Stellungnahme

Bernhard Rohleder
Hauptgeschäftsführer

zum Sachverständigengespräch des Unterausschusses Neue Medien des deutschen Bundestages „Kampf gegen Darstellung von Kindesmissbrauch im Internet: technische und organisatorische Fragen“ am 25. Oktober 2010
18. Oktober 2010

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.300 Unternehmen, davon 950 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Der Unterausschuss Neue Medien des Deutschen Bundestages führt am 25. Oktober 2010 ein Sachverständigengespräch zum Thema „Kampf gegen Darstellung von Kindesmissbrauch im Internet: technische und organisatorische Fragen“ durch. Im Vorfeld dieses Gesprächs wurde ein Fragenkatalog übermittelt, der der inhaltlichen Vorbereitung des Gesprächs dienen soll. BITKOM bedankt sich für die Einladung zum Gespräch und die hiermit verbundene Möglichkeit, vorab schriftlich Stellung zu nehmen. Aufgrund des engen zeitlichen Korridors für die Beantwortung der Fragen beschränken wir uns auf die Beantwortung derjenigen Fragen bzw. Unterfragen, die aus Sicht des BITKOM von besonderer politischer Bedeutung sind.

Vorbemerkung

Einzelne der nachfolgend dargelegten Erkenntnisse stammen aus Gesprächen mit Vertretern von Ermittlungsbehörden sowie der Wissenschaft, die BITKOM im Rahmen der Debatte um das Zugangserschwerungsgesetz bzw. im Rahmen der Arbeit im Bündnis WhiteIT[1] geführt hat. Das Bündnis WhiteIT hat unter anderem beim Lehrstuhl für Strafrecht, Strafprozessrecht und Kriminologie von Prof. Meier an der Leibnitz-Universität Hannover eine kriminologische Studie zu den Verbreitungsmechanismen und der Praxis der Strafverfolgung im Bereich Kinderpornografie[2] beauftragt. Diese Studie, die von BITKOM und einzelnen unserer Mitgliedsunternehmen mitfinanziert wird, wird im April 2011 veröffentlicht werden. Sie basiert unter anderem auf einer umfangreichen, in dieser Form einmaligen Auswertung von Fallakten der deutschen Strafverfolgungsbehörden. Soweit wir hier auf Erkenntnisse im Rahmen dieser Forschungsarbeit Bezug nehmen, bilden diese bereits verfestigte Tendenzen der Untersuchung ab, die gleichwohl nicht die finalen Ergebnisse vorwegnehmen können und sollen. Wir regen gegenüber dem Unterausschuss Neue Medien bereits jetzt eine entspre-

[1] http://www.whiteit.de .
[2] Informationen zur Studie sind hier abrufbar: http://www.jura.uni-hannover.de/1154.html?&no_cache=1 .

chende Beschäftigung des Bundestages mit den Ergebnissen dieser Studie nach deren Fertigstellung im Frühjahr 2011 an.

1. **Wie gestaltet sich die Zusammenarbeit der nationalen Beschwerdestellen mit den Behörden und den Internet Service Providern in Europa und im internationalen Bereich aus? Wie lange dauert es durchschnittlich und je nach Ländern, bis Seiten gelöscht sind? Wie erklären sich die unterschiedlich langen Löschzeiten? Sind die Erfolgschancen auf schnelle Löschung gestiegen? Wie zahlreich ist das Phänomen, dass gelöschte oder gesperrte Inhalte unter anderer Quelle wieder auftauchen? Wie reagieren die Täter auf das Löschen und wie auf das Sperren? Hat sich seit Beginn der Evaluierungsphase des Zugangserschwerungsgesetzes eine Veränderung ergeben?**

Die von BITKOM vertretenen Service-Provider löschen entsprechende Angebote nach entsprechenden Hinweisen, seien es Individualhinweise von Kunden, Hinweise von Behörden oder Hinweise von Beschwerdestellen innerhalb kürzester Zeit, in der Regel von Stunden nach der Inkenntnissetzung. Die Meldung von kinderpornografischen Inhalten für Server in Deutschland kommt allerdings insgesamt sehr selten vor.[3] Bezogen auf Fälle mit einem Bezug zu in Deutschland befindlichen Servern lässt sich daher keinesfalls von einem Massengeschäft sprechen. Die Zusammenarbeit zwischen Hosting-Providern und Strafverfolgungsbehörden geschieht in den wenigen vorkommenden Fällen reibungslos.

Hinsichtlich des Phänomens des „Wiederauftauchens von Inhalten“ weisen wir darauf hin, dass in der Regel ein auf einem spezifischen WWW-Server entdeckter Inhalt bereits zum Zeitpunkt seiner Entdeckung parallel auf zahlreichen anderen Quellen verfügbar ist. BITKOM geht aufgrund der bisher mit Vertretern von Strafverfolgungsbehörden geführten Gespräche davon aus, dass die auf WWW-Ebene verfügbaren Inhalte generell bereits weit verbreitete Inhalte sind, die parallel auf anderen Servern, vor allem aber auch im großen Stil innerhalb von Peer-to-Peer-Netzen verfügbar sind. Eine „Exklusivität“ einzelner Inhalte in einem spezifischen Angebot kann daher gerade für die Verbreitung auf Ebene des World Wide Web praktisch ausgeschlossen werden.

