KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK

Jahresbericht 2011

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
Nussbaumstrasse 29
3003 Bern

www.kobik.ch
www.cybercrime.ch

Veröffentlicht: 03.04.2012

Inhaltsverzeichnis

1. Das Wichtigste in Kürze

- Bei KOBIK gingen 2011 insgesamt 5‘330 Meldungen über das Online-Meldeformular ein. Das entspricht einem Rückgang von fast 14% gegenüber dem Vorjahr.

- Trotz des Rückgangs im Vergleich zum Vorjahr bleibt „harte Pornografie“ (insbesondere Kinderpornografie) die meistgemeldete Kategorie.

- Durch das aktive Monitoring in P2P-Netzwerken gelang es KOBIK im Berichtsjahr 214 Personen zu identifizieren, welche aktiv am Austausch von Kinderpornografie beteiligt waren. Wer Kinderpornografie konsumiert, fördert die Herstellung von neuem Bildmaterial und ist somit selbst indirekt am Kindsmissbrauch beteiligt.

- Ein erneuter Anstieg der Meldungen konnte bei den Fällen der Kategorien „Wirtschaftskriminalität“ festgestellt werden.

- Grosse Fortschritte erzielte KOBIK im Projekt Nationale Datei- und Hashwertesammlung (NDHS). Die kantonalen Polizeikorps wurden im Berichtsjahr erfolgreich geschult. Die ersten kantonalen Bildarchive wurden bereits an KOBIK übergeben.

- KOBIK ist seit Mai 2011 im Projektteam der Nationalen Strategie Cyber Defense und wird auch bei der Umsetzung der Strategie die Interessen der kantonalen und nationalen Strafverfolgungsbehörden vertreten.

- Die internationale Kooperation bei der Bekämpfung der Internetkriminalität konnte in enger Zusammenarbeit mit Interpol und Europol massgeblich ausgebaut werden.

2. Meldungseingang

Im Jahr 2011 gingen bei KOBIK 5’330 Verdachtsmeldungen per Internet-Meldeformular ein. Dies entspricht einem Rückgang von fast 14% gegenüber dem Vorjahr (6’181 Meldungen). Mit Ausnahme des Rekordjahres 2007 lag das Jahresmittel der Meldungen via Internet-Meldeformular stabil zwischen 6'000 und 7'500 Verdachtsmeldungen. Die Entwicklung des Meldungseinganges erlaubt keine Rückschlüsse auf die effektive Entwicklung der Internetkriminalität oder illegale Inhalte im Internet. Daraus lassen sich aber Tendenzen über die Meldebereitschaft der Bevölkerung und der Wahrnehmung von Internetkriminalität in der Gesellschaft ableiten. Die Gründe für den Rückgang der Meldungen über das Meldeformular können vielseitig sein. Möglicherweise sind verschiedene Arten der Internetkriminalität bereits so alltäglich, dass sie durch die Bevölkerung banalisiert werden und Betroffene auf eine Meldung an KOBIK verzichten. Im Vergleich zu den Vorjahren gingen im Berichtsjahr so weniger Meldungen ein, diese sind qualitativ jedoch nützlicher. Am Wahrscheinlichsten scheint, dass die tiefere Zahl der Meldungen im Berichtsjahr auf das Ausbleiben von Vorfällen mit grosser medialer und gesellschaftlicher Wirkung zurückzuführen ist.

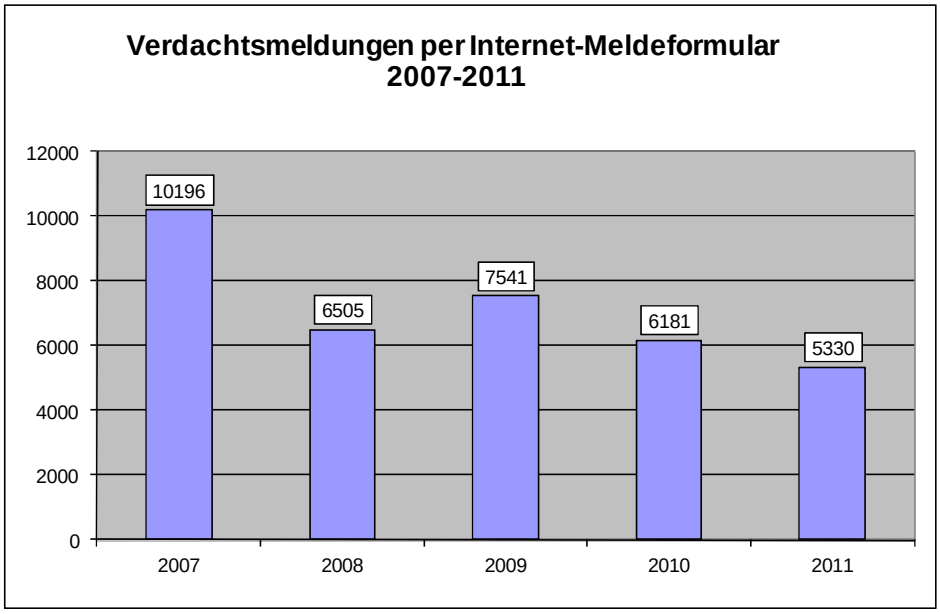

Abbildung 1 : Meldungseingänge über www.kobik.ch im Jahresvergleich

Die Meldungseingänge pro Monat waren im Berichtsjahr konstant (vgl. Abbildung 2). Abweichungen lassen sich oftmals auf konkrete und zeitlich begrenzte Ereignisse zurückführen. Dies unterstützt die Theorie, dass der Rückgang der Meldungen im Berichtsjahr in erster Linie auf das Ausbleiben grosser Vorfälle zurückzuführen ist.

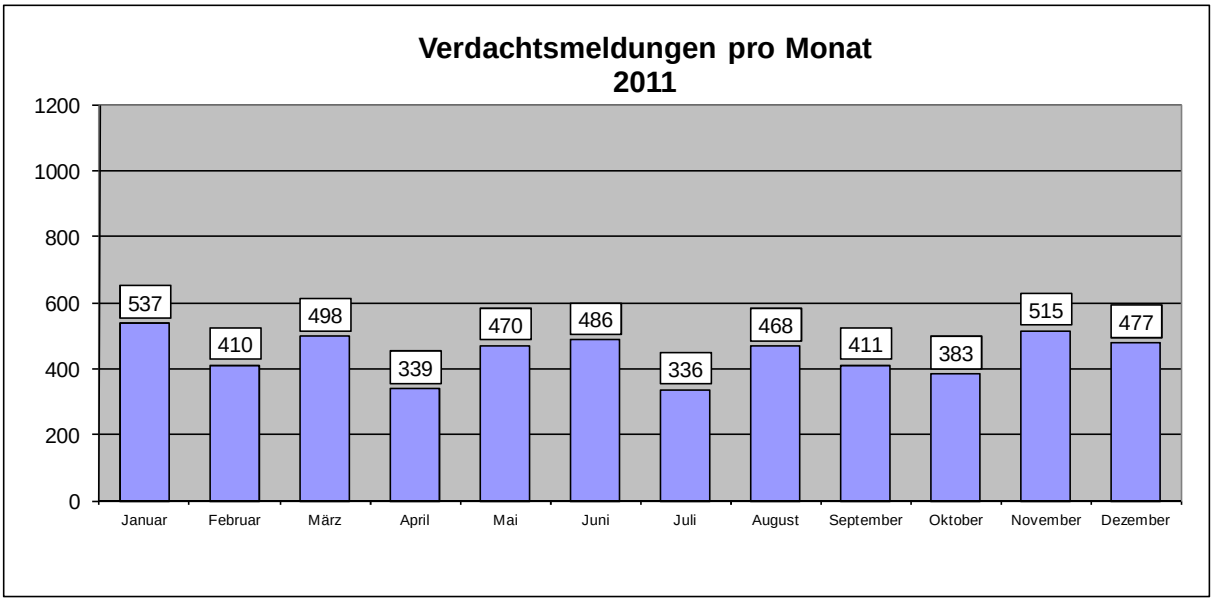

Abbildung 2 : Meldungseingänge über www.kobik.ch im Monatsvergleich (Total 5330 Meldungen)

3. Was wurde gemeldet?

Bei den Meldungseingängen nach Kategorie fällt im Vegleich zum Vorjahr vor allem der markante Rückgang von Meldungen im Bereich **«harte Pornografie»** auf (vgl. Abbildung 3). In diese Kategorie fallen Meldungen über unterschiedliche Tatbestände der Pornografie gemäss Art. 197 Abs. 3 StGB . 90% der Meldungen dieser Kategorie betreffen den Tatbestand der Kinderpornografie. Der Rückgang der Meldungen an KOBIK über das Online-Meldeformular in dieser Kategorie steht in direktem Zusammenhang mit der generellen Abnahme der Meldungen. Daraus kann jedoch nicht geschlossen werden, dass solche Inhalte und Verstösse im Internet effektiv abgenommen haben. Dies bestätigen sowohl die tägliche Arbeit von KOBIK als auch der Informationsaustausch mit den nationalen und internationalen Partnern. Der Rückgang der Meldungen ist in erster Linie darauf zurückzuführen, dass diese Inhalte öffentlich immer weniger sichtbar sind. Pädophile ziehen sich bewusst in geschlossene oder nur schwer zugängliche Plattformen (Foren, Gruppen, soziale Netzwerke) zurück, was ihnen einen diskreteren und anonymeren Austausch von kinderpornografischem Material erlaubt. Trotz des Rückganges im Vergleich zum Vorjahr, bleibt „harte Pornografie“ (insbesondere Kinderpornografie) die Kategorie mit den meisten Meldungen.

Nachdem die Meldungen in der Kategorie **«allgemeine Pornografie»** im letzten Jahr zurückgegangen sind, nahmen sie im Berichtsjahr wieder leicht zu. Im Gegensatz dazu gingen die Meldungen in der Kategorie **«SPAM»** das vierte Jahr in Folge zurück. Diese Zahlen verdeutlichen, dass die Entwicklung der Meldungen an KOBIK nicht im Einklang mit der reellen Entwicklung der Kriminalität im Internet stehen muss. Studien über die SPAM-Entwicklung konnten für 2011 weltweit zwar einen leichten Rückgang von SPAM feststellen[1], einen bereits mehrjährigen Rückgang konnte aber keine der Studien nachweisen. Möglicherweise sind Betroffene gegenüber SPAM generell gleichgültiger geworden und verzichten deshalb auf eine Meldung an KOBIK. Zudem haben immer besser funktionierende SPAM-Filter dazu geführt, dass unerwünschte Meldungen frühzeitig erkannt und so durch den Benutzer gar nicht mehr wahrgenommen werden.

Bei der **«Wirtschaftskriminalität»**[2] fällt vor allem der Anstieg von 53% bei den Meldungen der Kategorie **«Betrug»** auf. Damit bestätigt sich die Tendenz der Vorjahre. Insbesondere Personen, die ihre Einkäufe über Online-Tauschbörsen oder Kleinanzeigen (Autos, Wohnungen, Elektrogeräte usw.) tätigen, stehen im Fokus von meist ausländischen Betrügern. Auf den gleichen Internetseiten werden auch die Verkäufer mittels falscher Zahlungsbestätigungen oder nachträglich erhobenen Rückerstattungen um ihr Geld geprellt. Die sogenannten Vorschussbetrügereien, bei denen ein grosser Gewinn (z.B. Lotterie) gegen eine kleine Gebühr versprochen wird, sind nach wie vor aktuell. Neben den eigentlichen Vorschüssen, interessieren sich die Betrüger zunehmend auch für die persönlichen Daten und Ausweisschriften ihrer Opfer (Kopie von Pass oder ID). Wer persönliche Informationen weitergibt, muss heutzutage damit rechnen, dass seine Identität von der Täterschaft für weitere Betrügereien missbraucht wird.

