das BKA die Ermittlungen.
- Zwischenzeitlich konnten 5 Beschuldigte ermittelt werden.
- Anfang August 2011 fanden bundesweite, koordinierte Durchsuchungsmaßnahmen unter Vor-Ort-Beteiligung der ZIT statt.
- Es wurden umfangreiche Beweismittel sichergestellt, deren Auswertung in Kürze abgeschlossen sein wird.
- Beschuldigte kennen sich aus einschlägigen deutschsprachigen Szeneforen der Underground Economy.
- Die Beschuldigten stehen im Verdacht, zahlreiche weitere Straftaten aus dem Bereich der Computerkriminalität begangen zu haben.
- Insgesamt wurden ca. 50 Fälle bekannt, in denen Betreiber von Webshops mit DDoS-Attacken bedroht oder tatsächlich angegriffen wurden. Die von den geschädigten Unternehmen auf die DDoS-Angriffe zurück zu führenden, geschätzten Umsatzeinbußen belaufen sich insgesamt auf ca.sechsstellige Euro-Beträge.
- Zur Umsetzung der Erpressungsvorhaben wurden arbeitsteilig
    + Webserver unter unwahren Daten angemietet/vorgehalten, mit der Absicht darauf Botnet-Steuersoftware zu installieren,
    + Schadsoftware (für Antivirus-Software unkenntlich gemacht mittels sog."Crypter") im Internet verbreitet mittels derer infizierte Opfer-Rechner in das Botnet eingegliedert wurden,
    + unter Verwendung unwahrer Daten Emailkonten angelegt,
    + mobile Internetzugänge eines Providers, der keinerlei Datenspeicherung vornimmt, vorgehalten (wissend, dass eine Zurückverfolgung dieser UMTS-Zugänge bei diesem Provider nicht möglich ist).

Frage 10

Geben Sie einen kurzen historischen Rückblick auf die Themen „Kriminalität im Telefonnetz“ sowie „Telefon als Tatwaffe“. Wie sieht die Bearbeitungsrealität bei der Polizei (wie lange braucht es, um eine Betrugsanzeige zu bearbeiten) aus? Wie gestaltet sich das Verhältnis von aufgeklärten Taten von Kriminalitätsfällen, ohne Internetbezug und mit Internetbezug?

Phänomenologie:

- Missbrauch von Telefonkarten
  Ein Missbrauch von Telefonkarten ist dadurch möglich, dass rechtswidrig erlangte

Telefonkarten zu Anrufen zu eigenen Mehrwertdiensten genutzt werden. Darüber hinaus kommt auch die Verwendung von sog. Telefonkarten-Simulatoren in Betracht. Statt des üblicherweise in einer Telefonkarte eingesetzten Chips kommt ein Chip zum Einsatz, der dem Ablesegerät signalisiert, die Karte sei aufgeladen.

- Missbrauch von Mehrwertdiensten
  Bei Einführung der Mehrwertdienste waren die Verbindungskosten nach oben nicht begrenzt und mangels Verzeichnis der Zugangsnetzbetreiber (Carrier), denen Rufnummernkontingente zugewiesen waren, konnten Täter durch Einschaltung weiterer Unterhändler etc. durch die Carrier ihre Identität verschleiern.
  Inzwischen erfolgt der Missbrauch solcher Mehrwertdienste durch die Verwendung versteckter Auslandsvorwahlen. Der verdächtigen Anschlussnummer werden zu deren Verdeckung Länderkennungen vorangestellt und die Erkennung des Mehrwertdienstes durch geschickte Anordnung der Zahlen zusätzlich verschleiert: 004-990-076-543-210-876. In der Nummer sind zum einen die Auslandsvorwahl 0049, sodann die Nummer des Mehrwertdienstes 900 und die Anschlussnummer 76543210876 enthalten.
  Alternativ zur Verwendung der Auslandsvorwahl kann auch die Netzvorwahl der DTAG 01033 verwendet werden: 01033900987654321.
  Allein durch die Erlangung einer Mehrwertdienstenummer kann der Täter Gewinne erzielen, indem er sich z.B. Zugang zu fremden Telefonen verschaffen und von dort „seine“ Nummer anruft.

- Lockrufe
  Der Täter veranlasst manuell oder mittels eines automatisierten Verfahrens einen Anruf von einem Mehrwertdienst beim Opfer und unterbricht den Anruf vor Entgegennahme. Das Empfängertelefon zeigt dadurch einen Anruf in Abwesenheit an. Ziel der Täter ist, das Opfer zum Rückruf zu veranlassen, bei dem die Kosten des Mehrwertdienstes anfallen. Dabei wird dem Opfer teilweise ein Freizeichen vorgespielt, obwohl der Anruf bereits angenommen wurde. Eine Verschleierung der Rufnummer des Mehrwertdienstes erfolgt zum Beispiel über die Verwendung von Landeskennungen.