Die breite parallele Verfügbarkeit entsprechenden Materials innerhalb von Peer-to-Peer-Netzen lässt sich mit den allein auf die Ebene des WWW abzielenden Mechanismen Sperrung bzw. Löschung nicht bekämpfen, da Peer-to-Peer-Netzwerke aufgrund ihrer strikt dezentralen Struktur hierfür keinen Anknüpfungspunkt bieten. Netzwerke wie eDonkey oder auch BitTorrent bilden nach Einschätzung des BITKOM einen der maßgeblichen Verbreitungswege kinderpornografischer Inhalte, wobei diese Verbreitung hier jeweils ohne kommerziellen Hintergrund geschieht. Die Zusammenarbeit zwischen Ermittlungsbehörden und Internetzugangsprovidern in diesem Feld betrifft im Wesentlichen die

[3] Dies entspricht den Ergebnissen der Internet Watch Foundation (IWF) für Großbritannien, http://www.iwf.org.uk/resources/trends#Reports : “Almost all the content reported to us as allegedly criminally obscene adult content was either not hosted in the UK […]”.

Beauskunftung von Klarnamen nach Übermittlung von IP-Adressen durch die Staatsanwaltschaften. Dieser Bereich der Zusammenarbeit zwischen Ermittlungs- bzw. Strafverfolgungsbehörden hat in der Praxis zahlenmäßig eine höhere Bedeutung als Löschungsaufforderungen hinsichtlich in Deutschland gehosteter Inhalte. Die Zusammenarbeit in diesem Feld funktioniert nach Einschätzung des BITKOM reibungslos, wird allerdings dadurch limitiert, dass die Speicherung der entsprechenden Session-Daten bei den Zugangsprovidern zeitlich begrenzt ist.

2. Wie viele Hinweise sind beim BKA und den Selbstkontrolleinrichtungen und Beschwerdestellen oder andere Einrichtungen zu strafbaren Inhalten nach § 184b StGB auf Webangeboten sind seit Inkrafttreten des Zugangserschwerungsgesetzes eingegangen und wie viele Fälle gingen auf Ermittlungen der Polizeibehörden zurück? Wie viele Angebote enthielten tatsächlich strafbewehrte Inhalte nach § 184b StGB? In wie vielen Fällen konnte seit Verabschiedung bzw. seit Inkrafttreten des Zugangserschwerungsgesetzes und auf wessen Veranlassung eine Löschung – und in welchem Zeitraum – derartiger Angebote erreicht bzw. nicht erreicht werden? Welche Erkenntnisse gibt es zu den Serverstandorten (aufgeschlüsselt nach länderspezifischen Erkenntnissen)? Welche Erkenntnisse gibt es zu der Frage, warum eine Löschung nicht erreicht werden konnte?

BITKOM verfügt nicht über eigene Erkenntnisse zu den Serverstandorten. Allerdings ist – u.a. durch die Analyse der britischen Internet Watch Foundation (IWF) – bekannt, dass entsprechende Inhalte in der Regel in Regionen gehostet werden, in denen die notwendige technische Infrastruktur, insbesondere die entsprechende ausreichende Breitbandanbindung gegeben ist. Daher kann nicht davon ausgegangen werden, dass die Vorhaltung entsprechenden Materials schwerpunktmäßig in abgelegenen geografischen Regionen erfolgt; vielmehr zeigt gerade die Zusammenfassung der Internet Watch Foundation einen Schwerpunkt in technologisch fortentwickelten Regionen, etwa Nordamerika und Europa (inklusive Russland).[4] Diese Erkenntnisse werden auch gestützt durch Auswertungen der teils öffentlich gewordenen Sperrlisten anderer Staaten im Hinblick auf Verteilung der Server. Diese Auswertungen belegen, dass insbesondere Nordamerika einen Schwerpunkt bildet.[5]

Ein neueres Phänomen scheinen Fallgestaltungen zu sein, in welchen an sich legale Dienste, etwa Filehosting-Services missbräuchlich temporär für die Verteilung von kinderpornografischen Inhalten genutzt werden, wobei die entsprechenden Betreiber der in dieser Form okkupierten, an sich legalen Dienste in der Regel von den Aktivitäten keine Kenntnis haben. Die IWF hat für das Jahr 2009

[4] Vgl. http://www.iwf.org.uk/resources/trends#Location .
[5] Vgl. dazu die folgenden Analysen: https://scusiblog.org/?p=807 ; https://scusiblog.org/?p=330 ; https://scusiblog.org/?p=850 .

beispielsweise 286 solcher Fälle dokumentiert und hierin eine neue Tendenz in den Verbreitungsmechanismen ausgemacht.[6]

Soweit teilweise kritisiert wird, dass Löschungen erst nach zu langer Zeit erfolgen, muss berücksichtigt werden, dass Strafverfolgungsbehörden gerade im Ausland nach Inkenntnissetzung von einem Inhalt diesen teilweise gezielt noch mehrere Tage online lassen, um die entsprechende Seite zur Ermittlung von Konsumenten zu nutzen. Wird eine Seite nach dem Hinweis nicht sofort gelöscht, ist dies daher nicht zwangsläufig ein Indiz für eine Ineffizienz von Löschmechanismen, sondern kann im Gegenteil darauf hindeuten, dass die Hinweise gezielt zur Strafverfolgung genutzt werden.