---

[1] Siehe z.B. McAfee Threats Reports ;
http://www.mcafee.com/apps/view-all/publications.aspx?pg=1&sz=10&tf=mcafee_labs

[2] Statistik Wirtschaftskriminalität setzt sich aus Betrugs- und Wirtschaftsdelikten (vor allem Phising, Geldwäscherei) zusammen

Auch die Meldungen zu **anderen Wirtschaftsdelikten** (insbesondere Phishing- und Geldwäschereifälle) haben mit 28% markant zugenommen. Immer wieder wurde die Bevölkerung in der Schweiz im Berichtsjahr von Phishing-Versuchen heimgesucht. Dabei haben es die Täter hauptsächlich auf die Zugangsdaten von E-Banking-Konten und Online-Tauschbörsen abgesehen.

Die konstant hohe Anzahl Anfragen um Informationen oder Unterstützung bestätigen, dass die Bevölkerung und die Internet Service Provider (ISP) in KOBIK ein Kompetenzzentrum im Bereich der Internetkriminalität sehen.

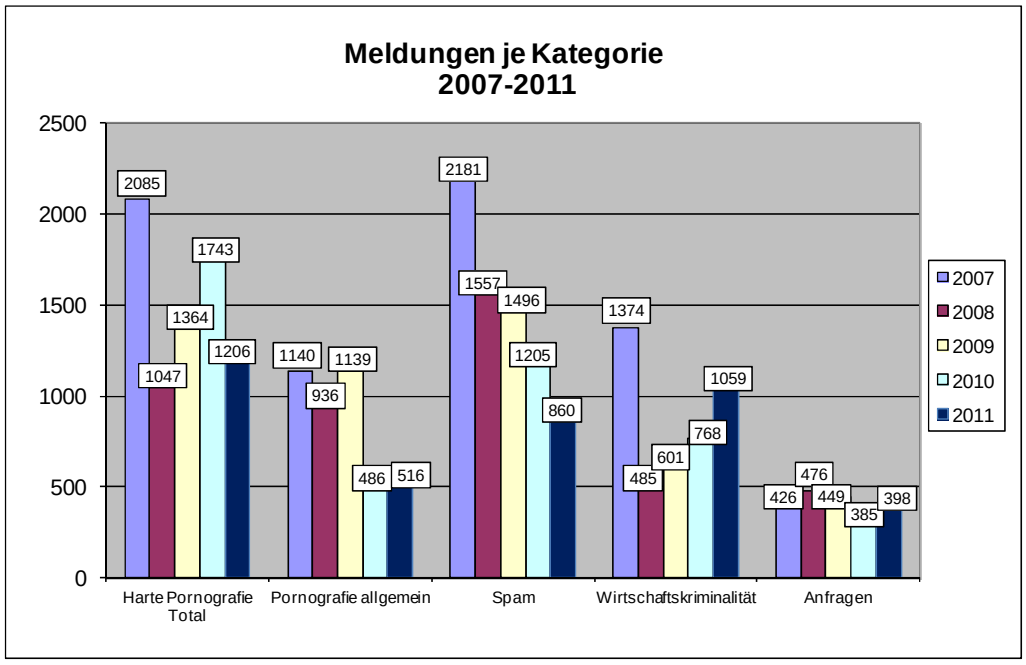

Abbildung 3 : Entwicklung der Kategorien von Straftaten mit den meisten Meldungen

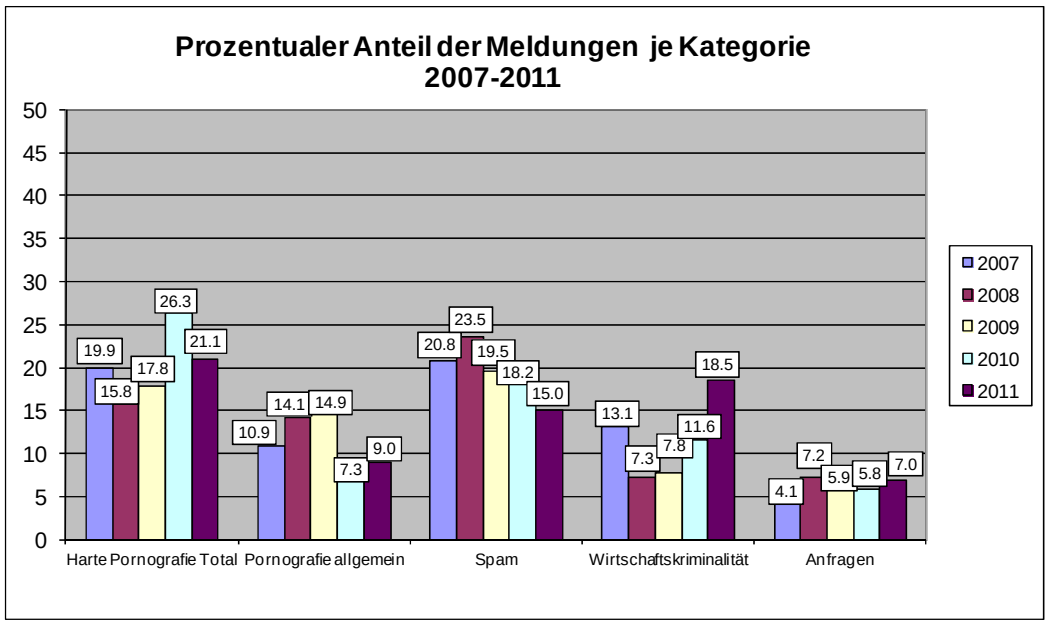

Abbildung 4 : Prozentualer Anteil ausgewählter Kategorien im Fünfjahresvergleich

Wie jedes Jahr gingen über das Meldeformular Meldungen zu verschiedensten Straftaten bei KOBIK ein. Die Abbildung 4 gibt einen Überblick über die Entwicklung

der wichtigsten Deliktskategorien in den letzten fünf Jahren. Eine auffallende Zunahme konnte bei den Meldungen der Kategorien **«Ehrverletzungsdelikte»** (von 0,70% auf 1,97%) und **«Drohung / Nötigung»** (von 0,42% auf 0,67%) registriert werden. Kriminelle benutzen in diesen Fällen vermehrt soziale Netzwerke als Tatwerkzeug. Die Kategorien „Ehrverletzungsdelikte“ und „Drohung und Nötigung“ enthalten auch 30 Fälle von **«Cyberbullying[3]»** (davon mindestens fünf, bei denen Minderjährige betroffen waren).

Im Bereich der Internetkriminalität nahmen die Meldungen in den Kategorien **«Unbefugtes Eindringen in eine Datenverarbeitungsanlage»** (von 0.44% auf 0.84%) und **«Datenbeschädigung»** (0.57% auf 1.29%) zu. KOBIK wurden verschiedene Angriffe auf Informatiksysteme von Privatpersonen gemeldet. Besonders genannt sei hier der Angriff einer Malware, welche in der Schweiz die Computer von unzähligen Personen blockierte und diese zur Zahlung einer Freischaltungsgebühr aufforderte (vgl. Kapitel 5, Fallbeispiele). Diese Entwicklung wird von KOBIK eng verfolgt.

[3] Cyberbullying: wenn mit Hilfe moderner Kommunikationsmittel diffamierende Texte, Bilder oder Filme veröffentlicht werden, um Personen zu verleumden, blosszustellen oder zu belästigen.

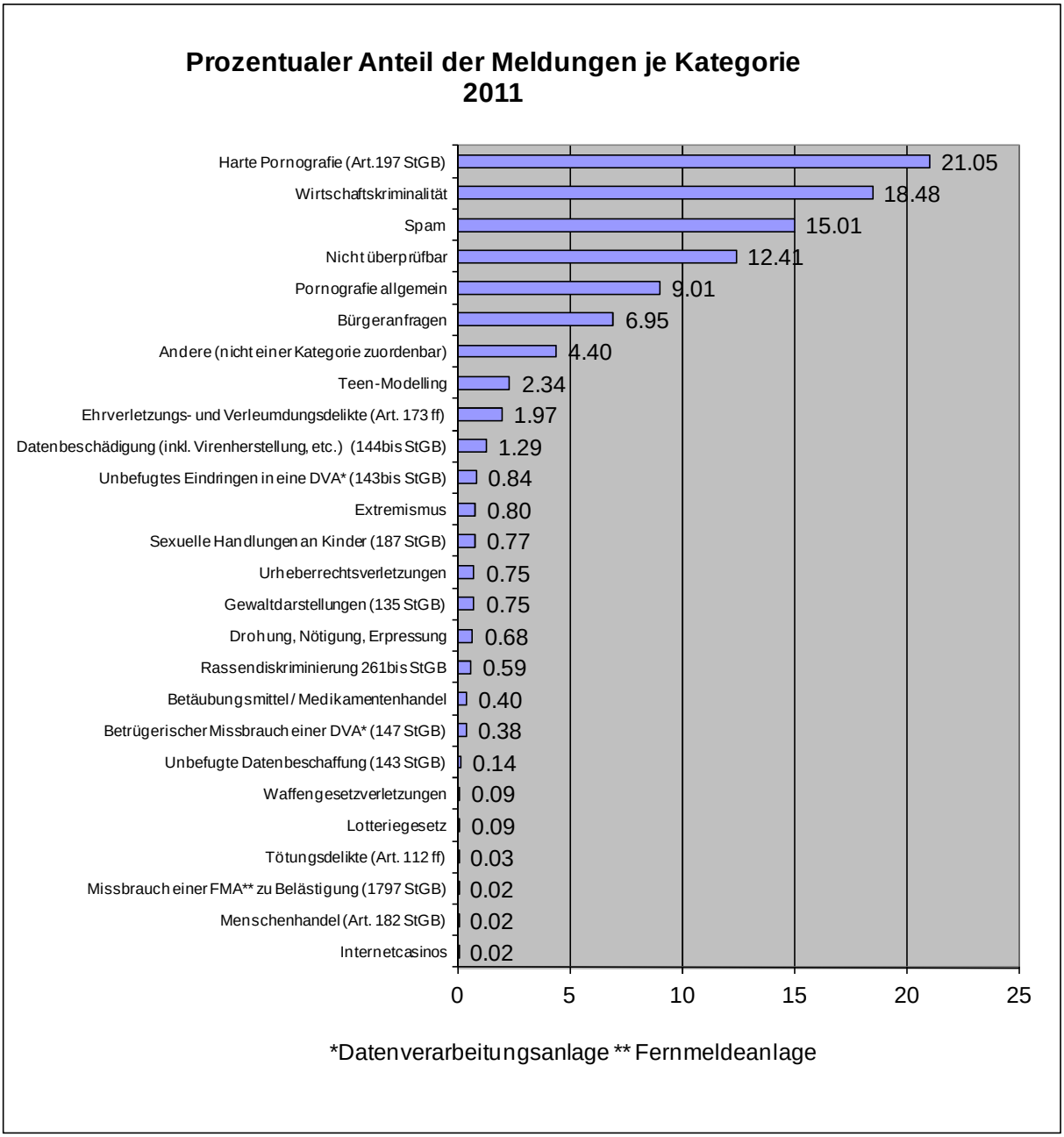

Abbildung 5 : Übersicht der kategorisierten Meldungen 2011 (prozentualer Anteil aller Meldungen)

4. Aktive Recherche (Monitoring)

KOBIK beschränkt sich nicht nur auf die Entgegennahme und Bearbeitung von Meldungen aus der Bevölkerung. Mit verdachtsunabhängigen Recherchen im Internet ist KOBIK auch in weniger zugänglichen Bereichen des Internet präsent und erzielt dadurch eine präventive Wirkung. Der Leitungsausschuss KOBIK legt den Schwerpunkt der aktiven Recherche jedes Jahr neu fest. Wie bereits in den Vorjahren wurde der Schwerpunkt der aktiven Recherchen auch 2011 auf die Bekämpfung der Pädokriminalität im Internet gesetzt. Jedoch hat der Leitungsausschuss explizit festgehalten, dass sich KOBIK den Wirtschaftsdelikten und der Internetkriminalität im engeren Sinn nicht verschliessen darf.

