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 2013

10 JAHRE KOBIK

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

Veröffentlicht: 27. März 2014

Bildquellen: Thinkstock, KOBIK

VORWORT

von Herrn Regierungsrat Christoph Neuhaus,
Vorsitzender des Leitungsausschusses KOBIK

Das einzig Konstante ist die Veränderung, orakelte schon der Grieche Heraklit. Nicht nachlassen gewinnt und Stillstand ist Rückschritt. Wer kennt sie nicht, diese geflügelten Worte. Für KOBIK sind diese Aussagen von besonderer Bedeutung. Zum einen, weil ein Internetjahr laut einer Studie von ibusiness.de über vier Lebensjahre umfasst und zum anderen, weil KOBIK nun auf ein Jahrzehnt Erfahrung zurückblicken darf. Visionär und von Beginn weg allen voraus - gilt es für KOBIK, auch weiterhin nach vorne zu schauen und in diesem Sinne zu handeln.

Mehr als acht von zehn Schweizerinnen und Schweizer tummeln sich heute mehrmals pro Woche im World Wide Web. Damit wurden sowohl für die Polizei als auch für die Justiz ganz neue Tätigkeitsfelder und Einsatzgebiete geschaffen. Polizei und Justiz haben mit den ihnen zur Verfügung stehenden Ressourcen bereits offline für die Sicherheit von rund acht Millionen Menschen zu sorgen. Was bedeutet es nun für diese beiden Institutionen, wenn zusätzlich rund 2,7 Milliarden Personen aus der ganzen Welt mit einem einfachen Mausklick online auf Schweizer Systeme zugreifen können? Was bedeutet es, wenn gemäss Europol diese Zahl bis zum Jahr 2017 gar auf 3,5 Milliarden steigt und auch nur ein Bruchteil davon unlautere Absichten hat?

Im Berichtsjahr wurde das erste Botnet entdeckt, bei dem ein Viertel der infizierten Computer „Dinge“ – oder präziser gesagt Fernseher, Kühlschränke und weitere Haushaltutensilien – waren. Was hat das für Konsequenzen, wenn im Jahr 2020 um die 200 Milliarden solcher Gegenstände mit dem Internet verbunden sind? Was bedeutet das für jeden einzelnen von uns, für den Wirtschaftsstandort Schweiz und für die Strafverfolgungsbehörden? Mit ihrem Wechsel vom Nachrichtendienst zur Bundeskriminalpolizei hat sich KOBIK erfolgreich zu einer Cyberkriminalpolizei und anerkannten Partnerin von internationalen Ermittlungsbehörden wie dem European Cybercrime Center von Europol (EC3) und dem Interpol Global Complex for Innovation (IGCI) in Singapur entwickelt. Die Weichen für eine erfolgreiche internationale Zusammenarbeit bei der Bekämpfung dieser neuen Kriminalitätsform sind gestellt. Die Schweiz verfügt über das Knowhow, die Ressourcen und, an und für sich, über eine optimale Ausgangslage.

Auf Bundesebene muss KOBIK dem Bundesrat bis Ende 2016 ein Konzept aus der Massnahme 6 der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (M6 NCS) zu einer Fallübersicht und der Koordination von interkantonalen Fallkomplexen unterbreiten. Die Herausforderung liegt einerseits darin, eine für alle akzeptable aber auch finanziell interessante Lösung zur optimalen Bekämpfung der international organisierten Cyberkriminalität zu finden und dies in einer Zeit, in der Budgetkürzungen überall ein Dauerthema sind. Auf der anderen Seite gilt es Lösungen zu einer arbeitsteiligen Vorgehensweise zu finden, ohne dass dabei das Projekt wegen Zuständigkeitsfragen zwischen den kantonalen und nationalen Strafverfolgungsbehörden in Frage gestellt wird. Die Chance, die sich mit dem Projekt M6 NCS für alle bietet, dürfen wir nicht aus dem Reflex „Wahrung des Föderalismus“ scheitern lassen. Vor allem gerade weil wir den Föderalismus bewahren wollen.

Fragen über Fragen, grosse Herausforderungen, es gibt viel zu tun – KOBIK packt das kommende Jahrzehnt, wie man es von ihr kennt, tatkräftig an – visionär und immer mit dem Blick in die (digitale) Zukunft!

Inhaltsverzeichnis

1. **DAS WICHTIGSTE IN KÜRZE 1**
2. **RÜCKBLICK AUF 10 JAHRE KOBIK 2**
3. **KOBIK, DIE MELDESTELLE 7**
   - 3.1. MELDUNGSEINGANG 7
   - 3.2. WAS WURDE GEMELDET? 8
   - 3.3. PRODUKTE 15
   - 3.4. AUSGEWÄHLTES FALLBEISPIEL 15
4. **AKTIVE RECHERCHEN DURCH KOBIK (MONITORING) 16**
   - 4.1. AKTIVE RECHERCHEN IN PEER-TO-PEER-NETZWERKEN (P2P) 17
   - 4.2. VERDACHTSUNABHÄNGIGE VERDECKTE VORERMITTLUNGEN 17
   - 4.3. VERDECKTE ERMITTLUNGEN NACH STPO 17
   - 4.4. FEEDBACK AUS DEN KANTONEN 18
   - 4.5. AUSGEWÄHLTE FALLBEISPIELE 23
5. **KRIMINALPOLIZEILICHER INFORMATIONSAUSTAUSCH 24**
   - 5.1. MELDUNGSEIN- UND AUSGANG 24
   - 5.2. NATIONALE UND INTERNATIONALE VERFAHRENSKOORDINATION 26
   - 5.3. AUSGEWÄHLTE FALLBEISPIELE 29
6. **PROJEKTE 30**
   - 6.1. NATIONALE STRATEGIE ZUM SCHUTZ DER SCHWEIZ VOR CYBER-RISIKEN (NCS) 30
   - 6.2. KOBIK GOES SOCIAL MEDIA 31
7. **ARBEITSGRUPPEN, PARTNERSCHAFTEN UND KONTAKTE 32**
   - 7.1. NATIONALE DATEI- UND HASHWERTESAMMLUNG (NDHS) 32
   - 7.2. NATIONALE ARBEITSGRUPPEN 32
   - 7.3. BUNDESINTERNE ZUSAMMENARBEIT 32
   - 7.4. ERFAHRUNGSAUSTAUSCH MIT DEN KANTONEN 33
   - 7.5. ZUSAMMENARBEIT MIT NGOS 33
   - 7.6. ZUSAMMENARBEIT MIT DEN SCHWEIZERISCHEN INTERNET-ACCESS-PROVIDERN . 34
   - 7.7. INTERNATIONALE ZUSAMMENARBEIT 34
8. **MEDIENAUFTRITTE, AUSBILDUNG UND KONFERENZEN 36**
   - 8.1. MEDIENPRÄSENZ 36
   - 8.2. SOCIAL MEDIA 36
   - 8.3. AUSBILDUNGEN UND KONFERENZEN 36
9. **POLITISCHE VORSTÖSSE AUF BUNDESEBENE 37**
10. **MÖGLICHE ENTWICKLUNGEN UND BEDROHUNGEN 2014 ..... 38**
11. **GLOSSAR 40**

1. Das Wichtigste in Kürze

- 2013 gingen bei KOBIK insgesamt 9208 Meldungen über das Online-Meldeformular ein. Dies entspricht einer Zunahme von 11,7 Prozent gegenüber dem Vorjahr.

- 61 Prozent der Meldungen betrafen Vermögensdelikte, welche im Verhältnis zu den strafbaren Handlungen gegen die sexuelle Integrität weiter zugenommen haben. Damit setzte sich der Trend der Vorjahre auch 2013 fort.

- Insgesamt 356 Meldungen führten direkt und aufgrund der strafrechtlichen Relevanz zur Übermittlung des Sachverhalts an nationale oder internationale Behörden und Organisationen.

- Durch das aktive Monitoring in Peer-to-Peer-Netzwerken (P2P) gelang es KOBIK im Berichtsjahr 238 Personen zu identifizieren, die aktiv am Austausch von Kinderpornografie beteiligt waren.

- Verdeckte Vorermittlungen gemäss Polizeigesetzgebung des Kantons Schwyz und Ermittlungen nach Strafprozessordnung (StPO) durch KOBIK führten 2013 in insgesamt 17 Fällen zu Strafanzeigen zuhanden der zuständigen Kantone und weiteren 176 Anzeigen zuhanden ausländischer Strafverfolgungsbehörden.

- KOBIK hat erfolgreich mit den Umsetzungsarbeiten zur Massnahme 6 der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) begonnen. Im Berichtsjahr konnten bereits eine detaillierte Projektanalyse erstellt und die Projektorganisation definiert werden.

- Im Rahmen des 10-jährigen Bestehens von KOBIK wurden am 22. Dezember 2013 mit Profilen auf Facebook (www.facebook.com/cybercrime.ch) und Twitter (@KOBIK_Schweiz) zwei neue Kommunikationskanäle aufgeschaltet.

2. Rückblick auf 10 Jahre KOBIK

2000–2002: Eine Idee entsteht

Die Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS) setzte im Juni 2000 eine interkantonale Arbeitsgruppe BEMIK[1] ein, mit dem Auftrag, die Voraussetzungen und Rahmenbedingungen für eine nationale Monitoringstelle vertieft zu prüfen und konkrete Vorschläge zu unterbreiten. Aufgrund der dringenden polizeilichen Koordinationsbedürfnisse schlug die AG BEMIK, unter der Leitung von Adrian Lobsiger, heute stv. Direktor fedpol, eine Reihe von konkreten Massnahmen vor und empfahl einstimmig die Bildung einer nationalen Koordinationsstelle im Bereich der Internetkriminalität.

Gestützt auf die Ergebnisse der AG BEMIK beschlossen das Eidgenössische Justiz- und Polizeidepartement (EJPD) und die Konferenz der kantonalen Justiz- und Polizeidirektoren (KKJPD) im Frühjahr 2001, bei der Bekämpfung der Internetkriminalität gemeinsam vorzugehen. In einer Verwaltungsvereinbarung wurden Auftrag, Organisation und Finanzierung einer nationalen Koordinationsstelle definiert.

Vorstand und Plenum der KKJPD sprachen sich einstimmig für die Umsetzung der Verwaltungsvereinbarung aus. Mit Schreiben vom 4. Februar 2002 lud der Präsident der KKJPD die Kantone ein, im Budget 2003 entsprechende Finanzmittel vorzusehen. In der Folge haben, mit Ausnahme des Kantons Zürich, alle Kantone ihre Beteiligung am Projekt bestätigt. Der Bundesrat bekräftigte seinerseits am 20. Februar 2002 die Absicht, auf den 1. Januar 2003 gemeinsam mit den Kantonen eine nationale Koordinationsstelle zur effizienteren Bekämpfung der Internetkriminalität (KOBIK) zu lancieren.

1. Januar 2003: Der Startschuss

KOBIK nahm am 1. Januar 2003 mit der Aufschaltung eines viersprachigen Meldeformulars im Internet (Bild rechts) den Betrieb auf. Unter der Adresse www.cybercrime.admin.ch finden sich seither nebst den Meldeformularen auch Hintergrundinformationen zu KOBIK und zur Internetkriminalität im Allgemeinen. Der Start von KOBIK stiess auf ein breites Medienecho. Besonders reges Interesse zeigten die elektronischen Medien und die IT-Fachpresse. Verschiedene Hintergrundartikel und Interviews rundeten in der Folge das Bild ab. In einer ersten Bilanz nach einem halben Jahr Betrieb konnte der erfolgreiche Start von KOBIK in einer Medienmitteilung kommuniziert werden.

[1] AG BEMIK = Arbeitsgruppe zur Bekämpfung des Missbrauchs von Informations- und Kommunikationstechnologien

Mai 2003: Aufnahme des aktiven Monitorings

Anfang Mai nahm die Koordinationsstelle das Internetmonitoring mit dem Schwerpunkt P2P-Netzwerke auf. Dabei wird in einem ersten Schritt nach illegalen Dateien gesucht, welche von Nutzern mit einer Schweizer IP-Adresse angeboten werden. Nach Abschluss der Vorarbeiten wird der Fall in Form einer Anzeige an den zuständigen Kanton übermittelt.

9. Januar 2004: Veröffentlichung des 1. Jahresberichtes KOBIK

Der erste Rechenschaftsbericht umfasste einen kurzen Rückblick auf die Entstehungsgeschichte von KOBIK, die Konstitution des Leitungsausschusses und die Rekrutierung des KOBIK-Teams. Im Weiteren gab ein kommentierter Statistikteil Aufschluss über die Meldungen und das Monitoring. So wurde festgestellt, dass im ersten Jahr 6457 Meldungen aus der Bevölkerung über das Meldeformular eingegangen sind und aufgrund des aktiven Monitorings über 100 Anzeigen zuhanden der Kantone erstellt wurden.

2004: Erste Reorganisation

Zur Verstärkung und Vereinheitlichung der Führung des KOBIK-Teams wurde beschlossen, das bisher bei der Bundeskriminalpolizei (BKP) angesiedelte KOBIK-Clearing organisatorisch ebenfalls beim Dienst für Analyse und Prävention (DAP) anzusiedeln.

2005: Eingliederung in die Sektion MELANI/Cybercrime

Die organisatorische Eingliederung des KOBIK-Clearings wurde mit der Zusammenfassung der KOBIK-Bereiche Analyse und Clearing sowie der Meldestelle Analyse und Informationssicherung (MELANI) in der neuen Sektion MELANI/Cybercrime abgeschlossen. Nach dem Beitritt des Kantons Zürich konnte das Monitoring-Team mit einem zusätzlichen Mitarbeiter auf insgesamt neun Angestellte verstärkt werden.

2005–2006: Präventionsarbeit wird ausgebaut

Im Rahmen der 2005 gestarteten nationalen Kampagne «Stopp-Kinderpornografie» arbeitete KOBIK eng mit der Schweizerischen Kriminalprävention (SKP) zusammen und beteiligte sich an diversen Ausbildungs- und Fachtagungen. Dieser Hintergrund führte schliesslich zur Schaffung des Projektes DNS-Blacklist im Jahr 2007. KOBIK wurde zudem ein Partner des Präventionsprogramms «Security for Kids» von Microsoft Schweiz.

2006: Vereinbarung mit der Landespolizei Liechtenstein

Aufgrund einer Vereinbarung mit der Landespolizei Liechtenstein erbringt KOBIK seine Dienstleistungen seit 2006 auch zugunsten des Fürstentums Liechtenstein.

2007: Roll-Out des Projekts DNS-Blacklist

Seit 2007 werden in der Schweiz Kinderpornografie-Webseiten mit Hilfe der Software Child Sexual Abuse Anti-Distribution Filter gesperrt. Das Projekt basiert auf einer freiwilligen Zusammenarbeit zwischen KOBIK und den grössten Internet-Service-Providern (ISP) der Schweiz. KOBIK verpflichtet sich darin, eine stets aktualisierte Liste von Internetseiten mit strafbaren kinderpornografischen Inhalten zu führen und den ISPs zur Verfügung zu stellen. Die Liste wird aufgrund von Meldungen aus der Bevölkerung erstellt. Die ISPs wiederum blockieren diese Seiten gestützt auf ihre allgemeinen Geschäftsbedingungen.

2007: Neuer Rekordwert an Meldungen

Das fünfte Betriebsjahr von KOBIK zeichnete sich durch einen markanten Anstieg der Meldungen aus der Bevölkerung aus. Mit über 10 000 Meldungen führte KOBIK eine wichtige Triagearbeit durch und konsolidierte ihre Rolle als nationale Ansprechpartnerin in Sachen Internetkriminalität. Die steigende Zahl der Meldungen war auf das starke Wachstum im Bereich der Wirtschaftskriminalität zurückzuführen sowie auf einzelne aktive Bürger, welche teilweise dutzende Meldungen pro Monat absetzten. Die Leitung von KOBIK zog nach fünf Jahren eine positive Bilanz: KOBIK ist als nationales Kompetenzzentrum gerüstet für künftige Herausforderungen.

2008: KOBIK im Wandel

Im Hinblick auf die bevorstehende Angliederung an die Bundeskriminalpolizei fanden im Folgejahr 2008 einige Anpassungen bei der Personalstruktur sowie der technischen Ausrüstung statt. So wurde die Informatikinfrastruktur modernisiert sowie durch zusätzliche Hard- und Softwarebeschaffungen ergänzt.

