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 2012

VORWORT

von Regierungsrat Neuhaus, Vorsitzender des Leitungsausschusses KOBIK

Wo viel Licht ist, gibt es bekanntlich auch viel Schatten. Schatten gibt es auch - in den schwer zugänglichen Bereichen des Internets, wo Kriminelle auf besonders schäbige Weise aktiv sind. Genau dort muss die Koordinationsstelle für Bekämpfung der Internetkriminalität (KOBIK) Licht ins Dunkel bringen, aktiv sein und bleiben, entlarven und Strafanzeigen möglich machen. Denn als nationale Anlaufstelle für Personen, die verdächtige Internetinhalte melden wollen, erlebt KOBIK mit seinen Aufgaben leider einen wahren Boom. Im vergangenen Jahr wurden 55% mehr Fälle gemeldet als noch im Vorjahr. Erstmals gingen mehr Meldungen im Bereich Wirtschaftskriminalität (37%) ein, als Meldungen zu verbotener Pornografie (33%).

KOBIK erfüllt ihre Kernaufgabe weiterhin kompetent, geht aber auch neue Wege. So wurde erstmals das „Forum Cybercrime Staatsanwaltschaften - KOBIK“ durchgeführt. Die Veranstaltung hatte unter anderem zum Ziel, bestehende Unsicherheiten bei den Staatsanwaltschaften im Umgang mit der Internetkriminalität und bezüglich der technischen Möglichkeiten auszuräumen.

KOBIK nimmt jedoch nicht nur Meldungen aus der Bevölkerung entgegen und bearbeitet diese. Sie erzielt durch verdachtsunabhängige Recherchen auch präventive Wirkung in den weniger zugänglichen Bereichen des Internets. Jährlich wird der Schwerpunkt der aktiven Recherche durch den Leitungsausschuss neu definiert. Auch 2012 lag dieser bei der Bekämpfung der Pädokriminalität im Internet. Der Leitungsausschuss hat bei der Festlegung der Prioritäten aber auch explizit festgehalten, dass sich KOBIK den Wirtschaftsdelikten und der Internetkriminalität im engeren Sinne nicht verschliessen darf. Eine Strategie, die von den aktuellen Zahlen bestätigt wird. KOBIK und ihre Aufgabe ist unverzichtbar geworden.

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
Nussbaumstrasse 29
3003 Bern
www.kobik.ch
www.cybercrime.ch

Veröffentlicht: 23. April 2013

Inhaltsverzeichnis

1. Das Wichtigste in Kürze

- 2012 gingen bei KOBIK insgesamt 8‘242 Meldungen über das Online-Meldeformular ein. Dies entspricht einer Zunahme von 55% gegenüber dem Vorjahr.

- 39% der Meldungen betrafen Vermögensdelikte. Somit gingen 2012 erstmals mehr Meldungen zu Wirtschaftsdelikten ein, als Meldungen betreffend strafbarer Handlungen gegen die sexuelle Integrität (33%). Dies, obwohl auch in dieser Kategorie deutlich mehr Meldungen eingingen als im Vorjahr.

- Insgesamt 383 Meldungen führten direkt und aufgrund der strafrechtlichen Relevanz zur Übermittelung eines Verdachtsdossiers an nationale oder internationale Behörden und Organisationen.

- Durch das aktive Monitoring in P2P-Netzwerken gelang es KOBIK, im Berichtsjahr 417 Personen zu identifizieren, die aktiv am Austausch von Kinderpornografie beteiligt waren.

- Verdeckte Vorermittlungen durch KOBIK führten 2012 in insgesamt 33 Fällen zu Strafanzeigen zuhanden der zuständigen Kantone.

- Die Nationale Datei- und Hashwertesammlung (NDHS) ist seit Oktober 2012 in Betrieb. Sämtliche Testarbeiten und Systemanpassungen konnten erfolgreich abgeschlossen werden.

- Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken gutgeheissen, bei welcher KOBIK aktiv mitgearbeitet hat. Mit der Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, welchen sie täglich ausgesetzt sind.

2. KOBIK, die Meldestelle

Die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) ist die zentrale Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Die Meldungen, welche über das Online-Meldeformular (www.cybercrime.ch) eingehen und strafrechtlich relevant sind, werden nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet.

2.1 Meldungseingang

Im Jahr 2012 gingen bei KOBIK **8‘242 Verdachtsmeldungen** per Online-Meldeformular ein. Dies entspricht einer markanten Zunahme von 55% gegenüber dem Vorjahr (5‘330 Meldungen). Die Entwicklung des Meldungseinganges erlaubt jedoch keine Rückschlüsse auf die effektive Entwicklung der Internetkriminalität oder illegaler Inhalte im Internet. Daraus lassen sich aber Tendenzen über die Meldebereitschaft der Bevölkerung und der Wahrnehmung von Internetkriminalität in der Gesellschaft ableiten.

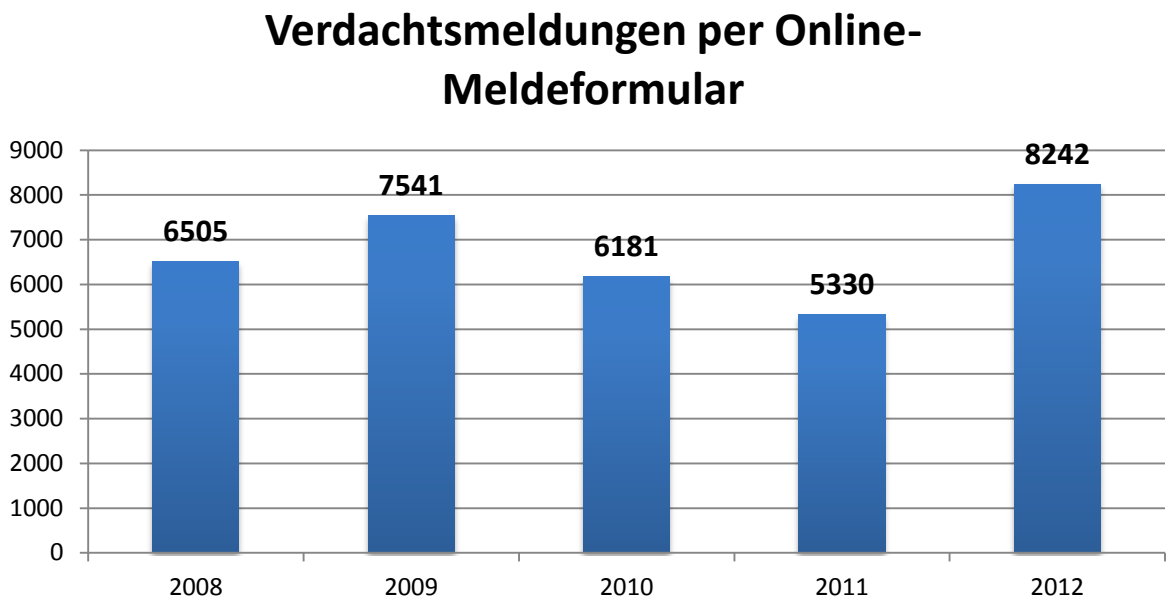


Abbildung 1 : Meldungseingänge über www.kobik.ch im Jahresvergleich

Mögliche Gründe für die Zunahme der Meldungen über das Meldeformular gibt es mehrere, wie zum Beispiel einzelne Vorfälle mit medialer Berichterstattung oder Warnmeldungen, welche KOBIK regelmässig kommuniziert.

Die Meldungseingänge waren Anfang 2012 sehr konstant. Diverse konkrete und zeitlich begrenzte Vorfälle trafen grosse Teile der Bevölkerung im Sommer und Herbst und führten zu einem erheblichen Anstieg der Meldungen (vgl. Abb. 2).

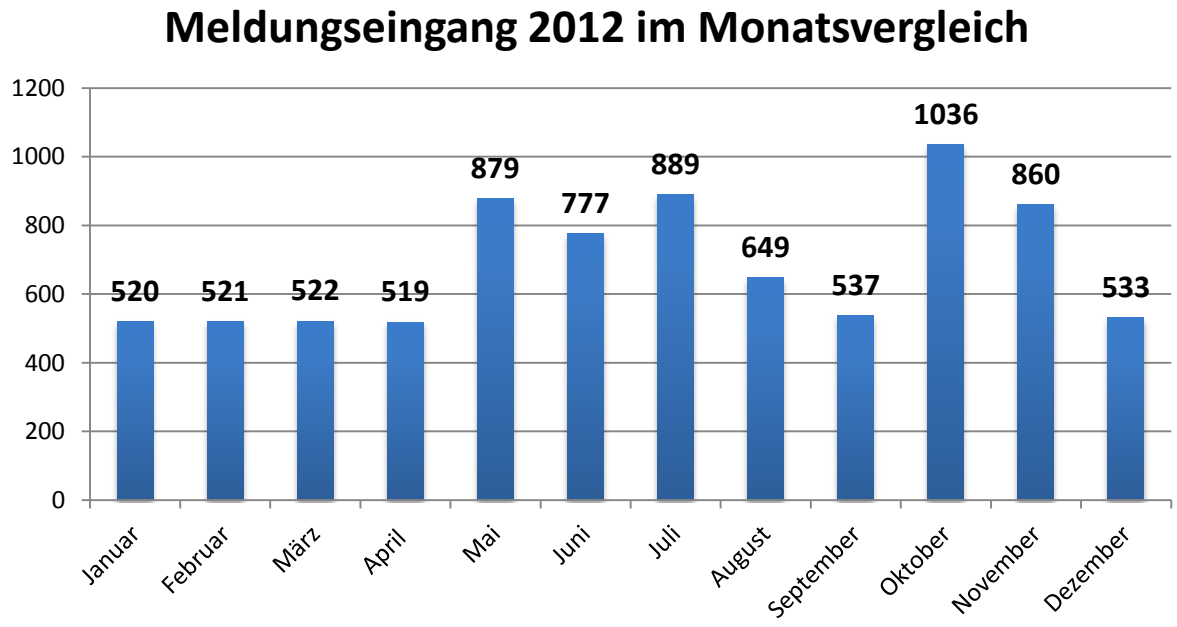


Abbildung 2 : Meldungseingänge über www.kobik.ch im Monatsvergleich (Total 8242 Meldungen)

2.2 Was wurde gemeldet?

Die Meldungen, welche KOBIK über das Meldeformular erreichen, sind vielseitig und in der Regel von guter Qualität. Über 80% der Meldungen (6‘639 Meldungen), die 2012 eingingen, wiesen eine strafrechtliche Relevanz auf. Die gemeldeten Delikte sind insbesondere verbotene Pornografie, Gewaltdarstellungen, Rassismus, Extremismus, Ehrverletzung, Drohung, Phishing, Betrug, unbefugtes Eindringen in Computersysteme, Datenbeschädigung und der betrügerische Missbrauch einer Datenverarbeitungsanlage. Viele Meldungen betreffen Antragsdelikte und bedürfen daher einer Strafanzeige durch die betroffene Person. In diesen Fällen verweist KOBIK die Melder an die lokal zuständige Polizeibehörde.

Zum ersten Mal seit Bestehen von KOBIK im Jahr 2003 betrafen die meisten Meldungen strafbare Handlungen gegen das Vermögen (Art. 137-172ter StGB). Bereits in den letzten Jahren nahmen Meldungen dieser Kategorie stetig zu. Konstant hoch blieb die Anzahl Meldungen zu strafbaren Handlungen gegen die sexuelle Integrität (Art. 187-212 StGB).

