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 2010

Inhaltsverzeichnis

1. Das Wichtigste in Kürze

- Trotz eines Rückganges der Gesamtzahl an Meldungen, sind im Berichtsjahr erneut deutlich mehr Meldungen der Kategorie «harte Pornografie» eingegangen, insbesondere von Seiten mit kinderpornografischen Inhalten. Pädophilen steht weiterhin eine Vielzahl von sich stetig weiterentwickelnden Kommunikationsplattformen zur Verfügung.

- Der erneute Anstieg der Betrugsmeldungen zeigt, dass Internetbenutzer in der Schweiz noch immer zu den beliebten Opfern von betrügerischen Handlungen im Internet zählen. Neue Modi Operandi erscheinen in regelmässigen Abständen, doch finden auch altbekannte Betrugsmaschen noch immer ihre Opfer.

- KOBIK hat den Einsatz bei den « aktiven Recherchen » erhöht, was sich in einem Anstieg der Verdachtsdossiers an die Kantone widerspiegelt.

- Die Auswertung der Rückmeldungen der kantonalen Polizeistellen und Justizbehörden belegt, dass die Verdachtsdossiers, die an die Kantone übermittelt werden konnten, solide recherchiert waren. Die meisten dieser Dossiers lösten Hausdurchsuchungen aus, bei denen belastendes Material sichergestellt wurde.

- Das Thema der «verdeckten Ermittlung» hat KOBIK im Berichtsjahr stark beschäftigt. Seit dem 1. Januar 2011 dürfen die meisten Kantonspolizisten nicht mehr präventiv verdeckt und ohne Verdachtsmoment im Internet gegen Pädokriminelle ermitteln, da ihre kantonalen Polizeigesetze dafür keine hinreichende Grundlage mehr bieten. Diese kantonale Gesetzeslücke ist durch die Inkraftsetzung der neuen Strafprozessordnung entstanden und hatte verschiedene parlamentarische Vorstösse zur Folge. Das EJPD hat mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren eine Lösung gefunden, die es KOBIK erlaubt, ihre Monitoring-Tätigkeit weiterzuführen. KOBIK kann dank einer Vereinbarung mit dem Kanton Schwyz weiterhin selber wie auch im Auftrag der Kantone präventiv verdeckt ermitteln und Chaträume überwachen.

2. Meldungseingang

Im Jahr 2010 gingen bei KOBIK 6’181 Verdachtsmeldungen per Internet-Meldeformular ein. Dies entspricht einem Rückgang von 18% gegenüber dem Vorjahr (7’541 Meldungen). Ob es sich dabei um eine generelle Tendenz oder lediglich um phänomenbedingte Schwankungen handelt, wie dies seit der Gründung der KOBIK schon mehrfach vorgekommen ist, wird sich zeigen. Mit Ausnahme des Rekordjahres 2007 liegt das Jahresmittel der Meldungen via Internet-Meldeformular stabil zwischen 6'000 und 7'500 Verdachtsmeldungen.

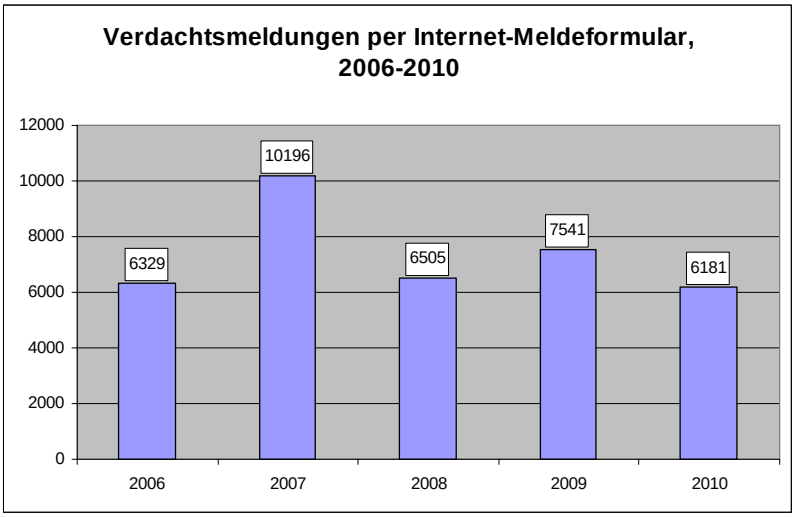

Abbildung 1 : Meldungseingänge über www.kobik.ch im Jahresvergleich

Bei der Betrachtung der Meldungseingänge nach Eingangsdatum können im Berichtsjahr grosse Unterschiede zwischen den einzelnen Monaten festgestellt werden (vgl. Abb. 2). Die Abweichungen sind jedoch oftmals auf konkrete und zeitlich begrenzte Ereignisse zurückzuführen.

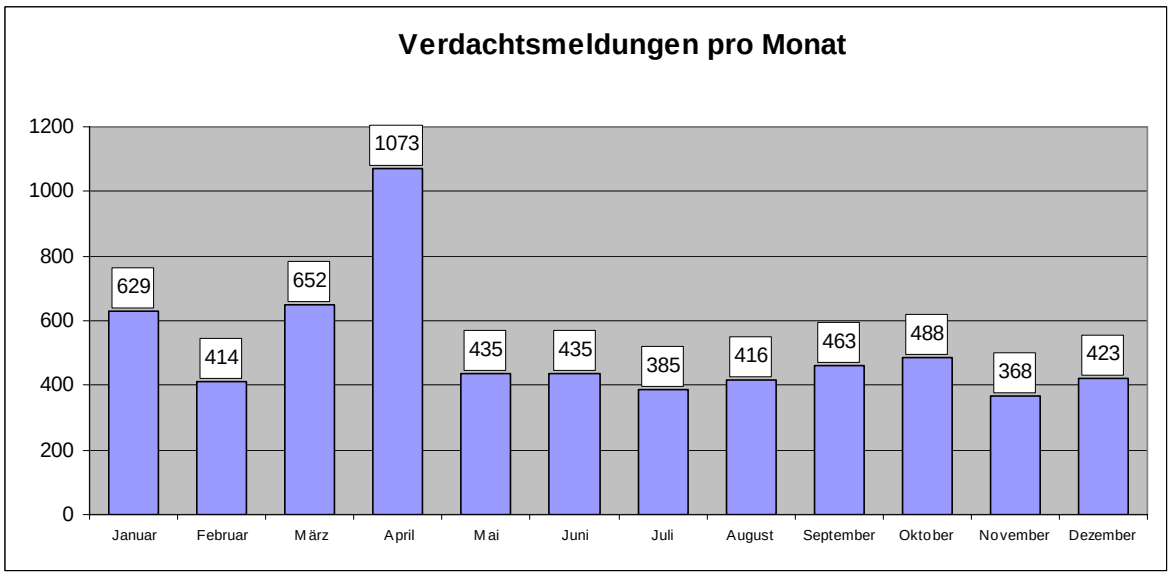

Abbildung 2 : Meldungseingänge über www.kobik.ch im Monatsvergleich (Total 6181 Meldungen)

