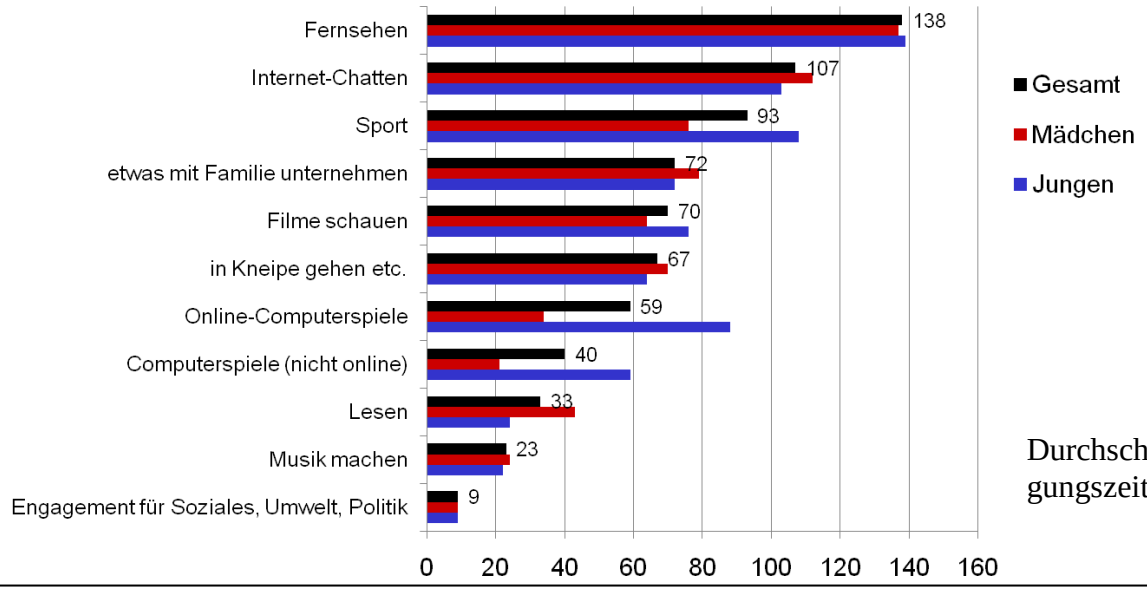
§ 12: Medien und Kriminalität

I. Begriff und Bedeutung der Medien

- Unter dem Oberbegriff Medien werden vielfältige Kommunikationsmittel zusammengefasst, deren Ziel in der Vermittlung und Weitergabe von Inhalten an ein anonymes, öffentliches Publikum besteht. Die Art der Inhaltsverbreitung führt zu der Unterscheidung in Printmedien, elektronische Medien, das Internet sowie soziale Medien. Die Medien stellen insofern ein heterogenes Bezugsobjekt dar.
- Die Zugänglichkeit des Einzelnen zu medialen Inhalten ist in den vergangenen Jahren stetig angewachsen, was hauptsächlich auf die Entwicklung des Internets zurückzuführen ist. So hat sich der Prozentsatz der in Deutschland mit einem Internetzugang ausgestatteten Haushalte in den Jahren 2005 bis 2010 von 28 % auf 64 % mehr als verdoppelt. Vor allem bei Jugendlichen ist eine mediale „Aufrüstung“ festzustellen. Im Jahre 2010 verfügten 69,8 % der Neuntklässler über einen Computer, 69,5 % über einen Fernseher und 46 % über eine Spielkonsole im eigenen Zimmer, wobei lediglich für die Spielkonsole ein deutlicher Zusammenhang mit der besuchten Schulform des Jugendlichen festgestellt werden konnte (56,3 % der Förder-/Hauptschüler gegenüber 32,2% der Gymnasiasten).
- Entsprechend der erweiterten Zugangsmöglichkeiten beschreiben auch die Werte der durchschnittlichen täglichen Beschäftigungszeit mit medialen Inhalten eine tendenziell ansteigende Kurve. Während das Zeitbudget für Mediennutzung im Jahre 1980 noch 5:46 Stunden am Tag betrug, wurden in den Jahren 2000 und 2010 Werte von 8:22 bzw. 9:43 Stunden ermittelt. Die Werte beschreiben dabei brutto-Angaben, d.h. dass bei der Parallelnutzung mehrerer Medien im gleichen Zeitraum diese auch mehrfach gezählt werden. Die größten Anteile kommen dem Fernsehen (220 Min/Tag), dem Radiohören (187 Min/Tag), sowie der Internetnutzung zu (83 Min/Tag; 144 Min/Tag bei den 14-29 Jährigen). Bei Schülern (Ergebnisse resultieren aus deutschlandweiten Befragungen in der vierten und neunten Jahrgangsstufe) stellen Fernsehen, Internet-Chatten und Computerspielen mittlerweile die dominierenden Freizeitaktivitäten dar.

