Masterarbeit

Masterstudiengang „Kriminologie und Polizeiwissenschaft“
Ruhr-Universität Bochum
Juristische Fakultät

Thema:

Informations- und Kommunikationskriminalität (IuK-Kriminalität) als Herausforderung für die Organe der Strafrechtspflege im 21. Jahrhundert

Neues Kriminalitätsphänomen oder
Wandel im Bereich des Modus Operandi

Gutachter:

1. LKD a.D. Robert Weihmann
2. Dr. phil. Oliver Bidlo

vorgelegt von:

Torben Huckenbeck
geb. 09.09.1987

E-Mail: torben.huckenbeck@web.de

Wuppertal, 09. Februar 2014

- graduiert am 21. März 2014 -

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	andere Ansicht
a.D.	außer Dienst
ABl	Amtsblatt
ACTA (engl.)	Anti Counterfeiting Trade Agreement
AG	Arbeitsgemeinschaft
AG Kripo	Arbeitsgemeinschaft Kriminalpolizei
AGB	Allgemeine Geschäftsbedingungen
ARD	Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Project Agency Netzwerk
Az	Aktenzeichen
Bd.	Band
Bearb.	Bearbeiter
Begr.	Begründer
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz und für Verbraucherschutz
BR-Drucks.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Besonderer Teil
BT-Drucks.	Bundestagsdrucksache
BT-Drucks.	Bundestagsdrucksache
BvE	Aktenzeichen des BVerfG; weist auf Verfassungsstreitigkeit zwischen Bundesorganen hin
BVerfG	Bundesverfassungsgericht
BvR	Aktenzeichen des BVerfG; weist auf Verfassungsbeschwerdeverfahren hin
bzw.	Beziehungsweise
ca.	circa
CERN (franz.)	Conseil Européen pour la Recherche Nucléaire
CIA (engl.)	Central Intelligence Agency
CR	Computer und Recht
DDos-Angriff (engl.)	Distributed-Denial-of-Service-Angriff
DFG	Deutsche Forschungsgemeinschaft
DIN	Deutsches Institut für Normung
Diss.	Dissertation
DNS	Desoxiribonukleinsäure
DP	Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei
Dr.	Doktor

DSWR	Datenverarbeitung-Steuern-Wirtschaft-Recht-Zeitschrift
DuD	Datenschutz und Datensicherheit
e.V.	eingetragener Verein
EC (engl.)	electronic cash
EDV	elektronische Datenverarbeitung
EMRK	Europäische Menschenrechtskonvention
engl.	englisch
ENIAC (engl.)	Electronic Numerical Integrator Computer
etc.	et cetera
EU	Europäische Union
EZB	Europäische Zentralbank
FASZ	Frankfurter Allgemeine Sonntagszeitung
FAZ	Frankfurter Allgemeine Zeitung
FBI (engl.)	Federal Bureau of Investigation
FDP	Freie Demokratische Partei
ff.	fortfolgende
FHöV	Fachhochschule für öffentliche Verwaltung
Frankfurt a.M.	Frankfurt am Main
Franz.	Französisch
FS	Festschrift
GCHQ (engl.)	Government Communications Headquarters
GEMA	Gesellschaft für musikalische Aufführungs- und Vervielfältigungsrechte
GG	Grundgesetz
GVG	Gerichtsverfassungsgesetz
HRRS	Online-Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
i.e.S.	im engeren Sinn
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinn
IHK	Industrie- und Handelskammer
IMK	Innenministerkonferenz
IP (engl.)	Internet Protocol
iPPP (engl.)	institutional Public Privat Partnership
IT	Informationstechnologie
IuK	Information und Kommunikation
JIM-Studie	Jugend, Information, (Multi-) Media Studie
K&R	Kommunikation & Recht
KD	Kriminaldirektor
KPMD	Kriminalpolizeilicher Meldedienst
KUG	Kunst- und Urheberrechtsgesetz
lat.	lateinisch
LG	Landgericht
LKA	Landeskriminalamt
LKÄ	Landeskriminalämter
LPD	Leitender Polizeidirektor
MIK	Ministerium für Inneres und Kommunales
Mio.	Millionen
MIT	Massachusetts Institute of Technology

MMR	Multimedia und Recht
MPFS	Medienpädagogischer Forschungsverbund Südwest
Mrd.	Milliarden
mTan	mobile Transaktionsnummer
MünchKomm	Münchener Kommentar
NJW	Neue Juristische Woche
NRW	Nordrhein Westfalen
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht
NSU	Nationalsozialistischer Untergrund
o.ä.	oder ähnlich(es)
OLG	Oberlandesgericht
PC	Personal Computer
PIN (engl.)	Personal Identification Nummer
PKS	Polizeiliche Kriminalstatistik
PSB	Periodischer Sicherheitsbericht
RAND-Corporation (engl.)	Research and Development Corporation
RdErl.	Runderlass
Rn.	Randnummer
Rz.	Randziffer
S.	Seite
SEV	Bezeichnung für Protokolle des Europarates
SH	Schleswig Holstein
[sic!] (lat.)	„wirklich so“, „auf diese Weise“
sog.	sogenannt(e)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StrÄndG	Strafrechtsänderungsgesetz
SZ	Süddeutsche Zeitung
TAN	Transaktionsnummer
TCP/IP	Transmission Control Protocol/Internet Protocol
TKG	Telekommunikationsgesetz
TOR-Netzwerk (engl.)	The Onion Router Netzwerk
u.a.	und andere
u.s.w.	und so weiter
Univ.	Universität
UrhG	Urheberrechtsgesetz
URL (engl.)	Uniform Resource Locator
USA	United States of America
v.	vom
Vgl.	Vergleiche
WiKG	Wirtschaftskriminalitätsgesetz
WLAN (engl.)	Wireless Local Area Network
WPA	Wi-Fi Protected Area
WWW	World Wide Web
z.B.	zum Beispiel
ZaRD	Zentralstelle für anlassunabhängige Recherche

1 Einleitung

„Für uns Ermittler tat sich hier eine völlig neue kriminelle Welt auf.“[1]

Dieses Zitat fasst die Schilderung zweier erfahrener Kriminalbeamter zusammen, die von einem Ermittlungsverfahren berichten, das sie im Jahr 2012 führten. Welches kriminelle Phänomen könnte diese zwei erfahrenen Kriminalbeamten dazu veranlasst haben, von einer „völlig neue[n] kriminelle[n] Welt“[2] zu sprechen? Es handelte sich um ein Strafverfahren mit Bezug zum Internet. Es ging um die sogenannte Informations- und Kommunikationskriminalität. Diese ‚neue kriminelle Welt‘ wird in dieser Arbeit untersucht.

1.1 Themendarstellung

Als das *US-Verteidigungsministerium* 1957 mit der Entwicklung eines dezentralen Datennetzes begann (dieses sollte später als Internet bekannt werden), um im Falle eines Nuklearangriffs handlungsfähig zu bleiben, hielten es die Entwickler vermutlich nicht für möglich, dass dieses Internet mehr als 50 Jahre später von den Organen der Strafrechtspflege als wesentliche Herausforderung im Zusammenhang mit Kriminalität diskutiert werden würde.
Als wesentlichstes Merkmal der modernen Informations- und Kommunikationstechnologie (IuK-Technologie) des 21. Jahrhunderts dominiert das Internet mit seinen Eigenschaften heute die Diskussion um ein Kriminalitätsphänomen, welches sich aus der Computerkriminalität entwickelt hat und inzwischen als Informations- und Kommunikationskriminalität bezeichnet wird. Dabei geht es um jegliche kriminellen Handlungen, die sich gegen die moderne IuK-Technologie richten oder sich dieser als Tatmittel bedienen.

Im Folgenden wird das Phänomen der Informations- und Kommunikationskriminalität (kurz: IuK-Kriminalität) als Herausforderung für die Strafrechtspflege im 21. Jahrhundert untersucht. Wenn dabei von Organen der Strafrechtspflege die Rede ist, sollen darunter die Gerichte der ordentlichen Ge-

[1] Burandt/Tölle, in: Kriminalistik 8-9/2013, 524.
[2] Burandt/Tölle, in: Kriminalistik 8-9/2013, 524.

richtsbarkeit in Strafsachen, die Staatsanwaltschaft und die Polizei des Bundes und der Länder verstanden werden. Andere Organe der Strafrechtspflege sind von der hiesigen Betrachtung nicht explizit umfasst.

Die Relevanz des hier zu untersuchenden Kriminalitätsphänomens wird mit Blick auf die sicherheitsbehördlichen Veranstaltungen und medialen Publikationen im Kalenderjahr 2013 deutlich. „Jeden Tag eine Million Opfer von Cybercrime“[3], titelte die Zeitung *Die Welt* am 19. Februar 2013. Parallel dazu fand in Berlin ein Europäischer Polizeikongress zum Thema „Schutz und Sicherheit im digitalen Raum“ statt. Das *Bundeskriminalamt* führte vom 12.-13. November 2013 eine zweitägige Veranstaltung zum Thema „Cybercrime – Bedrohung, Intervention, Abwehr“ durch. Der Präsident des Bundeskriminalamts *Ziercke* sprach dabei von einer „Bedrohung mit unvergleichbarer Dimension“[4].
Gleichermaßen ist die „Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten […] zu einer existenziellen Frage des 21. Jahrhunderts geworden.“[5]
Während unsere Gesellschaft also einerseits auf die moderne Technologie angewiesen ist, wird sie gleichermaßen durch die Technologie bedroht.

Der Jurist *Jofer* hat bereits 1999 festgestellt: „Die Strafverfolgungsorgane können die Prämissen bei der Strafverfolgung nur dann richtig und effizient setzen, wenn das Potential der kriminellen Gefährdung richtig eingeschätzt wird.“[6] Im Mittelpunkt der vorliegenden Arbeit steht daher eine phänomenologische Analyse des Kriminalitätsphänomens ‚IuK-Kriminalität‘. Forschungsleitend ist die Frage, ob es sich dabei um ein (tatsächlich) neues Kriminalitätsphänomen handelt, oder ob gesellschaftliche, soziale und technische Wandlungsprozesse vornehmlich zu einer Verschiebung im Bereich des Modus Operandi geführt haben. Es wird geprüft, welche Straftaten und Begehungsweisen worunter zu subsumieren sind. Nach der Einführung verschiedener Begrifflichkeiten und einer Erläuterung der Entwicklung des Kriminali-

[3] Die Welt-Online, 19.02.2013, www.welt.de.
[4] Ziercke, Cybercrime – Bedrohung, Intervention, Abwehr (Begrüßungsrede - gesprochenes Wort), 12.11.2013, www.bka.de; vgl. FAZ, 13.11.2013, 1.
[5] BMI (Hrsg.), Cyber-Sicherheitsstrategie für Deutschland, 1.
[6] Jofer, Strafverfolgung im Internet, 31.

tätsphänomens bedarf es einer Differenzierung zwischen Straftaten, die sich gegen die IuK-Technologie selber wenden und solchen, die das Internet als Tatmittel nutzen. Es gilt zu zeigen, dass lediglich eine differenzierte Betrachtung der von *Ziercke* skizzierten ‚unvergleichbaren Bedrohung' gerecht wird.

Die Erkenntnisse der phänomenologischen Analyse leiten dazu über, wie die Organe der Strafrechtspflege der Bedrohung durch die IuK-Kriminalität begegnen können. Ausgehend von der forschungsleitenden Frage und den Analyseergebnissen skizziert die Arbeit den Diskurs um die kriminalistischen und juristischen Herausforderungen und bewertet diesen kritisch.

Vor der Analyse und Diskussion der Aspekte der Kriminalitätsbekämpfung werden die Entwicklungsgeschichte des Internets, die damit einhergehenden gesellschaftlichen Veränderungen und der Begriff des Modus Operandi erklärt.

1.2 Methodik

Vorliegend handelt es sich um eine Literatur- und Medienanalyse, die sich verschiedenster Quellen bedient. Nachdem das einleitende *Kapitel 1* zum Thema hingeführt und Bezüge sowie Abgrenzungen des Untersuchungsgegenstands zur Spähaffäre um den amerikanischen Geheimdienst *National Security Agency (NSA)* hergestellt hat, dienen die *Kapitel 2* und *3* der Grundlagenarbeit und damit dem Verständnis der Argumentation. Die Grundlagenarbeit, sprich die Aufarbeitung der Internetentwicklung, der durch neue Technologien geprägte gesellschaftliche Wandel sowie allgemeine Ausführungen zum Modus Operandi erfolgen anhand einschlägiger, ausgewählter Literatur.
Die phänomenologische Analyse bzw. die die Beantwortung der Forschungsfrage erfolgt in *Kapitel 4*, zum einen durch die Auswertung der *Polizeilichen Kriminalstatistik (PKS)* und weitere öffentlich zugängliche Zahlen (z.B. Lagebilder des Bundeskriminalamts), zum anderen durch eine inhaltliche Analyse und Auswertung aktueller Literatur (aufgrund der hohen Dynamik des Themas mehrheitlich wissenschaftliche Aufsätze). Zudem wird die mediale Berichterstattung verfolgt, um mögliche Tendenzen bei der Begehung von Straf-

taten im Zusammenhang mit moderner IuK-Technologie und gesamtgesellschaftliche Entwicklungen identifizieren zu können.
Die Erkenntnisse des *Kapitels 4* leiten zu den Herausforderungen über, die sich für die Organe der Strafrechtspflege ergeben. Diese kriminalistische und juristische Ebene wird in *Kapitel 5* anhand aktueller Rechtsprechung, Gesetzgebung, Bekämpfungsmethoden, kriminalpolitischer Debatten und Fachaufsätzen analysiert.
Das abschließende *Kapitel 6* fasst zusammen, kommentiert die Ergebnisse, ordnet sie in den gesellschaftlichen Kontext ein und gibt einen Ausblick.

Aufgrund der dynamischen Entwicklung des Themas sei darauf hingewiesen, dass die Arbeit den Stand der wissenschaftlichen Literatur bis etwa August 2013 abbildet. Späteren Entwicklungen wurde immerhin durch die Einbeziehung der medialen Berichterstattung bis Ende Januar 2014 weitgehend Rechnung getragen.

1.3 Die NSA-Affäre – Bezug und Abgrenzung zum Untersuchungsgegenstand dieser Arbeit

Im Juni 2013 veröffentlichte *Edward Snowden*, ehemaliger Mitarbeiter des amerikanischen Geheimdienstes *National Security Agency (NSA)*, streng geheime Informationen zu den weltweiten Überwachungsaktivitäten seines früheren Arbeitgebers. Dadurch wurde er weltweit als *‚whistleblower‘*[7] bekannt. Seit den ersten Veröffentlichungen werden in unregelmäßigen Abständen neue Einzelheiten über die Tätigkeiten der NSA bekannt. Es geht um Computerspähprogramme, das Abhören des Mobiltelefons der *deutschen Bundeskanzlerin* und politischer Institutionen und um das massenhafte Abschöpfen persönlicher Daten unverdächtiger Bürger weltweit.[8] Eine proklamierte ständige Bedrohung der *Nationalen Sicherheit* dient als Generalermächtigung für diese Überwachung. Da die moderne IuK-Technologie bei diesen geheimdienstlichen Tätigkeiten von entscheidender Bedeutung ist, ist

[7] Whistleblower (engl.): „Jemand, der Missstände öffentlich macht“, Duden (Hrsg.), Deutsche Rechtschreibung, 1174.
[8] Zur Chronik der NSA-Affäre, vgl. FAZ, 25.10.2013, 4.

zu klären, ob die NSA-Affäre Bestandteil der IuK-Kriminalität ist und damit zum Untersuchungsgegenstand der vorliegenden Arbeit gehört. Zwar ist gegenseitige Spionage von Staaten kein neues Phänomen, die moderne IuK-Technologie hat jedoch zu einer Dimension geführt, deren Ausmaße kaum zu überschauen und zu kontrollieren sind.

Die Preisgabe der Geheimnisse durch *Edward Snowden* haben dreierlei ausgelöst. Erstens wird seither auf vielen politischen Ebenen um das Schicksal und Ansehen des aus den USA geflohenen *whistleblowers* verhandelt. Zweitens haben die deutsche und europäische Politik empört über die Tätigkeiten der NSA reagiert, den sich darin ausdrückenden Vertrauensmangel gerügt und das staatliche Verhältnis zueinander bisweilen erschwert. Drittens und am entscheidendsten hat eine gesamtgesellschaftliche Debatte eingesetzt, die den Diskurs zwischen Sicherheit und Freiheit erstmalig seit dem 11. September 2001 wieder entfacht hat. Für diese Debatte waren die Veröffentlichungen zur NSA-Affäre jedoch nur der Ausgangspunkt. Inzwischen geht es allgemeiner um die Nutzung moderner IuK-Technologie, die Preisgabe persönlicher Daten im Internet, die Verflechtung von Geheimdiensten und Wirtschaftsunternehmen, ökonomische Interessen und die Manipulierbarkeit, Vorausschaubarkeit bzw. Selbstbestimmung und Anonymität des eigenen Handelns. *Schirrmacher*, Mitherausgeber der *Frankfurter Allgemeinen Zeitung (FAZ)* schreibt, dass die Debatte um *Snowden* und die NSA zu einer tiefgreifenden Erkenntnis geführt hat, nämlich einer „Veränderung der sozialen Ordnung in den westlichen Demokratien.“[9] Von welch grundlegender Bedeutung die derzeitige Debatte für das zukünftige gesellschaftliche Leben ist, zeigt die Tatsache, dass sich der *deutsche Bundespräsident* und andere Intellektuelle wiederholt zu den nachrichtendienstlichen Enthüllungen und gesellschaftlichen Zuständen geäußert haben.[10] In Anlehnung an einen Artikel der FAZ geht es bei der Überwachungsdiskussion schlussendlich um nicht weniger als um die ‚Verteidigung der Demokratie im digitalen Zeitalter‘.[11]

[9] Schirrmacher, in: FASZ, 25.08.2013, 37.
[10] Vgl. FAZ, 04.10.2013, 2; Braun, in: SZ, 27./28.07.2013, 5; Nonnenmacher, in: FAZ, 27.07.2013, 1.
[11] FAZ, 10.12.2013, 27-28.

Insgesamt ist die NSA-Affäre mit ihren Auswüchsen eher ein politisches als strafrechtliches oder kriminalistisches Problem. Dementsprechend ist eine intensive Auseinandersetzung mit der NSA-Affäre im Rahmen dieser Arbeit nicht vorgesehen. Die Erscheinungsform unterscheidet sich von den Phänomenen der IuK-Kriminalität. Dennoch steht die skizzierte Debatte in einem solch engen Zusammenhang mit der modernen IuK-Technologie, dass diese im Verlauf der Arbeit nicht unbeachtet bleiben kann. Thematische Bezüge werden aufgezeigt und erläutert.

2 Technische und soziale Wandlungsprozesse

Vor dem Hintergrund der zu thematisierenden Bedrohungen durch die moderne Informations- und Kommunikationstechnologie ist im Weiteren von Wandlungsprozessen und nicht von einem grundsätzlichen Fortschritt die Rede. Folgendes verdeutlicht die Problematik: Gewährt der Computer heute eine erhebliche Arbeitserleichterung, kritisierte man während der Frühzeit der Computerindustrie bereits, dass die Menschen und die Gesellschaft durch die intensive Computernutzung zunehmend als Maschine betrachtet werden.[12] *Tim Berners-Lee* verfolgte mit der Entwicklung des *World Wide Web* das Ziel, Klassensystematiken zu durchbrechen, ein neues Denken und eine neue Freiheit zu fördern.[13] Gleichzeitig entwickelten sich mit dem Internet und dem *World Wide Web* aber auch neue Gefahren im Hinblick auf den Datenschutz, soziale Beziehungen und Kriminalität. Während die Wertung einzelner Entwicklungen also maßgeblich von der Perspektive und den jeweiligen Interessen des Bewertenden abhängt, kann der Aussage *Nicholas Negroponte*s, dem Mitbegründer des *Massachusetts Institute of Technology (MIT) Media Lab*, zugestimmt werden: „Like a force of nature, the digital age cannot be denied or stopped.“[14] – übersetzt: Das digitale Zeitalter lässt sich so wenig leugnen oder aufhalten wie eine Naturgewalt. Die moderne Informations- und Kommunikationstechnologie ist im Alltag ein ständiger Begleiter geworden – teilweise ohne dass wir uns dessen bewusst sind.

[12] Vgl. Passig/Lobo, Internet, 75.
[13] Vgl. Berners-Lee, Der Web-Report, 11-12.
[14] Negroponte, Being digital, 229.

2.1 Die Entwicklung des Internets

Die Ursprünge des Internets liegen im Kalten Krieg. 1957 gelang es der Sowjetunion, den ersten Sputnik-Satelliten im Weltall zu platzieren. Durch diesen Fortschritt wurde das Bedrohungspotenzial gegenüber den Vereinigten Staaten von Amerika gesteigert. Die US-Amerikaner durchdachten das Szenario eines Nuklearangriffs gegen sie und erkannten das Problem, dass die politische Führung und militärischen Einrichtungen in der Folge eines atomaren Angriffs nicht mehr sicher und effektiv miteinander kommunizieren könnten. Im Auftrag des US-Verteidigungsministeriums wurde daraufhin 1957 die *Advanced Research Project Agency (ARPA)* gegründet. Mit dem Ziel des Erhalts von Handlungs- und Regierungsfähigkeit im Notfall hatte sie den Auftrag, ein nuklearsicheres Befehls- und Kommunikationsnetzwerk zu entwickeln.[15]

In den Folgejahren arbeiteten Wissenschaftler namhafter Universitäten und anderer Institutionen an Computernetzen und deren Kommunikation untereinander. Es durfte sich um kein zentralisiertes Computernetz handeln, welches durch einen gezielten Angriff hätte zerstört werden können. Zudem musste die Kommunikation zwischen den Computern unabhängig des jeweiligen Herstellers und des verwendeten Betriebssystems möglich sein.

1964 gelang es *Paul Baran*, Mitglied der *‚Research-And-Development-Corporation‘ (RAND-Corporation)*[16], das erste dezentralisierte Computernetz zu errichten.[17] 1969 wurden die ersten vier Großrechner amerikanischer Universitäten miteinander verbunden. Damit entstand das vom Pentagon so bezeichnete *ARPANET*, die ‚Mutter des Internets‘. Durch die Verwendung eines gemeinsamen Kommunikationsprotokolls wurde in den 1980er Jahren das Problem der verschiedenen Hersteller und Betriebssysteme beseitigt.

Hervorzuheben ist, dass es sich um kein zentralisiertes Netz handelte. Eine Vielzahl von unabhängigen Computernetzen wurde miteinander verbunden. Diese Eigenschaft sorgte für die notwendige Störungsresistenz. Fielen Teile

[15] Vgl. Jaspersen, in: Grundwissen Medien, 295.

[16] Die RAND-Corporation wird inzwischen als die größte Denkfabrik der USA bezeichnet. Ihre Mitglieder waren zu Zeiten des Kalten Krieges als beratende Organisation des Militärs an der Implementierung der ‚rational choice theory‘ bzw. ‚Spieltheorie‘ beteiligt, vgl. Schirrmacher, EGO, 21-41.

[17] Vgl. Klau, Das Internet, 25-26.

des Netzes aus, funktionierte der restliche Teil uneingeschränkt weiter.[18] Diese Eigenschaft prägt das Internet bis heute.

Obwohl das Internet theoretisch seit 1977 der Öffentlichkeit zugänglich war, blieb es bis 1993 praktisch den Universitäten, Fachleuten und IT-Experten vorbehalten. Es war benutzerunfreundlich und beruhte auf der Eingabe von kryptischen Befehlen. Erst im April 1993 entwickelte *Marc Andreesen*, damaliger Student der Universität Illinois, einen neuen Internetbrowser namens *‚Mosaic‘*.[19] Ein Browser ist ein Programm, welches für die Darstellung der Inhalte im Internet verantwortlich ist. *Mosaic* revolutionierte das Netz und bereitete den Weg zur kommerziellen und partizipierenden Nutzung des Internets. Der neue Browser nutzte das sogenannte *World Wide Web (WWW)* als Netzbasis.[20] Dieses ist nicht mit dem Internet gleichzusetzen.

Während die Geschichte des Internets in den 1960er Jahren begann, stammt die Entwicklung des *World Wide Web* aus dem Jahre 1990. *Tim Berners-Lee* wollte die dezentralen Netze des Internets durch ein neues Medium miteinander verbinden. „Meine Vision für das Web ist, daß [sic!] prinzipiell alles mit allem verknüpft ist.“[21] Dadurch erhoffte er sich, dass selbstauferlegte, hierarchische Klassifikationssysteme aufgebrochen, ein neues Denken gefördert und neue Freiheiten ermöglicht werden.[22] 1990 realisierte er mit *Robert Cailliau* die erste Verbindung über das World Wide Web. Durch bestimmte Prinzipien war es damit möglich, nicht nur Textbausteine sondern auch Bilder, Audio- und Videodateien und Hyperlinks[23] im Internet zur Verfügung zu stellen.[24] Als die Technologie des WWW im Jahre 1992 veröffentlicht wurde, war ein Meilenstein in der Weiterentwicklung des Internets und des WWW zum Massenmedium der Zukunft gelegt.[25] Die Privatisierung und Ökonomisierung hatte begonnen. Dies stellt sich heute als Problem dar (vgl. Kapitel 4 und 5).

[18] Vgl. Lang/Bekavac, in: Grundwissen Medien, 434.
[19] Vgl. Dworschak, in: Der Spiegel 17/2013, 98.
[20] Vgl. Dworschak, in: Der Spiegel, 178/2013, 98.
[21] Berners-Lee, Der Web-Report, 11.
[22] Vgl. Berners-Lee, Der Web-Report, 11 ff.; Lang/Bekavac, in: Grundwissen Medien, 433
[23] Hyperlinks (engl.): „Stelle auf dem Bildschirm, die durch Anklicken zu weiteren Informationen führt“, Duden (Hrsg.), Die deutsche Rechtschreibung, 541.
[24] Vgl. Lang/Bekavac, in: Grundwissen Medien, 438-439.
[25] Vgl. Lang/Bekavac, in: Grundwissen Medien, 439.

2.2 Die Weiterentwicklung zum Web 2.0

Nach der Entwicklung von *Mosaic* und der Veröffentlichung der WWW-Technologie wuchs die Zahl der Internetnutzer auf weltweit ca. 15 Mio. heran. In den Folgejahren wurden immer mehr Facetten des Internets entdeckt. 1996 veröffentlichte eine 19 Jahre alte Studentin große Teile ihres Lebens im Internet. Das Ergebnis der sich daraus entwickelten öffentlichen Debatte war, dass das Internet als Informationsportal und nicht als Darstellungs- und Selbstoffenbarungsplattform genutzt werden sollte.[26] Diese Meinung muss mit Blick auf *Facebook*, *Online-Partnerbörsen* und *Youtube* aus heutiger Sicht als überholt angesehen werden. Der Schriftsteller, Filmemacher und Kulturberater *Schindhelm* skizziert in einem Artikel der *Süddeutschen Zeitung*, dass das Internet im Jahr 2012 nicht mehr zwischen Künstler und Publikum unterscheidet.[27] Von einem reinen Informationsportal kann demnach keine Rede mehr sein.

Zählte das Internet 1996 etwa 68 Mio. Nutzer, revolutionierten die Internetsuchmaschinen ab 1998 den Markt erneut. G*oogle* ging online und errichtete in den Folgejahren ein Imperium mit richtungsweisenden Entwicklungen: *Maps*, *StreetView*, *GoogleGlass*. Es handelte sich um ungeahnte Möglichkeiten, denen die Gesellschaft bis heute zwiespältig gegenübersteht – zwischen Faszination und Angst vor Fremdbestimmung.[28] Die Faszination überwiegt. Bis zur Jahrtausendwende stieg die Zahl der Nutzer auf 361 Mio.[29]

Kurz nach der Jahrtausendwende gab es trotz des Wachstums erste Anzeichen dafür, dass zahlreiche (Börsen-) Unternehmen der Internetbranche die hohen Gewinnerwartungen nicht erfüllen würden. Im Herbst 2001 kam es schließlich zum wirtschaftlichen Zusammenbruch. Dieses Phänomen ist unter dem Namen *‚Dotcom-Blase‘* bekannt geworden.[30] Es veranschaulicht den

[26] Vgl. Dworschak, in: Der Spiegel 17/2013, 98-103.
[27] Vgl. Schindhelm, in: SZ, 10./11.11.2012, 2.
[28] Zur Fremdbestimmung und Berechenbarkeit „homo oeconomicus“, vgl. Schirrmacher, EGO, 28 ff; Foucault, Michel, Die Geburt der Biopolitik, 300 ff.
[29] Vgl. Dworschak, in: Der Spiegel 17/2013, 98-103.
[30] Vgl. Dworschak, in: Der Spiegel 17/2013, 103; Huber, Kommunikation im Web 2.0, 14.

ersten Höhepunkt des Einflusses ökonomischer Interessen bei gleichzeitigem Verzicht auf staatliche Kontrolle im Internet.
Dieses abrupte Ende war jedoch gleichzeitig der Beginn des sogenannten *Web 2.0*. *Tim O'Reilly* u.a. verwendeten den Begriff erstmals im Jahr 2004, um das ‚neue' Internet zu charakterisieren.[31] Was hatte sich geändert? Der Journalist *Dworschak* schrieb: „Das Internet verwandelt sich in ein Medium, das Menschen verbindet, nicht Computer."[32] Das Netz entwickelte sich mit Fokus auf Nutzen, Ziele und Zielgruppen. Interaktivität wurde zum zentralen Begriff des *Web 2.0*. *Facebook* (2004), *Youtube* (2005), *Twitter* (2006) und ähnlich interaktive Angebote eroberten das Internet und eröffneten die Möglichkeit einer ‚Kultur des Selbermachens'.[33]

Heute verzeichnen die Statistiken knapp 2.500 Mio. Internetnutzer weltweit. Mit steigenden Nutzern und den neuen Funktionen steigt auch der Datenverkehr im Netz massiv. Wurden 1993 etwa 0,11 Petabytes/Jahr[34] über das Internet versendet, waren es 2011 368.808 Petabytes[35] - eine nicht greifbare, kaum zu handhabende Masse an Daten. Dass sich für diese Datenmasse inzwischen ein eigener Begriff gebildet hat, wird die phänomenologische Analyse der IuK-Kriminalität (Kapitel 4) zeigen.