Aufgrund der aktiven Recherchen konnten 2011 insgesamt 225 Verdachtsdossiers erstellt werden. Damit wurde das hohe Niveau des Vorjahres bestätigt.

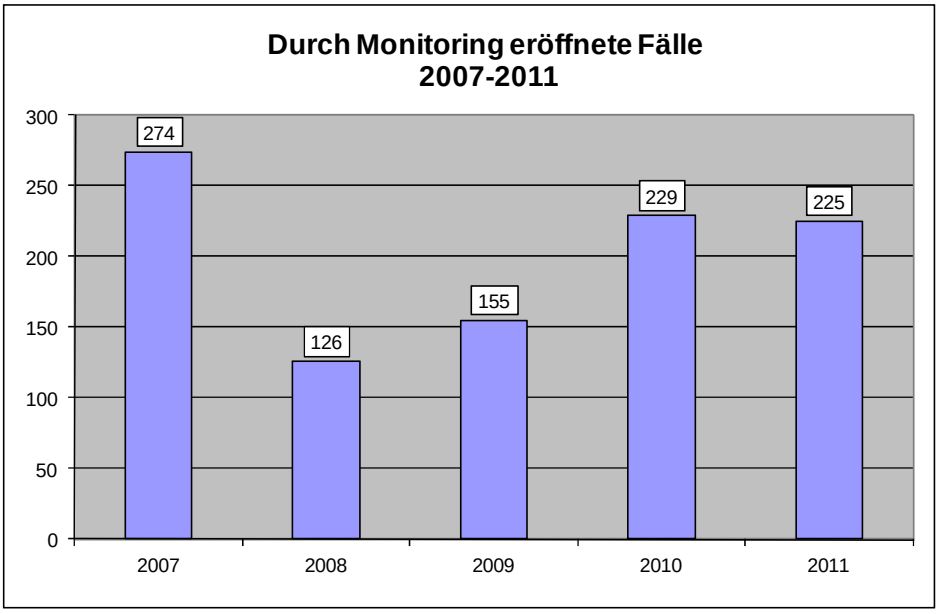

Abbildung 6: In Folge von aktiven Recherchen eröffnete Verdachtsdossiers

4.1 Aktive Recherchen in P2P-Netzwerken

Die Mehrheit der Verdachtsdossiers (214 von 225) resultiert aus der Überwachung von P2P-Netzwerken nach Internetbenutzern, die sich in der Schweiz aktiv am Austausch von kinderpornografischen Dateien beteiligen. P2P-Netzwerke sind nach wie vor eines der beliebtesten Mittel, um relativ anonym übers Internet Daten auszutauschen.

Obwohl KOBIK spezifisch nach Benutzern in der Schweiz sucht, wurden im Berichtsjahr auch Straftaten von zwei Personen aus dem Ausland festgestellt. KOBIK hat die Erkenntnisse den zuständigen Ländern via Interpol übermittelt.

4.2 Verdachtsunabhängige verdeckte Ermittlungen in Chats und Sozialen Netzwerken

Am 1. Januar 2011 ist die neue Eidgenössische Strafprozessordnung (StPO) in Kraft getreten. Dadurch wurde dem Bund die Kompetenz für verdachtsunabhängige verdeckte Ermittlungen entzogen. Die Kompetenz obliegt seither ausschliesslich bei den Kantonen und muss durch diese in den einzelnen kantonalen Polizeigesetzen geregelt werden. Da nur wenige Kantone am 1. Januar 2011 eine entsprechende Gesetzesgrundlage vorweisen konnten, wurde befürchtet, dass ein rechtsfreier Raum entstehen könnte.

Damit dies nicht eintrifft, fand das Bundesamt für Polizei (fedpol) gemeinsam mit dem Kanton Schwyz eine Lösung und schloss am 23.12.2010 eine unbefristete Vereinbarung ab. Die „Vereinbarung betreffend Zusammenarbeit bei den polizeilichen Vorermittlungen im Internet zur Bekämpfung der Pädokriminalität (Monitoring von Chat-Räumen)“ zwischen KOBIK, dem Sicherheitsdepartement des Kantons Schwyz und dem Bundesamt für Polizei (fedpol) regelt die Modalitäten des Einsatzes von KOBIK-Mitarbeitenden als verdeckte Vorermittler zur Bekämpfung der Pädokriminalität im Internet[4]. In diesem Sinne üben die Mitarbeitenden von KOBIK die verdeckte Vorermittlung ausschliesslich im Auftrag und unter Kontrolle der Kantonspolizei Schwyz aus. Damit ist gewährleistet, dass das Monitoring im Bereich Pädokriminalität im Internet auch im Sinne präventiver verdeckter Fahndungen im Internet weiterhin vorgenommen werden kann. Mit Verfügung vom 14.01.2011 genehmigte das Zwangsmassnahmengericht des Kantons Schwyz die Ernennung von sechs Mitarbeitenden von KOBIK zu verdeckten Vorermittlern. Mit Verfügung vom 11. Januar 2012 verlängerte das Zwangsmassnahmengericht des Kantons Schwyz die bestehende Ernennung der verdeckten Vorermittler mit Wirkung bis zum 14. Juli 2012 sowie verfügte die Ernennung von zwei weiteren KOBIK-Mitarbeitenden als verdeckte Vorermittler.

Im Anschluss an die Verfügung des Zwangsmassnahmengerichts realisierte KOBIK verschiedene technische und operative Aufbauarbeiten. Die notwendige Ausbildung innerhalb von KOBIK und die Definition der Prozesse mit den Kantonen und fedpol nahm aufgrund der zur Verfügung stehenden Ressourcen eine gewisse Zeit in Anspruch.

Im Jahr 2011 wurden 16 Fälle nach Schwyzer-Verordnung abgehandelt. Folgende Massnahmen wurden ausgelöst:

- Fünf Hausdurchsuchungen mit Befragungen vom Tatverdächtigen;
- Eine Befragung von einem Tatverdächtigen;
- Vier Fälle werden durch die zuständigen Staatsanwaltschaften noch geprüft;
- In einem Fall hat die Staatsanwaltschaft auf Nichteintreten entschieden;
- Vier Fälle konnten mangels Identifikation des Täters oder Konkretisierung eines hinreichenden Anfangsverdachts nicht weiter verfolgt werden;
- Ein Fall ist bei KOBIK noch pendent und weitere Ermittlungen werden noch getätigt.

[4] Einsatz im Sinne von § 9d der Verordnung des Kantons Schwyz über die Kantonspolizei vom 22.03.2000 (PolV – SRSZ 520.110).

Die Auswertung des Materials, das bei den Hausdurchsuchungen sichergestellt wurde, war Ende 2011 noch nicht abgeschlossen. Beurteilungen durch die zuständigen Gerichte lagen ebenfalls noch nicht vor.

5. Ausgewählte Fallbeispiele

KOBIK behandelte und koordinierte im Berichtsjahr ganz unterschiedliche Fälle. Die folgenden ausgewählten Fallbeispiele vervollständigen die Analyse der rein statistischen Zahlen und ermöglichen einen qualitativen Einblick in die Tätigkeit von KOBIK.

Im ersten Quartal des Berichtsjahres wurde im Rahmen der Überwachung von P2P-Netzwerken gegen eine Person ermittelt, die kinderpornografische Bilder und Videos heruntergeladen und anderen zur Verfügung gestellt hat. Bei der anschliessenden Hausdurchsuchung durch die zuständige Kantonspolizei gestand der Verdächtige nicht nur die Straftat im Bereich Kinderpornografie, er gab ausserdem zu, sich bereits mehrfach an Kleinkindern vergangen zu haben. Bei dem Täter handelte es sich um einen der Polizei noch unbekannten Kleinkinderzieher, der als Betreuer in einer Kinderkrippe tätig war. Das jüngste seiner Opfer war lediglich drei Jahre alt. In diesem Fall konnte dank der Überwachung von P2P-Netzwerken ein Pädokrimineller entlarvt und weitere Straftaten an Kindern verhindert werden.

In einem weiteren Fall war eine ausländische Strafverfolgungsbehörde im Rahmen verdeckter Ermittlungen auf Informationen gestossen, die darauf hindeuteten, dass ein Schweizer Bürger in Kürze nach Grossbritannien fliegen würde, um sich dort an einem Minderjährigen sexuell zu vergehen. Diese Information leitete die Behörde an KOBIK weiter. Abklärungen von KOBIK ergaben, dass der Verdächtige bereits mehrfach wegen sexueller Delikte mit Minderjährigen aufgefallen und auch schon rechtskräftig verurteilt war. Dank der engen Zusammenarbeit zwischen den beiden involvierten Ländern und des Internetdienstanbieters, der die Identifizierung der verdächtigten Person ermöglichte, konnte der Schweizer Bürger bei der Einreise in Grossbritannien festgenommen werden. Im Gepäck mitgeführtes Material erhärtete den Verdacht, dass der Mann tatsächlich einen Minderjährigen sexuell missbrauchen wollte. Neben einer Hotelreservation, die auf ihn selbst und eine minderjährige Person lautete, wurden auch eine Videokamera und eine beachtliche Menge an Aufnahmebändern sichergestellt. Dieser Fall zeigt auf, dass enge und zeitgerechte Zusammenarbeit der betroffenen Staaten und Internetdienstleister über eine zentrale nationale Ansprechstelle entscheidend für eine erfolgreiche Strafverfolgung ist. Ohne die verdeckten Ermittlungen durch die ausländische Strafverfolgungsbehörde wäre es nie zu einer Verhaftung des Täters vor Begehung der Tat gekommen.

Über das KOBIK-Meldeformular informierte ein Bürger über ein Forum, in dem ein Benutzer seine 13-jährige Tochter für den sexuellen Missbrauch anbot. Abklärungen von KOBIK führten zur Identifizierung der verdächtigen Person. Die anschliessende Befragung durch die zuständige Kantonspolizei ergab, dass der Verdächtige gar keine Tochter hat. Seine Äusserungen waren lediglich sexuelle Phantasien ohne Bezug zur Realität. Der Fokus der Ermittlungen richtete sich fortan auf die Vielzahl von Personen, die sich auf das Angebot per E-Mail meldeten und Interesse an dem minderjährigen Mädchen bekundeten. Bei der Identifizierung der verdächtigen Personen haben zwei verdeckte KOBIK-Ermittler den zuständigen Kanton für die Dauer der Abklärungen nach StPO unterstützt. Diese Zusammenarbeit führte Anfangs 2012 schlussendlich zur Festnahme von mehreren Personen in der Schweiz. Sämtliche Personen konnten im Rahmen eines fingierten Treffens mit der vermeintlich 13-jährigen Tochter durch die zuständige Kantonspolizei angehalten werden.

KOBIK beschäftigten auch verschiedene Fälle der Internetkriminalität im engeren Sinn. Unter anderem infizierten Kriminelle im Herbst 2011 beispielsweise die Rechner zahlreicher Schweizer Internetnutzer durch Video-Streaming-Websites. Die Täter nutzten dabei Schwachstellen in der Software sowie im Sicherheitssystem der privaten PCs aus. Die Angriffe waren bemerkenswert komplex und raffiniert: Eine Schadsoftware sperrte den infizierten Rechner und forderte den Benutzer in einem Pop-up-Fenster auf, eine Geldzahlung vorzunehmen, damit der Computer wieder benutzt werden könne. Als vermeintlicher Absender dieser Nachricht fungierte das Eidgenössische Justiz- und Polizeidepartement (EJPD), dessen Logo die Täterschaft verwendete und deren Internetauftritt nachgeahmt wurde. Vergleichbare deliktische Handlungen werden von Kriminellen regelmässig vorgenommen, es werden einzig die nachgeahmte Website und die Zielgruppe ausgetauscht.