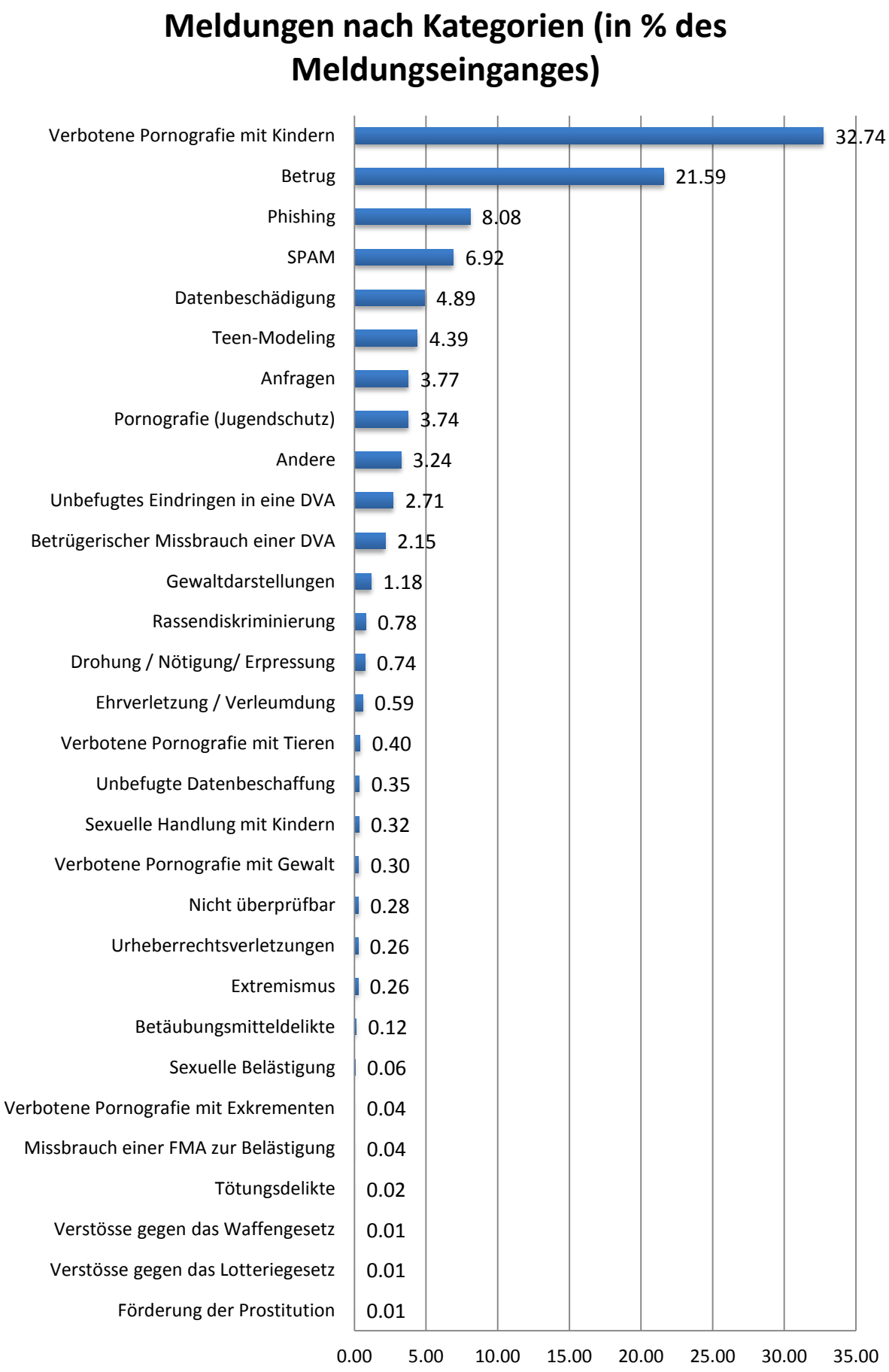


Abbildung 3 : Prozentualer Anteil der Kategorien am Meldungseingang 2012

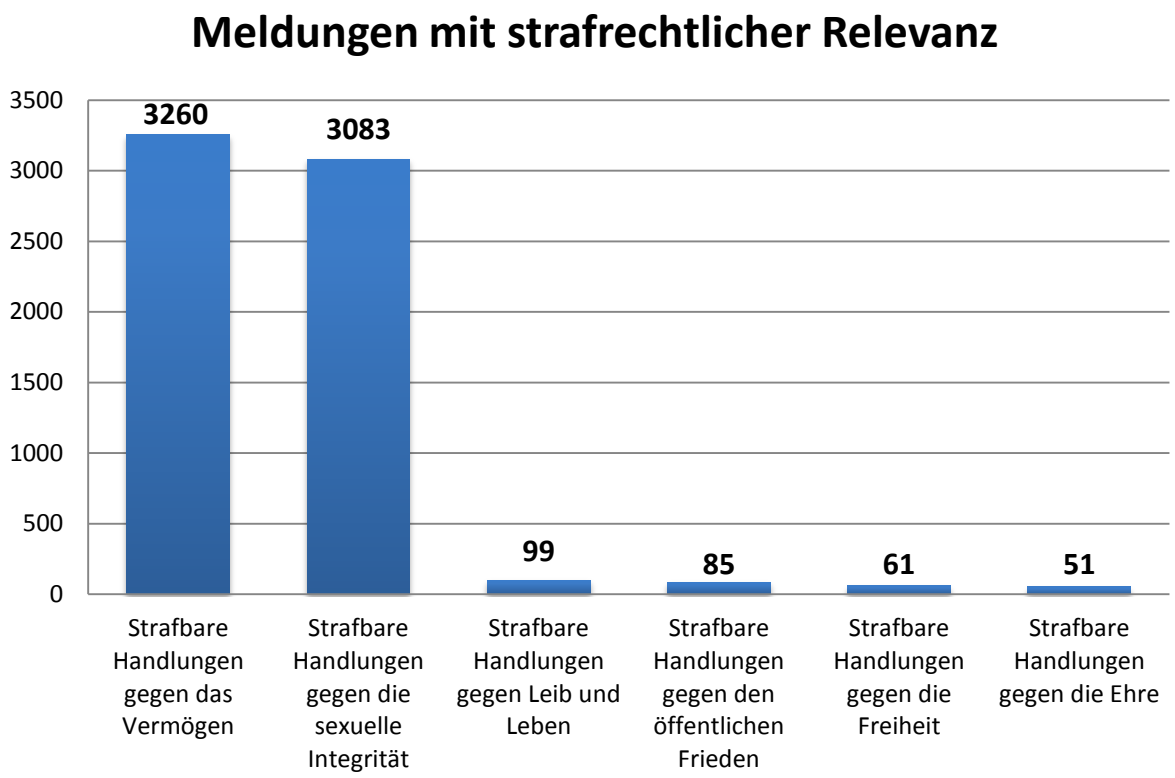


Abbildung 4: Meldungseingang 2012 nach strafrechtlicher Relevanz (Total 6‘639)

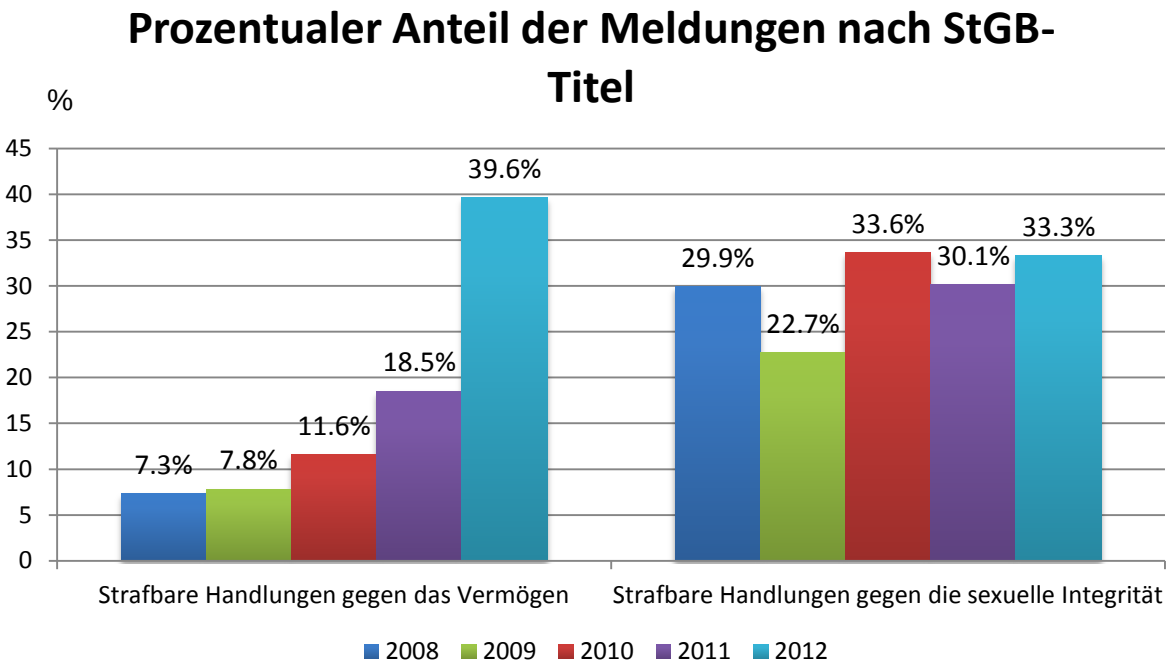


Abbildung 5: Prozentualer Anteil der Meldungen, 2008-2012

a) Strafbare Handlungen gegen das Vermögen

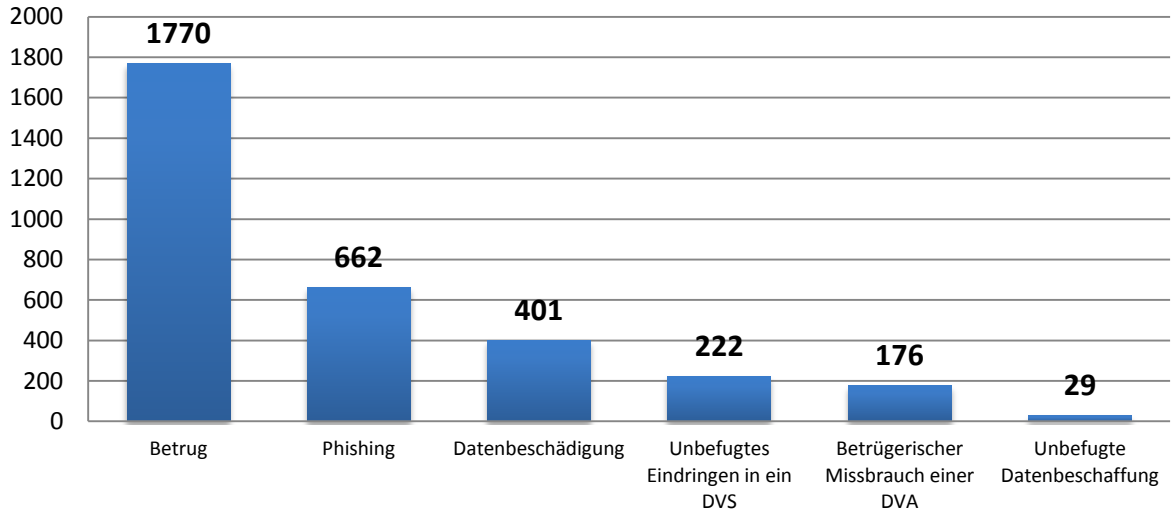


Abbildung 6: Meldungseingang zu strafbaren Handlungen gegen das Vermögen (Total 3260)

Mit insgesamt 1‘770 Meldungen steht der Bereich «Betrug» an der Spitze der strafbaren Handlungen gegen das Vermögen. Ein Grossteil der Meldungen betrifft betrügerische Angebote auf Kleinanzeigen- und Versteigerungsplattformen, bei denen den geschädigten Personen mittels einer Vorschusszahlung Geld abgeluchst wird, ohne die angepriesenen Waren/Dienstleistungen im Anschluss auch zu liefern. Zusätzlich werden zunehmend Vorfälle gemeldet, bei denen sich eine Täterschaft mit angeblichem Sitz im Ausland auf eine Anzeige hin meldet. Nach dem Zustandekommen des Geschäfts werden anfallende Gebühren und Zölle für die Finanztransaktion vom Geschädigten eingefordert. Später stellt sich heraus, dass die Betrüger ihrer Verpflichtung gar nie nachkommen wollten und es lediglich auf die erfundenen Gebühren und Zölle abgesehen haben. Besonders Immobilienplattformen sind von dieser Betrugsform betroffen.

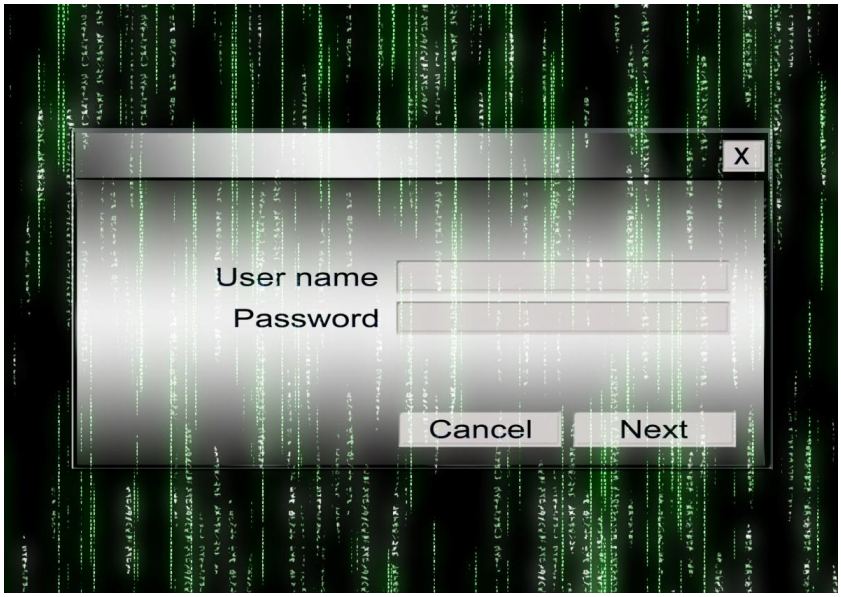
Der klassische Vorschussbetrug, bei welchem den Geschädigten gegen Anzahlung eines kleinen Vorschusses grosse Gewinne versprochen werden, wurde auch dieses Jahr häufig gemeldet. Diese Form des Betruges wird in der Regel mit Hilfe des Massenversandes von E-Mails praktiziert (Spam).

Erstmals wurden in diesem Jahr Meldungen zu Phishing-Versuchen getrennt von der Kategorie **«Spam»** erfasst, da sich der Fokus der Meldungen betreffend «Spam» von unerwünschten Werbe-E-Mails auf **«Phishing-Versuche»** verlagert hat. Nur noch 7% waren demnach Meldungen zu unerwünschten Werbemails. Insgesamt 8% der eingegangen Meldungen waren Hinweise zu Versuchen, an sensible Daten von Kunden zu gelangen. Dies geschah in der Regel mittels gefälschten E-Mails oder Telefonaten. Gefragte Daten sind beispielsweise Kreditkartennummern, Bankkontonummern, Zugangsdaten zu E-Mail-Accounts und E-Banking-Informationen. Zusammengefasst weisen die beiden Kategorien mit 15% der eingegangenen Meldungen einen gleich grossen Anteil aus wie letztes Jahr die Kategorie «Spam» gesamthaft. Daraus lässt sich keine tatsächliche Abnahme der Spam-E-Mails herleiten, da der Meldungseingang nicht zwangsläufig die effektive Situation widerspiegelt. Vielmehr spielen hier Gewöhnungseffekte der Computerbenutzer an massenhaft versandten Werbebotschaften und eine verbesserte Spam-Filterungstechnologie eine entscheidende Rolle, was sich nicht zuletzt auch darauf auswirkt ob Spam E-Mails bei KOBIK gemeldet werden oder nicht.