2009: Ansiedlung bei der Bundeskriminalpolizei

Auf den 1. Januar 2009 fand die Trennung von MELANI und KOBIK statt. KOBIK wurde innerhalb von fedpol in die Bundeskriminalpolizei integriert und der bei fedpol/DAP angesiedelte MELANI-Teil ging zum neu geschaffenen Nachrichtendienst des Bundes (NDB). Durch die Integration in die BKP nahm KOBIK fortan vermehrt auch operative und polizeiliche Aufgaben wahr, insbesondere die Koordination nationaler und internationaler Ermittlungen sowie den kriminalpolizeilichen Informationsaustausch. Diese neue Ausrichtung bedingte diverse organisatorische und personelle Anpassungen. Zudem wurde beschlossen, die vorher einzeln geführten Kommissariate Monitoring und Clearing im neuen Kommissariat KOBIK zusammen zu fassen.

2010–2011: Aktive Recherchen werden ausgebaut

KOBIK verstärkte die «aktiven Recherchen», was sich in einem Anstieg der Anzeigen an die Kantone niederschlug. Vor allem die «verdeckten Vorermittlungen» beschäftigten KOBIK 2010 stark.

Ab dem 1. Januar 2011 durften die meisten Kantonspolizisten nicht mehr präventiv verdeckt und ohne Verdachtsmoment im Internet gegen Pädokriminelle ermitteln, da ihre kantonalen Polizeigesetze dafür keine hinreichende Grundlage boten. Diese kantonale Gesetzeslücke war durch die Inkraftsetzung der neuen Strafprozessordnung (StPO) entstanden.

Einige Kantone wie Schwyz, Aargau und Obwalden erkannten den Handlungsbedarf frühzeitig und passten ihre Polizeigesetze auf den 1. Januar 2011 an. Das EJPD seinerseits fand mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) eine Lösung, die es KOBIK ermöglichte, die Monitoring-Tätigkeit im Internet im Bereich Pädokriminalität gestützt auf eine neue Rechstgrundlage auszubauen. KOBIK konnte dank einer Vereinbarung mit dem Sicherheitsdepartement des Kantons Schwyz im Auftrag der Kantone ab dem 1. Januar 2011 präventiv verdeckt vorermitteln und somit Chaträume überwachen. Die Arbeit von KOBIK im Bereich der verdeckten Vorermittlungen stützt sich auch 2013 noch auf das Polizeirecht sowie auf eine Bewilligung des Zwangsmassnahmengerichts des Kantons Schwyz. Damit ist sichergestellt, dass sich Pädokriminelle im Internet nicht in einem rechtsfreien Raum in Sicherheit wiegen können.

2011: Nationale Datei- und Hashwertesammlung (NDHS)

Schon in den vorangegangenen Jahren beschäftigte sich die damalige Arbeitsgruppe Bilddatenbank (später: Arbeitsgruppe NDHS) mit der Schaffung einer nationalen Sammlung von Bildern und Hashwerten von kinderpornografischem Material. Nachdem das Projekt 2010 durch KOBIK erneut an die Hand genommen wurde, konnten 2011 grosse Fortschritte im neu benannten Projekt Nationale Datei- und Hashwertesammlung (NDHS) erzielt werden. Die kantonalen Polizeikorps wurden erfolgreich geschult und die ersten kantonalen Bildarchive wurden bereits an KOBIK übergeben.

2011–2012: Nationale Strategie Cyber Defense (später Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS))

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

Am 27. Juni 2012 hat der Bundesrat die neubetitelte «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» (NCS) gutgeheissen. Mit der Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, denen sie täglich ausgesetzt sind. Der Abschluss der Umsetzungsarbeiten ist für 2017 geplant.

Januar 2012: Europaratskonvention über die Cyberkriminalität

Mit der Ratifikation der Europaratskonvention über die Cyberkriminalität beteiligt sich die Schweiz an der verstärkten internationalen Bekämpfung der 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.

Oktober 2012: Rollout NDHS

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

Dezember 2012: Beitritt der Schweiz zur Global Alliance against Child Sexual Abuse Online

Mitarbeiter von KOBIK begleiteten Bundesrätin Simonetta Sommaruga als Experten für den Beitritt der Schweiz zur Global Alliance in Brüssel.

Januar 2013: European Cybercrime Center bei Europol

Bereits seit 2011 ist KOBIK aktives Mitglied der Focal Points CYBORG und TWINS von Europol. Beide Focal Points[2] sind neu 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 unterstützt die EU-Staaten operationell und bringt das Fachwissen in die gemeinsamen Untersuchungen auf EU-Ebene ein. 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 Analysen und Bewertungen, um mögliche Bedrohungslagen früh erkennen und bekämpfen zu können.

2013: Umsetzung NCS hat begonnen

Im Zusammenhang mit der Umsetzung der Massnahme 6 der NCS ist festgehalten, dass das EJPD in Zusammenarbeit mit den Kantonen per Ende 2016 ein Konzept «Fallübersicht und Koordination interkantonaler Fallkomplexe» vorzulegen hat. Dieses Konzept umfasst auch die Klärung von Schnittstellen mit weiteren Akteuren auf den Gebieten der Minimierung von Cyber-Risiken, der Koordination der Lagedarstellung und der für die Umsetzung des Konzeptes benötigten Ressourcen und rechtlichen Anpassungen auf Stufe Bund und Kantone. 2013 konnte bereits eine detaillierte Projektanalyse erstellt und die Projektorganisation definiert werden.

Dezember 2013: Aufschaltung eines Facebook- und Twitter-Profils

Am 22. Dezember 2013 wurden mit Facebook und Twitter zwei neue Kommunikationskanäle durch KOBIK erschlossen.

[2] Bei den Focal Points handelt es sich um Abteilungen innerhalb Europol, die speziell auf die Koordination und Analyse internationaler Fallkomplexe ausgerichtet sind. Sie wurden aus den früheren Analysis Workfiles (AWF) gebildet.

3. 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.

3.1. Meldungseingang

Im Zeitraum vom 1. Januar 2013 bis 31. Dezember 2013 sind bei KOBIK insgesamt 9208 Verdachtsmeldungen über das Meldeformular auf www.cybercrime.ch eingegangen. Dies entspricht einer Zunahme um 11,7 Prozent im Vergleich zum Vorjahr (8242 Meldungen).

Aus der Anzahl eingehender Meldungen lassen sich keine zutreffenden Aussagen über die tatsächliche Zu- oder Abnahme der Internetkriminalität oder illegaler Inhalte im Internet machen. Die Anzahl Meldungen widerspiegelt lediglich die Wahrnehmung von Internetkriminalität in der Gesellschaft sowie die Bereitschaft, diese aktiv an die Behörden weiterzuleiten.

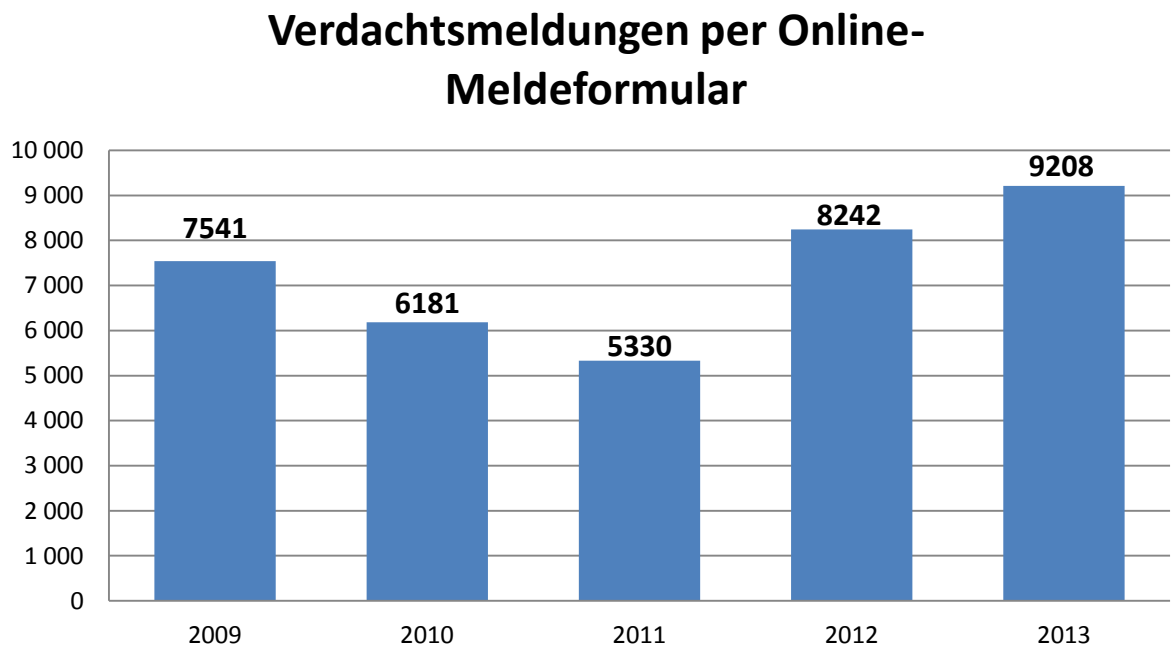


Abbildung 1 : Meldungseingänge über www.cybercrime.ch im Jahresvergleich

Im Durchschnitt gingen pro Monat 767 Meldungen ein, allerdings mit starken Schwankungen im Mai (1083 Eingänge) und im September (585 Eingänge). Diese Fluktuationen sind auf konkrete und zeitlich begrenzte Vorfälle zurückzuführen, insbesondere die Veröffentlichung einer Medienmitteilung durch KOBIK.

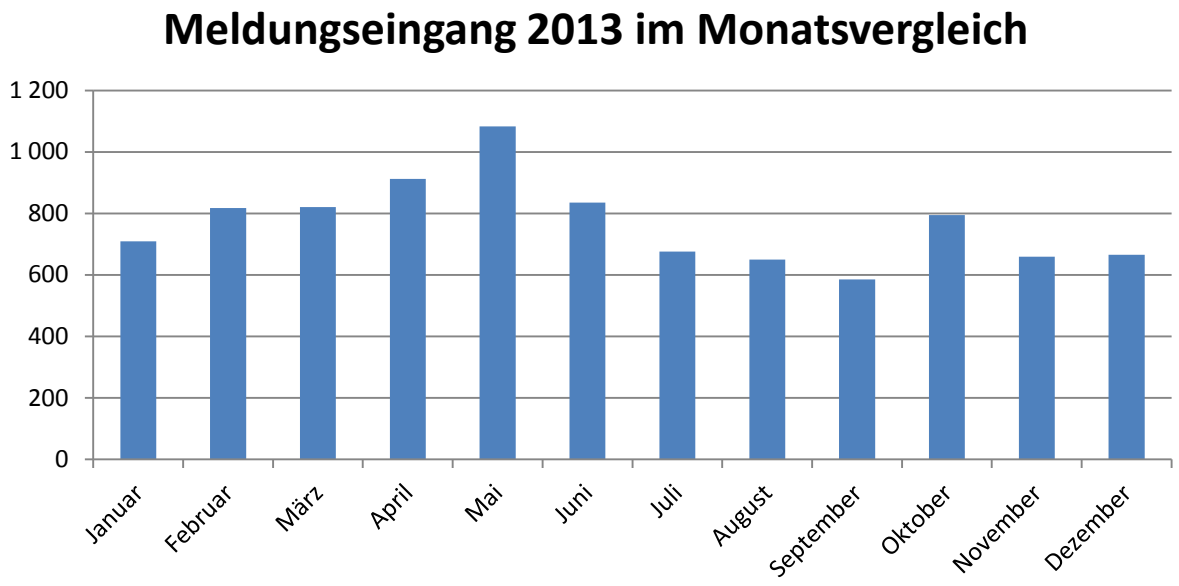


Abbildung 2 : Meldungseingänge über www.cybercrime.ch im Monatsvergleich (Total 9208 Meldungen)

3.2. Was wurde gemeldet?

Bei 86 Prozent der Meldungen (7910) wurde ein Bezug zum Strafgesetzbuch festgestellt. Die restlichen Meldungen betrafen unter anderem Verstösse gegen das UWG[3] (290 Meldungen), URG[4] (24 Meldungen), ZGB[5] (40 Meldungen), BetmG[6] (14 Meldungen) und GwG[7] (7 Meldungen). In rund zehn Prozent der gemeldeten Fälle war der Inhalt nicht strafbar.

Die gemeldeten Vorgänge lassen sich in zwei Teilbereiche aufteilen. Unter Internetkriminalität im engeren Sinne werden Straftaten verstanden, die mit Hilfe der Technologien des Internets verübt werden oder sich Schwachstellen dieser Technologien zu Nutze machen. Beispiele sind Delikte wie «Hacking», «Distributed Denial of Service» (DDoS) oder das Herstellen und In-Umlauf-Bringen von Schadsoftware. Diese Straftaten sind erst durch das Internet ermöglicht worden oder richten sich gezielt gegen dessen Technologien. Die Internetkriminalität im weiteren Sinne nutzt das Internet als Kommunikationsmittel, wobei die sich bietenden Möglichkeiten, wie beispielsweise der E-Mail-Verkehr oder der Austausch von Dateien für unlautere Zwecke, missbraucht werden. Beispiele sind das Versenden von Spam, Betrugsmaschen auf Inserateplattformen oder die Verbreitung von verbotener Pornografie.

Viele der gemeldeten Sachverhalte betrafen keine Offizialdelikte und bedurften daher einer Strafanzeige. In solchen Fällen verweist KOBIK die meldenden Personen an die hierfür zuständigen kantonalen Polizeistellen.

---

[3] Bundesgesetz gegen den unlauteren Wettbewerb, vom 19. Dezember 1986, SR 241

[4] Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, vom 9. Oktober 1992, SR 231.1

[5] Schweizerisches Zivilgesetzbuch, vom 10. Dezember 1907, SR 210

[6] Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe, vom 3. Oktober 1951, SR 812.121

[7] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung im Finanzsektor, vom 10. Oktober 1997, SR 955.0

Die Tendenz, dass der Anteil Meldungen zu strafbaren Handlungen gegen das Vermögen wächst, hat sich auch 2013 bestätigt. Insgesamt 60,7 Prozent der eingehenden Meldungen betrafen diesen Deliktsbereich (Art. 137–172ter StGB). An zweiter Stelle mit 20 Prozent der eingegangen Meldungen folgen Meldungen über strafbare Handlungen gegen die sexuelle Integrität (Art. 187–212 StGB). Dies entspricht einer deutlichen Abnahme von 40,3 Prozent im Vergleich zum Vorjahr.