2.3 Aktuelle Entwicklungen des Internets

Das *Statistische Bundesamt* gibt in seiner jährlichen Berichterstattung bekannt, dass im Jahr 2012 79% der deutschen Haushalte über einen Internetanschluss verfügten. Haushalte mit Kindern verfügten 2012 in über 95% der Fälle über einen Anschluss an das Netz. Das Nutzungsverhalten betrachtet, wurde das Internet zu einem großen Teil zum Senden und Empfangen von E-Mails (91%), zum Online-Banking (50%) und zur Beteiligung an sozialen Netzwerken (42%) genutzt.[36]

[31] Vgl. Huber, Kommunikation im Web 2.0, 14.
[32] Dworschak, in: Der Spiegel 17/2013, 103.
[33] Zur Entwicklung bzw. zum Vergleich des Web und des Web 2.0, vgl. Huber, Kommunikation im Web 2.0, 10-20.
[34] 1 Petabyte (PB) = 1.024 Terabyte
[35] Datenquelle: Dworschak, in: Der Spiegel 17/2013, 98-103.
[36] Vgl. Statistisches Bundesamt (Hrsg.), Statistisches Jahrbuch, 198-199.

Die Relevanz des Mediums Internet wird mit Blick auf die Nutzungsdauer abermals deutlich: Schätzten Jugendliche im Alter von 12-19 Jahren ihre tägliche Fernsehdauer auf 111 Minuten[37], lag die durchschnittliche Dauer der Internetnutzung nach eigenen Angaben bei etwa 131 Minuten pro Tag.[38] Das Internet scheint den lange vorherrschenden Fernseher überholt zu haben – nicht zuletzt deshalb, weil das Internet alle Funktionen miteinander vereint.

Bei den Jugendlichen der *Bundesrepublik Deutschland* dominieren in der Internetnutzung heute kommunikative Tätigkeiten, insbesondere soziale Netzwerke (*Facebook* etc.). Lediglich 15% der im Internet verbrachten Zeit werden zwecks Informationssuche verwendet; sprich 85% der Nutzungszeit ist Freizeit bzw. Spielerei. Die Möglichkeit der Nutzung von Videoportalen als Konsument, aber auch als Plattform der Selbstdarstellung und Selbstoffenbarung, findet in der Welt der Jugendlichen bedeutenden Anklang. Die Technologie ist zu einem Instrument der breiten Öffentlichkeit geworden, das durchschnittliche Alter zum Zeitpunkt der ersten Anmeldung in einer Online-Community beträgt 12,5 Jahre.[39]

Mit Blick auf die am zweithäufigsten aufgerufene Seite des Internets in Deutschland – nämlich *Facebook* – muss der Schutz der Privatsphäre betrachtet werden. Zwar hat eine öffentliche Diskussion der letzten Jahre eingesetzt und zu einer gesteigerten Sensibilität der Jugendlichen geführt. Dennoch zeugt eine durchschnittliche Anzahl von 272 Online-Freunden bei Facebook und eine Registrierung bei eben diesem Portal mit vollständigem Vor- und Nachnamen von einer nach wie vor vorhandenen Naivität.[40]

Eine weitere, zukunftsweisende Entwicklung ist der Weg in das Internet. War es anfänglich den fest installierten Desktop-Computern vorbehalten, sich in das Netz einzuwählen (per Kabel), eröffnen heute offene WLAN-Netze[41],

[37] In der Zeit von Montag bis Freitag.
[38] Vgl. MPFS (Hrsg.), JIM-Studie 2012, 31-32, 63.
[39] Vgl. MPFS (Hrsg.), JIM-Studie 2012, 33-43.
[40] Vgl. MPFS (Hrsg.), JIM-Studie 2012, 43-46.
[41] Wireless Local Area Network (WLAN) (engl.): Drahtloses lokales Netzwerk bestehend aus mehreren Computern.

Hotspots, die Verbreitung von Laptops und internetfähigen Smartphones wiederum eine neue Dimension digitaler Vernetzung.

Aus den hier skizzierten Entwicklungen ergeben sich Auswirkungen auf den individuellen und gesellschaftlichen Sozialisations- und Identitätsbildungsprozess. Handlungsweisen und Entscheidungen werden anders getroffen. Diese wiederum haben eine Bedeutung bezüglich der zu untersuchenden IuK-Kriminalität.

2.4 Gesellschaftliche Entwicklungen vor dem Hintergrund des technologischen Fortschritts

Nach dem hiesigen Verständnis von Sozialisation kann das Internet im 21. Jahrhundert als ein wesentlicher Sozialisationsmechanismus verstanden werden.[42] Da die Sozialisation dem Prozess des lebenslangen Lernens folgt, gilt das Internet als Sozialisationsmechanismus für Kinder, Jugendliche und Erwachsene gleichermaßen.

Die Informationsrechtler *Palfrey* und *Gasser*, die sich intensiv mit dem Identitätsbildungsprozess im digitalen Zeitalter beschäftigt haben, schreiben: „Das Wesen der Identität erlebt im 21. Jahrhundert gravierende Veränderungen. Davon sind nicht nur Digital Natives[43] und andere junge Leute betroffen, sondern alle, die in vernetzten Gesellschaften leben.“[44] Die Interaktivität des *Web 2.0* bietet heute die Möglichkeit, unmittelbar und schnell Einfluss auf die eigene, persönliche Identität zu nehmen – sei es durch den Austausch des Profilbildes bei *Facebook*, das Posten und Teilen verschiedener Beiträge oder auch schlicht die Anzahl der ‚Freunde‘ in sozialen Netzwerken.[45] Zudem bietet das Internet die Möglichkeit zur Herausbildung von Mehrfachidentitäten. Der Nutzer hat die Möglichkeit, sich in zahlreichen Kontexten unterschiedlich darzustellen. Dabei wird immer weniger zwischen Online- und Off-

[42] Vgl. Mühler, Sozialisation, 42, 46; Dimbath, Einführung in die Soziologie, 175.
[43] „[…] – Menschen also, die nach 1980 direkt in das Zeitalter hineingeboren wurden, […]. Sie sind durchweg vernetzt und mit den neuen digitalen Medien und Möglichkeiten bestens vertraut.“, Palfrey/Gasser, Generation Internet, 1.
[44] Palfrey/Gasser, Generation Internet, 42.
[45] Vgl. Palfrey/Gasser, Generation Internet, 39.

line-Identitäten unterschieden. Es besteht eine zentrale Nutzungsmotivation, Einblicke in das eigene Leben und Hinweise auf die reale Identität zu geben.[46] Die Jugendlichen stellen Werte und Normen in Frage und suchen nach Orientierung. Das Internet dient als wichtige Umgebung, um Sozialisations- und Identitätsbildung zu trainieren.[47] Der Ethnologe *Miller* kommt zu dem Ergebnis, dass sich soziale Netzwerke zu moralischen Instanzen entwickelt haben.[48]

Diese gestalterische Möglichkeit der persönlichen Identität zeigt jedoch nur eine Seite des Internets. Das Sozialisationsobjekt bzw. –subjekt hat keinen Einfluss auf die Wahrnehmung der jeweiligen Selbstdarstellung(en) durch andere.[49] Erschwerend kommt hinzu, dass im Netz einmal gespeicherte Daten dauerhaft recherchierbar bleiben und sich Zusammenhänge feststellen lassen.[50] Durch Datensammlung können Nutzer also ein umfassendes Bild der sich im Internet präsentierenden Person zeichnen. *Palfrey* und *Gasser* schreiben zutreffend: „So vielschichtig, interessant und einfach zu erzeugen die digitale Identität eines *Digital Native* auch sein mag, ist sie jedoch auch fragil und anfällig für Manipulationen und Verfälschungen.“[51] Die Verwirklichung der aus diesem Umstand resultierenden Gefahr zeigt sich in Form von verschiedenen Delikten der IuK-Kriminalität (Kapitel 4).

Die soziale Identität, die sich Jugendliche und Erwachsene im Laufe ihres Sozialisationsprozesses aufbauen, ist sehr komplex geworden. Der vordergründige Schein, ein hohes Maß an Kontrolle über seine Selbstdarstellung zu haben, täuscht demnach. Der Großteil der Nutzer ist sich den Gefahren nicht bewusst. Insbesondere die Gefahren durch die Preisgabe persönlicher Daten wird unterschätzt.[52] *Palfrey* und *Gasser* verleihen ihrer Äußerung dadurch

[46] Zwei Drittel der Nutzer von Online-Communities haben sich mit ihrem richtigen Vor- und Zunamen angemeldet, vgl. MPFS (Hrsg.), JIM-Studie 2012, 43.
[47] Vgl. Palfrey/Gasser, Generation Internet, 30.
[48] Vgl. Miller, Das wilde Netzwerk, 161.
[49] Vgl. Palfrey/Gasser, Generation Internet, 39
[50] Facebook-AGBs: Das Unternehmen erstellt zum einen Sicherheitskopien der persönlichen Daten und zum anderen erfolgt bei der Löschung eines Facebook-Accounts keine Löschung von persönlichen Inhalten, die mit anderen Facebook-Nutzern verknüpft bzw. ‚markiert‘ sind.
[51] Palfrey/Gasser, Generation Internet, 37.
[52] Vgl. Trepte/Reinecke, in: Zeitschrift für Kommunikationsökologie und Medienethik 11/(1), 35; Palfrey/Gasser, Generation Internet, 28

Nachdruck, dass der Identitätsdiebstahl eine der inzwischen häufigsten Straftaten weltweit ist.[53]

Warum aber sind insbesondere Jugendliche bereit, eine Vielzahl persönlicher Daten zu offenbaren? Es geht um den Wunsch der Teilhabe an sozialen Prozessen. *Laubner* und *Wagner* kommentieren: „Neben der Zugehörigkeit zur realen Peergroup wird auch der virtuelle Raum zunehmend relevant für die Erfahrung sozialer Gemeinschaft."[54] Die Offenbarung privater Informationen im Netz ist eng verbunden mit der Etablierung von Gruppenzugehörigkeiten.[55]

Die Erklärung für die große Sogwirkung des Internets (besonders soziale Netzwerke) liegt im Gesetz der Reziprozität[56]. Die Arbeitsweise sozialer Online-Netzwerke u.ä. beruht darauf, dass sich die Nutzer durch ein Prinzip des ‚Gebens und Nehmens' dazu verpflichten, etwas von sich preiszugeben. Hier wird das Dilemma rund um die Preisgabe privater Daten deutlich. Ein großer Teil der Sozialisation und Identitätsbildung von Jugendlichen findet heutzutage online statt. Eine Unterscheidung zwischen Online- und Offline-Identität gibt es kaum noch.[57] Die Teilhabe an der schönen, neuen, virtuellen Welt ‚erkauft' man sich letztlich durch die Preisgabe von Daten. Verweigert man sich diesbezüglich, birgt das die Gefahr sozialer Isolation. Inzwischen tangieren Online-Ereignisse das reale Leben (etwa wenn sich eine Peergroup in der Schule über veröffentliche Beiträge auf Facebook unterhält). Beispielsweise haben Jugendliche über produktives Medienhandeln (*Youtube* etc.) die Möglichkeit, ihre Autonomie zu verdeutlichen, was im Ergebnis zu der Chance der Partizipation in der sozialen Welt führt.[58]

Dass hier vielfach ökonomische Interessen der Internetunternehmen verfolgt werden, ist offensichtlich. Es geht häufig um personalisierte und standortbezogene Werbung auf der Grundlage erlangter persönlicher Daten. *Lindner*, Politiker der *Freien Demokratischen Partei (FDP)*, erklärt: „Daten sind die

[53] Vgl. Palfrey/Gasser, Generation Internet, 28.
[54] Lauber/Wagner, in: Kommunikation, Partizipation und Wirkungen im Social Web, 184.
[55] Vgl. Palfrey/Gasser, Generation Internet, 30.
[56] Reziprozität = Gegenseitigkeit, vgl. Palfrey/Gasser, Generation Internet, 27-30.
[57] Vgl. Palfrey/Gasser, Generation Internet, 42.
[58] Vgl. Lauber/Wagner, in: Kommunikation, Partizipation und Wirkungen im Social Web, 184.

neue Leitwährung.“[59] Häufig überwiegt die Faszination oder der offenkundige Vorteil, sodass Nutzer über die Preisgabe ihrer Daten hinwegsehen. Die Berechenbarkeit menschlichen Verhaltens im Netz ist dabei von entscheidender Bedeutung (vgl. ‚rational-choice-theory‘).[60]

2.5 Zwischenergebnis: Allgegenwärtige Vernetzung - Möglichkeiten und Missbrauch

Das Internet hat seit seiner Privatisierung in den 1990er Jahren eine unglaubliche Entwicklung durchlaufen. Diese lässt sich insgesamt durch einen stetigen technischen Fortschritt mit wachsenden Möglichkeiten und durch eine zunehmende Vernetzung verschiedener Lebensbereiche charakterisieren. Die Menschen sind generationsübergreifend von den Möglichkeiten und Vereinfachungen durch das Internet fasziniert. Dass dies allerdings nur eine Seite der Medaille ist, wird häufig ausgeblendet. Auch die Wirtschaft hat frühzeitig Einzug in das Internet genommen. Es überwiegen ökonomische Interessen, der Handel mit (persönlichen) Daten boomt. Erst die Enthüllungen *Edward Snowdens* im Juni 2013 sensibilisierten die Menschen in Bezug auf den Umgang mit persönlichen Daten. Dabei ist der Missbrauch von Daten und den modernen IuK-Technologien nicht erst seit der NSA-Affäre greifbar. Schon seit Jahren beobachten die Sicherheitsbehörden eine wachsende Anzahl von Straftaten im Bereich der IuK-Kriminalität (vgl. Kapitel 4.2.).
Dass *Bundeskanzlerin Merkel* noch im Juni dieses Jahres vom Internet als Neuland sprach, ließ viele Menschen schmunzeln.[61] Doch tatsächlich weist diese Aussage auf reale und gesamtgesellschaftliche Herausforderungen in der Zukunft hin. *Lindner* konstatiert einen Strukturwandel von Staat, Wirtschaft und Gesellschaft in Zeiten der Digitalisierung aller Lebensbereiche. Er fordert den Staat auf, Regeln zu setzten, um dem wachsenden Datenmarkt Einhalt zu gewähren.[62] Dass diese Datendebatte auch mit Blick auf die Straftaten der IuK-Kriminalität relevant ist, zeigt die nachfolgende Analyse.

[59] Lindner, in: FAZ, 14.08.2013, 25.
[60] Vgl. Gropp/Knop (im Interview mit dem Chef von Google-Deutschland), in: FAZ, 16.09.2013, 22.
[61] Knop, in: FAZ, 20.06.2013, 9.
[62] Vgl. Lindner, in: FAZ, 14.08.2013, 25.

3 Der Modus Operandi bei der Begehung von Straftaten

Groß, Begründer der deutschsprachigen wissenschaftlichen Kriminalistik, und *Geerds* diskutierten 1977, wie auf der Grundlage des ‚Modus Operandi' und der ‚Perseveranz' ein System der Verbrechenstechnik, also eine sinnvolle Kategorisierung krimineller Handlungen, funktionieren könnte.[63] Die Autoren definierten den Begriff Modus Operandi dabei als „[…] die durch bestimmte Merkmale gekennzeichnete Art und Weise der Ausführung einer kriminellen Tat […]"[64]. Unter Perseveranz verstanden sie „[…] das Phänomen wiederholt begangener Straftaten mit im wesentlichen [sic!] gleichartiger, eigentypischer Technik […]"[65]. Mit dem Wissen um diese beiden Faktoren wurden Fragen der Klassifikation erörtert. Das Begriffsverständnis hat sich bis zum heutigen Zeitpunkt nicht geändert.

3.1 Kriminalistische Bedeutung

Kriminalistisch haben der Modus Operandi und die Perseveranz damals wie heute vornehmlich eine Bedeutung für den *Kriminalpolizeilichen Meldedienst (KPMD)*. Ziel dieser Einrichtung ist der Vergleich von kriminellen Arbeitsweisen und der Erkenntnisabgleich von zeitlich und örtlich voneinander abweichenden Straftaten mit dem Ziel der Gewinnung von Täterhinweisen und der Aufdeckung von Straftatenserien.[66]

Der Meldedienst beruht auf der theoretischen Erkenntnis, dass ein Täter an einem bestimmten Deliktsfeld und einer bestimmten Vorgehensweise bei der Tatausführung festhält. Dadurch soll der Täter wiedererkannt werden können.[67] Durch die Mitteilung der Tatbegehungsweisen an den Meldedienst können Straftatenserien erkannt und Täterhinweise gesammelt werden.

---

[63] Vgl. Groß (Begr.)/Geerds (Bearb.), Handbuch der Kriminalistik, 152-162.
[64] Groß (Begr.)/Geerds (Bearb.), Handbuch der Kriminalistik, 148.
[65] Groß (Begr.)/Geerds (Bearb.), Handbuch der Kriminalistik, 157.
[66] Vgl. Weihmann/Schuch, Kriminalistik, 595.
[67] Gemeint ist die wiederholte Begehung der gleichen Straftat (Perseveranz) mit wiederholt gleicher Tatausführung (Modus Operandi), vgl. Karliczek, in: KrimLex-Online „Perseveranz".

Ob der KPMD ein taugliches Instrument der Kriminalitätsbekämpfung ist, ist seit jeher umstritten.[68] Unumstritten hat Kapitel 2 jedoch gezeigt, dass die moderne IuK-Technologie zu erheblichen gesellschaftlichen Veränderungen geführt hat. Als integraler Bestandteil der Gesellschaft ist davon auch die Kriminalität betroffen. *Groß* und *Geerds* wiesen schon 1977 darauf hin, dass sich auch die Rechtsbrecher neuen technischen und sozialen Gegebenheiten anpassen, was unweigerlich zu Schwierigkeiten eines langfristig gültigen Systems der Verbrechenstechnik bzw. zu dynamischen Wandlungsprozessen des Modus Operandi führt.[69] Dies leitet zur Forschungsfrage über. Wozu haben die moderne IuK-Technologie geführt. Wie hat sich Kriminalität verändert? Sind neue Kriminalitätsformen entstanden oder hat unsere Gesellschaft einen Wandel im Bereich des Modus Operandi erfahren?

Noch einmal zurück zum *Kriminalpolizeilichen Meldedienst*. Dort werden nur ausgewählte Straftaten (besondere Sozialschädlichkeit) bzw. ausgewählte Begehungsweisen erfasst und ausgewertet.[70] Davon waren Straftaten der IuK-Kriminalität nicht erfasst. Die Polizei hat aber auf den dargestellten Wandel reagiert. Die *Arbeitsgemeinschaft Kripo (AG Kripo)*, bestehend aus den Leitern der *Landeskriminalämter (LKÄ)* und dem Leiter des *Bundeskriminalamts (BKA)*, beschloss 1985 die Einführung des Sondermeldedienstes *‚Computerkriminalität und Bedrohung der Informationstechnik‘*. 1997 wurde der Meldedienst in die Bezeichnung *‚Informations- und Kommunikationstechnik‘* umbenannt. Der Meldeumfang wurde durch eine nicht abschließende Aufzählung geregelt. Dieser Umstand und die Tatsache, dass der Meldedienst zu wenig genutzt wurde, erschwerte die Informationsgewinnung.[71] Noch heute bestehen Mängel im Bereich des Informationsaustauschs. Ermittler fordern nach wie vor einen frühzeitigen und intensiven Informationsaustausch, der über den normalen Meldedienst hinausgeht.[72] Zusammenfassend muss also festgestellt werden, dass der Meldedienst allein kein taugli

[68] Untersuchungen des BKA und der FHöV NRW liefern Anzeichen dafür, dass selbst Sexualstraftäter (häufig Triebtäter) kein kriminelles Verhalten aufweisen, welches die theoretische Annahme des KPMD unterstützt, vgl. Burgheim/Friese, in: Kriminalistik 8-9/2006, 512; Straub/Witt, in: Kriminalistik 1/2003, 29.
[69] Vgl. Groß (Begr.)/Geerds (Bearb.), Handbuch der Kriminalistik, 162.
[70] Vgl. Weihmann/Schuch, Kriminalistik, 596.
[71] Vgl. Wiedemann, in: Kriminalistik 4/2000, 238.
[72] Vgl. Burandt/Tölle, in: Kriminalistik 8-9/2013, 525.

ches Instrument ist, um die Forschungsfrage beantworten zu können. Vielmehr bedarf es der angekündigten Analyse verschiedener Einzelfälle.

3.2 Strafrechtliche Bedeutung

Aus strafrechtlicher Sicht hat die Art und Weise der Begehung von Straftaten eventuell Auswirkungen auf die Strafbarkeit nach dem *Strafgesetzbuch (StGB)*. Dabei geht es insbesondere um Qualifizierungen, die durch eine bestimmte Begehung tatbestandsmäßig werden. Begeht ein Täter z.B. einen Totschlag gemäß § 212 StGB auf eine grausame Art und Weise, so handelt es sich um die tatbestandsmäßige Verwirklichung eines objektiven Mordmerkmals gemäß § 211 (2) StGB.[73] Der besondere Modus Operandi führt in diesem Fall zu einer lebenslangen Haftstrafe. Die Freiheitsstrafe für einen Totschlag hingegen beläuft sich auf maximal zehn Jahre.

Im Bereich der IuK-Kriminalität ist der strafrechtliche Aspekt des Modus Operandi zum Beispiel mit Blick auf eine Abgrenzung zwischen § 263 und § 263a StGB relevant. Darauf wird im Rahmen der phänomenologischen Analyse eingegangen (Kapitel 4.3.1.1).

4 Phänomenologische Analyse der IuK-Kriminalität

Die Thematik der IuK-Kriminalität, zuvor auch Computerkriminalität genannt, ist kein alleiniges Phänomen des 21. Jahrhunderts. Fragen zum Ausmaß und den phänomenologischen Erscheinungen beschäftigen die Organe der Strafrechtspflege schon lange. Verschiedene Kriminalisten, Kriminologen und Juristen äußerten sich dazu. Bereits im Dezember 1986 schrieb *Poerting*: „Der Begriffsumfang dessen, was mit dem Terminus Computerkriminalität bezeichnet wird, ist auch nach Verabschiedung des *Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)* weiterhin unscharf.“[74] Etwa zehn Jahre später, 1998, stellte *Janovsky* fest, dass der kriminelle Miss-

[73] Vgl. Kindhäuser, Strafrecht BT, § 1 Rn. 2, § 2 Rn. 31-32.
[74] Poerting, in: Kriminalistik 12/1986, 615.

brauch des Internets in seinen Dimensionen kaum abschätzbare Gefahren mitgebracht habe.[75] 2010, also wiederum gut zehn Jahre später, schrieb *Kreitlow*, dass die Erkenntnislage zur Bedrohung durch die IuK-Kriminalität unzureichend sei.[76] *Robertz* ergänzte 2011, dass eine quantitative Einschätzung des Phänomens der IuK-Kriminalität aus kriminologischer Sicht kaum möglich sei.[77]

Im Jahr 2013 ist das Thema der IuK-Kriminalität intensiver denn je Gegenstand medialer Berichterstattungen, wissenschaftlicher Untersuchungen und sicherheitspolitischer Debatten. Die hier einleitend skizzierten Aussagen lassen jedoch zunächst die Frage zu, wovon Medien, Wissenschaft und Akteure der Sicherheitspolitik überhaupt sprechen, wenn von Cybercrime, IuK-Kriminalität, Computer- oder Internetkriminalität und deren Ausmaß die Rede ist?

4.1 Definitorische Aspekte der IuK-Kriminalität

4.1.1 Die Entwicklung der IuK-Kriminalität im 20. Jahrhundert

Mit dem Einzug des modernen Computers in die Industrie und Wirtschaft – der Kriminologe *Kaiser* sprach 1989 von der „Verlagerung menschlicher Geistestätigkeit auf Maschinen“[78] – ergab sich bald auch das Problem der missbräuchlichen Nutzung von Computern. Erste Untersuchungen zum neuartigen Komplex der Computerkriminalität wurden in Deutschland in den 1970er und 1980er Jahren durchgeführt. *Sieben*, Betriebswirtschaftler und Wirtschaftsprüfer, und *von zur Mühlen*, Unternehmensberater für Sicherheits- und Revisionsfragen, definierten Computerkriminalität 1973 folgendermaßen: „Die Verfasser dieses Beitrags verstehen unter Computerkriminalität alle die Delikte, bei denen der Computer Werkzeug oder Ziel der Tathandlung ist, wobei die Tat durch den Einsatz des Computers ermöglicht, [sic!] oder erleichtert oder durch die Entdeckung erschwert wird.“[79] Da das Internet zum

[75] Vgl. Janovsky, in: Kriminalistik 7/1998, 500.
[76] Vgl. Kreitlow, in: Die Polizei 10/2010, 292.
[77] Vgl. Robertz, in: DP 9/2011, 29.
[78] Kaiser, Kriminologie, 456.
[79] Sieben/von zur Mühlen, in: DSWR 23/1973, 253.

Zeitpunkt dieser Definition lediglich in der Form des *ARPANET* bestand, wurde es keineswegs berücksichtigt. Computerkriminalität bezog sich also ausschließlich auf die Rechenleistung des Computers und dessen Manipulierbarkeit.

Die sich seit den 1960er Jahren stets weiterentwickelnde Computertechnik nahm zunehmend Einfluss auf das gesellschaftliche Leben. Schnell wurde es problematisch, von den gesellschaftlichen Normen abweichende Verhaltensweisen in Bezug auf die moderne Computertechnik unter den bestehenden Vorschriften des Strafgesetzbuchs zu subsumieren. Als Beispiel sei darauf hingewiesen, dass Tatmittel und Tatobjekt häufig in Form von unkörperlichen Gegenständen (Daten, Netzwerken, Software etc.) auftraten. Die herkömmlichen Straftatbestände begründeten somit keine Strafbarkeit.[80] Die Organe der Strafrechtspflege waren handlungsunfähig. Dieser Entwicklung wirkte der Gesetzgeber durch das *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)* vom 15. Mai 1986 entgegen.[81] Durch diesen Rechtsakt wurden neben Strafvorschriften der Wirtschaftskriminalität auch die Kerntatbestände der heutigen Computerkriminalität bzw. der IuK-Kriminalität verabschiedet.

Im einzelnen wurde durch das 2. WiKG folgendes unter Strafe gestellt:

§ 202a StGB	Ausspähen von Daten
§ 303a StGB § 303b StGB	Datenveränderung Computersabotage
§ 269 StGB § 270 StGB	Fälschung beweiserheblicher Daten Täuschung im Rechtsverkehr mit der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr
§ 263a StGB	Computerbetrug
§ 17 UWG	Schutz von Geschäfts- und Betriebsgeheimnissen

Mit den Inhalten des 2. WiKG war die Computerkriminalität jetzt auch unabhängig von den Tatbeständen der Wirtschaftskriminalität greifbar. Dies äußerte sich darin, dass die *Polizeiliche Kriminalstatistik (PKS)* die Computerkriminalität erstmalig 1987 gesondert auswies.[82]

[80] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 458.
[81] Vgl. BT-Drucks. 10/318; BGBl. 1986/21, 721.
[82] Vgl. Dornseif, Phänomenologie der IT-Delinquenz, 99.

Die *Polizeiliche Kriminalstatistik* ist seit jeher eine wichtige Arbeitsgrundlage für die polizeiliche Arbeit. Seit 1953 ist die Kriminalstatistik das maßgebliche Erkenntnismittel für die sogenannte Hellfeld-Kriminalität. Die Statistik erfasst alle der Polizei bekannt gewordenen Straftaten und berücksichtigt die im Rahmen der polizeilichen Ermittlungen gewonnen Erkenntnisse bis zur Abgabe des strafrechtlichen Sachverhalts an die Staatsanwaltschaft als Herrin des Ermittlungsverfahrens gemäß § 161 (1) *Strafprozessordnung (StPO)*. Es handelt sich um eine Ausgangsstatistik. Das Instrument der Kriminalstatistik hat sich im Laufe der Jahre gewandelt. Von ursprünglich 88 Seiten ist das jährliche Druckwerk auf inzwischen mehr als 455 Seiten angewachsen. Seit 1986 existieren in der PKS sogenannte Summenschlüssel[83]; dabei handelt es sich um Gruppen von Einzeldelikten, die unter einer bestimmten Ziffernfolge (Summenschlüssel) in der PKS zusammengefasst werden.
Wenn nun von Zahlen der Computerkriminalität (oder später: IuK-Kriminalität) die Rede ist, beziehen sich diese Angaben zumeist auf die frei zugänglichen bzw. vom Bundesinnenminister veröffentlichten Zahlen der Polizeilichen Kriminalstatistik. Denn diese werden in der PKS als Zusammenschluss einzelner Straftaten, sprich als Summenschlüssel, registriert.
Dass die PKS aufgrund zahlreicher Umstände nur ein ungenaues Bild der Kriminalitätslage Deutschlands zeichnet, ist umfänglich erörtert worden.[84] *Paul* hat diesen Umstand 1995 auch für das Deliktsfeld der Computerkriminalität festgestellt.[85] Mitursächlich dafür ist das sogenannte Dunkelfeld. Auch dieses Dunkelfeld, also die Anzahl derjenigen Straftaten, von denen die Polizei keine Kenntnis erhält, wird bereits seit Jahren im Hinblick auf den tatsächlichen Umfang und die Struktur der Computerkriminalität diskutiert.[86]

Der Summenschlüssel der Computerkriminalität umfasste 1987 alle vom 2. WiKG begründeten computerspezifischen Straftaten des StGB. Die Polizei registrierte für das erste Berichtsjahr 1987 insgesamt 3.067 Fälle. Mit 90% wurde der Deliktsbereich durch den Computerbetrug dominiert.[87]

---

[83] Vgl. Heinz, in: Kriminalistik 7/2013, 459.
[84] Vgl. Bundesministerium des Innern (Hrsg.), IMK-Kurzbericht PKS 2012, 2-3; Kerner, Der Bürger im Staat 1/2003, 4, 5, 7-8; Göppinger (Begr.), Kriminologie, 357-358.
[85] Vgl. Paul, in: NJW-Computerreport 1/1995, 45.
[86] Vgl. Poerting, in: Kriminalistik 12/1986, 598-615.
[87] Vgl. BKA (Hrsg.), PKS 1987, 88.