3. Es werden immer wieder Mängel wie fehlende Benachrichtigungspflichten oder Rückmeldungen an die Polizeibehörden und Selbstregulierungseinrichtungen genannt. Inwieweit können Sie diese bestätigen und konkretisieren? Wo bestehen hier konkrete Defizite bei der Zusammenarbeit der Polizeibehörden untereinander oder aber bei der Zusammenarbeit der Polizeibehörden und den Selbstkontrolleinrichtungen und inwiefern gibt es hier durch die neue Vereinbarung zur Zusammenarbeit gemäß „Harmonisierungspapier zum zukünftigen Umgang mit Hinweisen auf kinderpornografische Webseiten beim BKA, den deutschen Beschwerdestellen (eco e.V., FSM e.V., jugendschutz.net) sowie der BPjM“ Veränderungen? Wann traten die Änderungen in Kraft bzw. wann wurde das Harmonierungspapier unterzeichnet? Wie war das Prozedere vor der neuen Vereinbarung und welche Änderungen wurden mit welcher Begründung vereinbart?

BITKOM teilt die Auffassung, dass ein verlässliches Benachrichtigungs- und Rückmeldesystem einen bedeutsamen Faktor im Rahmen eines konsequenten Löschansatzes bildet. Die Studie von Moore und Clayton (vgl. Frage 11) belegt allerdings die verschiedenen Problemlagen, die bei der systematischen Erfassung der Löschvorgänge zwangsläufig gelöst werden müssten; hingewiesen sei hier etwa nur auf die Problematik der Wiedereinstellung nach einer Löschung bzw. des Umzugs ganzer Angebote auf andere URL.[7]

Soll die entsprechende Rückkontrolle durch die hiesigen Beschwerdestellen bzw. Ermittlungsbehörden selbst erfolgen hieße dies in der Praxis, dass diese Institutionen ein umfassendes eigenes Monitoringsystem für sämtliche jemals beanstandeten Inhalte vorhalten müssten – aufgrund der dezentralen Struktur der Beschwerdestellen müsste dies im Übrigen bei jeder Stelle parallel etabliert werden. Sinnvoller erscheint es hier tatsächlich, standardisierte Benachrichtigungs- und Rückmeldemechanismen zu installieren, für welche im internationalen Kontext insbesondere die entsprechenden Behörden eingebunden werden müssen. Daneben erscheint eine zentrale Verwaltung der entsprechenden Rückmeldungen sinnvoll.

[6] Vgl. http://www.iwf.org.uk/resources/trends#Hostsandhackedwebsites .
[7] Studie Moore & Clayton, S. 20 f., http://www.cl.cam.ac.uk/~rnc1/takedown.pdf .

4. Wie ist das Prozedere bei den Selbstkontrolleinrichtungen? Melden diese die fraglichen Inhalte an die zuständigen Polizeibehörden oder aber über die Partnerhotlines direkt an die entsprechenden Hostprovider? In welchem Zeitraum erfolgt eine Benachrichtigung der Polizeibehörden und der Hostprovider?

5. In welchen Intervallen und mit welchen Methoden wird überprüft, ob beanstandete Inhalte gelöscht wurden? In welchen Intervallen erfolgt eine Wiederaufforderung bei Nichtlöschung und welchen Zeitraum sehen Sie hier als sachgerecht an?

6. Wenn Aufforderungen zur Löschung beim Hosting-Provider nicht erfolgreich waren, welche alternativen Ansprechpartner haben Sie bzw. Ihre Partnerorganisationen angesprochen, und welche Ansprechpartner könnten Sie sich vorstellen?

7. Gibt es Erkenntnisse dahingehend, welche Art von Inhalten nach 184b StGB nicht zeitnah gelöscht werden können? Dies betrifft beispielsweise das Alter der Missbrauchs-Opfer und die Art der dargestellten sexuellen Handlungen.

BITKOM hat keine eigenen Erkenntnisse zu einer unterschiedlichen Behandlung bestimmter Darstellungsformen im Rahmen von Meldemechanismen. In strafrechtlicher Hinsicht schwierig umfänglich zu erfassen sind nach unserer Einschätzung weiterhin jene Darstellungsformen, die zwar nicht unmittelbar sexuellen Missbräuche dokumentieren, jedoch gleichwohl Minderjährige nackt abbilden. Inwieweit derartige Inhalte als sog. „Posenfotos“, durch das StGB erfasst werden, bleibt auch nach der Novelle des StGB 2006 teils noch auslegungsbedürftig. Insbesondere stellt sich in der Praxis offenbar teilweise die Frage, ab wann im konkreten Fall von einem „aufreizende[n] Zur-Schau-Stellen der Genitalien oder der Schamgegend von Kindern“[8], wie sie der Gesetzgeber mit der Novelle erfassen wollte, auszugehen ist. Strafverfolgungsbehörden sehen sich offenbar teils mit Darstellungsformen konfrontiert, die unter dieser Grenze bleiben, aber gleichwohl Minderjährige gezielt nackt im Stile von „Hochglanzaufnahmen“ präsentieren, ohne das die Fotos einen sexuellen Missbrauch im Sinne von § 176 StGB dokumentieren. Hier sollte ggf. in Zusammenarbeit mit den Strafverfolgungsbehörden etwaiger Klarstellungsbedarf ausgelotet werden.