3. Was wurde gemeldet?

Der signifikante Anstieg der Meldungen von Internetseiten mit verbotener Pornografie fällt auf. Die Kategorie „harte Pornografie“ fasst die Tatbestände des Artikels 197 Ziff. 3 StGB (Kinderpornografie, Pornografie mit Ausscheidungen, Tieren oder Gewalt) zusammen, wobei 96% der Meldungen kinderpornografische Seiten betreffen. Die im letzten Jahr festgestellte Tendenz setzt sich somit auch in diesem Jahr fort. Der deutliche Anstieg zeigt sich sowohl in den absoluten Zahlen, als auch im Verhältnis zu den anderen Straftatbeständen (vgl. Abb. 3 und 4). Der Anstieg der Meldungen betreffend Kinderpornografie steht teils in direktem Zusammenhang mit der steigenden Zahl an Web2.0-Anwendungen, wie z.B. „Communities, die vermehrt auch für den schnellen und anonymen Austausch von kinderpornografischem Material genutzt werden. Erstmals überstieg die Kategorie „harte Pornografie“ mit 1743 Meldungen zahlenmässig die Kategorie „SPAM“ (vgl. Abb. 3).

Parallel dazu wurde auch eine markante Abnahme der Meldungen zu sogenannter „legaler Pornografie“ festgestellt. Stark abgenommen haben insbesondere Meldungen über Internetseiten, die Pornografie via Streaming-Technologie zur Verfügung stellen. Die Abnahme dürfte unter anderem auf eine Abstumpfung oder auf eine gestiegene Toleranz de Internetbenutzer gegenüber solchen Angeboten zurückzuführen sein.

Die Meldungen zu Betrugsdelikten haben wie in den letzten Jahren auch im Berichtsjahr zugenommen. Seit dem Jahr 2006 stieg die Anzahl Meldungen in dieser Kategorie kontinuierlich an. Das zeigt, dass dieses Thema die Internetnutzer der Schweiz beschäftigt. Die Deliktskategorie befindet sich in einer stetigen Weiterentwicklung und verliert aufgrund neuer Modi Operandi nicht an Bedeutung. Besonders Kleinanzeige- und Auktionsseiten werden vermehrt als Tatort für betrügerische Handlungen genutzt. Beliebtes Ziel der Betrüger ist der Gebrauchtwagenhandel, wo ahnungslose Käufer oder Verkäufer mittels fingierten Transportunternehmen und lokalen Komplizen betrogen werden. Daneben sind auch andere Güter vom Onlinebetrug betroffen. Auch altbekannte Deliktsformen wie die sogenannten «Abofallen», bei denen der Benutzer mit einem vermeintlich kostenlosen Angebot ein kostenpflichtiges Abonnement abschliesst, oder der Vorschussbetrug[1] und seine diversen Varianten stellen immer noch aktuelle und effiziente Deliktsformen dar.

Im Vergleich zum Vorjahr wurde ein Anstieg der Meldungen bei der Kategorie «Wirtschaftsdelikte» festgestellt. 2010 fanden dabei verschiedene Wellen von Phishing-Attacken[2] gegen Bank- aber auch Übermittlungsdienstleister statt. Besonders aufgefallen ist der Modus Operandi, bei welchem sich Betrüger in einer ersten Phase illegal Zugang zu einem E-Mail-Konto verschaffen. In einer zweiten Phase werden die persönlichen Kontakte von den Betrügern angeschrieben und um eine Überweisung aufgrund eines Notfalls gebeten.

[1] Bei dieser Methode wird versucht, das Opfer mittels falscher Versprechen (z.B. grosser Lotteriegewinn) zur Vorausleistung einer Zahlung zu bewegen. Auf die versprochene Leistung wartet der Vorschussgeber vergeblich, weil die Gegenleistung von Anfang an nicht beabsichtigt war.

[2] Methode mit der versucht wird, über gefälschte WWW-Adressen an Daten eines Internet-Benutzers (Passwort, Benutzername usw.) zu gelangen.

Die Anfragen aus der Bevölkerung zu den Themen Internetkriminalität halten sich in den letzten Jahren auf stabil hohem Niveau, was daraufhin deutet, dass KOBIK national als Kompetenzzentrum in Sachen Internetkriminalität wahrgenommen wird.

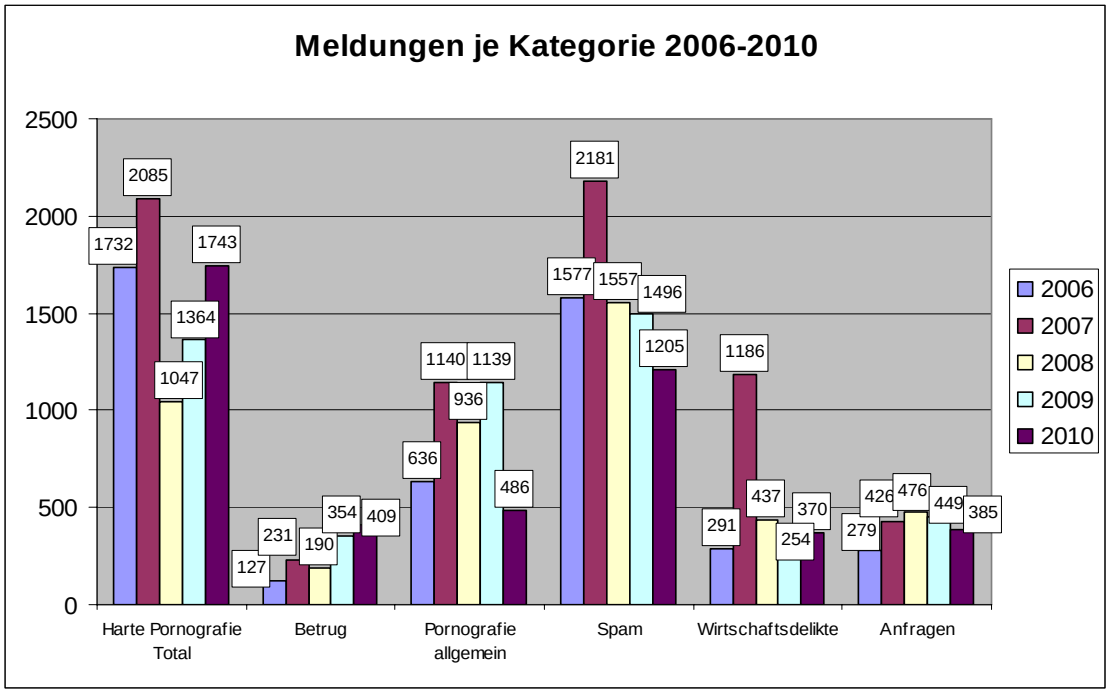

Abbildung 3 : Entwicklung der Kategorien von Straftaten mit den meisten Meldungen