Über das Meldeformular wurde KOBIK auf einen vermeintlich HIV-positiven Mann aufmerksam gemacht, der sich auf diversen Foren für die Ansteckung mit AIDS anbot. Die technische Abklärung der Zuständigkeit erwies sich als äusserst schwierig. Aufgrund der Monitoring-Tätigkeit von KOBIK wurden schliesslich genügend Elemente gefunden, um die kantonale Zuständigkeit zu bestimmen. Die fehlbare Person wurde anschliessend dem zuständigen Kanton zur Anzeige gebracht.

6. Adressaten der Verdachtsdossiers und Anzeigen

Im Berichtsjahr erstellte KOBIK insgesamt 263 Verdachtsdossiers zuhanden der kantonalen Strafverfolgungsbehörden. Trotz des leichten Rückgangs im Vergleich zum Vorjahr (299), kann nicht von einer Trendwende gesprochen werden.

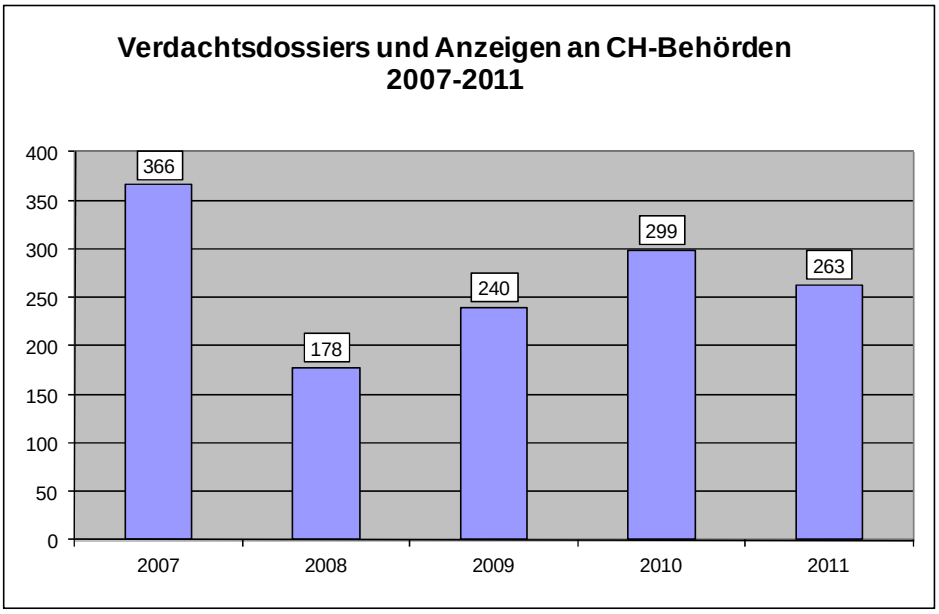

Abbildung 7: Weitergeleitete Verdachtsdossiers und Anzeigen

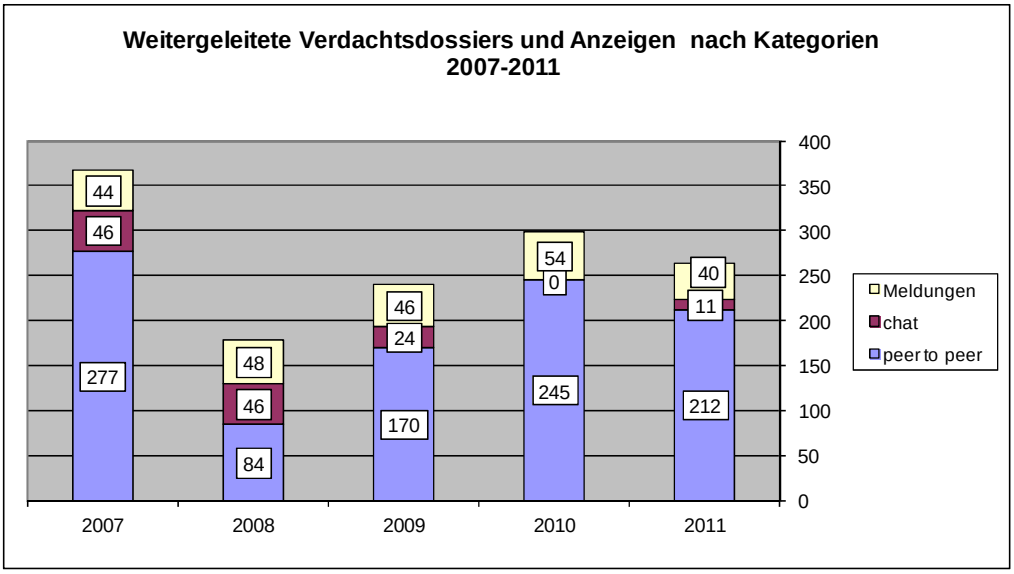

Abbildung 8: Weitergeleitete Verdachtsdossiers und Anzeigen nach Kategorien

Abbildung 8 gibt Auskunft über den Ursprung der Verdachtsdossiers. Die Graphik zeigt auf, dass der Rückgang teilweise auf die Abnahme von Verdachtsdossiers der Rubrik „Meldungen“ zurückzuführen ist. In dieser Rubrik sind sämtliche Fälle enthalten, die aufgrund einer Meldung an KOBIK zu einem Verdachtsdossier führten.
Auch die Anzahl weitergeleiteter P2P-Fälle (212) hat im Vergleich zum Vorjahr leicht abgenommen (-14%). Eine detailliertere Analyse dieses Resultates hat ergeben, dass dieser Rückgang auf die Monate Juli, August und September zurückzuführen sind. In diesen Monaten wurden zum Zwecke einer Effizienzsteigerung die systema-

tischen und technischen Prozesse des Projektes „P2P-Scans“ verbessert und ausgebaut.

Elf weitere Fälle erfüllten den Tatbestand der sexuellen Handlungen mit Kindern (Art. 187 StGB) und wurden von KOBIK im Rahmen verdeckter Ermittlungen in Chats erzielt.

Wie schon in den letzten Jahren wurden die meisten Verdachtsdossiers von KOBIK an die bevölkerungsstärksten Kantone (wie Zürich, Bern und Waadt) weitergeleitet (vgl. Abb. 9). Einige Verdachtsdossiers wurden fedpol-intern an die Kommissariate „Allgemeine-, Organisierte- und Finanzkriminalität“, „Pädokriminalität und Pornografie“ und „Staatsschutz“ der BKP übergeben.

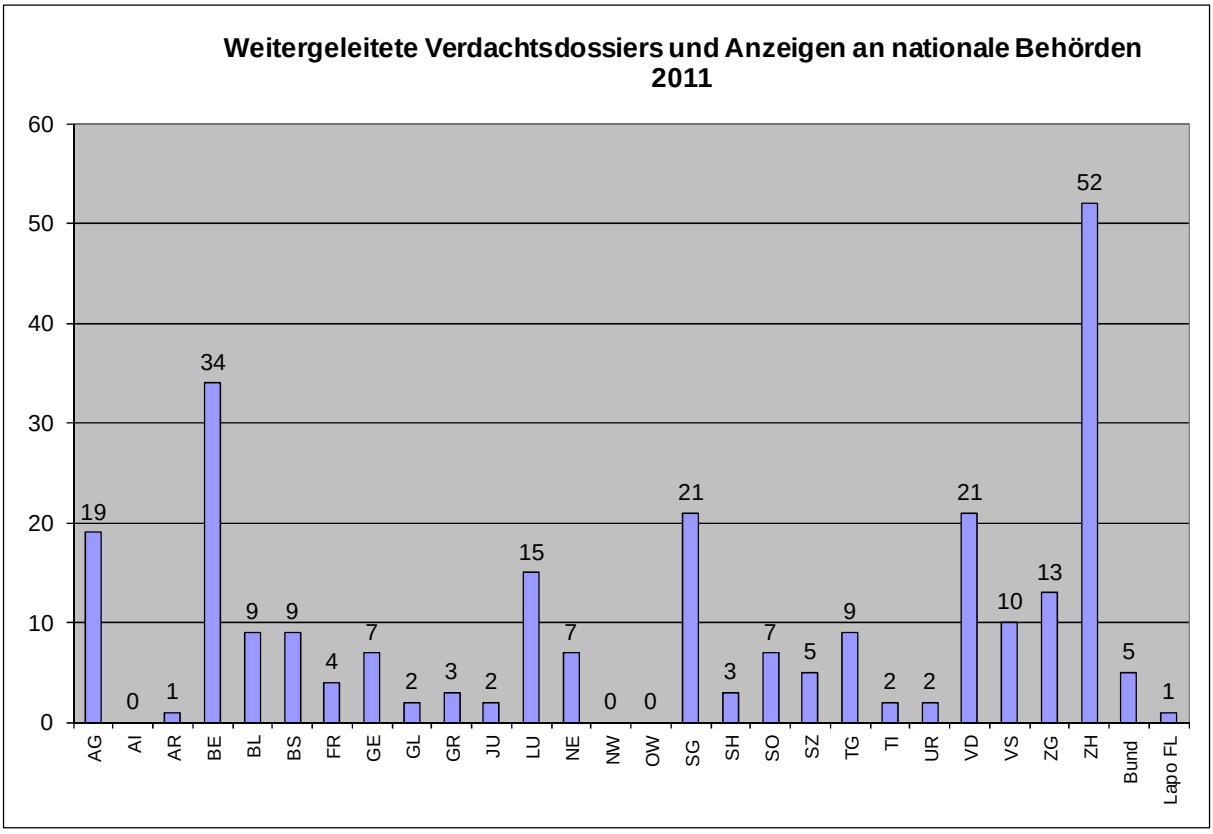

Abbildung 9: An Schweizer und Liechtensteiner Behörden weitergeleiteten Verdachtsdossiers und Anzeigen

In über fünfzig Fällen nutzte KOBIK die Kanäle von Interpol und Europol, um Meldungen an ausländische Strafverfolgungsbehörden weiterzuleiten. Dabei handelte es sich fast ausschliesslich um Internetseiten mit kinderpornografischen Inhalten oder Fälle der Internetkriminalität im engeren Sinn, die via Meldeformular bei KOBIK eingingen. Zusätzlich zu den Meldungen über Interpol oder Europol wurden strafbare Inhalte oftmals auch direkt den Internet Service Providern und Betreibern von Internetseiten zur Löschung gemeldet.

7. Rückmeldungen aus den Kantonen

KOBIK leitet Fälle, in denen der begründete Verdacht für eine Straftat besteht, zur Bearbeitung an die Kantone weiter (vgl. Abb.7). Um eine Gesamtübersicht über die in den Kantonen eingeleiteten Aktivitäten zu gewinnen, ersucht KOBIK die Kantone um Information über den Verlauf der ihnen gemeldeten Verdachtsfälle, insbesondere über die eingeleiteten polizeilichen Massnahmen und über den Ausgang des Gerichtsverfahrens.

Die Analyse dieser Rückmeldungen ist ein wichtiges Mittel zur Überprüfung der Effizienz der Tätigkeit und der Qualität der erstellten Verdachtsdossiers und Anzeigen zuhanden der Kantone. Die grosse Mehrheit (74%) der Verdachtsdossiers resultiert aus den aktiven Recherchen in P2P-Netzwerken. Die Dossiers betreffen somit Personen, die sich aktiv am Austausch von strafbaren Inhalten mit kinderpornografischem Charakter beteiligten.