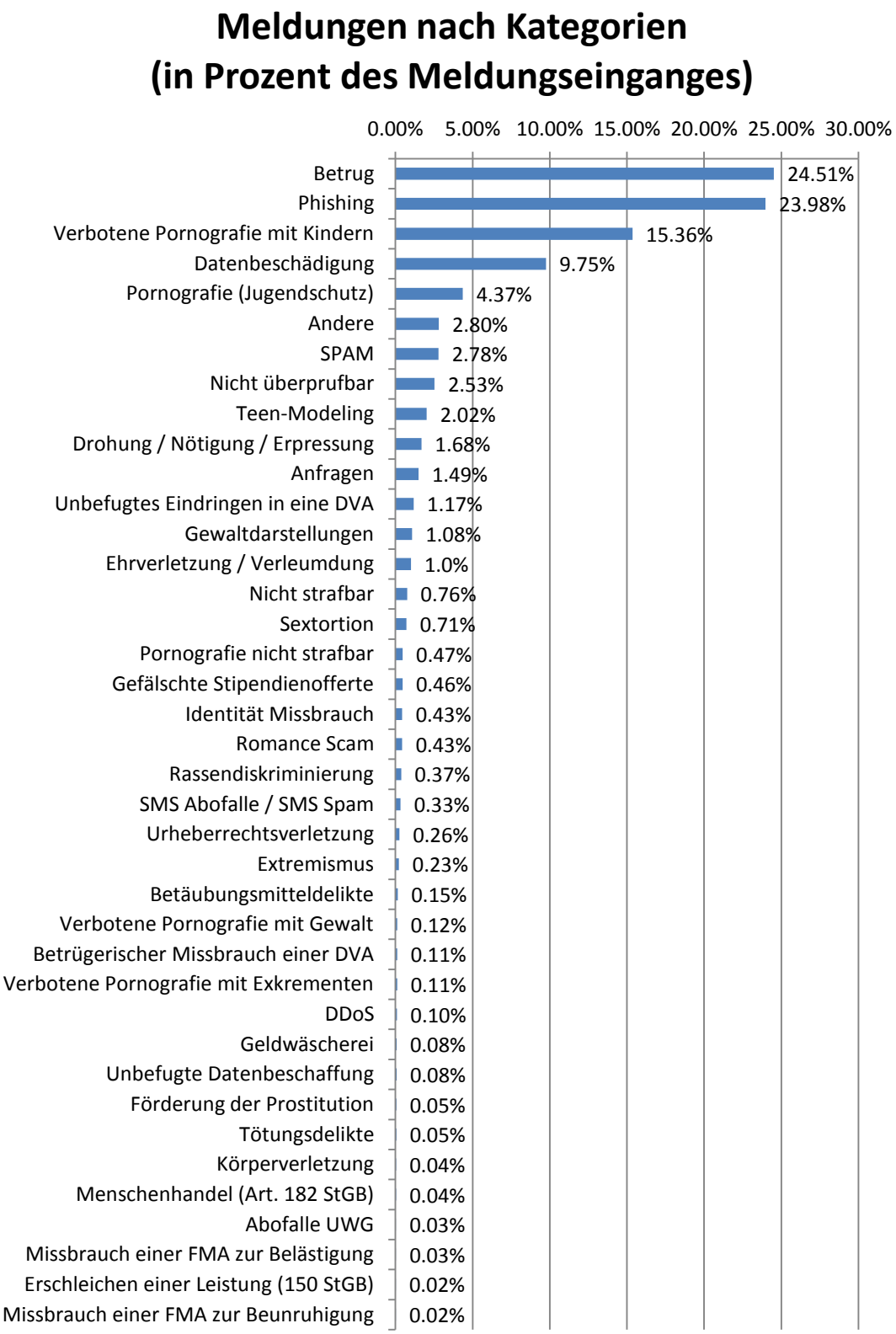


Abbildung 3 : Prozentualer Anteil der Kategorien am Meldungseingang 2013

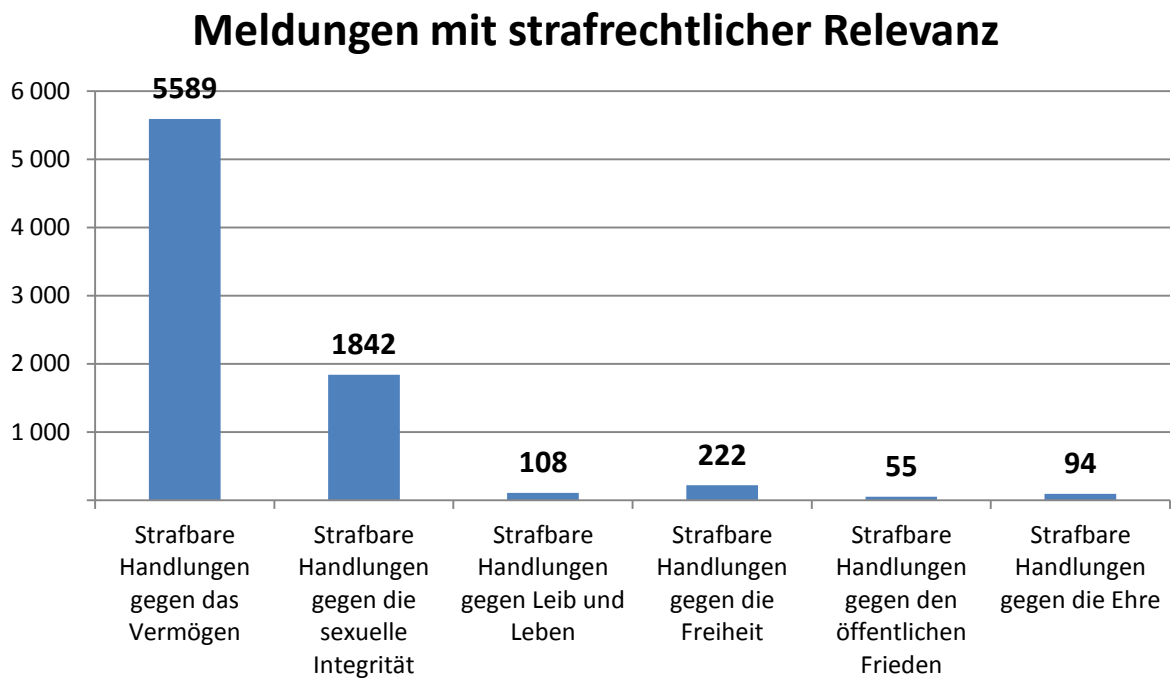


Abbildung 4 : Meldungseingang 2013 nach strafrechtlicher Relevanz (Total 7910 Meldungen)

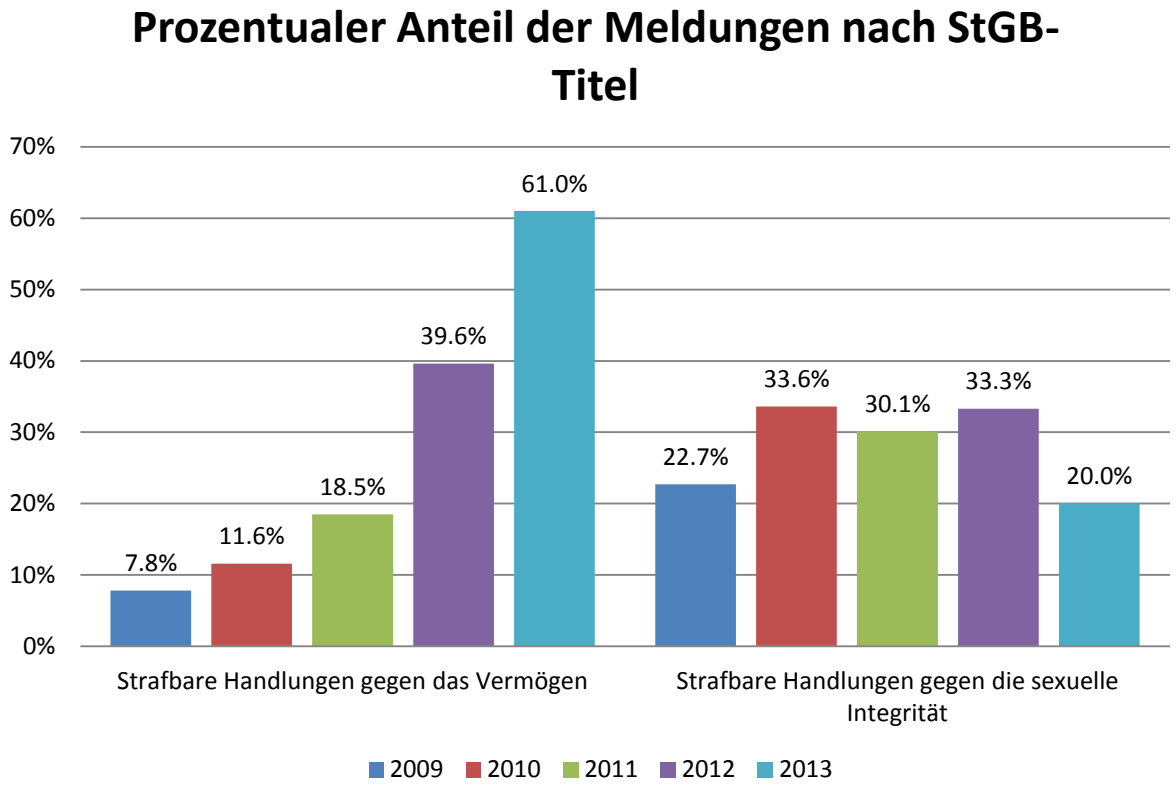


Abbildung 5 : Prozentualer Anteil der Meldungen, 2008–2013

3.2.1. Strafbare Handlungen gegen das Vermögen

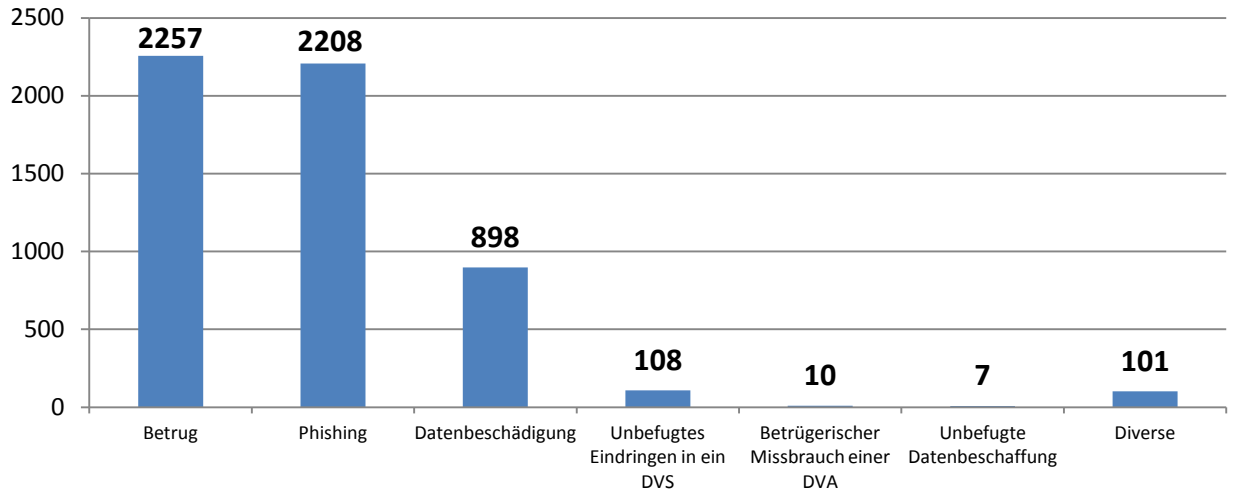


Abbildung 6 : Meldungseingang zu strafbaren Handlungen gegen das Vermögen (Total 5589)

Mit 60,7 Prozent am häufigsten gemeldet (5589) wurden im Berichtsjahr strafbare Handlungen gegen das Vermögen. Die Unterkategorie Betrug verzeichnet dabei mit 2257 Meldungen 25 Prozent des Gesamtvolumens an eingegangenen Meldungen. Die gemeldeten Betrugsvarianten sind vielzählig.

Zugenommen haben unter anderem Meldungen zu Betrugsversuchen auf Auktions- und Kleinanzeigeplattformen, bei denen sowohl Käufer als auch Verkäufer, respektive Interessenten und Inserenten Ziele der Täterschaft waren. Zudem wurde festgestellt, dass die Täterschaft zunehmenden Aufwand betreibt, um solchen Betrugsversuchen eine höhere Glaubwürdigkeit zu verleihen. So baut die Täterschaft beispielsweise komplette Webauftritte von erfundenen Transportfirmen mitsamt angeblichen Paket-Tracking-Systemen auf, um die Geschädigten möglichst lange im Glauben zu lassen, dass die bestellte oder versandte Ware sich noch im Transport befände. Auch sind die Täter bestens über aktuelle Gegebenheiten in der Schweiz informiert und machen sich diese zu Nutze. So wird beispielsweise die Wohnungsknappheit in Ballungsgebieten ausgenutzt, um von Wohnungssuchenden auf Immobilienplattformen über gefälschte Inserate für billigen Wohnraum in Zürich oder Basel Vorauszahlungen für Mietobjekte zu erschleichen, die gar nicht erst existieren.

Markant zugenommen hat die gemeldete Anzahl von Phishing-Versuchen. Mit einer Zunahme auf 2208 Meldungen des eingehenden Meldevolumens hat sich die totale Anzahl gegenüber dem Vorjahr (662 Meldungen) mehr als verdreifacht. Bei den meisten Varianten der gemeldeten Phishing-Versuche zielte die Täterschaft darauf ab, mittels nicht zielgerichtetem Massenversand von E-Mails ihre potentiellen Opfer auf Webseiten zu locken, die bekannten Internetdienstleistungen nachempfunden sind, und wo diese ihre Benutzerdaten (Benutzername, Passwort) angeben müssen.

Rund ein Fünftel der eingegangenen Meldungen zu Phishing betraf Versuche, an Zugangsdaten zu Dienstleistungen von Schweizer Bankinstituten zu kommen.

Im Bereich der Internetkriminalität im engeren Sinne ist eine erneute Zunahme der Meldungen von über 20 Prozent gegenüber dem Vorjahr zu verzeichnen. Einen markanten Anstieg haben insbesondere Meldungen zu Datenbeschädigungen (898 Meldungen, +124 Prozent) erfahren.

Im Bereich der Datenbeschädigung war ein häufig gemeldeter «Modus Operandi» das organisierte, nicht zielgerichtete Einschleusen von Schadsoftware auf Computer von Privatpersonen oder Firmen. Ein Beispiel für eine solche Schadsoftware sind Fälle so genannter «Ransomware» (Kombination aus den englischen Wörtern «Ransom» – Lösegeld und «Software»). Die Schadsoftware sperrt nach der Infektion den Computer der Opfer für jede weitere Aktivität und verlangt zur Aufhebung der Sperrung die Bezahlung eines Lösegeldes in Form eines Gutscheincodes eines anonymen Zahlungsdienstleisters. Im zweiten Halbjahr stieg zudem die Zahl der Meldungen über neue Varianten von Ransomware (sogenannte CryptoLocker), die auf dem Computer befindliche Daten zusätzlich verschlüsseln und somit unbrauchbar machen, um der Aufforderung zur Zahlung des geforderten Betrages mehr Druck zu verleihen.

Kleinere und mittlere Unternehmen (KMUs) wurden vermehrt durch gezielte Angriffe gegen ihren Webauftritt oder Telekommunikationsinfrastruktur geschädigt. Die Täter dringen dabei unbefugt in moderne Voice-over-IP-Telefonieanlagen (VoIP) der Geschädigten ein, um darüber Ferngespräche in afrikanische oder mittel- und südamerikanische Länder zu führen. Dies verursacht den betroffenen Betrieben erhebliche Kosten im Bereich von mehreren zehntausend Franken. Ein weiteres Ziel der Angriffe sind Kundendaten wie E-Mail-Adressen, Telefonnummern oder Rechnungsdaten, welche über Sicherheitslücken in Webseiten von Firmen beschafft werden. Obwohl kein direkter finanzieller Schaden entsteht, werden dennoch Folgekosten zur Sicherung des Datenbestandes, Einspielen eventueller Backups sowie Bereinigung der ausgenutzten Sicherheitslücken generiert. Auch entsteht oftmals ein Vertrauensverlust durch die Kundschaft, der einen nur schwer bezifferbaren finanziellen Schaden verursacht. Zudem werden die so gestohlenen Daten meist in weiteren Betrugsvarianten verwendet, beispielsweise, um fiktive Identitäten zu konstruieren oder E-Mail-Accounts zu übernehmen. Dies mit der Absicht, betrügerische Anfragen (z. B. Vorschussbetrug) zu verschicken.

3.2.2. Strafbare Handlungen gegen die sexuelle Integrität

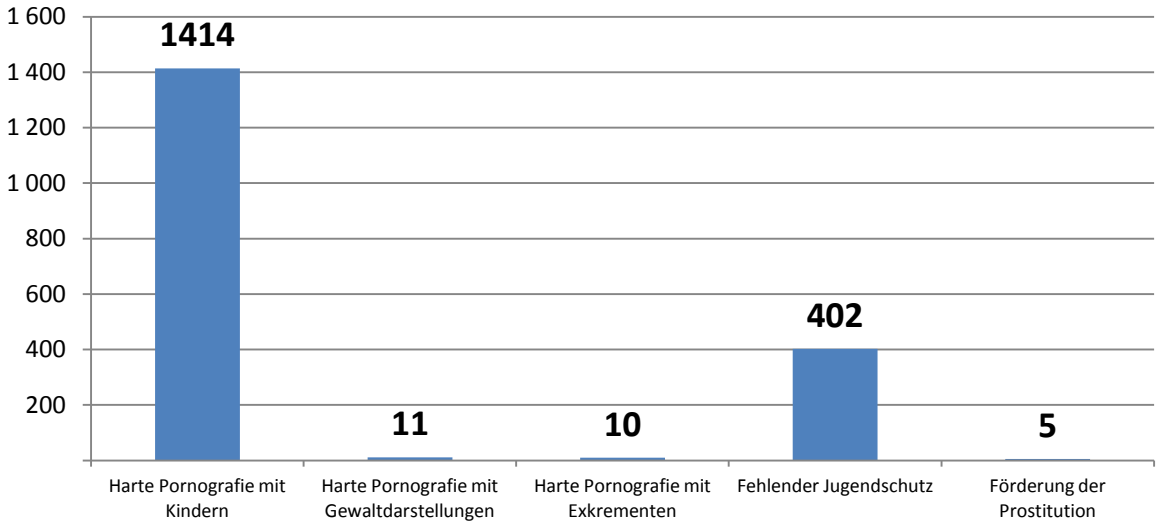


Abbildung 7 : Meldungseingang zu strafbaren Handlungen gegen die sexuelle Integrität (total 1842)

Der Zahl der Meldungen im Bereich der strafbaren Handlungen gegen die sexuelle Integrität hat sich im Berichtsjahr um fast 40 Prozent von 3083 im Vorjahr auf 1842 im Berichtsjahr reduziert. In 402 Fällen (307 im Vorjahr) wurde KOBIK auf Webseiten mit pornografischen Inhalten mit einem nach Ansicht des Melders ungenügenden Jugendschutz aufmerksam gemacht.

