Alvar C.H. Freude

Stellungnahme zu Internet-Sperren

Unterausschuss Neue Medien: Gespräch mit Sachverständigen zum Thema „Kampf gegen Darstellung von Kindesmissbrauch im Internet: technische und organisatorische Fragen“

Version 1.0 vom 21. Oktober 2010

Arbeitskreis gegen Internet-Sperren und Zensur
http://ak-zensur.de/

AK Zensur | c/o Alvar Freude | Fideliostraße 16 | 70597 Stuttgart | (01 79) 13 46 47 1

Vorbemerkung und Zusammenfassung

Sexueller Missbrauch gehört zum Furchtbarsten, was man einem Kind antun kann. Man möchte sich eine solche Tat am liebsten gar nicht vorstellen. Gerade deshalb ist es notwendig, sie effektiv und nachhaltig zu bekämpfen.

„Kinderpornografie“ als Bezeichnung für die Darstellung dieser Taten klingt für die Opfer oft zu verharmlosend. Deshalb sollte besser von Darstellungen sexuellen Missbrauchs von Kindern gesprochen werden.

Es ist höchste Zeit, dass diese Darstellungen auch im Internet effektiv bekämpft werden. Die alte Bundesregierung hat dafür einen Weg gewählt, der nach damaliger Kenntnislage zwar naheliegend war, sich aber zwischenzeitlich als nicht zielführend herausgestellt hat und daher von Anfang an kritisert wurde. So hat sich in Deutschland die Erkenntnis durchgesetzt, dass Internetsperren nicht effektiv sondern kontraproduktiv, ungenau und technisch ohne großen Aufwand zu umgehen sind. Sie leisten somit keinen Beitrag zur Bekämpfung der Kinderpornographie, sind verfassungsrechtlich zumindest bedenklich und schaffen zudem eine Infrastruktur, die von vielen zu Recht mit Sorge gesehen wird. Da es bessere, nachhaltigere, grundrechtsverträglichere und gleichzeitig strengere Maßnahmen gibt, sind Sperren gleichzeitig unnötig.

Bei der Verabschiedung des Zugangserschwerungsgesetzes ist der Deutsche Bundestag noch davon ausgegangen, dass einschlägige Webseiten nahezu ausschließlich in so genannten „failed states“ ins Internet gestellt werden, also Staaten, in denen so gut wie keine Strafverfolgung und damit auch keine Löschung möglich ist. In der Antwort vom 15. Juni 2009 auf auf die Kleine Anfrage der FDP-Bundestagsfraktion (Drucksache 16/13347) schrieb die damalige Bundesregierung:

> *Webseiten mit nach deutschem Recht als kinderpornografisch einzustufenden Inhalten werden nach Erkenntnissen des BKA fast ausschließlich über Server im Ausland bereitgestellt und dort bevorzugt in Staaten mit geringer Kontrollintensität oder aber dort, wo keine diesbezügliche Gesetzgebung existiert oder die entsprechenden Regelungen nicht konsequent durchgesetzt und überwacht werden.*

In der Zwischenzeit ist aber klar, dass die Inhalte hauptsächlich aus den USA und Westeuropa stammen, die Server also an Orten stehen, wo sehr wohl Recht durchgesetzt werden kann. Dies wird auch aus der Antwort des BKA an MdB Edelgard Bulmahn vom 9. Juni 2009 klar.[1] Trotz dieser Erkenntnis vom Juni 2009 hat BKA-Präsi-

[1] Siehe Anlage C: Demnach stammt die überwiegende Mehrheit der in Dänemark gesperrten Webseiten aus den USA. Auf Platz 2 war Deutschland mit 199 Einträgen.

dent Ziercke noch im August 2009 öffentlich behauptet, die Inhalte würden überwiegend aus „failed states“ verbreitet.[2]

Bei der automatischen Analyse verschiedenster bekannter Sperrlisten aus mehreren Ländern stellte sich bereits 2009 heraus, dass keine einzige Webseite aus einem „failed state“ stammt.[3]

Im September 2010 habe ich erneut einen repräsentativen Teil der tagesaktuellen Sperrliste aus Dänemark untersucht. Um die Probleme der Strafbarkeit beim Aufruf entsprechender Seiten zu umgehen hatte ich Unterstützung von anonymen Helfern aus Skandinavien. **Von den untersuchten 167 Webseiten verbreiteten nur drei Kindesmissbrauchsbilder.** Zwei davon waren seit mehreren Jahren auf verschiedenen skandinavischen Sperrlisten. **Nach Meldung an den Hosting-Provider in den USA konnte ich selbst an einem Freitag, mitten in der Nacht, innerhalb von 30 Minuten eine Löschung erreichen.** Eine weitere Webseite mit Server in den Niederlanden war seit Monaten auf der schwedischen und dänischen Sperrliste verzeichnet. **Nach dem Verschicken eines entsprechenden Hinweises wurde sie innerhalb von drei Stunden von der zuständigen indischen Domainvergabestelle (Registry) abgeschaltet.** Die Dokumentation dazu findet sich in Anlage B.

Auf einen Punkt ist noch hinzuweisen: die Diskussion um das „Sperren“ von Webseiten betrifft nur offen und öffentlich zugängliche Webseiten. Diese machen aber nach allen bekannten Erkenntnissen nur einen kleinen Teil der Verbreitung von Missbrauchsdarstellungen im Internet aus, da der überwiegende Teil über andere Kanäle verbreitet wird.

Eine weitergehende grundsätzliche nicht-technische/organisatorische Stellungnahme finden Sie anbei in Anlage A.

[2] http://www.heise.de/newsticker/meldung/BKA-Chef-Umgehen-von-Kinderporno-Sperren-ist-strafbar-752033.html

[3] vgl. auch die Karten in Anlage D

Antworten zu den Fragen

Im Folgenden gehe ich auf die Aspekte zu den Fragen ein, zu denen mir belastbare Kenntnisse vorliegen.

Frage 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?*

Antwort: Nach hiesiger Erfahrung lassen sich Webseiten, die den sexuellen Missbrauch von Kindern darstellen, sehr schnell entfernen.[4] Die vom BKA berichteten schlechten Erfahrungen lassen sich auf eine nicht optimale internationale Zusammenarbeit, bürokratische Verfahren und das Kontaktieren der falschen Ansprechpartner zurückführen. Hier bedarf es einer deutlich verbesserten Zusammenarbeit der Polizei- und Strafverfolgungsbehörden auf nationaler wie auch auf internationaler Ebene. Auch hat es sich als hinderlich erwiesen, dass sich die Polizeibehörden und das BKA ausschließlich an die ausländischen Polizei- und Sicherheitsbehörden gewandt haben, nicht aber an die ausländischen Hosting-Provider. Zudem gab es nach Auskunft des BKA oftmals auch keinerlei Rückmeldung über den Fortgang der Ermittlungen im Ausland. Derartige Verfahrensabläufe müssen dringend überprüft und effizienter werden, um die Löschung der Inhalte in kürzester Zeit zu erreichen.

So kann die Wahl des Ansprechpartners das Handeln beschleunigen oder verzögern. Viele Missbrauchsabteilungen der Provider werden von anderen Anfragen und Beschwerden (beispielsweise zum Thema Spam) überschwemmt, so dass einzelne Hinweise untergehen können. Wenn gar die falschen Ansprechpartner kontaktiert werden, verzögert sich die Bearbeitung weiter. Hier wäre die Einrichtung von direkten Kontaktstellen oder telefonisches Nachfragen sehr hilfreich.

Mit dem Memorandum bezüglich einer verbesserten Zusammenarbeit, wie es derzeit zwischen den Selbstkontrolleinrichtungen und dem BKA abgestimmt wird, sollen entsprechende Strukturen geschaffen werden. Diese sind auch dringend geboten, denn die jetzigen Verfahrensabläufe führen dazu, dass Seiten, die binnen kürzester Zeit gelöscht werden könnten, weiter online bleiben.

---

[4] Siehe Anlage B; auch online verfügbar unter http://ak-zensur.de/2010/09/29/analysis-blacklists.pdf

Aber auch die Art der beanstandeten Bilder und Videos sowie das Alter der abgebildeten Personen kann zu Verzögerungen führen, schon aus Gründen der Rechtssicherheit: handelt es sich nicht um eindeutige Fälle, sind u.U. genaue rechtliche Prüfungen nötig. So ist es bei älteren Jugendlichen und jungen Erwachsenen nicht einfach, anhand von Bildern ein korrektes Alter zu bestimmen. Insofern können die Polizeidienststellen unterschiedlicher Länder zu unterschiedlichen Ergebnissen kommen. Bei den viel zitierten Darstellungen von real vollzogenem Kindesmissbrauchs gibt es hingegen kaum Differenzen – diese können weltweit verfolgt werden.

Ein anderes Beispiel: Im Mai 2009 schrieb ich in einem automatisierten Verfahren alle Hosting-Provider an, die für Webseiten verantwortlich waren, die auf verschiedenen Sperrlisten standen.[5] Eine inhaltliche Kontrolle fand nicht statt. Am 26. Mai 2009 um 0:31 Uhr wurde durch das von mir entwickelte Programm eine Hinweis-E-Mail an einen Provider in Luxemburg verschickt. Um 1:50 Uhr kam die erste Antwort: Nach Einschätzung des Mitarbeiters im Nachtdienst würde es sich um eventuell strafbare Inhalte handeln, aber er sei sich nicht sicher. Am nächsten Morgen würde er die Polizei kontaktieren und dies klären. Die betreffende Webseite enthielt Fotos von durchgehend komplett bekleideten Kindern in teilweise sexuellen Posen. Am Mittag des 26. Mai um 12:02 kam die Rückmeldung: Die Polizei stuft die Inhalte nicht als illegale Kinderpornografie ein. Aber der Provider werde dem Kunden trotzdem fristgerecht zum Ende des Monats kündigen.

Dass bei legalen Inhalten keine Löschung erfolgt, ist nicht nur nachvollziehbar, sondern auch korrekt. Solche Probleme treten aber keinesfalls bei den in der Öffentlichkeit immer wieder zitierten harten Missbrauchsdarstellungen auf.

Die Antwort auf die Frage, ob gelöschte Inhalte wieder auftauchen, lässt sich nicht verallgemeinern. Einige Täter wollen nur provozieren, in einschlägigen Diskussionsforen Aufmerksamkeit erzeugen oder einer eingeschränkten Gruppe von Personen die Inhalte bereit stellen. Da der Täter damit seinen Zweck erreicht hat, stellt er selbst die Inhalte nicht wieder ins Netz ein. Aber diejenigen, die sie heruntergeladen haben, verbreiten sie eventuell wieder über andere Wege. Weder eine Sperrung noch die Löschung kann sie daran hindern, da hilft nur die Verfolgung der Täter.

Andere Täter wollen dauerhaft Inhalte verbreiten. Sie stellen diese immer wieder unter neuen Adressen ins Netz ein. Auch hier kann nur eine Verfolgung der Täter nachhaltig wirken. Insbesondere ist es wichtig, Spuren und Beweise zu sichern. Bei Sperren kann dies nicht erfolgen, da der Hosting-Provider des Täters davon gar nichts erfährt. Beim Löschen werden die Inhalte nicht vernichtet, sondern beschlagnahmt und dem Zugriff der gesamten Öffentlichkeit entzogen, beispielsweise in dem der Server

[5] http://ak-zensur.de/2009/05/loeschen-funktioniert.html

vom Netz getrennt wird. Daher beschreiben beide Begriffe das tatsächliche Handeln nur unzureichend.

Frage 2: *Wie viele Hinweise sind beim BKA und den Selbstkontrolleinrichtungen und Beschwerdestellen oder andere Einrichtungen zu strafbaren Inhalten nach § 184 b StGB auf Webangeboten seit Inkrafttreten des Zugangserschwerungsgesetzes eingegangen, und wie viele Fälle gingen auf Ermittlungen der Polizeibehörden zurück? Wie viele Angebote enthielten tatsächlich strafbewehrte Inhalte nach § 184 b 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?*

Antwort: Der AK Zensur hat diverse Erkenntnisse, die aus der Analyse von Sperrlisten anderer Länder herrühren. Gemeinsam ist allen Analysen, dass die Server im Wesentlichen in den USA, Westeuropa, Kanada und Russland stehen. Deutschland ist in der Regel je nach Sperrliste der zweit- bis vierthäufigste Server-Standort.