Durchschnittliche Beschäftigungszeiten mit verschiedenen Aktivitäten bei Schülern



Durchschnittliche Beschä
gungszeit am Tag in Minu

Quelle: KFN-Forschungsbericht 2010, Befragung in vierter und neunter Klasse

II. Mediale Berichterstattung über Kriminalität

1. Merkmale medialer Kriminalitätsdarstellung

- Der Kriminalität kommt offensichtlich eine hohe mediale Resonanz zu. Formate, die sich inhaltlich mit realer oder fiktiver Kriminalität befassen, finden sich quer durch alle Medienformen und Genres.
- Als Begründung für die mediale Attraktivität kriminalitätsbezogener Inhalte werden das öffentliche Interesse an der Berichterstattung über ein gesamtgesellschaftliches Problemfeld sowie die Eignung der Thematik zur Polarisierung und Emotionalisierung und damit zur Steigerung von Auflagenzahlen und Quoten angeführt. Der Nachrichtenwert krimineller Ereignisse erschöpft sich nicht im Wahrheitsgehalt, sondern umfasst erlebnisorientierte, spannungsgeladene und unterhaltende Aspekte.
- Kennzeichen der Kriminalitätsdarstellung in den Medien:
  - gezielte Selektion der Taten:

    Insgesamt ist eine deutliche Fokussierung auf den statistisch untergeordneten Bereich der Gewaltdelinquenz (vor allem Tötungs- und Sexualdelikte) zu konstatieren, während die Massenkriminalität der Eigentums- und Straßenverkehrsdelikte medial kaum eine Rolle spielt. Mitunter gehen mediale Inhaltsanalysen von einer 300fachen medialen Überrepräsentation bestimmter Gewaltstraftaten aus.

    Kriminalität im sozialen Nahraum (z.B. familiäre Gewalt) ist kaum einmal Gegenstand der Darstellung. Oftmals gehören die gezeigten Täter sozialen Randgruppen an.

  - unrealistische Darstellung der Taten:

    In der Realität typische Täter-Opfer-Konstellationen werden zum Zwecke der Dramatisierung allenfalls vereinfacht dargestellt: in der Regel wird der Täter als Stereotyp eines willkürlich und gewissenslos handelnden Verbrechers inszeniert, während das Opfer als sympathisch charakterisiert wird und von der Straftat völlig überrascht wird (in Einzelfällen kann es aber auch zur Heroisierung des Täters und seiner Motive kommen).

    Eine Analyse des sozialstrukturellen oder psychischen Hintergrundes einer Straftat unterbleibt zumeist. Vielmehr wird ihr häufig das Wesen des Unerklärlichen und Rätselhaften zugeschrieben.

  - vereinfachte Darstellung von Kriminalitätsbekämpfung:

    Oftmals wird die Perspektive der Strafverfolgungsorgane übernommen, wonach der Kriminalität allein mit einer personellen und materiellen Aufrüstung der Strafverfolgungsinstanzen sowie der Verhängung härterer Strafen zu begegnen sei. Kriminalitätsbekämpfung wird als repressive Spezialistentätigkeit geschildert, während die Bedeutung intakter Strukturen informeller Sozialkontrolle unberücksichtigt bleibt.
- Diese zum Zwecke der Emotionalisierung verwendeten Stilmittel bewirken ein stark verzerrtes und tendenziöses mediales Abbild von Kriminalität. Die Medien richten die soziale Sichtbarkeit von Verbrechen nach ihren eigenen Bedürfnissen unter Ausblendung wissenschaftlicher Befunde aus.

2. Auswirkungen der medialen Kriminalitätsdarstellungen

- Die individuelle Wahrnehmung von Kriminalität kann von eigenen Erlebnissen abhängen. Die Entwicklung von seltenen schwereren Gewaltstraftaten geht jedoch über die regional begrenzte Erfahrung des Einzelnen hinaus. Diesbezüglich besteht eine völlige Abhängigkeit von medialer Vermittlung. Nach Studien beziehen 96 % der Bevölkerung ihre Informationen über Kriminalität und Kriminaljustiz nahezu ausschließlich aus den Medien. Dies führt oftmals zu einer unkritischen Adaption des verzerrten, dramatisierten Kriminalitätsbildes der Medien.
- Folgen der Adaption

  - Fokussierung auf Gewaltkriminalität verstärkt die allgemeine Definitionsbereitschaft zur Stigmatisierung von Gewalthandlungen. Die mediale Identifizierung sozialer Randgruppen als Urheber der Bedrohung kann Tendenzen sozialer Desintegration fördern.