Die Zahl der gemeldeten Webseiten, die verbotene Pornografie mit Kindern anbieten, ist jedoch deutlich von 2684 Meldungen im Vorjahr auf 1414 Meldungen (-47 Prozent) gesunken.

3.2.3. Weitere strafbare Handlungen

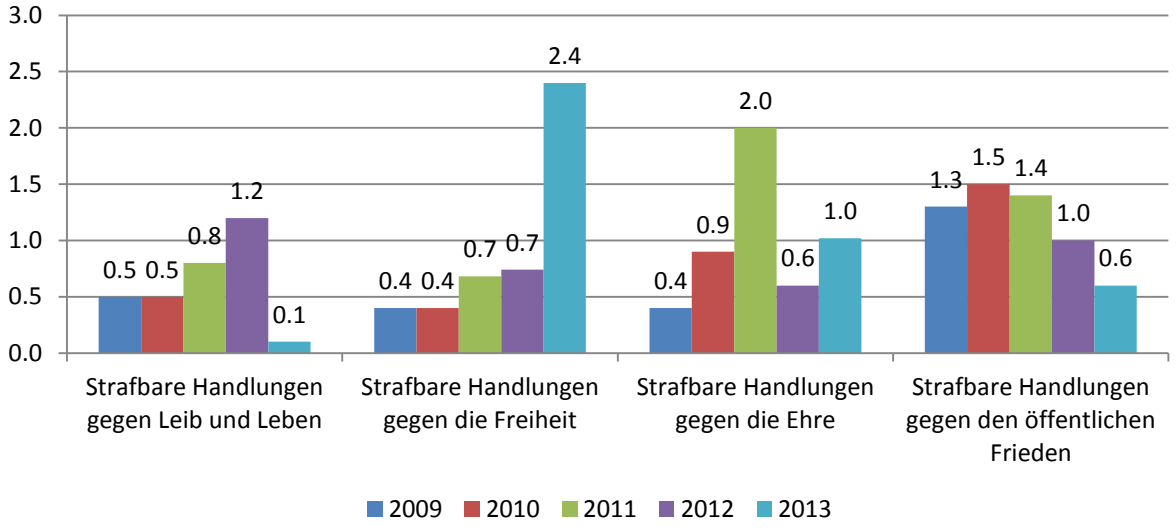


Abbildung 8 : Meldungseingang 2009–2013 zu weiteren StGB-Titeln (prozentualer Anteil aller Meldungen)

Etwa vier Prozent des Meldevolumens betraf die übrigen StGB-Titel der strafbaren Handlungen gegen Leib und Leben, die Freiheit, den öffentlichen Frieden und die Ehre. Insgesamt 2,4 Prozent der Meldungen betrafen strafbare Handlungen gegen die Freiheit. Die Melderinnen und Melder schilderten dabei meistens Fälle, in denen Personen über Online-Dating oder Social-Media Plattformen von einer meist weiblichen Täterschaft kontaktiert und zu sexuellen Handlungen vor laufender Kamera verführt wurden. Kurz darauf meldete sich die Täterschaft erneut und forderte die Bezahlung eines Schweigegeldes, da ansonsten Videoaufnahmen von den sexuellen Handlungen des Opfers im Internet veröffentlicht würden. Auch dieses Jahr blieb die Anzahl der gemeldeten strafbaren Handlungen gegen die Ehre relativ klein. Aufgrund der eingegangenen Meldungen lässt sich somit wie bereits im Vorjahr kein steigender Trend in dieser Deliktkategorie feststellen.

3.2.4. Zusammenfassung

Die Anzahl Meldungen bei Delikten gegen das Vermögen ist auch 2013 um einen Drittel weiter gestiegen. Die Tendenz des letzten Jahres hat sich somit bestätigt. Gleichzeitig ist die Anzahl Meldungen zu Delikten gegen die sexuelle Integrität um einen Drittel zurückgegangen. Neu steht nun auch die Deliktkategorie Phishing zusammen mit Betrug vor der Gesamtzahl der Meldungen der StGB-Titel der strafbaren Handlungen gegen die sexuelle Integrität.

3.3. 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:

- Insgesamt 9208 Meldungen wurden zeitgerecht auf allfällige strafrechtliche Relevanz geprüft und beurteilt.

- In 3457 von 9208 Fällen wurden die Melder mit einer persönlichen Antwort bedient.

- 35 Meldungen führten direkt und aufgrund der strafrechtlichen Relevanz zur Übermittlung des Sachverhaltes an den zuständigen Kanton oder die zuständige Behörde.

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

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

- Häufig gemeldete Sachverhalte führten zur Veröffentlichung von insgesamt neun Warnmeldungen auf der KOBIK-Webseite www.cybercrime.ch. Durch die Weiterleitung der Warnmeldung an MELANI, die Schweizerische Kriminalprävention (SKP) und die Medien konnte eine breite Öffentlichkeit über aktuelle Gefahren informiert werden.

3.4. Ausgewähltes Fallbeispiel

KOBIK wurde von einem Schweizer Hostingprovider kontaktiert, der feststellte, dass eine unbekannte Täterschaft seine Dienste zum Betrieb eines Online-Shops für gestohlene Kreditkartendaten missbrauchte. Die gestohlenen Informationen sowie Log-Dateien wurden vom Provider freiwillig übermittelt. KOBIK leitete die entsprechenden Daten an Europol weiter, wo das European Cybercrime Center (EC3) die technische Analyse der Daten vornahm und die entsprechenden Kreditinstitute zwecks Sperrung der kompromittierten Karten kontaktierte.

4. Aktive Recherchen durch KOBIK (Monitoring)

KOBIK ist durch verdachtsunabhängige Recherchen auch in den für die allgemeine Bevölkerung weniger zugänglichen Bereichen des Internets präsent und versucht dabei, eine präventive Wirkung zu erzielen. Der Leitungsausschuss KOBIK legt den Schwerpunkt dieser aktiven Recherchen jedes Jahr neu fest. Wie bereits in den Vorjahren wurde dieser für das Jahr 2013 auf die Bekämpfung der Pädokriminalität im Internet gesetzt. Aufgrund der weiter steigenden Anzahl Meldungen zu Wirtschaftsdelikten hat der Leitungsausschuss für das Jahr 2013 jedoch ausdrücklich festgehalten, dass sich KOBIK den Wirtschaftsdelikten und der Internetkriminalität im engeren Sinn nicht verschliessen darf. In der Praxis hat sich dieser Entscheid insbesondere auf die Koordinationstätigkeit und die Vorermittlungen durch KOBIK ausgewirkt (siehe Kapitel 5.2).

Aufgrund der aktiven Recherchen wurden 2013 insgesamt 423 Anzeigen erstellt. Dies entspricht einer leichten Abnahme von sechs Prozent gegenüber dem Vorjahr.

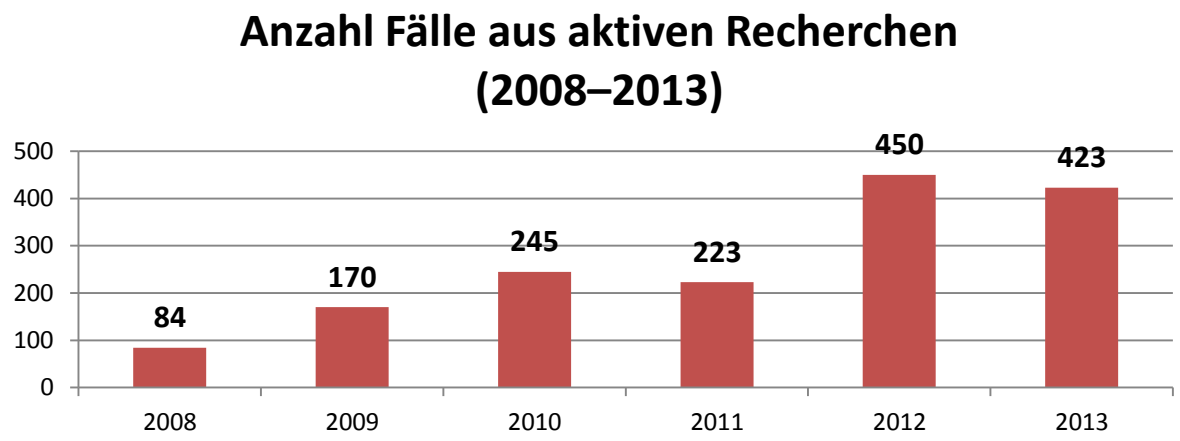


Abbildung 9 : Im Rahmen aktiver Recherchen eröffnete Strafverfahren (2008–2013)

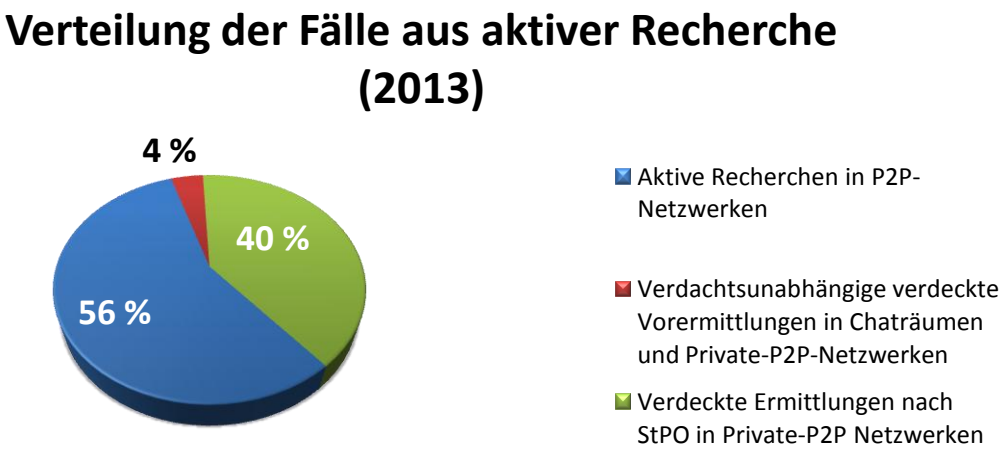


Abbildung 10 : Herkunft der Strafanzeigen aus aktiver Recherche (Total 423)

4.1. Aktive Recherchen in Peer-to-Peer-Netzwerken (P2P)

238 der 423 Anzeigen resultieren aus den aktiven Recherchen von KOBIK in öffentlichen Peer-to-Peer-Tauschbörsen. Die Dossiers richten sich gegen Internetbenutzer, die aktiv harte Pornografie mit Kindern gemäss Art. 197 Abs. 3 StGB austauschen. Die Anzahl der gemeldeten Fälle ist im Vergleich zum Vorjahr (450) um 47,1 Prozent zurückgegangen. Damit sank die Zahl der versendeten Dossiers auf das Niveau des Berichtsjahres 2011, obwohl das Monitoring mit der gleichen Intensität und denselben Kriterien wie 2012 durchgeführt wurde.

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

4.2. Verdachtsunabhängige verdeckte Vorermittlungen

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 regelt die Modalitäten des Einsatzes von KOBIK-Mitarbeitenden als verdeckte Vorermittler zur Bekämpfung der Pädokriminalität im Internet[8]. 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 2013 in insgesamt 17 Fällen zu Strafanzeigen zuhanden der zuständigen Kantone. Drei dieser Strafanzeigen basieren dabei auf Ermittlungen in speziell für Kinder vorgesehenen Chaträumen. In allen drei Fällen lautete die Anzeige auf versuchte sexuelle Handlungen mit Kindern nach Art. 187 StGB.

Die verbleibenden 14 Fälle beruhen auf verdeckten Vorermittlungen in sogenannten «privaten P2P-Tauschbörsen». Im Gegensatz zu den klassischen P2P-Netzwerken findet der Austausch der Dateien über eine öffentlich nicht einsehbare, verschlüsselte Direktverbindung der beteiligten Computer statt, weshalb für die Kontaktaufnahme mit den Tätern die Bestimmungen der verdeckten Vorermittlung Anwendung finden. Die meisten Anzeigen bei dieser Art der Ermittlungen lauteten auf den Besitz und die Verbreitung von verbotener Pornografie gemäss Art. 197 Abs. 3 oder Abs. 3bis StGB.

4.3. Verdeckte Ermittlungen nach StPO

Zum ersten Mal in der zehnjährigen Geschichte wurde KOBIK von kantonalen Staatsanwaltschaften ersucht, als direkt unterstellte Behörde verdeckte Ermittlungen

[8] Einsatz im Sinne von § 9d des Gesetzes des Kantons Schwyz über die Kantonspolizei vom 22.03.2000 (PolG – SRSZ 520.110).

in einem kantonalen Verfahren und gestützt auf die Strafprozessordnung (StPO) zu tätigen. Diese verdeckten Ermittlungen gemäss Art. 285a ff. StPO fanden ausschliesslich in privaten P2P-Tauschbörsen statt. Aufgrund dieser Ermittlungen erstellte KOBIK insgesamt 168 Anzeigen, welche an die zuständigen Polizeibehörden im In- und Ausland versendet wurden.

Aufgrund der globalen Umspannung der privaten P2P-Community ist die Fokussierung auf Schweizer Straftäter in solchen Fällen schwierig. Im Rahmen der angeordneten Ermittlungen konnten zwei Schweizer Benutzer identifiziert werden. Die restlichen 166 Anzeigen gingen im Rahmen des internationalen polizeilichen Informationsaustausches an ausländische Strafverfolgungsbehörden.

4.4. Feedback aus den Kantonen

Bei begründetem Verdacht auf eine Straftat leitet KOBIK Fälle zuständigkeitshalber an die Kantone weiter. Um eine Gesamtübersicht über die in den Kantonen eingeleiteten Massnahmen zu gewinnen, ersucht KOBIK die Kantone um Informationen über den weiteren Verlauf der ihnen angezeigten Verdachtsfälle (eingeleitete polizeilichen Massnahmen und/oder Ausgang des Gerichtsverfahrens).

Damit zeitnahe Entwicklungen besser erkannt werden können, wurden nachfolgend lediglich die im Berichtsjahr eingegangenen Rückmeldungen aus den Kantonen berücksichtigt. Die grosse Mehrheit der Anzeigen resultiert aus den aktiven Recherchen in P2P-Netzwerken aus dem Jahr 2012 (417). Die Dossiers betreffen somit Personen, die sich aktiv am Austausch von strafbaren Inhalten mit kinderpornografischem Charakter beteiligten.