8. Gibt es aussagekräftige Erkenntnisse über die Intensität von Strafverfolgungsmaßnahmen in Ländern, die über eine Sperrinfrastruktur verfügen, im Vergleich zu den Ländern, die keine Sperrung vornehmen? Mit welchen Verfahren – also Löschen oder Sperren – ist eine bessere Strafverfolgung der Täter möglich oder haben die Sperrungen Auswirkungen auf die Strafverfolgung? Lassen sich statistische Aussagen dahingehend treffen, dass die Strafverfolgung zu- bzw. abnimmt?

[8] Gesetzbegründung, BT-Drs. 16/3439, S. 9.

BITKOM liegen keine entsprechenden vergleichenden Erkenntnisse vor. Hinsichtlich der Frage der Effektivität der Verfahren Löschen bzw. Sperren im Kontext der Strafverfolgung verweisen wir auf unsere Antwort zu Frage 15.

9. Welche Erfahrungen haben Länder, in denen Netzsperren verpflichtend eingeführt wurden, bisher gemacht? In welchem Verfahren werden im Ausland die für die Liste mit Netzsperren notwendigen Daten erhoben? Wie ist sichergestellt, dass entsprechende Listen mit zu sperrenden Seiten (gelbe Seiten der Kinderpornographie) nicht in der Öffentlichkeit zugänglich gemacht werden können, wie in anderen Ländern geschehen? Ist die Anzahl der Meldungen bei den Hotlines/Behörden in den Ländern, in denen gesperrt wird, nach Einführung der Sperrung signifikant zurückgegangen?

Im Hinblick auf die Absicherung der entsprechenden Listen, die als Basis für listenbasierte Sperrverfahren unumgänglich sind, können diese zwar durch Verschlüsselungsverfahren im Rahmen der Übertragung zwischen Provider und staatlicher Stelle abgesichert werden. Dies löst aber nicht das grundsätzliche Problem des Sperransatzes, dass eine Generierung der entsprechenden Listen über reverse-engineering systemimmanent möglich bleibt, da über die angedachte Stoppseite eine Identifizierung jener Seiten möglich wird, die Bestandteil der Liste sind.

10. Welche Vor- und Nachteile hätte ein zentrales Sperrkonzept gegenüber einem dezentralen Melde- und Löschkonzept? Welchen Personalaufwand erfordern die jeweiligen Konzepte bei staatlichen Stellen?

BITKOM sieht keinerlei Vorteile eines Sperrkonzepts, da der Sperr- bzw. Zugangserschwerungsansatz als solcher gänzlich unzulänglich ist, um die Verfügbarkeit kinderpornografischer Inhalte im Internet zu begrenzen. Da die Angebote selbst auf identifizierten Servern vollständig verfügbar und mit geringstem Aufwand trotz der Zugangserschwerung erreichbar bleiben bewirken Zugangserschwerungen allenfalls Scheinsicherheit. Im Übrigen birgt die Verfügbarkeit entsprechender „Listen“ immer das Risiko ihrer Veröffentlichung, wie dies etwa im Falle der australischen, dänischen, norwegischen und thailändischen Liste bereits geschehen ist. Schließlich sind drohende Kollateralschäden wie die technisch bedingte Mitsperrung legaler Inhalte zu berücksichtigen.

Eine Einstufung des Ansatzes „Melden und Löschen“ setzt zunächst eine Auseinandersetzung mit der hierdurch verfolgten Zielsetzung voraus. Diese ist aus BITKOM-Sicht bisher unzureichend erfolgt, da im Rahmen der Erkenntnisse der Debatte um das Zugangserschwerungsgesetz der Löschansatz pauschal als Alternative zum Sperransatz diskutiert wurde. Im Rahmen einer objektiven, auf Sachlichkeit bedachten Analyse des Löschansatzes ist es daher unerlässlich, sich bereits im Ausgangspunkt auch die Grenzen eines solchen Konzepts zu vergegenwärtigen:

- Die Löschung von Inhalten betrifft immer nur den konkreten Server, die Vorhaltung des entsprechenden Inhaltes auf einem anderen Server bleibt von einer spezifischen Löschaufforderung unberührt.

- Eine Wiedereinstellung desselben oder neuer Inhalte unter der gleichen Domain wird durch Melde- und Löschverfahren nicht ausgeschlossen.

- Völlig außen vor bleiben Peer-to-Peer-Netzwerke, die keinen technischen Ansatzpunkt für eine Löschung bieten.

- Die Löschung eines Inhalts vom Server durch den Hosting-Provider kann für die Strafverfolgung kontraproduktiv sein, weil mit der Löschung der Ermittlungsansatz verlorengehen kann. Im Rahmen von Melde- und Löschkonzepten muss daher gerade das Zusammenspiel zwischen Meldeinstitution, Strafverfolgungsbehörden und Provider austariert sein, um zu verhindern, dass durch die Löschung die Ermittlungsarbeit unterlaufen wird.