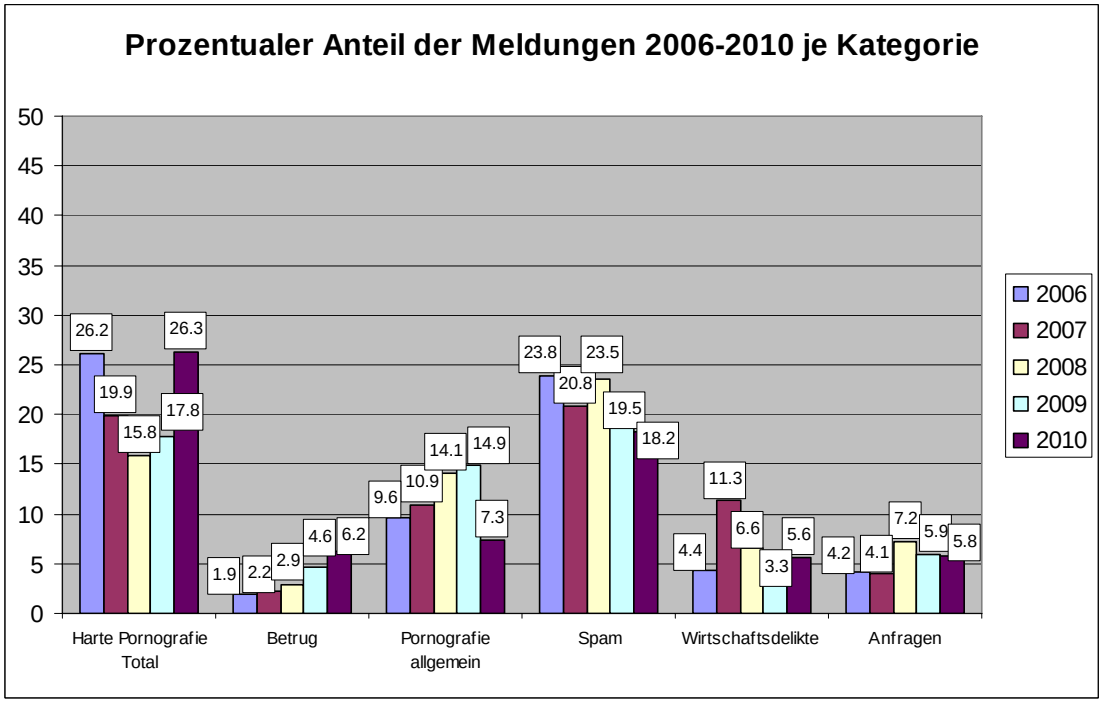

Abbildung 4 : Prozentualer Anteil ausgewählter Kategorien im Fünfjahresvergleich

Die Abbildung 5 gibt einen Überblick über die Entwicklung der wichtigsten Deliktskategorien der letzten fünf Jahre. Wie jedes Jahr gingen auch 2010 sehr viele Meldungen ein, die anschliessend den Kategorien „Andere“ (vgl. Seite 12) oder „Nicht überprüfbar“ zugeteilt werden mussten. Bei der letzten Kategorie handelt es sich in den meisten Fällen um Internetseiten, die zum Zeitpunkt der Überprüfung nicht mehr ak-

tiv waren. Die konstant hohen Zahlen dieser beiden Kategorien zeugen von der Schnelllebigkeit und Variabilität des Internets.

Obwohl in den Kategorien „Ehrverletzungsdelikte“ und „Drohung und Nötigung“ vergleichsweise wenige Meldungen eingingen, umfassen sie Phänomene, die KOBIK stark beschäftigten. So auch das Phänomen des „Cyberbullyings“, dem im Berichtsjahr eine besondere politische und mediale Aufmerksamkeit zukam. 2010 bearbeitete KOBIK insgesamt 25 Fälle (davon mindestens vier, bei denen Minderjährige betroffen waren), die unter die Definition des Cyberbullyings[3] fallen.

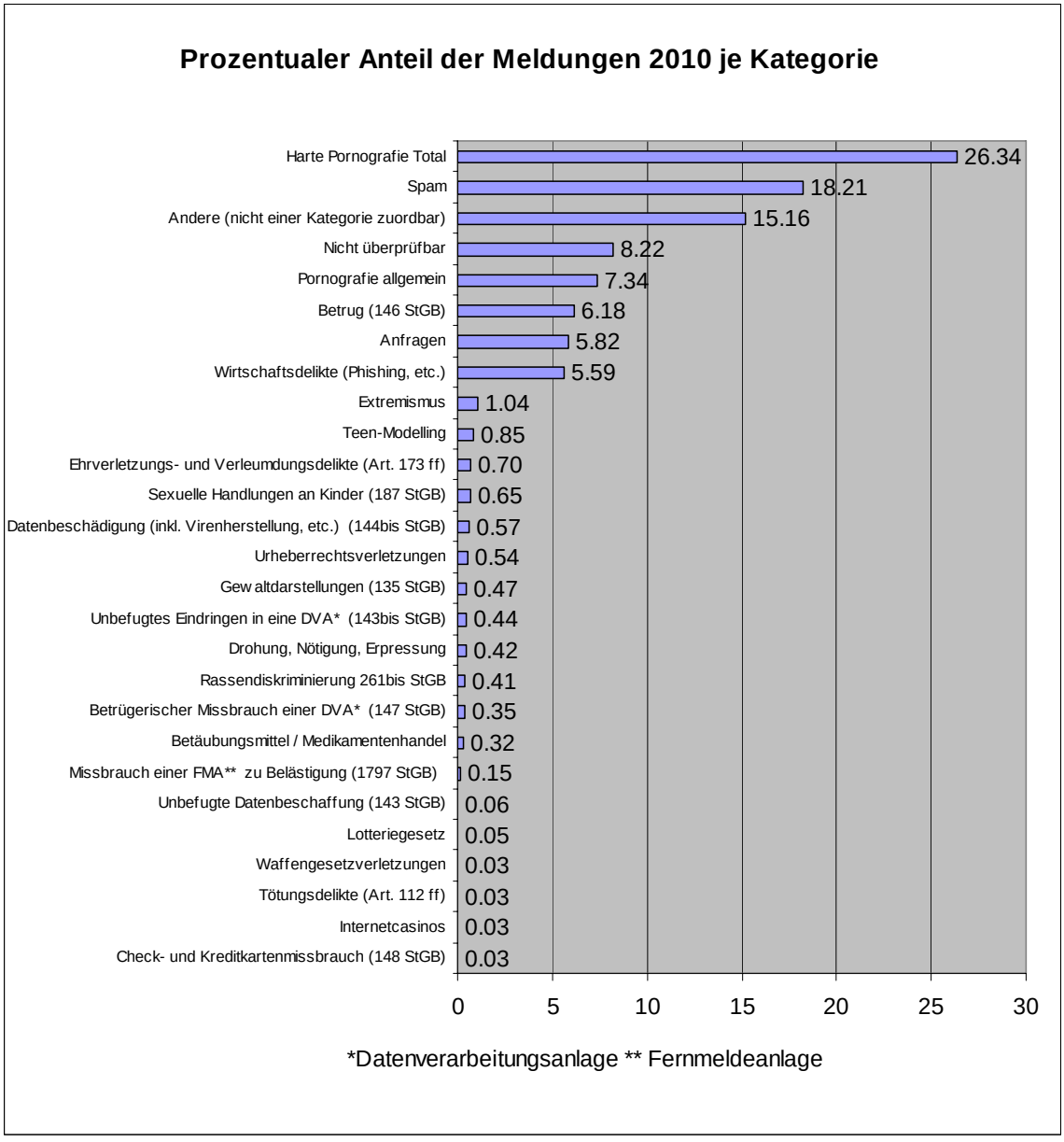

Abbildung 5 : Übersicht der kategorisierten Meldungen 2010 (prozentualer Anteil aller Meldungen)