  - Auseinanderklaffen von objektiver und subjektiver Sicherheit (Verbrechensfurcht): entgegen der ermittelten Daten sowohl der PKS als auch von Dunkelfeldstudien wird in der öffentlichen Wahrnehmung von einer Zunahme der Kriminalität, insbesondere der Gewalt- und Sexualdelikte, ausgegangen. Dabei lässt sich ein Zusammenhang zwischen dem Unterstellen eines stärkeren Anstiegs der Kriminalität und einer erhöhten Fernsehnutzung nachweisen.

Übersicht über die Einschätzung der prozentualen Veränderung der Häufigkeit bestimmter Delikte zwischen 1993 und 2003

	Geschlecht		Alter		Bildung		Fernsehstunden pro Woche	
	Mann	Frau	<45	>45	Hoch (Abitur)	gering	wenig	viel
Taten insgesamt	+39,9	+34,2	+38,0	+36,5	+32,5	+39,5	+31,1	+43,9
Körperverletzung	+55,3	+45,0	+57,4	+43,5	+38,2	+56,3	+46,9	+54,7
Voll. Sexualmord	+317,4	+195,9	+278,5	+242,2	+179,1	+299,0	+205,0	+316,1
Wohnungseinbruch	+44,1	+33,7	+35,3	+43,1	+31,0	+43,2	+38,6	+40,1

Quelle: KFN & TNS Infratest 2004

  - wachsendes Strafbedürfnis: Infolge des von den Medien wirkungsvoll erzeugten Klimas einer allgegenwärtigen Bedrohung durch Schwerstkriminalität wächst das öffentliche Bedürfnis nach einem repressiven Vorgehen formeller Kontrollinstanzen und der Aussprache härterer Strafen.

  - kriminalpolitischer Wandel und Verschärfung gerichtlicher Sanktionspraxis: Kriminalpolitische Entscheidungen werden zunehmend von empirisch-kriminologischen Erkenntnissen getrennt. Sie ergehen häufig als Reaktion auf das wachsende Strafbedürfnis der öffentlichen Meinung und dienen als Instrument zur Her-

stellung von Sicherheitsgefühlen. Auch Gerichte sehen sich einer punitiven öffentlichen Erwartungshaltung konfrontiert und laufen Gefahr, mit ihren Urteilen öffentlichen Bedürfnissen Rechnung tragen zu wollen. Insgesamt kommt es so zu einer Loslösung von Kriminalpolitik und Sanktionspraxis vom tatsächlichen Kriminalitätsaufkommen.

III. Medien als Verursacher von Kriminalität

- In der Folge Aufsehen erregender schwerer Gewaltstraftaten junger Täter (insbesondere nach Amokläufen) wird regelmäßig über den kausalen Zusammenhang zwischen dem Konsum gewalthaltiger Medieninhalte und individuellem Aggressionspotential diskutiert.
- In der Medienwirkungsforschung werden bezüglich der Frage, ob ein gehäufter Konsum realistisch wirkender Gewaltdarstellungen Einfluss auf das Verhalten im wirklichen Leben habe, folgende Theorien vertreten:
    - Katharsistheorie (Läuterung): ausgehend von der Annahme einer angeborenen Disposition zu aggressivem Verhalten wird dem Konsum von Gewaltdarstellungen eine Ventilfunktion zur Entladung aggressiver Spannungen zugesprochen. Durch ein identifizierendes Erleben einer dargestellten Gewalthandlung fiele der Verzicht auf das Ausleben eigener Aggression leichter.
    - Stimulierungsthese, basierend auf der sozial-kognitiven Lerntheorie: Gewaltdarstellungen fördern aggressive Verhaltensweisen, indem sie Konsumenten in eine aggressive Stimmung versetzen. Die Umsetzung beobachteter Gewaltmuster soll davon abhängen, inwiefern das mediale Vorbild Erfolg hat bzw. wie ähnlich die dargestellte Situation zur realen Lebenswelt des Konsumierenden ist.
    - Habitualisierungsthese: Regelmäßiger und gehäufter Konsum von Gewaltdarstellungen führe zu Gewöhnung und Abstumpfung, wodurch die emotionale Sensibilität reduziert werde. Die Anwendung von Gewalt erscheine infolgedessen als berechtigtes Mittel, um eigene Interessen durchzusetzen oder Konflikte zu lösen.
    - Anomie-Theorie: Wirkungsvoller als die detaillierten Gewaltdarstellungen seien die durch die Massenmedien vermittelten gesellschaftlichen Ziele, etwa Macht und materieller Erfolg, deren Verwirklichung für den Einzelnen gemäß der Medien nur mit gesellschaftlich nicht gebilligten Mitteln erreicht werden könne. Insofern entwürfen die Medien falsche Modelle zur Verfolgung unrealistischer Ziele.
- Von den dargestellten Theorien konnte jedoch keine empirisch valide bestätigt werden. Es fehlt bis heute an dem Nachweis einer einseitigen Kausalbeziehung zwischen einer medialen Gewaltdarstellung und einer realen Gewalthandlung.
- Aus diesem Umstand ist jedoch nicht die Wirkungslosigkeit eines andauernden Konsums gewalthaltiger Inhalte abzuleiten, zumal die empirische Erforschung der Wirkungen erheblichen methodischen Schwierigkeiten begegnet. Die Forschung begreift mediale Wirkungsmechanismen jedoch nicht mehr in einseitigen Ursache-Wirkungs-Modellen, sondern als Faktoren, die je nach Zusammentreffen mit anderen Risikofaktoren eine reale Gewalthandlung befördern können. Dabei ist insbesondere die Persönlichkeit des Konsumierenden (schwaches Selbstwertgefühl, fehlende Zukunftsperspektiven, Persönlichkeitsstörungen) sowie die soziale Situation des Medienkonsums (Wird regelmäßig alleine