Gemeldete Delikte im Bereich der **Internetkriminalität im engeren Sinne** stiegen im prozentualen Vergleich zum Vorjahr weiter an. In diesen Bereich fallen die Tatbestände «Unbefugtes Eindringen in ein Datenverarbeitungssystem», «Datenbeschädigung» und «Betrügerischer Missbrauch einer Datenverarbeitungsanlage» (Vergleich Abb. 3).

Zahlreiche Privatpersonen meldeten im Zusammenhang mit „unbefugtem Eindringen in ein Datenverarbeitungssystem“, dass Ihre E-Mail-Accounts von Betrügern übernommen und die Kontaktpersonen im Adressbuch des Mailkontos der Geschädigten zur Zahlung eines Betrages aufgefordert wurden. Im Schreiben der Betrüger bittet der vermeintliche Accountbesitzer um finanzielle Unterstützung, da sich dieser angeblich auf einer Auslandreise und in finanzieller Not befände.

Ein weiteres Beispiel für **«Unbefugtes Eindringen in ein Datenverarbeitungssystem»** ist das Eindringen in Webseiten von Firmen und Vereinen mit dem Ziel, an sensible Daten der jeweiligen Unternehmen und Benutzer der Webseiten zu gelangen. Die so gestohlenen Daten können E-Mail-Adressen, Passwörter für Online-Accounts, Kreditkartennummern etc. sein, welche in entsprechenden Märkten von den Tätern weiterverkauft werden. Einhergehend mit dem Datendiebstahl ist meist auch eine Verunstaltung der Webseite bis hin zum kompletten Löschen von Datenbanken und Seiteninhalten.



Bildquelle: Gerd Altmann /Pixelio

Zusätzlich gingen bei KOBIK Meldungen von angedrohten und durchgeführten **Distributed-Denial-of-Service-Attacken** (DDoS) gegen Betreiber von Online-Webshops ein. Die Täter drohten via E-Mail, bei Nichtbezahlen des geforderten Lösegeldes, die Seiten von Online-Shops mit einer überdurchschnittlich grossen Zahl von Anfragen für mehrere Stunden lahmzulegen.

Speziell zu erwähnen sind Meldungen in Zusammenhang mit einer bösartigen Software, die den Computer des Betroffenen sperrt und im Namen des Bundesamtes für Polizei oder der Urheberrechtsgesellschaft SUISA eine Geldstrafe im Bereich von hundert Franken für das angebliche Herunterladen verbotener Inhalte fordert. Eine Freischaltung sei nur bei Bezahlung möglich und bei Nichtbezahlung wird ein Strafverfahren angedroht.

b) Strafbare Handlungen gegen die sexuelle Integrität

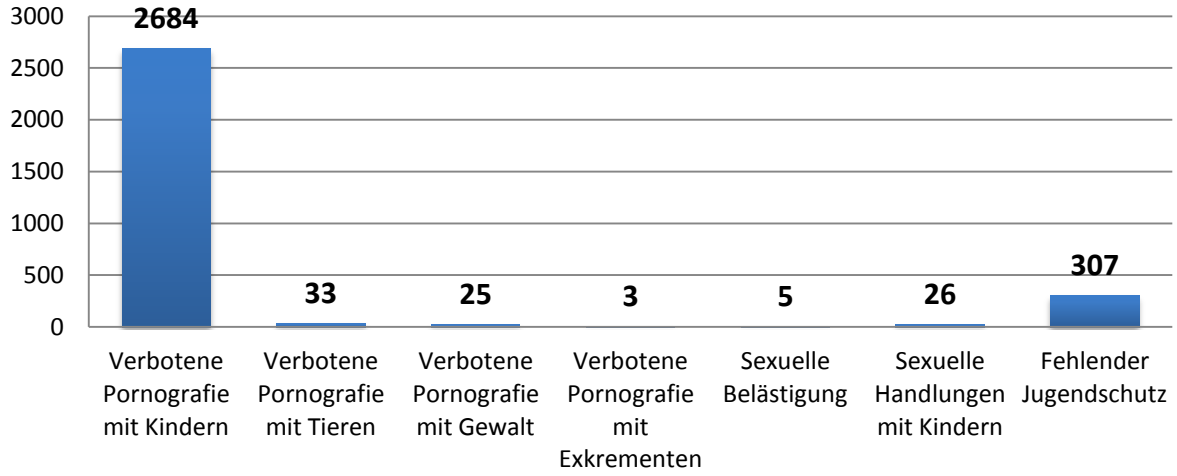


Abbildung 7: Meldungseingang zu strafbaren Handlungen gegen die sexuelle Integrität (Total: 3083)

Der prozentuale Anteil der Meldungen im Bereich der «**Strafbaren Handlungen gegen die sexuelle Integrität**» ist im Berichtsjahr wieder leicht angestiegen. Der Grossteil der Meldungen betraf den Vertrieb von verbotener Pornografie mit Kindern über Webseiten. Zusätzlich wurde KOBIK in 307 Fällen auf Seiten mit pornografischen Inhalten aufmerksam gemacht, deren Jugendschutz nach Ansicht des Meldungserstellers ungenügend war. Erstmals sind 2012 im Vergleich aber insgesamt weniger Meldungen dieser Kategorie eingegangen als zur Kategorie der «Strafbaren Handlungen gegen das Vermögen».

Bildquelle: S. Hofschlaeger /Pixelio

c) Weitere strafbaren Handlungen

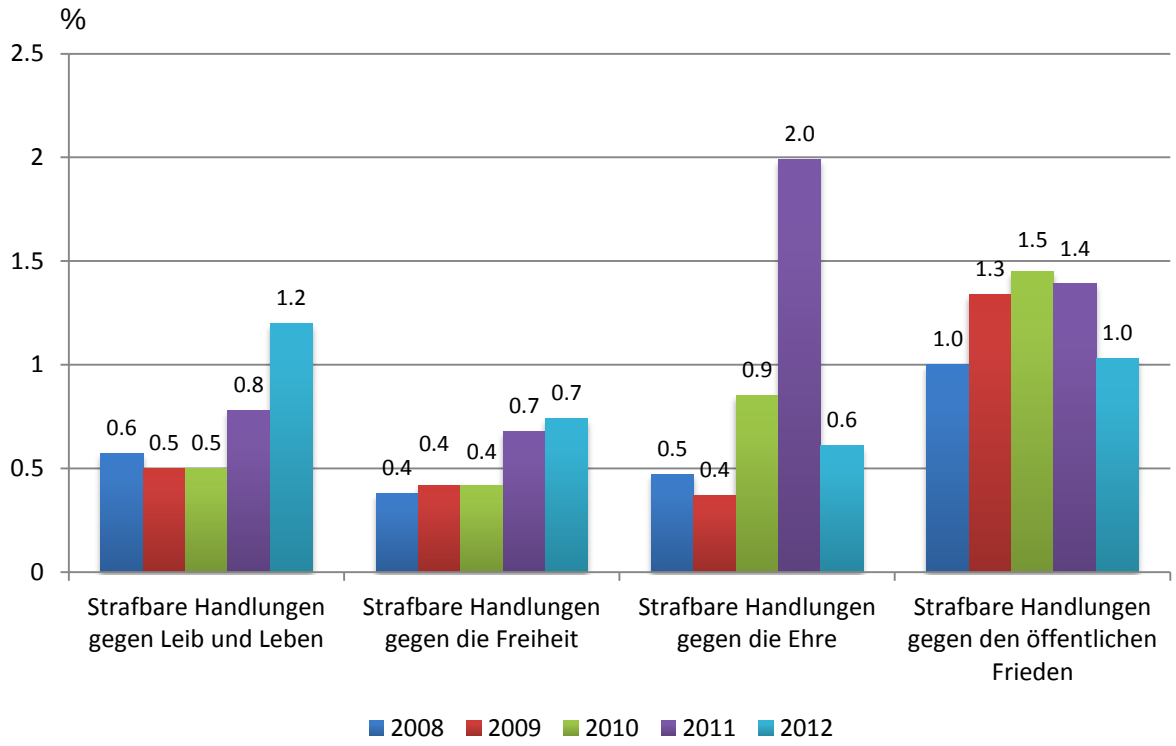


Abbildung 8: Meldungseingang 2008-2012 zu weiteren StGB-Titeln (prozentualer Anteil aller Meldungen)

Wie jedes Jahr gingen über das Meldeformular auch Meldungen zu anderen Straftaten bei KOBIK ein. Die markante Zunahme der «Strafbaren Handlungen gegen die Ehre» im 2011 bestätigte sich im Berichtsjahr nicht und stellt daher keinen erkennbaren Trend dar. Gründe für den Meldungsrückgang könnten in einem bewussteren Umgang mit Social Media aufgrund der vermehrten Mediatisierung von **«Cyberbullying»-Fällen,** liegen.

d) Zusammenfassung

Zwei Tendenzen werden beobachtet:

Zum Ersten ist die Anzahl der Meldungen zu **strafbaren Handlungen gegen das Vermögen (Wirtschaftsdelikte)**, allen voran Betrugs- und Phishing-Versuche, in den letzten Jahren stetig angestiegen, gefolgt von betrügerischem Missbrauch von Datenverarbeitungsanlagen mit dem Ziel, an sensible Daten zu gelangen oder Zahlungen zu erschleichen.

Als Zweites ist festzuhalten, dass die Anzahl Meldungen zu **strafbaren Handlungen gegen die sexuelle Integrität** auch 2012 hoch ausfällt (3083 Meldungen gegenüber 2150 Meldungen im Vorjahr). Prozentual gesehen wurde die Anzahl der gemeldeten Delikte in diesem Bereich dennoch von der Anzahl der Delikte gegen das Vermögen überholt (vgl. Abb. 5).

2.3 Produkte

Aufgrund der Meldungen, die KOBIK über das Online-Meldeformular erreichten, wurden diverse Arbeiten ausgeführt und Massnahmen getroffen. Anbei ein Überblick über die wichtigsten Kennzahlen und Informationen:

- Alle 8‘242 eingegangen Meldungen wurden zeitgerecht auf eine allfällige strafrechtliche Relevanz und die örtliche Zuständigkeit überprüft.

- Von den 8‘242 Meldungen wurden über 2‘200 in Form von individuellen Bürgerantworten erledigt.

- 38 Meldungen führten direkt und aufgrund der strafrechtlichen Relevanz zur Übermittlung eines Verdachtsdossiers an den zuständigen Kanton oder die zuständige Behörde.

- 345 Meldungen in Zusammenhang mit strafrechtlich relevanten Internetseiten wurden an ausländische Strafverfolgungsbehörden (via Interpol/Europol) oder Organisationen mit verwandten Aufgaben (wie z.B. In Hope) übermittelt.

- Hunderte von Meldungen gingen direkt an in- oder ausländische Internet Service Provider (z.B. Anträge um Löschung strafrechtlicher Inhalte und Anfragen für IP-Auskünfte).

- Etliche Meldungen führten zu fedpol-internen Hinweisen an die Kommissariate Allgemeine-, Organisierte- und Finanzkriminalität, Pädokriminalität und Pornografie und Staatsschutz der Bundeskriminalpolizei (BKP).

2.4 Ausgewähltes Fallbeispiel

In mehreren Fällen wurde KOBIK 2012 auf Suizidankündigungen im Internet hingewiesen. In einem Fall informierte ein französisches IT-Unternehmen via Meldeformular über eine Suizidankündigung auf einem Game-Server. Dem firmeneigenen Abuse-Team fiel ein Benutzer auf, welcher im Chat eines beliebten Online-Spieles diverse Bemerkungen hinterliess, die auf Selbstmordabsichten schliessen liessen. Die IP-Adresse des Nutzers wies in die Schweiz, weshalb sich das Abuse-Team zu einer Meldung an KOBIK entschied. KOBIK veranlasste im Anschluss eine sofortige IP-Abklärung und konnte innert kürzester Zeit die Adresse des Internetanschlusses und damit auch die zuständige Kantonspolizei eruieren. Nach entsprechender Information durch KOBIK konnte die Kantonspolizei innerhalb weniger Stunden sowohl Eltern als auch Tochter – der Verfasserin der Suizidankündigung - identifizieren und persönlich sprechen. Wie sich herausstellte, waren die Befürchtungen nicht unbegründet und die Jugendliche erhielt die notwendige psychologische Unterstützung. Der Fall zeigt auf, wie wichtig eine koordinierte und zentralisierte, internationale Zusammenarbeit zwischen Strafverfolgung und Privatwirtschaft ist.

3. Aktive Recherchen durch KOBIK (Monitoring)

KOBIK nimmt nicht nur Meldungen aus der Bevölkerung entgegen. Mit verdachtsunabhängigen Recherchen im Internet ist KOBIK auch in weniger zugänglichen Bereichen des Internets 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 dieser auch für das Jahr 2012 auf die Bekämpfung der Pädokriminalität im Internet gesetzt. Der Leitungsausschuss hat jedoch ausdrücklich festgehalten, dass sich KOBIK den Wirtschaftsdelikten und der Internetkriminalität im engeren Sinn nicht verschliessen darf.