[3] Definition von Cyberbullying gemäss Bericht des Bundesrates von Juni 2010: « Somit kann von Cyberbullying dann 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. ».

Neben den Meldungseingängen über das Online-Meldeformular sind auch jene hervorzuheben, welche KOBIK durch die Zusammenarbeit mit Telefono Arcobaleno[4] erhielt. 2010 meldete Telefono Arcobaleno 587 Links, welche zu kinderpornografischen Inhalten führten. In den meisten Fällen handelt es sich um Inhalte, welche sich auf sogenannten « One Click-Hostern[5] » mit Standort in der Schweiz befanden. KOBIK meldet die strafbaren Inhalte den Betreibern dieser Dienstleistung, welche sich anschliessend um deren Löschung kümmern. Die Anzahl Meldungen hat im Vergleich zum letzten Jahr stark abgenommen. Dies zeigt, dass diese Dienste unter anderem dank solcher Überwachungsmassnahmen mittlerweile weniger häufig für den Austausch von kinderpornografischem Material genutzt werden.

[4] Telefono Arcobaleno ist eine italienische Organisation, welche im Bereich Kinderschutz tätig ist.
[5] Diese Seiten bieten kostenloser Speicher an, welchen man nutzen kann um Daten ins Internet zu stellen. Mit einem einfachen Link können diese Daten beliebig vielen Internetbenutzern zur Verfügung gestellt werden.

4. Aktive Recherchen (Monitoring)

Als Folge der Optimierung der aktiven Recherchen (Monitoring) konnten im Berichtsjahr erneut mehr Verdachtsmeldungen zuhanden der Kantone eröffnet werden, womit sich die generelle Entwicklung der beiden Vorjahre bestätigt. So konnten 2010 insgesamt 229 Verdachtsdossiers zuhanden der kantonalen Strafverfolgungsbehörden erstellt werden. Wie der Leitungsausschuss festhält, ging es Fälle von systematischen Besitz und Verbreitung von kinderpornografischen Inhalten. Die Verdachtsdossiers resultieren aus der Überwachung von P2P-Netzwerken nach Schweizer Internetbenutzern, die sich aktiv am Austausch von kinderpornografischen Dateien beteiligen.

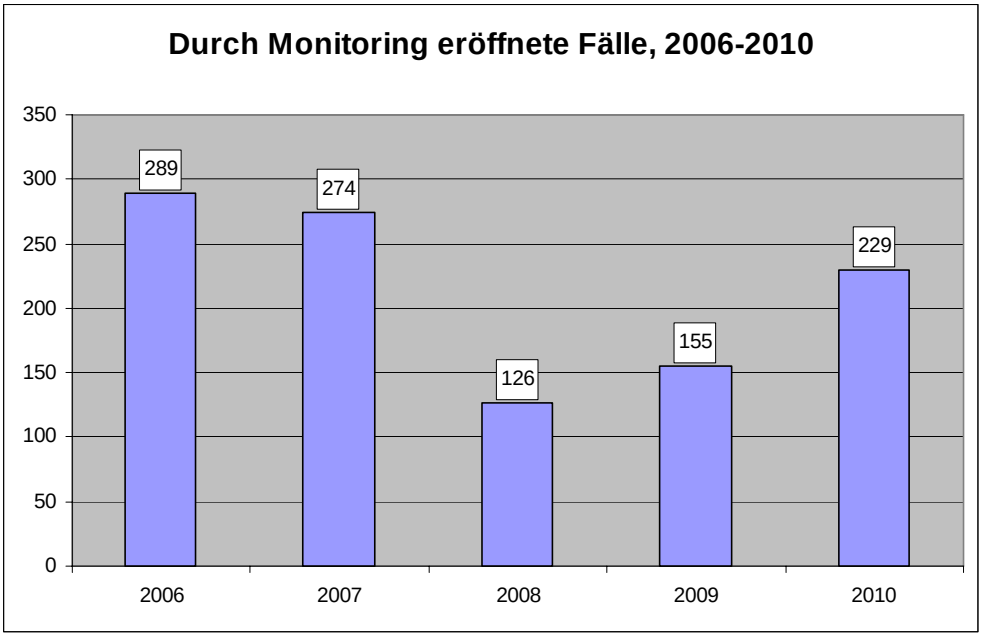

Abbildung 6: In Folge von KOBIK-Recherchen eröffnete Verdachtsdossiers [6]

[6] Erstellungsdatum des Verdachtsdossiers ist massgebender Zeitpunkt. Verdachtsdossiers wurden unter Umständen erst im Folgejahr an die zuständigen Strafverfolgungsbehörden weitergeleitet.

5. Ausgewählte Fallbeispiele

Im Rahmen der aktiven Recherche in P2P-Netzwerken fiel KOBIK unter anderem ein Schweizer auf, der sich kinderpornografisches Material aneignete und weiterverbreitete. Nach entsprechenden Abklärungen konnte der Standort des Internetanschlusses bestimmt werden und das Verdachtsdossier wurde der entsprechenden Kantonspolizei übergeben. Wie die Nachforschungen der ermittelnden Kantonspolizei ergaben, handelte es sich bei dem Verdächtigen um einen Wochenaufenthalter mit Wohnsitz in einem anderen Kanton. Das Verdachtsdossier wurde daraufhin dem Kommissariat Pädophilie/Pornografie der Bundeskriminalpolizei übergeben, welche die Koordination mit dem Wohnsitzkanton des Verdächtigen übernahm. KOBIK wurde kurze Zeit später von der zuständigen Kantonspolizei gebeten ,weitere Abklärungen vorzunehmen, da es sich bei dem Verdächtigen um eine beruflich exponierte Person handelte und die vorliegende Beweislage eine Hausdurchsuchung noch nicht rechtfertigte. Mittels verdeckter Ermittlung konnte KOBIK die Aktivitäten des Verdächtigen in sozialen Netzwerken mitverfolgen, neue Beweise sammeln und der Kantonspolizei die erforderliche Bestätigung des Verdachtes liefern. Bei der darauffolgenden Hausdurchsuchung konnte kinderpornografisches Bild- und Videomaterial beschlagnahmt werden. Die betroffene Person war in Anbetracht der Beweise geständig.