konsumiert? Verstärkt das soziale Umfeld Gewalttendenzen oder hilft es bei der Bewältigung?) in einer Wirkungsanalyse zu berücksichtigen.

- So soll sich einer Studie des Kriminologischen Forschungsinstituts Niedersachsen (KFN) zufolge die Wahrscheinlichkeit einer Gewaltanwendung um das 3 bis 4fache erhöhen, wenn medialer Gewaltkonsum mit folgenden Faktoren zusammentrifft: eigene Gewalterfahrung in der Familie, soziale Benachteiligung der Familie, niedriges Bildungsniveau, schlechte Zukunftsaussichten.

- Medialen Gewaltdarstellungen wird heute daher am ehesten die Rolle eines Verstärkers bereits bestehender kriminogener Dispositionen und antisozialer Einstellungen zugesprochen (mitunter werden diesbezüglich Vergleiche zum Alkoholkonsum gezogen).

- Die wissenschaftlich ungeklärte Wirkungsweise von Gewaltdarstellungen findet ihren Ausdruck auch in den international verschiedenen Arten des Umgangs mit solchen Medieninhalten. So wurde in Deutschland etwa die bei den Amoktätern von Erfurt und Winnenden festgestellte Vorliebe für gewalthaltige Computerspiele und Actionfilme als Anlass genommen, eine Verschärfung der Medienzensur zu gewaltpräventiven Zwecken zu fordern. Auf Grundlage des JuSchG bzw. des Jugendmedienschutz-Staatsvertrages erhalten bestimmte Filme und Videospiele keine Jugendfreigabe oder gelangen überhaupt nicht auf den Markt. Demgegenüber ordnete der US-Supreme Court jüngst auch brutale Videospiele dem Schutzbereich der Meinungsfreiheit zu und erachtete ein kalifornisches Gesetz, welches das Verleihen und Verkaufen solcher Videospiele an Minderjährige verbot, als verfassungswidrig, da es für eine Einschränkung der Meinungsfreiheit nicht ausreiche, dass der Gesetzgeber die Gewaltszenen schockierend finde.

IV. Medien als Tatmittel

1. Begriff

- Medien können weiterhin auch für die Begehung unterschiedlicher krimineller Handlungen benutzt werden. Hierbei stehen insbesondere die Computerkriminalität sowie die Straftaten unter Verwendung des Internets im Fokus.

- Zur Computerkriminalität im weiteren Sinne zählen solche Delikte, bei denen entweder das Tatobjekt oder das Tatwerkzeug ein Computersystem ist. Diese Definition wird jedoch als zu unscharf kritisiert, da sie etwa bei der Versendung einer Drohung per E-Mail auch die Nötigung zu einem Delikt der Computerkriminalität werden ließe. Die PKS legt den Begriff der Computerkriminalität daher eng aus und fasst darunter im wesentlichen zwei Deliktskategorien zusammen:

  - Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen (etwa §§ 202a ff., 303a f., 317 StGB)

  - Computerbezogene Straftaten (etwa §§ 263a, 269 StGB)

- Unter der Kennung „Straftaten mit Tatmittel Internet“ fasst die PKS Delikte zusammen, die unter expliziter Verwendung des Internets verwirklicht wurden. Zur Computerkriminalität ergeben sich dabei etwa im Bereich des Computerbetruges Schnittmengen. Erfasst werden aber auch „reguläre“ Straftaten, bei deren Begehung zwar Informationstechnologie genutzt wurde, der Schwerpunkt strafrechtlichen Unrechts jedoch nicht in der Manipulation von Computersystemen liegt. Von Bedeutung sind insoweit insbesondere Betrugsfälle nach § 263 StGB im Bereich des E-Commerce, die Verbreitung pornographischer Er-

zeugnisse sowie Straftaten im Zusammenhang mit Verletzungen des Urheberrechts (§§ 106 ff. UrhG).