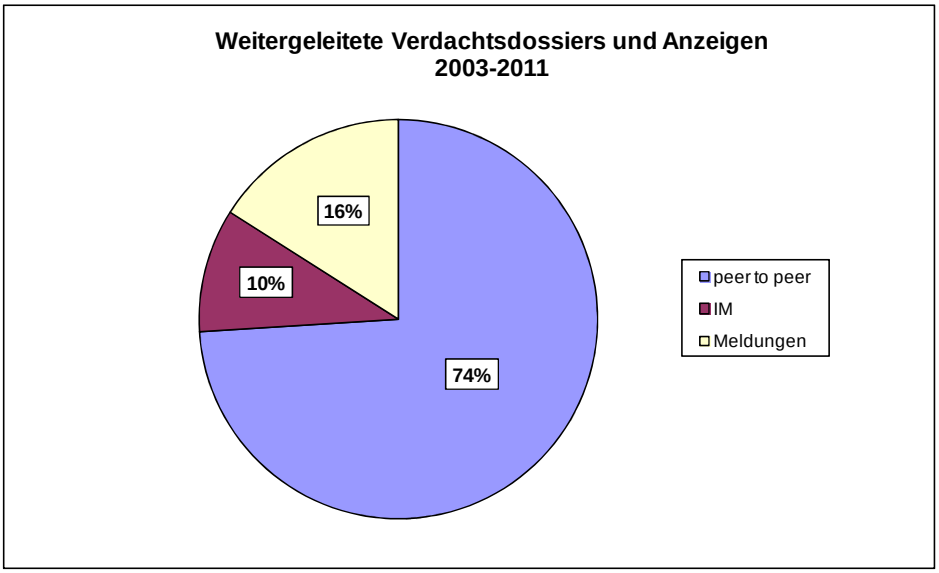

Abbildung 10 : Seit 2003 wurden 2437 Dossiers und Anzeigen weitergeleitet[5]

[5] IM = Instant Messaging oder Nachrichtensofortversand ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Textnachrichten unterhalten (chatten).

7.1 Rückmeldungen der kantonalen Polizeibehörden

Wie aus Abbildung 11 hervorgeht, führten 91% aller weitergeleiteten KOBIK-Fälle zu Hausdurchsuchungen durch kantonale Polizeibehörden. Verdachtsmeldungen der Kategorie „Peer-to-Peer“ lösten dabei in mehr als 98% der Fälle eine Hausdurchsuchung aus, während Verdachtsmeldungen der Kategorie „Meldungen“ (vgl. Grafik 10) selten Hausdurchsuchung rechtfertigen.

95% der Hausdurchsuchungen wurden aufgrund eines Verdachtsdossiers der Kategorie « Peer-to-Peer » angeordnet.

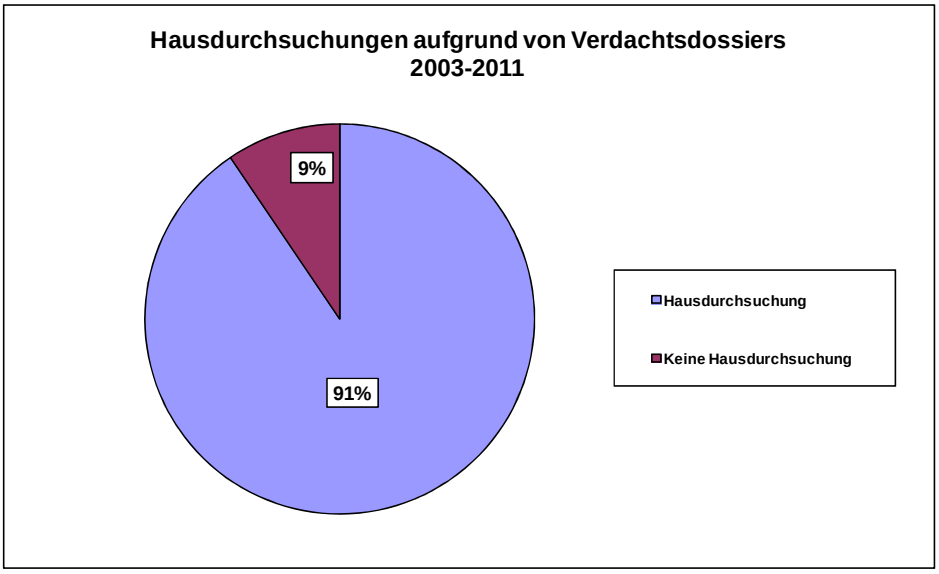

Abbildung 11 : Hausdurchsuchungen (791 Feedback)

Bei 84% der Hausdurchsuchungen, die aufgrund der Verdachtsmeldungen durchgeführt wurden, konnte einschlägiges illegales Material beschlagnahmt werden. In lediglich 16% der Fälle führten die Hausdurchsuchungen nicht zur Sicherstellung von strafrechtlich relevantem Material. Die Gründe für eine erfolglose Hausdurchsuchung sind vielfältig und nicht immer leicht zu eruieren. Bei 1/5 der 16% erfolglosen Hausdurchsuchungen verunmöglichen offene und ungeschützte Drahtlosnetzwerke eine effiziente Beweissicherung und eine eindeutige Identifizierung des Verdächtigen.

Eine nach Erhalt des Verdachtsdossiers zeitnahe Intervention (Hausdurchsuchung) der kantonalen Strafverfolgungsbehörden verringert die Gefahr, dass zwischenzeitlich Computer ausgetauscht und/oder Datenträger gelöscht werden.

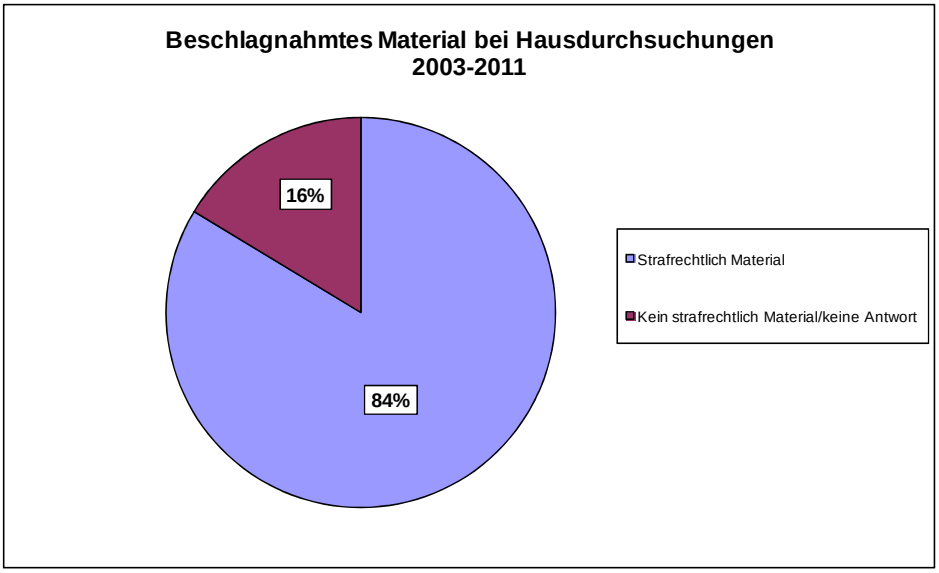

Abbildung 12 : Beschlagnahmung von illegalem Material (716 Hausdurchsuchungen)

Bei den sichergestellten strafbaren Inhalten handelte es sich in 94% um Kinderpornografie. Da bei den aktiven Recherchen in P2P-Netzwerken gezielt nach Straftaten dieser Art gesucht wird und die Mehrheit aller Verdachtsdossiers aus diesen Recherchen stammen, erstaunt dieser hohe Prozentsatz nicht. Erwähnenswert ist auch, dass in mehr als der Hälfte der Fälle zudem Vergehen gegen weitere Tatbestände der harten Pornografie (Art. 197 StGB) festgestellt wurden (vgl. Abb. 13). So wurde bei jeder zweiten Hausdurchsuchung zusätzlich auch noch Pornografie mit Tieren sichergestellt.

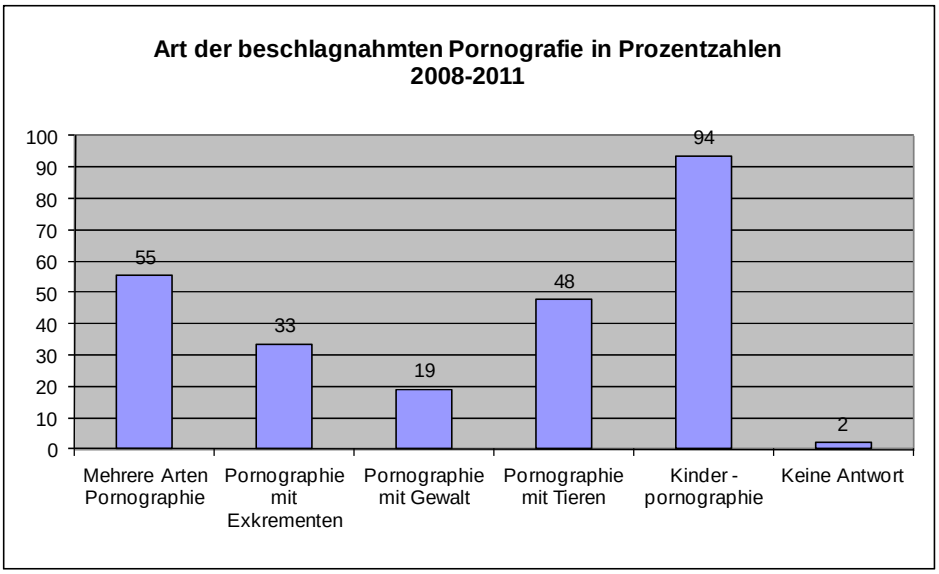

Abbildung 13 : Art des beschlagnahmten Materials (251 Feedback)

Aus den Rückmeldungen der kantonalen Polizeibehörden geht hervor, dass bei 80% der erfolgreichen Hausdurchsuchungen Videodateien und in 63% der Fälle Bilddateien beschlagnahmt wurden. In zahlreichen Fällen wurde belastendes Material beider Kategorien vorgefunden und beschlagnahmt. Insgesamt führten die Hausdurchsuchungen zu Sicherstellungen von zehntausenden von Videodateien und hunderttausenden von Bilddateien.

7.2 Rückmeldungen der kantonalen Justizbehörden

In 90% der Fälle, in denen die kantonalen Justizbehörden KOBIK eine Rückmeldung erstatteten, führten die Strafverfahren zu einer Verurteilung.

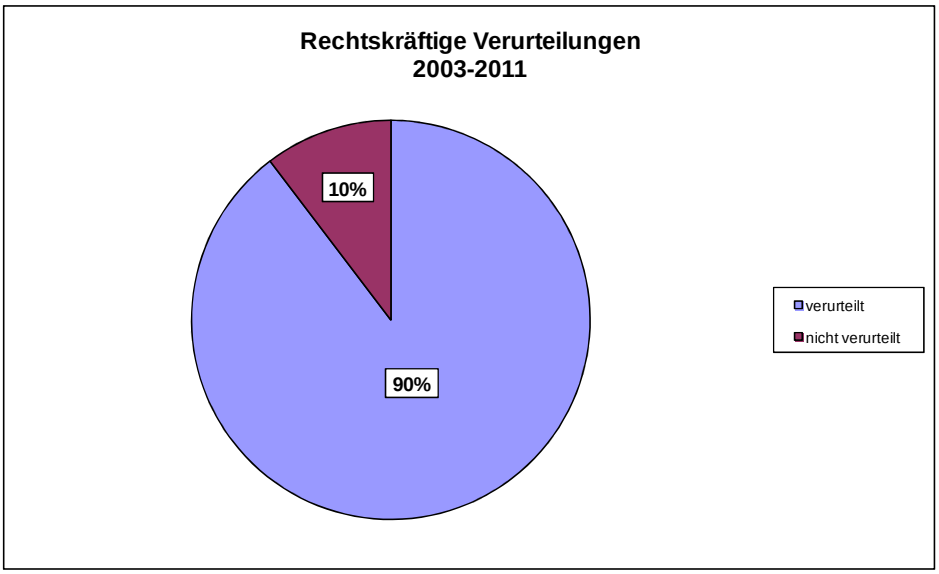

Abbildung 14 : Rechtskräftige Verurteilungen (589 Feedback)

Die meisten Verurteilungen wurden wegen Besitzes von harter Pornografie ausgesprochen, gestützt auf den Tatbestand der Pornografie (Art. 197 StGB) und insbesondere aufgrund der in den Ziffern 3 und 3bis[6] beschriebenen Tatbestände. In einzelnen Fällen kam es zu Verurteilungen wegen Verstoss gegen Art. 187 Ziffer 1 StGB (sexuelle Handlungen mit Kindern).