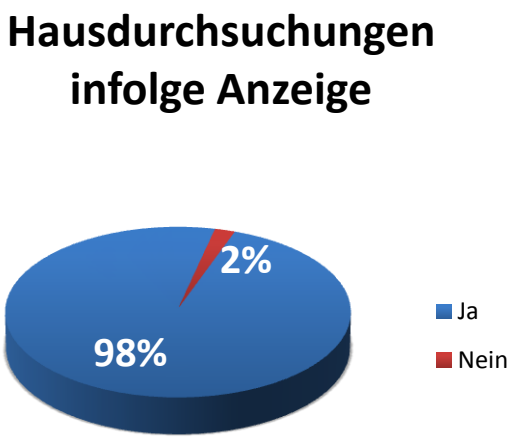


Abbildung 11 : Hausdurchsuchungen 2013

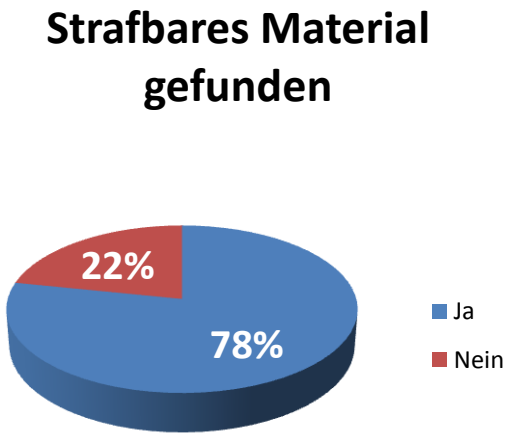


Abbildung 12 : Strafbares Material 2013

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

4.4.1. Rückmeldungen der kantonalen Polizeibehörden

Bei 78 Prozent der Hausdurchsuchungen, die aufgrund der Anzeigen von KOBIK durchgeführt wurden, konnte illegales Material beschlagnahmt werden. Die Gründe für eine erfolglose Hausdurchsuchung sind vielfältig. So verunmöglichen beispielsweise in der Regel offene und ungeschützte Drahtlosnetzwerke oder die Auslagerung der Daten auf Cloud-Dienste eine effiziente Beweissicherung sowie eine eindeutige Identifizierung der Verdächtigen.

Bei den sichergestellten strafbaren Inhalten handelte es sich bei 93 Prozent um kinderpornografisches Material. Da bei den aktiven Recherchen in P2P-Netzwerken gezielt nach Straftaten dieser Art gesucht wird und die Mehrheit aller Anzeigen aus diesen Recherchen stammen, erstaunt dieser hohe Prozentsatz nicht. Erwähnenswert ist jedoch, dass in mehr als der Hälfte der Fälle zusätzlich Vergehen gegen weitere Tatbestände der verbotenen Pornografie (Art. 197 StGB) festgestellt wurden (vgl. Abb. 14). Bei mehr als jeder zweiten Hausdurchsuchung wurde auch Pornografie mit Tieren sichergestellt.

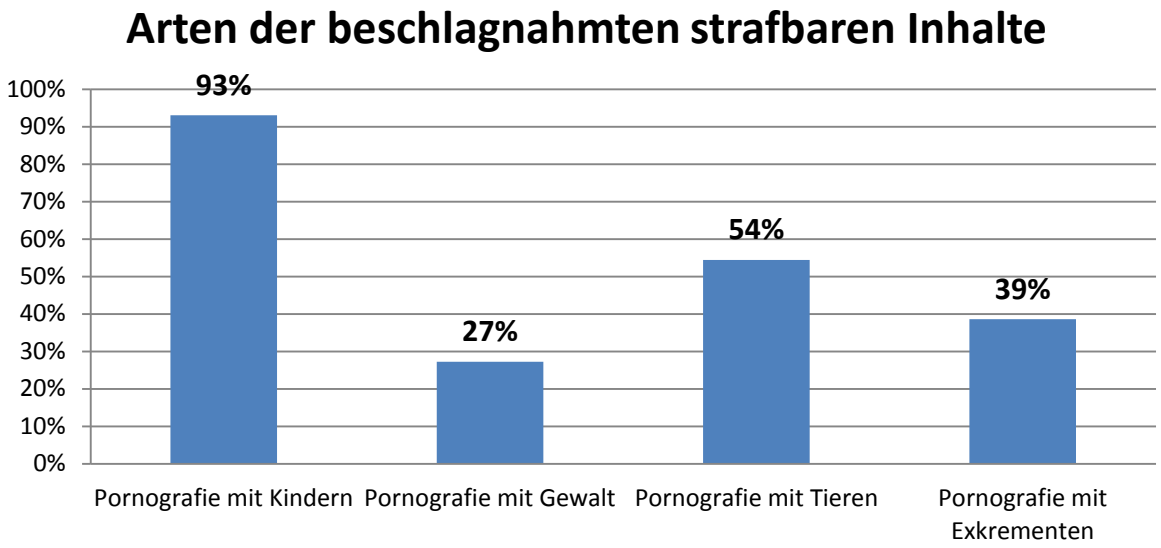
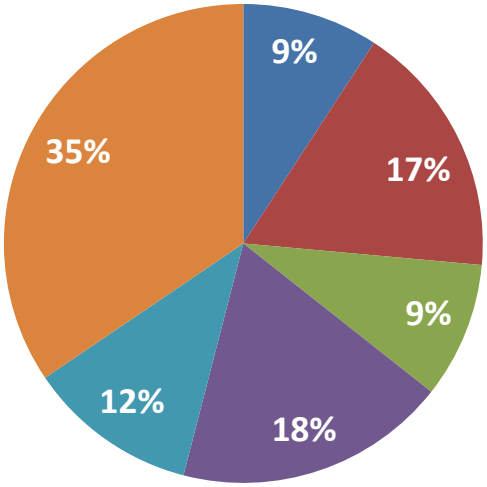


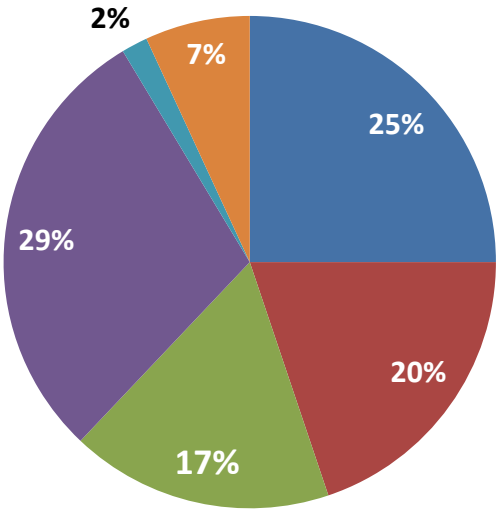
Abbildung 13 : Welche Arten von Material wurden 2013 bei Hausdurchsuchungen beschlagnahmt?

Aus den Rückmeldungen der kantonalen Polizeibehörden geht weiter hervor, dass bei 94 Prozent der erfolgreichen Hausdurchsuchungen Videodateien und in 66 Prozent 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.

Anzahl beschlagnahmter Bilddateien anlässlich der Hausdurchsuchungen



Anzahl beschlagnahmter strafbarer Videodateien anlässlich der Hausdurchsuchungen



1 - 10 Bilder / Videos
11 - 50 Bilder / Videos
51 - 100 Bilder / Videos
101 - 500 Bilder / Videos
501-1000 Bilder / Videos
> 1000 Bilder / Videos

Abbildungen 14 und 15 : Überblick über Art und Menge der beschlagnahmten Bild- und Videodateien

4.4.2. Rückmeldungen der kantonalen Justizbehörden

In 91 Prozent der Fälle, in denen die kantonalen Justizbehörden KOBIK eine Rückmeldung erstatteten, führten die Strafverfahren zu einer Verurteilung.

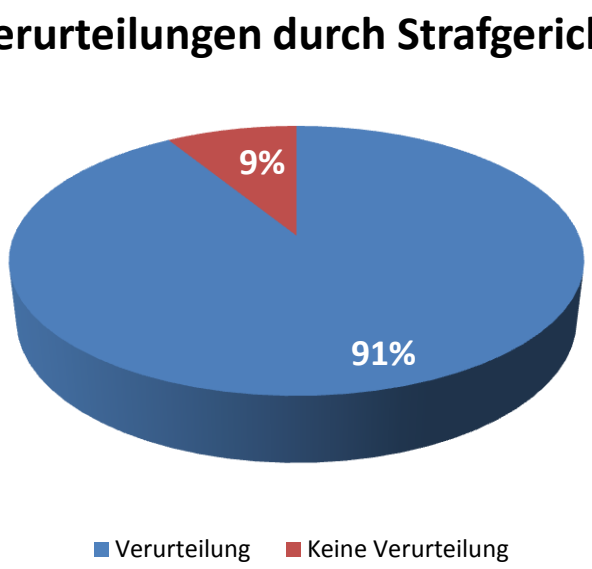


Abbildung 16 : Verurteilung durch Strafgericht, 2013

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.

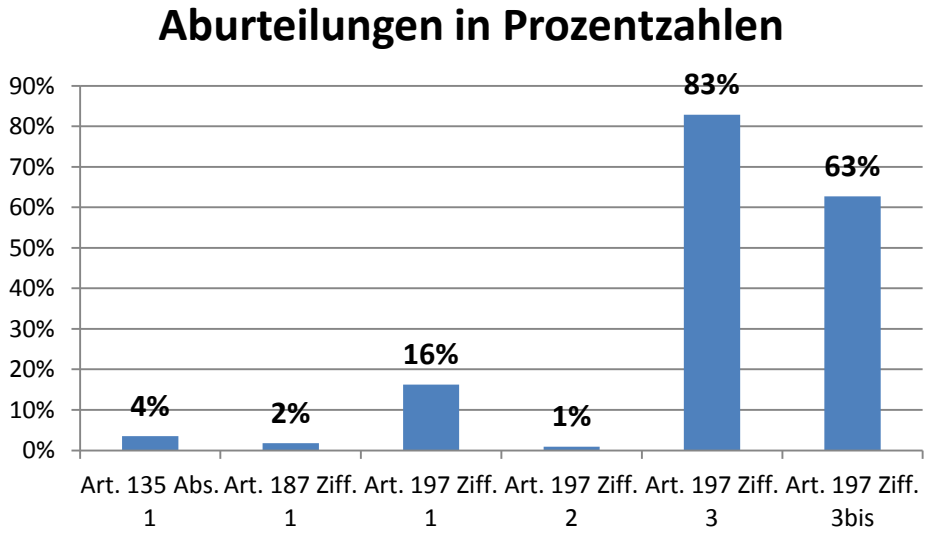


Abbildung 17 : Häufigste Aburteilungen in Prozentzahlen, 2013

Bei 85 Prozent der im Berichtsjahr gemeldeten Verurteilungen wurde eine Geldstrafe (Tagessatz) ausgesprochen. In 77 Prozent dieser Fälle wurde gleichzeitig eine Busse verhängt. Die Geldstrafen wurden bei 91 Prozent der Verurteilungen auf Bewährung ausgesetzt. Gemeinnützige Arbeit, Therapien, Freiheitsentzug (Gefängnis) oder

nicht auf Bewährung ausgesetzte Geldstrafen wurden in vier Prozent der Verurteilungen verhängt.

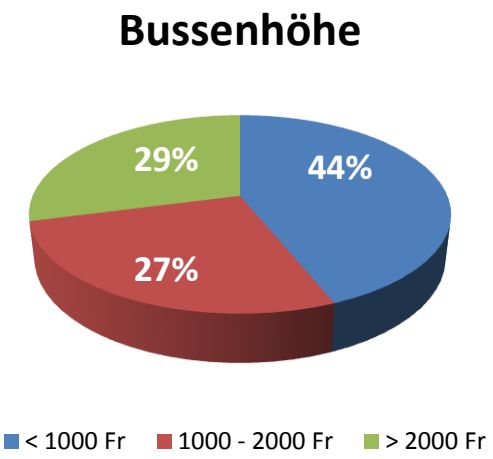


Abbildung 18 : Bussenhöhe bei Verurteilung

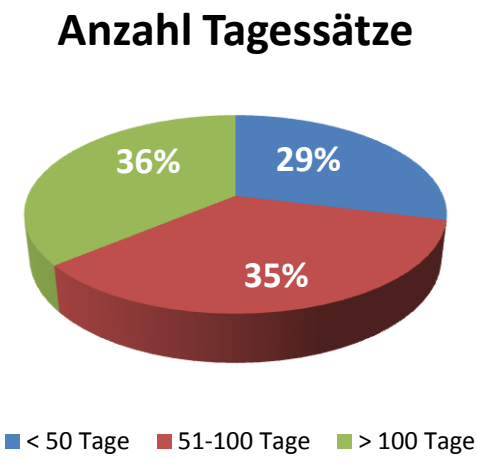


Abbildung 19 : Anzahl Tagessätze bei Verurteilung

In etwa 44 Prozent der Fälle beliefen sich die Bussen auf weniger als 1000 Franken; in 27 Prozent auf 1000 bis 2000 Franken. Lediglich 29 Prozent der Bussen waren höher als 2000 Franken.

29 Prozent der Geldstrafen wurden bei 50 oder weniger Tagessätzen festgelegt. Bei 36 Prozent wurden jeweils zwischen 51 und 100 Tagessätze angeordnet. Geldstrafen über mehr als 100 Tagessätze wurden in 36 Prozent der Fälle gesprochen.

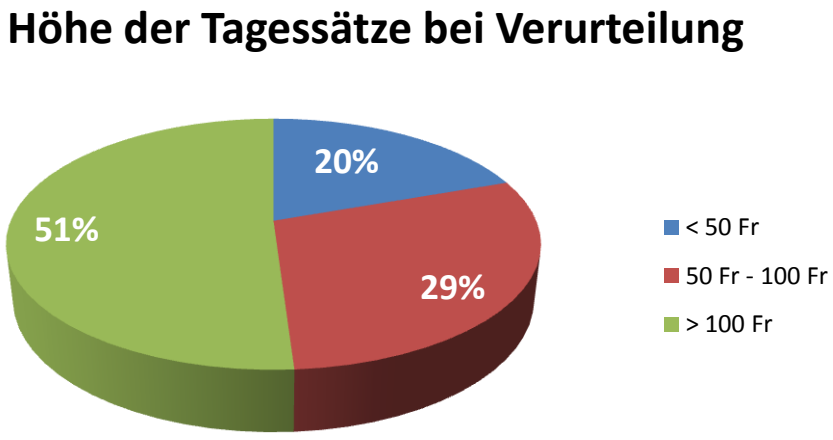


Abbildung 20 : Höhe der Tagessätze bei Verurteilung

In 20 Prozent der Fälle wurden Tagessätze in der Höhe von 1 bis 50 Franken, in 29 Prozent der Fälle zwischen 51 und 100 Franken und in 51 Prozent über 100 Franken festgesetzt.

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

4.5. Ausgewählte Fallbeispiele

Im Berichtsjahr konnten insgesamt drei Straftäter identifiziert und verhaftet werden, die auf Chatplattformen für Kinder auf der Suche nach sexuellen Kontakten mit Minderjährigen waren. In einem Fall drängte die Täterschaft bereits nach wenigen Minuten Konversation auf ein Treffen und äusserte die Absicht, mit dem als Mädchen auftretenden verdeckten Vorermittler von KOBIK sexuelle Handlungen vornehmen zu wollen. In der Folge gelang es der zuständigen Kantonspolizei, den Pädokriminellen anzuhalten, der mit einem Messer bewaffnet zum Treffen mit dem angeblich 13-jährigen Mädchen unterwegs war. Dieser Fall zeigt insbesondere auf, dass die Gefahr von in Kinder-Chats agierenden Sexualstraftätern nicht zu unterschätzen ist.

Im Bereich der aktiven Recherchen in P2P-Netzwerken konnte auch in diesem Jahr ein Fall von aktivem Kindsmissbrauch aufgedeckt werden. KOBIK übermittelte hierzu mehrmalig Anzeigen wegen illegaler Verbreitung von Pornographie in P2P-Netzwerken an die zuständige Kantonspolizei. Die Ermittlungen führten zur Erkenntnis, dass der gemeinsam mit Frau und Kindern lebende Familienvater seine eigene dreijährige Tochter über mehrere Monate hinweg sexuell missbraucht hatte. Der Täter war bis zum Zeitpunkt der Anzeige durch 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 vor weiterem Missbrauch geschützt werden.

In einem anderen Fall führten die aktiven Recherchen zu einem deutschen Staatsangehörigen, der aktiv an der Verbreitung von Kinderpornografie in einem privaten P2P-Netzwerk beteiligt war. KOBIK übermittelte den Fall via Interpol an Deutschland. Wie die zuständige Staatsanwaltschaft bekannt gab, handelt es sich beim Täter um einen 45 jährigen Geschäftsführer eines Jugendvereins. Zu den Schwerpunkten des Vereins gehörten nach eigenen Angaben «Fragen rund um den Kinder- und Jugendschutz, einschliesslich Gewalt, Pornografie, Cybermobbing, Altersfreigaben, Jugendschutzsoftware, Internetsicherheit, Computerspiele, Smartphones oder Medienprojektberatung». Der Verein wurde vom entsprechenden Bundesland mitfinanziert.

Diese Fälle zeigen auf, wie wichtig eine systematische Fallbearbeitung der übermittelten Anzeigen durch die kantonalen Behörden sind. Aufgrund der knappen Ressourcen sind einige Kantone bei der Bearbeitung der zahlenmässig konstant hohen KOBIK-Dossiers stark gefordert. Es ist teilweise eine grosse Herausforderung, den enormen zusätzlichen Arbeitsaufwand zeitgerecht bewältigen zu können.