In einem weiteren Fall konnte dank der aktiven Recherche in P2P-Netzwerken ein Schweizer identifiziert werden, der sich kinderpornografisches Material aneignete und weiterverbreitete. Bei der anschliessenden Hausdurchsuchung durch die zuständige Kantonspolizei wurde festgestellt, dass der Verdächtige bereits über einen längeren Zeitraum sexuelle Handlungen an einer Minderjährigen beging. Wie sich später herausstellte führte, die drogenabhängige Mutter des minderjährigen Opfers die Tochter der Prostitution zu.

Bei einem weiteren Fall konnte KOBIK dank einer verdeckten Ermittlung einen 42-jährigen Schweizer identifizieren, der in einem für Kinder und Jugendliche reservierten Chatraum gezielt den Kontakt zu einem Mädchen suchte, das angab, erst 13 Jahre alt zu sein. Das kindliche Alter des vermeintlichen Mädchens hielt den Erwachsenen nicht davon ab Bemerkungen mit eindeutig sexuellen Inhalten zu machen. Auch wurde wiederholt nach Fotos und weiterem Kontakt gefragt. Der Fall wurde an die zuständige kantonale Strafverfolgungsbehörde weitergeleitet.

6. Adressaten der Verdachtsdossiers

Im Berichtsjahr konnten insgesamt 299 Verdachtsdossiers und damit deutlich mehr als im Vorjahr an die kantonalen Strafverfolgungsbehörden weitergeleitet werden. Diese Entwicklung hängt direkt der verstärkten aktiven Recherchetätigkeit von KOBIK zusammen.

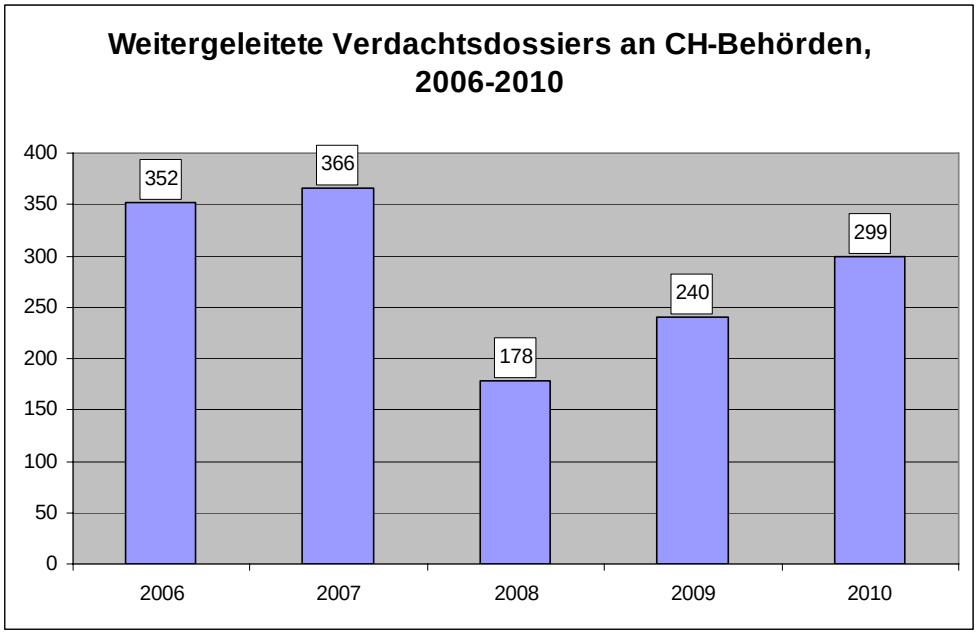

Abbildung 7: Weitergeleitete Verdachtsdossiers

Die genauere Analyse der weitergeleiteten Verdachtsdossiers (vgl. Abb. 8) zeigt, dass es sich dabei hauptsächlich um Fälle aufgrund aktiver Recherchen in den P2P-Netzwerken handelt. Im Berichtsjahr konnten insgesamt 245 solcher Verdachtsdossiers erstellt und an die kantonalen Strafverfolgungsbehörden weitergeleitet werden. Zusätzlich führten Meldungen aus der Bevölkerung zu 54 weiteren Verdachtsdossiers zuhanden der kantonalen Strafverfolgungsbehörden.

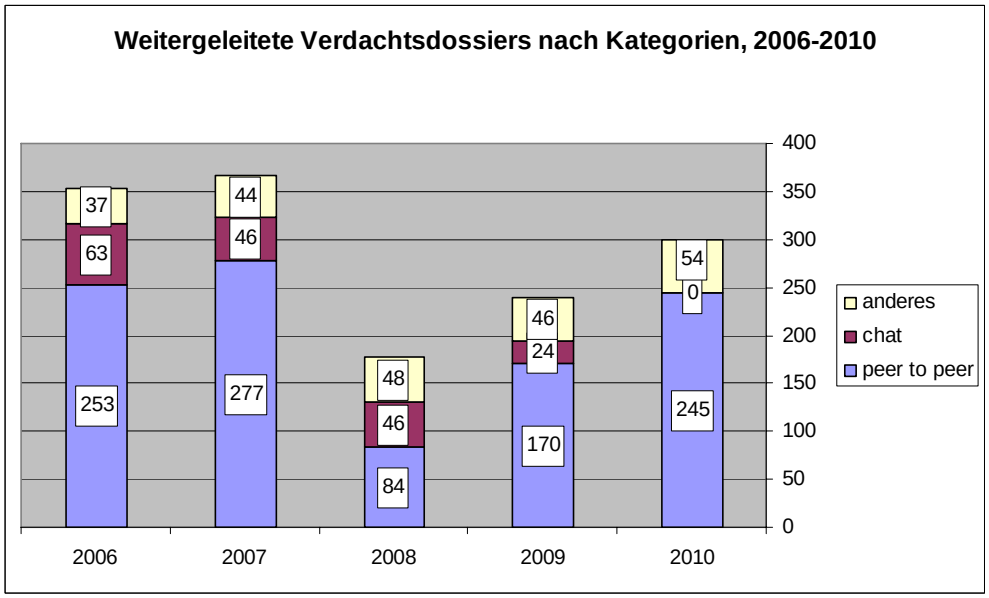

Abbildung 8: Weitergeleitete Verdachtsdossier nach Kategorien

Im Berichtsjahr konnten keine Verdachtsdossiers der Kategorie «Chat» erstellt werden. Dies liegt in erster Linie daran, dass sich Swisscom als Betreiber der beiden Plattformen «Teentalk» und «Kidstalk» im Jahr 2009 zurückgezogen hat. Die Verdachtsdossiers dieser Kategorie basierten auf einer langjährigen Zusammenarbeit zwischen KOBIK und der Swisscom. Die Entwicklungen im Bereich der verdeckten Ermittlungen (vgl. Kapitel 9.2) und der Wechsel der Betreiber dieser Chats zwangen KOBIK zu einer entsprechenden Aufgabenpriorisierung.