6
Ziff 3. Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder mit Tieren, menschlichen Ausscheidungen oder Gewalttätigkeiten zum Inhalt haben, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Die Gegenstände werden eingezogen.
Ziff. 3bis. Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder Tieren oder sexuelle Handlungen mit Gewalttätigkeiten zum Inhalt haben, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt.

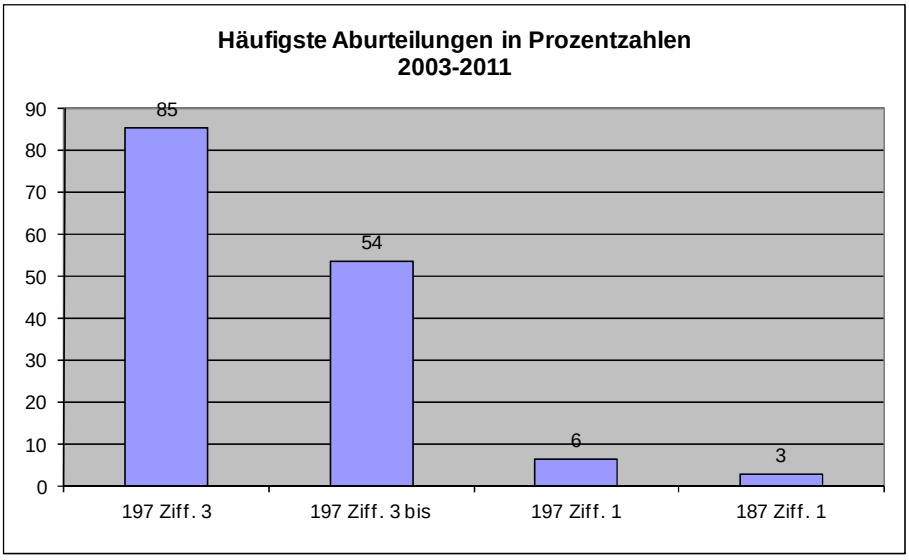

Abbildung 15 : Häufigste Verurteilungen (532 Verurteilungen)

Bei den meisten Verurteilungen wurde eine Geldstrafe (Tagessatz) ausgesprochen. In vielen dieser Fälle wurde gleichzeitig eine Busse verhängt. Die Geldstrafen wurden bei 91% der Verurteilungen auf Bewährung ausgesetzt. Gemeinnützige Arbeit und Therapien wurden nur in einigen wenigen Fällen angeordnet. Die strengsten Strafmassnahmen wie Freiheitsentzug (Gefängnis) und nicht auf Bewährung ausgesetzte Geldstrafen wurden fast ausschliesslich gegen Wiederholungstäter verhängt.

In etwa zwei Drittel der Fälle beliefen sich die Bussen auf weniger als tausend Franken; in 16% auf 1'000 bis 2'000 Franken. Lediglich 18% der Bussen waren höher als 2'000 Franken. 48% der Geldstrafen wurden bei 50 oder weniger Tagessätzen festgelegt; bei 35% wurden jeweils zwischen 51 und 100 Tagessätze angeordnet. Über 100 Tagessätze wurden nur in 17% der Fälle gesprochen. In 24 % der Fälle wurden Tagessätze in der Höhe von 1 bis 50 Franken, in 38 % der Fälle zwischen 51 und 100 Franken und in 38% über 100 Franken festgesetzt.

Die ausgesprochenen Bussen beliefen sich mehrheitlich zwischen 500 und 3‘000 Franken. Die höchste Busse betrug 6‘000 Franken. In der Regel müssen die Verurteilten zusätzlich die Verfahrenskosten tragen, welche die eigentliche Busse oftmals um ein Vielfaches übersteigen. Die Geldstrafen wurden mehrheitlich im Bereich von 20 bis 200 Tagessätzen in der Höhe von 20 bis 200 Franken festgelegt.

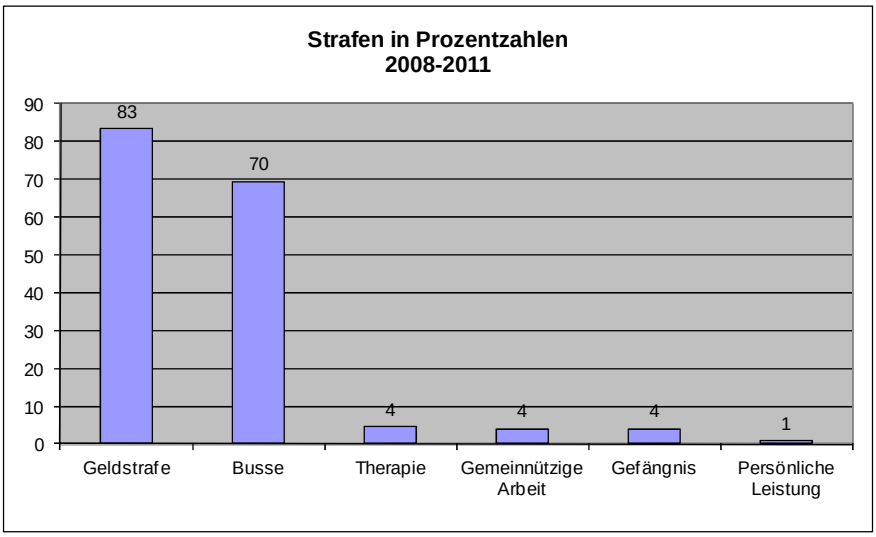

Abbildung 16 : Strafmass (242 Feedback)

8. Arbeitsgruppen

8.1 National

KOBIK war im Berichtsjahr in verschiedenen nationalen Arbeitsgruppen vertreten, namentlich im Bereich Kriminalprävention.

So beteiligte sich KOBIK, zusammen mit dem fedpol-Kommissariat Pädokriminalität und Pornografie, gemeinnützigen Organisationen, Kantonsvertretern und der Schweizerischen Kriminalprävention auch im Berichtsjahr aktiv in der nationalen Arbeitsgruppe «Kindsmissbrauch».

2011 war KOBIK im nationalen Programm „Jugendmedienschutz und Medienkompetenzen“ sowohl in der mit der Programmausarbeitung vertrauten Leitgruppe, als auch in der ausführenden Begleitgruppe vertreten. Das Programm soll Kindern und Jugendlichen helfen, einen sicheren, verantwortungsvollen und dem Alter angepassten Umgang mit den modernen Medien zu finden. Höhepunkt des Programmes war der „Tag der Medienkompetenzen“, welcher am 27. Oktober 2011 in Freiburg erstmals stattfand.

Seit 2011 ist KOBIK als Vertreter von fedpol auch in der neu geschaffenen Fachkommission „Schweizerische Kriminalprävention“ vertreten. Die Kommission entwickelt Projekte und Materialien für die Kriminalprävention in den Kantonen und evaluiert deren Umsetzung.

KOBIK war zudem weiterhin an der Umsetzung des Konzeptes «Sicherheit und Vertrauen» beteiligt, das unter der Leitung des Bundesamtes für Kommunikation (BAKOM) Massnahmen zur Förderung der Sicherheit und des Vertrauens der Bevölkerung in die modernen Informations- und Kommunikationstechnologien aufzeigt.

Dank der Vertretung in den Arbeitsgruppen „IT-Ermittler“ und „Telekommunikationsüberwachung“ konnte KOBIK nicht zuletzt auch 2011 den Bereichen der technischen Entwicklung und der effizienten Strafverfolgung Rechnung tragen.

8.2 International

Seit 2011 ist KOBIK neu Mitglied der Analysis Work Files (AWF) Cyborg von Europol, deren Ziel die Bekämpfung der supranationalen Internetkriminalität ist. Dabei liegt der Fokus auf den Phänomenen «Phishing», «Botnetze» und „Hacking“. KOBIK ist ebenfalls am Projekt „CIRCAMP“ beteiligt. Dieses Projekt bekämpft die Verbreitung von Kinderpornografie auf dem Internet und nimmt sich den Vertriebsplattformen an, welche für die Verbreitung genutzt werden. Wie bereits in den vergangenen Jahren war KOBIK zudem nach wie vor in der Arbeitsgruppe „European Financial Coalition“ in Brüssel vertreten.

KOBIK konnte 2011 auch im Convention Committee on Cybercrime (T-CY), der Konvention des Europarates über die Internetkriminalität in Strassburg, teilnehmen. Da-

bei wurde nicht nur das 10-jährige Jubiläum der Konvention, sondern auch deren Inkrafttreten in der Schweiz per 1. Januar 2012, gefeiert.

9. Projekte

9.1. Zusammenarbeit mit den Schweizerischen Internet Access Providern zur Filterung kinderpornografischer Internetseiten

Seit 2007 unterstützt KOBIK die grössten Schweizer Internetanbieter bei der Sperrung von kinderpornografischen Internetseiten. Die Sperre richtet sich dabei ausschliesslich gegen ausländische Internetseiten mit kinderpornografischem Inhalt, die trotz Meldung an die zuständige Strafverfolgungsbehörde nicht gelöscht wurden. KOBIK stellt den Internetanbietern eine stetig aktualisierte Liste von kinderpornografischen Internetseiten zur Verfügung. Die Internetanbieter sperren aufgrund ihrer Firmenethik und den AGB's[7] den Zugang zu strafrelevanten Seiten und leiten den Benutzer auf eine « Stopp-Seite » weiter.

Im Rahmen dieses Projektes arbeitet KOBIK eng mit Interpol zusammen, die auch eine Liste von Internetseiten mit kinderpornografischen Bildern und Videos führen («worst of list»). Die Zusammenarbeit mit Interpol in diesem Projekt, an dem mehrere Länder beteiligt sind, konnte 2011 weiter ausgebaut werden. Die in der Schweiz erstellte Liste basiert einerseits auf der Interpol-Liste und wird ergänzt durch eigene, selbsterkannte Internetseiten. Die «worst of list» wird täglich in die KOBIK-Liste integriert. KOBIK seinerseits meldet Interpol neue Internetseiten zur Ergänzung der «worst of list».

9.2 Nationale Datei- und Hashwertesammlung (NDHS)

Dateien (bspw. Bilder, Videos, usw.), die im Rahmen von Ermittlungen im Bereich Kinderpornografie sichergestellt wurden, werden von den zuständigen kantonalen Behörden an KOBIK übermittelt. KOBIK generiert von jeder Datei einen Hashwert[8] und speichert diesen in der Nationalen Datei- und Hashwertesammlung (NDHS) ab. Diese Liste von Hashwerten wird den Kantonen über die JANUS-Community[9] zur Verfügung gestellt. Die zuständigen kantonalen Behörden generieren zu den Dateien, die sie neu sicherstellen, ebenfalls die Hashwerte. Diese eigenen kantonalen Bestände an Hashwerten können die kantonalen Behörden anschliessend mit der Liste der Hashwerte von KOBIK vergleichen. Mittels Vergleich dieser Hashwerte können umfangreiche Dateien miteinander auf Übereinstimmungen geprüft werden, ohne das strafrechtsrelevante Material (Rohdaten) visuell geprüft werden müssen. So können Duplikate identifiziert werden. Dies bringt den Ermittlern eine grosse zeitliche und nicht zuletzt psychische Entlastung.

Das Projekt konnte im Berichtsjahr massgeblich vorangetrieben werden. Die Projektplanung wurde in Zusammenarbeit mit den Kantonen abgeschlossen und die notwendige Infrastruktur durch fedpol beschafft. Vertreter aller Kantone wurden anlässlich von Informationsveranstaltungen für den Einsatz der NDHS geschult. Die ersten kantonalen Datensätze mit Bildern und Videos wurden KOBIK erfolgreich übergeben.