4.1.2 Die IuK-Kriminalität im 21. Jahrhundert

Während bis in die 1990er Jahre nahezu ausschließlich von Computerkriminalität die Rede war[88], ist dieser Begriff in der Wissenschaft, Lehre und Praxis 1997 durch die Bezeichnung ‚Informations- und Kommunikationskriminalität' ergänzt und bisweilen ersetzt worden.[89] Ursächlich hierfür sind die in Kapitel 2 skizzierten technischen Entwicklungen. Während die Möglichkeiten der elektronischen Datenverarbeitung lange Zeit dem Staat und einzelnen Wirtschaftsunternehmen vorbehalten waren, hat die ‚Privatisierung der Computerindustrie' dazu geführt, dass die sog. Personal-Computer (PC) Einzug in das gesellschaftliche Leben nahmen.[90] Als dieser Umstand im Laufe der 1990er Jahre durch die wachsenden Möglichkeiten des Internets ergänzt wurde, stand nicht mehr (nur) die Rechenleistung eines Gerätes der elektronischen Datenverarbeitung im Fokus. Die Nutzungsvielfalt der in den Wohn- und Arbeitszimmern stehenden Computer war nicht mehr mit den Anwendungen der Wirtschaftsrechner zu vergleichen. Mit der durch das Internet gestiegenen Nutzungsvielfalt stieg jedoch gleichzeitig die Vielfalt an computer- und netzspezifischen Straftaten. Der Begriff der Computerkriminalität griff also langfristig zu kurz.[91]

Bislang war ausschließlich von Computerkriminalität und IuK-Kriminalität die Rede. Nun muss ein weiterer Begriff eingeführt werden. Polizeiliche und politische Institutionen nutzen im Kontext von IuK-Kriminalität häufig den Begriff ‚Cybercrime'.

Das Bundeslagebild Cybercrime des *Bundeskriminalamts (BKA)* definiert das Kriminalitätsphänomen im Jahr 2013 wie folgt: „Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden."[92]

Die Nutzung dieses englischen Begriffs im Kontext eines deutschen Kriminalitätslagebildes ist beachtlich. Der Runderlass des *Ministeriums für Inneres*

[88] Vgl. Paul, in: NJW-Computerreport 1/1995, 42.
[89] Vgl. BKA (Hrsg.), Bericht AG Internet, zitiert nach: Jofer, Strafverfolgung im Internet, 33.
[90] Vgl. Sieber, in: CR 2/1995, 106.
[91] Vgl. Jofer, Strafverfolgung im Internet, 33.
[92] BKA (Hrsg.), Cybercrime Bundeslagebild 2012, 3.

und Kommunales des Landes Nordrhein-Westfalen (NRW) zur Bekämpfung der IuK-Kriminalität stellt dazu fest: „IuK-Kriminalität ist dem international gebräuchlichen Begriff ‚Cybercrime' gleichzusetzen."[93] Allein die Einführung dieses Anglizismus in die Sprache der deutschen Sicherheitsarchitektur ist ein Beleg für die internationale Bedeutung dieses Kriminalitätsphänomens. Damit tragen die Sicherheitsbehörden der Tatsache Rechnung, dass die Täter in einer virtuellen Welt ohne Staatsgrenzen agieren und territoriale Geltungsbereiche von Sprache und Recht weitgehend unerheblich sind (vgl. Kapitel 5). Ein eindrucksvoller Beweis dafür ist sicherlich die aktuelle Debatte um die nachrichtendienstlichen Tätigkeiten der NSA und bisweilen des britischen Geheimdienstes *Government Communication Headquarters (GCHQ)* rund um die Späh- und Abhörprogramme ‚Prism' und ‚Tempora'.

Zurück zu den definitorischen Aspekten: Die Formulierung im Lagebild des BKA „[…] umfasst auch solche Straftaten, […]"[94] deutet auf eine Differenzierung des Kriminalitätsphänomens hin. Es wird zwischen einer IuK-Kriminalität im engeren Sinn (i.e.S.) und einer IuK-Kriminalität im weiteren Sinn (i.w.S.) unterschieden. Diese Einteilung hat sich seit 1973 entwickelt, durchgesetzt und wird von der Wissenschaft, Praxis und Lehre aufgegriffen. Die Polizeiliche Kriminalstatistik arbeitet damit[95], *Ratzel* nimmt darauf im Rahmen der *BKA-Herbsttagung* 2003 Bezug[96], die *Fortschreibung des Programms Innere Sicherheit 2008/2009* macht sich der Kategorisierung zu eigen[97] und auch Lehrbücher vermitteln diese Einteilung[98].

Für weitergehende definitorische Aspekte können die Inhalte des Programms Innere Sicherheit als Ausgangspunkt herangezogen werden. Diese sind von der Innenministerkonferenz festgeschrieben worden und haben einen richtungsweisenden Charakter als kriminalpolitische Grundentscheidung und für ein in der Bundesrepublik abgestimmtes Handeln.[99]

[93] Vgl. Rd.-Erlass des MIK NRW v. 29.02.2013 – 423-62.18.09.
[94] Vgl. BKA (Hrsg.), Cybercrime Bundeslagebild 2012, 3.
[95] Vgl. BMI (Hrsg.), IMK-Kurzbericht PKS 2012, 4.
[96] Vgl. Ratzel, in: IuK-Kriminalität, 33-34.
[97] Vgl. Innenministerkonferenz (Hrsg.), Programm Innere Sicherheit, 33-37.
[98] Vgl. z.B. Wernert, Internetkriminalität, 14-17.
[99] Vgl. Weihmann/Schuch, Kriminalistik, 132.

Demnach umfasst die IuK-Kriminalität i.e.S. alle Straftaten, „bei denen Elemente der Elektronischen Datenverarbeitung (EDV) in den Tatbestandsmerkmalen enthalten sind (Computerkriminalität).“[100] Komplettiert wird das Kriminalitätsphänomen schließlich durch die IuK-Kriminalität i.w.S. Dabei geht es um diejenigen Straftaten, „bei denen Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird.“[101]. Erfasst werden diese durch eine vom BKA seit 2004 geführte Tabelle, in welcher sämtliche Straftaten aufgeführt werden, die unter Ausnutzung des Internets als Tatmittel begangen werden bzw. wurden (Tabelle: ‚Tatmittel Internet‘). Die potenziell möglichen Straftaten der IuK-Kriminalität i.w.S. sind demnach kaum überschaubar – dazu später mehr (vgl. Kapitel 4.3.3).
Die Taten der IuK-Kriminalität i.e.S. hingegen sind definiert und werden als Summenschlüssel und Teilmenge der Straftatengruppe der Computerkriminalität erfasst. Zwecks größtmöglicher Transparenz werden nachfolgend die Straftatengruppen aufgeschlüsselt und vergleichend dargestellt:

PKS-Schlüssel	**Straftatengruppe: Computerkriminalität[102]**	**Straftatengruppe: IuK-Kriminalität[103]**
516300	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	
517500	Computerbetrug § 263a StGB	Computerbetrug § 263a StGB
517900	Betrug mit Zugangsberechtigung zu Kommunikationsdiensten	Betrug mit Zugangsberechtigung zu Kommunikationsdiensten
543000	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung - §§ 269, 270 StGB -	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung - §§ 269, 270 StGB -
674200	Datenveränderung, Datensabotage - §§ 303a, 303b StGB -	Datenveränderung, Datensabotage - §§ 303a, 303b StGB -
678000	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlung	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlung
715100	Softwarepiraterie (private Anwendung z.B. Computerspiele)	
715200	Softwarepiraterie in Form gewerbsmäßigen Handelns	

Wie die tabellarische Übersicht zeigt, herrscht zwischen den Gruppen der Computer- und IuK-Kriminalität zwar eine gewisse Übereinstimmung. Da der ‚Betrug mittels rechtswidrig erlangter Debitkarte mit PIN‘ und die Delikte der ‚Softwarepiraterie‘ jedoch nicht unter der Definition der IuK-Kriminalität i.e.S.

[100] Vgl. Innenministerkonferenz (Hrsg.), Programm Innere Sicherheit, 33.
[101] Vgl. Innenministerkonferenz (Hrsg.), Programm Innere Sicherheit, 34.
[102] Vgl. BKA (Hrsg.), PKS 2011, 254.
[103] Vgl. BKA (Hrsg.), PKS 2011, 29.

subsumiert werden, besteht doch keine Deckungsgleichheit. Folgerichtig muss zwischen Computer- und IuK-Kriminalität genau unterschieden werden. Das *Landeskriminalamt (LKA) NRW* hat für das Berichtsjahr 2012 ein umfassendes Lagebild zum Phänomen IuK-Kriminalität (unter der Überschrift ‚Cybercrime') veröffentlicht. Interessant ist hier, dass beispielsweise das LKA NRW bei seiner Erfassung und Auswertung auch die vom BKA herausgefilterten Straftaten:

- Betrug mittels rechtswidrig erlangter Debitkarte mit PIN
- Delikte der Softwarepiraterie

unter der Kategorie Cybercrime i.e.S. subsumiert.[104] Folglich besteht zwischen den Daten von Bundesland und Bundesrepublik ein Unterschied, der sich auf angestrebte Auswertungen, Vergleiche und Aussagen auswirken kann.

In diesem Punkt besteht offensichtlich Uneinigkeit darüber, ob die IuK-Kriminalität bei diesen Straftaten das Tatobjekt darstellt, oder vielmehr als Tatmittel fungiert. Es zeigt sich, dass diese Entscheidung im Einzelfall nicht einfach ist.

In der Nachbetrachtung ist bemerkenswert, dass die *AG Projektgruppe Internet* des BKA 1997 den Begriff des „Mißbrauchs [sic!] der Informations- und Kommunikationstechnik"[105] prägte. Trotz dieser frühzeitigen begrifflichen Reaktion auf den technischen Wandel, wird die IuK-Kriminalität (als Untergruppe der Computerkriminalität) erst seit 2010 explizit auf Bundesebene von der PKS ausgewiesen. Aufgrund der weitreichenden Überschneidung mit den Delikten der Computerkriminalität und der Tatsache, dass die IuK-Kriminalität als Teilmenge der Computerkriminalität definiert ist, sind Vergleiche mit den Jahren vor 2010 nur bedingt möglich. Es ist zu vermuten, dass die begriffliche Einführung der Kategorie IuK-Kriminalität in der PKS erst eine Folge der Schwerpunktsetzung im Rahmen der *Fortschreibung des Programms Innere Sicherheit 2008/2009* war. Die gestiegene Bedeutung des Internets als Tatmittel findet immerhin seit 2004 Beachtung in der *Polizeilichen Kriminalstatistik*.[106]

[104] Vgl. LKA NRW (Hrsg.), Cybercrime in NRW Lagebild 2012, 31.
[105] BKA (Hrsg.), Bericht AG Internet, zitiert nach: Jofer, Strafverfolgung im Internet, 33.
[106] Vgl. BKA (Hrsg.), PKS 2010, 27; BKA (Hrsg.), PKS 2004, 247.

4.1.3 Die IuK-Kriminalität im Strafgesetzbuch und im internationalen Kontext

Die 1986 durch das 2. WiKG eingeführten Straftatbestände wurden letztmalig durch das *41. Strafrechtsänderungsgesetz (StrÄndG)* zur Bekämpfung der Computerkriminalität vom 11.08.2007 modifiziert. Es beruht vornehmlich auf einem EU-Rahmenbeschluss über Angriffe auf Informationssysteme.[107] Damit sollten Anpassungen der nationalen Strafgesetzgebung mit Blick auf die internationale Herausforderung vorgenommen werden.
Eine wichtige Erkenntnis dieser letzten Anpassung ist in dem Wortlaut der Gesetzestexte der Strafvorschriften des StGB zu sehen. Die Vorschriften verwenden die Begrifflichkeiten der Informations- und Kommunikationskriminalität bzw. -technologie nicht. Es ist ausschließlich von Daten, Datenverarbeitung und Computern die Rede. Der Datenbegriff wird durch § 202a (2) StGB näher beschrieben: „Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden." Das Strafgesetzbuch reduziert das Kriminalitätsphänomen der IuK-Kriminalität i.e.S. somit auf elektronische Prozesse im Zusammenhang mit Daten und auf die dazu notwendigen Geräte elektronischer Datenverarbeitung.

Neben diesem Aspekt unterstreicht das 41. StrÄndG die internationale Dimension des hier diskutierten Kriminalitätsphänomens. Folglich ist auch ein kurzer Blick auf definitorische Aspekte im internationalen Kontext notwendig.
Seitens des Europarates wurde seit 1997 an einem *‚Übereinkommen über Computerkriminalität' (Cybercrime Konvention)* gearbeitet. Der *Europarat* ist nicht auf die Mitgliedsstaaten der Europäischen Union beschränkt. Die Institution umfasst insgesamt 48 Mitgliedsstaaten, darunter auch die *Vereinigten Staaten von Amerika*. Die Konvention wurde im Jahr 2001 verabschiedet[108] und 2009 schließlich von *Deutschland* ratifiziert.[109] Grund für die achtjährige Dauer war große Kritik an den Inhalten der Konvention.[110] Die nun auch für Deutschland gültige Konvention hält eine eigene Definition von ‚Cybercrime'

[107] Vgl. ABl. EU 2005 L 69, 67.
[108] Vgl. SEV Nr. 185.
[109] Zum Gesetzesentwurf der Bundesregierung: Vgl. BT-Drucks. 16/7218.
[110] Breyer, in: DuD 25/2001, 592-600.

bereit. Bei der Beurteilung der folgenden Definition muss allerdings berücksichtigt werden, dass der Europarat im Gegensatz zum Bundeskriminalamt eine politische Institution ist. Dadurch verfolgt die Begriffsbestimmung auf dieser Ebene einen politischen Anspruch und weniger den einer effektiven, kriminalistischen Kriminalitätsbekämpfung.
Die Konvention umfasst folgende Straftaten vom Begriff der Cybercrime:

Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und –systemen
Computerbezogene Straftaten (computerbezogene Fälschung und Betrug)
Inhaltsbezogene Straftaten (Kinderpornografie)
Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte
Mittels Computersystemen begangene Handlungen rassistischer und fremdenfeindlicher Art (gem. Zusatzprotokoll aus dem Jahr 2006)[111]

Der *Europarat* nimmt mit dieser Aufzählung Abstand von einer Teilung in einen engeren und einen weiteren Sinn. Insbesondere durch die Berücksichtigung ‚inhaltsbezogener Straftaten' werden aber auch die Delikte abgedeckt, die mittels moderner IuK-Technologien begangen werden – also Straftaten der IuK-Kriminalität i.w.S.

Insbesondere die politischen Organe der deutschen Sicherheitsarchitektur nähern sich dem internationalen Sprachgebrauch an. Das *Bundesministerium des Innern* spricht inzwischen vornehmlich von ‚Cyberkriminalität'. Unabhängig der PKS tragen auch die jährlichen Lagebilder des *Bundeskriminalamts* und der *Landeskriminalämter* den Titel ‚Lagebild Cybercrime' o.ä. Insgesamt scheint sich dieser Begriff langfristig durchzusetzen.

[111] Vgl. SEV Nr. 185; zum Zusatzprotokoll, vgl. SEV Nr. 189.

4.1.4 Zwischenergebnis: Von Computerkriminalität über IuK-Kriminalität zu Cybercrime

Zusammenfassend kann folgendes festgestellt werden:

- Die IuK-Kriminalität hat sich aus der Computerkriminalität entwickelt
- National wird zwischen der IuK-Kriminalität i.e.S. (IuK-Technologie als Tatobjekt) und der IuK-Kriminalität i.w.S. (IuK-Technologie als Tatmittel) unterschieden
- Die IuK-Kriminalität i.e.S. wird von der PKS als Untergruppe der Computerkriminalität erfasst
- Die IuK-Kriminalität i.w.S. wird von der PKS durch eine Tabelle ‚Tatmittel Internet' gesondert erfasst
- Der Begriff IuK-Kriminalität ist dem Begriff Cybercrime gleichzusetzen
- Cybercrime ist durch die ‚Cybercrime Konvention' des Europarates definiert. Dabei wird einer Kategorisierung in einen engeren und einen weiteren Sinn nicht entsprochen. Die Definition umfasst das Kriminalitätsphänomen dennoch ganzheitlich
- Es ist eine begriffliche Entwicklung von Computerkriminalität, über IuK-Kriminalität zu Cybercrime zu verfolgen

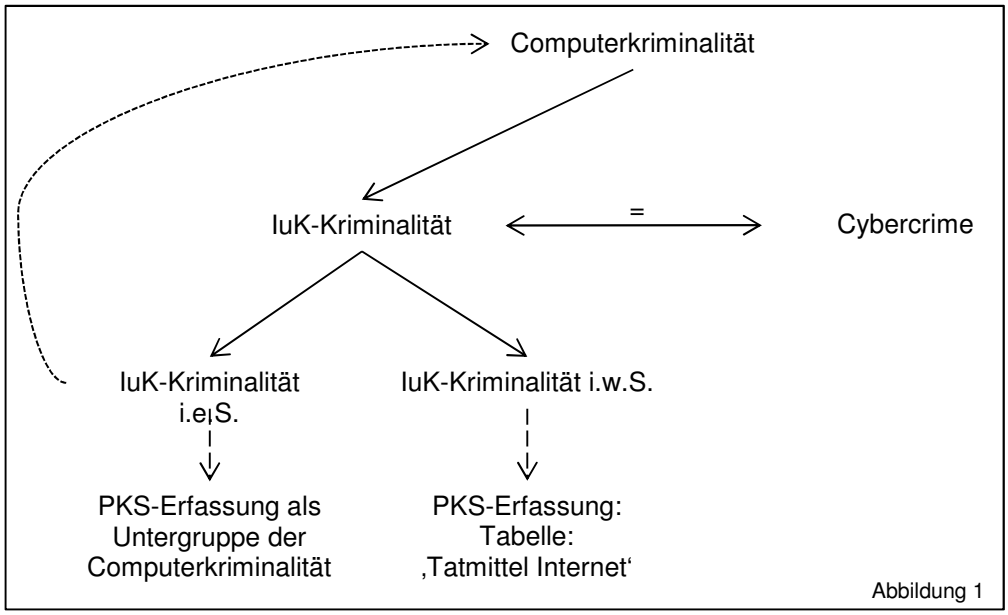

Abbildung 1

Die begriffliche Vielfalt, die Modifizierung und die in Ansätzen aufgezeigte Uneinheitlichkeit der im Kontext von IuK-Kriminalität relevanten Begriffe erschweren die Orientierung. Letztlich erschweren sie aber auch ein realistisches Lagebild und lassen weitergehende Schwierigkeiten im Bereich der Arbeit von Strafverfolgungsbehörden und Gerichten vermuten.

Für den weiteren Verlauf der Arbeit gilt, dass mit dem Begriff der IuK-Kriminalität gearbeitet wird. Bei der Einzelfallanalyse dient die in Deutschland gängige Kategorisierung des Kriminalitätsphänomens als Ausgangspunkt.

4.2 Lagebild der IuK-Kriminalität

Bis ins Jahr 2013 haben sich die Erfassungsmodalitäten der PKS wiederholt geändert. Teils sind Straftatenkategorien hinzugefügt worden, teils haben (länderspezifische) Erfassungsfehler zu Verzerrungen und mangelnder Vergleichbarkeit geführt. Diese Aspekte führen zwangsläufig in ein Dilemma, wenn es um haltbare Aussagen zur IuK-Kriminalität geht. Dem wird in der Einzelanalyse Rechnung getragen. Zunächst ein Überblick:

4.2.1 Erkenntnisse zum Hellfeld

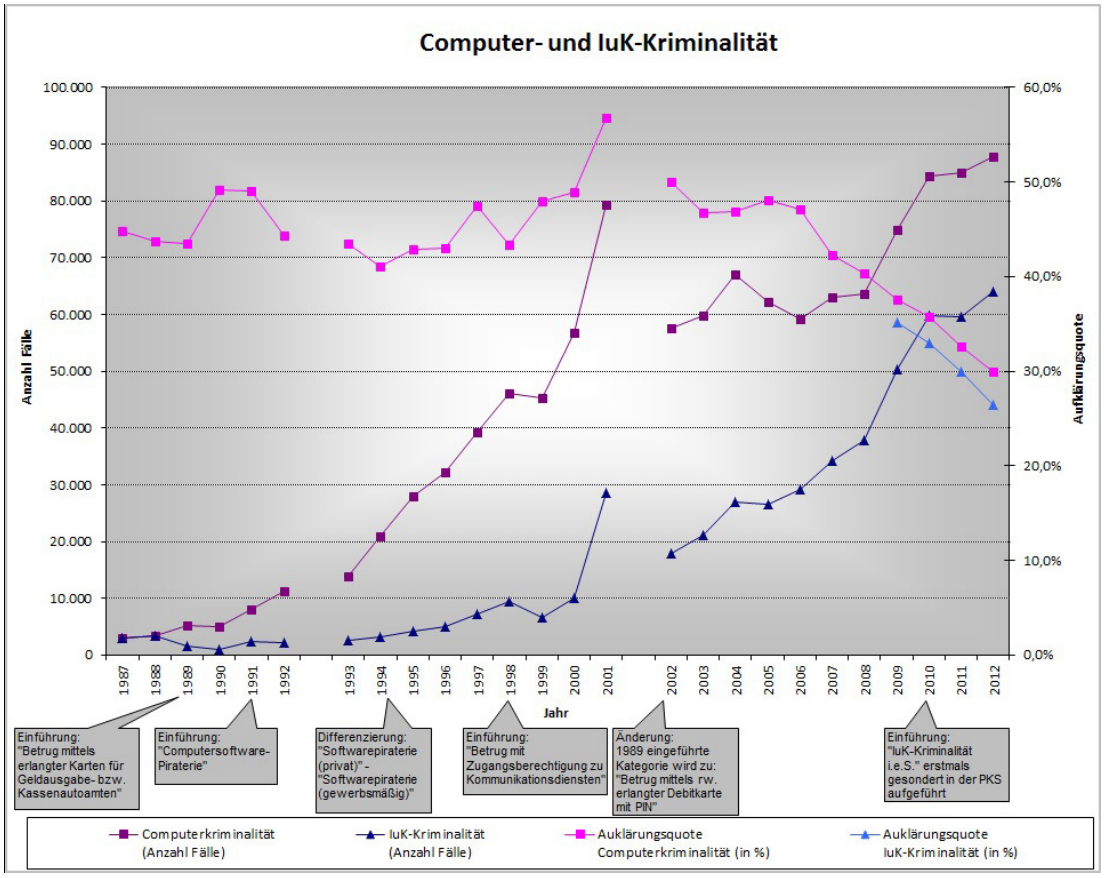

Abbildung 2

Von der erstmaligen Registrierung der Computerkriminalität 1987 bis zu den aktuell verfügbaren Daten des Jahres 2012, hat sich die Fallzahl von 3.067 auf 84.981 registrierte Fälle gesteigert.[112] Dieser Anstieg ist enorm, relativiert sich jedoch durch die bereits skizzierten Schwächen und Erfassungsmodifikationen der Kriminalstatistik (vgl. Abbildung 2).

[112] Vgl. BKA (Hrsg.), PKS 1987, 88; BMI (Hrsg.), IMK-Kurzbericht PKS 2012, 4.

Unabhängig davon ist jedoch ein im Vergleich zu anderen Deliktsgruppen starker Anstieg über die Jahre nicht zu bestreiten. Dieser Zuwachs der Fallzahlen wurde bis zur Jahrtausendwende erheblich durch die Delikte des Computerbetrugs geprägt. Zwar dominieren die Betrugsdelikte auch heute die Fallzahlen des Summenschlüssels Computerkriminalität, dennoch haben auch andere Kategorien an Bedeutung gewonnen. Eine gewisse Ausdifferenzierung der Computerkriminalität ist zu beobachten.
Für das Berichtsjahr 2010 erfasste die PKS 59.838 Taten der IuK-Kriminalität i.e.S. als Teilmenge der Computerkriminalität. Diese Zahl wuchs bis 2012 um 6,88% auf 63.959 Fälle. BKA-Präsident *Ziercke* hatte 2007 festgestellt, dass sich die Quantität der Straftaten der IuK-Kriminalität i.e.S. seit 2002 auf einem relativ hohem, aber konstanten Niveau von 30.000 Taten jährlich bewegen.[113] Mit Blick auf die Fallzahlenentwicklung von 2002 bis 2012 gilt diese Feststellung nicht. Demnach sind die Taten seit 2002 konstant gestiegen und haben sich seit 2007, innerhalb von etwa fünf Jahren, mehr als verdoppelt. Allein der Anstieg im Vergleich von 2011 auf 2012 betrug 8%.[114]

Eine deliktspezifische Aufklärungsquote der einzelnen Straftaten zwischen 17,0% und 42,0% ist im Vergleich mit der durchschnittlichen Aufklärungsquote der Gesamtkriminalität (54,7%) unterdurchschnittlich. Im Durchschnitt ist die Quote für die Delikte der IuK-Kriminalität i.e.S. von 30,0% (2011) auf 26,5% (2012) gesunken. Auch wenn berücksichtigt werden muss, dass der Kriminologe und Polizeiwissenschaftler *Feltes* zu dem Ergebnis kommt, dass die Aufklärungsquote kein wirklich zuverlässiger Indikator für die Beurteilung einer effektiven Kriminalitätsbekämpfung ist[115], ist das gegenläufige Verhalten bezüglich Fallzahlenentwicklung und Entwicklung der Aufklärungsquote besorgniserregend. Dies gilt sowohl für die Delikte der Computerkriminalität, als auch für jene der Teilgruppe der IuK-Kriminalität i.e.S.

Die Tatsache, dass der Anteil der IuK-Kriminalität i.e.S. an der Gesamtkriminalität 2012 lediglich 0,9% beträgt, täuscht über die tatsächliche Bedrohung durch die IuK-Kriminalität hinweg. Als Indikator für die Bedeutung des Krimi-

[113] Vgl. Ziercke, in: Kriminalistik 2/2008, 78.
[114] Vgl. BKA (Hrsg.), Cybercrime Bundeslagebild 2012, 3.
[115] Vgl. Feltes, in: Kriminalistik 1/2009, 36-41.

nalitätsphänomens könnte sich der durch diese Taten verursachte wirtschaftliche Schaden eignen. Während dieser bis 2011 auf 71,2 Mio. Euro anwuchs, konnte für 2012 ein enormer Rückgang um ca. 40% auf 42,5 Mio. Euro verzeichnet werden. Die Aussagekraft wird jedoch abermals gemindert. Eine Schadenserfassung findet ausschließlich für die Delikte statt, die eine Strafbarkeit nach § 263a StGB begründen, sprich: ‚Computerbetrug' und ‚Betrug mit Zugangsberechtigung zu Kommunikationsdiensten'.[116] Im Hinblick auf die gesamte IuK-Kriminalität lassen sich also kaum Aussagen ableiten. Hier wir das angekündigte Dilemma deutlich: Haltbare Aussagen sind schwierig.

Ein insgesamt ähnliches Bild gilt für das Ausmaß an Straftaten mit dem Tatmittel Internet. Eine für 2012 registrierte absolute Fallzahl von 229.408[117] entspricht einem prozentualen Anteil an der Gesamtkriminalität von lediglich 3,83%. Die kriminalistische Herausforderung wird erst deutlich, wenn man die Entwicklung betrachtet. *Ziercke* konstatierte 2007 bereits einen Anstieg der Fallzahlen ‚Tatmittel Internet' (von 2005 auf 2006) von ca. 40% auf 165.000 registrierte Taten.[118] Der BKA-Präsident folgerte, dass es „kaum noch einen Kriminalitätsbereich gibt, in dem das Internet als Tatmittel keine Rolle spielt."[119] Zum Zeitpunkt dieser Aussage konnte Ziercke lediglich ahnen, dass sich die Anzahl der ‚Internetstraftaten' bis 2012 um ca. weitere 40% steigern wird.

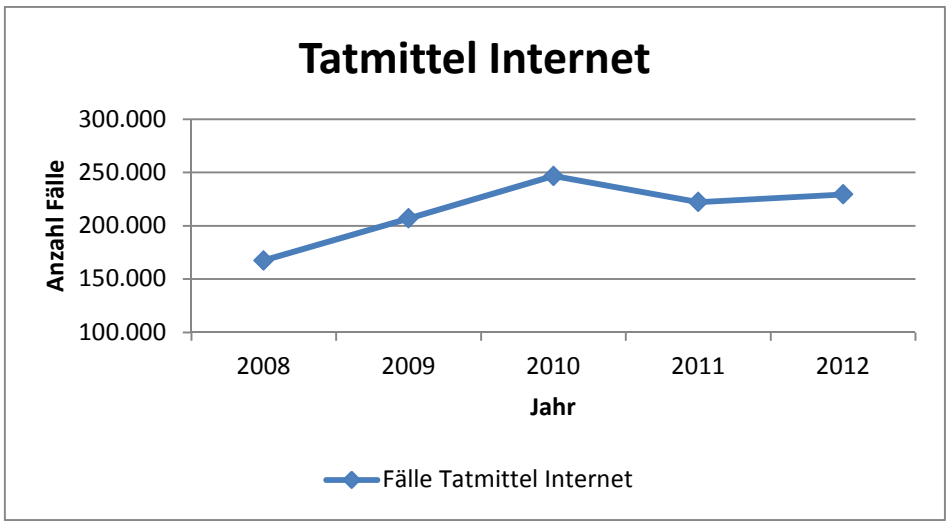

Abbildung 3

[116] Vgl. BKA (Hrsg.), Cybercrime Bundeslagebild 2012, 4.
[117] Vgl. BMI (Hrsg.), IMK-Kurzbericht PKS 2012, 9.
[118] Vgl. Ziercke, in: Kriminalistik 2/2008, 77.
[119] Ziercke, in: Kriminalistik 2/2008, 77.