2. Befunde

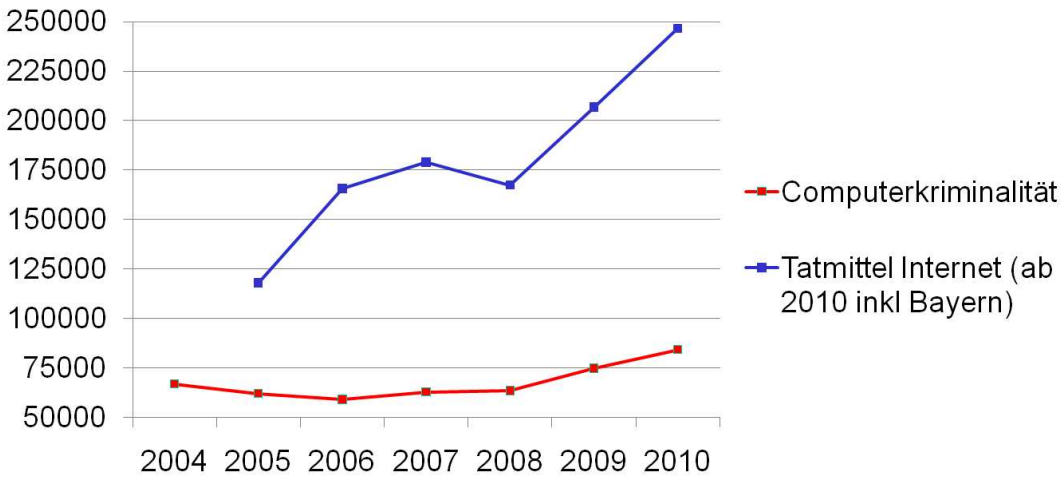
- Merkmale der Internetkriminalität
  - Verfügbarkeit von Tatwerkzeugen: die zur Begehung von Internetstraftaten notwendigen Tatwerkzeuge sind zumeist frei erhältlich. Der Austausch kinderpornographischer Erzeugnisse bzw. das Herunterladen urheberrechtlich geschützter Werke erfordert nur ein Internetanschluss sowie die geeignete Hard- und Software. Aber auch Softwareprodukte, deren vorrangiger Zweck die Begehung von Straftaten ist (z.B. Programme zur Überwindung von Passwort- oder Kopierschutzmaßnahmen) sind verfügbar.
  - Anonymität: vielfältige Möglichkeiten der Anonymisierung (Verwendung öffentlicher Internetterminals, Nutzung von Anonymisierungstechniken) erschweren die Rückverfolgung von Straftätern im Internet.
  - Automatisierung: der Zahl der über das Internet ausgeführten Angriffe steht vermutlich eine relativ kleine Anzahl von Tätern gegenüber, was auf eine zunehmende Automatisierung von Angriffsprozessen schließen lässt. Dies gilt insbesondere für den Versand von SPAM E-Mails und Hackingangriffen. Schätzungen gehen von 150 Milliarden versendeter SPAM E-Mails und 72 Millionen Angriffen auf Computersysteme pro Tag aus, was manuell nicht erreichbar wäre und nur durch den Einsatz von Softwaretools zur Automatisierung von Prozessen möglich ist.
  - Transnationalität / Unabhängigkeit von Tat- und Handlungsort: Der Zugriff auf Inhalte ist infolge der Netzwerkarchitektur weltweit möglich. Die Begehung einer Internetstraftat setzt nicht voraus, dass der Täter an dem Ort, an dem der Erfolg seiner Tat eintritt, anwesend ist. Zahlreiche Dienstanbieter (z.B. E-Mail Provider), deren Dienste bei der Begehung von Straftaten genutzt werden, bieten ihre Dienste aus dem Ausland an.
- Moderne Erscheinungsformen der IT-Kriminalität: In den Fokus der weltweiten öffentlichen Wahrnehmung rückten zuletzt vermehrt sogenannte Cyber-Angriffe. Als Opfer dieser über das Internet lancierten Angriffe kommen sowohl staatliche Behörden als auch Wirtschaftsunternehmen und Privatpersonen in Betracht. So mussten zuletzt der amerikanische Rüstungskonzern Lockheed Martin, der Internationale Währungsfonds, der US-Senat sowie die CIA einräumen, Opfer einer Cyber-Attacke geworden zu sein. Weiterhin seien laut Veröffentlichungen im Internet Angriffe auf den Chef der US-Notenbank sowie mehrere internetzensierende Regierungen geplant. Differenzierend nach der Art und Weise ihrer technischen Durchführung kommt nach Einschätzung des BSI folgenden Erscheinungsformen ein besonders hohes Gefährdungspotential zu:
  - Drive-by-Exploits: Sie verursachen die unbemerkte Infizierung eines PC beim „Vorbeisurfen“. Dabei werden beim Betrachten einer Website automatisiert und ohne weitere Nutzungsinteraktion Sicherheitslücken im Browser oder Betriebssystem ausgenutzt, um schädliche Software wie Trojanische Pferde unbemerkt auf dem PC zu installieren.
  - Botnetze: sie bezeichnen den Zusammenschluss mehrerer infizierter PCs, die von einem Angreifer ferngesteuert werden. So lassen sich unbemerkt Spam-Mails versenden, Tastatureingaben ausspähen oder Angriffe auf andere Systeme vornehmen. Ist ein PC erst einmal infiziert (z.B. durch Drive-by-Exploits), kann ihn der Angreifer als Teil des Netzes für vielfältige Zwecke missbrauchen. Bedeutung erlangen die Botnetze auch beim sogenannten „Hacktivismus“ (zusammengesetzt aus Hacking und Aktivis-