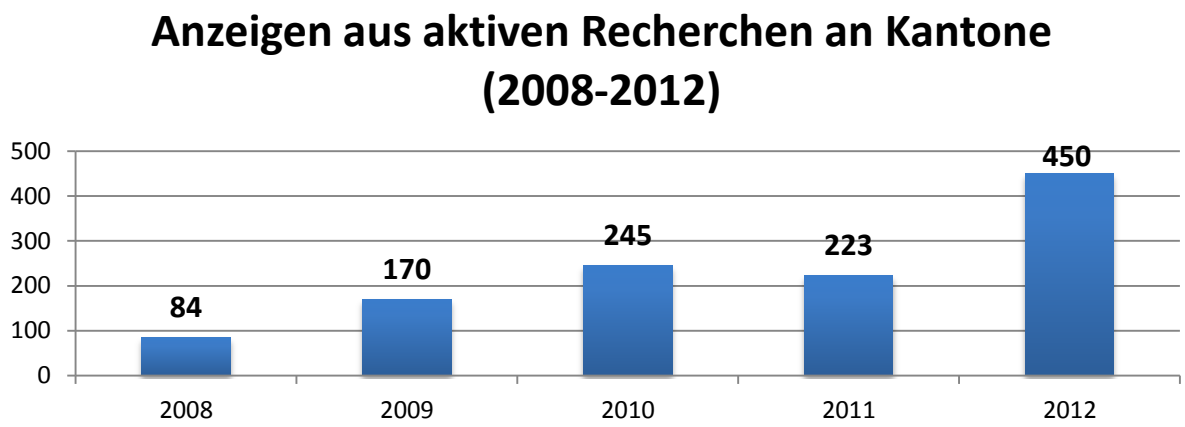


Abbildung 9: Im Rahmen aktiver Recherchen eröffnete Strafverfahren (2008-2012)

Aufgrund der aktiven Recherchen wurden 2012 insgesamt 450 Verdachtsdossiers erstellt. Dies entspricht einer Verdoppelung gegenüber dem Vorjahr.

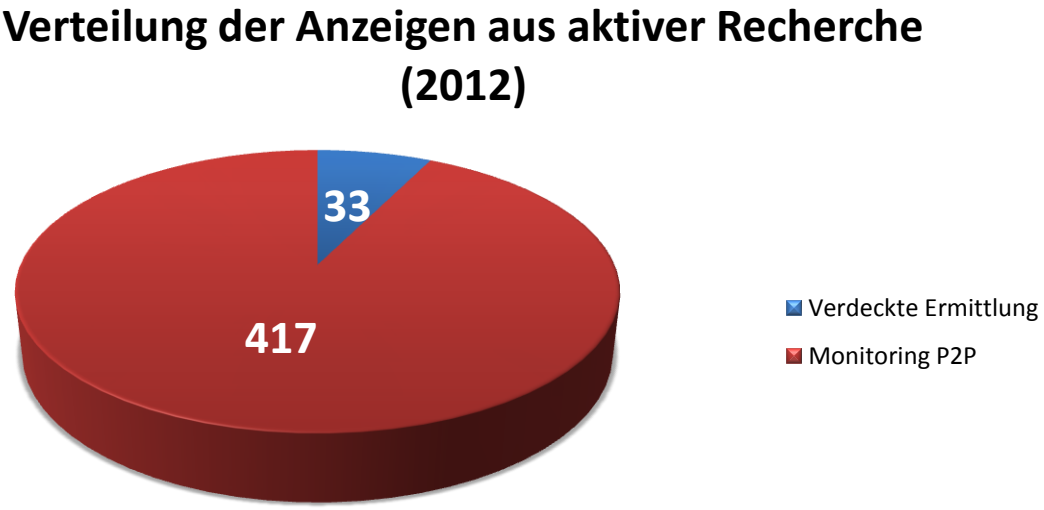


Abbildung 10: Herkunft der Strafanzeigen aus aktiver Recherche (Total 450)

3.1 Aktive Recherchen in Peer-to-Peer-Netzwerken (P2P)

417 von 450 Verdachtsdossiers resultierten aus der Überwachung von P2P-Netzwerken von Internetbenutzern, die in der Schweiz aktiv kinderpornografische Dateien austauschen. Im Vergleich zum Vorjahr stieg die Zahl der Verdachtsdossiers um 214, was einer Zunahme von 95% entspricht. P2P-Netzwerke sind nach wie vor ein beliebtes Mittel, um relativ anonym über das Internet illegale Daten auszutauschen. Dennoch ist die markante Zunahme der Verdachtsdossiers in erster Linie auf die Weiterentwicklung der eingesetzten Software und die Optimierung der KOBIK-internen Abläufe zurückzuführen.

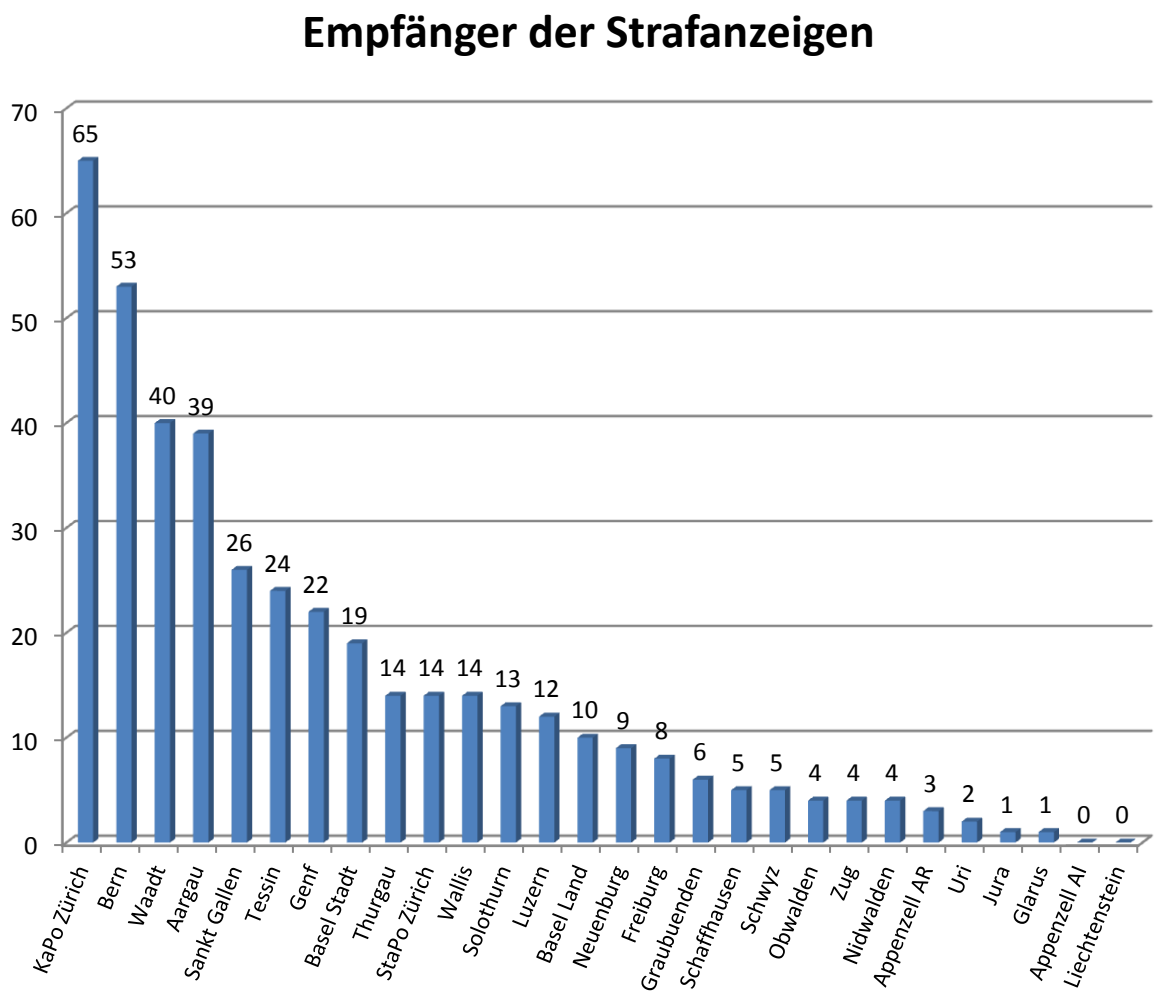


Abbildung 11: Aufteilung der Strafanzeigen nach kantonaler Zuständigkeit (Total 417)

Wie schon in den letzten Jahren wurden die meisten Verdachtsdossiers von KOBIK an die bevölkerungsstärksten Kantone (Zürich, Bern und Waadt) weitergeleitet (vgl. Abb. 11).

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

3.2 Verdachtsunabhängige verdeckte Vorermittlungen

Bildquelle: Alexander Klaus /Pixelio

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[1]. 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 neben den Kantonen weiterhin auch durch eine zentrale Stelle auf nationaler Ebene vorgenommen werden kann.

Verdeckte Vorermittlungen durch KOBIK führten 2012 in insgesamt 33 Fällen zu Strafanzeigen zuhanden der zuständigen Kantone. Davon basieren 13 Strafanzeigen auf Ermittlungen in Schweizer Kinderchats. Sämtliche dieser 13 Anzeigen lauteten auf versuchte sexuelle Handlungen mit Kindern und/oder betreffen das Versenden von Pornografie an Minderjährige.

Bei den verbleibenden 20 Fällen fanden die verdeckten Vorermittlungen in sogenannten „privaten P2P-Tauschbörsen“ statt. Im Gegensatz zu den klassischen P2P-Netzwerken werden die Daten nicht mehr in einem öffentlichen Raum ausgetauscht. Der Austausch findet direkt zwischen zwei Computern statt, weshalb die Bestimmungen der verdeckten Vorermittlung Anwendung finden. Das private P2P-Umfeld konnte von der Schweizer Strafverfolgung bislang kaum abgedeckt werden, da die Ermittlungen sehr personal- und zeitintensiv sind. Da bereits zahlreiche der 20 Tatverdächtigen als Wiederholungstäter im Bereich der verbotenen Pornografie oder gar als Täter von Sexualdelikten polizeilich bekannt sind, sieht sich KOBIK im Entscheid zur Ausweitung der verdeckten Vorermittlungen auf private P2P-Tauschbörsen bestätigt.

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

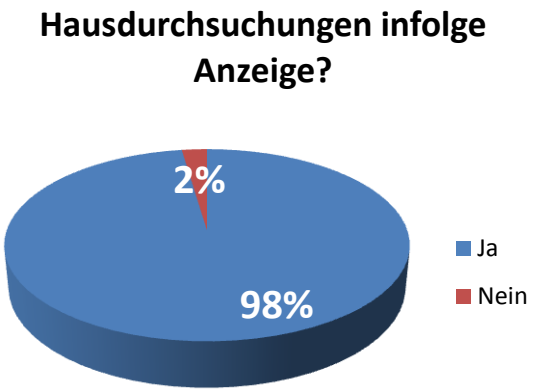
3.3 Feedback aus den Kantonen

Bildquelle: Thorben Wengert /Pixelio

KOBIK leitet Fälle bei begründetem Verdacht auf eine Straftat zur Bearbeitung zuständigkeitshalber an die Kantone weiter (vgl. Abb.11). Um eine Gesamtübersicht über die in den Kantonen eingeleiteten Aktivitäten zu gewinnen, ersucht KOBIK die Kantone um Information über den weiteren Verlauf der ihnen gemeldeten Verdachtsfälle (eingeleitete polizeilichen Massnahmen und/oder Ausgang des Gerichtsverfahrens.)

Die Analyse dieser Rückmeldungen ist ein wichtiges Mittel zur Prüfung der Effizienz der Tätigkeit und der Qualität der erstellten Verdachtsdossiers und Anzeigen zuhanden der Kantone. Die Aussagen der vergangenen Jahre bezogen sich jeweils auf die Gesamtheit der seit 2003 erhaltenen Rückmeldungen. Damit zeitnahe Entwicklungen besser erkannt werden können, wurden nachfolgend lediglich die im Berichtsjahr eingegangenen Rückmeldungen aus den Kantonen berücksichtigt. Durch diese Prozessoptimierung lassen sich auch die Unterschiede zu den Vorjahren erklären.

Die grosse Mehrheit der Verdachtsdossiers resultiert aus den aktiven Recherchen in P2P-Netzwerken (417). Die Dossiers betreffen somit Personen, die sich aktiv am Austausch von strafbaren Inhalten mit kinderpornografischem Charakter beteiligten.



Abbildungen 12: Hausdurchsuchungen 2012

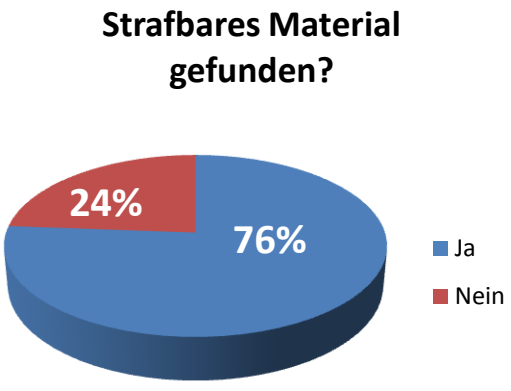


Abbildung 13: Strafbares Material 2012

Wie aus obigen Abbildungen hervorgeht, führten 98% aller weitergeleiteten KOBIK-Fälle zu Hausdurchsuchungen durch kantonale Polizeibehörden.

a) Rückmeldungen der kantonalen Polizeibehörden

Bei 76% der Hausdurchsuchungen, die aufgrund der Verdachtsmeldungen durchgeführt wurden, konnte einschlägiges illegales Material beschlagnahmt werden. Die Gründe für eine erfolglose Hausdurchsuchung sind nicht immer leicht zu eruieren. In der Regel verunmöglichen offene und ungeschützte Drahtlosnetzwerke oder die Auslagerung der Daten auf Cloud-Dienste 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.