Auch das BKA hatte diese Erkenntnisse bereits im Sommer 2009, wie aus einem Schreiben an MdB Edelgard Bulmahn[6] hervorgeht:

Land	Anzahl an Domains
USA	1148
Deutschland	199
Niederlande	79
Kanada	57
Russland	27
Japan	20
Korea	19
Tschechien	15
Großbritannien	14

[6] siehe Anlage C

Eine im Internet veröffentlichte Analyse der finnischen Sperrliste[7] kommt zu ähnlichen Ergebnissen. In Anlage D finden Sie weitere Auflistungen, die ebenfalls zu ähnlichen Ergebnissen kommen: primäres Hosting-Land sind die USA, gefolgt von Westeuropa einschließlich Deutschland.

In den letzten Monaten ist zu beobachten, dass die Sperrlisten aus den skandinavischen Ländern immer kleiner werden. 2008 und 2009 umfassten sie in der Regel noch mehrere tausend Seiten, enthalten sie in der Zwischenzeit oftmals nur noch wenige hundert Einträge:

Land, Sperrliste von	Anzahl
Dänemark, Februar 2008	3863
Norwegen, 18. März 2009	3518
Dänemark, Ende 2009	>5000
Schweden, Anfang 2010	1697
Schweden, 25. Mai 2010	323
Dänemark, 23. Juni 2010	636
Dänemark, 20. Oktober 2010	328

Dies lässt sich damit erklären, dass die Listen in der Zwischenzeit bereinigt wurden, nachdem zuvor immer nur neue Domains dazu kamen, ohne die alten zu überprüfen. Dies ist auch ein Grund für die teilweise kommunizierten hohen Zugriffszahlen.

Die aktuell (Stand 20. Oktober 2010) in Dänemark blockierten Webseiten kommen primär aus den USA (134 Einträge) gefolgt von Europa (20) Einträge und Kanada sowie Russland (je 13 Enträge). Die komplette derzeitige Sperrliste im Detail:

Land	Anzahl an Domains
USA	134
Offline (keine IP)	124
Russland	13
Kanada	13
Ungültige IP	11
Deutschland	11
Südkorea	4

[7] http://maraz.kapsi.fi/sisalto-en.html

Land	Anzahl an Domains
China	3
Schweden	2
Niederlande	2
Japan	2
Großbritanien	2
Tschechien	2
Ukraine	1
Türkei	1
Bahamas	1
Kuweit	1
Frankreich	1
Summe	328

Wenn eine Löschung der Inhalte nicht erreicht wurde, liegt dies nach unserer Kenntnis entweder daran, dass es nicht versucht wurde, die falschen Ansprechpartner kontaktiert wurden oder weil es sich um Darstellungen handelt, die gerade noch legal sind. Eine Analyse vom September 2010 zeigte, dass von einer Stichprobe von 167 in Dänemark blockierten Webseiten nur drei kinderpornografische Darstellungen enthielten. Zwei davon waren seit mindestens 2008 auf der Sperrliste verzeichnet und konnten nach Meldung an den Host-Provider innerhalb von 30 Minuten gelöscht werden. Eine weitere Domain mit indischer Länderkennung war mindestens seit Anfang 2010 auf der Sperrliste, und wurde in den Niederlanden gehostet. Nach Meldung an die indische Registry wurde die Domain innerhalb von drei Stunden abgeschaltet (siehe auch Anlage B).

Frage 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 Harmonisierungspapier unterzeichnet? Wie war das Prozedere vor der neuen Vereinbarung und welche Änderungen wurden mit welcher Begründung vereinbart?

Antwort: Aus hiesiger Kenntnislage sind keine belastbaren detaillierten Aussagen möglich. Das BKA hat aber in Medienberichten immer wieder zu Recht beklagt, dass ein entsprechendes Melde- und Rückmeldesystem etabliert werden muss. Auch sei auf Frage 1 verwiesen und den Hinweis, dass nicht nur die ausländischen Polizei- und Strafverfolgungsbehörden informiert werden sollten, sondern darüber hinaus auch die ausländischen Diensteanbieter. Hier müsste lediglich sichergestellt sein, dass durch derartige Hinweise an ausländische Provider keine Ermittlungsmaßnahmen beeinträchtigt werden, was sich aber durch entsprechende Datenbanken und Informationssysteme o.ä. einfach realisieren ließe, zumal es sich zunehmend um internationale Verfahren handelt.

Generell gilt, dass auf Nachrichten an die Missbrauchs-Kontakt-Adressen (Abuse-Adressen, meist abuse@provider.tld) meist sofort automatisierte Eingangsbestätigungen verschickt werden. Dies ist bei fast allen Providern weltweit üblich.

Frage 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?*

Antwort: Aus hiesiger Kenntnislage sind keine belastbaren Aussagen zu den Erfahrungen der Selbstkontrolleinrichtungen möglich. Eigene Erfahrungen bestätigen aber, dass bei einer direkten Kontaktierung der ausländischen Diensteanbieter eine Löschung binnen Stunden durchsetzen lässt.

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

Antwort: Die Intervalle zur Überprüfung sollten möglichst kurz sein. Nach meinem derzeitigen Kenntnisstand werden die Inhalte meist manuell überprüft. Dies kostet Zeit und bindet Ressourcen. Es wäre aber durchaus möglich, maschinell die Verfügbarkeit von Domains, einzelnen HTML-Seiten oder spezifischen Bildern/Filmen zu überwachen. Hier sind auch sehr kurze Intervalle denkbar, die Überprüfung kann beispielsweise kurz nach der Entdeckung der Inhalte stündlich oder halbstündlich erfolgen und mit der Zeit verlängert werden. Bei Änderungen der Inhalte ist eine manuelle

Überprüfung möglich, um so festzustellen, ob die Inhalte entfernt oder ersetzt wurden.

Frage 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?*

Antwort: Insgesamt gibt es je nach Art des betreffenden Angebots bzw. der betreffenden Webseite und je nach Kontext des Hostings verschiedene Möglichkeiten, eine Löschung bzw. permanente Abschaltung zu erreichen.

a) **Der Betreiber der Webseite.** Handelt es sich um einen typischen Web 2.0 Dienst, bei dem beispielsweise Bilder oder Filme hochgeladen werden können, ist der Betreiber der Webseite i.d.R. der schnellste direkte Ansprechpartner. Er hat die Kontrolle über sein System und kann gezielt einzelne Inhalte entfernen und die Spuren der Täter für weitere polizeiliche Ermittlungen sichern.

   Ähnliches gilt für die Anbieter von kostenlosem Webspace.

b) **Der Hosting-Provider.** Dies ist häufig auch der Betreiber des Rechenzentrums, in dem der Server steht. Hosting-Provider haben so genannte Abuse-Abteilungen. Dort kümmern sich die Mitarbeiter um alle Missbrauchsfälle wie beispielsweise Spam-Versand. Dies ist in der Regel der beste und schnellste Weg. Große Provider haben rund um die Uhr besetzte Abuse-Abteilungen, so dass eine Entfernung der Inhalte häufig sehr schnell möglich ist.

c) **Betreiber des Rechenzentrums.** Bei größeren Rechenzentren werden einzelne Server-Stellplätze vermietet. Reagiert ein Hosting-Provider nicht oder handelt es sich um besonders schwerwiegende Darstellungen, kann daher auch der Betreiber des Rechenzentrums kontaktiert werden. Er hat oft auch einen direkten Kontakt zu seinem Kunden. In besonders schweren und eiligen Fällen kann er den betreffenden Server vom Netz trennen. Zudem hat er physikalischen Zugriff auf die Hardware, in entsprechend dringenden Fällen kann also auch die lokale Polizei einschreiten.

d) **Der Uplink-Provider.** Dies ist der Provider, der den Hosting-Provider ans Internet anschließt. Ähnlich wie der Betreiber des Rechenzentrums kann er in besonders schweren Fällen den betreffenden Server (genauer: die betreffende IP-Adresse) vom Netz trennen.

e) **Der Betreiber des Autonomen Systems (AS).** Dieser ist häufig mit dem Uplink oder dem Betreiber des Rechenzentrums identisch. Auch größere Hosting-Provider haben häufig ein eigenes AS. In besonders schweren Fällen kann es sinnvoll sein, diesen zu kontaktieren.

In Einzelfällen kann es auch sinnvoll sein, andere Wege zu beschreiten. So können die Betreiber der Nameserver kontaktiert werden. Jede Domain braucht mindestens zwei Nameserver. Fallen beide aus oder stellen beide ihre Dienste für die betreffende Domain ein, ist diese nicht mehr erreichbar. Dazu können wie oben erläutert auch hier alle Infrastruktur-Betreiber (Provider des DNS-Servers, Hosting-Provider, Rechenzentrums-Betreiber usw.) kontaktiert werden. Dieser Weg kann für die Fälle genutzt werden, in denen Domains sehr schnell umziehen und die Hosting-Provider wechseln.

Das gleiche gilt für den Registrar der Domain (die Firma, die dem Domaininhaber die Domain verkauft bzw. die Registrierung vornimmt), auch der kann in Ausnahmefällen kontaktiert werden. Da die einschlägigen Domains in der Regel unter falscher Identität registriert wurden, besteht hier entsprechende Handhabe.

Desweiteren besteht die Möglichkeit, direkt die Registry – die Registrierungsstelle der Domain, gelegentlich auch Network Information Center (NIC) genannt – selbst zu kontaktieren. In Ausnahmefällen kann dies durchaus sinnvoll sein. So habe ich für die Abschaltung einer Webseite der dänischen Sperrliste die indische Domain Registry kontaktiert, nach drei Stunden war die Domain eingefroren und damit nicht mehr unter Kontrolle des Täters und für Internet-Nutzer nicht mehr erreichbar. Diese Methode sollte aber nur mit Bedacht eingesetzt und auf solche Fälle beschränkt werden, in denen die betreffende Domain einzig zum Zwecke der Verbreitung von Darstellungen sexuellen Missbrauchs von Kindern registriert wurde. Wie auch beim Vorgehen gegen die Nameserver kann dies insbesondere bei sehr schnell wechselnden Servern sinnvoll sein, beispielsweise wenn per Botnetz kompromittierte Rechner von Privatanwendern missbraucht werden.

Daneben besteht die Möglichkeit, Dienstleister von Teilen des Gesamtangebots zu kontaktieren. Beispielsweise eventuelle Anbieter von Bezahlsystemen.

Zudem kann es der Fall sein, dass einzelne Elemente einer Seite wie Texte und Bilder aber auch Gästebücher, Foren usw. von verschiedenen Servern stammen. Sofern die strafrechtlich releanten Inhalte von anderen Servern kommen, kann und sollte in diesem Falle wiederum der jeweilige Anbieter bzw. Provider kontaktiert werden.

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

Antwort: Inhalte nach § 184b StGB können nach meinem Kenntnisstand weltweit zeitnah gelöscht werden. Schwieriger ist es demgegenüber bei gerade noch legalen Inhalten – aber bei legalen Inhalten wäre eine Löschung sowieso nicht angebracht.

Schwierig kann sich die Löschung gestalten, wenn sich die Inhalte sehr schnell ändern und beispielsweise nur zeitweise illegal sind. In solchen Fällen ist aber auch die Entdeckung nicht einfach. Eine enge und vertrauensvolle internationale Zusammenarbeit und Zusammenarbeit mit den Hosting-Providern ist in diesem Fall unabdingbar.