Die Löschung von entsprechenden Inhalten auf öffentlich zugänglichen Webservern dient daher aus Sicht des BITKOM zum einen dem allgemeinen gesellschaftspolitischen Ziel, die Verbreitung entsprechender Inhalte zu ächten und dies durch konsequentes Vorgehen zu dokumentieren. Zum anderen dient sie bei sachgerechter Koordinierung einer effektiveren Strafverfolgung der Konsumenten und ggf. der Distributoren. Hinsichtlich der Betreiber stellt sich allerdings in der Praxis regelmäßig das Problem, dass diese aufgrund unrichtiger Whois-Angaben und weiterer Verschleierungsmechanismen nicht identifizierbar sind, so dass als Ermittlungsansatz allenfalls etwaige Zahlungsströme verbleiben, wenn es sich um ein kommerzielle betriebenes Angebot handelt. Dieses Problem von Domainregistrierungen unter falscher Identität ist eine internationale Herausforderung, da für jede nationale Domain eigenständige Registrare zuständig sind, wobei die Anforderungen an die Identifizierung eines Domaininhabers variieren. Allein aus Deutschland heraus wird diese Problem nicht in den Griff zu bekommen sein, da die von der Denic verwalteten de-Domains typischerweise nicht für entsprechende Plattformen genutzt werden.

11. In einer Untersuchung im Juni 2008 legten Tyler Moore und Richard Clayton von der University of Cambridge dar, dass Seiten mit kinderpornographischem Inhalt eine längere Lebensdauer hätten als andere illegale Webangebote wie z.B. *phishing-sites*. Dies begründeten Sie vor allem mit der damals mangelhaft koordinierten internationalen Kooperation. Worin liegen die Hauptgründe für die unterschiedlichen Zeiten, die das Löschen der jeweiligen Inhalte benötigt? Wäre beispielsweise ein verbessertes *notice-and-take-down*-Verfahren ein gangbares Mittel, um die Entfernung von Missbrauchsdokumenten analog zur Entfernung von *phishing-sites* durchzuführen?

BITKOM teilt grundsätzlich die Auffassung, dass die internationale Zusammenarbeit im Bereich der Kinderpornografiebekämpfung unzureichend ist; dies

betrifft insbesondere die Zusammenarbeit der Strafverfolgungsbehörden untereinander. Moore und Clayton bezogen sich in Ihrer Untersuchung[9] auf die Praxis der Internet Watch Foundation (IWF) in Großbritannien und die Tatsache, dass diese ihre Erkenntnisse zunächst an Strafverfolgungsbehörden gebe und nicht direkt an die Provider herantrete, wie dies Banken im Falle von Phishing-Seiten tun. Hierin sahen Moore & Clayton ein Defizit. Aus Sicht des BITKOM ist hierzu zunächst darauf hinzuweisen, dass die von Moore & Clayton durchschnittlich ermittelte Dauer von 30 Tagen bis zur Löschung eines kinderpornografischen Inhaltes im Hinblick auf deutsche Hosting-Anbieter keinesfalls zutrifft; wir verweisen auf unsere Antwort zu Frage 1.

Außerdem sollte aus der Studie von Moore und Clayton nicht unmittelbar der Schluss gezogen werden, allein ein ausschließlich auf direkte Kooperation von Beschwerdestellen und Host-Providern setzendes System arbeite effizient. Zum einen bedarf es auch in einem solchen Verfahren jedenfalls einer standardisierten Koordinierung der Aktivitäten der Ermittlungsbehörden, um zu verhindern, dass bei deren Einschaltung die Löschung bereits vonstatten und somit mit der Löschung auch etwaige Ermittlungsansätze verloren gegangen sind. Zum anderen hängt die Schlussfolgerung von Moore & Clayton damit zusammen, dass die Arbeit der Ermittlungsbehörden heute offenbar angesichts fehlender koordinierender Strukturen und teils auch fehlender personeller Ressourcen zu langsam geschieht. Moore und Clayton weisen in ihrer Studie gerade auf die Ineffizienz dieser staatlichen Strukturen explizit hin und verorten dort das eigentliche Problem.[10] Es bedarf daher gerade eines Systems, welches die möglichst schnelle Löschung von Inhalten mit einer effizienten Strafverfolgung verbindet. Auch ist der direkte Kontakt der Beschwerdestellen mit Host-Providern nur dort möglich, wo ein entsprechender Kanal, etwa über das Beschwerdestellennetzwerk auch tatsächlich besteht. Wo dies nicht der Fall ist, bleibt auch heute nur der Weg über die jeweiligen nationalen staatlichen Behörden; schon aus diesem Grund muss die Stärkung dieses Bereichs im Vordergrund der politischen Bemühungen stehen.

Als Lösung kommt aus Sicht des BITKOM ein möglichst europaweit und mittel- bis langfristig international organisiertes und standardisiertes Meldesystem durch eine Behörde wie Europol in Betracht, die nach einheitlichen Verfahren auf Hinweis durch die nationalen Ermittlungsbehörden, nationalen Beschwerdestellen oder deren Verbundorganisation an die entsprechenden Hosting-Provider herantritt. Eine solche Lösung hätte den Vorteil klar definierter Zuständigkeiten und Abläufe bzgl. des Notice-and-Takedown-Verfahrens. Provider würden nicht durch verschiedenste nationale Beschwerdestellen kontaktiert, sondern immer von ein und derselben Institution in einem standardisierten Verfahren adressiert. Dies würde auch die Rechtssicherheit für die Provider erhöhen, die selbst keine rechtliche Bewertung entsprechender Inhalte vornehmen können und dürfen. Voraussetzung für das Funktionieren eines solchen Systems bilden allerdings entsprechende Strukturen bei Europol, die eine extrem schnelle Bearbeitung

[9] http://www.cl.cam.ac.uk/~rnc1/takedown.pdf .
[10] Studie von Moore & Clayton, S. 22, http://www.cl.cam.ac.uk/~rnc1/takedown.pdf .

sicherstellen. In einem solchen Verfahren würde zwangsläufig auch der Informationsaustausch zwischen Selbstregulierungsinstitutionen, Providern, nationalen Ermittlungsbehörden und Europol verbessert, so dass auch eine höhere Effizienz der Strafverfolgung im europäischen bzw. internationalen Kontext erwartet werden darf. Die Lösung würde überdies eine statistische Auswertung der Maßnahmen erleichtern, da bei Europol als zentraler Zwischenstelle sämtliche Informationen zusammenlaufen würden.