Seit Jahren sind die Zahlen der Kategorie «Andere» stabil (vgl. Abb. 8). In diese Kategorie fallen unter anderem Hinweise auf pornografische Seiten ohne ordentliche Altersüberprüfung, aber auch Hinweise auf andere Arten von Seiten mit Standort in der Schweiz, deren Inhalte strafrechtlich relevant sein könnten. Verdachtsdossiers, die an eine Bundesbehörde weitergeleitet wurden, fallen ebenfalls in diese Kategorie.

Wie bisher wurden die meisten Verdachtsdossiers der Koordinationsstelle zur Bekämpfung der Internetkriminalität an die Stadt- und Kantonspolizei Zürich weitergeleitet (vgl. Abb. 9). Es folgen die Kantone Waadt, Aargau und Bern. In 22 Fällen wurde das Verdachtsdossier an eine Bundesbehörde weitergeleitet. Hauptadressaten dieser Verdachtsdossiers waren das Kommissariat Pädophilie/Pornografie der Bundeskriminalpolizei, Swissmedic, die Melde- und Analysestelle Informationssicherheit MELANI oder die Lotteriekommission (Comlot).

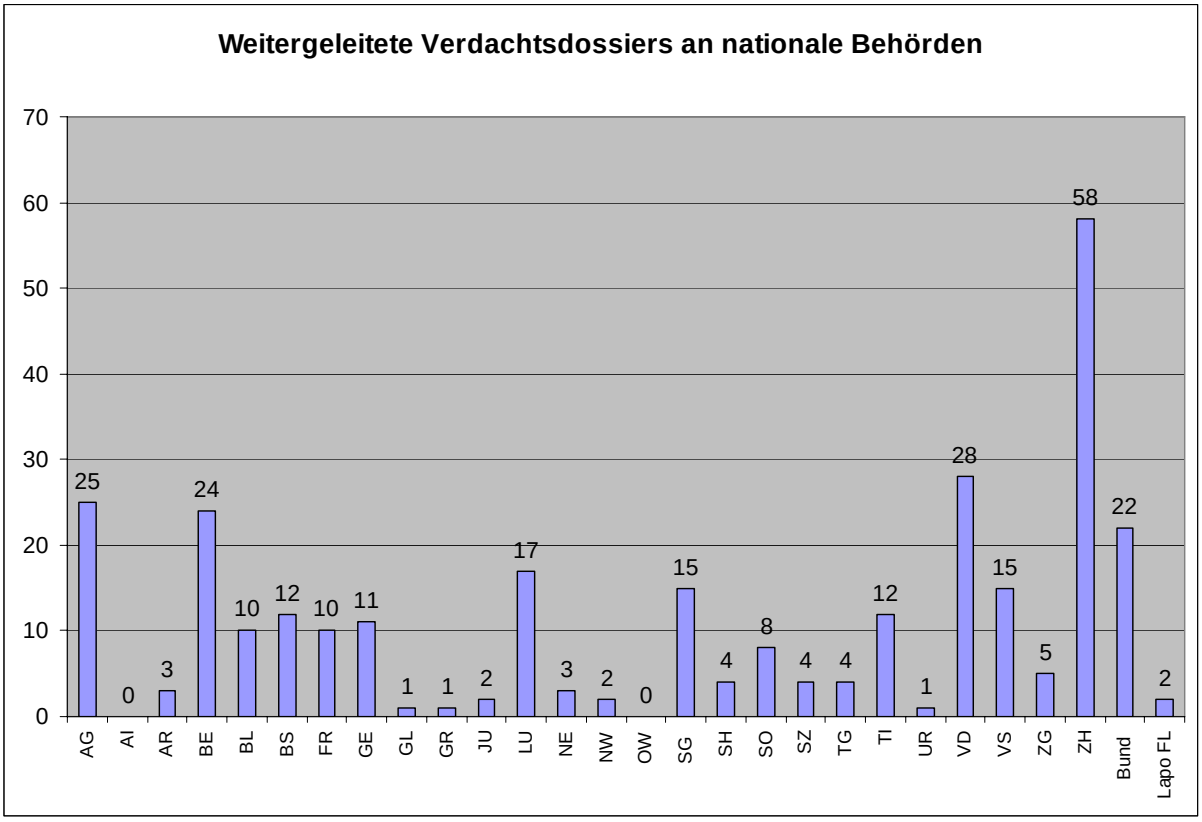

Abbildung 9: Anzahl der an Schweizer und Liechtensteiner Behörden weitergeleiteten Verdachtsdossiers (Total= 299)

Zusätzlich meldete KOBIK 2010 insgesamt 231 Internetseiten den zuständigen Stellen im Ausland. Dabei handelte es sich fast ausschliesslich um Interseiten mit kinderpornografischen Inhalten, die via Meldeformular bei KOBIK eingingen.

7. Rückmeldungen aus den Kantonen

KOBIK leitet Fälle, in denen der begründete Verdacht für eine Straftat besteht, zur Bearbeitung an die Kantone weiter (siehe Kapitel 5). Um sich einen Überblick über die Schritte verschaffen zu können, die in den Kantonen eingeleitet wurden, ersucht KOBIK die Kantone um Informationen über den Verlauf der ihnen gemeldeten Verdachtsfälle, über die eingeleiteten polizeilichen Massnahmen und über den Ausgang der Gerichtsverfahren. Ungefähr 90 % aller weitergeleiteten KOBIK-Fälle führten zu Hausdurchsuchungen durch kantonale Polizeibehörden. In über 80 % der Hausdurchsuchungen, die aufgrund der Verdachtsmeldungen durchgeführt wurden, konnte einschlägiges illegales Material beschlagnahmt werden. In ungefähr 90 % der Fälle, in denen die kantonalen Justizbehörden KOBIK eine Rückmeldung erstatteten, endeten die Strafverfahren mit einer Verurteilung.

8. Arbeitsgruppen

Während des Berichtsjahres war KOBIK in verschiedenen nationalen Arbeitsgruppen vertreten, namentlich im Bereich Kriminalprävention.

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

Seit 2010 arbeitet KOBIK im nationalen Programm „Jugendmedienschutz und Medienkompetenzen“ sowohl in der mit der Programmausarbeitung vertrauten Leitgruppe, als auch in der ausführenden Begleitgruppe mit. Das Programm soll Kindern und Jugendlichen helfen, einen sicheren, verantwortungsvollen und dem Alter angepassten Umgang mit den modernen Medien zu finden. In einem ähnlichen Gebiet unterstützte KOBIK das Eidg. Justiz- und Polizeidepartement bei der Ausarbeitung des Berichtes über „Cyberbullying“ (Belästigung übers Internet), wie dies Nationalrätin Barbara Schmid-Federer in einem Postulat gefordert hatte. Der Bericht wurde am 2. Juni 2010 veröffentlicht und ist auf der Internetseite von fedpol verfügbar.