Frage 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?*

Antwort: Bei der Analyse der skandinavischen Sperrlisten fällt auf, dass es offensichtlich keine oder nur eine geringe Zusammenarbeit mit den Ermittlungsbehörden in anderen Ländern gibt. So stehen derzeit auf der aktuellen dänischen Sperrliste (vom 20. Oktober 2010) elf Domains aus Deutschland. Zwar bedeutet das nicht, dass die Webseiten tatsächlich auch Missbrauchsdarstellungen zeigen, aber sollte dies nicht der Fall sein, müsste die entsprechende Domain auch von der Sperrliste entfernt werden. Mindestens eine der in Dänemark derzeit (und seit mindestens 2009) gesperrten und in Deutschland gehosteten Webseiten enthält vollkommen legale Inhalte. Bei anderen sind eventuell einschlägige Inhalte bereits gelöscht.

Alle Beobachtungen deuten darauf hin, dass die Sperren die Bemühungen der Ermittlungsbehörden, eine Löschung der Inhalte zu erreichen, reduzieren. Es ist einfacher, eine Webseite auf eine Liste zu setzen. Dies hat aber auch nur eine entsprechend marginale Wirkung.

Frage 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 sicher gestellt, dass entsprechende Listen mit zu sperrenden Seiten (gelbe Seiten der Kinderpornographie) nicht in der Öffentlichkeit zugänglich gemacht werden können, wie in anderen Ländern gesche-*

hen? Ist die Anzahl der Meldungen bei den Hotlines/Behörden in den Ländern, in denen gesperrt wird, nach Einführung der Sperrung signifikant zurückgegangen?

Antwort: Die Erfahrung insbesondere aus den skandinavischen Ländern zeigt, dass die Sperrlisten früher oder später bekannt werden. Teilweise öffentlich (z.B. bei Wikileaks), teilweise sind sie aber auch nur einer eingeschränkten Öffentlichkeit bekannt.

Es ist aber auch unmöglich, die Sperrlisten komplett geheim zu halten, schon aus technischen Gründen. Zwar werden die Listen häufig verschlüsselt übertragen, für den Einsatz beim Access-Provider wird die Liste aber entschlüsselt und liegt somit im Klartext vor.

Eine Folge vom Einsatz von Sperren ist zudem, dass die Sperrliste quasi öffentlich bzw. teilöffentlich wird: Ein Nutzer kann eine beliebige Webseite aufrufen, und wenn ein Stopp-Schild erscheint ist sie auf der Sperrliste, ansonsten nicht. Dieses Verfahren lässt sich natürlich automatisieren, beispielsweise mit passenden DNS-Aufrufen. So lassen sich pro Sekunde hunderte bis tausende Domains prüfen. Mit dieser Methode lässt sich auch mit vertretbarem Aufwand zumindest eine Teil-Liste der gesperrten Domains erstellen.

Die Erfahrung in den skandinavischen Ländern zeigen auch, dass von den **jeweils aktuell blockierten Inhalten nur ein Bruchteil Darstellungen sexuellen Missbrauchs von Kindern zeigen.** Siehe auch Anlage B. In vielen Fällen lässt sich dies zwar damit erklären, dass die betreffenden Webseiten mal einschlägige Inhalte enthalten hatten und extra dafür bevorzugt bei Dienstleistern, die kostenlosen Webspace anbieten, angelegt wurden. Dies ist aber nicht immer der Fall. So werden in Dänemark aktuell (Stand: 20. Oktober 2010) einige Domains blockiert, die keine einschlägigen Inhalte haben:

- **bimseregitim.com.tr**
  Hierbei handelt es sich um die Webseite eines türkischen IT-Schulungsunternehmens.
- **yourjokes.co.uk**
  Eine Witze-Webseite aus Großbritannien, mit sexistischen Witzen.

Diese Domains stehen schon mindestens seit Monaten auf der Sperrliste.

In der Vergangenheit wurde in Dänemark auch eine Islam-Webseite aus Deutschland blockiert.[8] Aufgrund eines Gerichtsbeschlusses war eine weitere Webseite blockiert:

[8] siehe http://blog.odem.org/2009/05/islam-website-aus-deutschland-auf-sperr-liste.html

die türkische Firma Homeco hatte eine Namensähnlichkeit mit einer dänischen Firma,[9] die Domain *homeco.com.tr* kam auf die Sperrliste.[10]

Die Provider in Dänemark wurden auch gerichtlich verpflichtet, die schwedische Webseite PirateBay aufgrund Urheberrechtsverletzungen zu sperren. Dies wurde vom obersten Gerichtshof Dänemarks bestätigt.[11] Laut Medienberichten war es Strategie der Musikindustrie in Dänemark, Internet-Sperren mit der Begründung des Kampfes gegen Kinderpornographie durchzusetzen.[12]

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

Antwort: Bei Sperren werden die Inhalte nicht entfernt, sondern quasi nur versteckt. Für interessierte Konsumenten ist es aber ein Leichtes, jegliche Art von Sperren zu umgehen. Die Erfahrung aus den skandinavischen Ländern (siehe Antwort zu Frage 2) zeigt zudem, dass nach dem Eintrag auf eine Sperrliste die Gefahr besteht, dass die Löschung und die Verfolgung der Täter unterlassen werden.

Eine Löschung kann vom Konsumenten nicht umgangen werden, da die Inhalte nicht mehr erreichbar sind. Das bedeutet aber nicht, dass die betreffende Webseiten und alle Spuren der Täter vernichtet sind, sondern nur, dass sie nicht mehr zugänglich sind, weil beispielsweise der Stecker des betreffenden Servers gezogen wird. Die Bezeichnung „Löschen“ ist also insofern irreführend, als dass damit nicht zwangsläufig eine Vernichtung der Spuren einhergeht. Letztlich handelt es sich um eine Art Beschlagnahme. Die Hosting-Provider sollten die Inhalte als Beweise immer für die Ermittlungsbehörden sicherstellen.

Auch ein Melde- und Löschkonzept kann (und sollte zumindest in Teilen) zentral koordiniert werden. So ist es durchaus sinnvoll, dass es in allen Ländern zentrale Anlauf- und Meldestellen gibt.

Sperren bringen zudem als systemimmanentes Problem mit, dass den Tätern ein automatisierbares Frühwarnsystem geboten wird (siehe Anlage E). Technisch lässt sich dies mit wenigen Zeilen Quellcode umsetzen. Da die Täter aber weiter Zugriff auf den Server haben, können sie vorhandene Spuren vernichten, falsche Spuren legen und die

---

[9] siehe http://www.oasisestate.dk/index.php?lng=en&section=info&mod=display&contentid=68

[10] Laut dem Project Herdict Web des Berkman Center for Internet & Society an der Harvard University: http://www.herdict.org/web/explore/detail/id/DK/8659/32767

[11] siehe http://merlin.obs.coe.int/iris/2010/8/article24.de.html

[12] http://www.heise.de/tp/r4/artikel/32/32562/1.html

Inhalte auf einen neuen Server umziehen. Mit der gleichen Methode kann die Sperrliste automatisiert herausgefunden werden (siehe auch Antwort zu Frage 9).

Frage 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?*

Antwort: Banken haben ein finanzielles Interesse daran, dass phishing-sites schnell offline gehen. Je länger sie online sind, desto größer kann der Schaden werden. Daher bemühen sie sich um eine schnelle Abschaltung und erreichen diese in der Regel – obwohl diese Inhalte nicht weltweit geächtet sind.

Bei Webseiten mit Missbrauchsdarstellungen werden in vielen Fällen nicht alle Möglichkeiten zur Entfernung der Inhalte ausgeschöpft und die Verfahrensabläufe (siehe Antwort auf Frage 1) sind zumindest deutlich verbessungsfähig. Oftmals wurde beispielsweise noch nicht einmal der Hosting-Provider über die Inhalte informiert.

Daher wäre ein verbessertes notice-and-take-down-Verfahren durchaus ein gangbares Mittel.

Das bereits geschilderte und in Anlage B beschriebene Verfahren zeigt, dass bisher offensichtlich kein notice-and-take-down-Verfahren angewandt wurde und dadurch jahrelang Kindesmissbrauchsdarstellungen im Netz verfügbar waren, die innerhalb von 30 Minuten gelöscht werden konnten.

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

Antwort: Ein strategisches und von möglichst vielen Staaten mitgetragenes Gesamtkonzept könnte die Erfolge signifikant erhöhen.

Dieses Gesamtkonzept kann beispielsweise auf den folgenden Punkten beruhen:

- In jedem Staat sollte eine Zentralstelle zur Koordinierung aller Maßnahmen, zur Verfolgung der Straftäter und zur Weitergabe von Meldungen über entsprechende Webseiten eingerichtet werden.

- Gleichzeitig sollte es für Polizeibehörden und den Meldestellen der Privatwirtschaft möglich sein, Hosting-Provider in anderen Ländern formlos über einschlägige Inhalte zu informieren.
- Die Hosting-Provider sollten in das Gesamtkonzept mit eingebunden sein und schnelle Kommunikationskanäle bereitstellen, so dass entsprechende Meldungen bevorzugt behandelt werden.
- Gleichzeitig ist es aber wichtig, die Strafverfolgung der Täter zu intensivieren, um nachhaltig erfolgreich zu sein.
- Dazu ist auch eine bessere technische Ausstattung und breitere technische Kompetenz der Ermittlungsbehörden wichtig.
- Der Austausch von Informationen zwischen den Strafverfolgungsbehörden der einzelnen Staaten sowie anderen einbezogenen Stellen sollte intensiviert werden, beispielsweise um mehrfache Ermittlungen zum gleichen Sachverhalt zu vermeiden.
- Das Internet bietet verschiedene Möglichkeiten zur weltweiten Kommunikation und Vernetzung. Diese sollten auch von den Ermittlungsbehörden und anderen Stellen genutzt werden.

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

Antwort: Es gibt auch kommerzielle Webseiten, die Inhalte nach § 184b StGB verkaufen oder dies zumindest vorgeben. Dieser Markt ist aber nach allen vorliegenden Studien sehr klein. Dies ist nachvollziehbar, da sowohl die Verkäufer als auch die Käufer ein sehr hohes Risiko eingehen. Zudem ist für einen blühenden Markt eine starke öffentliche Präsenz notwendig, die Missbrauchsdarstellungen nach § 184b StGB aber nicht haben.[13]

Nach einer Studie der European Financial Coalition[14] gibt es keinen nennenswerten kommerziellen Markt für Darstellungen sexuellen Missbrauchs von Kindern nach § 184b StGB. Um überhaupt einige Fälle zu finden, wurden sowohl der Missbrauchsbegriff als auch die Kommerzialität sehr weit gefasst: Von 14.579 untersuchten einschlägigen Webseiten enthielten insgesamt nur vier (!) kommerzielle Seiten Bilder von nackten Kindern. Zwei Seiten (0,0137%) enthielten Comic-Zeichnungen mit nackten Kindern, zwei weitere waren Nudisten-Seiten (Seiten mit FKK-Bildern).

---

[13] vgl. Korinna Kuhnen: Kinderpornographie und Internet; Göttingen, 2007: Hogrefe Verlag; Seite 132f

[14] http://www.ceop.police.uk/Documents/EFC%20Strat%20Asses2010_080910b%20FINAL.pdf

Das Kriminalwissenschaftliche Institut der Uni Hannover erstellt derzeit eine Studie zu dieser Frage. Erste Ergebnisse zeigen, dass es keinen umfangreichen kommerziellen Markt für derartige Inhalte gibt.[15]

Alle belastbaren Untersuchungen sowie Praxisberichte zeigen, dass der kommerzielle Markt für Darstellungen sexuellen Missbrauchs von Kindern („Kinderpornographie" nach § 184b StGB) nur sehr klein ist.[16] Die Täter agieren vor allem im Verborgenen, wollen nicht gefunden werden. Da sich Geldströme nachvollziehen lassen, ist für sie hier das Risiko relativ hoch.