Mittel- bis langfristig müsste dieses System angesichts der Konzentration kinderpornografischer Inhalte auf Servern außerhalb der EU jedoch internationalisiert werden, d.h. letztlich internationale Vereinbarungen zur Kooperation der Ermittlungsbehörden in Fällen kinderpornografischer Inhalte geschlossen werden.

BITKOM sieht daher insgesamt nach wie vor die schwerfällige und stark bürokratisierte Zusammenarbeit der Strafverfolgungsbehörden selbst innerhalb der europäischen Union als Kernproblem der sehr schleppenden Ermittlungsarbeit und teilweise nicht konsequente erfolgenden Löschung von Inhalten an. Wir sehen mit Besorgnis, dass die EU nun offenbar erwägt, statt dieses grundsätzliche Problem anzugehen, das Instrument der Zugangserschwerung als Lösung zu etablieren. Angesichts der bekannten Unzulänglichkeiten des Zugangserschwerungsansatzes muss ein solcher Vorstoß letztlich als politische Kapitulation vor dem eigentlichen Problem einer konsequenten organisatorisch wie technologisch vernetzten Zusammenarbeit der Ermittlungsbehörden in Europa bewertet werden. BITKOM begrüßt daher nachdrücklich, dass sich die Bundesregierung nunmehr auf europäischer Ebene gegen diesen Vorstoß und stattdessen für ein effizientes Melde- und Löschsystem ausgesprochen hat, in dessen Rahmen auch die Zusammenarbeit der Ermittlungsbehörden, insbesondere mit Drittstaaten verbessert werden soll.

12. Wie kann die Zusammenarbeit zwischen den Strafverfolgungsbehörden, den Selbstregulierungskräften der Privatwirtschaft wie INHOPE und den Internet Service Providern weiter verbessert werden?

Aus Sicht des BITKOM ist es von entscheidender Bedeutung, dass klare Regularien im Hinblick auf die Zusammenarbeit der Selbstregulierungsstellen bzw. der Wirtschaft und den Strafverfolgungsbehörden geschaffen werden, wobei zunächst eine europaeinheitliche und mittel- bis langfristig eine weltweit koordinierte Strategie erforderlich ist, vgl. auch unsere Antwort zu Frage 12.

Im Hinblick auf die Arbeit von Selbstkontrolleinrichtungen und insbesondere Beschwerdestellen regen wir spezifisch an, zu prüfen, inwieweit das geltende Strafrecht Mitarbeiter von Beschwerdestellen im Rahmen ihrer Prüftätigkeit mit Strafbarkeit bedroht. Durch die Entscheidung des Oberlandesgerichts Hamburg vom 15.2.2010[11] wurde festgestellt, dass bereits das Anklicken bzw. Betrachten kinderpornografischer Inhalte strafbar ist, da auch das kurzfristige Herunterladen

[11] OLG Hamburg, Urt. V. 15. Februar 2010, Aktenzeichen: AZ: 2-27/09 REV .

in den Arbeitsspeicher, ohne ein manuelles Abspeichern, den jeweiligen Nutzer in den „Besitz der Dateien“ bringe. Vor dem Hintergrund dieses Urteils lässt sich der Ausschluss der Strafbarkeit nach § 184b Abs. 4 StGB im Rahmen der Arbeit der Mitarbeiter der Beschwerdestellen allenfalls über den Ausnahmetatbestand des § 184b Abs. 5 StGB[12] rechtfertigen, dessen konkrete Reichweite allerdings auslegungsfähig ist.

BITKOM geht zwar grundsätzlich davon aus, dass die entsprechende Arbeit der Beschwerdestellen sowohl von politischer Seite, als auch von Seiten der involvierten Strafverfolgungsbehörden, insbesondere des BKA, grundsätzlich anerkannt ist. Um aber jede Restunsicherheit zu beseitigen, regt BITKOM an, eine gesetzliche Klarstellung im Hinblick auf die Tätigkeit der Mitarbeiter anerkannter Selbstkontrolleinrichtungen zu schaffen. Da Selbstkontrolleinrichtungen europaweit arbeiten, sollte diese Frage nicht zuletzt auch zum Gegenstand europäischer Harmonisierungsbemühungen gemacht werden, wofür sich die Bundesregierung im Rat einsetzen sollte.

13. Welche Erkenntnisse gibt es darüber, ob und inwieweit es einen kommerziellen Markt für diese Inhalte nach § 184 b gibt?