5. Kriminalpolizeilicher Informationsaustausch

5.1. Meldungsein- und Ausgang

Mit der Einbettung von KOBIK in die Bundeskriminalpolizei im Jahre 2009 und dem Entscheid des Leitungsausschusses, wonach sich KOBIK den Wirtschaftsdelikten und der Internetkriminalität im engeren Sinn nicht verschliessen darf, hat der kriminalpolizeiliche Informationsaustausch mit dem In- und Ausland an Bedeutung gewonnen. KOBIK ist zur Drehscheibe für den Informationsfluss geworden. Die Kantone werden in ihren Ermittlungen durch KOBIK als koordinierendes Kompetenzzentrum mit der Sicherstellung des Informationsaustausches unterstützt. Dies nicht zuletzt, da KOBIK ein grosses Netzwerk im Ausland und in den Kantonen sowie in der Privatwirtschaft und im öffentlichen Sektor unterhält. Zudem bildet KOBIK eine Schnittstelle zu den internationalen Organisationen Interpol und Europol und insbesondere auch zum European Cybercrime Center (EC3).

Seit Inkrafttreten des Übereinkommens über die Internetkriminalität des Europarates (Cybercrime Convention, CCC) am 1. Januar 2012, wird die Schweiz international als aktiver Partner in der Bekämpfung der Internetkriminalität wahrgenommen. Dies wird vor allem beim markanten Anstieg des kriminalpolizeilichen Informationsaustausches mit ausländischen Behörden zu Sachverhalten deutlich, die unter den Anwendungsbereich des Übereinkommens fallen. Die nachfolgenden Zahlen zeigen dies klar auf.

2013 sind insgesamt 739 Meldungen zum Anwendungsbereich des Übereinkommens eingegangen. Das entspricht einem Anstieg von über 53 Prozent gegenüber dem Vorjahr. 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 im Auftrag der Kantone und in eigener Kompetenz insgesamt 946 Meldungen ans Ausland (Interpol und Europol), was einem Anstieg von über 68 Prozent entspricht.

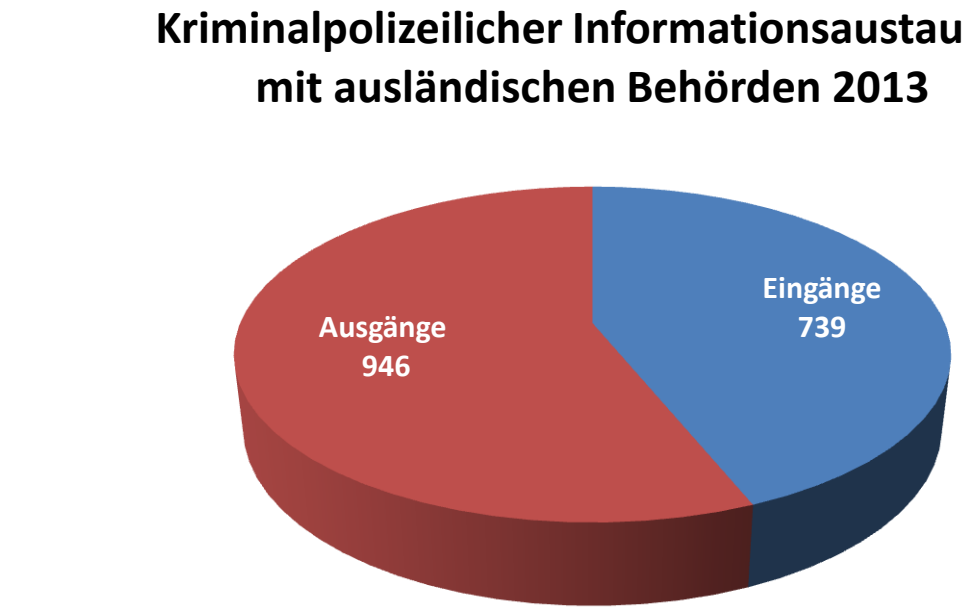


Abbildung 21 : Kriminalpolizeilicher Informationsaustausch mit dem Ausland

Eine Besonderheit der Cybercrime Convention ist die Möglichkeit, auf dem polizeilichen Wege unter in Aussichtstellung eines Rechtshilfeersuchens die sofortige Sicherstellung von Daten zu veranlassen (Art. 29 ff.). Diesbezüglich hat KOBIK acht Anfragen der Kantone an ausländische Behörden weitergeleitet. Umgekehrt wurden von ausländischen Polizeistellen vier Ersuchen weitergeleitet.

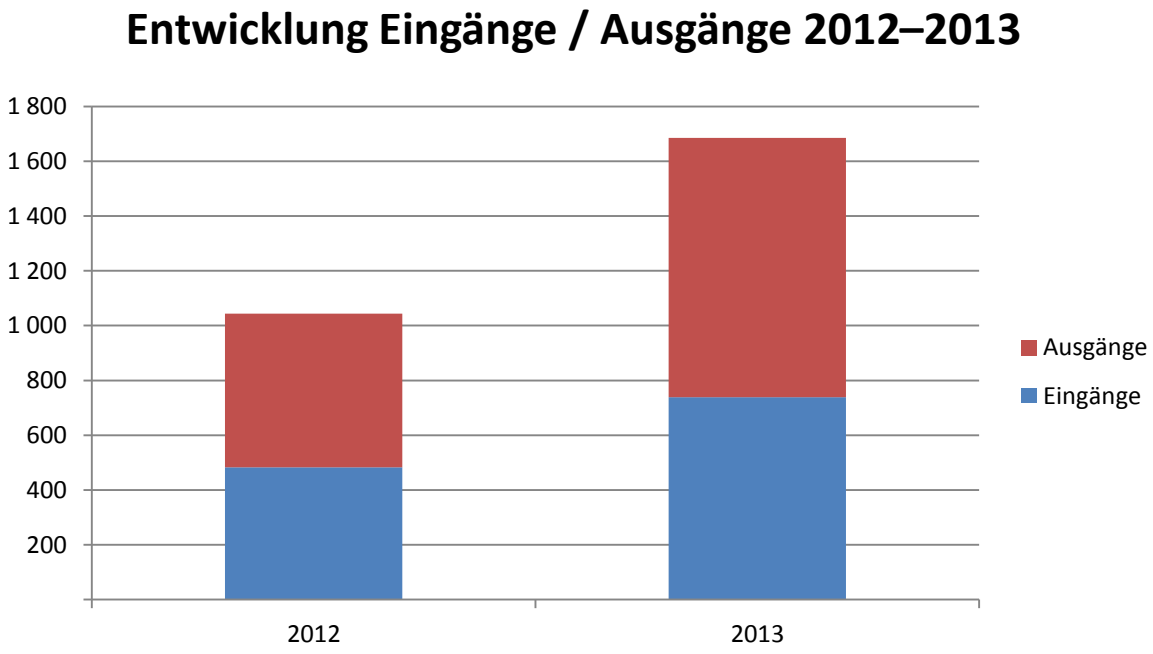


Abbildung 22 : Entwicklung Kriminalpolizeilicher Informationsaustausch 2012–2013

5.2. Nationale und internationale Verfahrenskoordination

Im Rahmen des kriminalpolizeilichen Informationsaustausches drängten sich in rund 180 Fällen koordinierende Massnahmen auf.

Die Art der Unterstützung und die Rolle von KOBIK sind abhängig von der konkreten Ausgangslage. Koordinierend wird KOBIK insbesondere im Rahmen internationaler Ermittlungsverfahren tätig. In diesen Fällen ist KOBIK nationale Ansprechstelle für in- und ausländische Strafverfolgungsbehörden und am Verfahren beteiligte Stellen und Personen. Bei anderen Fällen, insbesondere solchen mit kantonaler Zuständigkeit, unterstützt KOBIK die zuständigen Stellen mit analytischen, technischen und rechtlichen Expertisen oder mit dem Einsatz von verdeckten Ermittlern.

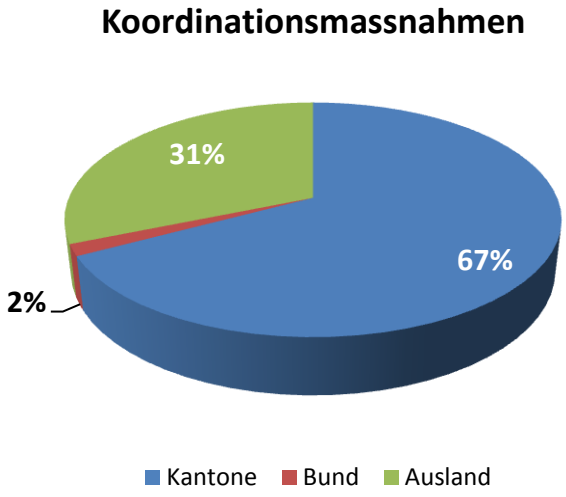


Abbildung 23 : Prozentuale Aufteilung der Koordinationsmassnahmen

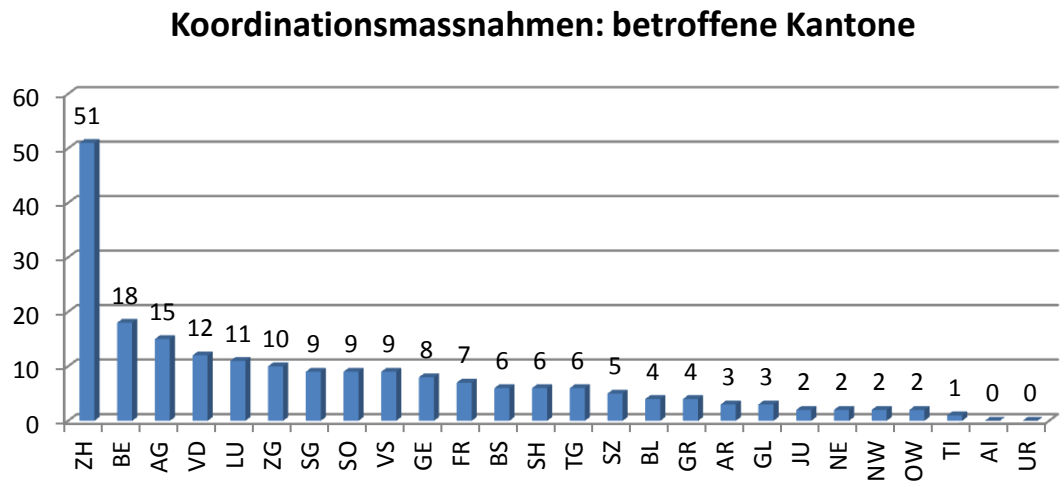


Abbildung 24 : von Koordinationsmassnahmen betroffene Kantone

Der Kanton Zürich war durch überdurchschnittlich viele Massnahmen betroffen. Bei genauerer Betrachtung lassen sich insbesondere zwei massgebende Faktoren eruieren. Einerseits ist Zürich als Wirtschaftszentrum auch Standort für viele wichtige nationale und globale Informations- und Kommunikationsunternehmen. Andererseits hat der Kanton Zürich mit der Schaffung des kantonalen Kompetenzzentrums Internetkriminalität eine optimale Ausgangslage geschaffen, um Ermittlungsverfahren im digitalen Raum führen oder im Rahmen internationaler Ermittlungen einen Beitrag leisten zu können.

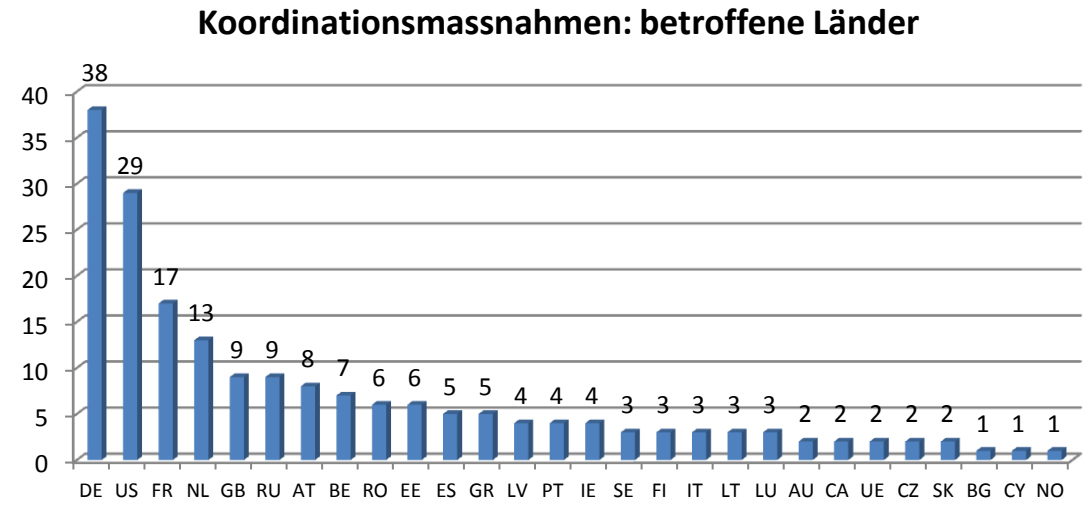


Abbildung 25 : von Koordinationsmassnahmen betroffene Länder

Im Rahmen internationaler Ermittlungen ist KOBIK zentraler Ansprechpartner und Bindeglied zwischen den nationalen und internationalen Verfahrensbeteiligten. Dadurch ist sichergestellt, dass die Schweiz über eine zentrale Fall- und Informationsübersicht verfügt und die notwendigen Schritte im In- und Ausland sicherstellen kann.