Bei vorhandenen kommerziellen Seiten ist auch nicht immer klar, ob sie wirklich die Inhalte liefern, die sie versprechen. Welcher betrogene Konsument würde sich schon an die Polizei wenden, weil er die bestellten und bezahlten Missbrauchsbilder nicht erhält? Zudem ist bekannt, dass das FBI so genannte Honeypots betreibt, mit denen potentielle Konsumenten angelockt werden sollen. Wer diese Angebote nutzt, wird dann strafrechtlich verfolgt.[17]

Frage 14: *Welche Maßnahmen sind sinnvoll und geboten, um gegen die aktive Nachfrage vorzugehen?*

Antwort: In den letzten Jahren gab es einige Projekte, die in die Prävention investiert haben. Das bekannteste ist „Kein Täter werden" von der Charité unter der Leitung von Prof. Klaus M. Beier.[18] Entsprechende Projekte sollten weiterhin unterstützt und ausgebaut werden.

Bezüglich des Internets ist es wichtig, die Quellen für Missbrauchsdarstellungen trocken zu legen. Dies kann nur dann erfolgreich sein, wenn die Verfolgung der Täter und die Entfernung der Inhalte intensiviert werden. Indem man gegen Primärtäter und Einsteller vorgeht, reduziert man das Angebot und damit die Möglichkeit einer erfolgreichen Nachfrage wirksam und nachhaltig. Sperren reduzieren das Angebot nicht.

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

---

[15] http://www.heise.de/ct/artikel/Deja-vu-971943.html

[16] siehe auch http://www.sueddeutsche.de/panorama/kindesmissbrauch-mitten-am-rand-1.396436-6 und http://www.lawblog.de/index.php/archives/2009/03/25/die-legende-von-der-kinderpornoindustrie/

[17] http://news.cnet.com/8301-13578_3-9899151-38.html

[18] http://www.kein-taeter-werden.de/, http://www.sexualmedizin.charite.de/

Antwort: Die strafrechtliche Verfolgung der Täter ist erst einmal unabhängig von den Maßnahmen zur Bekämpfung der Inhalte. Das Blockieren (Sperren) der Inhalte bietet dem Täter die Möglichkeit festzustellen, ob er im Fokus der Ermittler steht.[19] Gleichzeitig hat der Täter aber weiterhin vollen Zugriff auf den Server und ist in der Lage, beispielsweise Spuren zu vernichten.

Beim „Löschen" werden die Inhalte nicht vernichtet, sondern der betreffende Server abgeschaltet bzw. sowohl dem Täter als auch allen Konsumenten der Zugriff entzogen. Im Gegensatz zur Sperre lässt sich dies nicht umgehen. Die vorhandenen Daten bleiben aber bestehen und können kriminaltechnisch untersucht werden – daher ist der Begriff „Löschen" auch nicht ganz korrekt.

In Einzelfällen kann es aus ermittlungstaktischen Gründen sinnvoll sein, eine Webseite wenige Tage weiter laufen zu lassen, um den Täter zu beobachten. Dies sollte aber immer nur für sehr kurze Zeit geschehen, um die Verbreitung der Inhalte möglichst schnell zu unterbinden. Mit Blick auf den Schutz der Menschenwürde der Opfer ist dies unabdingbar.

Zur strafrechtlichen Verfolgung der Täter ist es allgemein wichtig, schnell zu reagieren. Gleichzeitig sollten die technischen Möglichkeiten genutzt werden, um die Täter und neue Webseiten aufzuspüren. So ist es mit Techniken ähnlich denen von Suchmaschinen oder dem Monitoring von Änderungen an DNS-Einträgen möglich, einschlägige Webseiten zu finden, bevor oder kurz nachdem sie in den einschlägigen Zirkeln bekannt werden. Um diese Möglichkeiten zu nutzen wäre es wichtig, dass die Ermittlungsbehörden auch mit Softwareentwicklern ausgestattet werden, die in der Lage sind entsprechende Programme zu schreiben. Hier rege ich an, interdisziplinäre Arbeitsgruppen zu bilden sowie Kriminalbeamte auch aus technischer Sicht permanent fortzubilden. So wäre es sinnvoll, wenn zumindest einige Ermittler pro Abteilung mindestens eine Programmiersprache (es bieten sich Skripting-Sprachen wie Perl an) beherrschen würden, beispielsweise um wiederkehrende Aufgaben zu automatisieren oder einen Werkzeugkasten für die Ermittlungsarbeit zusammenzustellen.

Alvar Freude, Arbeitskreis gegen Internet-Sperren und Zensur, im Oktober 2010
alvar@a-blast.org | (01 79) 13 46 47 1 | http://alvar.a-blast.org/
Fideliostraße 16 | 70597 Stuttgart

Kontakt AK Zensur: info@ak-zensur.de, (01 79) 13 46 47 1

[19] siehe Anlage E

Löschen und Strafverfolgung statt Löschen und Sperren

Grundsätzliches zum Thema Internet-Sperren

Seit fast zwei Jahren diskutieren wir in Deutschland nun über das Für und Wider von „Internet-Sperren“ im Kampf gegen die Verbreitung von Bildern und Filmen, die den sexuellen Missbrauch von Kindern (oft verharmlosend „Kinderpornografie“ genannt) zeigen.

Die Unvorstellbarkeit der hinter den Bildern stehenden Taten brachte es mit sich, dass selten sachlich und emotionslos diskutiert und nach der besten Lösung gesucht wurde – denn die Lösung war in Gestalt der „Sperren“ schon gefunden. Und auf den ersten Blick klingt das ja auch gut: Da unternimmt endlich jemand etwas gegen den sexuellen Missbrauch von Kindern! Wer hingegen an den Instrumenten Kritik übte, wurde häufig auf eine Ebene mit den Missbrauchstätern gestellt oder zumindest als Verharmloser gebrandmarkt.

Erst bei genauerer Betrachtung wurde klar: Mit Internet-Sperren kann weder etwas gegen den Missbrauch unternommen werden (denn der findet nicht im Internet statt), noch verschwinden Bilder und Filme, die diesen dokumentieren. Sie werden nur vor den Augen derjenigen versteckt, die sich das sowieso nicht anschauen. Denn es ist weitaus leichter die „Sperren“ zu umgehen, als entsprechende Darstellungen zu finden.[1] Das Wort „Sperren“ suggeriert aufgrund unterschiedlicher Bedeutung aus anderen Kontexten, der Inhalt sei nicht mehr verfügbar. Dies ist aber schlicht falsch, denn es wird noch nicht einmal eine relevante Hürde für den Konsumenten aufgebaut.

Aber auch gegen die Täter, die diese Bilder ins Netz stellen, wird mit Internet-Sperren und dem Aufstellen von Stopp-Schildern nichts unternommen, im Gegenteil: Die Erfahrung mit den Sperren in den skandinavischen Ländern zeigt, dass mit der Aufnahme auf die Liste die Polizeiarbeit in der Regel erledigt ist. Die Inhalte bleiben im Netz, werden weiter verbreitet, können weiter konsumiert werden. Und, auch wenn dies unvorstellbar erscheint: Im Sommer 2009 enthielt die dänische Sperrliste nach BKA-Informationen 199 Einträge aus Deutschland.[2] Auch wenn sich dies in der Zwischenzeit gebessert hat, stehen aktuell (stand 20. Oktober 2010) in Dänemark immer noch elf Webseiten aus Deutschland auf der „Kinderpornografie-Sperrliste“. Und

[1] http://www.google.de/search?q=internet+sperren+umgehen

[2] http://blog.odem.org/2010/01/30/bka-antwort-spd-bulmahn.pdf

mindestens eine davon zeigt – dies haben Auswertungen der Listen ergeben – weder Bilder von Kindern noch pornografische Darstellungen, wird aber schon seit Jahren blockiert.

Netzsperren stehen seit Jahren für verschiedenste Inhalte auf dem Wunschzettel vieler Interessensgruppen.[3] Mit Kindesmissbrauch wurde das Thema gefunden, mit dem man die Politik von der Notwendigkeit der Sperren überzeugen konnte. Ein dänischer Lobbyist äußerte gar die Meinung, „Kinderpornografie ist großartig",[4] weil man damit Politiker zum Einführen von Sperren bewegen könne – um sie dann auf andere Inhalte auszudehnen. Um dies zu erreichen, sollten gezielt Politiker angesprochen werden,[5] was zumindest in Skandinavien auch geschah.

Und ist der Vorschlag erst einmal ernsthaft in der Welt, ist es in der politischen Kommunikation – auch dies hat die Diskussion vor einem Jahr in Deutschland gezeigt – schwierig, dagegen zu sein: aus Angst, in eine „Kinderschänder-Lobby"-Ecke gestellt zu werden, spricht sich öffentlich kaum jemand gegen entsprechende Vorschläge und Wünsche aus, selbst wenn noch so viele Zweifel angebracht sind.

Zahlenspielereien

Was ist der beste Weg, um im Internet gegen das vorzugehen, was Juristen „Kinderpornografie" und Opfer „Dokumentation sexuellen Missbrauchs von Kindern" nennen? Einleuchtend ist die Forderung, dass diese Inhalte gelöscht und nicht nur blockiert oder „gesperrt" – also notdürftig versteckt – werden sollen.

Aber, so war letztes Jahr allerorten zu hören, man könne gegen die Inhalte nichts unternehmen. Selbst BKA-Chef Jörg Ziercke sagte noch im August 2009, die Inhalte würden aus entfernten „Failed States" verbreitet, Ländern, in denen keine Strafverfolgung möglich sei.[6] Doch das ist falsch: die meisten Server stehen in den USA und in Westeuropa – einschließlich Deutschlands. Dies war dem BKA schon im Juni bekannt,[7] Sperrgegner haben bereits im März darauf hingewiesen.[8]

---

[3] http://odem.org/informationsfreiheit/o-ton--wieviel-und-was.html

[4] http://ak-zensur.de/2010/04/kinderpornos-grossartig.html

[5] http://www.heise.de/tp/r4/artikel/32/32562/1.html

[6] http://www.heise.de/newsticker/meldung/BKA-Chef-Umgehen-von-Kinderporno-Sperren-ist-strafbar-752033.html

[7] http://blog.odem.org/2010/01/30/bka-antwort-spd-bulmahn.pdf

[8] http://blog.odem.org/presse/FITUG-Pressemeldung-Internet-Sperren.pdf

Schon seit Beginn der Debatte wurde mit fragwürdigen und sogar teilweise widerlegten Zahlen und Behauptungen operiert.[9] Auch EU-Kommissarin Cecilia Malmström übernahm diese Tradition.[10] Wie sie in einer Anhörung der EPP-Fraktion im Europäischen Parlament im Juli 2010 einräumte, hat die EU-Kommission ihren aktuellen Vorschlag für Netzsperren nicht etwa auf nachvollziehbare Fakten gestützt, sondern kurzerhand eine „politische Entscheidung" getroffen. „Wir wissen nicht, was wir nicht wissen" entgegnete sie auf die Frage nach den Grundlagen für ihre Entscheidungsfindung.[11]

Löschen funktioniert

Da verwundert es umso mehr, dass zahlreiche Sperrbefürworter weiterhin behaupten, das Löschen kinderpornografischer Darstellungen dauere in den Herkunftsländern Ländern zu lange bzw. sei in vielen Fällen nicht möglich. Jeder, der sich rudimentär mit der Thematik auskennt, reibt sich verwundert die Augen: „Die USA als Hort der Kinderpornografie?" Eine seltsame Vorstellung. Denn tatsächlich zeigt eine Studie der Universität Cambridge,[12] dass es Banken innerhalb von durchschnittlich vier Stunden schaffen, Betrugs-Webseiten (Phishing-Sites) abzuschalten. Warum sollte dies bei Kindesmissbrauchs-Bildern, die weltweit nicht nur verboten, sondern geächtet sind, nicht auch klappen?