Die Frage der Existenz eines kommerziellen Marktes für kinderpornografische Inhalte im Internet und vor allem dessen Umfang muss aus Sicht des BITKOM als ungeklärt bewertet werden. Wir teilen insoweit die Einschätzung der European Financial Coalition against commercial sexual exploitation of children online (EFC)[13], wonach die verfügbaren Indizien eher gegen einen kommerziellen Massenmarkt sprechen. Neben der Studie der EFC sind uns bislang vor allem die Berichte der britischen Internet Watch Foundation (IWF) bekannt, deren Analyse ebenfalls kein verlässliches Bild im Hinblick auf den absoluten Umfang und den Anteil kommerzieller Angebote zeichnen können.[14]

Zwar belegen einzelne Ermittlungserfolge von Strafverfolgungsbehörden auch in Deutschland, dass es Konsumenten gibt, die für den Zugang zu entsprechenden Angeboten, in der Regel in Form von Abonnements zu spezifischen Angeboten auf WWW-Ebene, Zahlungen leisten. Es kann daher zwar grundsätzlich davon ausgegangen werden, dass es auch Angebote mit kommerziellem Hintergrund gibt. Welchen Umfang diese Angebote haben und welchen Anteil kommerziell betriebene Angebote im Verhältnis zu der dezentralen Verbreitung über Peer-to-Peer-Netzwerke oder der Verbreitung in Tauschringen und ähnlichen Vereinigungen haben, in denen entsprechend veranlagte Täter ohne kommerziellen Hintergrund kinderpornografisches Material austauschen, ist nach unserem Kenntnisstand bislang nicht empirisch belastbar erforscht. Politische Aussagen aus der Diskussion um das Zugangserschwerungsgesetz, wonach es sich um einen „Milliardenmarkt“ handeln soll, werden von uns als übertrieben und speku-

[12] Wortlaut § 184b Abs. 5 StGB: „Die Absätze 2 und 4 gelten nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.“
[13] http://www.ceop.police.uk/Documents/EFC%20Strat%20Asses2010_080910b%20FINAL.pdf .
[14] Vgl. etwa die WF Operational Trends 2009, http://www.iwf.org.uk/resources/trends#Reports .

lativ bewertet; sie wurden bislang nicht empirisch nachgewiesen. BITKOM geht auf Basis von Gesprächen mit Vertretern von Strafverfolgungsbehörden stattdessen davon aus, dass eine Vielzahl der Delikte in Bezug auf kinderpornografisches Material keinen kommerziellen Hintergrund hat, sondern von pädophil veranlagten bzw. Tätern, die als „Sammler“ zu klassifizieren sind, begangen wird.

BITKOM ist Mitbegründer des 2009 ins Leben gerufenen Bündnisses WhiteIT unter Federführung des Niedersächsischen Innenministeriums. Im Rahmen dieses Projekts erstellt die Uni Hannover derzeit eine kriminologische Studie zu Tätertypen, Strukturen und Verbreitungsmechanismen kinderpornografischer Inhalte im Netz. Im Rahmen dieser Studie werden erstmals überhaupt umfassend Fallakten der Staatsanwaltschaften systematisch ausgewertet, auch um die Frage der Kommerzialisierung der Verbreitung von Kinderpornografie im Internet auszuwerten. Die Studie ist derzeit noch nicht abgeschlossen, jedoch lässt sich als erste Tendenz klar erkennen, dass der Kommerzialisierungsgrad im ermittlungstechnisch erfassten „Hellfeld“ als sehr gering zu bewerten ist. Zwar gibt es vereinzelt entsprechende Angebote, die gegen Bezahlung im Rahmen eines „Mitgliedschaftsmodells“ entsprechende Inhalte verfügbar machen, jedoch bilden solche Angebote im Rahmen der Ermittlungsarbeit der Behörden die klare Ausnahme. Dabei spielt unter anderem eine Rolle, dass kommerzielle Angebote aufgrund der bei Zahlungsvorgängen anfallenden Spuren eine höhere Entdeckungsgefahr sowohl für den Anbieter als auch für die Kunden mit sich bringen. Außerdem sind die in entsprechenden Angeboten bereit gestellten Inhalte in den seltensten Fällen „exklusiv“ verfügbar, sondern in der Regel Sammlungen bereits weit verbreiteter Videos oder Bilder, die insbesondere auch in Peer-to-Peer-Netzwerken zirkulieren, weshalb die Ermittlung innerhalb dieser Tauschbörsen eher einen Schwerpunkt der Arbeit der Behörden bildet.

BITKOM geht demnach davon aus, dass die Analyse eines etwaigen „Marktes“ für kinderpornografische Inhalte inner- und außerhalb des Internets jedenfalls weiterer, insbesondere auch international ausgerichteter, Untersuchungen bedarf. Nur auf Basis konkreter Kenntnisse zu den Verbreitungsmechanismen und Täterstrukturen kann eine sinnvolle internationale Strategie in der Bekämpfung der entsprechenden Verbrechen entwickelt werden.

14. Welche Maßnahmen sind sinnvoll und geboten, um gegen die aktive Nachfrage vorzugehen?

Bei der Evaluation von Maßnahmen zur Eindämmung der Nachfrage muss berücksichtigt werden, dass die Gründe für Konsum von kinderpornografischem Material je nach Tätertyp verschieden gelagert sind. Aus Sicht des BITKOM kann es daher nicht eine einzige Strategie der Nachfragebekämpfung gehen, sondern es müssen verschiedenste Maßnahmen gebündelt werden. Offensichtlich ist dies in Bezug auf tatsächlich pädophil veranlagte Täter, für die aus medizinischer Sicht davon auszugehen ist, dass die entsprechende Prägung dauerhaft und unveränderbar vorliegt. Hinsichtlich entsprechender Tätertypen können

strafrechtliche Sanktionsmechanismen nur einen Teil des Instrumentariums bilden. Ebenso bedeutsam sind therapeutische Angebote, die insbesondere therapiebereiten Tätern schon vor der Erstbegehung von Straftaten Hilfestellung im Umgang mit der entsprechenden Prägung geben, um gerade die Begehung von Straftaten, seien es Missbräuche oder Straftaten im Kontext von § 184b StGB zu verhindern.