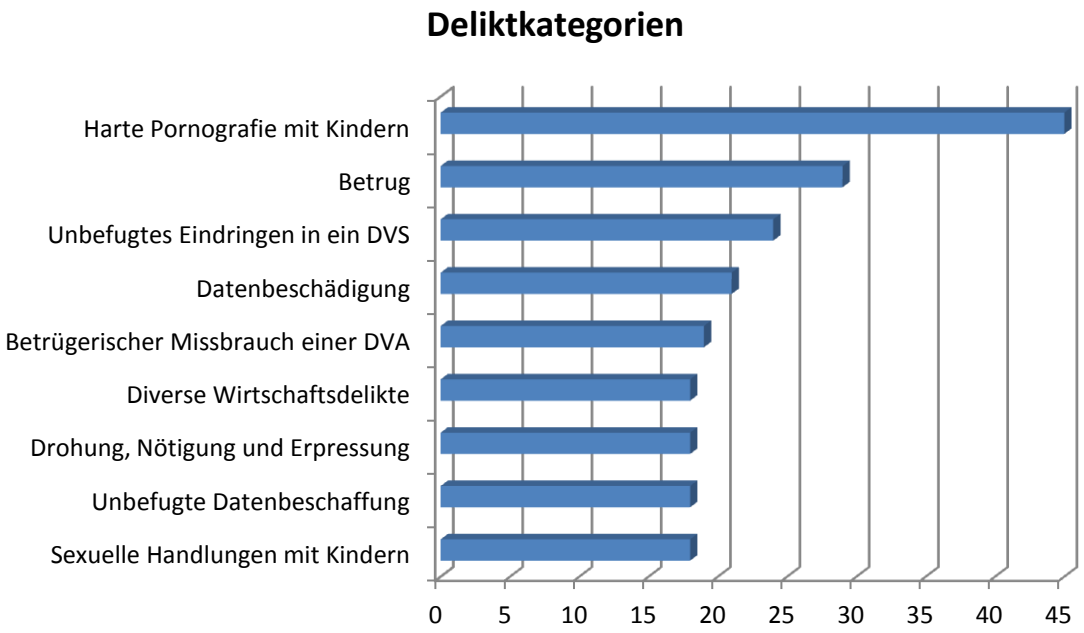


Abbildung 26 : Aufteilung der Koordinationsmassnahmen 2013 nach Deliktkategorien

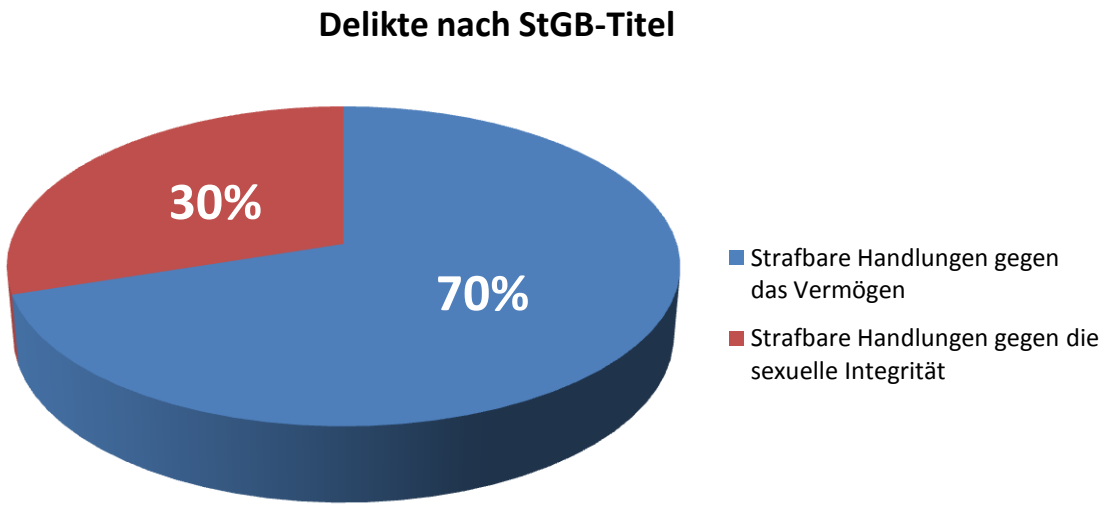
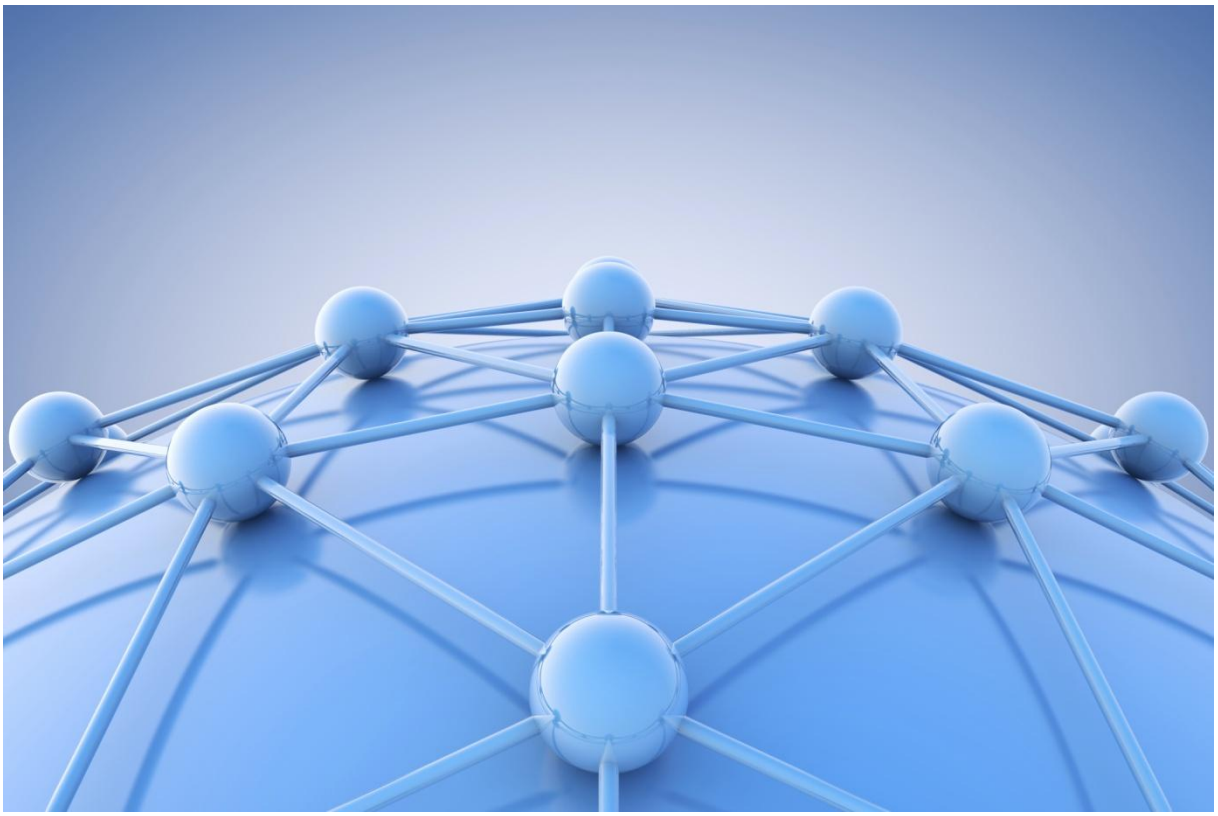


Abbildung 27 : Aufteilung der Koordinationsmassnahmen 2013 nach StGB-Titel

5.3. Ausgewählte Fallbeispiele

Vom BKA Wiesbaden ging bei KOBIK eine Meldung ein, wonach eine unbekannte Täterschaft in die Computersysteme einer der grössten landesweiten Telekommunikationsanbieter eingedrungen ist und die gestohlenen Daten über einen Server in der Schweiz leitet. Innerhalb weniger Stunden konnte KOBIK mit dem zuständigen Cybercrime Kompetenzzentrum in Zürich Kontakt aufnehmen und die Sicherung von Verbindungs- und Inhaltsdaten gemäss Art. 29 der Cybercrime Convention veranlassen. Eine erste Analyse erlaubte es, die Täter nach Deutschland zurück zu verfolgen. Nach Rücksprache mit der ermittelnden Stelle wurde zwei Tage später eine erneute Sicherung und Analyse des fraglichen Servers vorgenommen. Dabei wurde festgestellt, dass die Täterschaft die Spuren bereits grösstenteils verwischt hatte. Hätte die Sicherung erst zu diesem Zeitpunkt stattgefunden, so wäre es praktisch unmöglich gewesen, die Täterschaft noch zu identifizieren.



KOBIK wurde auch in die Koordination zur Vollstreckung von Rechtshilfeersuchen aus dem Ausland einbezogen. Ein Beispiel dafür ist der Takedown von Liberty-Reserve durch den US Secret Service (USSS). KOBIK wurde als koordinierendes Element zwischen dem Bundesamt für Justiz, dem USSS, der Bundesanwaltschaft und der Bundeskriminalpolizei beigezogen. Bereits im Vorfeld wurde KOBIK durch den USSS zwecks Verbindungsaufnahme mit den beteiligten Stellen und Vorabklärungen kontaktiert, da ansonsten die Zeit zwischen Eingang des Rechtshilfeersuchens beim Bundesamt für Justiz und der geplanten Vollstreckung zu kurz gewesen wäre. Dank der koordinierenden Funktion von KOBIK als zentraler Ansprechpartner und Vermittlerin in diesem Falle konnten sich die beteiligten Stellen auf ihre wesentlichen Aufgaben in der Vorbereitung konzentrieren und die im Rechtshilfeersuchen gewünschte Sicherung des Servers vollstrecken.

6. Projekte

6.1. 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 gutgeheissen. Mit der Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, denen 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 bei den Verantwortlichen eine Informationsgrundlage über Cyber-Risiken geschaffen und ihre Wahrnehmung dafür geschärft werden.

Dazu erteilt der Bundesrat den Departementen den Auftrag, die Umsetzung der insgesamt sechzehn 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 auf internationaler Ebene.

Die Massnahme 6 sieht vor, dass auf nationaler Ebene eine möglichst vollständige Fallübersicht (Straffälle) geführt wird und interkantonale Fallkomplexe koordiniert werden müssen. Die gewonnenen 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 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 hat KOBIK die Koordination und die Auftragserfüllung im Zusammenhang mit den Umsetzungsarbeiten zur Strategie NCS für fedpol sicherzustellen, wobei die Projektleitung durch den Chef der Bundeskriminalpolizei wahrgenommen wird.

Im Rahmen des Projekts geht es in einem nächsten Schritt darum, die verschiedenen Aufgaben im Zusammenhang mit der Entwicklung und Organisation der Fallübersicht anzugehen und zusammen mit den Kantonen ein tragfähiges Konzept zum Aufbau einer gesamtschweizerischen Fallübersicht und zur Koordination interkantonaler Fallkomplexe zu erarbeiten. Dabei geht es insbesondere um die Klärung von organisatorischen, technischen, rechtlichen, ressourcenmässigen (z.B. Personal, Infrastruktur, Informatik usw.) sowie fachlichen Aspekten und Fragestellungen. In einem ersten Schritt wurde bereits eine detaillierte Auftragsanalyse erstellt und die Projektorganisation bestehend aus Vertretern von fedpol, der KKJPD, der KKPKS, der SSK (ehemals KSBS), einem Vertreter der Swiss Police ICT (Anspruchsgruppe) sowie einem Vertreter der Bundesanwaltschaft und des Bundesamts für Justiz (Anspruchsgruppe) definiert. Bereits 2014 soll das Konzept zwei Mal bei den Kantonen und beteiligten Stellen in die Vernehmlassung gehen.

6.2. KOBIK goes Social Media

Als Meldestelle muss sich KOBIK ständig den neusten Entwicklungen im und um das Internet anpassen. Die technische Entwicklung verändert die Kommunikationsangebote und entsprechend auch die Mediennutzung. KOBIK erhält vermehrt auch Meldungen zu möglichen strafbaren Inhalten oder Verhalten in Zusammenhang mit Facebook.

In Anbetracht dieser Ausgangslage beantragte KOBIK beim Leitungsausschuss KOBIK verschiedene Massnahmen zum besseren Kundendialog. Der Leitungsausschuss entschied, dass KOBIK künftig unter anderem über ein eigenes Facebook- und Twitter-Profil verfügen soll und dass die Aufschaltung der neuen Kommunikationskanäle im Rahmen des zehnjährigen Jubiläums von KOBIK erfolgen soll. Am 22. Dezember 2013 wurden die neuen Profile[9] in drei Sprachen aufgeschaltet und stehen der Bevölkerung seither zur Verfügung.

[9] www.facebook.com/cybercrime.ch und auf Twitter @KOBIK_Schweiz

7. Arbeitsgruppen, Partnerschaften und Kontakte

7.1. Nationale Datei- und Hashwertesammlung (NDHS)

Seit Oktober 2012 ist die NDHS in Betrieb und steht den kantonalen und städtischen Fachstellen zur Verfügung. Damit die NDHS effizient genutzt werden kann, müssen genügend bekannte Bilder kategorisiert und die entsprechenden Hashwerte erstellt sein. Die Kategorisierung von Bildmaterial ist sehr zeitaufwändig und kann aufgrund der beschränkten Ressourcen von KOBIK nur mit der Unterstützung der Kantone sichergestellt werden.

7.2. Nationale Arbeitsgruppen

KOBIK war im Berichtsjahr in verschiedenen nationalen Arbeitsgruppen vertreten.

Im Berichtsjahr organisierte KOBIK zusammen mit dem Kommissariat Pädokriminalität/Pornografie der Bundeskriminalpolizei das jährliche Treffen der Arbeitsgruppe «Kindsmissbrauch». Gemeinsam mit gemeinnützigen Organisationen, Kantonsvertretern und der Schweizerischen Kriminalprävention geht die Arbeitsgruppe aktuelle Fragestellungen zum Thema Kindsmissbrauch und deren Bekämpfung an.

Wie bereits in den Vorjahren war KOBIK auch 2013 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 in der Fachkommission der «Schweizerischen Kriminalprävention (SKP)» vertreten. Die Kommission entwickelt Projekte und Materialien für die Kriminalprävention in den Kantonen und evaluiert deren Umsetzung.

KOBIK ist 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.

7.3. 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/Pornografie, IT-Ermittlungen und Verdeckte Ermittlungen der Bundeskriminalpolizei aber auch mit der Hauptabteilung Internationale Polizeikooperation (IPK) im Vordergrund. Aufgrund des gemeinsamen Aufgabengebietes besteht zwischen dem Kommissariat Pädokri-

minalität/Pornografie und KOBIK eine besonders intensive Zusammenarbeit. Weiter konnten departementsübergreifend diverse Kontakte mit Bundesstellen ausgebaut und intensiviert werden. Zu erwähnen sind unter anderem MELANI, die Abteilung internationale Rechtshilfe im Bundesamt für Justiz (BJ), das Bundesamt für Informatik und Telekommunikation (BIT), das Bundesamt für Sozialversicherungen (BSV), das Bundesamt für Kommunikation (BAKOM), die Eidgenössische Kommission gegen Rassismus (EKR), die Eidgenössische Zollverwaltung (EZV), die Eidgenössische Alkoholverwaltung (EAV), die Finanzmarktaufsicht (FINMA), das Institut für Geistiges Eigentum (IGE) und die Eidgenössischen Spielbankenkommission (ESBK).

7.4. Erfahrungsaustausch mit den Kantonen

Im Berichtsjahr pflegte KOBIK zahlreiche Kontakte mit Vertretern diverser Polizeikorps und Staatsanwaltschaften.

Von besonderer Bedeutung ist dabei die Zusammenarbeit und der Erfahrungsaustausch mit dem Kompetenzzentrum Cybercrime des Kantons Zürich, das 2013 seinen Betrieb aufnahm. Die klar definierten Strukturen zur Bekämpfung der Internetkriminalität und Ansprechpartner bei Staatsanwaltschaft und Polizei haben in diversen Fällen eine Beweisvernichtung verhindert oder die Eröffnung eines Verfahrens erst ermöglicht.

Neben dem normalen Erfahrungsaustausch mit den Kantonen fanden insbesondere im Rahmen der verdeckten Vorermittlungen (vgl. Kapitel 4) und des Projektes NDHS (vgl. Kapitel 6.1.) verschiedene Arbeitssitzungen statt.

Weiter fand am 19. November 2013 zum zweiten Mal das «Forum Cybercrime Staatsanwaltschaften - KOBIK» statt. Experten und Referenten aus Strafverfolgung und Wissenschaft präsentierten den Teilnehmenden einen praxisnahen Einblick in die internationale Bekämpfung der Internetkriminalität. So erhielten die Teilnehmer Einblick in laufende Ermittlungsverfahren gegen Bot-Netze sowie Geldwäscherei über Online-Währungen. Zudem wurden die Anwesenden durch Vertreter von EUROPOL über die koordinierenden Fähigkeiten des seit Januar 2013 operativen European Cybercrime Centers EC3 in Den Haag informiert. Rund 100 Staatsanwältinnen und Staatsanwälte haben am diesjährigen Forum teilgenommen, was das Bedürfnis nach einem solchen Ausbildungsangebot deutlich macht. Die Teilnahmen von Ständerat Luc Recordon, Nationalrat Daniel Jositsch und Strafrechtsprofessor Christian Schwarzenegger von der Universität Zürich am Podiumsgespräch ermöglichte zudem einen direkten Austausch der praktischen Probleme der Staatsanwaltschaften mit Vertretern der Politik und der Hochschulen.

7.5. Zusammenarbeit mit NGOs

Seit mehreren Jahren arbeitet KOBIK bei der Bekämpfung der Kinderpornografie eng mit der NGO[10] Action Innocence Genève (AG) zusammen. Dank der Unterstützung durch AG konnte das Projekt zur Überwachung von Peer-to-Peer-Netzwerken in den letzten Jahren erfolgreich betrieben und weiterentwickelt werden. Die Zusammenar-

10 Non-Governmental Organization / Nichtregierungsorganisation (NRO)

beit mit AG ist von grosser Bedeutung, da die Mehrheit der aktiven Recherchen von KOBIK nur dank der von AG zur Verfügung gestellten Software möglich ist. Gleichzeitig unterstützt AG KOBIK durch die Entwicklung diverser Zusatzprojekte, die im Rahmen der Bekämpfung von Pädokriminalität zum Einsatz gelangen sollen.

Die Stiftung Kinderschutz Schweiz und ECPAT Schweiz setzen sich u. a. auch für den Schutz und die Prävention von Gewalt an Kindern im Internet ein. Durch regelmässige Treffen wird sichergestellt, dass Synergien genutzt und Bestrebungen vereinheitlicht werden.

Durch die Einladung zur Tagung der Arbeitsgruppe Kindsmissbrauch konnte im vergangenen Jahr auch mit Pro Juventute eine engere Zusammenarbeit aufgenommen werden.