Ein Blick auf die bisherige Praxis zeigt, dass die Bemühungen, tatsächlich gegen die Inhalte vorzugehen – sie also zu „löschen" –, in der Vergangenheit einfach ungenügend waren. Aber auch im ersten Halbjahr 2010 verbesserte sich dies nur geringfügig, die internationale Zusammenarbeit läuft weiterhin zäh.[13] Nicht nur Verbrecher profitieren vom Internet, auch die Strafverfolger können mit den Mitteln des Netzes schneller und effektiver gegen Straftäter vorgehen. Der Standort einer neu entdeckten Webseite kann innerhalb von Sekunden automatisch ermittelt werden; innerhalb von Minuten ist es möglich, die Ansprechpartner des Providers für Missbrauchsfälle zu kontaktieren oder lokale Polizeidienststellen zu informieren. Dass es in der Praxis beispielsweise am Wochenende auch einmal zu Verzögerungen kommen kann, ist im Vergleich zu den angedachten Blockaden nicht weiter relevant: diese wirken allein aufgrund technischer Notwendigkeit auch frühestens am nächsten Werktag.

---

[9] http://www.heise.de/ct/artikel/Verschleierungstaktik-291986.html

[10] http://www.heise.de/ct/artikel/Deja-vu-971943.html

[11] http://www.heise.de/newsticker/meldung/Websperren-EU-Kommission-will-schnell-handeln-1032329.html

[12] http://www.cl.cam.ac.uk/%7Ernc1/takedown.pdf

[13] http://ak-zensur.de/2010/08/kapitulation.html

So erziehlt das Meldestellennetzwerk INHOPE in der Zwischenzeit deutlich bessere Erfolge beim Löschen,[14] und die ausgeweitete Zusammenarbeit von BKA und Meldestellen dürfte die Ergebnisse weiter verbessern.[15]

Im September 2010 hat der Autor einen repräsentativen Teil der tagesaktuellen Sperrliste aus Dänemark untersucht. Von 167 Webseiten verbreiteten nur drei Kindesmissbrauchsbilder. Zwei davon waren seit mehreren Jahren auf der dänischen und anderen skandinavischen Sperrlisten. Nach Meldung an den Hosting-Provider in den USA konnten die Inhalte selbst an einem Freitag, in der Nacht, innerhalb von 30 Minuten abschalten lassen eine Löschung erreichen. Eine weitere Webseite auf einem Server in den Niederlanden war seit Monaten auf der schwedischen und dänischen Sperrliste verzeichnet. Nach Meldung wurde sie innerhalb von drei Stunden von der zuständigen indischen Domainvergabestelle (Registry) abgeschaltet. Eine komplette Dokumentation findet sich unter http://ak-zensur.de/2010/09/29/analysis-blacklists.pdf bzw. in Anlage B.

Unerwünschte Nebenwirkungen

Eine naheliegende Forderung ist – und diese wird ja gegenwärtig sehr massiv in die politische Debatte eingebracht: Könnte man dann nicht wenigstens eine Doppelstrategie fahren? Zusätzlich zum Löschen auch das Sperren bei solchen Inhalten, die vielleicht doch nicht sofort löschbar sind? Abgesehen von der Tatsache, dass das Löschen – wie es die Banken vormachen – tatsächlich funktioniert,[16] bringen Sperren systemimmanente Probleme[17] mit sich: Die Betreiber entsprechender Webseiten können feststellen, ob sie im Fokus der Ermittler und ihre Webseiten auf der Sperrliste stehen: ein Aufruf der Seite genügt. So erhalten sie ein wirksames Frühwarnsystem.

Auch die Konsumenten dieser Bilder können profitieren. Die Behörden versichern zwar, dass sie die Sperrlisten streng geheim halten, doch dies ist ein leeres Versprechen. Man muss einen Computer lediglich alle in Frage kommenden Webseiten durchprobieren lassen und erhält die Sperrliste. Doch dieser Aufwand ist nicht einmal nötig, denn die Vergangenheit hat gezeigt: früher oder später sickern die Sperrlisten durch. Damit erhalten Interessierte einen Wegweiser zu den blockierten Seiten, das Gegenteil des Erhofften tritt ein.

Gleichzeitig muss für die Etablierung von Sperren eine Technik aufgebaut werden, die zum Blockieren beliebiger Inhalte genutzt werden kann. Viele Interessengruppen ste-

[14] http://www.netzpolitik.org/2010/eco-loschen-funktioniert-zu-98/

[15] http://www.heise.de/newsticker/meldung/Provider-halten-Kinderporno-Sperren-fuer-unverhaeltnismaessig-1070689.html

[16] http://ak-zensur.de/2009/05/loeschen-funktioniert.html

[17] http://ak-zensur.de/2010/03/sperren-ueber-eu.html

hen Schlange, um eine Ausweitung auf andere Inhalte durchzusetzen. Und Europa begibt sich damit auf ein ähnliches Niveau wie autoritäre Staaten wie China oder dem Iran – die sich bei der Rechtfertigung ihrer Internet-Zensur darauf berufen, dass dies in Europa ja auch üblich sei, und es betreffe hier wie da ja nur „illegale“ Inhalte.

Strafverfolgung statt Verstecken

Aber nicht nur die Löschung der Inhalte ist wichtig. Noch wichtiger ist die Verfolgung der Täter, derjenigen, die diese unmenschlichen Bilder und Filme erzeugen und verbreiten. Auch dies kann nicht dadurch erledigt werden, dass einschlägige Angebote auf eine Sperrliste gesetzt werden. Die Server, über die die Verbreitung stattgefunden hat, müssen untersucht und eventuelle Geldströme verfolgt werden. Dies ist harte kriminalistische Arbeit, schwerer als das Entfernen der Inhalte. Wer es aber wirklich ernst meint mit dem Kampf gegen die Verbreitung von Missbrauchsdarstellungen, kommt darum nicht herum. Wer hingegen auf wirkungslose Sperren setzt, duldet weiterhin diese Verbreitung. Denn selbst wenn die Sperren im World Wide Web funktionieren sollten – die Täter verbreiten die Inhalte schon lange in Chats, auf Tauschbörsen oder in privaten Netzwerken. Sperrsysteme suggerieren Aktivität, sind aber dort wirkungslos, wo sich die Täter aufhalten. Die Menschenwürde der Opfer bleibt auf der Strecke.

Klar ist auf jeden Fall: Bilder und Videos, die Kindesmissbrauch zeigen („Kinderpornografie“), lassen sich bei geeignetem Vorgehen problemlos und schnell entfernen. Die seit nun rund zwei Jahren fehlgeleitete Diskussion in Deutschland hat den Blick auf unwirksame Blockadesysteme beschränkt, anstatt ihn auf wirksame Verfahren zu richten. Das ist längst überfällig, und daher ist zu hoffen, dass sich diese Erkenntnis im EU-Parlament schneller durchsetzt.

Alvar Freude
http://alvar.a-blast.org/
alvar@a-blast.org

(07 11) 75 88 47 79
(01 79) 13 46 47 1

Anlage B

Zur Stellungnahme von Alvar Freude, Fachgespräch Unterausschuss Neue Medien am 25. Oktober 2010

Blacklists of Denmark and Sweden analysed (preliminary version)

Analysis of domains blocked in Denmark on 28 September 2010, 14:20:00 GMT+0200 (CEST)

Blocking websites is suggested by some politicians to be a measure of last resort, based on the claim that removing child abuse images from certain websites can be impossible. Although the blocking of websites is highly controversial, there is very little data available on the extent to which attempts have been made to remove illegal material. In this report, we investigate this by analysing a representative sample of 167 websites currently blocked in Denmark and requesting the removal of detected illegal material from the hosting providers. In this investigation we only analysed a preliminary sample, a more comprehensive study will follow.

Results:

- **Three domains** were found to contain illegal child abuse images.
  - Two of these have been on the Danish blacklist since 2008 and were also blocked in Norway, Finland and Sweden. After sending an abuse message to the hosting provider in the USA, the websites were **removed in less than 30 minutes.** This suggests that the police did nothing to shut these sites down for about two years.
  - One domain has been on these blacklists since about spring 2010, in the TLD .in (India), hosted in the Netherlands. The domain was **suspended by the Indian domain name registry three hours after a request was sent.**
- More than half of the blocked domains (92) were already deleted.
- Many domains (66) were not registered anymore.
- Some domains (6) did not contain any child abuse images or obvious illegal content.

Summary:

The vast majority of the blocked domains are no longer active. Only a few still are.

- 164 domains were blocked in Denmark, but offered no illegal material or were not connected at all at the time of our investigation.
- 3 of the blocked domains were found to contain child abuse images, even though two of them had been blocked for as long as two years. After 30 minutes and 3 hours of action respectively, they were taken down by their webhoster or registry. This could have been achieved much earlier. All we had to do was to send a few emails.

Background:

A Swedish blacklist leaked earlier this year was used as a source of potentially blocked domains. We then verified that these domains were blocked in Denmark on 28 September 2010, 14:20 GMT+0200 (Central European Summer Time).

Content analysis was performed from 25 to 28 September 2010 by a team which will remain anonymous for the moment to avoid legal risks for the volunteers.
Software development and technical analysis was performed from 9 to 28 September 2010 and abuse management on 25 and 28 September by Alvar Freude (Working group against access blocking and censorship, Germany).

Media Contact:

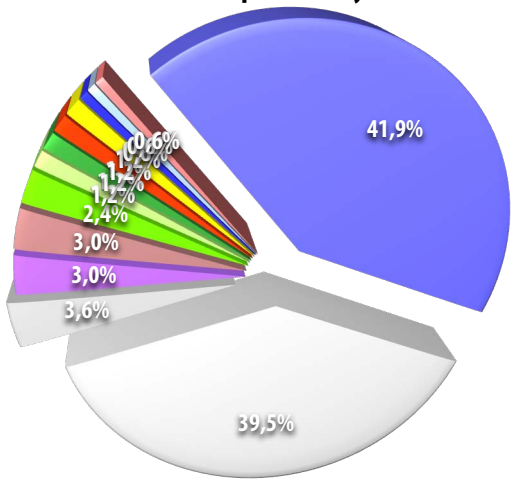
Germany/German; technical issues, takedown:
Alvar Freude, presse@ak-zensur.de
AK Zensur, http://ak-zensur.de/
Tel: +49 (0) 179 / 13 46 47 1

Sweden/Swedish:
Karin Ajaxon, karin@juliagruppen.se
http://www.juliagruppen.se/
Tel: +46 (0) 706369970

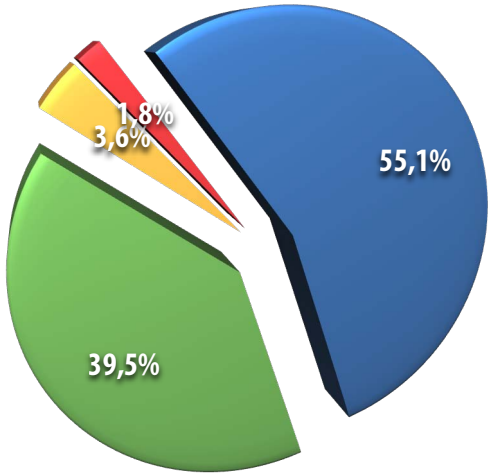
Brussels, English:
Joe McNamee, joe@mcnamee.eu
Advocacy Coordinator, European Digital Rights
http://www.edri.org/
Tel: +32 2 550 4112

Netherlands, Dutch:
Ot van Daalen, ot.vandaalen@bof.nl
Bits of Freedom, https://www.bof.nl/
Tel: +31 (0)6 5438 6680

Sites per Country



Type of blocked domains



Analysed Domains

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
2..to	67.222.20.X	US	deleted		account terminated
12.mb.com	174.142.79.X	CA	deleted		suspended
0.e-topl***.de	82.98.201.X	DE	deleted		„Die von Ihnen aufgerufene Topliste ist nicht vorhanden, zur Zeit gesperrt oder noch nicht aktiv.“
an3..ru			domain not registered or resolvable		
***llpus.in			domain not registered or resolvable		
ewq.is-se***.net	115.179.210.X	JP	deleted		not found
wihq.ura.**.jp			domain not registered or resolvable		
cq..***modelstu***.cn			domain not registered or resolvable		
cq.**.acol.com	74.54.82.X	US	deleted		