KOBIK war zudem an der Ausarbeitung 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 2010 den Bereichen der technischen Entwicklung und der effizienten Strafverfolgung Rechnung tragen.

9. Projekte

9.1. Zusammenarbeit mit den Schweizerischen Internet Access Providern[7] zur Filterung kinderpornografischer Internetseiten

Seit 2007 werden in der Schweiz Kinderpornografie-Websites mithilfe der Filtersoftware *Child Sexual Abuse Anti-Distribution Filter* gesperrt. Die Sperre richtet sich dabei gegen ausländische Internetseiten mit kinderpornografischem Inhalt.

9.2 Verdeckte Ermittlung

Viel Einsatz forderte die Klärung der rechtlichen Situation im Zusammenhang mit der neuen eidgenössischen Strafprozessordnung (StPO) und die Aufgabenpriorisierung des Kommissariates im Hinblick auf die neue Ausgangslage. Seit dem 1. Januar 2011 dürfen die meisten Kantonspolizisten nicht mehr präventiv verdeckt und ohne Verdachtsmoment im Internet gegen Pädophile ermitteln, da ihre kantonalen Polizeigesetze dafür keine hinreichende Grundlage bieten. Diese Gesetzeslücke ist durch die Inkraftsetzung der neuen Strafprozessordnung entstanden. Die bisherige Grundlage für die präventive verdeckte Ermittlung war im Bundesgesetz über die verdeckte Ermittlung BVE zu finden, welches mit Inkrafttreten der StPO aufgehoben wurde.

Einige Kantone wie Schwyz, Uri und Obwalden haben den Handlungsbedarf erkannt und ihre Polizeigesetze auf den 1. Januar 2011 angepasst. Das EJPD seinerseits hat mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) eine Lösung gefunden, die es der gemeinsamen Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) ermöglicht, ihre Monitoring-Tätigkeit im Internet hinsichtlich Pädokriminalität weiterzuführen. KOBIK kann dank einer Vereinbarung mit dem Sicherheitsdepartement des Kantons Schwyz weiterhin im Auftrag der Kantone präventiv verdeckt ermitteln und somit Chaträume überwachen. Die Arbeit der KOBIK stützt sich zurzeit auf das Polizeirecht des Kantons Schwyz sowie auf eine Bewilligung des Zwangsmassnahmegerichts des Kantons Schwyz. Damit ist sichergestellt, dass Pädokriminelle im Internet weiterhin nicht in einem kontrollfreien Raum wähnen können.

[7] Internet Access Provider ermöglichen einem Internetbenutzer den Zugang zum Internet.

10. Politische Vorstösse auf Bundesebene

Die im Berichtsjahr eingereichten parlamentarischen Vorstösse:

Kinder- und Jugendschutz

- Kantonale Initiative BE: Mediengewalt. Umfassender Schutz von Kindern und Jugendlichen
- Initiative Schmid-Federer: Effektivität und Effizienz in den Bereichen Jugendmedienschutz und Internetkriminalität
- Interpellation Amherd: Jugendmedienschutz. Weiteres Vorgehen nach den Präventionsprogrammen
- Motion Bischofberger: Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität
- Motion Schweiger: Jugendliche den gezielten Umgang mit neuen Medien lehren
- Frage Graber: Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch
- Frage Schmid-Federer: Überwachung von Chatrooms
- Motion Amherd: UNO-Resolution zur Bekämpfung des virtuellen Kindsmissbrauchs
- Interpellation Markwalder: Effizienz im Bereich Jugendmedienschutz und Medienkompetenz
- Motion Amherd: Jugendmedienschutz. Schaffung eines nationalen Kompetenzzentrums für elektronische Medien
- Motion Amherd: Zertifizierung von Internetseiten
- Postulat Amherd: Verfassungsgrundlage für die Schaffung einer nationalen Kontrollstelle für die Zertifizierung von Websites

Verdeckte Ermittlung

- Initiative Schlüer: Verdeckte Fahndung zur Verbrechensprävention
- Motion Fiala: Verdeckte Ermittlung
- Frage Baumann: Abwehr pädosexueller Straftaten im Internet
- Frage Rickli: Verdeckte Ermittlung gegen Pädophile
- Frage Schmid-Federer: Verdeckte Ermittlung im Internet
- Frage Schmid-Federer: Verdeckte Ermittlung, Artikel 286a StPO

Schutz der Persönlichkeit

- Interpellation Hiltpold: Eigenmächtige Verbreitung von Fotos oder Videos und Schutz der betroffenen Personen
- Postulat Graber: Angriffe auf die Privatsphäre und indirekte Bedrohung der persönlichen Freiheit
- Postulat Hodgers: Anpassung des Datenschutzgesetzes an die neuen Technologien

Cyberwar

- Motion Büchler: Schutz vor Cyberangriffen
- Postulat Recordon: Analyse der Bedrohung durch Cyberwar
- Postulat Büchler: Kapitel zu Cyberwar im sicherheitspolitischen Bericht

Cybermobbing / Cyberbullying

- Postulat Schmid-Federer: Einsetzung eines eidgenössischen Mobbing- und Cyberbullying-Beauftragten

Internetkriminalität im Generellen

- Frage Büchler: Internetkriminalität
- Postulat Kommission für Rechtsfragen SR: Ermittlung von Internetstraftätern
- Motion Barthassat: Mehr Sicherheit dank besserer Beherrschung der Technik
- Motion Barthassat: Verlängerung der Aufbewahrungspflicht von Protokollen über die Zuteilung von IP-Adressen
- Postulat Darbellay: Konzept zum Schutz der digitalen Infrastruktur der Schweiz
- Postulat FDP-Liberale Fraktion: Leit- und Koordinationsstelle im Bereich der Cyber-Bedrohung

Andere

- Kantonsinitiative ZG: Verbot von Gewaltspielen
- Interpellation Mörgeli: Kostenintensive Auflagen des EJPD an private Internet-Dienstleistungsfirmen
- Interpellation Parmelin: Gefahren der Medikamentenfälschung und des Medikamentenschmuggels
- Interpellation Schmid-Federer: KOBIK/Melani. Bilanz nach der Reorganisation des DAP
- Postulat Savary: Braucht die Schweiz ein Gesetz gegen das illegale Herunterladen von Musik?
- Question Graber: Wikileaks-Affäre. Auswirkungen für die Schweiz und Meinung des Bundesrates
- Frage Rickli: Switch
- Motion Darbellay: Verdoppelung der Stellen bei KOBIK und Klärung des Auftrags und der Organisationsstruktur
- Initiative Schmid-Federer: Straftatbestand „digitaler Hausfriedensbruch“

11. Medienauftritte, Ausbildung und Konferenzen

11.1 Medienpräsenz

Wie auch in den Vorjahren konnte KOBIK im Allgemeinen eine äusserst positive Resonanz in den Medien verzeichnen. Zahlreiche Artikel in den Printmedien und einige Berichte in den elektronischen Medien befassten sich mit der Arbeit von KOBIK. Besondere mediale Aufmerksamkeit kamen im Berichtsjahr der Thematik «Cybermobbing» und der verdeckten Ermittlung durch KOBIK zu. Die Koordinationsstelle zur Bekämpfung der Internetkriminalität ihrerseits hatte diverse Gelegenheiten zur Stellungnahme bei Themen, welche in ihre Zuständigkeit fallen.