Bei den sichergestellten strafbaren Inhalten handelte es sich bei 97% um Kinderpornografisches Material. 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 jedoch, dass in mehr als der Hälfte der Fälle zudem Vergehen gegen weitere Tatbestände der verbotenen Pornografie (Art. 197 StGB) festgestellt wurden (vgl. Abb. 14). So wurde bei jeder zweiten Hausdurchsuchung zusätzlich auch noch Pornografie mit Tieren sichergestellt.

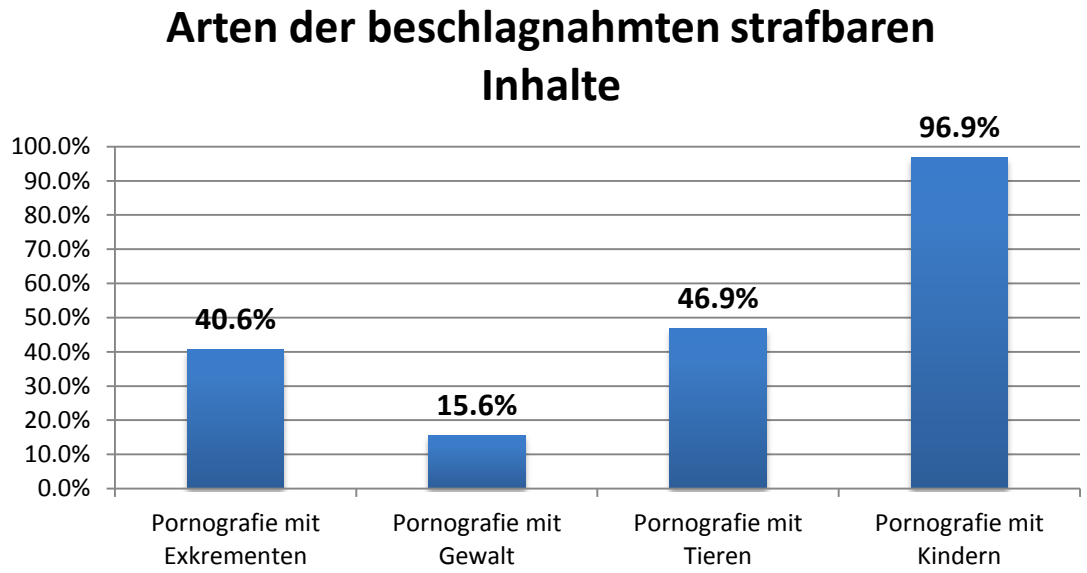
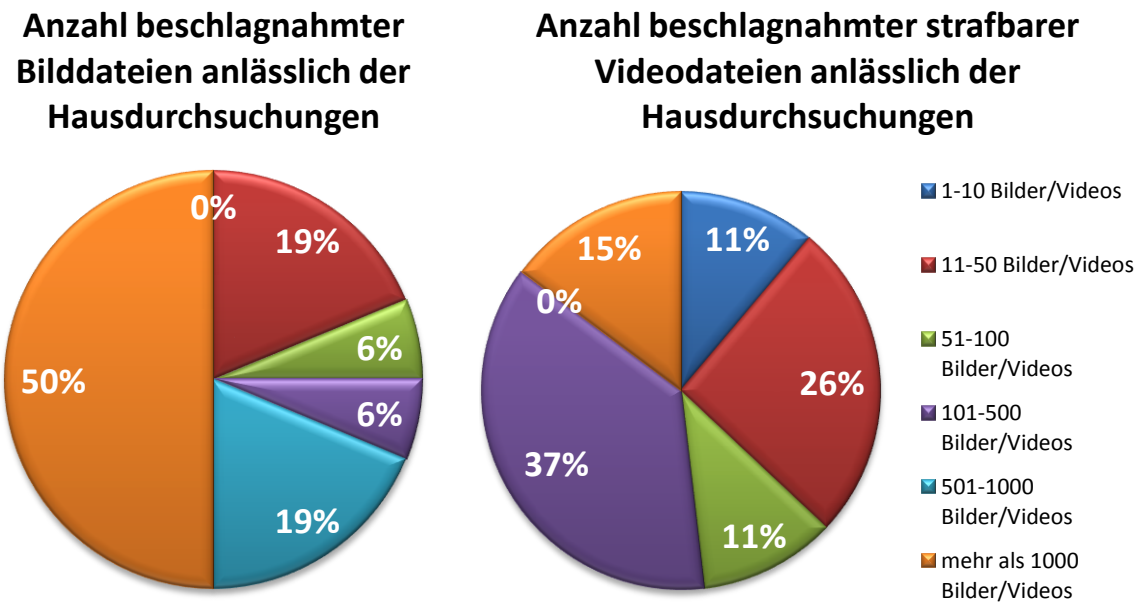


Abbildung 14: Welche Arten von Material wurden 2012 beschlagnahmt?

Aus den Rückmeldungen der kantonalen Polizeibehörden geht weiter hervor, dass bei 94% der erfolgreichen Hausdurchsuchungen Videodateien und in 66% der Fälle Bilddateien beschlagnahmt wurden. In zahlreichen Fällen wurde belastendes Material beider Kategorien vorgefunden und beschlagnahmt. Insgesamt führten die Hausdurchsuchungen zu Sicherstellungen von mehreren Millionen strafbaren Bild- und Videodateien.



Abbildungen 15 und 16: Überblick über die Menge beschlagnahmter Bild- und Videodateien

b) Rückmeldungen der kantonalen Justizbehörden

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

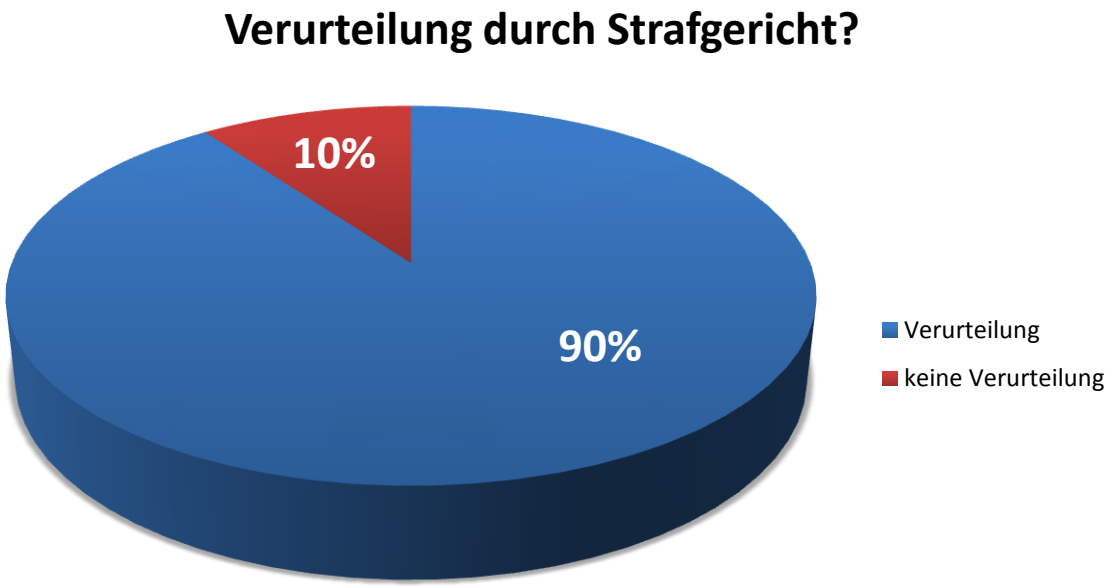


Abbildung 17: Verurteilung durch Strafgericht, 2012

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 beschriebenen Tatbestände.

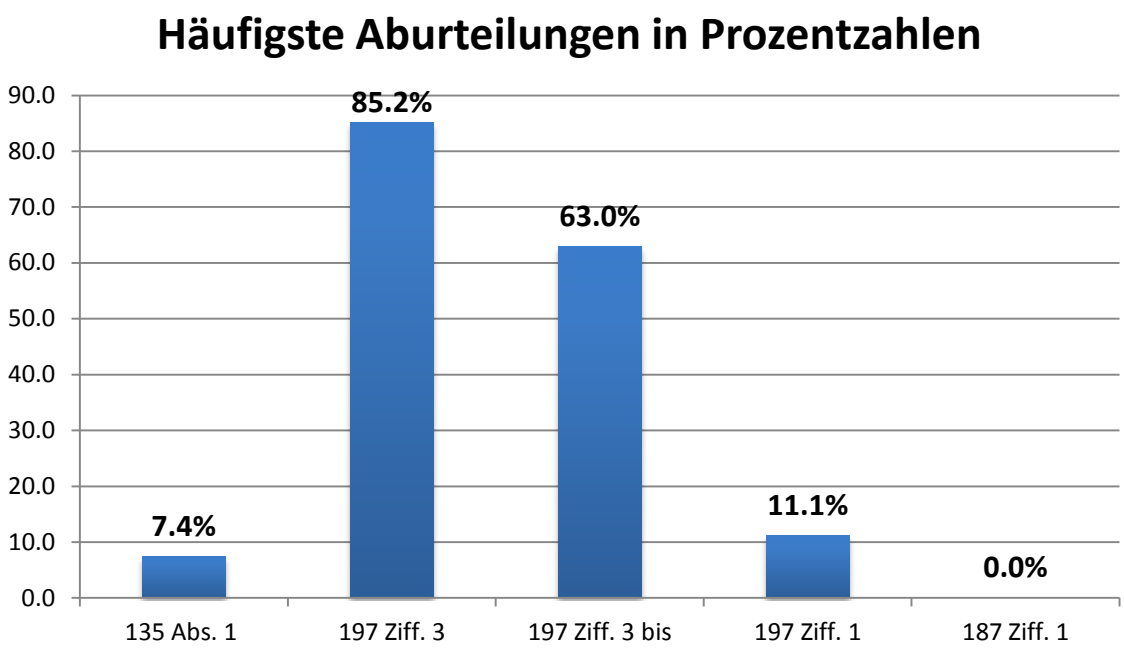
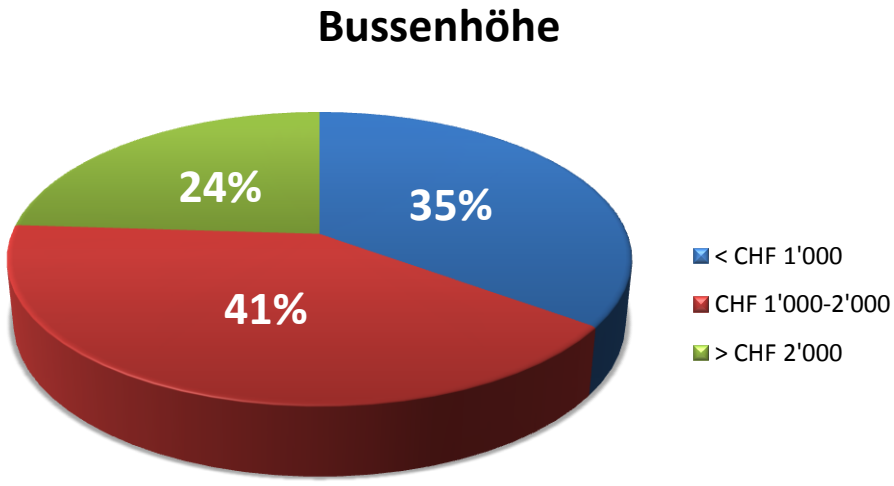


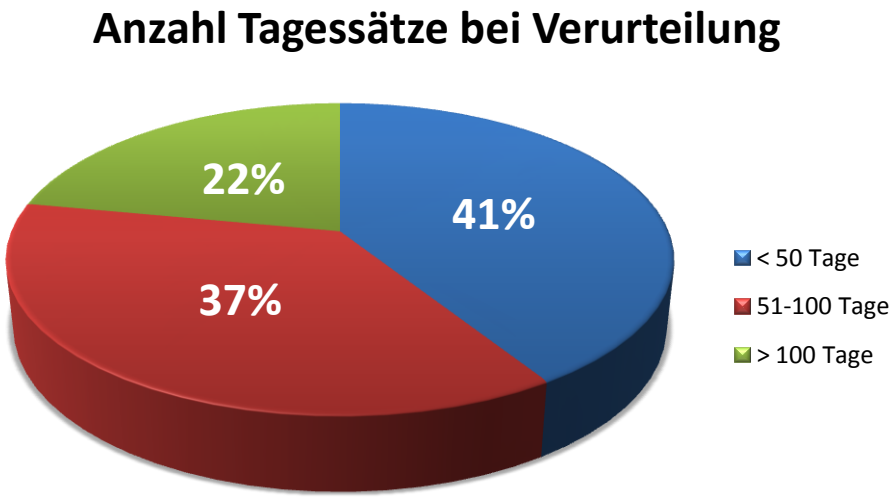
Abbildung 18: Häufigste Aburteilungen in Prozentzahlen, 2012

Bei sämtlichen im Berichtsjahr gemeldeten Verurteilungen wurde eine **Geldstrafe (Tagessatz)** ausgesprochen. In 63% dieser Fälle wurde gleichzeitig eine **Busse** verhängt. Die Geldstrafen wurden bei **96% der Verurteilungen auf Bewährung** ausgesetzt. Gemeinnützige Arbeit, Therapien, Freiheitsentzug (Gefängnis) und nicht auf Bewährung ausgesetzte Geldstrafen wurden nicht verhängt. Diese Entwicklung zeichnete sich bereits in den letzten Jahren ab.