mus), bei welchem Internet-Nutzer ihre PCs freiwillig zur Verfügung stellen, um politisch motivierte Angriffe auf ein Unternehmen durchzuführen.

- Stuxnet: ist eine Schadsoftware, die unter enormem Aufwand programmiert wurde, um besondere Schutzmechanismen zu umgehen. Sie ist in der Lage, nicht nur private PCs zu infizieren, sondern auch industrielle und militärische Prozesssteuerungssysteme anzugreifen und zu sabotieren. So soll der Stuxnet-Virus 2010 gezielt zur Sabotage einer iranischen Anlage zur Uran-Anreicherung eingesetzt worden sein.

- Die Entwicklung der Straftaten im Bereich der Computerkriminalität verlief in den Jahren 2004 – 2008 relativ konstant. In den vergangenen beiden Jahren wurde jedoch ein deutlicher Anstieg der Taten verzeichnet. So wurden für 2010 insgesamt 84 377 Taten erfasst. Damit stieg die Anzahl im Vergleich zum Vorjahr um 12,6 %, was überwiegend mit einer Steigerung der Fallzahlen beim Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlung (Plus von 32 % im Vergleich zum Vorjahr) zusammenhängt.
- Die Kategorie der Straftaten mit Tatmittel Internet wird in der PKS seit 2005 gesondert dargestellt. Für das Jahr 2010 wurde ein Anstieg der Taten um 19 % auf 246 607 Fälle bekannt gegeben. Angesicht der allgemein leicht rückläufigen Kriminalität wurden die Taten mit Tatmittel Internet aufgrund ihrer Wachstumsraten von Politik und Medien als neues Kernproblem ausgemacht. Relativiert wird die Deliktsentwicklung allerdings dadurch, dass in einzelnen Jahren ganze Bundesländer, die zuvor keine gesonderte Erfassung durchführten, in die Statistik erstmalig miteinbezogen worden sind (2005 Niedersachsen, 2010 Bayern). So würde sich der 2010 vermerkte Anstieg bei einer Nichtbeachtung Bayerns auf ein Plus von 8 % reduzieren.

Entwicklung der Fallzahlen von Computerkriminalität und Tatmittel Internet



Quelle: PKS 2010 Kurzbericht

- Im Bereich der Computerkriminalität entfallen die größten Anteile registrierter Taten auf den Betrug mittels rechtswidrig erlangter Debitkarten mit PIN (30,9 %) sowie auf den Computerbetrug im engeren Sinne (30,7 %). Das Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen macht 15,3 % aus, während auf Computersabotage, Datenveränderung und Softwarepiraterie zusammengefasst knapp 5 % entfallen.

- Bei den Straftaten mit Tatmittel Internet dominieren eindeutig Betrugsdelikte (82 %). Hierunter kommt dem Warenbetrug mit allein 37,5 % der größte Umfang zu.
- Ein großer Unterschied zwischen den Bereichen der Computerkriminalität und den Delikten mit Tatmittel Internet stellt die Aufklärungsquote dar. Sie betrug im Jahre 2009 für die Straftaten mit Tatmittel Internet 75,7%, für die Computerkriminalität gerade einmal 37,5%.