11.2 Ausbildung und Konferenzen

Im Berichtsjahr nahmen KOBIK-Mitarbeitende an einer Vielzahl von Konferenzen, internationalen Tagungen und Ausbildungslehrgängen teil:

In der Schweiz :

- IT-Ermittler Tagung
- Lehreinsatz im Rahmen des MAS Forensics der HSW Luzern.
- Lehreinsatz im Rahmen des jährlichen Hauptkurses der Mitteleuropäische Polizeiakademie (MEPA)
- Teilnahme am Podiumsgespräch, Tweakfest 2010
- Teilnahme am Roundtable « Cybercrime & Cybersecurity » des Democratical Control of Armed Forces (DCAF)

Im Ausland :

- RIPE NCC Meeting, London
- Octopus Interface, Strasbourg
- E-Crime Congress, London

12. Partnerschaften und Kontakte

12.1 Zusammenarbeit mit anderen Bundesstellen

Die Fülle an Themen und Problemstellungen im Bereich Internetkriminalität erfordert eine enge Zusammenarbeit mit anderen Bundesstellen. Innerhalb der Bundeskriminalpolizei arbeitet KOBIK eng mit den Kommissariaten „Pädophilie-Pornografie", „IT-Ermittler" und „Verdeckte Ermittlungen" zusammen. Je nach Tatbestand kommt die Zusammenarbeit mit weiteren Kommissariaten der Bundeskriminalpolizei zum Tragen.

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 des Bundesamtes für Justiz (BJ), das Bundesamt für Kommunikation (BAKOM), Swissmedic und die Lotteriekommission (Comlot).

12.2 Arbeitssitzungen und Erfahrungsaustausch mit den Kantonen

Im Berichtsjahr fanden Kontakte mit diversen kantonalen Polizeikorps und Untersuchungsrichterinnen und –richtern statt. Teils fanden Arbeitssitzungen mit Kantonsvertretern aufgrund konkreter Themen statt. Im Rahmen des jährlichen Erfahrungsaustausches stattete zudem die Landespolizei Liechtenstein (LAPO) KOBIK einen Arbeitsbesuch ab.

12.3 Externe Besucher

Im Berichtsjahr interessierten sich auch diverse externe Besucher für die Tätigkeit von KOBIK. Diese Besuche ermöglichen den Mitarbeitern der KOBIK, ihre Arbeit zu präsentieren und die Besucher auf die damit verbundenen Problemstellungen und Zusammenhänge aufmerksam zu machen. Zu den Höhepunkten zählten die Besuche der Departementschefin Bundesrätin Widmer-Schlumpf, verschiedener Nationalräte, Journalisten aber auch derjenige der Direktorin von Action Innocence (AIG), einer Nichtregierungsorganisation, mit welcher KOBIK eine langjährige Zusammenarbeit im Kampf gegen die Kinderpornografie im Internet verbindet.

12.4 Internationale Zusammenarbeit

Zusätzlich zu oben genannten internationalen Konferenzen boten sich KOBIK im Rahmen konkreter Projekte oder Arbeitsgruppen zahlreiche Möglichkeiten der operativen Zusammenarbeit mit internationalen Partnerstellen. Wie im Vorjahr war KOBIK auch 2010 in der „Law Enforcement Cooperation Working Group" (LECWG) der „European Financial Coalition" (EFC) in Brüssel vertreten.

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 zuordenbarer 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 Resource Locator (dt. einheitlicher Quellenanzeiger) Eine aus Ziffern und Zahlen bestehende Adresse (umgangssprachlich: Internetadresse).

14. Trends 2010

Ein wichtiges Merkmal des letzten Jahres stellt die Zunahme der Meldungen betreffend kinderpornografischer Inhalte im Internet dar. Die Tendenz der letzten Jahre wurde auch 2010 bestätigt. Die Speicher- und Distributionsmöglichkeiten für strafbare Inhalte im Internet sind vielfältig und erleben eine rasante Entwicklung. Was den Modus Operandi betrifft, so erweisen sich die Täter als sehr flexibel und anpassungsfähig. Stark zugenommen hat die Nutzung von sozialen Netzwerken zum Austausch kinderpornografischer Inhalte innerhalb geschlossener Benutzergruppen.

Die Zunahme der Meldungen von Betrugsopfern beziehungsweise Betrugsversuchen im Internet hat KOBIK im Berichtsjahr stark beschäftigt. Neue Modi Operandi sind aufgetaucht, aber auch altbekannte und meist leicht durchschaubare Betrugsmaschen, auf die immer wieder Opfer hereinfallen. Dabei werden bewusst grenzüberschreitende Mechanismen eingesetzt, die eine Strafverfolgung schwierig und komplex gestalten. Dieser Umstand zeigt einerseits die Bedeutung der Förderung internationaler Koordination im Bereich Internetkriminalität auf, aber andererseits auch, dass die Prävention und Sensibilisierung der Internetbenutzer oftmals das effizienteste Mittel im Kampf gegen Online-Betrug darstellen. Unter Einhaltung einfachster Vorsichtsregeln können die meisten Betrugsfälle rechtzeitig als solche erkannt werden. Viele Betrüger nutzen frei zugängliche Daten, um ihre Opfer gezielt anzugehen.

2010 konnten die Ressourcen im Bereich der aktiven Recherchen in Peer-to-Peer-Netzwerken erhöht werden. Die aktive Recherche stellt immer noch das wichtigste Mittel der Koordinationsstelle zur Bekämpfung der Internetkriminalität in der Bekämpfung der Kinderpornografie im Internet dar, hat aber auch einen wichtigen Einfluss auf die Sensibilisierung der Täter, die sich nie in einem rechtsfreien Raum wähnen können. Um mit den technischen Veränderungen und dem angepassten Verhalten der Täter Schritt zu halten, werden die von KOBIK eingesetzten Hilfsmittel und Arbeitsmethoden laufend weiterentwickelt.

Den Schwierigkeiten bei der Identifizierung von Personen, welche mit Mobiltelefonen auf das Internet zugreifen, wird im Rahmen der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) Rechnung getragen. Zudem wird das BÜPF den technischen Entwicklungen angepasst und erfasst das Internet nun ausdrücklich, also auch E-Mail-Verkehr und Internettelefonie.