Auch bei der Interpretation dieser Zahlen gilt besondere Vorsicht. Die Sondertabelle wurde zwar 2004 eingeführt, zu diesem Zeitpunkt lieferten aber lediglich zehn Bundesländer auswertbare Daten. Diese Situation verbesserte sich fortlaufend. 2005 und 2006 blieben lediglich *Bayern* und *Niedersachsen* unberücksichtigt. Seit 2007 hat auch *Niedersachsen* Anschluss gefunden. Kumulierte Zahlen für die gesamte *Bundesrepublik* liegen erst seit 2010 vor. Folglich sind Aussagen zur Entwicklung der Zahlen beeinträchtigt.[120]

Auf den ersten Blick beachtlich ist bei den ‚Internetdelikten' eine durchschnittliche Aufklärungsquote von immerhin 60,1% im Jahr 2012. Da sich diese jedoch auf sämtliche Straftaten aller kriminellen Phänomenbereiche bezieht, ist sie ebenso bedeutungslos.[121]

Festzuhalten bleibt, dass die *Polizeiliche Kriminalstatistik* trotz ihres 60-jährigen Bestehens nur bedingt geeignet ist, die Fragen im Zusammenhang mit der IuK-Kriminalität zu beantworten. Nicht umsonst erstellen die LKÄ und das BKA jährlich ein um weitere Informationen angereichertes Lagebild zum Thema Cybercrime bzw. IuK-Kriminalität.

4.2.2 Erkenntnisse zum Dunkelfeld

Neben den bereits erläuterten Schwächen der Polizeilichen Kriminalstatistik (PKS) muss das Fehlen einer systematischen Dunkelfeldforschung in Deutschland kritisiert werden. Die Kriminalität bzw. deren Ausmaß und Struktur ist die Summe des Hellfeldes und des Dunkelfeldes. Während die PKS Erkenntnisse zum Hellfeld liefert, bedarf es empirisch gesicherter Informationen zum Dunkelfeld, um das Bedrohungspotenzial eines Kriminalitätsphänomens und di e verschiedenen Möglichkeiten einer effektiven Kriminalitätsbekämpfung bewerten zu können.
Der Mangel an einer solchen „bundesweit repräsentative[n], kontinuierlich durchgeführte[n] statistikbegleitende[n] [sic!] Dunkelfeldforschung"[122] wird

[120] Vgl. BKA (Hrsg.), PKS 2004-2012, jeweilige Anmerkungen zur Auswertung ‚Tatmittel Internet'.
[121] Vgl. BKA (Hrsg.), PKS 2011, 261.
[122] Heinz, in: Kriminalistik 7/2013, 460.

seit jeher kritisiert – dies gilt sowohl allgemein als auch deliktspezifisch für die Computer- bzw. IuK-Kriminalität.

Aufgrund der Tendenz der Ausdifferenzierung der IuK-Kriminalität in alle kriminellen Bereiche, gewinnt die Erkenntnisgewinnung zunehmend an Bedeutung. *Jofer* fasst zusammen: „Die kriminalistische Bedeutung der Netzkriminalität wird auch davon abhängen, ob kriminelles Geschehen erkannt und zur Anzeige gebracht wird.“[123] *Dornseif*, der ebenfalls Ausführungen zur Dunkelfeldproblematik gemacht hat, kam 2005 zu dem Ergebnis, dass die mangelnde Datenbasis für eine Aufhellung des Dunkelfeldes im Bereich der IT-Delinquenz wesentlich einfacher sei, als in anderen Kriminalitätsbereichen. Er sah bzw. sieht Möglichkeiten der Gewinnung ungewöhnlich großer Mengen an Datenmaterial bei gleichzeitig moderatem Aufwand.[124]
Ein Jahr nach dieser Feststellung von *Dornseif* hat das *Bundesministerium des Innern* in Kooperation mit dem *Bundesministerium der Justiz* den *Zweiten Periodischen Sicherheitsbericht* veröffentlicht, der die Kriminalitätslage Deutschland unter Berücksichtigung verschiedener Erkenntnisquellen zum Hell- und Dunkelfeld zeichnet.[125] Das 830 Seiten fassende Dokument nutzt die Begriffe Computerkriminalität zweimal, IuK-Kriminalität einmal und Internetkriminalität gar nicht. Aus heutiger Sicht und vor dem Hintergrund des Themas der hiesigen Arbeit klingt diese Feststellung paradox. Folgern lässt sich daraus, dass das Phänomen der IuK-Kriminalität in all seinen Facetten erst in den letzten Jahren auf die Tagesordnung der Sicherheitspolitik gekommen ist, obwohl das Grundphänomen bereits Jahrzehnte zuvor diskutiert wurde.

Auch wenn es an validen und systematischen, deliktspezifischen Dunkelfelderkenntnissen mangelt, vermuten die Sicherheitsbehörden eine sehr große Ausdehnung.[126] Für diese Vermutung gibt es verschiedene Indizien. Zunächst wird aus unterschiedlichen Gründen nur ein Teil der tatsächlich relevanten Vorfälle als strafrechtlich relevanter Sachverhalt überhaupt wahrge-

[123] Jofer, Strafverfolgung im Internet, 39.
[124] Dornseif, Phänomenologie der IT-Delinquenz, 74.
[125] BMI/BMJ (Hrsg.), Zweiter PSB, Vorwort.
[126] Vgl. LKA NRW (Hrsg.), Cybercrime in NRW Lagebild 2012, 3; vgl. auch: BKA (Hrsg.), Kernaussagen zur IuK-Kriminalität, 2.

nommen (Angriffe auf Computer oder Netzwerk wurde nicht registriert, Antivirenprogramme haben die Straftaten im unerkannten Versuchsstadium versickern lassen). Von den wahrgenommenen Sachverhalten bringt wiederum nur ein Teil der Privatpersonen die Tat zur Anzeige.[127] Die Gründe für eine Nichtanzeige reichen vom Eindruck der Machtlosigkeit der *Polizei* bis zu einem Gefühl des als zu groß empfunden Aufwands der Anzeigenerstattung.[128]
In diesem Zusammenhang muss auf ein weiteres Phänomen verwiesen werden. Die exzessive und freiwillige Preisgabe persönlicher Daten im Internet führt zu einem Denken, das mit einer Umdefinierung der Viktimisierung[129] beschrieben werden kann. Das eigentliche Opfer fühlt sich selbst dafür verantwortlich, Opfer einer IuK-Straftat geworden zu sein und erstattet in dessen Folge keine Anzeige.[130]
Ein ganz wesentlicher und besorgniserregender Faktor im Zusammenhang mit dem Dunkelfeld und der Nichtanzeige ist die Tatsache, dass Wirtschaftsunternehmen Angriffe gegen ihre IT-Infrastruktur o.ä. nicht zur Anzeige bringen.[131] Die Forschung hat gezeigt, dass der Großteil der Unternehmen inzwischen abhängig von Informations- und Kommunikations-Systemen ist und Wirtschaftsunternehmen in hohem Maße von Cybercrime betroffen sind. Sowohl Industrie- und Wirtschaftsspionage als auch Sabotagehandlungen sind Normalität. Eine Untersuchung der *Industrie- und Handelskammer (IHK)* zusammen mit dem LKA *Schleswig-Holstein* hat 2008 herausgefunden, dass 96% der von IuK-Kriminalität betroffenen Unternehmen keine Strafanzeige erstattet haben.[132] Eine aktualisierte Studie der *IHK Nord* aus dem Jahr 2013 lässt zwar einen positiven Trend erkennen nichtsdestotrotz halten sich immer noch mehr als die Hälfte der Betroffenen zurück.[133] Die Unternehmen sorgen

[127] Ziercke, in: Kriminalistik 2/2008, 78.
[128] Für eine Übersicht zu grundsätzlichen Ursachen für die Nichtanzeige von Straftaten, vgl. Weihmann/Schuch, Kriminalistik, 583.
[129] Viktimisierung: Viktimisierung erfasst in der kriminologischen Terminologie den Prozess des ‚Zum-Opfer-Werdens'. Der Begriff beschreibt zunächst die opferorientierten Ursachen und Wirkungen der Straftat (primäre Viktimisierung). Es geht aber auch um die Folgen der Straftat für das Opfer im Kontext des sozialen Umfelds und den Instanzen sozialer Kontrolle (sekundäre, tertiäre Viktimisierung), vgl. Landwehr, in: KrimLex-Online „Viktimisierung".
[130] Vgl. Dornseif, Phänomenologie der IT-Delinquenz, 50.
[131] Vgl. Dornseif, Phänomenologie der IT-Delinquenz, 52-63; Kreitlow, in: Die Polizei 10/2010, 292.
[132] IHK Schleswig-Holstein/LKA SH (Hrsg.), Hohe Dunkelziffer und großer Informationsbedarf, 4; Gatzke, in: Kriminalistik 2/2012, 76.
[133] Vgl. IHK Nord (Hrsg.), Unternehmensbefragung zu Betroffenheit von Cybercrime, 10.

sich vor Reputationsverlust gepaart mit Umsatzeinbußen durch sich abwendende Kunden.[134] Folglich werden solche Vorfälle vorzugsweise intern behandelt. Zudem wird ein vertrauensvoller Informationsfluss zwischen Unternehmen und Polizei durch das Legalitätsprinzip (§ 163 (1) StPO) gestört, das zwar nicht allen, aber doch einigen und immer mehr Firmen bekannt sein dürfte. Durch das genannte Prinzip sind Polizeibeamte nämlich verpflichtet, im Falle des Anfangsverdachts einer Straftat (§ 152 (2) StPO) erforschend tätig zu werden.[135] Sieht ein Polizeibeamter davon ab, so kann dies eine Strafbarkeit wegen Strafvereitelung gemäß § 258a StGB begründen.
Besonders problematisch bei IuK-Straftaten, die sich gegen Wirtschaftsunternehmen wenden, ist der Umstand, dass es sich bei diesen Cybercrime-Attacken häufig um Angriffe aus dem Bereich der Organisierten Kriminalität handelt, also professionell agierende Täter mit dem Ziel maximaler Gewinnoptimierung und einer Vielzahl von Straftaten. Auf diesen Umstand haben die Sicherheitsbehörden inzwischen verschiedentlich reagiert.[136]

Ein wichtiger, allgemeiner Faktor im Hinblick auf ein ‚realistisches' Lagebild der IuK-Kriminalität in Deutschland wurde bisher vernachlässigt. Die moderne Informations- und Kommunikationskriminalität ist durch einen dynamischen Entwicklungs- und Wandlungsprozess gekennzeichnet. Das bedeutet, dass zunehmend mehr Menschen vom Computer, Internet und all seinen facettenreichen Möglichkeiten Gebrauch machen. Dass dadurch die Anzahl der Gefahren und auch Missbräuche steigt, ist unabdingbar.
Es geht also um das Verhältnis zwischen Nutzungsintensität einerseits und Anzahl der IuK-Straftaten andererseits.[137] Steigende Fallzahlen beweisen folglich (aufgrund der Verhältnismäßigkeit) nicht zwingend eine dramatische Ausbreitung der IuK-Kriminalität.
Dennoch zeigen die Zahlen eine zunehmende Relevanz des Internets bzw. der modernen IuK-Technologie für kriminelles Verhalten. Die Täter machen sich die zunehmende Verlagerung vieler gesellschaftlicher Bereiche in die

[134] Vgl. Dornseif, Phänomenologie der IT-Delinquenz, 59-62.
[135] Vgl. Weihmann/Schuch, Kriminalistik, 398-399.
[136] Vgl. BKA (Hrsg.), Handlungsempfehlung für die Wirtschaft in Fällen von Cybercrime; LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 2: Einrichtung eines Single-Point-of-Contact.
[137] Vgl. Robertz, in: DP 9/2011, 29.

Welt des Internets (Online-Shopping, Online-Banking, Online-Partnerbörsen, soziales Leben im Netz) zu nutzen. Dies begründet für die Polizei und andere Organe der Strafrechtspflege eine intensive Beobachtung dieser Entwicklung bei gleichzeitiger Anpassung kriminalitätsbekämpfender Maßnahmen.

4.3 Phänomenologische Einzelfallanalyse

Die bisherigen Ausführungen zu Kapitel 4 haben zweierlei gezeigt. Zum einen wird das Gesamtphänomen der IuK-Kriminalität seit Jahrzehnten diskutiert. Offensichtlich zeichnet sich eine quantitativ besorgniserregende Entwicklung ab. Zum anderen ist es schwierig, ein realitätsgetreues Kriminalitätslagebild zu zeichnen. Auch Aussagen, wonach die Fallzahlen im Zusammenhang mit IuK-Kriminalität bei gleichzeitig sinkender Aufklärungsquote steigen, sind wenig hilfreich.

Insgesamt handelt es sich um wenig differenzierte Darstellungen, die der Komplexität des Kriminalitätsphänomens nicht gerecht werden. Dazu *Robertz*: „Bei dieser Vielfalt an Gefahren erscheint es zur gelingenden Bekämpfung von Cybercrime durchaus relevant, zum Einen die Ebenen der privaten und industriellen, sowie der nationalen Datensicherheit analytisch zu trennen und spezialisiert dagegen vorzugehen. Zum Anderen sollten auch die Schädigungsebenen differenziert werden. Experimentelles Verhalten von Jugendlichen, gezielte Straftaten zum monetären oder Machtgewinn und terroristische Angriffe müssen auf völlig unterschiedlichen Ebenen analysiert und bekämpft werden.“[138] Es handelt sich also um eine Herausforderung, der man nicht in Form von IuK-Kriminalität im Allgemeinen begegnen kann. Vielmehr ist eine differenziertere, phänomenologische Analyse gefordert. Diese hat zu prüfen, welchen kriminellen Verhaltensweisen die Gesellschaft ausgesetzt ist, wo Gemeinsamkeiten und Unterschiede bestehen. Ansätze einer solchen Analyse folgen nun. Entscheidend ist dabei die Forschungsfrage dieser Arbeit – nämlich, ob es sich bei den einzelnen Phänomenen um neue, IuK-bedingte Kriminalitätsbereiche handelt, oder ob die moderne Technologie vornehmlich als Tatmittel genutzt wird. Die seit 1973 erfolgte

[138] Robertz, in: DP 9/2011, 32.

Einteilung in IuK-Kriminalität in eine i.e.S. und eine andere i.w.S. wird dabei kritisch hinterfragt.

4.3.1 Die IuK-Technologie als Ziel von Straftaten (IuK-Kriminalität im engeren Sinn)

Die IuK-Kriminalität i.e.S. ist dadurch definiert, dass Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind.[139] Die *Polizeiliche Kriminalstatistik* hat definiert, welche Verhaltensweisen hierunter zu subsumieren sind (vgl. Kapitel 4.1.2). Demnach müsste bei all diesen Straftaten die IuK-Technologie Ziel bzw. Objekt der Straftat sein. Das bedeutet, dass sich das tatbestandliche Verhalten eines Täters gegen Prozesse der elektronischen Datenverarbeitung richten muss. Die IuK-Technologie ist somit wesentliches Kennzeichen dieser Taten.

Dabei darf die Objekt- bzw. Zieleigenschaft der IuK-Technologie nicht falsch verstanden werden. Die Täter verfolgen in der Regel nicht das Ziel, die Technologien zu beschädigen oder zu zerstören. Es geht vielmehr darum, eine tatbestandliche Handlung gegen Elemente der elektronischen Datenverarbeitung vorzunehmen, um das eigentliche Ziel der Tat zu erreichen. Bei diesem Ziel handelt es sich fast ausschließlich, so die begründete Meinung des Verfassers, um betrügerische Handlungen mit dem Ziel der Vermögenssteigerung.

Schlussendlich werden die Technologien in der Vielzahl der Fälle genutzt, um in der virtuellen Welt eine (tatbestandliche) Handlung zu begehen, die sich in der realen Welt schließlich in einem direkten oder indirekten monetären Mehrwert äußert.

Die einzelnen Straftaten werden im Folgenden mit Blick auf die Forschungsfrage und PKS-Klassifikation analysiert.

[139] Vgl. IMK (Hrsg.), Programm Innere Sicherheit, 33.

4.3.1.1 Computerbetrug

Beim Computerbetrug handelt es sich um ein Vermögensdelikt in Anlehnung an den klassischen Betrug gemäß § 263 StGB. Der Straftatbestand des Computerbetrugs (§ 263a StGB) wurde durch das 2. WiKG vom 15. Mai 1986 eingeführt. Dabei ging es um die Schließung von Strafbarkeitslücken.

Der klassische Betrug setzt für die Erfüllung des objektiven Tatbestands einen durch Täuschung herbeigeführten Irrtum eines Menschen voraus. Diese Eigenschaft war vor dem Hintergrund der sich entwickelnden Technologien problematisch. Vor 1986 waren beispielsweise die Fälle, in denen ein Täter sich Magnetstreifendaten einer EC- bzw. Debitkarte und die dazugehörige PIN[140] verschaffte, um im Anschluss an einem Geldautomaten unberechtigterweise Bargeldabhebungen vorzunehmen, nicht gemäß § 263 StGB strafbar. Der durch die Täuschungshandlung herbeigeführte Irrtum richtete sich nämlich ausschließlich gegen ein Datenverarbeitungssystem (den Geldautomaten). Der 1986 eingeführte § 263a StGB ersetzt den menschlichen Irrtum durch die Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs und schließt damit die durch die fortschreitende Technik entstandene Strafbarkeitslücke.[141]

Die moderne Informations- und Kommunikationstechnik hat im Verlauf der Jahre zu einer erheblichen Differenzierungen der Tatmodalitäten des Computerbetrugs geführt. Die Polizeiliche Kriminalstatistik unterscheidet heute zwischen drei Kategorien, die alle eine Strafbarkeit gemäß § 263a StGB begründen:[142]

- Computerbetrug (seit 1987)
- Betrug mittels rechtswidrig erlangter Karten für Geldausgabe bzw. Kassenautomaten (von 1989-2002) – seit 2002: Betrug mittels rechtswidrig erlangter Debitkarte mit PIN
- Betrug mit Zugangsberechtigung zu Kommunikationsdiensten (seit 1998)

[140] PIN (engl.): Personal Identification Number.
[141] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 493-494.
[142] Vgl. BKA (Hrsg.), PKS 2011, 13.

Von der IuK-Kriminalität i.e.S. wird dabei die zweite Kategorie ausgeklammert. Diese unterscheidet sich von den anderen Tatausführungen wie folgt: Die Täter erlangen die Debitkarte im Original und die dazugehörige PIN durch eine Vortat. Dabei handelt es sich meist um einen Diebstahl oder ein Raubdelikt (Handtaschendiebstahl, Handtaschenraub). Die PIN findet sich entweder auf einer handschriftlichen Notiz in der Geldbörse oder der Täter hat die PIN-Eingabe während des Geldabhebevorgangs durch den Geschädigten beobachtet. Als Verwertungstat folgt nun der Betrug gegenüber dem Geldautomaten. Dieser erfolgt unter Ausnutzung der rechtswidrig erlangten Gegenstände mit den Daten. Die Tatausführung hat demnach keinen wirklichen Bezug zur modernen IuK-Technologie.
Auch im Hinblick auf die anderen Fallgestaltungen des Computerbetrugs ist die Strafbarkeit gemäß § 263a StGB meistens das Ergebnis einer Verwertungs- bzw. Anschlusstat. Dabei sind Prozesse elektronischer Datenverarbeitung aber von größerer Bedeutung, sodass diese von der IuK-Kriminalität i.e.S. umfasst werden. Im Kontext des strafrechtlich relevanten Vorverhaltens sind die Phänomene des *‚Skimmings'*[143] und *‚Phishings'*[144] von großer Bedeutung (vgl. Kapitel 4.3.2.1)

Die Tatsache, dass sich insbesondere die Geldströme und Bankgeschäfte von Unternehmen und Privatleuten über die Jahre zunehmend digitalisiert haben, hat zu einer rasanten Entwicklung der Fallzahlen des Computerbetrugs geführt. Nach 2.777 Taten im Jahr 1987 registriert die PKS seit 2009 eine konstante Fallzahl zwischen ca. 22.000 und 27.000 Taten. „Die mit Abstand größte Straftatengruppe ist der Computerbetrug mit einem Anteil von rund 39% aller Fälle."[145], so das Cybercrime Bundeslagebild 2012.

Selbst der PC-Betrug, der bereits zur IuK-Kriminalität i.e.S. zählt, verlagert sich zunehmend in die digitale Welt. Wurden 2006 ‚nur' ca. 58% der Delikte

[143] Skimming: „[…] Abschöpfen von Daten aus einer Bank- oder Kreditkarte durch Auslesen und Kopieren des Inhalts des auf der Karte enthaltenen Magnetstreifens, um die Information anschließend auf einen Kartenrohling zu übertragen und diesen in der Folge gemeinsam mit der ebenfalls ausspionierten persönlichen Identifikationsnummer (PIN) für Geldabhebungen […] zu missbrauchen.", Seidl, in: DP 7/2013, 5.

[144] Phishing: Oberbegriff für Aktivitäten, „[…] bei denen der Täter mit Hilfe gefälschter E-Mails versucht, vertrauliche Identifikationsdaten zu erschleichen. […]", Seidl, in: DP 7/2013, 6.

[145] BKA (Hrsg.), Bundeslagebild Cybercrime 2012, 4.

des Computerbetrugs unter Ausnutzung des Internets begangen, waren es im Kalenderjahr 2011 mehr als drei Viertel aller Taten.[146] Im Vordergrund stehen heute nicht mehr die Manipulation einer wiederaufladbaren Telefonkarte oder das systematische Leerspielen eines Geldspielautomaten. Die Digitalisierung der Gesellschaft schafft neue Tatumstände im Zusammenhang mit Datennetzen bei gleichzeitig höherer Beuteerwartung.

4.3.1.2 Betrug mit Zugangsberechtigung zu Kommunikationsdiensten

Das nun zu diskutierende Kriminalitätsphänomen begründet keine eigene Strafbarkeit. Wer einen Betrug mit Zugangsberechtigung zu Kommunikationssystemen begeht, macht sich in der Regel auch wegen eines Computerbetrugs gemäß § 263a StGB strafbar.

Von dieser Kategorie werden Taten erfasst, bei denen der Täter in betrügerischer Absicht in automatisierte Kommunikationsprozesse eingreift, was bei dem Geschädigten schließlich zu einem Vermögensschaden führt. Von dem Begriff der Kommunikationsprozesse sind alle Übertragungswege von Sprache/Ton, Texten und Bildern erfasst.[147] Die Art und Weise der Zugangsberechtigung ist variabel. Telefonkarten mit Vorausgebühr, Chips als Zugangsberechtigung oder Passwörter sind denkbar. Der Täter überwindet bzw. hackt[148] die jeweilige Zugangsberechtigung und verschafft sich Zugang zum Kommunikationsdienst.
Eine Abweichung von der Regelstrafbarkeit nach § 263a StGB kommt in Betracht, wenn die Anmeldung zum geforderten Kommunikationsdienst – der Zugang – nicht automatisiert und per Computer abläuft, sondern von einem Menschen überprüft wird. Dies würde Fälle umfassen, in denen ein Administrator[149] regelmäßig die vom Nutzer eingegebenen Zugangsdaten persönlich auf Übereinstimmung mit den hinterlegten Zugangsdaten überprüft. In dieser

[146] Vgl. PKS (Hrsg.), PKS 2011, 262.
[147] Vgl. BKA (Hrsg.), PKS 2011, 14.
[148] Hacken (engl.): „Unter Hacken versteht man heutzutage zumeist das unberechtigte Eindringen in ein Computer- oder Netzwerksystem.“ , Pierrot, in: Hacker, Cracker & Computerviren, Rz. 1.
[149] Administrator: Eine Person, die innerhalb eines Computersystems oder –netzwerks mit besonderen (Verwaltungs-) Rechten ausgestattet ist.

Fallgestaltung wäre aufgrund der Täuschung gegenüber eines Menschen § 263 StGB einschlägig.[150]
Aufgrund der im Zeitalter von *‚Big Data‘* zu bearbeitenden Datenmenge ist eine Überprüfungstätigkeit durch den Menschen jedoch nicht möglich. Big Data ist ein inzwischen vielfach verwendeter Begriff, um das Datenaufkommen in unserem Zeitalter zu beschreiben. *Jakobs* erklärt: „Ein sogenanntes intelligentes Telefon enthält heute mehr Rechenkapazität als alle Computer der Apollo-11-Rakete von 1969 zusammen.“[151] Es geht damit um das exponentielle Wachstum von Daten jeglicher Art und um dessen Umgang – sei es deren Verwaltung, Auswertung oder Speicherung.[152]

Nach Auskunft des LKA NRW umfasst die Deliktskategorie vielfach Fälle des missbräuchlichen Einsatzes von SIM-Karten nach betrügerischem Vertragsabschluss mit missbräuchlich genutzter Identität.[153] Eine weitere Fallkonstellation ist die Manipulation von Telekommunikationsanlagen mit dem Ziel der Anrufumleitung auf teure Auslandsvorwahlen oder kostenpflichtige 0180-Nummer zwecks Gebührensteigerung. Weiterhin handelt es sich häufig um Dialer-Fälle. Dialer sind Programme, die auf einem Rechner einen neuen Internetzugang einrichten. Dieser neue Internetzugang, von dessen Existenz der Internetnutzer meist nichts bemerkt, wählt sich über kostenpflichtige bzw. kostensteigernde Dienste in das Netz ein. Die Installation der neuen Internetzugänge erfolgt getarnt als Softwareupdate oder Plug-in-Installation.[154]

Ob die gesonderte Einführung dieser PKS-Kategorie im Jahre 1998 auch vor dem Hintergrund der Internetentwicklung erfolgte, ist fraglich. Es ist zu vermuten, dass zu Zeiten, in denen noch keine unbegrenzten Internetflatrates flächendeckend und günstig verfügbar waren, die Einwahl für Täter über eine fremde Telefonleitung zwecks Nutzung der Internetdienste sehr lukrativ gewesen ist. Allerdings begründet ein solches Verhalten nicht unbedingt die Strafbarkeit gemäß § 263a StGB. Ob diese gegeben ist, muss jeweils im

[150] Vgl. MünchKomm-StGB/Wohlers (Bearb.), Bd. 4, § 263a, Rn. 62; Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 494-495.
[151] Jakobs, in: DP 7/2013, 8.
[152] Vgl. Müller-Jung, in: FAZ, 06.03.2013, N1.
[153] Vgl. LKA NRW. (Hrsg.), Cybercrime 2012 Lagebild NRW, 5-6.
[154] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 471, 474; Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 316 ff.

Einzelfall geprüft werden. Dies ist von vielen Faktoren abhängig und wird in der Rechtsprechung und Lehre kontrovers diskutiert.[155] Fallzahlenentwicklungen können mit dieser Fallkonstellation folglich nicht erklärt werden. Vor dem Hintergrund, dass die Nutzung von Kommunikationsdiensten heute meist günstig zu finanzieren ist und Flatrate-Angebote Standard geworden sind, hat die Attraktivität eines solchen Verhaltens zudem nachgelassen.

Die PKS verzeichnet seit 2010 eine fallende Anzahl dieser Straftaten. Bis 2012 sind die Fallzahlen um ca. 63% auf 2.952 Taten gesunken. Das Bundesland Nordrhein Westfalen verzeichnete zuletzt einen jährlichen Rückgang von ca. 50% (von 2011-2012).[156]
Trotz eines auch hier vorhandenen Dunkelfeldes machen die Delikte nicht den Großteil der IuK-Taten aus. Im Ergebnis ist die IuK-Technologie dennoch in allen geschilderten Fallkonstellationen als Tatobjekt betroffen.

4.3.1.3 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung

Die nun zu analysierenden Delikte sind in § 269 StGB bzw. § 270 StGB normiert. Damit gehören die Tatbestände zu den im 23. Abschnitt des StGB niedergelegten Fälschungsdelikten im Rechtsverkehr. Ähnlich wie beim Computerbetrug wurde § 269 StGB durch das 2. WiKG eingeführt, um Strafbarkeitslücken zu schließen. Schutzgut ist die Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs.[157] Damit besteht ein Näheverhältnis zu § 267 StGB.