- Eingriffe in fernwartungsfähige Telefonanlagen
  Bei Telefonanlagen, die fernwartungsfähig sind, besteht die Möglichkeit einer Umstellung durch Hacker von außen, sodass die Anlage automatisch Mehrwertdienstenummern anwählt.

- Stalking
  Das Tatmittel Telefon ist das klassische Instrument für die Begehung von Stalking-Taten. Darunter fallen nicht nur wiederholte Anrufe, sondern auch der Versand von SMS.

- „Happy Slapping“ u.a.
  Insbesondere im Bereich der Jugenddelinquenz sind vermehrt Fälle aufgetreten, bei denen die Opfer durch die Täter verprügelt werden und diese Tat mittels eines Telefons mit Kamerafunktion gefilmt wird. Das so erstellte Video wird im Nachgang an weitere Personen mobil übertragen, wodurch eine Perpetuierung der Tat zum Nachteil des Opfers erfolgt.
  Auch das Filmen von sexuellen Handlungen und die Weitergabe der Aufnahmen mittels kamerafähiger Telefone stellt ein zunehmendes Problem dar.

- Enkeltrick
  Die Tätergruppierung ruft bei älteren Menschen an und startet das Gespräch häufig mit

den Worten: „Rate mal, wer hier ist!“ Wenn das Opfer dann einen Namen sagt, bestätigt der Täter, diese Person zu sein. In der Folge wird der vermeintlichen „Oma“ dann eine Geschichte über Geldsorgen erzählt und schließlich – nachdem sich das Opfer zur Zahlung von Geld bereiterklärt hat – mitgeteilt, dass das Geld von einem Freund abgeholt wird.

- Applikationen für Smartphones
  Die Verwendung von Applikationen bietet ähnliche Möglichkeiten, wie im Bereich des Internets durch Nutzung herkömmlicher Endgeräte bereits hinreichend bekannt ist. Dazu zählen Abofallen, verdeckte Kostenfallen etc.
  Nicht unterschätzt werden darf jedoch in diesem Zusammenhang, dass die Täter bei der Verwendung von Applikationen durch das Opfer häufig bereits die Daten des Opfers wie z.B. die Telefonnummer übermittelt bekommen, sodass eine Abbuchung direkt über die Telefonrechnung möglich wird und eine bewusste Übermittlung von Kontodaten nicht mehr erforderlich ist.

Bearbeitungsdauer:

Bei der Staatsanwaltschaft wird keine Statistik über die Bearbeitungsdauer von Verfahren durch die Polizei geführt, weshalb Zahlen insoweit nicht vorliegen. Die Bearbeitungsdauer ist naturgemäß von verschiedenen Faktoren, wie zum Beispiel Umfang des zu führenden Verfahrens, aktuelle Arbeitsbelastung etc. abhängig. Dabei ist zu berücksichtigen, dass die Dauer der Bearbeitung nur teilweise durch die Polizeibeamten zu beeinflussen ist. Dies gilt zunehmend mit einer steigenden Anzahl an zu vernehmenden Zeugen, mit denen jeweils Termine abgestimmt werden müssen. Leider zeigt die Praxis, dass hier Termine durch die zu Vernehmenden häufig nicht eingehalten werden. Auch Anfragen an Firmen werden, wenn überhaupt, häufig nur mit einer erheblichen Verzögerung beantwortet. Es ist nachteilig für die polizeiliche Bearbeitung von Ermittlungsverfahren, dass Zeugen gesetzlich nicht verpflichtet sind, auf polizeiliche Ladung zu erscheinen. Vielmehr ist es zu beobachten, dass polizeiliche Zeugenladungen häufig ignoriert werden.

Eingehende Verfahren werden bei der Polizei in der Regel zunächst ohne Einbindung der Staatsanwaltschaft bearbeitet. Nur wenn Eilmaßnahmen durchzuführen, andere Entscheidungen zu treffen sind oder das Verfahren gehobene Bedeutung hat, findet eine frühe Einbindung der Staatsanwaltschaft statt. Von einer Bearbeitungsdauer einer einfachen Betrugsanzeige mit geringer Schadenshöhe von unter einer Woche ist in der Regel nicht auszugehen.

Aufklärungsquoten:
Zum Verhältnis der Aufklärungsquoten ist zunächst auf die Antwort zu Frage 5 (S. 13) zu verweisen. Ein Vergleich von Aufklärungsquoten dürfte vor allem bei den Auswertungen zur IuK-Kriminalität im engeren Sinne aussagekräftig sein, bei denen allerdings wiederum beispielsweise die Verbreitung kinderpornographischer Schriften nicht erfasst ist.
Die Gesamtaufklärungsquote für alle Straftaten im Jahr 2009 von 55,6% und im Jahr 2010 von 56% steht den Aufklärungsquoten bei der IuK-Kriminalität im engeren Sinne von 35,2% im Jahr 2009 und 33% im Jahr 2010 gegenüber.