7.6. Zusammenarbeit mit den Schweizerischen Internet-Access-Providern

Seit 2007 unterstützt KOBIK die grössten Schweizer Internetanbieter bei der Sperrung von Internetseiten mit verbotenen kinderpornografischen Inhalten. Die Sperre richtet sich dabei ausschliesslich gegen ausländische Internetseiten, die verbotene Pornografie mit Kindern gemäss Art. 197 Ziff. 3 zum Download anbieten. KOBIK stellt den Internetanbietern eine laufend aktualisierte Liste von Webseiten mit solchen Inhalten (ca. 200-300 Internetseiten) zur Verfügung. Die Internetanbieter sperren aufgrund ihrer Firmenethik und ihren jeweiligen allgemeinen Geschäftsbedingungen den Zugang zu strafrelevanten Seiten und leiten den Benutzer auf eine «Stopp-Seite» weiter.

Im Rahmen dieses Projektes arbeitet KOBIK eng mit Interpol zusammen. Die in der Schweiz erstellte Liste alimentiert zu einem grossen Teil die Interpol «Worst-Of»-Liste von Webseiten, welche kinderpornografische Inhalte anbieten. KOBIK sucht täglich proaktiv neue Internetseiten mit kinderpornografischen Inhalten und ergänzt laufend die Interpol-Liste, welche in Zusammenarbeit mit diversen internationalen Polizeistellen unterhalten wird.

7.7. 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». Im gleichen Jahr ist KOBIK zusätzlich 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. KOBIK pflegt einen intensiven Kontakt mit dem EC3 und konnte bereits in diversen Fällen einen aktiven Beitrag zu Operationen in Anonymisierungsnetzwerken leisten.

Seit dem Berichtsjahr vertritt KOBIK die Schweiz zudem in der European Union Cybercrime Task Force (EUCTF). Die im Jahr 2010 gegründete Expertengruppe be-

steht aus Vertretern von EUROPOL, EUROJUST und der Europäischen Kommission. Die Expertengruppe soll in Zusammenarbeit mit den Leitern der nationalen Cybercrime-Einheiten die Bekämpfung von Internetkriminalität im EU-Raum erleichtern und optimieren. Die EUCTF hilft bei der Entwicklung und Förderung eines harmonisierten EU-Konzeptes für den Kampf gegen Internetkriminalität und den Problemen, die durch den Einsatz von Cyber-Technologien für die Begehung von Verbrechen entstehen. Die EU hat der Bekämpfung von Internetkriminalität auch im Rahmen der «European Multidisciplinary Platform against Criminal Threats (EMPACT)» einen sehr hohen Stellenwert zugeschrieben und Cybercrime zu einem der acht Schwergewichtsthemen erkoren. KOBIK begleitet die Bestrebungen der Europäischen Union und bringt die Interessen der Schweiz aktiv in die Diskussionen ein.

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 2013 in Verbindung zur „European Financial Coalition“ (EFC). Die von der EU mitfinanzierte EFC besteht aus wichtigen Akteuren aus der Strafverfolgung und dem privaten Sektor mit dem gemeinsamen Ziel, die kommerzielle sexuelle Ausbeutung von Kindern im Internet zu bekämpfen.

Ähnliche Ziele verfolgt auch die «Global Alliance Against Child Sexual Abuse Online», welcher die Schweiz am 6. Dezember 2012 in Brüssel beigetreten ist. Anlässlich der Unterzeichnung bekräftigte Bundesrätin Simonetta Sommaruga, dass die Schweiz der internationalen Zusammenarbeit zur Bekämpfung der Pädokriminalität einen hohen Stellenwert zumisst und die Zusammenarbeit weiter gefördert werden muss. Einer der von KOBIK definierten Meilensteine bei der Zusammenarbeit mit der Global Alliance betrifft den Beitritt der Schweiz zur Virtual Global Taskforce (VGT). Die VGT ist eine internationale Partnerschaft von Strafverfolgungsbehörden, Nicht-Regierungs-Organisationen und Privatindustrie zum Schutz der Kinder vor Online-Kindsmissbrauch. Die VGT will das Internet sicherer machen, Missbräuche erkennen, lokalisieren, Kindern in Not helfen und die effiziente Strafverfolgung der Täterschaft sicherstellen. Derzeit zählt die VGT zwölf Vollmitglieder und diverse Partner (siehe www.virtualglobaltaskforce.com). Im Berichtsjahr wurde der Antrag der Schweiz um Aufnahme in die VGT vom «Board of Directors» einstimmig gutgeheissen. Im Mai 2014 wird KOBIK die Schweiz als neuer Mitgliedstaat beim nächsten VGT-Treffen in Brüssel vertreten.

8. Medienauftritte, Ausbildung und Konferenzen

8.1. Medienpräsenz

Im Berichtsjahr fanden die Tätigkeiten von KOBIK in zahlreichen Medienberichten Niederschlag. Zudem wurden die von KOBIK erstellten Warnmeldungen zu kriminellen Phänomenen im Internet auch den Medien zur Kenntnis gebracht.

Speziell erwähnenswert ist die Beteiligung von KOBIK im Beitrag «Chronik eines Missbrauchs» in der SRF-Doku-Reihe «Schweizer Verbrechen im Visier».

8.2. Social Media

Das bisherige Echo der Facebook- und Twitter-Nutzer auf die neuen Social-Media-Auftritte von KOBIK ist durchwegs positiv (www.facebook.com/cybercrime.ch und Twitter unter @KOBIK_Schweiz).

8.3. Ausbildungen und Konferenzen

Im Berichtsjahr nahmen KOBIK-Mitarbeitende an mehreren Konferenzen, internationalen Tagungen und Ausbildungslehrgängen teil. Diese Gelegenheiten wurden zur Kontaktpflege mit Partnern und Experten genutzt.

Mitarbeitende von KOBIK waren zudem an diversen Anlässen als Ausbildungsfachleute aktiv. Beispielsweise wurden am Schweizerischen Polizei-Institut SPI erneut Workshops über die internationale Polizeikooperation in Sachen Cybercrime durchgeführt. Daneben fanden am Weiterbildungsanlass der IT-Ermittler des Konkordates Nordwestschweiz Vorträge über die Cybercrime Untergrund-Ökonomie statt. Bei über 50 weiteren Anlässen hielt KOBIK 2013 Vorträge oder nahm an Podiumsgesprächen teil.

9. Politische Vorstösse auf Bundesebene

Interpellation 13.3229: Cyberkrieg und Cyberkriminalität. Wie gross sind die Bedrohungen und mit welchen Massnahmen können sie bekämpft werden? - Recordon Luc, 22.3.2013

Interpellation 13.3986: Anfragen bei sozialen Netzwerken. Warum erhält die Schweiz so wenig Informationen? - Vogler Karl, 27.9.2013

Motion 13.3490: Kompetenzzentrum für ICT-Sicherheit - Guhl Bernhard, 19.6.2013

Frage 13.5380: Ungenügendes Instrumentarium zur Bekämpfung der Cyberkriminalität - Reimann Maximilian, 18.9.2013

Frage 13.5356: Bestellung von Drogen über die Website Silk Road - Geissbühler Andrea Martina, 16.9.2013

Frage 13.5321: Wirtschaftsspionage der NSA auch in der Schweiz? - Leutenegger Oberholzer Susanne, 11. 9.2013

Frage 13.5281: Tätigkeit der US-Geheimdienste in der Schweiz - Vischer Daniel, 12.6.2013

Frage 13.5059: Haftbarkeit von Hosting-Providern, Blog- und Forenbetreibern - Glättli Balthasar, 6.3.2013

Frage 13.5224: Zur Präsenz von US-Geheimdiensten und ihren Cyber-Schnüffelaktivitäten in der Schweiz - Reimann Maximilian, 10.6.2013

Interpellation 13.4077: Datenspionage und Internetsicherheit - Clottu Raymond, 5.12.2013

Parlamentarische Initiative 13.442: Grooming mit Minderjährigen - Kommission für Rechtsfragen, 15.8.2013

Postulat 13.3707: Ganzheitliche und zukunftstaugliche Cyberraumstrategie - Guhl Bernhard, 17.9.2013

Interpellation 13.3773: Pour une loi sur les télécommunications nous permettant d'affronter l'avenir. Elaborer une stratégie globale consacrée au cyberespace - Groupe libéral-radical, 24.9.2013

Interpellation 13.3033 : Comment protéger les données personnelles des citoyens suisses détenues par des entreprises américaines? - Schwaab Jean-Christophe; Groupe socialiste, 6.3.2013

Interpellation 13.3726: Usurpation d'identité. Une lacune du droit pénal à combler? - Schwaab Jean-Christophe; Groupe socialiste, 18.9.2013

Postulat 13.3678: Evaluer les risques de la monnaie en ligne bitcoin - Schwaab Jean-Christophe; Groupe socialiste, 11.9.2013

10. Mögliche Entwicklungen und Bedrohungen 2014

Aus dem Meldungseingang von KOBIK lassen sich keine direkten oder nur vage Rückschlüsse auf die effektive Entwicklung der Internetkriminalität oder illegaler Inhalte im Internet ableiten. Die Zahlen widerspiegeln lediglich das Meldeverhalten der Bevölkerung. Allenfalls lassen sich daraus Tendenzen hinsichtlich der Wahrnehmung von Internetkriminalität in der Gesellschaft ableiten. Die nachfolgenden Aussagen basieren auf Open-Source-Recherchen und der Interpretation dieser Quellen aus KOBIK-Sicht unter Berücksichtigung eigener operativer Erkenntnisse.

Zunahme von erfolgreichen Betrugsversuchen über das Internet

Aufgrund der gemeldeten Betrugsversuche wurde festgestellt, dass diese über das Jahr hinweg sowohl orthographisch als auch gestalterisch immer professioneller wurden. Dies gilt für fast alle Arten von Betrugsversuchen, vom Versenden von Phishing-E-Mails über das Erstellen betrügerischer Inserate und Antworten auf Anzeigeplattformen bis hin zu Sperrbildschirmen von Ransomware. Es ist davon auszugehen, dass dieser Trend sich fortsetzt. Für den Internetnutzer dürfte es somit immer schwieriger werden, einen Betrug als solchen zu erkennen. Da viele dieser Betrugsversuche ihren Ursprung in nord- und westafrikanischen Ländern haben, die Täter über ein globales Netzwerk von Money-Mules[11] verfügen und die juristischen Hürden für eine Strafverfolgung für ihre Zwecke zu nutzen wissen, ist ein strafrechtliches Vorgehen gegen dieses Phänomen äusserst schwierig. Es ist daher vermehrt auf Prävention und technische Massnahmen seitens der Plattformbetreiber zu setzen.

Wachstum der Cybercrime Untergrund-Ökonomie

In den letzen Jahren hat sich rund um die Internetkriminalität im weiteren und engeren Sinne eine regelrechte Untergrund-Ökonomie entwickelt. Dienstleistungen wie die gezielte Herstellung von Schadsoftware, der Versand von Massen-E-Mails, DDoS-Attacken, falsche Accounts auf Social-Media-Netzwerken, etc. können im Internet problemlos anonym und schnell gekauft werden. Die Bezahlung erfolgt ausschliesslich über quasi-anonyme und virtuelle Währungen wie beispielsweise Bitcoin, oder deren Austauschplattformen. Auch beliebt sind Überweisungsdienstleistungen grosser internationaler Zahlungsdienstleistungsanbieter, welche in Ländern ausserhalb Europas mit geringem Aufwand ohne Angabe einer wahren Identität genutzt werden können. Eine Verfolgung der finanziellen Mittel wird somit fast unmöglich.

Aufgrund der wirtschaftlichen Situation in Europa ist von einem Zuwachs der Akteure in dieser Ökonomie auszugehen. Eine Bekämpfung mit herkömmlichen Ermittlungsmethoden ist nicht wirkungsvoll. Vielmehr muss vermehrt auf verdeckte Ermittlung im Rahmen einer internationalen Zusammenarbeit gesetzt werden, um ein globales Lagebild dieser Ökonomie zu erstellen und deren Hauptakteure zu identifizieren. Konkret für die Schweiz heisst das, dass eine Verfolgung der Täterschaft durch einen einzigen Kanton vermutlich kaum erfolgreich durchführbar sein wird. Effizienter wäre ein koordiniertes Vorgehen mit einer gesamtschweizerischen Fallübersicht, so wie dies in der NCS vorgesehen ist. Die Verfahren könnten entsprechend durch gemeinsame Arbeitsgruppen unter der Führung eines Leitkantons oder auch des Bundes geführt werden.

[11] an der Geldwäscherei beteiligte Finanzagenten

KMU vermehrt im Visier

Durch das in der Cybercrime Untergrund-Ökonomie vorhandene Know-How sowie die weite Verbreitung von Anwendungssoftware ist davon auszugehen, dass KMU vermehrt in das Visier für Datendiebstahl durch Dritte geraten werden. KMU bieten für Cyberkriminelle ein lukratives Ziel, da die dort geführten Datenbestände an E-Mail-Adressen, Passwörtern, Kontaktdaten und Postadressen einen grossen Wert in der Cybercrime Untergrund-Ökonomie haben und die Infrastruktur oft nicht über die gleichen Sicherheitsmechanismen wie beispielsweise Grossbanken verfügen. Auch ist von einer zunehmenden Zahl von Erpressungsversuchen mit vorgängigem Datendiebstahl sowie DDoS-Angriffe auf Webseiten kleiner Firmen auszugehen. Insbesondere wird eine Zunahme von Erpressungen mit Hilfe sogenannter CryptoLocker erwartet. Diese Malware verschlüsselt die Daten auf dem Computer und macht sie somit unbrauchbar. Daraufhin erfolgt eine Aufforderung zur Zahlung eines bestimmten Betrages.

Gestohlene Zertifikate

Im Berichtsjahr wurden KOBIK bereits Verluste von Zertifikaten[12] bei grossen Certificate-Authorities gemeldet, die dann von Cyberkriminellen benutzt wurden, um Malware digital zu signieren, um so Sicherheitsvorrichtungen wie Anti-Viren-Scans zu umgehen. Die Folge davon ist, dass ein grosser Eckpfeiler der Internet-Sicherheit, die Chain-Of-Trust von Certificate Authorites, ins Wanken geraten könnte. Für Endbenutzer würde dies bedeuten, dass unter Umständen sicher geglaubte Verbindungen zu Webservern unbemerkt von Kriminellen abgefangen und der Datenaustausch so mitgelesen, umgeleitet und für unlautere Zwecke modifiziert werden könnte. Dem Endbenutzer würde aber weiterhin im Browser angezeigt, dass er mit einem Server mit legitim signiertem Zertifikat kommuniziert. Dies könnte schwerwiegende Konsequenzen beispielsweise für E-Banking, die Datenübertragung bei Online-Einkäufen und anderen sicherheitskritischen Anwendungen zur Folge haben.

Mehr Mobile Malware erwartet

Die Verlagerung der primären Internetnutzung auf mobile Endgeräte könnte den Anstieg der Zahl an Malware-Varianten für Handys, Smartphones und Tablets beschleunigen. Mit der grösseren Verbreitung von Authentifizierungsmechanismen für E-Banking Systeme, die das Vorhandensein eines zusätzlichen Kommunikationsgerätes wie beispielsweise Handys oder Smartphones benötigen, ist nicht auszuschliessen, dass auch die Zahl von Angriffen gegen solche Systeme über Mobile-Malware ansteigen wird. Die Vielzahl der Geräte, deren verschiedene Bauweisen, das benötigte Know-How und die damit verbundene wachsende Anzahl von benötigten Fachkräften wird für kantonale Polizeikorps mit kleinen IT-Abteilungen vermehrt zu einer forensischen, aber auch finanziellen Herausforderung.

[12] Zertifikate sind digitale Identitäten, welche von berechtigten Stellen (Certificate Authorities) vergeben und beglaubigt werden. Das Signieren von Zertifikaten für elektronische Entitäten, allen voran Web-Server durch Zertifizierungsstellen kommt dem Ausstellen eines Passes für eine reelle Person gleich.

11. 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 und Textform, 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.
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.
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).
Phishing	(engl. Slang: *Phreaking* = Benutzen von falschen Zugangsdaten und Fishing) Bezeichnet das unerlaubte Erlangen von Zugangsdaten von Online-Diensten über das Internet, typischerweise durch Massenversand von E-Mails von gefälschten Absendern, die zur «Verifizierung» von Kundendaten auffordern.
Proxy	(Von engl. *proxy* = Stellvertreter) Kommunikationsschnittstelle in einem IT-Netz zwischen Klient und einem Server, über den beispielsweise eine Website aufgerufen wird.
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).