Eine Urkunde, als Tatbestandsmerkmal der Urkundenfälschung gemäß § 267 StGB, ist jede Verkörperung menschlicher Gedankenerklärung, die zum Beweis im Rechtsverkehr geeignet und bestimmt ist und ihren Aussteller er-

[155] Vgl. z.B. Buermeyer, in: HRRS 8/2004, 285-289; MünchKomm-StGB/Wohlers (Bearb.), Bd. 4, § 263a, Rn. 61-62; LG Wuppertal, Beschl. vom 19.10.2010, Az: 25 Qs-10 Js 1977/08-177/10, MMR 2011, 65.
[156] Vgl. BKA (Hrsg.), Bundeslagebild Cybercrime 2012, 3; LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 1, 5-6.
[157] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 613-614; Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 292.

kennen lässt. Die sogenannte Perpetuierungsfunktion[158] verlangt von der Urkunde, dass diese optisch-visuell wahrnehmbar ist.[159]
Aufgrund der zunehmenden Abwicklung rechtserheblicher Geschäfte in der digitalen Welt (elektronische Dokumente), garantierte § 267 StGB keinen hinreichenden Rechtsschutz für Fälschungsdelikte im digitalen Raum. In den Computer eingegebene Gedankenerklärungen waren nämlich nicht in der von § 267 StGB geforderten Art und Weise optisch-visuell wahrnehmbar.[160]
§ 269 StGB schloss diese Strafbarkeitslücke. Seit 1986 ist somit auch die Urkundenfälschung in Datenform strafbar. In Anlehnung an die klassische Urkundefälschung besteht die Tathandlung des § 269 StGB im Speichern, Verfälschen oder Gebrauchen der beweiserheblichen Daten.
Die seitens des subjektiven Tatbestands geforderte Täuschungsabsicht im Rechtsverkehr findet eine Alternative in § 270 StGB. Demnach steht dieser die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich. Mit dieser Vorschrift wurde die Strafbarkeitslücke geschlossen, dass Daten teilweise direkt in ein Datenverarbeitungssystem eingegeben werden ohne, dass diese zuvor durch einen Menschen verwendet wurden.[161]

Klassisches Beispiel für ein nach § 269 StGB strafbares Verhalten ist der Identitätsdiebstahl. Verwendet ein Täter personenbezogene Daten einer anderen Person, um sich beispielsweise in einem sozialen Netzwerk (*Facebook*) anzumelden, macht er sich gemäß § 269 StGB strafbar.
Ein weiteres Beispiel: Fälschen Täter die Website eines Geldinstituts mit dem Ziel, dass die Online-Banking-Nutzer ihre Zugangsdaten auf der gefälschten Internetseite eingeben, kann auch eine Fälschung beweiserheblicher Daten vorliegen. Voraussetzung dafür ist, dass die im Browser[162] angegebene Uniform Resource Locator (URL)[163] das Geldinstitut als Herausgeber dieser Seite ausgibt. Dann handelt es sich um einen Fall des *Phishings*. Das LKA NRW erklärt die steigenden Fallzahlen mit diesem verstärkten Auftreten von

[158] Perpetuierungsfunktion: Auf Dauer angelegte Verkörperung, haltbare Dokumentation.
[159] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 613-612; Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 294.
[160] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 613-612.
[161] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 640.
[162] Browser: Dabei handelt es sich um Programme, die der Darstellung von Webseiten im World Wide Web u.ä. dienen (z.B. Firefox, Google Chrome, Internet Explorer).
[163] Uniform Resource Locator (URL) (engl.): Fachterminus für die Internetadresse einer Website.

Phishing-Fällen. Auch der Volljurist *Seidl* schreibt, dass Phishing-Mails und Phishing-Websites regelmäßig die Strafbarkeit des § 269 StGB begründen.[164] Die Kategorie der IuK-gestützten Fälschungsdelikte wird demnach vielfach von diesen Datenbeschaffungsdelikten dominiert.

Noch 2004 schrieb der Medienrechtler *Ernst*, dass § 269 StGB kaum praktische Bedeutung habe. Er erklärte diesen Umstand (registriert wurden im Jahr 2004 570 Fälle) damit, dass der Anwendungsbereich der Vorschrift eher gering sei.[165] In den letzten Jahren misst die *Polizeiliche Kriminalstatistik* allerdings steigende Fallzahlen. Die Delikte der §§ 269, 270 StGB machten mit einer Anzahl von 63.959 Taten im Jahr 2012 ca. 13% der gesamten IuK-Kriminalität i.e.S. aus. Insgesamt ein Indiz dafür, dass rechtserhebliche Geschäfte tatsächlich zunehmend unter Zuhilfenahme moderner IuK-Technologie getätigt und auch angegriffen werden.

4.3.1.4 Datenveränderung, Computersabotage

Bei den Delikten der Datenveränderung und Computersabotage handelt es sich um Straftaten, bei denen die Hardware des Computers (Festplatte, Drucker, Bildschirm) oder das Computernetzwerk tatsächlich angegriffen werden.[166] Normiert ist die jeweilige Strafbarkeit des Verhaltens in den §§ 303a, 303b StGB. Eingeführt wurden die Vorschriften wiederum durch das 2. WiKG. Zudem wurden die Vorschriften im Rahmen des 41. StrÄndG vom 07.08.2007 ergänzt und modifiziert.

Zur Datenveränderung gemäß § 303a StGB:
Ähnlich wie zuvor, ist auch diese Vorschrift einer anderen Norm des StGB angegliedert. Gemeint ist hier die Sachbeschädigung gemäß § 303 StGB. Durch die Strafbarkeit der Datenveränderung, wurde jedes Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten unter Strafe gestellt. Zielrichtung war es, Daten als unkörperliche Gegenstände zu schützen. Geschützt werden alle Daten im Sinne des § 202a (2) StGB. Es sind solche

[164] Vgl. Seidl, in: DP 7/2013, 7.
[165] Vgl. Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 292-293.
[166] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 534.

Daten umfasst, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.
§ 303a stellt keine Voraussetzungen an die Qualität der Daten. Diese müssen weder besonders gegen fremden Zugriff gesichert noch von einem Geheimhaltungsinteresse geprägt sein. Zielrichtung ist lediglich der Schutz der in den Daten enthaltenen Informationen, unabhängig von deren Qualität.[167]

Wichtig in diesem Kontext sind die sogenannten Distributed-Denial-of-Service-Angriffe (DDos-Angriffe). Unter Ausnutzung von ferngesteuerten Computernetzwerken, die mit Schad-Software infiziert wurden (Botnetze) versuchen Kriminelle, einen Rechner/Server durch immer wiederkehrende, sinnlose Anfragen in sehr kurzen zeitlichen Abständen so zu überlasten, dass dieser schließlich zusammenbricht und keine Anfragen mehr bearbeiten kann.[168] Hat dies zur Folge, dass auch der Verfügungsberechtigte nicht mehr auf seine Daten (häufig die Website) zugreifen kann, haben sich die Täter gemäß § 303a StGB (in der Alternative der Datenunterdrückung) strafbar gemacht. Für die Aufhebung der Blockade fordern die Täter die Zahlung eines erheblichen Geldbetrags.

Juristisch kompliziert ist die Beurteilung/Abgrenzung von Computerviren und ‚Trojanischen Pferden'. Viren sind sich selbst verbreitende Schad-Programme, die Dateien und/oder andere Programme beschädigen. Begrifflich gehören auch Trojanische Pferde zu den Schad-Programmen. Sie gelangen unbemerkt, häufig getarnt als nützliches Programm, in das Rechnersystem und spähen auf dem jeweiligen PC befindliche Daten oder Tastatureingaben aus.[169] Die ausgespähten Daten werden mittels E-Mail an den Täter weitergeleitet. Im Unterschied zu den Viren findet aber keine unmittelbare Beschädigung statt. Während im Fall von tatsächlichen Beeinträchtigungen der Daten durch Computerviren eine Strafbarkeit nach § 303a StGB vorliegt, erfüllt die Tätigkeit von Trojanischen Pferden in einem Computersystem keine solche Handlung.[170]

[167] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 588-594.
[168] Zum Phänomen der DDos-Angriffe, vgl. Kreitlow, in: Die Polizei 10/2010, 291.
[169] Vgl. Ziercke, in: Kriminalistik 2/2008, 78.
[170] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 597.

Zur Computersabotage gemäß § 303b StGB:
Seit dem Inkrafttreten des 41. StrÄndG schützt § 303b StGB den störungsfreien Ablauf jedweder Datenverarbeitung, die für einen anderen von erheblicher Bedeutung ist. Noch 2004 fokussierte die Vorschrift überwiegend auf die Interessen der Wirtschaft und Verwaltung.[171]
Tathandlung ist das Stören der Datenverarbeitung. Diese Störung kann auf drei verschiedenen Wege erfolgen. Erstens verweist die Vorschrift auf die Tathandlungen des § 303a StGB. Wird die Datenverarbeitung durch ein Computervirus o.ä. erheblich gestört, liegt eine Tat in dieser ersten Variante vor. Zweitens kann die Beeinträchtigung durch eine Einwirkung auf die körperlichen Gegenstände der Datenverarbeitungsanlagen bzw. Datenträger erfolgen. Drittens kann die Störung auch dadurch erfolgen, dass einer Person Daten mit der Absicht übermittelt werden, dieser einen Nachteil zuzufügen. Diese letzte Alternative ist ebenso ein Ergebnis des 41. StrÄndG. Aus heutiger Sicht ist diese Tatbestandsvariante mit Blick auf Distributed-Denial-of-Service-Angriffe besonders relevant.[172]

Die PKS differenziert bei der Erfassung nicht zwischen Datenveränderung und Computersabotage. Die Fallzahlen sind von 2011 auf 2012 um 134% auf 10.857 Taten gestiegen. Das entspricht der größten Steigerungsrate im Bereich des Summenschlüssels IuK-Kriminalität i.e.S. Gleichzeitig ist die Aufklärungsquote von etwa 41% auf 17,5% gesunken. Auch vor dem Hintergrund statistischer Schwächen ist dies eine besorgniserregende Entwicklung. Das BKA führt diesen Umstand auf Angriffe mittels Schad-Software zurück. Das LKA NRW konkretisiert diese Feststellung und sieht Angriffe mit Ransomware[173] und den Einsatz kompromittierter Computer in einem Botnetz als Ursache für die Fallzahlen.[174]
Schad-Software oder Malware ist ein Oberbegriff für eine Vielzahl von Programmen, die auf einem Rechner unerwünschte Funktionen ausführen. Bei Ransomware handelt es sich um ein Schad-Programm, welches das Computersystem des betroffenen Rechners sperrt oder dessen Daten verschlüsselt.

[171] Vgl. Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 279.
[172] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 600-604, 610.
[173] Ransom (engl.): Lösegeld.
[174] Vgl. BKA (Hrsg.), Bundeslagebild Cybercrime 2012, 4; LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 4.

Der Betroffene kann seinen Computer nicht mehr oder nur noch eingeschränkt nutzen. Der Nutzer wird dann durch eine Mitteilung auf dem Bildschirm, ein sogenanntes Pop-up-Fenster, aufgefordert, einen (Löse-) Geldbetrag zu bezahlen. Nur so würde die Funktionsfähigkeit des Computers wieder hergestellt. Häufig gehen diese Taten damit einher, dass den Betroffenen als Ursache für die Systemblockade vorgeworfen wird, illegale Aktivitäten im Netz begangen zu haben (z.B. das Aufrufen von kinderpornografischen Internetseiten). Als Strafe und Voraussetzung für die Freischaltung des Systems wird die elektronische Zahlung eines Geldbetrags gefordert. Regelmäßig bedienen sich die Kriminellen bei ihrer Forderung der Logos nationaler Strafverfolgungsbehörden. Sie fälschen deren Website und verschaffen ihren Geldforderungen damit einen vermeintlich seriösen Eindruck. Medial wurden diese Fällen in den vergangenen Jahren unter dem Begriff *‚BKA-Trojaner‘* thematisiert.[175] Durch eine solche Tat erfüllen die Täter zahlreiche weitere Straftatbestände neben denen der §§ 303a, 303b StGB; wie z.B. § 269 StGB oder § 253 StGB.

Die konkreten Tatausführungen unterliegen einem dynamischen Wandel. Früher wurden die Schad-Programme über massenhaft versendete E-Mails verbreitet, heute erfolgt die Verbreitung durch Werbebanner im Internet, die mit den entsprechenden Schad-Programm versehen sind. So gelangen die Schad-Programme durch das Surfen auf eigentlich vertrauenswürdigen Websites auf den Computer. Diese Verbreitung wird als Drive-by-Download bzw. Drive-by-Infections bezeichnet.[176] Eine weitere Entwicklung steht in engem Zusammenhang mit dem Nutzerverhalten der Betroffenen. Die Kriminellen machen sich das Surfverhalten der Nutzer und die im Internet veröffentlichten Daten zunutze. Die Zahlungsaufforderungen werden inzwischen mit personalisierten Vorwürfen des illegalen Verhaltens gekoppelt.

[175] Vgl. Kirchhoff, in: Kriminalistik 7/2013 (Kriminalistik-Campus), 492; LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 17; BKA (Hrsg.), Cybercrime Bundeslagebild 2012, 7.
[176] Vgl. Seidl, in: DP 7/2013, 8-9.

4.3.1.5 Ausspähen, Abfangen von Daten

Während der Tatbestand des Ausspähens von Daten durch das 2. WiKG geschaffen wurde (§ 202a StGB), wurde das Abfangen von Daten erst durch das 41. StrÄndG im Jahr 2007 unter Strafe gestellt. Statistisch werden beide Vorschriften von der PKS zusammen erfasst.

Zunächst einige Ausführungen zu § 202a StGB:
Die Vorschrift schützt vor spionierenden Angriffen im Zusammenhang mit computergestützter Kommunikation. Genauer geht es um das Verfügungsrecht über Daten, die in Datennetzen vorgehalten werden.
Die Vorschrift ist letztlich auch das Ergebnis einer sich entwickelnden Technologie, die zweierlei möglich macht. Erstens ist das Ausspionieren von Daten mittels moderner technischer Geräte möglich geworden. Zweitens ist es inzwischen möglich, große Datenmengen auf zentralen Servern zu speichern, seien es Web-Server, E-Mail-Server oder Kundendatenserver jeglicher Art (dazu gehört auch das *Cloud Computing*). Vereinfacht dargestellt, werden dabei verschiedene Daten von dem privaten Rechner (der Festplatte) in einen Speicher des Internets ausgelagert. Die ausgelagerten Daten werden dann in räumlicher Entfernung im Rechenzentrum des jeweiligen Anbieters gespeichert.[177] Vorteilhaft ist beispielsweise, dass der Nutzer oder Verfügungsberechtigte von jedem Ort auf seine Daten zugreifen kann. Gefährlich ist jedoch, dass die ‚in der *Cloud*' abgelegten Daten leicht ausgespäht werden können.[178]

Im Hinblick auf die Datenqualität wird lediglich auf § 202a (2) StGB verwiesen. Strafbarkeitsvoraussetzung ist, dass die Daten vor einem unberechtigten Zugang gesichert sind und dadurch der Zugang erschwert oder gar verhindert wird bzw. werden soll.[179] Nach *Ernst* birgt dieses Merkmal die größten Schwierigkeiten bei der Auslegung. Seinen Ausführungen folgend genü-

[177] Vgl. Boie/Obermaier, in: SZ 3./4.08.2013, 6-7
[178] Vgl. von Leitner, in: FAZ, 26.11.2013, 25; Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 535-536.
[179] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 546.

gen Pass- oder Kennwörter auch unabhängig ihres Einfallsreichtums, um die Strafbarkeitsvoraussetzung zu erfüllen.[180]
Die Tathandlung bezieht sich auf die Kenntnisnahme der Daten durch den Täter oder die Erlangung der Verfügungsgewalt über die Daten.[181]

Durch das 41. StrÄndG ist die Strafbarkeit des § 202a StGB vorverlagert worden. Seither genügt es, sich den Zugang zu den eigentlichen Tatobjekten (Daten) zu verschaffen. Damit wurde das als ‚Hacking' bezeichnete Verhalten kriminalisiert. Während *Hacker* nach früherem Verständnis die Ambitionen hegten, Sicherheitslücken in Computersystemen aufzuzeigen, stehen sie heute eher im Zusammenhang mit systematischen Angriffen auf die Integrität von Computersystemen und deren Daten.[182]
Die Vorverlagerung der Strafbarkeit betrifft explizit den Einsatz von Trojanischen Pferden. Während deren Einsatz keine Strafbarkeit gemäß § 303a StGB begründet, erfüllt die Tätigkeit dieser Schadprogramme, nämlich die Bereitstellung des Zugriff auf sensible (Benutzer-) Daten, den Tatbestand des § 202a StGB.[183]

Ein weiteres Beispiel für eine Straftat nach § 202a StGB ist das *‚Schwarzsurfen'* in einem durch WPA2-Schlüssel[184] gesicherten kabellosen Computernetzwerk (WLAN). Mit einem Zugang zum WLAN verschafft sich der Täter nämlich Zugriff auf im Netzwerk bereitgestellte Daten.[185]

Nun zur Thematik des Abfangens von Daten:
§ 202b StGB schützt den nichtöffentlichen Kommunikationsvorgang, der mittels moderner Kommunikationstechnologie geführt wird.
Hinsichtlich der abzufangenden Daten muss es sich um solche handeln, die zum Tatzeitpunkt aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage stammen.

[180] Vgl. Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 239, 245.
[181] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 556.
[182] Vgl. Ester/Benzmüller, GData Whitepaper 2009, 19; zur früheren Rechtslage des bloßen ‚hackens' und der juristischen Argumentation der Ablehnung einer Strafbarkeit, vgl. Ernst (Hrsg.), in: Hacker, Cracker und Computerviren, Rz. 232-233.
[183] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 5560-563.
[184] WiFi-Protected-Access (WPA2) (engl.): Weiterentwickelter Sicherheitsstandard zur Zugangssicherung von Funknetzwerken, wie z.B. WLANS.
[185] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 552-553.

Das heißt, es sind ausschließlich Daten während ihrer Übertragung geschützt. Die Datenqualität ist auch hier nicht näher bestimmt.[186]
Für die Erfüllung des § 202b reicht die Zugangsverschaffung nicht aus. Es bedarf explizit der Erlangung der Verfügungsgewalt. Möglich sind hier Aufzeichnung, Kopie, Übermittlung o.ä.[187]

Wichtig ist abschließend, dass auch Vorbereitungshandlungen des Ausspähend und Abfangens von Daten unter Strafe gestellt wurden. Dieses abstrakte Gefährdungsdelikt geht auf die bereits angesprochene Cybercrime Convention zurückgeht. Die Vorschrift wurde vielfach kritisch diskutiert. Fraglich ist beispielsweise die juristische Beurteilung von Computerprogrammen, die schlicht objektiv dazu geeignet sind, eine Tat nach §§ 202a, 202b zu begehen.[188] Der Meinungsstreit, mit dem sich auch das *Bundesverfassungsgericht (BVerfG)* beschäftigt hat[189], muss hier dahinstehen und ist nicht Gegenstand weiterer Betrachtung.
Laut PKS steigen auch die Fallzahlen dieser Untergruppe der IuK-Kriminalität i.e.S. seit einigen Jahren kontinuierlich auf zuletzt 16.794 Fälle (2012). Seit 2008 haben sich die Zahlen mehr als verdoppelt.[190] Ein prozentualer Anstieg von ca. 60% in der Zeit von 2007 auf 2008[191] könnte mit der Vorverlagerung der Strafbarkeit auf die Vorbereitungshandlungen zu erklären sein. Mit 17,2% wurden die Delikte der §§ 202a, 202b StGB am seltensten in der Gruppe der Straftaten der IuK-Kriminalität i.e.S. aufgeklärt.[192]

4.3.2 Zwischenergebnis: Daten, Vermögen und Wandel als Charakteristika der IuK-Kriminalität im engeren Sinn

Die Ausführungen zu den einzelnen Phänomenen der IuK-Kriminalität i.e.S. haben die Schwierigkeit pauschaler Aussagen unterstrichen. Es handelt sich um Kriminalitätsphänomene, die sich in ihrer Zielrichtung und Motivationslage teils erheblich unterscheiden. Zudem variieren die Fallzahlen, die Entwick-

[186] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 565-567.
[187] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 571.
[188] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 572-586.
[189] Vgl. BVerfG, 2 BvR 2233/07 v. 18.05.2009.
[190] Vgl. BKA (Hrsg.), Bundeslagebild Cybercrime 2012, 4.
[191] Vgl. BKA (Hrsg.), PKS 2007, 41; BKA (Hrsg.), Bundeslagebild Cybercrime 2012, 4.
[192] Vgl. BMI (Hrsg.), IMK-Kurzbericht PKS 2012, 4.

lungen dergleichen und die Aufklärungsquote erheblich. Ein DDos-Angriff der Internetaktivistengruppierung *‚Anonymous‘* gegen die Unternehmen Mastercard und Visa, wie er sich Ende 2010 als Reaktion auf die Distanzierung der Unternehmen zu der Enthüllungsplattform *‚Wikileaks‘* ereignete,[193] kann hinsichtlich der Motivlage nicht mit einem DDos-Angriff mit dem Ziel der Vermögensmehrung durch digitale Schutzgelderpressung[194] verglichen werden. Zudem ist es durch die Datennetze in Einzelfällen möglich, mittels eines Mausklicks eine Vielzahl von Geschädigten zu produzieren[195], was sich in Form untypisch hoher Fallzahlen äußern kann.

Andererseits ist eine Differenzierung zwischen den Kategorien schwierig. Es existieren Überschneidungen in den Strafbarkeiten und juristische Feinheiten können häufig kaum überblickt werden. Die Fortentwicklung des Rechts (z.B. 41. StrÄndG) bzw. dessen Internationalisierung sind notwendig, aber gleichzeitig erschwerend mit Blick auf eine Kategorisierung mit strafrechtlichem Ansatz und Bewertung der Fallzahlenentwicklung.

Entscheidender für eine strategische Grundlage zur effektiven Kriminalitätsbekämpfung ist jedoch die Tatsache, dass die Fortentwicklung der IuK-Technologie zu einer großen Dynamik und zu stetigen Wandlungsprozessen des Kriminalitätsphänomens führt. Dieser Umstand erschwert eine Orientierung und Ausrichtung für Strategien der Strafrechtspflege erheblich.

Der Jurist *Jofer* hat sich bereits 1999 intensiv mit der Strafverfolgung im Internet beschäftigt. Bei der Analyse der kriminellen Handlungen gab er bereits damals zu bedenken, dass es „entsprechend schwer fällt […], die aufgetretenen Einzeldelikte so zu konkretisieren, dass die Einteilung nicht morgen schon wieder obsolet ist.“[196] Gleichzeitig kam er aber zu dem Ergebnis, dass das Potenzial der kriminellen Gefährdung richtig eingeschätzt werden muss, damit Prämissen bei den Strafverfolgungsbehörden effizient gesetzt werden können.[197] Der Autor hatte somit bereits damals bemerkt, was die Akteure der Sicherheitsbehörden heute in der gleichen Form diskutieren. Der Unterschied liegt lediglich darin, dass die Komplexität der IuK-Kriminalität um ein

[193] Vgl. Robertz, in: DP 9/2011, 29.
[194] Vgl. Gatzke, in: Kriminalistik 2/2012, 76.
[195] Vgl. Ziercke, in: Kriminalistik 2/2008, 77.
[196] Jofer, Strafverfolgung im Internet, 32.
[197] Vgl. Jofer, Strafverfolgung im Internet, 31.

Vielfaches gestiegen ist. 1999 war das Internet schließlich noch weit hinter den heutigen Möglichkeiten zurück.

Schließlich münden die hiesigen Aussagen erneut in einem Dilemma. Während eine differenzierte Aufstellung der Phänomene unabdingbar scheint, um der Bedrohung begegnen zu können, wird hier gleichzeitig festgestellt, dass viele Differenzierungsversuche nur die Gültigkeit einer Momentaufnahme besitzen. Dennoch ist die Feststellung charakteristischer Merkmale notwendig, um die Forschungsfrage beantworten zu können.
Bei nahezu allen Delikten der IuK-Kriminalität i.e.S. geht es um Daten, sei es im Bereich der betrügerischen Handlungen, der Fälschungsdelikte oder der spionierenden Angriffe. Zusammenfassend ist der Umgang mit Daten das Kernelement dieser Taten. Dabei sind die Daten entweder Ziel, Mittel zum Zweck oder notwendiger Bestandteil der Tat. Lediglich die §§ 303a, 303b StGB schützen als Sonderfall in erster Linie die Hardware der elektronischen Datenverarbeitung. Davon abgesehen, ist IuK-Kriminalität i.e.S. demnach fast ausschließlich Datenkriminalität.
Sieht man von gesonderten Motivationslagen ab, ist es das vorrangigste Ziel der bislang diskutierten Straftaten der IuK-Kriminalität, in letzter Konsequenz, das eigene Vermögen zu steigern. IuK-Kriminalität i.e.S. ist folglich nahezu ausschließlich Vermögenskriminalität.

Allgemeiner gilt die Feststellung, dass die Herschafft über Daten bzw. deren Gewinn gleichbedeutend ist mit Macht. Sämtliche Daten lassen sich nämlich verwerten, sei es durch eine Anschlusstat, wie es regelmäßig der Computerbetrug ist, sei es durch den Verkauf der Daten oder durch wirtschaftliche Nutzung (Wirtschaftsspionage, -sabotage).
In Deutschland und auch weltweit hat sich eine sogenannte *Underground Community* entwickelt. Dabei handelt es sich um einen freien Markt in der Parrallelwelt des Cybercrime.[198] Hier werden Daten, Waren, Geschäftsmodelle etc. gehandelt, die aus einer Straftat stammen (Hehlerware) oder die zur Begehung von Straftaten verwendet werden können.[199]

[198] Vgl. Ester/Benzmüller, GData Whitepaper 2009; Wernert, Internetkriminalität, 14.
[199] Vgl. Kreitlow, in: Die Polizei 10/2010, 291; Wernert, Internetkriminalität, 14.

Damit einher geht die Entwicklung, dass sich Täter beim Abgreifen von Daten nicht mehr auf Zugangsdaten des Online-Bankings begrenzen. Vielmehr wird alles an Datenaufkommen abgeschöpft, was sich auf dem Markt der *Underground Community* handeln lässt. Die Nachfrage bestimmt das Angebot. Es gelten betriebswirtschaftliche Grundsätze. Da zunehmend soziale Daten gehandelt werden (vergleiche die Anpassung der Ransomware auf das soziale Verhalten der Betroffenen im Netz), wird heute vermehrt vom ‚Diebstahl digitaler Identitäten' gesprochen.[200] Durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde zuletzt ein Hackingangriff in Deutschland auf 16 Millionen digitale Identitäten bekannt.[201] Da die Grenzen zwischen Online- und Offlinewelt für die moderne Gesellschaft zunehmend verschwimmen und die Preisgabe von Daten im Internet Hochkonjunktur hat, ist der Diebstahl digitaler Identitäten langfristig mit einem Persönlichkeitsdiebstahl gleichzusetzen. So sieht es auch das BSI, dass von vielen ‚offenen Türen' für Cyberkriminelle spricht.[202]

Dazu einige Anmerkungen: Angesichts der Debatte um die NSA hat der weißrussische Publizist *Morozov*, der sich in seinen Veröffentlichungen mit den politischen und sozialen Auswirkungen von Technik beschäftigt, Gedanken zur Internetfreiheit und der Verlockung des Datenkonsums verfasst und zu diesem Thema derzeit an einer amerikanischen Universität promoviert. In einem umfassenden Artikel der *Frankfurter Allgemeinen Sonntagszeitung (FASZ)* kommt *Morozov* zu dem bereits in Kapitel 2 angedeuteten Ergebnis, dass es keine neue digitale Welt bzw. Macht gibt. „Wir haben eine Welt, eine Macht, und Amerika gibt die Kommandos."[203] Der Publizist warnt vor einer wachsenden Kommerzialisierung von Daten und stellt fest, dass die Kommerzialisierung nach dem Willen der Menschen erfolgt. *Morozov* nimmt die NSA-Diskussion schließlich nur als Ausgangspunkt, um zu folgern, dass der ganze ‚digitale Kram" von entscheidender Bedeutung für die Zukunft von Pri-

[200] Vgl. Kreitlow, in: Die Polizei 10/2010, 291; BKA (Hrsg.), Bundeslagebild Cybercrime 2011, 10-11.
[201] Vgl. Bünder/Gropp, in: FAZ, 22.01.2014, 15.
[202] Vgl. Bünder/Gropp, in: FAZ, 22.01.2014, 15.
[203] Morozov, in: FASZ, 24.07.2013, 25.

vatsphäre, Freiheit und schließlich Demokratie ist.[204] Er appelliert, den Daten die Warenqualität abzusprechen und bezeichnet das Internet in einem späteren FAZ-Artikel als eine „Ideologie“[205]. Sein Beitrag in der FASZ schließt mit dem Satz: „Der Datenkonsum ist, […], eine sehr viel größere Bedrohung für die Demokratie als die NSA.“[206]

In dieser Gesellschaftskritik finden sich zwei wesentliche Aspekte, die sich auf die IuK-Kriminalität i.e.S. übertragen lassen. Erstens geht es bei der IuK-Kriminalität vornehmlich um den Umgang mit Daten und es geht um ökonomische Interessen (Vermögenssteigerung durch Straftaten der IuK-Kriminalität i.e.S. oder durch den Handel mit Daten in der *Underground Community*). Zweitens geht es um einen Aspekt, der genauer erklärt werden muss: Unser Sprachgebrauch ist geprägt von der IuK- oder Cyberkriminalität. Dahinter steht die Vorstellung eines digitalen Raumes/einer digitalen Welt, in welcher IuK-Straftaten begangen werden. Ebenso besteht in den Köpfen der Gesellschaft noch das Bild einer Online- und einer Offlinewelt. *Morozov* versucht dieses Bild durch das einer Welt ohne Grenzen zwischen Online und Offline zu ersetzen. Neue Veröffentlichungen zur IuK-Kriminalität greifen diesen Gedanken auf und üben Kritik an der bisherigen Kategorisierung der Thematik IuK-Kriminalität. Die IuK-Kriminalität als Teil der Gesamtkriminalität darzustellen halten sie inzwischen für verkürzt.[207] „Mit dem Beharren auf das Cybercrime i.e.S., […], kann der zuvor beschriebenen Verwebung digitaler Medien in den Alltag nicht hinreichend Rechnung getragen werden. Hier muss ein Umdenken stattfinden.“[208] Darin ist eine Forderung nach definitorischer oder begrifflicher Erweiterung zu sehen, um dem gesellschaftlichen Wandel im Bezug auf Kriminalität gerecht werden zu können.