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
ir..***slola.com	69.43.160.X	AU	deleted		
lotra.free.com	205.134.160.X, 205.134.160.X	US	NOW deleted!	thumbnails of child abuse images, links	Active at least since early 2009; listed on old blacklists; links to a lot of other sites; other (linked) seem to be legal or inactive, but not checked all links **Abuse Mail sent:** 2010-09-25 04:04:35; **Auto-Reply:** 04:20:45; **checked and deleted:** 04:35 (local time at hosting location: Friday night between 22:04 and 22:35)
sf..***modelstu***.cn			domain not registered or resolvable		
sf.es.***modelstu***.cn			domain not registered or resolvable		
utifult.***mb.com	174.142.79.X	CA	deleted		suspended
seregi.***.tr			domain not registered or resolvable		
gh..***modelstu***.cn			domain not registered or resolvable		
anto.com			domain not registered or resolvable		
.sxx.info			domain not registered or resolvable		
***agur.com			domain not registered or resolvable		
ink.es.***dpr***.com	72.233.2.X, 72.233.69.X, 72.233.104.X, 72.233.127.X, 74.200.243.X, 74.200.244.X, 74.200.247.X, 74.200.247.X, 76.74.254.X, 76.74.254.X, 76.74.255.X, 76.74.255.X	US	deleted		
dygi.***mb.com	174.142.79.X	CA	deleted		missing / 404
ssicsbl.com	74.208.217.X	US	deleted		Parking domain; Page title: “Blues Guitar Lessons, The King Blues, Blues in Britain”
hy..***modelstu***.cn			domain not registered or resolvable		
erdp.ebs.com	209.25.137.X	US	deleted		“not active”
***ywad.com			domain not registered or resolvable		
kni.***o.com	127.0.0.X	--	internal IP (local)		

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
riodaputa.***star.com	69.64.147.X	US	deleted		
fd.*.acol.com	74.54.82.X	US	deleted		
rv.s.***real***.cn			domain not registered or resolvable		
tb.t.***modelstu***.cn			domain not registered or resolvable		
fn..***modelstu***.cn			domain not registered or resolvable		
***rch3.**.st	195.178.160.X	SE	deleted		
uristdr.com	74.208.216.X	US	deleted		empty, 1and1, sedoparking, perfora.net
kj.*.acol.com	74.54.82.X	US	deleted		
***cotop.com			domain not registered or resolvable		
***oys.com	64.74.223.X	US	deleted		parking
l2v.**.tv	127.0.0.X	--	internal IP (localhost)		
lsonl.**.tv	66.40.52.X	US	deleted		showing directory index
lybe.***o.com	127.0.0.X	--	internal IP (local)		
girls.mb.com	174.142.79.X	CA	deleted		missing / 404
sd..***modelstu***.cn			domain not registered or resolvable		
sd.*.acol.com	74.54.82.X	US	deleted		expired
xh..***modelstu***.cn			domain not registered or resolvable		
hb.l.***lysw***.cn			domain not registered or resolvable		
iz.es.***modelstu***.cn			domain not registered or resolvable		
ik.t.***modelstu***.cn			domain not registered or resolvable		
lia.com	74.208.216.X	US	deleted		empty, 1and1, sedoparking, perfora.net
iouyi.***ebs.com	209.25.137.X	US	deleted		"not active"
uc.*.acol.com	74.54.82.X	US	deleted		expired
uc..***modelstu***.cn			domain not registered or resolvable		
obpl.***2mb.com	127.0.0.X	--	internal IP (localhost)		
lbait.efo***.tw	58.61.157.X	CN	deleted		"The forum is closed for Containing forbidden contents"

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
aneseg.***tente***.com			domain not registered or resolvable		
qw.*.acol.com	74.54.82.X	US	deleted		expired
jp.*.acol.com	74.54.82.X	US	deleted		expired
***uwib.com			domain not registered or resolvable		
sz.t.***modelstu***.cn			domain not registered or resolvable		
sz.*.acol.com	74.54.82.X	US	deleted		expired
sz.**.acol.com	74.54.82.X	US	deleted		expired
pi.k.***wnallb***.com	208.73.210.X	US	deleted		
***gtop.**.tv	174.129.222.X	US	deleted		domain available
nd..***modelstu***.cn			domain not registered or resolvable		
hw.*.acol.com	74.54.82.X	US	deleted		expired
tvir.**.am	195.216.243.X	GB	deleted		site not found
cikmpbuh-qeaboriz.net			domain not registered or resolvable		
ipopgi.***mb.com	174.142.79.X	CA	deleted		account suspended
ov..to	67.222.20.X	US	deleted		Error: Cannot Open Links File : /home/domains/cgispy/data5/top100/randomfiles/randomlink.txt, Error No such file or direktory
***in.**.tv	174.129.222.X	US	deleted		domain available
***coll.**.ro	222.122.47.X	KR	deleted		
***2.**.st	195.178.160.X	SE	deleted		
l.teen.net	206.161.193.X	US	offline		server not answering on port 80; ping successful
civiyjeh-yiacubuk.net			domain not registered or resolvable		
***bbs.**.tv	174.129.222.X	US	deleted		domain available
ti.t.***real***.cn			domain not registered or resolvable		
wr.*.acol.com	74.54.82.X	US	deleted		expired
i789.zy.com	209.51.195.X	US	deleted		
em.*.acol.com	74.54.82.X	US	deleted		expired
ky.urf.de	85.195.104.X	DE	deleted		

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
qg.**.acol.com	74.54.82.X	US	deleted		expired
kob.***free.com	205.134.160.X, 205.134.160.X	US	NOW deleted!	thumbnails of child abuse images, links	still blocked in sweden; similar to the other domain on 100free.com **Abuse Mail sent:** 2010-09-25 04:04:35; **Auto-Reply:** 04:20:45; **checked and deleted:** 04:35 (local time at hosting location: Friday night between 22:04 and 22:35)
***unyt.com			domain not registered or resolvable		
comp.***.***lstrai***.com			domain not registered or resolvable		
si.*.acol.com	74.54.82.X	US	deleted		expired
ris.lad***.com			domain not registered or resolvable		
th.rlisti***.com			domain not registered or resolvable		
ty99.ebs.com	209.25.137.X	US	deleted		"not active"
eb..***modelstu***.cn			domain not registered or resolvable		
ix.es.***modelstu***.cn			domain not registered or resolvable		
p-boystob.***gspot.com	173.194.37.X	US	deleted		removed
fec.com	74.208.216.X	US	deleted		empty, 1and1, sedoparking, perfora.net
ny.**.acol.com	74.54.82.X	US	deleted		expired
***nhome.com	216.45.58.X	US	online		Free Porn Hoster; online since 1999; was in the list of top 5000 websites worldwide about one year ago, now in top 200000, but is not a child abuse site. Self description: *"Free Adult Web Hosting, gives you unlimited space, unlimited bandwidth, a web based file manager, a guest book, your own WWWboard, form mail, 24/7 tech support, and much more"*. **This blocked site might be one reason for high hit rates on the stop page (the page which will be shown instead of the blocked site).** Some "High Impact Search Queries" - popular search queries on search engines - which found this domain do not indicate searches for illegal content: *porn web hosting, strapse, kontakt, web hosting, kontakte* (Source: Alexa)
***alo.com	74.208.216.X	US	deleted		empty, 1and1, sedoparking, perfora.net
view.ikon.biz	89.248.168.X	NL	online	pornographic comics	Hentai site: Japanese pornographic comics (drawings)
maryst.com	74.208.216.X	US	deleted		not found

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
sy.efo***.tw	58.61.157.X	CN	deleted		"The forum is closed for Containing forbidden contents"
zi.t.***modelstu***.cn			domain not registered or resolvable		
zi.*.acol.com	74.54.82.X	US	deleted		expired
***ucyn.com			domain not registered or resolvable		
xv.*.acol.com	74.54.82.X	US	deleted		expired
gm.*.acol.com	74.54.82.X	US	deleted		expired
gm..***modelstu***.cn			domain not registered or resolvable		
gm.*.acol.com	74.54.82.X	US	deleted		expired
achki..***.com	208.71.106.X	US	deleted		403Error
qf..***modelstu***.cn			domain not registered or resolvable		
ns.l.***lysw***.cn			domain not registered or resolvable		
sy.es.***modelstu***.cn			domain not registered or resolvable		
ra..***modelstu***.cn			domain not registered or resolvable		
bast.com	74.208.216.X	US	deleted		empty, 1and1, sedoparking, perfora.net
pp.t.***modelstu***.cn			domain not registered or resolvable		
***orsex.in	95.211.108.X	NL	NOW deleted!	thumbnails of child abuse images, links	Hosted in the netherlands, domain from india. Russian language. **Abuse message sent to domain Registry NIXI (India):** 2010-09-28 09:55:04; **Auto-Reply:** 09:57:47; **Personal reply ("forwarded to the concerned team"):** 10:41:57 **Domain suspended according to Whois:** 13:08:37 (2010-09-28 11:08:37 UTC) **message with the confirmation, that the domain is suspended:** 13:43:40 **Abuse Message sent to hosting Provider:** 2010-09-28 10:08:42 **Auto-Reply:** 10:09:01 **Personal reply ("we will contact our customer"):** 11:15:30 **Additional replay ("1 hour warning"):** 11:15:52
ycot.***.org	10.6.139.X	--	internal IP		
males.eo-loli***.info	209.85.51.X	US	deleted		
ckingmov.***o.com	127.0.0.X	--	internal IP (local)		

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
***ocute.**.tv	174.129.222.X	US	deleted		
***oyo.**.tv	174.129.222.X	US	deleted		
th.rlisti***.com			domain not registered or resolvable		
qj.*.acol.com	74.54.82.X	US	deleted		expired
qj.es.***modelstu***.cn			domain not registered or resolvable		
ract.ebs.com	209.25.137.X	US	deleted		"not active"
p.iti.dk			domain not registered or resolvable		
ervideoz.***od.ru	213.180.199.X	RU	deleted		404
n.sxx.info			domain not registered or resolvable		
nief.net	67.228.238.X	US	online	legal porn	No child abuse images; All models 18+ years old according to 18 U.S.C. Section 2257 Compliance Notice
***2010.**.tv	174.129.222.X	US	deleted		
ypage.od.ru	213.180.199.X	RU	deleted		404
.w.com			domain not registered or resolvable		
.dgel***.com	74.208.214.X	US	deleted		empty, 1and1, sedoparking, perfora.net
.sxx.info			domain not registered or resolvable		
under.od.ru	93.158.135.X	RU	deleted		
ae.*.acol.com	74.54.82.X	US	deleted		expired
ae.*.acol.com	74.54.82.X	US	deleted		expired
***ube.**.tv			domain not registered or resolvable		
cb..***modelstu***.cn			domain not registered or resolvable		
ry.t.***modelstu***.cn			domain not registered or resolvable		
ry.*.acol.com	74.54.82.X	US	deleted		expired
***eoee.com	74.208.216.X	US	deleted		empty, 1and1, sedoparking, perfora.net
***zone.**.tv	174.129.222.X	US	deleted		
.ufol.com	173.201.140.X	US	deleted		"not available"
.ydof.com			domain not registered or resolvable		
.aruk.com			domain not registered or resolvable		

Blocked Domain	IPs	Hosting Country	Status	Type of Content	Info, Description
.e-l-acc***.com	208.87.34.X	US	deleted		parking
.trio***.***.ru	77.234.201.X	RU	deleted		
.dots.cn	184.105.216.X	US	deleted		domain for sale
.modelstu***.cn			domain not registered or resolvable		
.okid.com			domain not registered or resolvable		
.tal.***real***.cn			domain not registered or resolvable		
.osen.com			domain not registered or resolvable		
.nief***.net	67.228.238.X	US	online	legal porn	No child abuse images; All models 18+ years old according to 18 U.S.C. Section 2257 Compliance Notice
.nst***.cn	76.73.89.X	US	online	legal; search engine	Search engine embedded as HTML-Frame; all content from 898.com
.ujap.com			domain not registered or resolvable		
.under.***od.ru	93.158.135.X	RU	deleted		404
.eot***.**.to	175.125.92.X	KR	deleted		404
.260.com	69.163.228.X	US	deleted		
.6x.ru	92.61.146.X	DE	deleted		
.atev.com			domain not registered or resolvable		
xz.t.***modelstu***.cn			domain not registered or resolvable		
xz..***modelstu***.cn			domain not registered or resolvable		
xz.**.acol.com	74.54.82.X	US	deleted		expired
ve.*.acol.com	74.54.82.X	US	deleted		expired
***atax.com			domain not registered or resolvable		
cr.*.acol.com	74.54.82.X	US	deleted		expired
y.ehomep***.com	64.136.20.X	US	deleted		
delanizmy.***.***.com	208.71.106.X	US	deleted		
ng-bea.info	94.101.38.X	DE	online	legal, no nudity	
gn..***modelstu***.cn			domain not registered or resolvable		
***ymyx.com			domain not registered or resolvable		