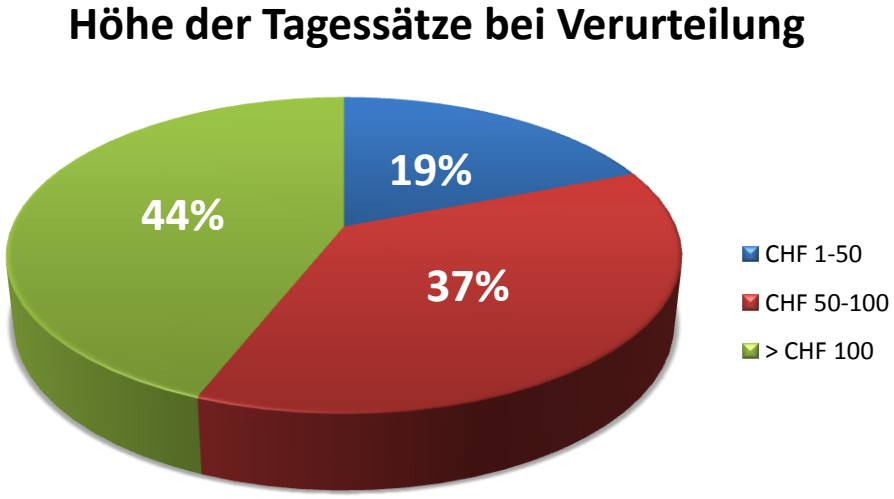


In etwa 35% der Fälle beliefen sich die Bussen auf weniger als tausend Franken; in 41% auf 1'000 bis 2'000 Franken. Lediglich 24% der Bussen waren höher als 2'000 Franken.

41% der Geldstrafen wurden bei 50 oder weniger Tagessätzen festgelegt; bei 37% wurden jeweils zwischen 51 und 100 Tagessätze angeordnet. Über 100 Tagessätze wurden nur in 22% der Fälle gesprochen.



In 19 % der Fälle wurden Tagessätze in der Höhe von 1 bis 50 Franken, in 37 % der Fälle zwischen 51 und 100 Franken und in 44% über 100 Franken festgesetzt.



In der Regel mussten die Verurteilten zusätzlich die Verfahrenskosten tragen, welche die eigentliche Busse oftmals um ein Vielfaches überstiegen.

3.4 Ausgewähltes Fallbeispiel

Fallbeispiel aus dem Bereich der verdachtsunabhängigen Vorermittlungen in P2P-Netzwerken: Die gestützt auf das KOBIK-Verdachtsdossier durchgeführten Ermittlungen durch die zuständige Kantonspolizei zeigten auf, dass sich der Tatverdächtige zweimal ins Ausland begeben hatte, wo er sich an mehreren Kindern vor laufender Kamera verging. Anschliessend stellte der Tatverdächtige die Bilder ins Internet. Weiter ergaben die Ermittlungen, dass der Tatverdächtige auch sein eigenes dreijähriges Kind missbrauchte.

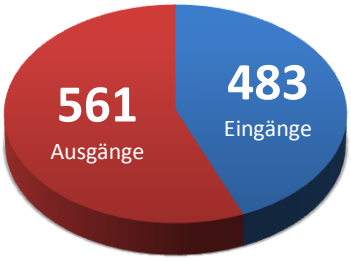
Der Täter war bis zum Zeitpunkt der Verdachtsmeldung von KOBIK polizeilich nicht verzeichnet. Dank der professionellen Zusammenarbeit zwischen KOBIK und der zuständigen Kantonspolizei sowie der anschliessenden intensiven Ermittlungsarbeit durch die Polizei konnte der Täter überführt und sein Kind wie möglicherweise auch weitere andere Kinder vor weiterem Missbrauch geschützt werden.

Dieser Fall zeigt exemplarisch auf, wie wichtig eine systematische Fallbearbeitung der P2P-Verdachtsdossiers durch die kantonalen Behörden ist. Aufgrund der knappen Ressourcen sind einige Kantone bei der Bearbeitung der zahlenmässig massiv angestiegenen KOBIK-Dossiers stark gefordert. Es ist zum Teil eine grosse Herausforderung den enormen zusätzlichen Arbeitsaufwand zeitgerecht bewältigen zu können.

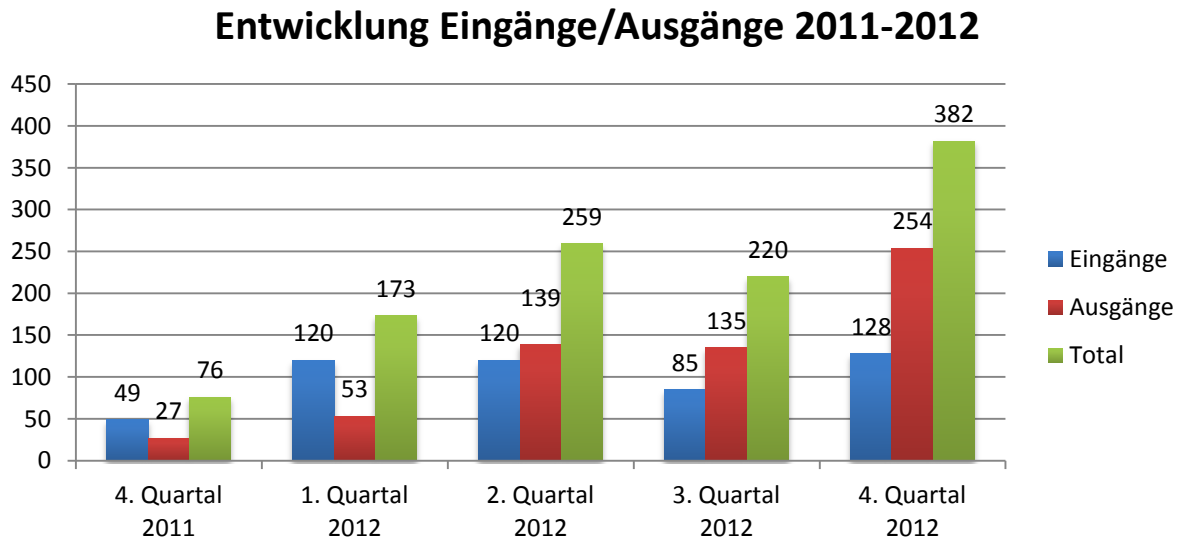
4. Kriminalpolizeilicher Informationsaustausch

Seit Inkrafttreten des Übereinkommens über die Internetkriminalität des Europarates (Cybercrime Convention, CCC) am 1. Januar 2012, wird die Schweiz international verstärkt als aktiver Partner in der Bekämpfung der Internetkriminalität wahrgenommen. Dies zeigt sich vor allem im markanten Anstieg des kriminalpolizeilichen Informationsaustausches mit ausländischen Behörden zu Sachverhalten, die unter den Anwendungsbereich des Übereinkommens fallen. Eine Rolle spielt hier auch der Entscheid des Leitungsausschusses KOBIK, wonach sich KOBIK der Internetkriminalität im engeren Sinn und der damit verbundenen Wirtschaftskriminalität nicht verschliessen darf. Ein weiterer Grund ist die Überführung von KOBIK in den polizeilichen Bereich von fedpol. Mit der Einbettung von KOBIK in die Bundeskriminalpolizei 2009 haben der kriminalpolizeiliche Informationsaustausch sowie die Koordinationstätigkeit an Bedeutung gewonnen. Die nachfolgenden Zahlen zeigen dies deutlich auf.

Kriminalpolizeilicher Informationsaustausch mit ausländischen Behörden 2012



Die statistische Erhebung zeigt, dass 2012 insgesamt 483 Meldungen zum Anwendungsbereich des Übereinkommens eingegangen sind. Allein im 4. Quartal 2012 erhielt KOBIK 128 Meldungen aus dem Ausland. Das entspricht einem Anstieg von über 161% gegenüber dem Vorjahr (4. Quartal 2011: 49 Meldungen). Gleich verhält es sich bei den Ausgängen, die KOBIK an ausländische Strafverfolgungsbehörden verfasste und die in einer direkten Korrelation mit dem angestiegenen Meldungseingang stehen. Im Berichtsjahr verfasste KOBIK insgesamt 561 Meldungen ans Ausland (Interpol und Europol). Vergleicht man die Meldungen des 4. Quartals 2012 (254 Meldungen) mit dem Vorjahr (27 Meldungen), ergibt sich eine beachtliche Zunahme an verfassten Meldungen.



4.1 Ausgewählte Fallbeispiele

Zwei Fälle als Beispiel für den raschen und erfolgreichen kriminalpolizeilichen Informationsaustausch gemäss Übereinkommen über die Internetkriminalität des Europarates (Cybercrime Convention, CCC) :

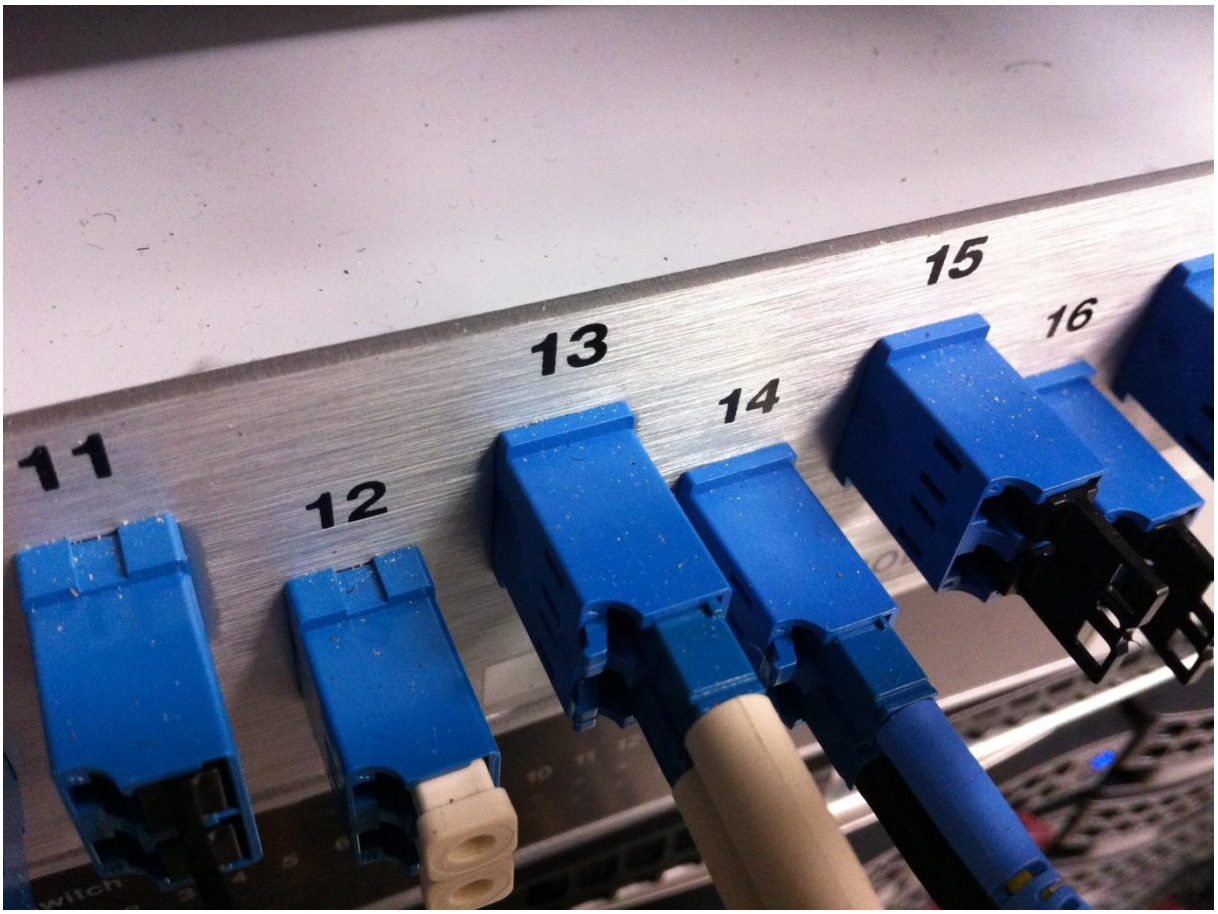
Von einer Interpolstelle ging bei KOBIK die Meldung ein, wonach Mitglieder politischer Parteien des anfragenden Landes per E-Mail gegen Leib und Leben bedroht wurden. Die Angaben zum Absender der Drohmails mit Verbindung in die Schweiz wurden an KOBIK gemeldet. Dank der bereits definierten Prozessabläufe von KOBIK mit dem entsprechenden Provider konnten innerhalb 24 Stunden sämtliche Daten vorabgesichert sowie ergänzende Angaben zur Identifikation des Anschlussinhabers erhältlich gemacht und die zuständige Kantonspolizei informiert werden. Die Interpolstelle wurde umgehend mit allen Angaben bedient, die in ein mögliches Rechtshilfeersuchen einfliessen konnten.

In einem zweiten Fall wurde KOBIK von einer ausländischen Interpolstelle über erpresserische E-Mails mit identischem Inhalt und Absender informiert. Die Verfasser der Schreiben forderten eine beachtliche Geldsumme und drohten einem international tätigen Grossverteiler bei Nichtbezahlung mit Bombenanschlägen in Filialen. Eine der E-Mails hatte den Absender eines Schweizer Mail-Accounts und war persönlich an den Direktor einer Filiale des Grossverteilers gerichtet. KOBIK veranlasste beim zuständigen Polizeikommando umgehend die Sicherung der relevanten Daten beim Schweizer Provider. Dadurch wurden die Ermittlungen der ersuchenden Interpolstelle bei der Identifikation der mutmasslichen Täterschaft wesentlich und schnell unterstützt.