Aller Gesellschaftskritik zum Trotz ist aktuell zum Beispiel die Etablierung und Begeisterung von einer rein digitalen Internetwährung wahrzunehmen. Dieses Internetgeld nennt sich *‚Bitcoins‘* und existiert seit 2009. Positive Aussagen einzelner Fachleute vor dem amerikanischen Senat haben dazu ge-

[204] Morozov, in: FASZ, 24.07.2013, 27; vgl. auch Lindner: „Daten sind die neue Leitwährung“, in: FAZ, 14.08.2013, 25.
[205] Morozov, in: FAZ, 15.01.2014, 25.
[206] Morozov, in: FASZ, 24.07.2013, 27.
[207] Vgl. Rüdiger/Denef, in: DP 11/2013, 6-7.
[208] Vgl. Rüdiger/Denef, in: DP 11/2013, 7.

führt, dass ein *Bitcoin* mit 900 US Dollar in der Spitze gehandelt wurde. Dabei existiert die Währung ausschließlich in der digitalen Welt und hat einen zweifelhaften Ursprung. Damals galten die *Bitcoins* als Leitwährung einer Internetplattform, auf der eine Vielzahl rechtswidriger Güter (kinderpornografisches Material, Waffen, Drogen) vertrieben wurden.[209] Mit Blick auf die datenbasierte Vermögenskriminalität der IuK-Kriminalität dürften die *Bitcoins* zukünftig interessant werden. Sorgen vor vereinfachten Formen der Geldwäsche dürften mit einem Verweis auf die im Mai 2013 wegen eines Geldwäsche-Ermittlungsverfahrens geschlossene Firma *‚Liberty Reserve'* aus Costa Rica begründet sein.[210] Die Firma handelte mit Online-Geld.

Der Ausblick eines Wandels der Geldwäsche und anderer Tatumstände im Zusammenhang mit Cyberkriminalität leitet zu der wichtigsten Schlussfolgerungen im Kontext der Forschungsfrage über.
Die Straftatbestände der IuK-Kriminalität i.e.S. existieren grundsätzlich seit der Einführung des 2. WiKG im Jahr 1986. Computer- und IuK-Kriminalität wurden und werden am Ausmaß dieser Taten gemessen. Allerdings hat die vorstehende Analyse gezeigt, dass sich die Tat-Modalitäten und Tat-Begehungsweisen erheblich gewandelt haben und immer noch wandeln. Dies ist zurückzuführen auf den fortschreitenden technischen Wandel. Während das 2. WiKG also die Geburtsstunde eines neuen Kriminalitätsphänomens gewesen ist, ist heute vornehmlich ein Wandel des Modus Operandi auf verschiedenen Ebenen zu beobachten. Zum einen eine Verschiebung von Kriminalität zur IuK-Kriminalität allgemein (dazu: Kapitel 4.3.3) und zum anderen ein ständiger Wandel innerhalb der IuK-Kriminalität i.e.S. Das Entstehen neuer Straftatbestände, wie z.B. durch das 41. StrÄndG, begründet nach Meinung des Autors kein neues Kriminalitätsphänomen. Vielmehr zeigt sich darin, dass neue Tat-Varianten nicht mehr unter bestehende Strafvorschriften subsumiert werden können und es der Anpassung bedarf. Phänomenologisch geht es nach wie vor um Daten, Vermögen und eine Auflösung von On- und Offline.

[209] Vgl. FAZ, 20.11.2013, 17; Nestler, in: FAZ, 20.11.2013, 16.
[210] Vgl. FAZ, 31.05.2013, 20; SZ, 31.05.2013, 18.

Da die *Polizeiliche Kriminalstatistik* ausschließlich die harten Fakten anhand der strafrechtlichen Vorschriften betrachtet, kann die Statistik den dynamischen Wandlungsprozessen der Tatbegehungsweise nicht gerecht werden. Im Rahmen der Einzelphänomendarstellung war häufig von *‚Phishing'* die Rede. Es existiert allerdings kein Straftatbestand, welcher dieses Phänomen namentlich unter Strafe stellt. Die Notwendigkeit eines solchen Tatbestands wurde zwar 2004 juristisch diskutiert, allerdings für nicht notwendig befunden.[211] Folglich gibt es keine gesonderte Erfassung durch die Statistik und das Phänomen findet lediglich über die PKS-Schlüssel des jeweils verwirklichten Tatbestands Eingang.[212] Aufgrund der Besonderheit des *Phishings* und weil dieses Phänomen geeignet ist, Wandlungsprozesse und Komplexität des Phänomens darzustellen, soll es im Rahmen der IuK-Kriminalität i.e.S. gesondert betrachtet werden.

4.3.2.1 Sonderbetrachtung Phishing

„Seit 2005 wird die ‚IuK-Kriminalität im engeren Sinne' zu mehr als 90% durch *‚Phishing'* in unterschiedlichen technischen Modi Operandi begangen."[213] Nach dieser Aussage des BKA-Beamten *Kreitlow* bedarf es keiner weiteren Rechtfertigung für eine gesonderten Analyse dieses Phänomens. Zielrichtung des *Phishing* ist immer die Erschleichung von vertraulichen Identifikationsdaten.

Ursprünglich wurden massenhaft E-Mails mit Links zu gefälschten Websites (Anmeldeseiten von *ebay* oder *PayPal*) versendet. Unter einem in der Mail geschilderten Vorwand verfolgten die Täter das Ziel, die Betroffenen zur Eingabe von Zugangsdaten (häufig ihrer Bankverbindungsdaten) zu bewegen. Die Links führten zu gefälschten Websites, die beispielsweise der Homepage der eigenen Bank so ähnlich war, dass die Aufforderung seriös wirkte. Die eingegebenen Daten wurden schließlich den Tätern zugeleitet.[214]
Bis heute hat sich diese ursprüngliche Begehungsform erheblich erweitert und gewandelt. Zwar geht es inzwischen um das Abfischen möglichst vieler

[211] Vgl. Weber, in: HRRS 12/2004, 406-410.
[212] Vgl. BKA (Hrsg.), Bundeslagebild Cybercrime 2012, 4.
[213] Kreitlow, in: Die Polizei 10/2010, 291; Wernert, Internetkriminalität, 14.
[214] Vgl. Seidl, in: DP 7/2013, 6; Kreitlow, in: Die Polizei 10/2010, 291.

und unterschiedlicher Daten, dennoch genießen Bankzugangsdaten etc. Priorität. Diese Tatsache hat zu einem Wettrüsten zwischen den Banken und Sicherheitsgesellschaften einerseits und den Tätern andererseits geführt. Erwähnenswert ist in diesem Zusammenhang die Einführung verschiedener TAN-Verfahren (*mTan*, *ChipTan*)[215], die zunächst zu einer Verschärfung der Sicherheitsvorkehrungen von Online-Transaktionen führten. Das mTan-Verfahren funktioniert in zwei Schritten: Durch die Anmeldung des Online-Banking-Nutzers beim Online-Portal seiner Bank und durch den Abgleich der sog. Transaktionsnummer (TAN) als Ersatz der Unterschrift. Dabei wird die TAN an das zuvor bei der Bank registrierte Handy des Kunden gesendet. Bestätigt der Kunde die TAN durch deren Eingabe, wird die Überweisung vorgenommen.

Die Erhöhung dieses Sicherheitsstandards funktionierte nur zeitlich begrenzt. Ein kürzlich durchgeführter Test der Zeitschrift Computerbild stellt die Sicherheit des mTan-Verfahrens erheblich in Frage. Durch den Einsatz von Trojaners und betrügerische Handlungen gegenüber dem Mobilfunkanbieter des Bankkunden, konnten sämtliche TANs abgefangen werden.[216]

Alternativ nutzen die Täter sogenannte Man-In-The-Middle[217] oder Man-In-The-Browser-Attacken[218]. Beim Kunden eingehende TANs werden durch eine Schad-Software auf das Handy des Täters weitergeleitet. Mittels dieser können Kriminelle in die Transaktionsvorgänge eingreifen, Daten abschöpfen oder Geldströme direkt auf ein anderes Konto umleiten. Im Falle neuer Sicherheitsmechanismen wird die Software schlicht neu programmiert.[219]

Je nach Ausgestaltung wird durch das *Phishing* gegen verschiedene Strafvorschriften des StGB verstoßen. Die Juristen *Seidl* und *Fuchs* haben die Strafbarkeit des *Phishings* gutachterlich untersucht und unter anderem festgestellt, dass die Datenbeschaffung den Tatbestand des § 263a StGB nicht

[215] Tan-Verfahren: Die verschiedenen TAN-Verfahren beschreiben Möglichkeiten der Generierung von Transaktionsnummer (TAN) für Bankgeschäfte.
[216] Vgl. Stern-Online, 21.11.2013, 14:40 Uhr, www.stern.de.
[217] Man-In-The-Middle: Angreifer steht zwischen zwei Kommunikationsendpunkten und kann den Datenverkehr manipulieren, vgl. LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 15.
[218] Man-In-The-Browser: Manipulationen von Darstellungen und Transaktionen direkt im vorgenommen, vgl. LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 15.
[219] Vgl. Kreitlow, in: Die Polizei 10/2010, 291.

erfüllt.[220] Daher ist zwingend zwischen der Phase der Datenbeschaffung und jener der Datenverwertung zu unterscheiden. Für die Datenbeschaffung kommt zunächst eine Strafbarkeit gemäß § 269 StGB in Betracht. Die Datenverwendung in Form von Online-Überweisung erfüllt die Tatbestände der §§ 202a, 269, 270, 263a StGB. Hat der Täter sich zusätzlich eines Finanzagenten bedient, der als Mittelsmann das rechtswidrig erworbene Geld ‚wäscht', macht sich dieser nach § 261 StGB (Geldwäsche) strafbar.[221]
Die Problematik der verschiedenen Strafbarkeiten beim *Phishing* demonstriert einmal mehr, wie schwer eine eindeutige Kategorisierung der kriminellen Erscheinungsformen ist.

Die Tatsache, dass auch im Bereich des *Phishings* zunehmend Schad-Software eingesetzt wird, unterstreicht letztlich den Trend eines gestiegenen Einsatzes von Schad-Software im gesamtphänomenologischen Bereich der IuK-Kriminalität i.e.S. Faktisch bedeutet dies, dass sich Täter durch Programmierung oder Erwerb eine Schad-Software verschaffen, die als Tatwerkzeug gegen die IuK-Technologie eingesetzt wird. Der eigentliche Täter tritt dabei in den Hintergrund. Nachdem die entsprechende Taste der Tastatur gedrückt wurde, verläuft die Tat vollautomatisch und zwar ausschließlich unter Beteiligung von Daten und Programmen. Auch dies ist als Wandel im Bereich des Modus Operandi zu werten.

4.3.3 Die IuK-Kriminalität als Tatmittel (IuK-Kriminalität im weiteren Sinn)

Straftaten der IuK-Kriminalität im weiteren Sinn sind dadurch gekennzeichnet, dass IuK-Technik zur Planung, Vorbereitung oder Ausführung der Tat eingesetzt wird. Im Unterschied zur IuK-Kriminalität i.e.S. wird die Technologie in verschiedenen Tat-Phasen also nur als Tatwerkzeug eingesetzt. BKA-Präsident *Ziercke* hat 2007 schon angemerkt, dass es kaum noch einen Kriminalitätsbereich gibt, „in dem das Internet als Tatmittel keine Rolle [mehr] spielt."[222]

[220] Vgl. Seidl/Fuchs, in: HRRS 2/2010, 85-86; a.A. Weber, in: HRRS 12/2004, 407-409.
[221] Vgl. Seidl/Fuchs, in: HRRS 2/2010, 85-92; Seidl, in: DP 7/2013, 6-7.
[222] Ziercke, in: Kriminalistik 2/2008, 77.

Im Folgenden sollen einige dieser Kriminalitätsphänomene näher betrachtet werden. Auch dabei steht die zu beantwortende Frage im Vordergrund: Inwiefern ist ein Wandel der Begehungsweise zum Tatmittel Internet festzustellen, was sind dessen Hintergründe und welche Auswirkungen ergeben sich? Oder haben sich gar neue Kriminalitätsformen gebildet?
Problematisch im Bereich dieser Teilmenge der IuK-Kriminalität ist, dass Straftaten bzw. Straftatengruppen differenziert betrachtet werden müssen. Eigentumsdelikte, Rohheitsdelikte und Delikte der Organisierten Kriminalität unterscheiden sich durch eine Vielzahl kriminalistischer und kriminologischer Faktoren voneinander. Während die IuK-Kriminalität i.e.S. bereits eine eigene Straftatengruppe bildet, können alle erdenklichen Straftaten der deutschen Gerichtsbarkeit als IuK-Kriminalität i.w.S. in Erscheinung treten. Umso mehr ist eine differenzierte Betrachtungsweise gefordert.
Da eine Analyse aller Delikte nicht Anspruch dieser Arbeit sein kann, werden nur bestimmte Phänomene analysiert. Dabei waren eine Vielzahl von Faktoren zu beachten, darunter: Die quantitative Relevanz, die Sozialschädlichkeit, das Bedrohungspotenzial der Delikte und andere Besonderheiten.

4.3.3.1 Kinderpornografie

Die Nachricht, dass Mitte November 2013 nach jahrelangen Ermittlungen der kanadischen Polizei ein internationaler Kinderpornografiering zerschlagen werden konnte, bei dem 340 Verdächtige in zahlreichen Staaten festgenommen und 386 missbrauchte Kinder gerettet wurden[223], zeugt von der Notwendigkeit einer genauen Analyse. Diesem Deliktsbereich muss aufgrund der hohen Sozialschädlichkeit eine besondere Aufmerksamkeit der Strafverfolgungsbehörden zuteilwerden. Denn gerade diese Straftaten haben durch das Internet einen rasanten und erheblichen Wandel der Tatbegehungsweise erfahren. „Während früher in Pädophilenkreisen Bücher und Hefte ‚unter dem Ladentisch' verkauft wurden, bietet das ‚World-Wide-Web' völlig neue Verbreitungswege für die Kriminellen."[224] Diese neuen Verbreitungswege zeigten sich auch in dem einleitend skizzierten Fall. Die Ermittler stellten 45 Terabyte

[223] Vgl. FAZ, 16.11.2013, 10.
[224] Kindler, in: IuK-Kriminalität, 150.

Datenmaterial sicher und erklärten, dass das pornografische Material über eine Firmenwebsite weltweit vertrieben wurde.[225]

Eine juristische Auseinandersetzung des Begriffs ‚pornografische Inhalte' ist nicht Bestandteil der hiesigen Fragestellung.[226] Grundsätzlich sollen Kinder und Jugendliche vor dem Umgang mit Pornografie und der Teilnahme an sexuellen Handlungen geschützt werden. Jugendliche sind aufgrund ihrer besonderen Schutzwürdigkeit ganz bewusst von der nachfolgenden Betrachtung mit erfasst. Wichtig ist, dass das Strafgesetzbuch zwar mit dem Begriff der ‚pornografischen Schriften' arbeitet (§ 11 (3) StGB), dieser aber auch andere Medien umfasst, sodass den modernen IuK-Medien (dem Internet) Rechnung getragen wird.[227]

Der Wandel vom Ladentisch zum Internet äußert sich in den Zahlen der *Polizeilichen Kriminalstatistik*. In der Statistik erfolgt keine gesonderte Erfassung kinderpornografischer Delikte unter Ausnutzung des Internets. Es bedarf einer genazen Aufschlüsselung.
Die PKS erfasst oberbegrifflich die Kategorie der ‚Straftaten gegen die sexuelle Selbstbestimmung'. Hinter diesem Summenschlüssel verbirgt sich eine Vielzahl von Unterkategorien und Einzeldelikten. Wichtig im Kontext des Tatmittels Internet ist die Unterkategorie *‚Verbreitung pornografischer Schriften (Erzeugnisse)'*. Die PKS und Teile der Literatur[228] sprechen im Zusammenhang mit der *Verbreitung pornografischer Schriften (Erzeugnisse)* von sogenannten Äußerungs- oder Verbreitungsdelikten. Hintergrund ist, dass allein das Einstellen der Informationen (hier: pornografische Schriften bzw. Erzeugnisse) die entsprechenden Straftatbestände erfüllt.[229] Dabei handelt es sich vornehmlich um Straftaten der §§ 184 ff StGB. Für 2012 registrierte die Kriminalstatistik insgesamt 7.709 Fälle dieser Art. Davon wurden 5.031 unter Zuhilfenahme des Internets begangen. Absolut betrachtet werden seit

[225] Vgl. FAZ, 16.11.2013, 10.
[226] Ein Überblick über die juristische Diskussion des Pornografiebegriffs bei: Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 274-275.
[227] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 165-167, 266.
[228] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, § 3, Rn. 263 ff.; Jofer, Strafverfolgung im Internet, 45 ff.; BKA (Hrsg.), PKS 2012, 288-289.
[229] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 263; BKA (Hrsg.), PKS 2012 Tabellenerläuterungen, 8.

einigen Jahren insgesamt zwar leicht sinkende Fallzahlen registriert. Jedoch steigt der Anteil derjenigen Taten, die mit dem Internet begangen werden. Waren es 2010 noch 60,1%, entsprechen die registrierten Zahlen für 2012 bereits einem Anteil von 65,3% (5.031 Fälle).[230]

Auch wenn die *Verbreitung pornografischer Schriften (Erzeugnisse)* insgesamt nur 2,2% aller Straftaten ausmacht, die mit dem Internet begangen werden, wird die besondere Betrachtung dieser Delikte mit Blick auf die kriminalpolitische Bedeutung gerechtfertigt.
Die Schwerpunktsetzung der Strafrechtspflege zeigt sich zum Beispiel darin, dass die Cybercrime-Lagebilder die Delikte der Kinderpornografie trotz verhältnismäßig geringer Fallzahlen gesondert ausweisen[231] und auf nationaler und internationaler Ebene verschiedene Rechtsakte zu verzeichnen sind, die in den vergangenen Jahren, als Folge des technischen Fortschritts, den Rechtsschutz der Kinder und Jugendlichen vor Pornografie und sexueller Ausbeutung stärken sollten.

Die von den Äußerungs- und Verbreitungsdelikten abzugrenzenden weiteren ‚Straftaten gegen die sexuelle Selbstbestimmung' machen mit Blick auf die Zahlen keinen Schwerpunkt der IuK-Kriminalität i.w.S. aus. Insbesondere bei Delikten der Kinderpornografie dürfen die verhältnismäßig geringen Fallzahlen jedoch nicht darüber hinwegtäuschen, dass viele Faktoren zu einem unbekannten Dunkelfeld beitragen. Neben der Funktion des Internets, pornografisches Material schnell und unkompliziert versenden, empfangen und anschauen zu können, führt die primäre Funktion des Internets, nämlich die moderne Kommunikation, zu problematischen Missbrauchsmöglichkeiten. Kinder und Jugendliche nutzen im Internet vielfältige Formen sogenannter Chats. Bei den Chats handelt es sich um internetbasierte Diskussionsforen. Unter der Angabe eines meist frei wählbaren Namens (Nickname) werden Textbotschaften und auch Dateien (Bilder) in Echtzeit in dem Diskussionsforum übertragen. Chaträume werden im Internet vielfach angeboten, sei es im Rahmen von Onlinespielen, auf Kontaktseiten wie z.B. *Knuddels.de* oder *Teens.de* oder für Erwachsene zwecks Partnersuche. Die Chatkommunikati-

[230] Vgl. BKA (Hrsg.), PKS 2012, 29; BKA (Hrsg.), PKS 2010, 255.
[231] Vgl. LKA NRW (Hrsg.), Cybercrime 2012 Lagebild NRW, 8.

on weist im Vergleich zu anderen Kommunikationsmitteln wie Telefon, E-Mail und persönlichen Gesprächen eine Vielzahl von Besonderheiten auf. Die Chatkommunikation ermöglicht die Kommunikation mit fremden Menschen wie kein zweites Medium. Soziale Grenzen werden verdrängt und Chatter können sich einer neuen Persönlichkeit im Chat bedienen. Zudem gilt eine eigene Sprache.[232]

Wie in allen Bereichen des Internets bieten Chaträume somit Chancen und Risiken. Ein großes Risiko besteht in der Instrumentalisierung der kinder- und jugendspezifischen Chaträume durch Pädophile[233]. Im Schutz der Anonymität können sich Pädokriminelle den Kindern nähern und sexuell auf sie einwirken. Im Vergleich zum passiven Beobachterverhalten auf Spielplätzen in den Jahren zuvor wird den Tätern der Zugang zu Kindern um ein Vielfaches erleichtert. Die Journalistin *Sonja Süss* hat sich 2012/2013 in einem Selbstversuch in zahlreichen Chats als Kind ausgegeben, um zu erfahren, wie groß die Gefahr bzw. Bedrohung durch pädophile Menschen im Internet ist. Die erschreckenden Ergebnisse hat die Journalistin in einem Artikel der FASZ veröffentlicht.[234] Den Artikel zusammenfassend geschieht in den Chats regelmäßig folgendes: Nach kürzester Zeit werden die Mädchen im Alter von zehn bis zwölf Jahren von unterschiedlichen, männlichen Chatnutzern angeschrieben. Ohne Umschweife werden die Mädchen mit sexuellen Fantasien, Aufforderungen zu sexuellen Handlungen an sich selber und Fragen auf sexueller Basis konfrontiert. Dabei schmeicheln die Täter den Mädchen mit Lob. Häufig locken die Täter die Mädchen in einen bilateralen Chat und versuchen sie zu überreden, die Webcam einzuschalten. Nicht selten schlagen die Täter auch ein reales Treffen vor (sog. *Cyber-Grooming*).

Problematisch ist die Rolle der Chatraumbetreiber. Die bislang eingerichteten Vorsichtsmaßnahmen und Tipps zum Umgang mit aufdringlichen Chatpartnern laufen meistens ins Leere. Es entspricht dem Internet und dessen Freiheitsgedanken, dass eine effektive Kontrolle der Chatraum-Kommunikation nicht funktionieren kann. *Big Data*, die Angst vor Zensur und ökonomische

[232] Zur Chat-Kommunikation, vgl. Glasenapp, in: Grundwissen Medien, 148-156.
[233] Pädophilie: Auf Dauer angelegtes, sexuelles Interesse an Kindern, vgl. Blaustein, in: der kriminalist 10/2013, 12.
[234] Vgl. Süss, in: FASZ, 24.03.2013, 2.

Interessen der Betreiber stehen einem effektiven Schutz bisweilen entgegen. Nahtlos schließen sich hier Forderungen der Sicherheitsbehörden nach weitreichenderen Ermittlungsbefugnissen an. Doch auch hier – und trotz aller vermeintlichen Offensichtlichkeit – muss zunächst die Frage gestellt werden, ob das geschilderte Verhalten überhaupt einen Straftatbestand erfüllt. Letztlich muss eine Strafbarkeit gemäß §§ 176 (4) Nr. 2-4 StGB einzelfallabhängig geprüft werden. Klar ist immerhin, dass die Vorschrift(en) die sexuelle Einwirkung auf Kinder in verschiedenen Konstellationen unter Strafe. Die Eigenschaft, dass es im Chat nicht zu physischen Kontakten zwischen Kind und Täter gekommen ist, ist unerheblich.

Die Tatsache, dass die PKS für die beschriebenen Konstellationen lediglich 649 Fälle in der Tabelle ‚Tatmittel Internet' ausweist, lässt auf ein großes Dunkelfeld schließen. Die betroffenen Kinder können mit den Erlebnissen nicht rational umgehen. Sie schämen sich, haben Angst vor Verboten der Eltern (Computerverbot) und sie lassen sich von den in der Regel erwachsenen Tätern manipulieren. Süss schreibt zutreffend, dass Kinder Aufmerksamkeit genießen und Erwachsenen und deren Urteil vertrauen.[235] In der Folge gelangen die Fälle kaum zur Anzeige.
Ziercke erklärte 2007: „Kinderpornografie ist ein wachsender Kriminalitätsbereich, dessen Ausmaß nur schwer abzuschätzen ist."[236] Er erklärte weiter, dass in einem einzigen Verfahren in Deutschland bereits über 238.000 Zugriffe auf 4.600 kinderpornografische Dateien festgestellt wurden.[237] Allein diese beiden Feststellungen lassen vermuten, wie sehr die von der PKS registrierten Fallzahlen unter der Realität bleiben.

Auf Täterseite erfüllt das Internet heute auch andere Funktionen als ein Mittel zur Tatbegehung. Über das Internet kann das Bedürfnis und der Kontakt nach Gleichgesinnten unter Wahrung von Anonymität gestillt werden.[238] Eine weitreichende nationale und internationale Verflechtung von Tätern wird ermöglicht und äußert sich beispielsweise in dem eingangs dargestellten Fall

[235] Vgl. Süss, in: FASZ, 24.03.2013, 2.
[236] Ziercke, in: Kriminalistik 2/2008, 78.
[237] Vgl. Ziercke, in: Kriminalistik 2/2008, 78.
[238] Vgl. Blaustein, in: der kriminalist 10/2013, 10-11.

des zerschlagenen Kinderpornografierings. Gefährlich ist dabei insbesondere, dass durch den Kontakt mit Gleichgesinnten moralische Zweifel abgelegt werden und die Hemmschwelle sinkt, weitere Taten zu begehen. Kriminologisch kann darin eine Neutralisierungstechnik erkannt werden. Der Täter rechtfertigt über den Austausch mit Gleichgesinnten sein meist pathologisch veranlagtes Verhalten.[239]

Darüber hinaus darf hinsichtlich des Viktimisierungsprozesses der Kinder nicht vergessen werden, dass im Internet eingestellte Bilder oder Videos kaum vollständig gelöscht werden können (vgl. Kapitel 2). Das Internet vergisst nicht. Während ausgedruckte Bilder und Videokassetten eines Pädophilen in früheren Jahren beschlagnahmt werden konnten, ist eine staatliche Inverwahrungnahme aller Ableger und Kopien des beweiserheblichen Materials in Zeiten des Internets nicht möglich. Dies führt unweigerlich zu der Gefahr von Sekundärviktimisierungen der Kinder oder Jugendlichen.[240]

Ein abschließender Aspekt in Bezug auf die hier diskutierte Thematik. Das Thema der Kinderpornografie eignet sich in der sicherheitspolitischen Diskussion, um Forderungen nach Eingriffsbefugnissen zu unterstreichen. Über alle gesellschaftlichen Schichten und Ansichten hinweg werden die Delikte der §§ 176 ff. StGB bzw. §§ 184 ff. StGB verabscheut. Das machen sich Akteure zunutze. *Kindler* beispielsweise, der als Leiter der Abteilung Öffentliche Sicherheit und Ordnung im Bayerischen Staatsministerium des Innern, im Rahmen der *BKA-Herbsttagung* 2003 für weitergehende Ermittlungsbefugnisse der Sicherheitsbehörden plädierte, kam in seinen Forderungen immer wieder auf die Delikte der Kinderpornografie mit Fallbeispielen zurück, allerdings ohne das Delikt näher zu analysieren.[241]

Nach Meinung des hiesigen Autors bedarf es der Vorsicht, das Phänomen der Kinderpornografie und der Missbrauchsmöglichkeiten durch das Internet nicht dauerhaft als undifferenziertes und unschlagbares Argument für eine Ausweitung von Ermittlungskompetenzen anzuführen. Dies würde der Komplexität der Straftaten gegen die sexuelle Selbstbestimmung und den be-

[239] Vgl. Schwind, Kriminologie, § 19 Rn. 27.
[240] Zum Viktimisierungsprozess inkl. Primär-, Sekundär- und Tertiärviktimisierung, vgl. Landwehr, in: KrimLex-Online „Viktimisierung“.
[241] Vgl. Kindler, in: IuK-Kriminalität, 147-157.

troffenen Kindern nicht gerecht. Vielmehr ist es die Aufgabe, Forschung zu betreiben und die offenkundig unzureichende Datenqualität zu verbessern.

4.3.3.2 Wirtschaftskriminalität

Die kriminologische Literatur versteht unter dem Begriff der Wirtschaftskriminalität heute die „Gesamtheit der Straftaten, die bei wirtschaftlicher Betätigung unter Mißbrauch [sic!] des im Wirtschaftsleben nötigen Vertrauens begangen werden und über eine individuelle Schädigung hinaus Belange der Allgemeinheit berühren."[242] Die Polizeiliche Kriminalstatistik erfasst die Delikte der Wirtschaftskriminalität wiederum als Summenschlüssel.[243]
Die von der PKS erfassten Zahlen sind nach einhelliger Meinung der Literatur und nach den eigenen Anmerkungen der PKS kaum aussagekräftig. Dieser Umstand wurde bereits wiederholt festgestellt und gilt für die Wirtschaftskriminalität besonders. *Schwind* fasst Aussagen zum deliktspezifischen Dunkelfeld zusammen. Danach geht der Kriminologe *Kerner* von einer Dunkelzifferrelation von eins zu zehn aus[244] und *Ziercke* beziffert das Ausmaß auf 80%.[245]

Nichtsdestotrotz wird die Wirtschaftskriminalität in der Sonderauswertung der Straftaten mit Tatmittel Internet gesondert ausgewiesen. Die PKS des Jahres 2012 hat 10.135 Fälle gezählt. Das entspricht lediglich 12,4% der Gesamtdelikte der Wirtschaftskriminalität. Inwiefern der Anstieg um 7,2 Prozentpunkte im Vergleich zum Vorjahr zu bewerten ist, ist mit Blick auf die Kritik an den PKS-Zahlen fraglich. Schlussendlich machen die 10.135 Delikte nur 4,4% der Gesamtstraftaten aller Internetdelikte aus.[246]
Unabhängig dieser Zahlen qualifiziert sich der Bereich der Wirtschaftskriminalität dennoch für eine tiefergehende Betrachtung im Rahmen der IuK-Kriminalität. Zunächst stehen die Computer- und Wirtschaftskriminalität in historischem Zusammenhang zueinander. Diesbezüglich darf auf die Einfüh-

[242] Schwind, Kriminologie, § 21 Rn. 17.
[243] Vgl. BKA (Hrsg.), PKS 2010, 17.
[244] Dunkelzifferrelation eins zu zehn: Das bedeutet, dass auf eine bekannt gewordene Tat zehn Taten kommen, von denen die Polizei keine Kenntnis erhält.
[245] Vgl. BKA (Hrsg.), PKS 2012, 262; Schwind, Kriminologie, § 21 Rn. 39-41.
[246] Vgl. BKA (Hrsg.), PKS 2012 Grundtabelle „Tatmittel Internet", 13.

rung des 2. WiKG[247] und auf die bisherigen Ausführungen des Kapitel 4.1.1 verwiesen werden. Die Verfügbarkeit von Geräten der elektronischen Datenverarbeitung in den Wirtschaftsunternehmen führte zu neuen Möglichkeiten der Wirtschaftsspionage.[248] Auch dabei haben sich die Begehungsweisen (der Modus Operandi) erheblich gewandelt. Das zeigt das jüngste Beispiel eines Angriffs auf Firmendaten eines Unternehmens während eines Geschäftsbesuchs. Mittels eines USB-Sticks, der mit Schad-Software präpariert war, gelangte das konkurrierende Unternehmen an wichtige Firmeninterna.[249] In diesem Fall begründet der Einsatz von Schad-Software sogar eine Straftat der IuK-Kriminalität i.e.S. Da dies kein Einzelfall ist, muss festgestellt werden, dass die Delikte der Wirtschaftskriminalität zunehmend als IuK-Kriminalität i.e.S. in Erscheinung treten. Eine Reduktion auf das Tatmittel Internet ist folglich unzureichend.