About:
Most work was done by some anonymous supporters and the German Working Group against Access-Blocking and Censorship (AK Zensur); technical analysis, software development and takedown by Alvar C.H. Freude (AK Zensur).

http://ak-zensur.de/ | http://alvar.a-blast.org/

More background information:

Internet Blocking Booklet of European Digital Rights (English, German, Czech and Romanian version available):
http://www.edri.org/internet-blocking-brochure/

Some texts in German:
http://ak-zensur.de/2010/03/sperren-ueber-eu.html
http://ak-zensur.de/2010/04/kinderpornos-grossartig.html
http://ak-zensur.de/2010/08/kapitulation.html

Media Contact:

Germany/German; technical issues, takedown:
Alvar Freude, presse@ak-zensur.de
AK Zensur, http://ak-zensur.de/
Tel: +49 (0) 179 / 13 46 47 1

Sweden/Swedish:
Karin Ajaxon, karin@juliagruppen.se
http://www.juliagruppen.se/
Tel: +46 (0) 706369970

Brussels, English:
Joe McNamee, joe@mcnamee.eu
Advocacy Coordinator, European Digital Rights
http://www.edri.org/
Tel: +32 2 550 4112

Netherlands, Dutch:
Ot van Daalen, ot.vandaalen@bof.nl
Bits of Freedom, https://www.bof.nl/
Tel: +31 (0)6 5438 6680

Anlage C

Zur Stellungnahme von Alvar Freude, Fachgespräch Unterausschuss Neue Medien am 25. Oktober 2010

Bundeskriminalamt

POSTANSCHRIFT Bundeskriminalamt 65173 Wiesbaden

Per E-Mail

An die
Vorsitzende des Ausschuss für
Wirtschaft und Technologie
Frau Edelgard Bulmahn

HAUSANSCHRIFT Thaerstraße 11, 65193 Wiesbaden
POSTANSCHRIFT 65173 Wiesbaden

TEL +49(0)611 55-14676
FAX +49(0)611 55-45155
BEARBEITET VON
E-MAIL und.de

AZ SO AS 207
DATUM 09.06.09

BETREFF **Öffentliche Anhörung des Ausschusses für Wirtschaft und Technologie zum Gesetz zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen am 27.05.09**

BEZUG Ihre Nachfrage zu Serverstandorten

Sehr geehrte Frau Bulmahn,

im Rahmen der Öffentlichen Anhörung am 27.05.09 baten Sie um Übermittlung einer Aufstellung zu den Staaten, in denen Server mit kinderpornografischen Inhalten stehen.

Nach hiesigen Erkenntnissen werden Webseiten mit nach deutschem Recht als kinderpornografisch einzustufenden Inhalten fast ausschließlich über Server im Ausland bereitgestellt.

Einerseits werden Staaten mit geringer Kontrollintensität oder solche in denen keine Gesetzgebung gegen Kinderpornografie existiert oder die entsprechenden Regelungen nicht konsequent durchgesetzt und überwacht werden. Hierzu zählen insbesondere Staaten in Osteuropa und Asien.

Andererseits sind auch regelmäßig Staaten betroffen, auf die diese Kriterien nicht zutreffen. Besonders technisch und wirtschaftlich entwickelte Staaten mit intensiv ausgebauter Internet-Infrastruktur/Internetwirtschaft (gilt z.B. insbesondere für die USA) werden von Tätern bevorzugt. Trotz der bestehenden Strafbarkeit und entsprechenden Strafverfolgungsmaßnahmen/Kontrolldichte in diesen Staaten ist von einer besonderen Dynamik der Flüchtigkeit der Inhalte auszugehen. Von den Tätern wird einerseits die Infrastruktur genutzt, andererseits

BKA

besteht das Bestreben das Strafverfolgungsrisiko zu minimieren. Dies dürfte Ursache für einen häufigen Wechsel der Speicherorte sein. Selbst einmal gelöschte Inhalte können an einer Vielzahl anderer „Orte" im Netz kurzfristig neu und/oder parallel gehostet werden und stehen wieder für den Zugriff zur Verfügung.

Über eigene statistische Erhebungen zu den Standorten von Servern verfügt das Bundeskriminalamt nicht, so dass wir Ihnen eine solche Liste nicht zur Verfügung stellen können.

Dem Bundeskriminalamt liegt jedoch eine Auswertung der dänischen Strafverfolgungsbehörden vor, wonach im Zeitraum Oktober 2008 bis Januar 2009 die durch die dortigen Access-Blocking-Maßnahmen betroffenen Domains in den nachfolgend aufgeführten Ländern gehostet wurden (nach Häufigkeit geordnet):

USA:	1148
Deutschland:	199
Niederlande:	79
Kanada:	57
Russland:	27
Japan:	20
Korea:	19
Tschechien:	15
Großbritannien:	14

Der dänischen Statistik ist zu entnehmen, dass neben den USA und Staaten in Europa und Asien eine ganze Reihe weiterer Staaten aus dem südamerikanischen, südostasiatischen und mittelosteuropäischen Raum betroffen sind.

Bei der Interpretation der genannten Zahlen ist zu berücksichtigen, dass die Strafbarkeit von Kinderpornografie in Dänemark erheblich weitergehender gefasst ist als in Deutschland. Das diesbezügliche Schutzalter in Dänemark beträgt 18 Jahre (Deutschland: 14 Jahre) und inhaltlich reicht die bloße Abbildung der sichtbaren Genitalien aus (Deutschland: sexuelle Handlungen erforderlich).

Insofern ist davon auszugehen, dass ein erheblicher Teil der in Dänemark (und anderen skandinavischen Staaten mit vergleichbarer Gesetzeslage) auf den Sperrlisten befindlichen Webinhalte nicht die Tatbestandsmerkmale des § 184b StGB, d.h. für Kinderpornografie nach deutschem Recht, erfüllt. Gleiches dürfte auch für andere Staaten gelten, die sich an der Spitze der dänischen Statistik befinden.

Die von Dänemark ermittelten Zahlen zur geografischen Verteilung des Hostings kinderpornografischer Inhalte haben keine direkte Aussagekraft zur Bewertung der Situation aus deutscher Sicht. Trotz der unterschiedlichen Tatbestandsvorrausetzungen der Kinderpornografie

liefern die Daten aus Dänemark jedoch einen ersten – wenn auch zurückhaltend zu bewertenden - Indikator für die bisherigen Aussagen des Bundeskriminalamtes zu den Serverstandorten.