5. Projekte

5.1 Nationale Datei- und Hashwertesammlung (NDHS)

Das Projekt sieht vor, dass Dateien (Bilder und Videos), die im Rahmen von Ermittlungen im Bereich Kinderpornografie sichergestellt werden, von den zuständigen kantonalen Behörden vorkategorisiert an KOBIK übermittelt werden. KOBIK berechnet von jeder Datei einen Hashwert[2] und speichert diesen in der Nationalen Datei- und Hashwertesammlung (NDHS) ab. Die Liste der Hashwerte wird den Kantonen anschliessend zur Verfügung gestellt. Die zuständigen kantonalen Behörden berechnen 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. Mit dem Vergleich dieser Hashwerte können umfangreiche Datenmengen auf Übereinstimmungen geprüft werden, ohne dass das strafrechtsrelevante Material (Rohdaten) visuell geprüft werden muss. So können Duplikate und bereits bekanntes Bild- und Videomaterial automatisiert identifiziert werden. Dies bringt den Ermittlern eine grosse zeitliche und nicht zuletzt psychische Entlastung.



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

Die Nationale Datei- und Hashwertesammlung (NDHS) wurde unter der Leitung von KOBIK und der Mitwirkung kantonaler Polizeibehörden konzipiert und erarbeitet. Erstmals wurden allgemeingültige Anforderungen an eine NDHS eruiert und definiert (z.B. die einheitliche Kategorisierung).

Im Zentrum der softwaretechnischen Realisierung stand die Entwicklung einer leistungsfähigen Lösung für die Verarbeitung und den Abgleich grosser Datenmengen in Datenbanksystemen.

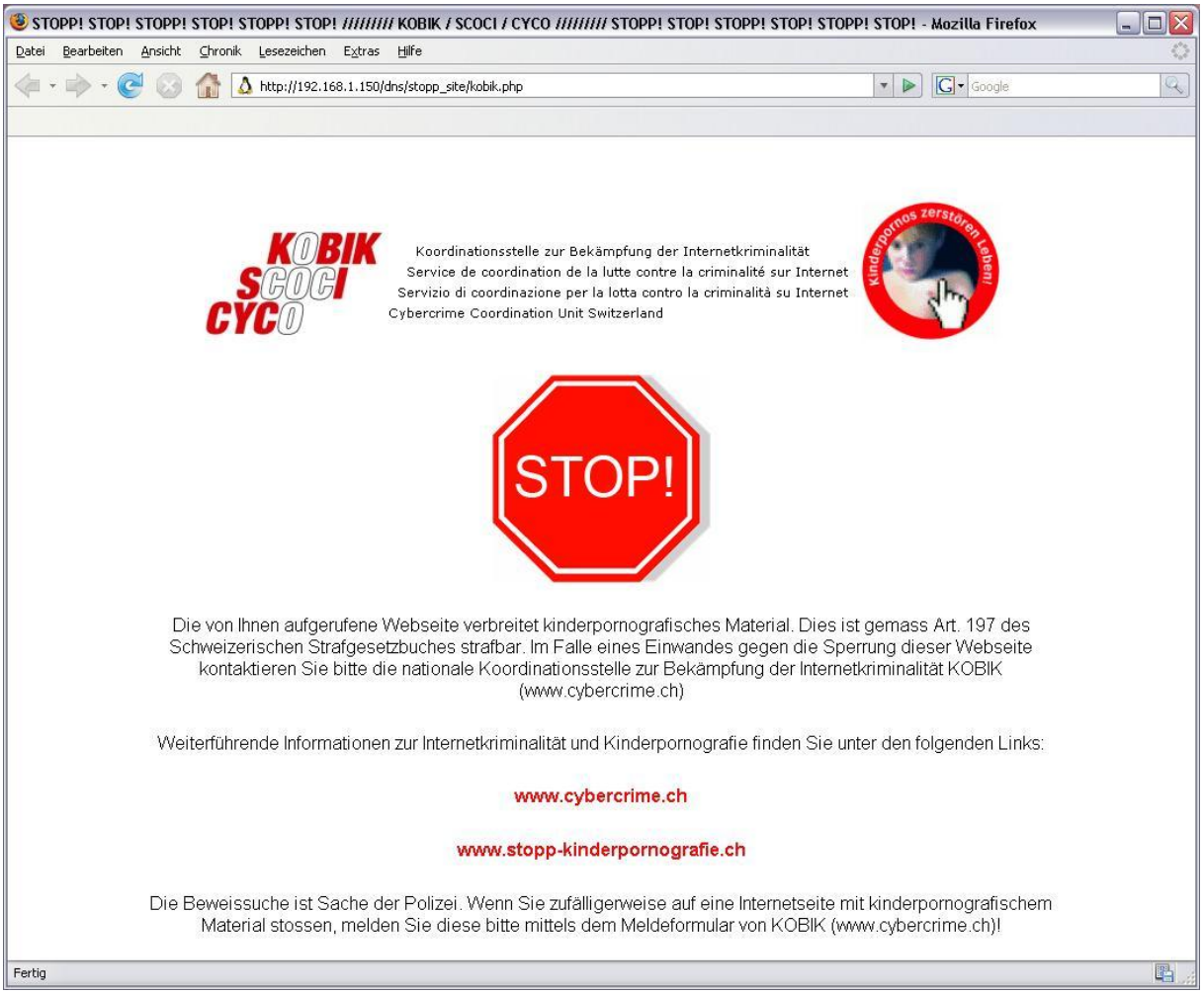
Das Jahr 2012 gilt als Meilenstein bei der Realisierung des Pilotprojektes der NDHS. Im Februar des Berichtsjahres wurde die für die NDHS benötigte Hardware aufgebaut. Zwischen April und Juli installierte KOBIK speziell konzipierte Software und führte erste Tests durch. Im Oktober konnten sämtliche noch ausstehenden Testarbeiten und Systemanpassungen erfolgreich abgeschlossen werden und die NDHS nahm ihren Betrieb auf. Die kantonalen und städtischen Fachstellen können KOBIK nun ihr vorkategorisiertes Bildmaterial zustellen, das durch KOBIK nach dem „Vieraugenprinzip“ definitiv kategorisiert und in die NDHS eingelesen werden kann.

5.2 Projekt zur Überwachung von Peer-to-Peer-Netzwerken

Im Rahmen des verdachtsunabhängigen Monitoring hat KOBIK in den letzten Jahren in Zusammenarbeit mit der NGO Action Innocence Genève (AG), das Überwachungsprogramm P2P-Scan entwickelt. Mit dieser Software kann der Austausch von kinderpornografischem Material in P2P-Netzwerken im Internet bekämpft werden. Dieses Programm wird in enger Zusammenarbeit mit Action Innocence Genève, welche die vollumfängliche Finanzierung übernimmt, laufend weiterentwickelt und anderen Strafverfolgungsbehörden zur Verfügung gestellt.

Mit diesem verdachtsunabhängigen Monitoring im Internet konnten in der Schweiz nicht nur reine „Konsumenten“ entdeckt und verhaftet werden, die durch ihr Verhalten die Produktion von immer neuem Material verursachen, sondern auch pädokriminelle „Täter“, die zum Teil selber Kleinkinder missbrauchten und dabei Bildmaterial produzierten.

5.3 Zusammenarbeit mit den Schweizerischen Internet Access Providern



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. KOBIK stellt den Internetanbietern eine laufend aktualisierte Liste von kinderpornografischen Internetseiten (ca. 200-300 Internetseiten) zur Verfügung. Die Internetanbieter sperren aufgrund ihrer Firmenethik und den AGBs[3] den Zugang zu strafrelevanten Seiten und leiten den Benutzer auf eine « Stopp-Seite » weiter.

Im Rahmen dieses Projektes arbeitet KOBIK eng mit Interpol zusammen. Interpol führt ebenfalls eine Liste von Internetseiten mit kinderpornografischen Bildern und Videos («worst of list»). Die in der Schweiz erstellte Liste basiert einerseits auf der Interpol-Liste und wird zusätzlich ergänzt durch eigene, selbsterkannte Internetseiten. Die «worst of list» wird täglich in die KOBIK-Liste integriert. KOBIK seinerseits meldet Interpol neue Internetseiten zur Ergänzung deren Liste.

[3] Allgemeine Geschäftsbedingungen (abgekürzt AGB)

6. Arbeitsgruppen, Partnerschaften und Kontakte

6.1 Nationale Arbeitsgruppen

KOBIK war im Berichtsjahr in verschiedenen nationalen Arbeitsgruppen vertreten.

So beteiligte sich KOBIK, zusammen mit dem Kommissariat Pädokriminalität /Pornografie der Bundeskriminalpolizei, gemeinnützigen Organisationen, Kantonsvertretern und der Schweizerischen Kriminalprävention weiterhin aktiv in der nationalen Arbeitsgruppe «Kindsmissbrauch».

Wie bereits im Vorjahr war KOBIK auch 2012 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.

Seit 2011 ist KOBIK als Vertreterin von fedpol auch in der Fachkommission der „Schweizerischen Kriminalprävention (SKP)“ vertreten. Die Kommission entwickelt Projekte und Materialien für die Kriminalprävention in den Kantonen und evaluiert deren Umsetzung.

Dank der Vertretung in den Arbeitsgruppen „IT-Ermittler“ und „Telekommunikationsüberwachung“ konnte KOBIK nicht zuletzt auch 2012 in die Bereichen der technischen Entwicklung und der effizienten Strafverfolgung erfolgreich mitgestalten und weiterentwickeln.

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.

Bildquelle: Gerd Altmann /Pixelio

6.2 Bundesinterne Zusammenarbeit

Auch im Berichtsjahr arbeitete KOBIK zur Bekämpfung der Internetkriminalität eng mit verschiedenen Bundesstellen zusammen. Innerhalb von fedpol stand vor allem die intensive Zusammenarbeit mit den Kommissariaten Pädokriminalität und Pornografie, IT-Ermittlungen, Staatsschutz und Verdeckte Ermittlungen der Bundeskriminalpolizei aber auch mit der Hauptabteilung Internationale Polizeikooperation (IPK) im Vordergrund. Aufgrund des gemeinsamen Aufgabengebietes besteht zwischen dem Kommissariat «Pädokriminalität/Pornografie» und KOBIK eine besonders intensive Zusammenarbeit. Weiter konnten diverse Kontakte mit departementsübergreifenden Bundesstellen ausgebaut und intensiviert werden. Zu erwähnen sind 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), das Bundesamt für Kommunikation (BAKOM) und die Eidgenössische Kommission gegen Rassismus (EKR).

Mit der Bundesanwaltschaft konnten wichtige gemeinsame Prozesse diskutiert und die Zusammenarbeit optimiert werden. Konkretes Ergebnis ist der Entscheid der Bundeskriminalpolizei, KOBIK zeitgerecht über sämtliche Informationen aus Bundesermittlungsverfahren mit Bezug zur Internetkriminalität im engeren Sinn in Kenntnis zu setzen. So kann KOBIK ihre Aufgaben, wie beispielsweise die Fallübersicht, die Situationsanalyse der Internetkriminalität in der Schweiz oder die Schnittstellenfunktion zwischen den Polizeibehörden und dem Nachrichtendienst via MELANI besser wahrnehmen.

6.3 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 Vorermittlungen und des Projektes NDHS verschiedene Arbeitssitzungen statt.

2012 fand das erste „Forum Cybercrime Staatsanwaltschaften - KOBIK“ statt. Es hatte unter anderem zum Ziel gewisse Unsicherheiten bei den Staatsanwaltschaften im Umgang mit der Internetkriminalität und den technischen Möglichkeiten auszuräumen. An diesem Forum präsentierten diverse Experten einen praxisnahen und den Bedürfnissen angepassten Einblick in die Bekämpfung der Internetkriminalität. Das grosse Interesse der Staatsanwaltschaften zeigte, dass die ursprüngliche Initiative der Staatsanwaltschaft Zürich berechtigt und die Ausweitung des Forums über kantonale Grenzen hinweg sinnvoll war.

Bildquelle: Gerd Altmann /Pixelio

6.4 Zusammenarbeit mit Action Innocence Genève (AG)

Seit mehreren Jahren arbeitet KOBIK bei der Bekämpfung der Kinderpornografie eng mit der NGO[4] Action Innocence Genève (AG) zusammen. Dank der tatkräftigen Unterstützung durch AG konnte das Projekt zur Überwachung von Peer-to-Peer-Netzwerken in den letzten Jahren erfolgreich betrieben und weiterentwickelt werden. Die Zusammenarbeit mit AG ist von grosser Bedeutung, da eine klare Mehrheit der aktiven Recherchen von KOBIK nur dank der von AG zur Verfügung gestellten Software möglich ist. Gleichzeitig unterstützt AG die KOBIK durch die Entwicklung diverser Zusatzprojekte, die im Rahmen der Bekämpfung von Pädokriminalität zum Einsatz gelangen sollen.