Gleichzeitig werden verschiedene Betrugstaten oder Spionageangriffe der Wirtschaftskriminalität auch lediglich unter Ausnutzung des Internets begangen. Beispielhaft sei hier die Problematik der Abo-Fallen im Internet genannt. Dabei werden Internetnutzer auf einer Website zur Eingabe persönlicher Daten bewegt in dem Versprechen, einen kostenlosen Dienst o.ä. in Anspruch nehmen zu können. Tatsächlich wird durch die Eingabe der Daten jedoch ein rechtsgültiger und zahlungsverpflichtender Vertrag abgeschlossen. Das Internet dient demnach lediglich als Medium. Hinter den häufig organisiert agierenden Tätern verbergen sich Briefkastenfirmen. Da die Zahlungsverpflichtung für die Internetnutzer meist in einer Randnotiz der Website vermerkt ist, war eine Strafbarkeit gemäß § 263 StGB lange Zeit fraglich. Das *Oberlandesgericht (OLG) Frankfurt a.M.* hat allerdings in einer 2010 getroffenen Entscheidung die Betrugsstrafbarkeit bestätigt.[250] Ob diese Delikte nun der Wirtschaftskriminalität zugerechnet werden können, ist diskutabel. Nach Meinung des Verfassers begründen solche Taten jedoch einen Vertrauensverlust in den Wirtschaftszweig Internet. Aufgrund der zunehmenden Digitalisierung der Märkte kann darin folglich durchaus eine Beeinträchtigung der

[247] Vgl. Schwind, Kriminologie, § 21 Rn. 30.
[248] Vgl. Schneider, Kriminologie, 48.
[249] Vgl. Brandt-Zimmermann, in: Streife Nr. 4 2011, 18.
[250] Vgl. OLG Frankfurt a.M., Beschl. vom 17.12.2010, AZ. 1 Ws 29/09, NJW 6/2011, 398-404

Belange der Allgemeinheit und damit eine Form der Wirtschaftskriminalität gesehen werden.

Ein weiteres Beispiel, dass im Zusammenhang mit dem Internet immer mehr an Bedeutung gewinnt, wird durch die Machenschaften einer als *Wettmafia* titulierten Organisation offenkundig. Sportwetten haben im Internet Einzug genommen und schweben im Grenzbereich zwischen Legalität und Illegalität. Das gilt insbesondere vor dem Hintergrund der wiederholten Meldung von manipulierten Fußballspielen. Strafrechtlich kommt § 284 (1) StGB in Betracht. Die *Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten (ARD)* sendete am 14.10.2013 eine Reportage/Dokumentation zu diesem Thema. Die Sendung lieferte Einblicke in ein Kriminalitätsphänomen, dem man zukünftig vermehrt Aufmerksamkeit schenken sollte.[251] Das Internet fungiert dabei zunehmend als weltweites Kommunikationsmittel. Zudem werden Transaktionen digital abgewickelt.

Trotz der unzureichenden Datenqualität darf die Bedeutung der Wirtschaft und der damit einhergehenden IuK-Kriminalität nicht unterschätzt werden. Die Wirtschaftskriminalität charakterisiert sich dadurch, dass gerade verhältnismäßig geringe Fallzahlen einen erheblichen wirtschaftlichen Schaden verursachen (2012: 3,75 Mrd.). So stellte auch schon der *Zweite Periodische Sicherheitsbericht (PSB)* im Jahr 2006 fest, dass die Wirtschaftskriminalität fast 50% des gesamten materiellen Schadens verursachte.[252] Hinzu kommen Dunkelfeldschätzungen, die von Schäden zwischen fünf Mrd. und 230 Mrd. ausgehen.[253] Dass die modernen IuK-Technologien auch bei den Wirtschaftsstraftaten die Transkationen und Geldströme erleichterten ist offenkundig. Was im kleinen Stil funktioniert, funktioniert auch im Großen, könnte das Motto lauten. Es darf gefolgert werden, dass die Wandlungsprozesse zukünftig zu weiteren Schwierigkeiten der Daten- und Zahlenerhebung führen werden. Ein wachsendes Dunkelfeld ist zu befürchten.

[251] Vgl. Best/Schwering/Delpierre, “Die Story im Ersten: Im Griff der Zockermafia“, 14.10.2013, www.ard.de.
[252] Vgl. BMI/BMJ (Hrsg.), 2. PSB, 149.
[253] Vgl. Schwind, Kriminologie, § 21 Rn. 7-10.

4.3.3.3 Cybermobbing

Das Cybermobbing ist ein Phänomen, bei dem die Eigenschaft des Internets als Tatmittel besonders deutlich wird. Um dem Phänomen in seinen facettenreichen Ausprägungen des Internetzeitalters gerecht zu werden, muss ein weites Begriffsverständnis gelten. Eine Reduktion auf strafrechtlich relevante Verhaltensweisen greift insgesamt zu kurz. Cybermobbing kann verschiedene strafrechtliche Ausprägungen haben. Vornehmlich sind zwei Bereiche zu nennen:

Erstens können durch das Cybermobbing bestimmte Äußerungsdelikte verwirklicht werden. Wie bereits im Zusammenhang mit den Delikten der Kinderpornografie erläutert, handelt es sich dabei um Delikte, bei denen an sich strafbare Inhalte/Äußerungen im Internet veröffentlicht werden. Für das Cybermobbing kommen in erster Linie die §§ 185, 186, 187 StGB (Beleidigung, Üble Nachrede, Verleumdung) in Betracht.

Zweitens greifen Cybermobbing-Handlungen häufig in den persönlichen Lebensbereich ein. Persönlichkeits- und Freiheitsrechte werden beeinträchtigt. Das StGB stellt solche Eingriffe nicht generell unter Strafe, sondern regelt Beeinträchtigungen im Zusammenhang mit den einzelnen Schutzgütern der Persönlichkeit und Freiheit. Dies sind im vorliegenden Zusammenhang die Vertraulichkeit des Wortes und das Recht am eigenen Bild, normiert in §§ 201, 201a StGB. Geschützt wird sowohl die Konservierung (Aufnahme, Aufzeichnung) des Wortes oder Bildes durch technische Mittel als auch deren Verbreitung. Wie die systematische Anordnung der Paragrafen schon andeutet, ist § 201a StGB eingeschoben worden. Die Vorschrift wurde am 30. Juli 2004 durch das 36. StrÄndG vor dem Hintergrund der technischen Entwicklungen in das StGB aufgenommen.[254] Die Digitalisierung von Bildern, allzeit zur Verfügung stehende Handykameras, Webcams und Minikameras im privaten Gebrauch begründeten für den Gesetzgeber die Notwendigkeit eines Schutzes gegen Eingriffe in den höchstpersönlichen Lebensbereich durch Bildaufnahmen.[255]

[254] Vgl. BGBl. I Nr. 41, 2012.
[255] Vgl. Beck, in: MMR 2/2008, 78.

Die Bestimmungen der Vorschriften des *Kunst- und Urheberrechtsgesetzes (KUG)* gehören auch zu den Schutzvorschriften, fristen in der Praxis allerdings ein eher subsidiäres Dasein.

Das Internet hat in seiner Eigenart zu erheblichen Veränderungen und neuen Dimensionen des Cybermobbings geführt. Wesentlich sind diesbezüglich die Interaktivität des *Web 2.0* und die Möglichkeit der schnellen, weltweiten und unwiderruflichen Veröffentlichung von Bild- und Videodateien durch mobile internetfähige Geräte (Smartphones, Tablets etc.). Jugendliche können ihre Handlungen im Internet hinsichtlich der Auswirkungen nicht abschätzen. Zu sehr dominiert noch das Verständnis einer Online- und einer davon unabhängigen Offlinewelt. Diese kurz skizzierten technischen Möglichkeiten und Umstände liefern im Bezug auf Mobbingtaten nicht zu überblickende Missbrauchsmöglichkeiten und machen die Handlungen gefährlich.

Da es sich insgesamt um zu viele Tatausprägungen handelt, als dass einzelne Straftatenkategorien das Ausmaß des Phänomens Cybermobbing abbilden könnten und auch antisoziales Verhaltens umfasst ist, welches keinen Eingang in die Statistik findet, müssen die Zahlen der PKS hier vernachlässigt werden.
Kranawetter, Chief Security Advisor der Microsoft Deutschland GmbH und BITKOM-Mitglied, sagt zum Ausmaß des Cybermobbing folgendes: „[…] 2012 wurde für Deutschland festgestellt, dass mittlerweile 39% der Jugendlichen zwischen 8 und 17 Jahren Opfer von Verunglimpfungen, Schikanen und Hänseleien durch Online-Aktivitäten wurden, damit ist Deutschland weltweit auf Platz 11.“[256] Gleichzeitig stellt er fest, dass Schulen die Thematik nur selten aufgreifen, Sanktionen verhängen und aufklären.
Dass *Kranawetter* den Lebensraum Schule in seine Überlegungen zum Cybermobbing einbezieht, ist nachvollziehbar. Das Zentrum des sozialen Lebens findet für Kinder und Jugendliche in der Schule statt. Hier treffen Kinder und Jugendliche in sämtlichen emotionalen Lebenslagen mit Freunden, ‚Feinden‘, Lehrern etc. zusammen. Insofern kommt der Schule als Institution eine besondere Bedeutung zu.

[256] Kranawetter, zitiert nach: LKA NRW (Hrsg.), Cybercrime NRW Lagebild 2012, 23.

Auch früher kam es zu Mobbinghandlungen in der Schule. Dabei war das Ausmaß der Viktimisierung jedoch geringer. Nach Schulschluss galt die Familie als Ruhepol und Schutz vor weiteren Attacken. Heute bietet das Internet die Möglichkeit, unabhängig von der Schule, jederzeit verunglimpfende und schikanöse Äußerungen oder Inhalte zum Nachteil einer Person zu verbreiten. Mit dem Begriff *‚Flames'* hat sich für solche ausschließlich auf Diffamierung abzielenden verbalen Beiträge inzwischen sogar ein eigenes Wort etabliert.[257] Mittels der von den Tätern genutzten Smartphones werden die Mobbingtaten häufig gefilmt und im Anschluss im Internet verbreitet. Somit beschränkt sich die Tat nicht auf ein Schulereignis mit einer überschaubaren Anzahl von Beteiligten. Die ständige Konfrontation und die potenziell mögliche Kenntnisnahme durch die gesamte Schülerschaft führen zu immer wiederkehrenden Viktimisierungen.[258] Nicht selten entgleitet den Tätern am Ende die Situation.

Es wäre allerdings stark verkürzt, dass Phänomen auf Taten unter Kindern und Jugendlichen zu beschränken. Ebenso sind Lehrer als Opfer betroffen. Auch hier ist die Grenze zwischen Schülerstreich und strafbarer Handlung zum Nachteil des Lehrers fließend.[259] Aber auch abseits der Schule kann es überall dort zu Mobbingfällen kommen, wo Menschen für eine gewisse Zeit in einem sozialen Gefügen zusammentreten, sei es in der Arbeitswelt oder in der Freizeit (z.B. Sportverein). Besonders in der Arbeitswelt dürfen Taten auf sexueller Grundlage nicht außer Acht gelassen werden. Es handelt sich folglich um ein Phänomen mit einer durchmischten Täter-, Opfer- und Motivationsstruktur, welches zu jeder Zeit in allen gesellschaftlichen Bereichen in Erscheinung treten kann.

Problematisch ist, dass die Thematik des Cybermobbings bislang wenig Aufmerksamkeit in der Gesellschaft erfährt. Anders als beim allseits geächteten Phänomen der Kinderpornografie wird das Cybermobbing in seinem Gefahrenpotenzial und der Sozialschädlichkeit unterschätzt. Mitursächlich für

[257] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 332.
[258] Vgl. Robertz, in: DP 9/2011, 31; zum Prozess der sog. 'peer-victimization', vgl. Schwind, Kriminologie, § 11 Rn. 27.
[259] Vgl. Beck, in: MMR 2/2008, 77-82.

die mangelnde Beachtung ist, dass die Intensivierung der Tat und Potenzierung der Viktimisierung durch das Tatmittel Internet bislang kaum erkannt wurde. Hoffnung machte zuletzt ein internationaler Kongress des ‚Bündnisses gegen Cybermobbing' in Berlin im September 2013. Dabei wurde festgestellt: „Cybermobbing ist ein zentrales Gesellschaftsproblem des digitalen Zeitalters."[260]
Einen Beweis für diese Feststellung liefert das Beispiel *Amanda Todd*. Die fünfzehnjährige Kanadierin nahm sich im Oktober 2012 das Leben. In einem achtminütigen *Youtube*-Video berichtet sie vor ihrem Suizid von den Demütigungen, die sie jahrelang über das Internet ertragen musste. Das Video haben sich inzwischen mehr als 17 Mio. Menschen angesehen.[261]

Auf eine andere Art und Weise beunruhigend waren die internetbasierten Aufrufe zur Lynchjustiz im Mordfall der elfjährigen Lena in Emden. Öffentliche Aufrufe im Netz, den durch die Polizei vorläufig festgenommenen Jugendlichen zu töten, mündeten in realen Belagerungsszenen des Polizeigebäudes, in dem sich der Verdächtige befand. Rechtsstaatliche Prinzipien, wie die Unschuldsvermutung gemäß § 160 (2) StPO und Art. 6 (2) *Europäische Menschenrechtskonvention (EMRK)*, wurden außer Kraft gesetzt.[262]
Diese Kommunikationstechnologien haben zu einer außergewöhnlichen Mobilisierung geführt. Ob der Jugendliche, der im Internet zu der Tat aufgerufen hatte, die Auswirkungen seines *Facebook*-Eintrags abschätzen konnte, darf bezweifelt werden. Dabei geht es wiederum um das Verständnis zwischen Online- und Offlinewelt.

Eine weitere Erscheinungsform im Kontext des weiten Begriffsverständnisses ist das Cyberstalking. Damit ist die permanente Überwachung, Belästigung oder Bedrohung eines anderen Menschen über das Internet gemeint. *Hilgendorf* und *Hong*, beides Juristen, schreiben zutreffend: „Das Phänomen des dauerhaften Verfolgens und Belästigens, das als solches schon so alt wie die Menschheit selbst sein dürfte, erreicht damit eine neue Dimensi-

[260] Wilde, in: FAZ, 13.09.2013, 39.
[261] Vgl. Wilde, in: FAZ, 13.09.2013, 39.
[262] Vgl. FAZ, 02.04.2012, 7; FAZ, 13.04.2012, 8; FAZ, 31.05.2012, 9.

on.“[263] Die Autoren sprechen von einer anderen Qualität und verweisen auf die hier bereits thematisierten Eigenarten des Internets. Sie fassen zusammen: „Die Verwendung von Datennetzen als Tatmedium führt zu einer besonderen Situation auf Täter- wie auf Opferseite, die es angeraten sein lässt, rechtzeitig Vorkehrungen zu treffen, ehe diese neue Form von Psychoterror überhand [sic!] nimmt.“[264]

Diese Schlussfolgerung der Juristen kann für das gesamte Phänomen Cybermobbing gelten. Die Ausführungen jedenfalls haben gezeigt, dass auch dieses Kriminalitätsphänomen einem dynamischen Wandel des Modus Operandi unterliegt. Ein neues Kriminalitätsphänomen ist demnach nicht zu beobachten. Allerdings hat das Internet hintergründig zu erheblichen phänomenologischen Veränderungen geführt, die über einen Wandel des Modus Operandi hinausgehen.

4.3.3.4 Cyberterrorismus und Cyberextremismus

Nachdem die Bekämpfung des internationalen Terrorismus spätestens seit den Attentaten vom 11. September 2001 den sicherheitspolitischen Diskurs weltweit dominierte, begründeten 2010 die Enthüllungen um den Virus *‚Stuxnet‘* die potenzielle Gefahr von terroristischen Angriffen unter Ausnutzung der modernen IuK-Technologie.[265] *‚Stuxnet‘* war ein äußert raffiniert programmiertes Virus, das vermutlich von einem westlichen Geheimdienst programmiert wurde und die Sabotage des iranischen Atomprogramms zum Ziel hatte.

Der Begriff Cyberwar oder Cyberterrorismus hingegen hatte seine inhaltliche Bestimmung schnell gefunden. Die Begriffe stehen heute als Oberbegriff für eine Vielzahl von kriminalistisch und sicherheitspolitisch relevanten Erscheinungsformen. Dabei muss nach Meinung des hiesigen Autors jedoch zwischen Cyberwar und Cyberterrorismus unterschieden werden. Cyberwar bzw. Cyberkrieg umschriebt sämtliche kriegerischen Handlungen unter Aus-

[263] Hilgendorf/Hong, in: K&R 4/2003, 168.
[264] Hilgendorf/Hong, in: K&R 4/2003, 172.
[265] Vgl. BMI (Hrsg.), Cyber-Sicherheitsstrategie, 3.

nutzung des Internets. In diesem Kontext müssten folglich zwischenstaatliche Auseinandersetzungen[266] und auch die NSA-Affäre untersucht werden. (Dies soll mit Verweis auf die Einleitung nicht geschehen).
Im Fokus der nachfolgenden Betrachtung stehen terroristisch motivierte Cyberangriffe (Cyberterrorismus), auch unter Einbeziehung politisch motivierter Straftaten (Cyberextremismus).

Im Bereich des Cyberterrors können verschiedene Ebenen ausgemacht werden, auf denen das Internet als Tatwerkzeug instrumentalisiert wird. Erstens wird das Internet von extremistischen Bewegungen jeglicher Richtung als Plattform, Organisations- und Kommunikationsstruktur genutzt. Neben klassischen Internetauftritten nutzen Extremisten zunehmend Kommunikationsdienste wie Twitter, um sich zu organisieren. Zweitens dient das Internet als Publikationsplattform für Äußerungsdelikte. Extremistische Gruppierungen veröffentlichen über das Internet Inhalte, die gemäß §§ 86, 86a, 130 StGB strafbar sind. Propagandainhalte (Bilder, Videos) komplettieren die extremistischen Inhalte im Netz. Diese sind mannigfaltig und reichen von politischer Meinungsäußerung über radikale Berichterstattungen bis zu Mobilisierungsvideos aus akuten Krisengebieten (z.B. Anwerbung von Kämpfern für den Bürgerkrieg in Syrien).
Die zu erstens und zweitens aufgeführten Aspekte verdeutlichen wiederum einen Wandel in der Begehungsweise. Waren es früher Flugblätter in limitierter Zahl und geheime Telefonlisten über die man Propaganda betrieb beziehungsweise Kontakt miteinader aufnahm, vereinfacht das Internet die entsprechenden Handlungen heute enorm. Gleichzeitig bleibt aber festzustellen, dass Extremisten sich der jeweils zur Verfügung stehenden IuK-Technologie schon seit jeher bedienen. Bereits vor der Jahrtausendwende wies *Janovsky* auf diesen Umstand hin.[267] *Wisotzky*, Staatsschützer beim BKA, stellte ebenfalls bereits 1998 fest, dass „eine nahezu tägliche technische ‚Auseinandersetzung' mit den modernen Kommunikationstechnologien für den polizeilichen Staatsschutz unabdingbar ist."[268] Insofern kann gefolgert werden, dass sich extremistische Gruppierungen regelmäßig der modernen Technologien

[266] Siemons, in: FAZ 26.11.2013, 27.
[267] Vgl. Janovsky, in: Kriminalistik 7/1987, 501-502.
[268] Wisotzky, in: FS Herold, 503.

bedienten und bedienen und der Wandel des Modus Operandi von dem jeweiligen Stand der technischen Fortentwicklung abhängig ist.

Kriminalstatistische Zahlen liegen nur unvollständig vor, da die Delikte der §§ 86, 86a StGB als Staatsschutzdelikte nicht von der PKS erfasst werden.[269] Seit 2011 wird jedoch jede fünfte Handlung, die nach § 130 StGB strafbar ist, mittels Internet begangen.[270]

Die Argumentation, dass die Strafverfolgungsbehörden aufgrund der Öffentlichkeit des Netzes gute Einblicke in die Szene haben müssen, gilt nur bedingt. Zunächst werden organisatorische Inhalte durch passwortgeschützte Bereiche gegen Ermittlungszugriff gesichert. Des weiteren werden sogenannte Anonymisierungsnetzwerke (auch *‚Darknet'* genannt) genutzt, wie zum Beispiel *‚The Onion Router' (TOR)*. Dabei handelt es sich um ein Datennetz im Internet, welches den Datenverkehr vielfach umleitet und damit eine Zuordnung von IP-Adressen unmöglich macht. Ähnliche Verschleierungsmechanismen sind auch für ganze Server möglich. Das *TOR-Netzwerk* hat zuletzt nach den Enthüllungen der NSA-Affäre an Prominenz gewonnen.[271] Schließlich muss bezüglich der Möglichkeiten der Ermittlungsbehörden auf die ungeheure Menge an digitalen Daten *(‚Big Data')* verwiesen werden. Der amerikanische Hard- und Softwarehersteller *EMC* sagt, dass bereits heute lediglich 0,5% aller digitalen Daten analysiert bzw. ausgewertet werden.[272] Es verwundert daher beispielsweise nicht, dass das im Internet zugängliche ‚Manifest' des norwegischen Rechtsextremisten *Behring Breivik* vor seiner Tat nicht entdeckt wurde.[273]

Nun zu einem Aspekt, der sich von den bislang erklärten Ausprägungen des Cyberterrorismus erheblich unterscheidet. Unter Cyberterrorismus im eigentlichen Sinne sind Angriffe auf Kritische Infrastrukturen zu verstehen. Energieversorgung, Verkehrslenkung und andere wesentliche Elemente des

[269] Vgl. z.B. BKA (Hrsg.), PKS 2012, 7.
[270] Vgl. BKA (Hrsg.), PKS 2011, Grundtabelle „Tatmittel Internet", 15.
[271] Wiedemann, in: FASZ, 21.07.2013, 37.
[272] Vgl. Knop/Finsterbusch, in: FAZ 29.08.2013, 15.
[273] Vgl. Becker/von Bredow/Darnstädt, in: Der Spiegel 31/2011, 74.

staatlichen Gemeinwesens basieren auf moderner Informations- und Kommunikationstechnologie und sind somit angreifbar.[274]

Der Leiter des Europäischen Cybercrime Centre schreibt: „Der Schutz unserer Kritischen Infrastrukturen ist von essenzieller Bedeutung und ein vorsichtiges Verhalten im Internet generell geboten.“[275]

Durch den technischen Fortschritt wächst die Verwundbarkeit der Gesellschaft. Gefährlich ist dabei die zunehmende Abhängigkeit von modernen Kommunikations- und Informationstechnologien, in die sich unsere Gesellschaft vielfach begibt. Dadurch werden Handlungen und Reaktionen berechenbar. Das wissen auch Menschen mit terroristischen Absichten. *Kreitlow*, der die Ergebnisse einer *Bund-Länder-Projektgruppe zur Bekämpfung der IuK-Kriminalität* erläutert, sieht die wesentliche Entwicklung darin, dass Steuerungs- und Produktionssysteme, die früher noch physikalisch vom Internet getrennt waren, heute zunehmende Schnittstellen mit dem Internet aufweisen. Da die Systeme folglich auch über das Internet angreifbar sind, potenziert das die Gefahr digitaler Angriffe.[276]

Natürlich hat auch die Wirtschaft den Markt des Schutzes von *Kritischen Infrastrukturen* erkannt. Deren Lösung lautet: Mehr vom Gleichen! Die Wirtschaft entgegnet den Bedrohungen mit Vorschlägen, die eine Absicherung gefährdeter Anlagen durch ausgefeiltere Leitstellentechnik bei gleichzeitiger Vernetzung möglichst vieler Systeme vorsehen. Daran muss kritisiert werden, dass gerade die Abhängigkeit von der modernen Technologie die Schwäche ausmacht.

Richtigerweise kommt der Siemens-Sicherheitsexperte *Voigt* zu dem Schluss, dass „eine Langzeitunterbrechung kritischer Infrastrukturen […] katastrophale Auswirkungen auf das Leben von Millionen von Menschen [hat].“[277] Beispielhaft sind die großen Stromausfälle der USA in den letzten Jahren zu nennen. Medien berichteten unter Bezugnahme auf Quellen der *Central Intelligence Agency (CIA)*, dass die Ausfälle teils auf Hackingangriffe gegen die Energieversorger zurückzuführen waren.[278]

[274] Vgl. Voit, in: S+S report Nr. 2 6/2013, 54-55; BMI (Hrsg.), Cyber-Sicherheitsstrategie, 3-4.
[275] Oerting, in: Kriminalistik 12/2012, 706.
[276] Vgl. Kreitlow, in: Die Polizei 10/2010, 291.
[277] Voigt, in: S+S+ report Nr. 2 6/2013, 59.
[278] Vgl. z.B. Heise-Online, 19.01 2008, www.heise.de.

Abschließend sei erwähnt, dass die Motivationslage terroristischer Angriffe in den letzten Jahren vielfältiger geworden ist. Neben Angriffen extremistischer Gruppierungen sind seit einigen Jahren unterschiedlichste Taten von Hackingaktivisten zu beobachten. Dabei geht es meist um die Aufdeckung von Skandalen, die Offenlegung von staatlich geschützten Geheimnissen oder um die Bekanntmachung zweifelhaften Regierungshandelns. Es ist diskutabel, ob diese Taten tatsächlich im Zusammenhang mit Cyberterrorismus besprochen werden können. Phänomenologisch existieren Parallelen. Die Aktivisten bedienen sich des Internets in der Art und Weise, wie sie von *Berners-Lee*, dem Erfinder des *World Wide Web*, ursprünglich angestrebt war – als Schlüssel zum Aufbrechen der Klassifikationssysteme, als Förderung neuen Denkens und als neue Freiheit (vgl. Kapitel 2).
Da die NSA-Affäre vermutlich zu einer weiter anwachsenden Zahl von gesellschafts- und regierungskritischen Aktivisten führen wird, sollte dieser Ausprägung zukünftig größere Aufmerksamkeit geschenkt werden. Aufgrund der differenzierten Motivationslage sollte man sich dem Phänomen dann jedoch jenseits von Kriminalität und Cyberterrorismus nähern.

Zusammenfassend muss festgestellt werden, dass die Handlungen des Cyberterrorismus teils als IuK-Kriminalität i.e.S. klassifiziert werden müssten. Im Falle des Angriffs auf kritische Infrastrukturen geht es um Handlungen, welche die IuK-Technologie wesentlicher Elemente des staatlichen Gemeinwesens als Ziel haben (Energieversorger, Verkehrsleitzentrale, Flughafen, Energiekraftwerke). Für Angriffe auf Kritische Infrastrukturen gilt somit, dass ein tendenzieller Wandel von physischen Taten wie Flugzeugentführungen oder Bombenanschlägen zu gezielten computergestützten Angriffen auf IuK-gestützte Elemente des Gemeinwesens zu beobachten ist.
Für die Instrumentalisierung des Internets als Mittel der Propaganda, Spendensammlung, Radikalisierung, Rekrutierung, Ausbildung und Tatvorbereitung[279] gilt hingegen, dass ein Wandel des Modus Operandi festzustellen ist, der von den jeweiligen technischen Möglichkeiten abhängt.

[279] Vgl. Ziercke, in: Kriminalistik 2/2008, 78.

4.3.3.5 Betrugsdelikte

Über betrügerische Handlungen wurde bereits im Kontext der IuK-Kriminalität i.e.S. gesprochen. Jedoch wird das Internet auch zunehmend für die Begehung klassischer Betrugsdelikte instrumentalisiert. Durch die Weiterentwicklung des Datennetzes zum *Web 2.0* haben sich im Internet zahlreiche Online-Shops oder Auktionsplattformen etabliert. Exemplarisch seien hier *ebay*, *Kleiderkreisel*, *amazon* genannt. Auf diesen internetbasierten Plattformen wird eine Vielfalt an Produkten auf unterschiedlichsten Wegen angeboten. Allen genannten Plattformen gemein ist die Tatsache, dass es einen Verkäufer und einen Interessenten bzw. Käufer gibt. Es handelt sich um eine rechtsgeschäftliche Beziehung. Bedingt durch die Anonymität im Internet birgt der Online-Handel eine große Gefahr an betrügerischen Handlungen. In erster Linie handelt es sich dabei um Delikte des Warenbetrugs (dabei täuscht der Verkäufer über die zu verkaufende Ware, um den Käufer zur Zahlung zu veranlassen) oder um Delikte des Warenkreditbetrugs (dabei täuscht der Verkäufer über seine Zahlungswillig- bzw. -fähigkeit, um in den Besitz der Ware zu gelangen).