Zu betonen ist schließlich, dass die Nachfragebekämpfung allein keine hinreichende Strategie im Kampf gegen sexuellen Missbrauch bildet. Wir verweisen hierzu auf die Ausführungen zu Frage 15.

15. Mit welchem Verfahren (Sperren oder Löschen) können die Täter strafrechtlich besser verfolgt werden?

Aus Sicht des BITKOM sollten beide Instrumente nicht schwerpunktmäßig anhand einer Verbesserung der Strafverfolgung bewertet werden. Die Diskussion um die Zugangserschwerung oder auch Entfernung strafrechtlich relevanten Materials hat nach unserer Einschätzung den Blick für die Hürden bei der eigentlichen Verfolgung der Täter verdeckt. Sowohl dem Instrument der Zugangserschwerung als auch der Löschung von Inhalten liegt eine rezipientenorientierte Wirkung dergestalt zugrunde, dass „lediglich“ der Zugang zu entsprechendem Material über das World Wide Web erschwert wird. Die strafrechtliche Perspektive berühren beide Instrumente unmittelbar allenfalls dergestalt, als die Begehung des Straftatbestands „Besitz von Kinderpornografie“ für die jeweils konkret in Rede stehenden Inhalte erschwert wird. Beschränkt auf diesen Kontext kann die Bewertung erfolgen, dass eine Löschung das effektivere Mittel ist, da Zugangserschwerungsmechanismen auf dem Access-Level immer umgehbar sind, so dass diese gerade für gezielt agierende Täter keinerlei ernstzunehmende Hürden bilden.

Bedeutsamer als diese Feststellung ist allerdings die Grunderkenntnis, dass für die eigentlich relevanten Straftaten im Kontext des Problemkreises „Kinderpornografie“ beide Instrumente keine Wirkung zeitigen können, da sie notwendigerweise zu spät ansetzen. Denn weder Zugangserschwerungsmechanismen noch die Löschung von Inhalten sind geeignet, die auf entsprechendem Material dokumentierten Missbräuche zu verhindern. Die Fragestellung belegt insoweit eine generelle Schieflage der durch das Zugangserschwerungsgesetz angestoßenen Debatte um die Bekämpfung des sexuellen Missbrauchs von Kindern und den Problemkreis Kinderpornografie: Die Annahme, dass die Bekämpfung der Verfügbarkeit entsprechender Inhalte im Internet gewissermaßen rückwirkend die Begehung von Missbräuchen und die Herstellung von Bild- und Videomaterial einzudämmen geeignet sei, geht aus Sicht des BITKOM fehl und ist empirisch nicht belegbar. Eine rein nachfrageorientierte Bekämpfungsstrategie kann Rückwirkungen auf das Angebot allenfalls für den kleinen Bereich kommerzieller Angebote zeitigen. Im Bereich anders motivierter Tätertypen, insbesondere tatsächlich pädophil veranlagter Personen und „Sammlern“ führt die Bekämpfung der Nachfrage dagegen nicht zu einer Verringerung des Angebotes, da die

Motivation derartiger Täter überhaupt nicht dem Prinzip von Angebot und Nachfrage unterliegt. Eine auf Nachfrageeindämmung zielende Strategie vermag die Problematik außerdem auch deshalb nicht zu lösen, weil die in Betracht kommenden Maßnahmen einer Zugangserschwerung wie auch der Löschung letztlich immer nur auf einen einzelnen spezifischen Verbreitungsweg, in der Regel das World Wide Web, abzielen; sämtliche anderen Verbreitungswege werden dagegen nicht tangiert.

BITKOM warnt daher davor, den Eindruck zu vermitteln, dass derartige Maßnahmen geeignet seien, die eigentlich zugrunde liegenden Verbrechen einzudämmen. Weder Zugangserschwerung noch die Löschung von Inhalten entlasten Politik und Ermittlungsbehörden davon, verstärkte Anstrengungen der internationalen Zusammenarbeit zu unternehmen, um bereits die Produktion entsprechenden Materials konsequenter zu bekämpfen. Eine ernstgemeinte staatliche Initiative muss eben diesen Aspekt in den Vordergrund stellen und darf die Eindämmung der nachgelagerten Verbreitungsvorgänge letztlich nur als bedeutsame, aber flankierende Maßnahmen begreifen.

BITKOM weist abschließend darauf hin, dass hiermit keineswegs die bisherige Arbeit von Beschwerdestellen und Ermittlungsbehörden in Frage gestellt werden soll. Vielmehr unterstützen wir nachdrücklich eine konsequente Löschung entsprechender Inhalte. Dies gründet sich jedoch nicht schwerpunktmäßig in der Annahme einer Stärkung der Strafverfolgung, sondern vor allem in dem damit verbundenen gesellschaftspolitisch notwendigen Signal, dass die Perpetuierung der entsprechenden Missbräuche durch die Verfügbarkeit des Materials nicht geduldet wird.