3. Ursachen

- Der Anstieg der mit dem Tatmittel Internet verübten Straftaten lässt sich überwiegend mit dem rasanten Bedeutungsgewinn des E-Commerce erklären, infolgedessen große Teile des Geschäftsverkehrs bargeldlos ablaufen. Im Internet abgeschlossene Geschäfte begünstigen dabei die Entstehung betrugsrelevanter Sachverhalte, wobei auf Aspekte der Routine Activity-Theory Bezug genommen werden kann: Tatbereite Betrüger finden über Online-Kaufportale oder Ähnliches eine Vielzahl lohnender Tatobjekte sowie unerfahrene, mit den Gefahren online abgewickelter Kaufverträge nicht vertraute und somit nicht hinreichend geschützte Opfer.
- Auch die technische Fortentwicklung von Internet und Computersystemen lässt sich im Sinne erweiterter Möglichkeiten von Rechtsgutsverletzungen als Erklärung steigender Fallzahlen heranziehen: so ermöglichen etwa verbesserte Datenübertragungsgeschwindigkeiten den massenhaften Austausch urheberrechtlich geschützter Filmdaten über das Internet.
- Rational-Choice: Der Aussicht, mittels des Ausspähens von Zugangsdaten oder internetbasierenden Betrugsdelikten hohe finanzielle Gewinne einstreichen zu können, steht ein vermeintlich geringer Kostenfaktor entgegen. Zum einen erfordert die Tatbegehung angesichts der generellen Verfügbarkeit von Tatwerkzeugen keinen größeren Aufwand, zum anderen verspricht die Anonymität des Internets Sicherheit vor Identifizierung und strafrechtlicher Verfolgung. Auch die sog. moralischen Kosten fallen vergleichsweise gering aus, da das Tatopfer zumeist gesichtslos bleibt und der verursachte Schaden eine abstrakte Komponente.
- Hinsichtlich der Erklärung des oftmals politisch motivierten „Hacktivismus“ lassen sich Neutralisierungstechniken geltend machen. Individuelle Verantwortlichkeit wird anonymisiert und löst sich innerhalb der Gruppe auf (beispielhaft: Masken und Selbstbild der Anonymous-Gruppe). Verdammung der Verdammenden: Aktionen richten sich gegen vermeintlich korrupte und freiheitsbeschränkende Konzerne und Einrichtungen (Rüstungsunternehmen, Scientology, GVU).

4. Strafverfolgung.

- Die Abhängigkeit heutiger Informationsgesellschaften von der Funktionsfähigkeit ihrer Kommunikationsinfrastruktur (insbesondere IT-Systemen) und die Verletzbarkeit dieser technischen Infrastruktur haben zu einer zunehmenden Einflussnahme des Gesetzgebers auf dieses Gefüge geführt.
- Ansätze zur Bekämpfung der Computer- und Internetkriminalität liegen dabei unter anderem in der Verhinderung des Zugangs zu Tatwerkzeugen, etwa zu geeigneten Softwares. So stellen die Tatbestände der §§ 263a III bzw. 202c StGB bereits die Entwicklung einer Software zur Begehung eines Computerbetruges bzw. die Vorbereitung bestimmter Computerdelikte durch die Erstellung von Programmen unter Strafe. Folge ist eine bedenkliche Überkriminalisierung von Vorbereitungshandlungen im Bereich bestimmter Computer- und

Internetdelikte, während die Begehung vergleichbarer Handlungen außerhalb dieser Bereiche keine strafrechtliche Sanktionierung erfährt.

- Abseits des materiellen Strafrechts führte das Bemühen zur Bekämpfung der Computer- und Internetkriminalität zu der Erweiterung strafverfahrensrechtlicher Ermittlungsbefugnisse (§§ 110a, 100g, 100f StPO).
- Dennoch stellen die speziellen Wesensmerkmale der Computer- und Internetkriminalität sowie deren stetiger technischer Wandel den Strafverfolgungsbehörden nach wie vor besondere Herausforderungen. Als Grundproblem stellt sich dabei die dezentrale Netzwerkarchitektur des Internets dar, die äußerst resistent gegenüber jeglichen autoritären Eingriffen und Kontrollversuchen von außen ist. Zur Bewältigung weiterer Probleme der Strafverfolgung werden laufend neu entwickelte, passgenaue Konzepte verfolgt:

  - Der Transnationalität vieler Computer- und Internetdelikte und der damit einhergehenden Beschränkung der Strafverfolgungsmöglichkeiten durch das Souveränitätsprinzip soll durch eine enge Verzahnung und Koordinierung der nationalen Behörden sowie einer Harmonisierung strafrechtlicher Vorschriften begegnet werden.