---

[7] Allgemeine Geschäftsbedingungen (abgekürzt AGB)

[8] Eindeutig zuordnungsbarer Kennwert eines Bildes (digitaler Fingerabdruck)

[9] Intranet, das schweizweit den Polizeibehörden Informationen zur Verfügung stellt

Dank einer von der Schweizer Firma ATG gemeinsam mit KOBIK entwickelten Bilderkennungssoftware soll der Zeitaufwand für das Kategorisieren und Überprüfen der an KOBIK übergebenen Bilddateien deutlich verkürzt werden. Es ist geplant, die Software auch zur Unterstützung operativer Einsätze zu nutzen.

9.3 „Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken“ (vormals Nationale Strategie Cyber Defense)

Der Bundesrat hat am 10. Dezember 2010 das VBS beauftragt, eine nationale Strategie Cyberdefense zu entwickeln und Divisionär Kurt Nydegger zum Projektleiter ernannt. Ziel der Strategie ist namentlich der Schutz der kritischen Infrastrukturen vor Cyberbedrohungen. Sie muss präzise Auskunft zu den vorgesehenen Umsetzungsarbeiten und deren Konsequenzen in Bezug auf Zeit, Kosten, Fähigkeiten, Recht und Ressourcen geben. Die definitive nationale Strategie Cyberdefense inklusive Vorschlägen von Umsetzungsmassnahmen in Varianten erwartet der Gesamtbundesrat im ersten Quartal 2012. KOBIK arbeitete ab Mai 2011 im Projektteam mit und wird auch bei der Umsetzung der Strategie die Interessen der kantonalen und nationalen Strafverfolgungsbehörden vertreten.

10. Politische Vorstösse auf Bundesebene

10.1 Die im Berichtsjahr eingereichten parlamentarischen Vorstösse:

Kinder- und Jugendschutz / Pädokriminalität

Interpellation Pasquier : Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113141

Motion Savary : Pornografie im Internet. Vorbeugend handeln
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113314

Frage Bruderer-Wyss : Bestrafung sexueller Kontakte mit 16- bis 18-Jährigen
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115351

Frage Rickli : Pädophilenregister
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115008

Motion Schmid-Federer : Grooming unter Strafe stellen
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20114002

Geschäft des Bundesrates StGB, MStG und JStG. Unverjährbarkeit sexueller und pornografischer Straftaten an Kindern
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20110039

Andere

Interpellation Amherd : Verschärfung der Internetüberwachung
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113862

Postulat Eichenberger-Walther : Nationales Netz polizeilicher Kompetenzzentren
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113642

Frage Leutenegger-Oberholzer : Einsatz von Bundes-Trojanern
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115541

Frage Reimann : Fragwürdige Praktiken von PayPal in der Schweiz
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115438

Frage Schmid-Federer : Stand der Präventionskampagnen des BSV nach einem Jahr http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115198

Postulat Amherd : Rechtliche Basis für Social Media
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113912

Postulat Schmid-Federer : IKT-Grundlagengesetz
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113906

Pétition : Verbot von Killerspielen
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20112005

10.2 Rechtliche Entwicklung

Die Bekämpfung der Internetkriminalität stellt auch die Rechtsprechung und Rechtsetzung vor neue Herausforderungen. In diesem Kapitel wird auf die besonderen nationalen und internationalen Rechtsentwicklungen eingegangen.

Bundesgerichtsentscheid 6B_744/2010

Das Bundesgericht wurde 2011 mit der Frage nach der Strafbarkeit von Kinderpornografie im Cache des Computers konfrontiert. In einem Entscheid vom 12. Mai 2011 hielt das Bundesgericht fest: Alle elektronischen Daten und Formen der Speicherung würden von Art. 197 Ziff. 3bis StGB erfasst. Besuchte Webseiten würden im temporären Internetspeicher automatisch auf der Festplatte zwischengespeichert, was bei einem erneuten Aufrufen der Webseite dazu führe, dass diese schneller geladen werde. Mittels gängiger und kostenloser Software (Cache-Viewer oder Cache-Reader) könne auch ohne Internetverbindung, d.h. im Offline-Modus, auf die gespeicherten Internetseiten zugegriffen werden. Der nach Art. 197 Ziff. 3bis StGB strafbare Besitz harter Pornographie umfasse Herrschaftsmöglichkeit und Herrschaftswillen. Zwar nehme der durchschnittliche Internetbenutzer keinen Einfluss auf die Zwischenspeicherung im Cache, weshalb dies noch nicht als Besitz zu qualifizierende Sachherrschaft sei. Wer aber über einen längeren Zeitraum mehrfach gezielt Webseiten mit hartem pornographischem Inhalt aufsuche, beschränke sich nicht auf das blosse Betrachten. Durch den wiederholten Zugriff zeige er seinen Herrschaftswillen. Obwohl die Zwischenspeicherung automatisch geschehe, habe es der Benutzer in der Hand, diese zu deaktivieren oder den temporären Internetspeicher zu löschen. Es müsse heute als allgemein bekannt gelten, dass besuchte Internetseiten im Cache zwischengespeichert würden.

Ein Beschaffen von Daten im Sinne von Art. 197 Ziff. 3bis StGB liege schon vor, wenn ein Täter über ein Passwort einen dauernden und unbeschränkten Zugang zu einer Webseite mit harter Pornographie erhalte und über diese Daten frei verfügen könne. Dasselbe müsse für die Tatbestandsvariante des Besitzes gelten. Dieser sei gegeben, wenn der Zugriff auf gespeicherte Dateien mit illegalem pornographischem Inhalt jederzeit möglich sei, z.B. durch den temporären Internetspeicher. Nur so könne die vom Gesetzgeber angestrebte lückenlose Strafbarkeit im Umgang mit harter Pornographie erreicht werden.

Bundesrat bestätigt Urhebergesetz

Mit einem Bericht erfüllte der Bundesrat im November 2011 ein Postulat von Ständerätin Géraldine Savary (SP/VD) vom März 2010. Der Ständerat hatte den Bundesrat mit Annahme des Postulats beauftragt zu prüfen, ob Massnahmen gegen Urheberrechtsverletzungen nötig sind. Der Bericht hält fest, dass jede dritte Person über 15 Jahre in der Schweiz Musik, Filme und Spiele aus dem Internet herunterlädt, ohne dafür zu bezahlen. Das Internet habe die Nutzung und Beschaffung von Musik, Filmen und Spielen zwar fundamental verändert. Auf das kulturelle Schaffen wirke sich dies jedoch nicht nachteilig aus. Aus diesen Gründen verzichtet der Bundesrat auf eine Anpassung des Urheberrechts. Das heisst für Schweizer Internetbenutzer unter anderem, dass sie für den Eigenbrauch auch weiterhin straffrei Filme und Songs herunterladen können, da der Download von urheberrechtlich geschützten Liedern und Filmen zu Privatzwecken in der Schweiz legal bleibt.

Cybercrime Convention

Mit der Ratifikation der Europaratskonvention über die Cyberkriminalität beteiligt sich die Schweiz an der verstärkten internationalen Bekämpfung der Computer- und Internetkriminalität. Die Konvention trat für die Schweiz am 1. Januar 2012 in Kraft. Auf den gleichen Zeitpunkt hat der Bundesrat die erforderlichen Gesetzesanpassungen in Kraft gesetzt.

Die Europaratskonvention über die Cyberkriminalität ist das erste internationale Übereinkommen zur Bekämpfung von Computer- und Internetkriminalität. Sie verpflichtet die Vertragsstaaten unter anderem, Computerbetrug, Datendiebstahl, Fälschung von Dokumenten mit Hilfe eines Computers oder das Eindringen in ein geschütztes Computersystem unter Strafe zu stellen. Die Vertragsstaaten müssen zudem Kinderpornografie sowie die Verletzung von Urheberrechten im Internet bestrafen.

Die Konvention regelt ferner, wie in der Strafuntersuchung Beweise in Form von elektronischen Daten erhoben und gesichert werden. Sie will insbesondere sicherstellen, dass die Untersuchungsbehörden rasch auf elektronisch bearbeitete Daten zugreifen können, damit diese im Laufe des Verfahrens nicht verfälscht oder vernichtet werden. Schliesslich will die Konvention eine schnelle, wirksame und umfassende Zusammenarbeit zwischen den Vertragsstaaten gewährleisten.

Die Umsetzung der Konvention erforderte je eine kleinere Anpassung des Strafgesetzbuches und des Rechtshilfegesetzes. Beim Straftatbestand des unbefugten Eindringens in eine Datenverarbeitungsanlage („Hacking“) ist die Strafbarkeit vorverlagert worden. Demnach werden künftig bereits das Zugänglichmachen und das in Verkehr bringen von Passwörtern, Programmen und anderen Daten unter Strafe gestellt, wenn der Betreffende weiss oder annehmen muss, dass diese für das illegale Eindringen in ein geschütztes Computersystem verwendet werden sollen.

Das Rechtshilfegesetz räumt zukünftig der schweizerischen Rechtshilfebehörde die Kompetenz ein, in bestimmten Fällen Verkehrsdaten bereits vor Abschluss des Rechtshilfeverfahrens zu Ermittlungszwecken an die ersuchende Behörde zu übermitteln. Diese Daten – die Aufschluss über Absender und Empfänger, Zeitpunkt, Dauer, Grösse und Weg einer Nachricht geben – dürfen allerdings erst als Beweismittel verwendet werden, nachdem die Schlussverfügung über die Gewährung und den Umfang der Rechtshilfe rechtskräftig geworden ist.

Es wurde entschieden, dass die durch Art. 35 der Konvention geforderte Funktion als 24/7-Kontaktstelle durch die Einsatzzentrale fedpol (SPOC, EZ fedpol) wahrgenommen wird. KOBIK unterstützt die SPOC im Rahmen der Bearbeitung von Anfragen gemäss Konvention.

.

11. Medienauftritte, Ausbildung und Konferenzen

11.1 Medienpräsenz

KOBIK und ihre Tätigkeit fand 2011 in zahlreichen Medienberichten Niederschlag. Besondere Aufmerksamkeit schenkten die Medien den (präventiven) verdeckten Vorermittlungen durch KOBIK und einzelnen spektakulären Angriffen auf Informationssysteme (DDoS-Angriffe[10]). Die Berichterstattung war über das Jahr verteilt insgesamt positiv.

11.2 Ausbildung und Konferenzen

Im Berichtsjahr nahmen KOBIK-Mitarbeitende an verschiedenen Konferenzen, internationalen Tagungen und Ausbildungslehrgängen teil und nutzten die Gelegenheit zur unerlässlichen Kontaktpflege zu Partnern und Experten.
In der Schweiz :

- Nationale IT-Ermittler-Tagung, Bern
- Tag der Medienkompetenzen (Im Rahmen des nationalen Programmes « Jugend und Medien »), Freiburg
- World Summit Information Society (WSIS), Genf
-

Im Ausland :

- «RIPE NCC Meeting», London
- «Octopus Interface» Konferenz, Strassburg
- «E-crime Congress», London
- Expertentreffen Cybercrime der UNO, Wien
- OSCE-Konferenz „Cybersecurity and Cybercrime“, Wien
- Symposium « Neue Technologien » BKA Wiesbaden
- «Fighting Cybercrime : cooperation between law enforcement agencies and the internet industry», Europarechtsakademie, Trier
- «Child Sexual Exploitation Experts Conference» Europol, Den Haag

[10] Distributed Denial of Service

12. Partnerschaften und Kontakte

12.1 Zusammenarbeit mit anderen Bundesstellen

2011 arbeitete KOBIK zur Bekämpfung der Internetkriminalität eng mit anderen Bundesstellen zusammen. Innerhalb von fedpol stand vor allem die intensive Zusammenarbeit mit den Kommissariaten «Pädokriminalität und Pornografie», «IT-Ermittler», «Staatsschutz» und «Verdeckte Ermittlungen» der Bundeskriminalpolizei und der Hauptabteilung IPK im Vordergrund. Aufgrund der gemeinsamen Schwerpunktthematik und den vom Bundesrat 2011 neu gesprochenen sechs Stellen zur Bekämpfung der Pädokriminalität, besteht zwischen dem Kommissariat «Pädokriminalität und Pornografie» und KOBIK eine besonders intensive Zusammenarbeit.