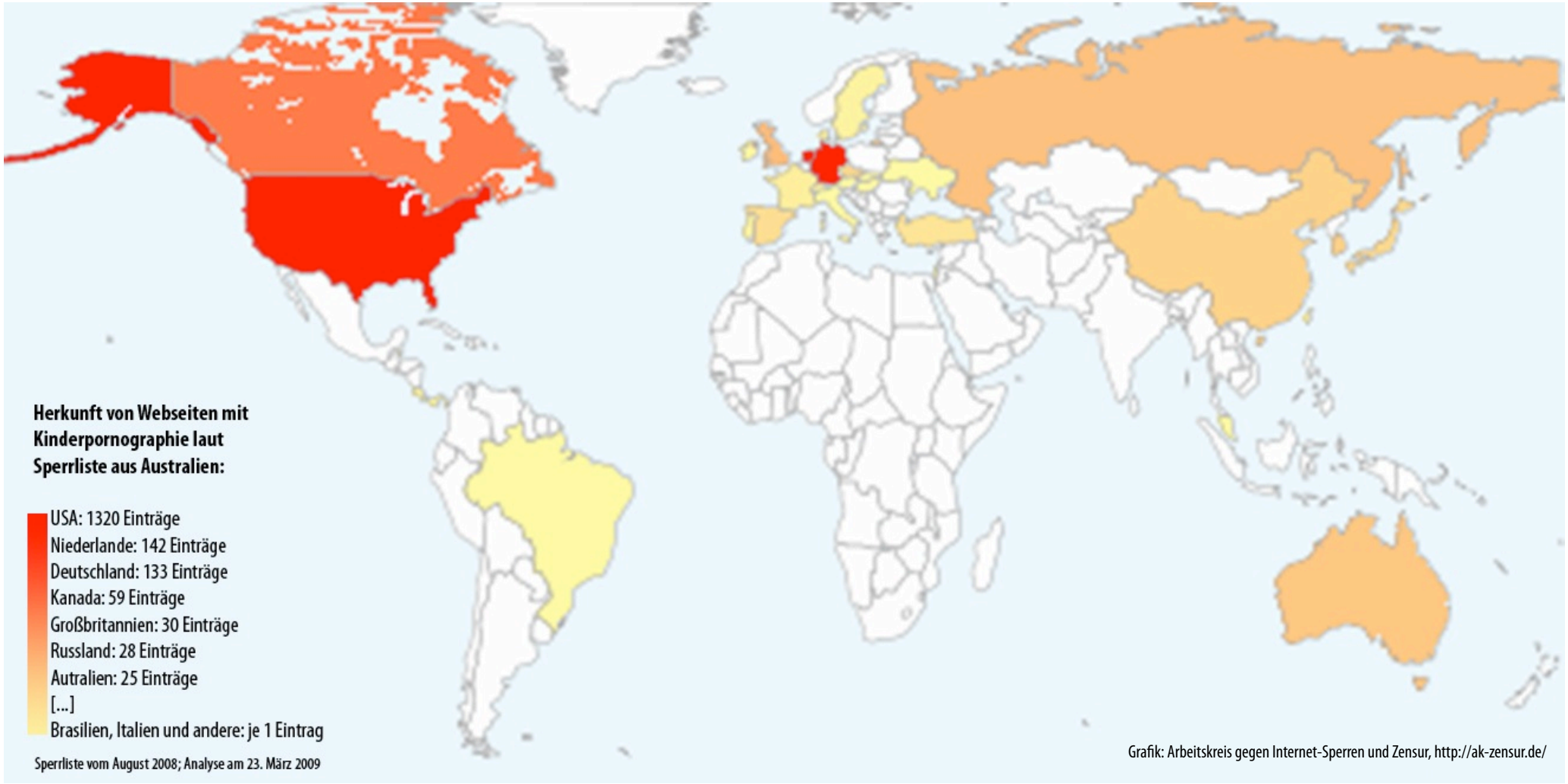
Mit freundlichen Grüßen
im Auftrag

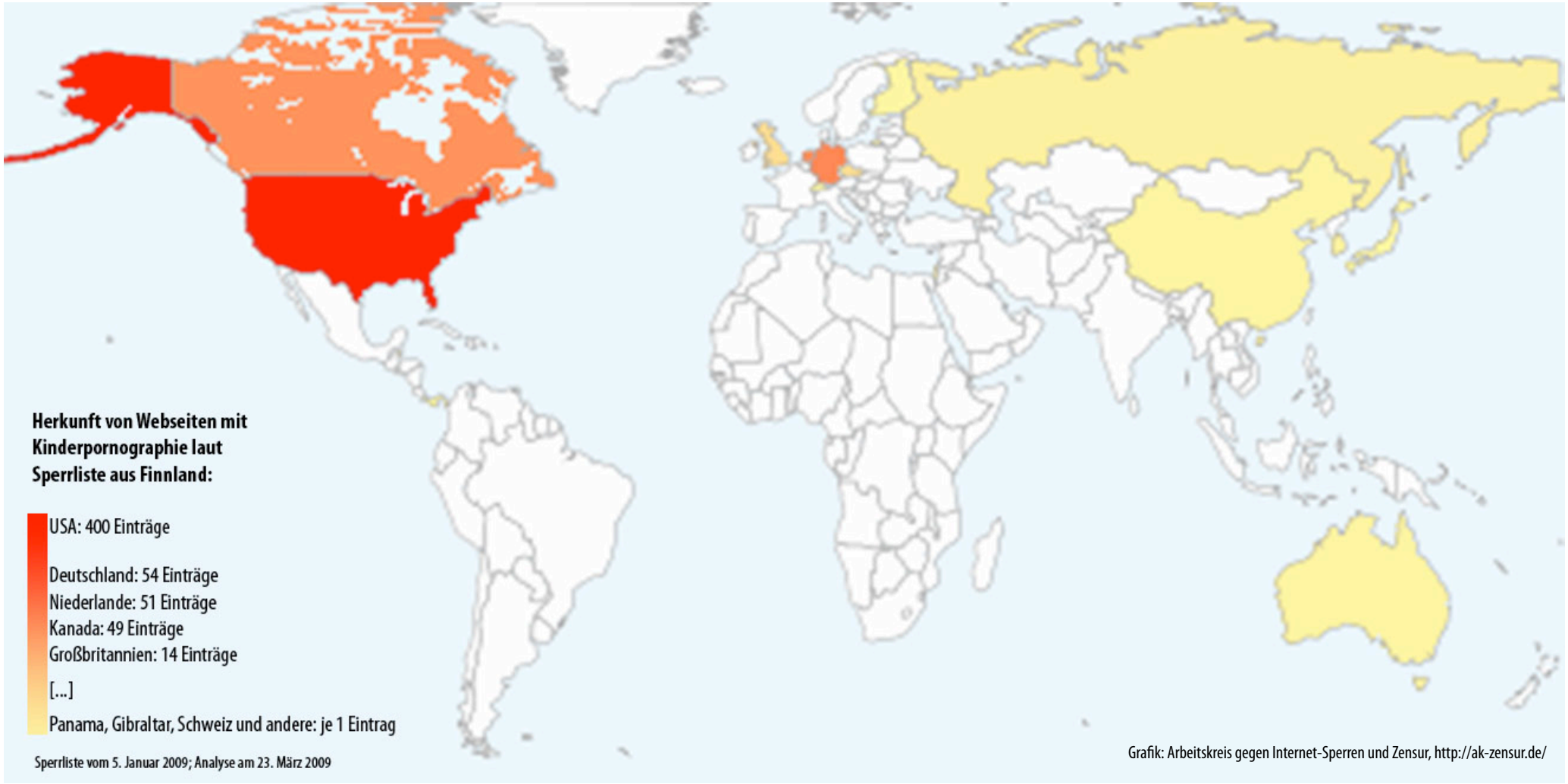
gez.
Jürgen Maurer
Direktor beim Bundeskriminalamt

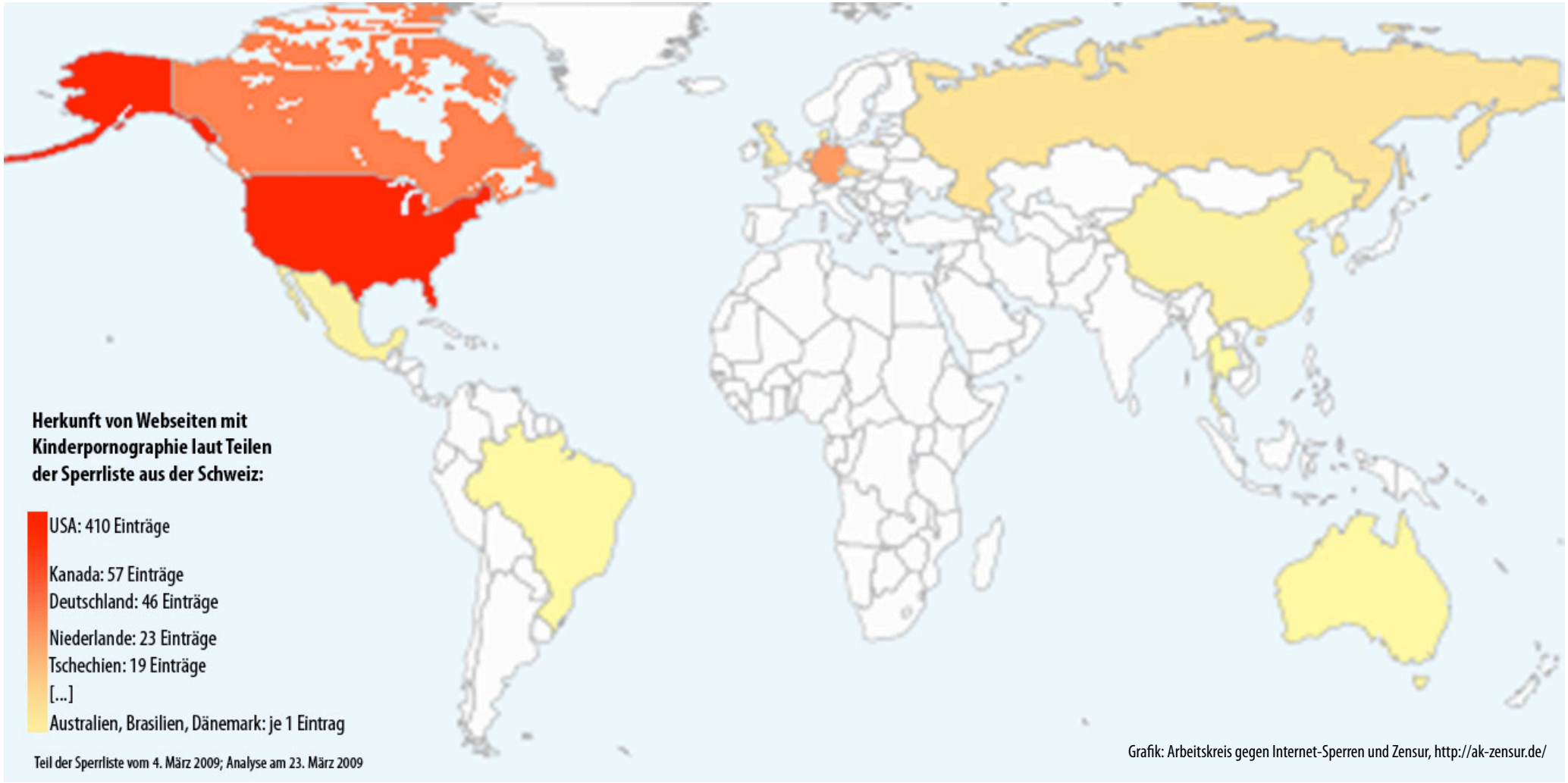
Beglaubigt:
Lob

Anlage D

Zur Stellungnahme von Alvar Freude, Fachgespräch Unterausschuss Neue Medien am 25. Oktober 2010

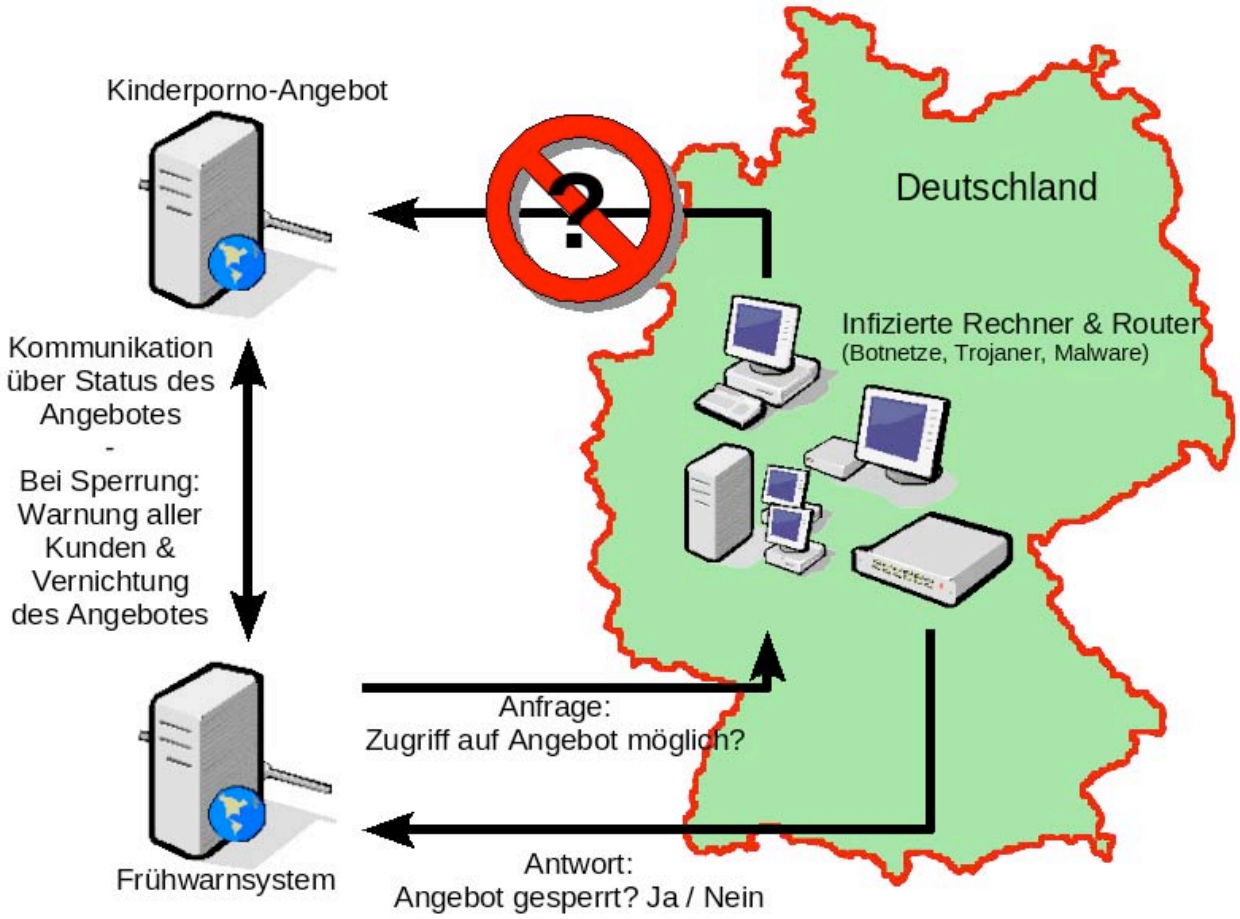



Herkunft von Webseiten mit Kinderpornographie laut Sperrliste aus Finnland:
USA: 400 Einträge
Deutschland: 54 Einträge
Niederlande: 51 Einträge
Kanada: 49 Einträge
Großbritannien: 14 Einträge
[...]
Panama, Gibraltar, Schweiz und andere: je 1 Eintrag
Sperrliste vom 5. Januar 2009; Analyse am 23. März 2009
Grafik: Arbeitskreis gegen Internet-Sperren und Zensur, http://ak-zensur.de/


Herkunft von Webseiten mit Kinderpornographie laut Teilen der Sperrliste aus der Schweiz:
USA: 410 Einträge
Kanada: 57 Einträge
Deutschland: 46 Einträge
Niederlande: 23 Einträge
Tschechien: 19 Einträge
[...]
Australien, Brasilien, Dänemark: je 1 Eintrag
Teil der Sperrliste vom 4. März 2009; Analyse am 23. März 2009
Grafik: Arbeitskreis gegen Internet-Sperren und Zensur, http://ak-zensur.de/

Anlage E

Zur Stellungnahme von Alvar Freude, Fachgespräch Unterausschuss Neue Medien am 25. Oktober 2010



Quelle: http://wiki.ak-zensur.de/index.php/Datei:Netzsperren-Fruehwarnsystem.png