  - Auf die Anonymität des Kriminalitätsbereiches wird vermehrt mit der Blockade des Zugangs zu Anonymisierungsservern reagiert. Des Weiteren werden technische Maßnahmen zur Identifizierung des vom Täter tatsächlich genutzten Internetzugangs weiterentwickelt, etwa die Ermittlung der IP-Adresse des Nutzers durch den Einsatz von Cookies oder Flash-Dateien. Auch hinsichtlich der Vorratsdatenspeicherung, die über den Zugriff auf bestimmte Verkehrsdaten eine Identifizierung erleichtern soll, ist ein neues Gesetz zu erwarten.

- Präventive Maßnahmen zur Vorbeugung von Computer- und Internetkriminalität liegen in der Beobachtung einschlägiger Internetforen, der Verbesserung technischer Selbstschutzmaßnahmen durch Behörden und Unternehmen sowie der Schaffung spezialisierter Kooperationseinrichtungen zur Analyse des weltweiten Datenverkehrs (Nationales Cyber-Abwehrzentrum).
- Auch jenseits der konkreten Bekämpfung der Internet- und Computerkriminalität nutzen Behörden die Medien zu Zwecken der Aufklärung und Verfolgung von Straftaten in vielfältiger Weise:

  - Zugriff auf neue Informationsquellen: aus der Überprüfung von Computer- und Telekommunikationsdaten versprechen sich Sicherheitsbehörden Hinweise auf begangene oder geplante Straftaten. Wenngleich die Rechtsgrundlage mancher Eingriffsmaßnahmen (etwa beim Zugriff auf E-Mails) nach wie vor umstritten ist, stellt die Überprüfung von Telekommunikationsdaten eine zentrale Vorgehensweise der Behörden bei der Aufklärung von Straftaten dar. Für das Jahr 2010 wurden im Jahresbericht der Bundesnetzagentur 6 Millionen Auskunftsersuche der Sicherheitsbehörden (auf Grundlage des § 112 TKG) und 36 Millionen Abfragen bei Telekommunikationsdienstanbietern verzeichnet. Auf sog. „Internet-Streifen“ überprüfen Ermittlungsbehörden anlassunabhängig Online-Inhalte auf strafrechtlich relevante Hinweise, etwa auch in Gestalt der verdeckten Teilnahme an Kommunikationseinrichtungen (öffentliche Chatrooms, Social Networks). Problematisch erscheinen solche Vorgehensweisen insofern, als die Objekte der staatlichen Ermittlungsbegehrlichkeiten stets besonders grundrechtssensibel sind. So kann das heimliche Abrufen, Zusammentragen und Verknüpfen einer Vielzahl von Daten aus unterschiedlichen Lebensbereichen erhebliche Eingriffe in die Grund-

rechte des Fernmeldegeheimnisses und der informationellen Selbstbestimmung darstellen.

- Neue Ermittlungsmaßnahmen und Zugriffsmöglichkeit: der Ausweitung staatlicher Zugriffsmöglichkeiten dienen Instrumente wie die Online-Durchsuchung (die heimliche Online-Installation spezieller Softwares auf einem fremden Rechner ermöglicht es den Ermittlungsbehörden, sämtliche dort gespeicherten Inhalte zu durchsuchen und online zu den Ermittlungsbehörden zu übertragen) und die Vorratsdatenspeicherung. Obwohl das BVerfG erste Versuche der gesetzlichen Umsetzung beider Instrumente für verfassungswidrig erklärte, betonte es, dass sowohl die Online-Durchsuchung als auch die Vorratsdatenspeicherung nicht grundsätzlich unzulässig seien. Entsprechende Neuregelungen sind daher zu erwarten (siehe auch bereits § 20k BKAG).
- Verfolgungsaufrufe: zur Herstellung einer umfangreichen Kontrolldichte wird durch den Einsatz von Fernsehen (Aktenzeichen XY) und Internet als Fahndungsmittel eine möglichst breite Öffentlichkeit in die konkrete Strafverfolgung einbezogen.
- Staatliche Reaktion auf private Ermittlungen: In neueren TV-Formaten (Tatort Internet) werden reale Straftaten von Privatpersonen provoziert und zum Zwecke der gezielten Diffamierung der Täter ausgestrahlt. Knüpfen staatliche Strafverfahren daran an, besteht neben den ohnehin zu befürchtenden Stigmatisierungswirkungen die Gefahr, dass elementare Verfahrensgrundsätze – etwa die Beschuldigtenrechte im Ermittlungsverfahren - umgangen werden.

Literaturhinweis:

Pfeiffer/Windzio/Kleimann, Die Medien, das Böse und wir, in: MschrKrim 2004, S. 415

Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Kapitel 3

IT-Sicherheitsbericht 2011 des Bundesamtes für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html