Während des Berichtsjahres konnten diverse Kontakte sowie die departementsübergreifende Zusammenarbeit mit verschiedenen Bundesstellen ausgebaut und intensiviert werden. Zu nennen sind dabei unter anderem die Melde- und Analysestelle Informationssicherung (MELANI), die Abteilung internationale Rechtshilfe im Bundesamt für Justiz (BJ), das Bundesamt für Kommunikation (BIT), das Bundesamt für Sozialversicherungen (BSV), Swissmedic und die Lotteriekommission (Comlot)

Die bereits bestehende Zusammenarbeit mit der Schweizerischen Kriminalprävention (SKP) wurde dieses Jahr durch die Aufnahme von KOBIK als Vertretung von fedpol in der SKP-Fachkommission weiter ausgebaut.

12.2 Arbeitsgruppen und Erfahrungsaustausch mit den Kantonen

Im Berichtsjahr pflegte KOBIK zahlreiche Kontakte mit Vertretern diverser Polizeikorps und Staatsanwaltschaften. Neben dem normalen Erfahrungsaustausch fanden insbesondere im Rahmen der verdeckten Ermittlung und des Projektes NDHS verschiedene Arbeitssitzungen statt.

Im Rahmen der Nationalen Strategie Cyber Defense und anlässlich diverser politischen Anfragen zur Internetkriminalität, hat sich ein guter Kontakt zum Schweizerischen Polizei Informatik Kongress (SPIK) ergeben.

12.3 Zusammenarbeit mit Action Innocence (AIG)

Seit mehreren Jahren arbeitet KOBIK bei der Bekämpfung der Kinderpornografie eng mit der NGO[11] Action Innocence (AIG) zusammen. Dank der tatkräftigen und finanziellen Unterstützung durch AIG konnte das Projekt zur Überwachung von Peer-to-Peer-Netzwerken in den letzten Jahren erfolgreich betrieben und weiterentwickelt werden. Die Zusammenarbeit mit AIG ist von grosser Bedeutung, da eine klare Mehrheit der aktiven Recherchen von KOBIK nur dank der von AIG zur Verfügung gestellten Software zur Überwachung von P2P-Netzwerken möglich ist. Zudem un-

11 Non-Governmental Organization / Nichtregierungsorganisation (NRO)

terstützt AIG KOBIK durch die Entwicklung diverser Zusatzprojekte, die im Rahmen der Bekämpfung von Pädokriminalität zum Einsatz gelangen sollen.

12.4 Zusammenarbeit mit der Privatwirtschaft (Public-Private-Partnership, PPP)

Die Zusammenarbeit von KOBIK mit der Privatwirtschaft ist für die Bekämpfung der Internetkriminalität von steigender Bedeutung. Im Berichtsjahr fanden verschiedene Besuche oder Treffen mit Vertretern der Internetbranche und von neuen Technologien statt. Positiv sind namentlich die Kontakte, die zu diversen Internetdienstanbietern geknüpft werden konnten. Eine solche Zusammenarbeit ist unter anderem entscheidend für die Abklärung von Internetanschlüssen verdächtiger Personen (IP-Adresse) im Rahmen von polizeilichen Ermittlungen und Vorermittlungen. Die Bekämpfung der Internetkriminalität erfordert ein schnelles und interaktives handeln sämtlicher Beteiligter.

12.5 Externe Besucher

Im Berichtsjahr interessierten sich auch diverse externe Besucher für die Tätigkeit von KOBIK. Bei diesen Besuchen bietet sich den KOBIK-Mitarbeitenden die Gelegenheit, ihre Arbeit zu präsentieren und die Besucher auf die damit verbundenen Problemstellungen und Zusammenhänge aufmerksam zu machen. Auch verschiedene Medienschaffende haben KOBIK im 2011 im Hinblick auf eine Berichterstattung besucht und dabei einen umfassenden Einblick in die Tätigkeit der Spezialisten gewonnen.

12.6 Internationale Zusammenarbeit

Zusätzlich zu den in Kapitel 8.2 genannten internationalen Konferenzen und Arbeitsgruppen, hat KOBIK den Kontakt zu verschiedenen ausländischen Partnerstellen gepflegt. Dieser Austausch dient in erster Linie der gemeinsamen Entwicklung von Prozessen zur verbesserten Zusammenarbeit. Dabei konzentriert sich die internationale Zusammenarbeit längst nicht mehr ausschliesslich auf die Bekämpfung der Pädokriminalität. Immer mehr tritt die Bekämpfung der Internetkriminalität im engeren Sinn und die Wirtschaftskriminalität in den Vordergrund der internationalen Bestrebungen. Gerade auch im Rahmen von operativen Einsätzen (z.B. verdeckte Ermittlungen, Kapitel 9.2) ist der direkte Austausch mit ausländischen Strafverfolgungsbehörden von grossem Nutzen.

13. Glossar

Adult check	(Dt: Altersnachweissystem) Ein System, das dem Jugendschutz dient. Es ermöglicht Minderjährigen den Zugang zu bestimmten Websites zu verwehren.
Chat	Elektronische Kommunikation in Echtzeit, meist über das Internet.
Cloud Computing	(Zu Deutsch etwa *Rechnen in der Wolke*) Cloud Computing bezeichnet IT-Infrastruktur (Rechenkapazität, Datenspeicher von Computern und Servern), die aus verschiedenen Teilen der Welt über ein Netzwerk, wie das Internet, zur Verfügung gestellt werden. Statt Systemanwendungen und Daten auf einigen wenigen lokalen Rechnern zu speichern, wird die Rechenlast zur optimalen Ressourcennutzung auf möglichst viele Rechner verteilt und so von einer Vielzahl von Servern in der ganzen Welt (sozusagen einem "Wolkenhaufen") bereitgestellt. Eine leistungsstarke Bandbreite ist eine der Grundvoraussetzungen für Cloud Computing.
Cyberbullying	Von Cyberbullying kann gesprochen werden, wenn mit Hilfe moderner Kommunikationsmittel wie Handy, Chat, sozialer Internet-Netzwerke wie Netlog oder Facebook, Videoportale oder Foren und Blogs diffamierende Texte, Bilder oder Filme veröffentlicht werden, um Personen zu verleumden, blosszustellen oder zu belästigen. Dabei erfolgen die Angriffe in der Regel wiederholt oder über längere Zeit und die Opfer zeichnen sind durch besondere Hilflosigkeit aus.
One-Click-hosting	One-Click-Hosting bietet Anwendern die Möglichkeit, bei Anbietern Dateien (hauptsächlich Video- und Audiodateien) unmittelbar und ohne vorherige Anmeldeprozedur zu speichern. Der Anwender erhält eine URL, unter der die Datei angezeigt und heruntergeladen werden kann.
Peer-to-Peer	(Engl. *peer* für Gleichgestellter) In einem Peer-to-Peer-Netz haben Mitglieder Zugriff auf gemeinsame Dateien und können diese auch mit Dritten austauschen.
Phishing	Methode, mit der versucht wird, über gefälschte www-Adressen an Daten eines Internet-Benutzers (Passwort, Benutzername usw.) zu gelangen.
Harte Pornografie	Sexuelle Handlungen mit Kindern (Synonym: Pädopornografie), Tieren oder menschlichen Ausscheidungen oder auch Gewalt darstellende sexuelle Handlungen (Art. 197 Ziff. 3 StGB).
Hashwerte	Eindeutig zuordnungsbarer Kennwert eines Bildes (digitaler Fingerabdruck)
Proxy	(Von engl.: *proxy* = Stellvertreter) Kommunikationsschnittstelle in einem IT-Netz zwischen Klient und einem Server, über den beispielsweise eine Website aufgerufen wird.
Redirect Service	Ein Weiterleitungs-Dienst (engl.: *redirect service*) wandelt lange URLs in kurze um, die leicht zu merken sind. Der Browser wird angewiesen, ohne Verzögerung über eine verkürzte URL den Inhalt der angegebenen Seite aufzurufen.
Spam	Als Spam werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden. Spams werden oft zu Werbezwecken versandt, bisweilen auch, um in einem Benutzersystem Malware (ein Schadprogramm) einzuschleusen.
Streaming	Das Übertragen von Audio- oder Videodateien. Dateien werden nicht erst vollständig auf ein System, sondern kontinuierlich über ein Computernetz heruntergeladen. Es braucht somit keine komplette Datei heruntergeladen zu werden, ein "Reinhören" wird möglich.
URL	Uniform Ressource Locator (dt. einheitlicher Quellenanzeiger) Eine aus Ziffern und Zahlen bestehende Adresse (umgangssprachlich: Internetadresse).

14. Trends 2011

Rückschlüsse auf die effektive Entwicklung der Internetkriminalität oder illegaler Inhalte im Internet sind anhand des Meldungseinganges bei KOBIK nur sehr bedingt möglich. Allenfalls lassen sich daraus Tendenzen hinsichtlich der Meldebereitschaft der Bevölkerung und der Wahrnehmung von Internetkriminalität in der Gesellschaft ableiten. Die Gründe für den Rückgang der Meldungen können vielseitig sein. Es kann sein, dass verschiedene Arten der Internetkriminalität bereits so alltäglich sind, dass sie durch die Bevölkerung banalisiert werden und auf eine Meldung an KOBIK verzichtet wird. Meldungen aus der Bevölkerung sind jedoch wichtig, da nur so das Ausmass von Internetkriminalität erfasst und durch die Strafverfolgungsbehörden oder durch andere Massnahmen angegangen werden kann.

Der Rückgang der Meldungen ist zudem auf eine geminderte öffentliche Sichtbarkeit der Inhalte zurückzuführen. Pädophile ziehen sich bewusst in geschlossene oder nur schwer zugängliche Plattformen (Foren, Gruppen, soziale Netzwerke) zurück, was ihnen einen diskreteren und anonymeren Austausch von kinderpornografischem Material erlaubt. Aufgrund der rasanten technischen Entwicklung des Internets ist davon auszugehen, dass sich diese Entwicklung noch weiter verschärfen wird.

Dadurch kommt den polizeilichen Ermittlungen im Internet, namentlich den verdeckten Ermittlungen, eine immer wichtigere Rolle bei der Erkennung und Aufklärung von Straftaten im Internet zu.

Es ist zudem mit einem anhaltenden Anstieg von Betrugsfällen zu rechnen, die von Kriminellen, die vom Ausland aus operieren, begangen werden. Diese Entwicklung wird bereits seit einigen Jahren beobachtet und hat sich im Berichtsjahr fortgesetzt. Die Prävention und Sensibilisierung der Bürgerinnen und Bürger über den richtigen Umgang mit dem Internet ist deshalb von grosser Bedeutung.

In diesen Fällen, aber auch bei allen anderen Arten der Internetkriminalität, kann eine Lösung oder Bekämpfung nur in Zusammenarbeit aller Beteiligten (Regierungen, Strafverfolgungsbehörden, Internetanbieter, Internetdienstleister und Regulatoren) erfolgen. KOBIK beteiligt sich bereits an diversen nationalen und internationalen Arbeitsgruppen, welche die Bekämpfung deliktspezifischer Phänomene bezwecken. Es ist davon auszugehen, dass die Zusammenarbeit zwischen privaten und öffentlichen Institutionen (Public-Private-Partnership) zur Bekämpfung der Internetkriminalität eine immer wichtigere Rolle einnehmen wird.