6.5 Zusammenarbeit mit der Privatwirtschaft (Public-Private-Partnership)

Die Zusammenarbeit von KOBIK mit der Privatwirtschaft ist für die Bekämpfung der Internetkriminalität von steigender Bedeutung. Im Berichtsjahr fanden daher verschiedene Besuche und Treffen mit Vertretern der Internetbranche statt. Positiv sind namentlich die Kontakte, die zu diversen Internetdienstanbietern geknüpft werden konnten. Eine Zusammenarbeit ist unter anderem entscheidend für die Abklärung von Internetanschlüssen verdächtiger Personen (IP-Adressen) im Rahmen von polizeilichen Vorermittlungen und Ermittlungen. Die Bekämpfung der Internetkriminalität erfordert ein schnelles und interaktives Handeln sämtlicher Beteiligter. Aufgrund der steigenden Wirtschaftskriminalität im Internet wurden 2012 unter anderem Gespräche mit Vertretern von Online-Verkaufsplattformen aufgenommen.

4 Non-Governmental Organization / Nichtregierungsorganisation (NRO)

6.6 Internationale Zusammenarbeit

Seit 2011 ist KOBIK Mitglied des Focal Point (FP) «Cyborg» von Europol, dessen Ziel die Bekämpfung der grenzüberschreitenden Internetkriminalität ist. Dabei liegt der Fokus auf den Phänomenen «Phishing», «Botnetze» und «Hacking». Neu ist KOBIK 2012 dem FP «Twins», der sich der Bekämpfung der Pädokriminalität widmet, beigetreten. Beide Focal Points sind im European Cybercrime Center (EC3) integriert, das am 1. Januar 2013 seine Arbeit aufgenommen hat.

Das bei Europol in Den Haag angesiedelte Zentrum zur Bekämpfung der Internetkriminalität soll die EU-Staaten operationell unterstützen und Fachwissen in die gemeinsamen Untersuchungen auf EU-Ebene einbringen. Dabei konzentrieren sich die Ermittler auf organisierte Kriminalität im Cyberspace. Schwerpunkte sind der Kampf gegen die sexuelle Ausbeutung von Kindern im Internet sowie die Aufklärung von Finanzdelikten. Zudem befassen sich die EU-Cybercops mit Attacken auf kritische Infrastrukturen und Informationssysteme. Zu den Aufgaben gehören Analyse und Bewertungen, um mögliche Bedrohungslagen früh erkennen und bekämpfen zu können.

KOBIK ist ebenfalls am Projekt «CIRCAMP» beteiligt, das die Verbreitung von Kinderpornografie bekämpft und durch die EPCTF (European Chief of Police Task Force) initiiert wurde. Dieses Projekt bekämpft die Verbreitung von Kinderpornografie im Internet. Wie bereits in den vergangenen Jahren war KOBIK auch 2012 in Verbindung zur „European Financial Coalition“ (EFC). Die von der EU mitfinanzierte EFC besteht aus wichtigen Akteure aus der Strafverfolgung und dem privaten Sektor, mit dem gemeinsamen Ziel die kommerzielle sexuelle Ausbeutung von Kindern im Internet zu bekämpfen.

KOBIK hat im Berichtsjahr den Kontakt zu verschiedenen ausländischen Partnerstellen aktiv gepflegt. Der Austausch dient in erster Linie der gemeinsamen Entwicklung von Prozessen zur verbesserten Zusammenarbeit. Diese konzentriert sich 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 Anstrengungen. Gerade auch im Rahmen von operativen Einsätzen (z.B. verdeckte Ermittlungen) ist der direkte Austausch mit ausländischen Strafverfolgungsbehörden von grossem Nutzen. Auch hier baute KOBIK eine intensive und erfolgsversprechende Zusammenarbeit mit verschiedenen Behörden.

7. Medienauftritte, Ausbildung und Konferenzen

7.1 Medienpräsenz

Die Tätigkeit von KOBIK fand 2012 in zahlreichen Medienberichten Niederschlag. Besondere Aufmerksamkeit schenkten die Medien den (präventiven) verdeckten Vorermittlungen durch KOBIK, einzelnen spektakulären Angriffen auf Informationssysteme (DDoS-Angriffe[5]) und Malware-Infektionen, die zahlreiche Computernutzer betrafen. Die Berichterstattung war über das Jahr verteilt positiv.

7.2 Ausbildung und Konferenzen

Im Berichtsjahr nahmen KOBIK-Mitarbeitende an mehreren Konferenzen, internationalen Tagungen und Ausbildungslehrgängen teil und nutzten die Gelegenheit zur unerlässlichen Kontaktpflege mit Partnern und Experten.

[5] Distributed Denial of Service

8. Politische Vorstösse auf Bundesebene

8.1 Auswahl der 2012 eingereichten parlamentarischen Vorstösse

- Frage 12.5264: Straftatbestand Grooming - Amherd Viola; Fraktion CVP-EVP
- Frage 12.5198: Netzneutralität auch in der Schweiz sichern - Glättli Balthasar
- Frage 12.5185: Drei Hackerangriffe auf das EDA in fünf Jahren - Killer Hans
- Frage 12.5005: Verdeckte Ermittlung. Stand der Arbeiten - Schmid-Federer Barbara; Fraktion CVP-EVP
- Postulat 12.4238: Volkswirtschaftlicher Schaden durch illegale Angebote auf Internet - Fluri Kurt
- Motion 12.4212: Gesetzliche Festschreibung der Netzneutralität - Glättli Balthasar; Grüne Fraktion
- Motion 12.4161: Nationale Strategie gegen Cyberbullying und Cybermobbing - Schmid-Federer Barbara; Fraktion CVP-EVP
- Interpellation 12.4086: Technische Überwachungsmassnahmen und moderne Kommunikationsmittel - Janiak Claude; Sozialdemokratische Fraktion
- Interpellation 12.3902: Die Schweiz als Hort für illegale Angebote im Internet - Fluri Kurt; FDP-Liberale Fraktion
- Interpellation 12.3898: Mehr Rechtssicherheit beim elektronischen Geschäftsverkehr - Amarelle Cesla; Sozialdemokratische Fraktion
- Motion 12.3834: Schutz des Urheberrechts - Freysinger Oskar; Fraktion der Schweizerischen Volkspartei
- Postulat 12.3545: Facebook-Zugang für Kinder - Amherd Viola; Fraktion CVP-EVP
- Motion 12.3476: Anpassung des Tatbestandes sexueller Belästigung von Minderjährigen - Schmid-Federer Barbara; Fraktion CVP-EVP
- Postulat 12.3326: Für ein Urheberrecht, das fair ist und im Einklang mit den Freiheiten der Internetgemeinde steht - Recordon Luc; Grüne Fraktion
- Postulat 12.3289: Persönlichkeitsverletzungen im Internet - Malama Peter; FDP-Liberale Fraktion
- Postulat 12.3152 : Recht auf Vergessen im Internet - Schwaab Jean Christophe; Sozialdemokratische Fraktion

8.2 Rechtliche und politische 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.

Bildquelle: Gerd Altmann /Pixerio

a) 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. Zum 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 sollen. 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“, Art. 143bis StGB) ist die Strafbarkeit vorverlagert worden. Demnach werden neu 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 können.

- 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 (vgl. Art. 18b IRSG). 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.

- Zudem 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 den SPOC im Rahmen der Bearbeitung von Anfragen gemäss Konvention.

b) Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken[6] gutgeheissen. Mit der Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, welchen sie täglich ausgesetzt sind.

Die Strategie identifiziert Cyber-Risiken in erster Linie als Ausprägung bestehender Prozesse und Verantwortlichkeiten. Entsprechend sollen diese Cyber-Risiken auch in bereits bestehende Risikomanagementprozesse Eingang finden. In erster Linie soll die Informationsgrundlage über Cyber-Risiken bei den Verantwortlichen geschaffen und ihre Wahrnehmung dafür geschärft werden.

Dazu erteilt der Bundesrat den Departementen den Auftrag, die Umsetzung der insgesamt 16 festgestellten Massnahmen auf ihrer Ebene und im Verbund und Dialog mit kantonalen Behörden und der Wirtschaft an die Hand zu nehmen. Die Massnahmen erstrecken sich dabei von Risikoanalysen zu kritischen ICT-Infrastrukturen bis zur stärkeren Einbringung der Schweizer Interessen in diesem Bereich auf internationaler Ebene.

[6] www.admin.ch/ch/d/ff/2013/563.pdf

Die Massnahme 6 sieht vor, dass auf nationaler Ebene eine möglichst vollständige Fallübersicht (Straffälle) geführt wird und interkantonale Fallkomplexe koordiniert werden müssen. Die gewonnen Informationen sollen in eine gesamtheitliche Lagedarstellung einfliessen. Das EJPD hat in Zusammenarbeit mit den Kantonen per Ende 2016 ein entsprechendes Konzept vorzulegen. Dieses Konzept muss auch die Klärung von Schnittstellen mit weiteren Akteuren auf dem Gebiet der Minimierung von Cyber-Risiken, die Koordination mit der Lagedarstellung und die für die Umsetzung des Konzeptes benötigten Ressourcen und rechtlichen Anpassungen auf Stufe Bund und Kantone umfassen. Gemäss Entscheid des Leitungsausschusses KOBIK und der Direktion fedpol wird KOBIK die Koordination und die Auftragserfüllung im Zusammenhang mit den Umsetzungsarbeiten zur Strategie NCS für fedpol koordinieren und sicherstellen.

9. 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-Infrastrukturen (Rechenkapazität, Datenspeicher von Computern und Servern), die aus verschiedenen Teilen der Welt über ein Netzwerk wie dem 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, sozialen 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	Kennwert eines Bildes, der eindeutig zugeordnet werden kann (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. Spam wird oft zu Werbezwecken versandt, bisweilen auch, um in einem Benutzersystem Malware (ein Schadprogramm) einzuschleusen.
Streaming	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).

10. Mögliche Entwicklungen und Bedrohungen **2013**

Gestützt auf den Meldungseingang bei KOBIK können keine oder nur sehr wenige Rückschlüsse auf die effektive Entwicklung der Internetkriminalität oder illegaler Inhalte im Internet gezogen werden. Allenfalls lassen sich daraus Tendenzen hinsichtlich der Meldebereitschaft der Bevölkerung und der Wahrnehmung von Internetkriminalität in der Gesellschaft ableiten.

Banktrojaner: Es ist nicht auszuschliessend, dass die von russischen Gruppierungen angekündigte Operation ‚Blitzkrieg', die hauptsächlich gegen US-amerikanische Banken gerichtet sein soll, auch zu Angriffen auf Schweizer Banken führt. Die Angriffe sollen hauptsächlich darin bestehen, Login-Daten mittels Trojaner abzufangen. Da die meisten Banken in der Schweiz mehrstufige Authentifizierungsmechanismen haben, ist das Risiko für direkte finanzielle Schäden durch fälschlich ausgelöste Transaktionen zwar gering, aber nicht auszuschliessen.

Mobile-Malware: 2012 explodierte die Anzahl von Schadsoftware-Varianten, die vor allem Android-Smartphones infizieren. Experten erwarten, dass die Zahl weiter ansteigt. Folgen für Betroffene sind Mehrkosten durch Nutzung von Internet-Bandbreite, da infizierte Geräte zu DDoS-Attacken verwendet werden können, sowie unerwünschtes Versenden von Spam-SMS. Zudem muss damit gerechnet werden, dass persönliche Daten wie Adressbuchinhalte, Passwörter etc. unerlaubterweise ausgelesen und an weitere Kriminelle verkauft werden.

Malware: Auch hier ist mit einem weiteren Anstieg der Fälle zu rechnen. Im Zentrum steht weiterhin das Ausspionieren von Bankdaten, Kreditkartennummern und Passwörtern. Sekundäre Ziele sind Adressbuchdaten zum Aufbau von Schein-Identitäten für Betrugsversuche und der Aufbau eines Botnetzes für DDoS-Attacken. Es ist zudem mit neuen Infektionswegen zu rechnen, beispielsweise Add-Ons für Browser oder Webapps für Social-Media Seiten. Denkbar ist zudem, dass Sicherheitslücken in Cloud-Diensten ausgenutzt werden, um Schadsoftware auf Zielrechnern zu installieren.

Datendiebstahl: Wie diverse Fälle aufzeigen, sind auch kleine Webseiten nicht vor Angreifern geschützt. Kundendaten wie Adressen sind für Hacker mehr denn je ein wertvolles Ziel, da sie Social Engineering wesentlich erleichtern und somit bei weiteren Betrugsmaschen eingesetzt werden können. Zudem können Email-Adressen lukrativ auf entsprechenden Foren verkauft werden. Dadurch, dass Cyberkriminelle sich auf bestimmte Dienstleistungen spezialisieren, wie z.B. das Beschaffen von Daten und deren Verkauf, könnten inskünftig auch kleinere Ziele für solche Angriffe interessant und ins Visier genommen werden.

Scams: Mit der steigenden Verbreitung des Internets in Afrika und dem entstehenden (am westlichen Massstab gemessen schlecht verdienenden Mittelstand in Ländern wie Nigeria, Südafrika oder Marokko befürchten Experten, dass betrügerische Angebote auf Kleinanzeigen- und Auktionsseiten in den nächsten Jahren erneut erheblich zunehmen werden. Man spricht von einer Verdoppelung des Anzeigevolumens bis 2015.

DDoS-Attacken: 2012 wurden diverse DDoS-Attacken zu erpresserischen aber auch politisch motivierten Zwecken gestartet. Es ist auch 2013 davon auszugehen, dass solche Attacken stattfinden werden. Grossmächte sind daran, militärische und nachrichtendienstliche Reserveeinheiten zur Verteidigung der kritischen Infrastrukturen gegen DDoS- oder andere Hacking-Attacken aufzubauen. Das zeigt, dass grossangelegte DDoS-Angriffe als ernstzunehmendes Bedrohungsszenario wahrgenommen wird.

Bei sämtlichen 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.