Die PKS des Jahres 2012 weist aus, dass insgesamt 162.350 Betrugsstraftaten mittels Internet begangen wurden. Damit machen die Betrugsstraftaten unter Ausnutzung des Internets 70,8% aller Straftaten aus, die mit dem Internet begangen werden. Eine Aufschlüsselung der einzelnen betrügerischen Handlungen zeigt, dass 54.164 Warenbetrugsdelikte und 37.398 Warenkreditbetrugsdelikte mittels Internet begangen wurden. Die verbleibenden Taten verteilen sich auf andere Betrugsarten. Der Warenkreditbetrug wird zu inzwischen 70,4% über das Internet begangen. Beim Warenkreditbetrug ist es etwa jedes fünfte Delikt (193.511 Warenkreditbetrügereien insgesamt).[280] Während seit 2010 leicht sinkende Fallzahlen des Warenbetrugs mit Tatmittel Internet zu verzeichnen sind, steigen die Fallzahlen des Warenkreditbetrugs leicht. Ob diese Fallzahlenentwicklung auf einen gesteigerten Käuferschutz durch verschiedene Mechanismen zurückzuführen sind, kann nicht gesagt werden.

[280] Vgl. BKA (Hrsg.), PKS 2012, 262.

Interessant sind die Betrugsdelikte der Netzwelt aufgrund ihrer Quantität (70,8%). Das korrespondiert letztlich mit den Ergebnissen einer BITKOM-Studie zur Mediennutzung der deutschen Gesellschaft. Bereits 2011 wurde in einer repräsentativen Studie festgestellt, dass 85% der Internetnutzer bereits im Internet Waren- und Dienstleistungen gekauft haben.[281] Aus heutiger Sicht dürfte der prozentuale Anteil noch höher ausfallen.
Folglich ist ein Wandel des Kauf- und Konsumverhaltens zu beobachten, der auch zu einem Wandel in der Begehungsweise der dafür typischen Straftaten führt. Die quantitative Ausprägung ist auf das mannigfaltige Angebot bei gleichzeitig hoher Nachfrage von Online-Shopping durch die Internetnutzer zu erklären.

4.3.3.6 Urheberrechtsverletzungen

Ein weiteres Phänomen wird durch die Verstöße gegen das Urheberrecht geprägt. Das Urheberrecht schützt gemäß § 1 *Urheberrechtsgesetz (UrhG)* die Werke der Urheber von Literatur, Wissenschaft und Kunst. Die Sanktionstatbestände des Urheberrechtsgesetzes in den §§ 106-108b (UrhG) weisen dabei die Besonderheit aus, dass sie eher nach den Vorschriften des Zivilrechts gestaltet sind.[282]
Die PKS verfolgt auf Bundes- und Landesebene teils unterschiedliche Vorgehen bezüglich der Erfassung von Straftaten gegen Urheberrechtsbestimmungen bzw. private/gewerbliche Softwarepiraterie (vgl. Kapitel 4.1.2).
Dass die Entwicklung des Internets einen erheblichen Einfluss auf das Urheberrecht hat, zeigt sich an den politischen und gesellschaftlichen Debatten zu urheberrechtlichen Fragen seit Februar 2012. [283] Es ging um das *Anti Counterfeiting Trade Agreement (ACTA-Abkommen)*, welches die Produktpiraterie eindämmen sollte, aufgrund von Angst vor Einschränkung der Meinungsfreiheit allerdings heftig kritisiert und vom Europaparlament schließlich abgelehnt wurde. Es ging um den Streit zwischen der *Gesellschaft für musikalische Aufführungs- und Vervielfältigungsrechte (GEMA)* und *Youtube*. Zwischen beiden konnte keine Gebühr ermittelt werden, die Youtube für die Ver-

[281] Vgl. BITKOM (Hrsg.), Netzgesellschaft, 6.
[282] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 686-687.
[283] Für eine ausführliche Darstellung der chronischen Entwicklung der Diskussion um das Urheberrecht vgl. Gispert, in: FAZ-Online, www.faz.net.

öffentlichung von Musikvideos u.ä. bezahlen sollte. In der Folge wurden etliche Musikvideos auf Youtube gesperrt. Es ging außerdem um das Strafverfahren gegen die Betreiber der Website *Kino.to*. Auf dieser Seite war eine Vielzahl von aktuellen Filmen und Serien bereitgestellt, die sich Nutzer als sog. Stream ansehen konnte. Bei einem Stream wird der Inhalt nicht heruntergeladen und auf der Festplatte des jeweiligen Rechners gespeichert. Es erfolgt lediglich eine Zwischenspeicherung im Arbeitsspeicher. Dadurch ergaben sich komplexe Fragen der Strafbarkeit. Letztlich ging es auch wiederholt um verschiedene Aktionen, mit denen Urheber einerseits und Aktivisten andererseits für eine Wahrung bzw. Modifikation des Urheberrechts warben. Die Aktivistengruppierung *Anonymous* griff eine Internetkampagne der Urheberrechtsschützer durch eine DDos-Attacke an und drohte mit der Veröffentlichung von (persönlichen) Daten. Schließlich wurde eine Diskussionen der großen Online-Verlage mit *GoogleNews* geführt, ob die Suchmaschine auch künftig Meldungen der Nachrichtendienste anzeigen darf/soll.[284]
Die Diskussion veranschaulicht, wie sehr die Digitalisierung der Welt zu urheberrechtlichen Fragestellungen geführt hat. Mit Blick auf die PKS werden seit 2010 zwischen 46,7% und 49,5% aller Urheberrechtsverletzungen unter Ausnutzung des Internets begangen. Hinzu kommen die separat erfassten Delikte der Softwarepiraterie. Mit einer absoluten Zahl von gut 700 Taten im Jahr 2012 können diese aber statistisch vernachlässigt werden. Außerdem sind diese Delikte eher dem Bereich der IuK-Kriminalität i.e.S. zuzuweisen. Dies gilt, wie in Kapitel 4.1.2 erläuteret, zumindest im Hinblick auf die Erfassung des LKA NRW.

Insgesamt handelt es sich um eine sehr interessengeleitete Diskussion, deren Legitimation sich nach Meinung des hiesigen Autors großenteils entzieht. Schließlich hat das Internet zwar zu erheblichen Möglichkeiten und zu freizügigen Nutzungsmöglichkeiten von urheberrechtlich geschützten Werken geführt. Letztlich muss man jedoch erkennen, dass das Netz auch hier lediglich ein Mittel zum Zweck ist. Es geht vielmehr um den Schutz geistigen Eigentums und um eine Entlohnung und Anerkennung von Werken der Wissenschaft, Literatur und Kunst. Dass neben diesem Grundsatz Aspekte wie das

[284] Für eine ausführliche Darstellung der chronischen Entwicklung der Diskussion um das Urheberrecht vgl. Gispert, in: FAZ-Online, www.faz.net.

ACTA-Abkommen oder die Regelungen der GEMA kritisch diskutiert werden müssen, ist selbstverständlich. Letztlich macht die Diskussion jedoch deutlich, dass die schleichende Entwicklung des Internets bei vielen Nutzern zu einem anderen Denken geführt hat. Es geht um die Entkriminalisierung von strafrechtlichen Urheberrechtsverletzungen.

4.3.3.7 Facebook-Partys

Zuletzt wird ein Phänomen betrachtet, welches zunächst keine Straftat an sich begründet. Jedoch hat es insbesondere ordnungsrechtliche Relevanz und nur mittelbare Auswirkungen auf Kriminalität. Gemeint ist die Erscheinungsform sogenannter Facebook-Partys.

Im Zeitalter des *Web 2.0* kommunizieren Freunde vielfach durch soziale Netzwerke miteinander. Dass Facebook mit knapp einer Milliarde Nutzern dabei eine besondere Stellung zukommt, wurde bereits verdeutlicht. Zu der Kommunikation gehört auch, dass Einladungen zu Veranstaltungen (Geburtstage, Partys, Hochzeiten etc.) häufig über *Facebook* verschickt werden. Inzwischen gibt es bei Facebook sogar die Möglichkeit, sog. Gruppen zu erstellen, in welche man die gewünschten Personen per persönlicher Benachrichtigung einlädt. Der Veranstalter kann in dieser geschlossenen Nutzergruppe dann alle notwendigen Informationen zu der Veranstaltung verbreiten. Problematisch wird diese Form der Einladung, wenn die Gruppe versehentlich als öffentliche Gruppe angelegt wird, sodass eine unbegrenzte Vielzahl von Facebook-Mitgliedern Kenntnis von der Party nehmen kann. So geschehen im Präzedenzfall der 16-Jährigen *Thessa* aus Hamburg im Jahr 2011. Im Bereich des Elternhauses, wo die Geburtstagsfeier stattfinden sollte, kamen 1.600 Jugendliche zusammen, um zu feiern.[285] Durch solch ein Ausmaß wird dem Veranstalter jegliche Einflussnahme auf die Feier und deren Verlauf genommen.
Zu einem ähnlichen Vorfall kam es am 17. Juni 2011 in *Wuppertal*, als über Facebook anonym zur Teilnahme an einer Veranstaltung aufgerufen wurde. Es erschienen ca. 800 Menschen. 40 festgestellte Verstöße gegen die

[285] Vgl. Levin/Schwarz, in: Die Polizei 3/2012, 72.

Rechtsordnung machten schließlich die Auflösung der Veranstaltung notwendig. Das ist in erster Linie eine Aufgabe der Stadt/Kommune, die von der Polizei unterstützt werden kann.

Dass es im Rahmen großer Menschenansammlungen regelmäßig zu Straftaten kommt (vgl. Sportveranstaltungen, Volksfeste, Festivals) ist nicht neu. Die Besonderheit dieser Facebook-Partys liegt jedoch darin, dass die tatsächlich teilnehmende Anzahl an Personen kaum abgeschätzt werden kann, dass der Veranstalter (häufig eine Privatperson) weder über den notwendigen Platz sowie die erforderlichen Ver- und Entsorgungsmöglichkeiten verfügt und dass es kein behördliches Sicherheitskonzept gibt. In der Folge kann es zu jugendtypischen Straftaten und Auseinandersetzungen kommen.

Die Juristen *Levin* und *Schwarz* erörtern die rechtlichen Möglichkeiten der Behörden im Vorfeld und während solcher Veranstaltungen. Dabei geht es auch um die Frage der anfallenden Kosten und wer diese zu tragen hat. Dabei kommen sie zu dem Ergebnis, dass es grundrechtsdogmatische Schwierigkeiten beim frühzeitigen Vorgehen gegen Facebook-Partys gibt. Es besteht die Notwendigkeit einer rechtspolitischen Diskussion. Allerdings weisen die Juristen richtigerweise daraufhin, dass es zunächst abzuwarten gilt, ob es sich bei dem Phänomen der Facebook-Partys nicht um eine Modeerscheinung handelt, die schon bald wieder vorüber ist.[286] Der Artikel von *Levin* und *Schwarz* stammt aus März 2012. Mit Blick auf das heutige Datum (Dezember 2013) kann bestätigt werden, dass die Beliebtheit von Facebook-Partys offenkundig stark nachgelassen hat. Zumindest im Ausmaß der oben genannten Partys hat es später keine mehr gegeben.

4.3.4 Zwischenergebnis: Instrumentalisierung des Internets zur Begehung klassischer Straftaten

Die bisherige Einzelphänomenanalyse hat dem Umstand Rechnung getragen, dass einzelne Straftaten und Straftatenkategorien aufgrund ihrer kriminalistischen und kriminologischen Besonderheiten nicht miteinander zu ver-

[286] Vgl. Levin/Schwarz, in: Die Polizei 3/2012, 79.

gleichen sind. Aus den Einzelanalysen können jedoch einzelne Aspekte gefolgert werden, die zumindest für einen Großteil der IuK-Kriminalität i.w.S. Gültigkeit besitzen.
Die Analyse hat für alle phänomenologischen Erscheinungsformen gezeigt, dass das Internet bei der Begehung von Straftaten inzwischen eine erhebliche Bedeutung hat. Ganz entscheidend ist die Feststellung, dass nahezu alle untersuchten Kriminalitätsbereiche auch ohne das Internet begangen werden können. Klassische Straftaten, die früher ausschließlich durch Handlungen in der physischen Welt begangen wurden, haben sich zunehmend in die virtuelle Welt verlagert. Dies belegen auch die vielfach kritisierten Daten der PKS.

Es konnte festgestellt werden, dass das Internet seitens der Täter auf zwei Ebenen eingesetzt wird – als Kommunikationsmittel und zur Organisation einerseits und als eigentliches Tatwerkzeug andererseits.
Der Einsatz des Internets als Kommunikationsmedium gilt für alle der hier untersuchten Straftaten mehr oder weniger. Nahezu jede erdenkliche Straftat kann durch den planerischen, vorbereitenden oder ausführenden Einsatz des Internets zumindest effizienter gestaltet werden. Vielfach begründet die Kommunikation über das Internet bereits die Strafbarkeit. IuK-Kriminalität i.w.S. ist daher häufig Kommunikationskriminalität.
Für das Internet als Tatwerkzeug im eigentlichen Sinn wurde folgendes gezeigt: Die Möglichkeiten der Instrumentalisierung des Internets zur Begehung von Straftaten werden komplexer. Einerseits findet ein Wandel des Modus Operandi zum Tatmittel Internet statt. Andererseits ist die Gesellschaft einem einem dauerhaften Wandel der Begehungsweise innerhalb der IuK-Kriminalität i.w.S. ausgesetzt, der jeweils auf den technischen Fortschritt zurückzuführen ist.
Für die Wirtschaftskriminalität und den Cyberterrorismus wurde festgestellt, dass einige Taten dieser Kategorien per Definition der IuK-Kriminalität i.e.S. zugerechnet werden müssten. Diese Vermischung deutet wiederum die Schwierigkeiten der Differenzierung und Kategorisierung an.

Festzustellen bleibt, dass auch die IuK-Kriminalität i.w.S. kein neues Kriminalitätsphänomen begründet. Nichtsdestotrotz hat die moderne IuK-

Technologie zu deliktspezifischen Veränderungen geführt, die sowohl kriminalistisch, kriminologisch als auch juristisch von großer Bedeutung sind. Die Taten unterscheiden sich teils erheblich von den gleichen, jedoch ohne Internet begangnen Delikten.

5 Aspekte wirksamer Kriminalitätsbekämpfung

Das Lagebild und die Zwischenergebnisse aus Kapitel 4 leiten zwangsläufig zu der Frage über, wie die Organe der Strafrechtspflege dem Phänomen der IuK-Kriminalität begegnen müssen, um diese Kriminalitätsform effektiv bekämpfen zu können. Schließlich handelt es sich sowohl bei der Strafverfolgung um eine Staatsaufgabe mit Verfassungsrang. Das *Bundesverfassungsgericht* hat in einer Entscheidung vom 02. März 2010 festgestellt: „In einem Rechtsstaat darf auch das Internet keinen rechtsfreien Raum bilden.“[287] Gleichwohl muss zur Kenntnis genommen werden, dass es eine Straftaten freie Gesellschaft nicht gibt[288], sodass hier die Balance zwischen Freiheit und Rechtsstaatlichkeit angestrebt werden muss.

Die Eigenschaften der modernen Informations- und Kommunikationskriminalität erfordern eine Anpassung von Strategien und Maßnahmen der Kriminalitätsbekämpfung. *Oerting* stellt fest, dass wir uns nicht technisch vor der Bedrohung durch die IuK-Kriminalität schützen können.[289] Das Internet unterliegt schließlich weder einer zentralen technischen noch einer einheitlich staatlichen Kontrolle. Der Leiter des *Europäischen Cybercrime Centre (EC3)* fordert deshalb: „Wir müssen Täter festnehmen, sie strafrechtlich verfolgen und es unattraktiv werden lassen, Cyberkrimineller zu sein.“[290] Diese Zielsetzung erfordert große Anstrengungen in verschiedenen Bereichen.

[287] BVerfG, 1 BvR 256/08 v. 02.03.2010, Rn. 260.
[288] Vgl. Haferkamp, Kriminalität ist normal; Bott, in: KrimLex-Online „Normalität des Verbrechens“; Schwind, Kriminologie, § 3, Rn. 14, 28.
[289] Vgl. Oerting, in: Kriminalistik 12/2012, 706.
[290] Oerting, in: Kriminalistik 12/2012, 706.

5.1 Kriminalstrategische Herausforderungen

Unter Kriminalstrategie versteht man das Gesamtkonzept kriminalpolizeilicher Verbrechensbekämpfung. Gemeint ist eine grundsätzliche Ausrichtung, die sich an den gesellschaftlichen Gegebenheiten orientiert und der Verwirklichung Innerer Sicherheit dient.[291] Die Notwendigkeit, kriminalstrategische Ansätze zu diskutieren, wird mit Blick auf die Erkenntnisse zum Lagebild und der Einzelfallanalyse deutlich. Die Fallzahlen, das Dunkelfeld, die Aufklärungsquote und die phänomenologischen Eigenschaften der IuK-Kriminalität zeugen von Handlungsbedarf.
Über diese Erkenntnis hinaus sind die Daten der *Polizeilichen Kriminalstatistik* jedoch unzureichend, um eine kriminalstrategische Ausrichtung zu planen. Das hat Kapitel 4 gezeigt. Diesen Umstand haben auch die beteiligten Sicherheitsakteure erkannt. Die frühzeitige Einrichtung einer *Zentralstelle für anlassunabhängige Recherche in Datennetzen (ZaRD)* beim BKA (1998/1999)[292] und des *Sondermeldedienstes ‚IuK-Kriminalität'* (1985), die Erstellung separater Cybercrime-Lagebilder und die Partnerschaft zwischen dem LKA NRW und dem BITKOM[293] (als Beispiel) haben zumindest zu einer Verbesserung der Datenqualität geführt. Dennoch müssen weiterhin statistische Erfassungsfehler beseitigt und differenziertere Erhebungen insbesondere für die IuK-Kriminalität i.w.S. forciert werden. Eine zentrale Herausforderung im Kontext eines realistischen Kriminalitätslagebildes als Ausrichtungsgrundlage bleibt zudem das große Dunkelfeld – vielfach bedingt durch eine mangelnde Anzeigebereitschaft von Wirtschaftsunternehmen. Für die Polizei gilt es zukünftig, Vertrauen zu schaffen und sich als professioneller Partner in Sicherheitsfragen zu präsentieren.

Dieser Aspekt leitet dazu über, dass die Bekämpfung der IuK-Kriminalität nur durch eine intensive Zusammenarbeit zwischen Behörden, Unternehmen und der Gesellschaft möglich ist. „Sichere Netzwelten sind Gemeinschaftsaufgabe"[294], so *Gatzke,* als Leiter des LKA in Nordrhein-Westfalen. Auch die vom

[291] Weihmann/Schuch, Kriminalistik, 77
[292] Vgl. Wiedemann, in: Kriminalistik 4/2000, 236; BKA (Hrsg.), (ZaRD), www.bka.de; rechtlichen Bedenken gegenüber der Internet-Streife, vgl. Rüdiger/Denef, in: DP 11/2013, 9 ff.
[293] Vgl. LKA NRW (Hrsg.), Cybercrime in NRW Lagebild 2012, 25.
[294] Gatzke, in: Kriminalistik 2/2012, 75.

Bundesministerium des Innern herausgegebene Cyber-Sicherheitsstrategie setzt auf ein solches Verständnis.[295] Dazu zählt auch ein intensiver und regelmäßiger Informationsaustausch zwischen den Sicherheitsbehörden (*Bundesnachrichtendienst, Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst, Bundesamt für Sicherheit in der Informationstechnik* etc.).[296] Die Bedeutung eines solchen Informationsaustauschs bei gleichzeitiger Berücksichtigung der Rechtmäßigkeit der Datenweitergabe und -nutzung wird mit Blick auf die Ermittlungsfehler im Verfahren gegen den *Nationalsozialischen Untergrund (NSU)* deutlich.
Kreitlow fordert eine institutionalisierte Zusammenarbeit zwischen Sicherheits- und Strafverfolgungsbehörden und Vertretern der Privatwirtschaft im Rahmen einer sogenannten *Public Private Partnership (iPPP)*.[297] Nach langwierigen Verhandlungen wurde am 07. November 2013 schließlich eine solche Gründungsvereinbarung unterzeichnet, die eine Kooperation zwischen dem BKA und der Geldwirtschaft in Form eines Vereins beschloss.[298] Die Zukunft wird zeigen, ob sich solche Modelle etablieren werden.

Zusammenarbeit ist auch auf anderer Ebene eine zentrale Herausforderung für die Bekämpfung der IuK-Kriminalität. Die Eigenschaften der IuK-Kriminalität erfordern eine internationale Zusammenarbeit der Strafverfolgungsbehörden. Das wird bereits an der Einführung des international gebräuchlichen Begriffs ‚Cybercrime' deutlich. Ein weiterer Beleg für die internationale Relevanz ist, dass der *Meldedienst ‚IuK-Kriminalität'* im Jahr 2013 in einen *Meldedienst ‚Cybercrime'* umbenannt wurde. Neben einer internationalen Ausrichtung sollte die Umbenennung dazu beitragen, weitergehende Tatbestände darunter zu subsumieren bzw. abbilden zu können.[299] Damit wird dem Ergebnis Rechnung getragen, dass das Kriminalitätsphänomen einem ständigen, vielschichtigen Wandel unterliegt. Darüber hinaus wurden insbesondere im europäischen Raum seit der Jahrtausendwende unterschiedliche Anstrengungen unternommen, Handlungsschwerpunkte zu be-

[295] Vgl. BMI (Hrsg.), Cyber-Sicherheitsstrategie.
[296] Vgl. Kreitlow, in: Die Polizei 10/2010, 293; Burandt/Tölle, in: Kriminalistik 8-9/2013, 525; Oerting, in: Kriminalistik 12/2012, 706.
[297] Vgl. Kreitlow, in: Die Polizei 10/2010, 293.
[298] Schriftliche Expertenauskunft eines KD a.D. des BKA.
[299] Schriftliche Expertenauskunft eines KD a.D. des BKA.

stimmen und die Zusammenarbeit zu intensivieren. Dies wird durch verschiedene nationale Rechtssysteme und die Erfordernis des Verzichts auf Souveränitätsrechte erschwert (vgl. Kapitel 5.2).[300] Ein wesentlicher Erfolg in diesem Kontext kann in der Etablierung eines *Europäischen Cybercrime Centres (EC3)* im Jahr 2013 gesehen werden.[301]

Wesentlich im Zusammenhang mit internationaler Ermittlungsarbeit ist das Instrument der justiziellen Rechtshilfe. Aufgrund der Internationalität der IuK-Kriminalität sind Ermittlungspersonen häufig davon abhängig, dass ausländische Behörden Rechtshilfe gewähren und damit die örtlichen Ermittlungen unterstützen.[302] Die Erfahrungen zeigen, dass solche Rechtshilfeverfahren äußerst langwierig sind und effektive Ermittlungen erschweren oder gar verhindern.[303] Mit Blick auf die Tatsache, dass sich die Begehung von (herkömmlichen) Straftaten zunehmend in das Internet verlagert, handelt es sich um ein wichtiges Instrument der zukünftigen Kriminalitätsbekämpfung. Da es folglich nicht um Einzelfälle geht, ist es eine kriminalstrategische und kriminalpolitische Herausforderung, für die Zukunft ein rechtsstaatliches Instrument zu gestalten, das internationale Ermittlungen erleichtert.

Nach diesem Ausblick auf internationale Problemfelder soll der Fokus erneut auf die nationalen Strukturen gelenkt werden: Weil Kapitel 4 gezeigt hat, dass die IuK-Kriminalität auf allen Ebenen dynamischen Wandlungsprozessen unterliegt und Kategorisierungsversuche zwangsläufig in ein Dilemma führen, ergeben sich organisatorische und personelle Herausforderungen für die Organe der Strafrechtspflege.

Organisatorisch haben die polizeilichen Einrichtungen in den letzten Jahren begonnen, Cybercrime-Dienststellen einzurichten und Kompetenzen zu bündeln. Dies gilt für die Landeskriminalämter und das Bundeskriminalamt grundsätzlich, für die örtlichen Kreispolizeibehörden bedingt. Die Erfahrungen der Kriminalbeamten *Burandt* und *Tölle* aus einem Umfangverfahren mit

[300] Für eine ausführliche Abhandlung, vgl. Gleß, Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung.

[301] Vgl. Oerting, in: Kriminalistik 12/2012, 705-706.

[302] Die ‚Polizeiliche Zusammenarbeit' und die ‚Justizielle Zusammenarbeit in Strafsachen' ist auf gemeinsame Ermittlungstechniken zur Aufklärung schwerer Kriminalität begrenzt. Gemeinsame Strafverfolgungsmaßnamen bzw. die Wahrnehmung von Hoheitsrechten im jeweiligen Ausland ist (noch) nicht möglich, vgl. Vertrag über eine Verfassung für Europa v. 29.10.2004, Teil 3, Abschnitt 4, Art. 270-277.

[303] Vgl. Wiedemann, in: Kriminalistik 4/2000, 236; Kreitlow, in: Die Polizei 10/2010, 294-295.

Bezug zur IuK-Kriminalität sollen als Ansatz für die Erläuterung weiterer kriminalistischer Herausforderungen dienen.[304] Die Beamten fordern den flächendeckenden Aufbau eigener Cybercrime-Dienststellen bzw. von IuK-Fachdienststellen auf der Ebene kriminalpolizeilicher Sachbearbeitung.[305] Für *Nordrhein-Westfalen* ist dies bereits per Erlass vorgeschrieben.[306] Nach der Ergebnissen der Analyse aus Kapitel 4 weist der Autor dieser Arbeit diesbezüglich auf folgendes hin: Die Einzelphänomene haben gezeigt, dass die kriminalistische Bearbeitung von Delikten der gesamten IuK-Kriminalität ein sehr unterschiedliches Ausmaß an informationstechnischem Know-How von den Ermittlern verlangt. Tat- und Tätertypologien haben sich geändert. Es reicht folglich nicht aus, nur Taten der IuK-Kriminalität i.e.S. von IuK-Fachdienststellen bearbeiten zu lassen und die Delikte der IuK-Kriminalität i.w.S. den herkömmlichen Fachdienststellen oder Regionalkommissariaten (je nach zugrunde liegender Straftat) zu überlassen. IuK-Kriminalität kann vor dem Hintergrund einer Auflösung von Online- und Offlinewelt langfristig nicht mehr isoliert betrachtet werden. Es werden nahezu alle Bereiche des Lebens und damit auch alle Bereiche kriminalistischer Arbeit tangiert. Es geht um Strukturen Organisierter Kriminalität *(Underground Community)*, Wirtschaftskriminalität, Vermögenskriminalität, terroristische Bedrohungen und Erscheinungen der Jugendkriminalität (Cybermobbing). Flexible Lösungen und Arbeitsweisen sind gefordert.

Zurück zu den Erfahrungen von *Burandt* und *Tölle*. Die Ermittler weisen auf die große Bedeutung einer intensiven Spurensuche und -auswertung digitaler Medien hin.[307] Der Umgang mit ‚digitalen' Beweismitteln bringt erhebliche Herausforderungen mit sich. Einerseits geht es dabei um die Masse der anfallenden Daten *(Big Data)*[308] und andererseits um das Suchen, Sichern und Auswerten rechtlich zulässiger Beweismittel. Wie gezeigt, ist IuK-Kriminalität zumeist Daten-, Vermögens- oder Kommunikationskriminalität. Es fallen also zunehmend Beweismittel an, die nicht gegenständlicher, sondern digitaler Natur sind. Das Verschlüsselungs- und Anonymisierungspotenzial des Internets kennt (insbesondere nach der NSA-Affäre) keine Grenzen. IuK-

[304] Vgl. Burandt/Tölle, in: Kriminalistik 8-9/2013, 523-525.
[305] Vgl. Burandt/Tölle, in: Kriminalistik 8-9/2013, 525.
[306] Vgl. RdErl. MIK NRW v. 29.02.2013 - 423-62.18.09
[307] Burandt/Tölle, in: Kriminalistik 8-9/2013, 525.
[308] Zum Thema Massendaten als Herausforderung, vgl. Ziercke, in: Kriminalistik 2/2008, 81.

Kriminalität zeichnet sich dadurch aus, dass es zumeist zu keinem physischen Kontakt zwischen Täter und Opfer kommt. Dies führt dazu, dass dem Sachbeweis eine erhebliche Bedeutung zu Teil wird. Die zunehmende Bedeutung dieser IT-Forensik zeigt sich darin, dass Ermittler inzwischen häufig als Sachverständige im Strafverfahren auftreten müssen. Sachverständige verfügen über eine dem Gericht fehlende Sachkunde. Der Sachverständige tritt somit als Gehilfe des Richters auf und macht objektive Angaben zu einem bestimmten Beweisthema.[309] Neben dieser personellen Qualifikation erfordert ein beweissicheres Strafverfahren zertifizierte Labore für die IT-Forensik, wie dies auch für Untersuchungen von Fingerabdrücken und DNS der Fall ist.[310] Nach Auskunft des BKA existieren in Deutschland seit 2008 zertifizierte und akkreditierte IT-Forensik-Labore.[311] Neben dem BKA gilt dies inzwischen auch für einige Bundesländer. Ein flächendeckender Ausbau ist mit Blick auf eine möglichst kurze zeitliche Dauer vom Untersuchungsantrag bis zum Ergebnis notwendig.

Abschließend bedarf es entsprechend ausgebildeter Ermittlungspersonen, die in den erarbeiteten Strukturen professionell arbeiten können. Da die IuK-Kriminalität sich in alle Bereiche des gesellschaftlichen Lebens ausbreitet und der menschliche Umgang mit moderner Informationssystemen häufig der größte Risikofaktor ist[312], müssen Grundkompetenzen und Handlungswerkzeuge für Sicherungsmaßnahmen im Rahmen des *Ersten Angriffs*[313] bei IuK-Straftaten bereits in der Grundausbildung gelegt werden.[314] Kriminalisten, die in IuK-Fachdienststellen, Kompetenzzentren oder IT-Forensik-Laboren arbeiten, müssen ständig fortgebildet werden. Nur so können die Organe der Strafrechtspflege den professionellen Täterstrukturen und neuen Tatmodalitäten begegnen. Schließlich muss auch der Einsatz externer IT-Fachleute diskutiert werden. Die Diskussion um IT-Fachleute muss mit Blick auf die Befugnisse von Nicht-Ermittlungspersonen, die Attraktivität der Poli-

[309] Vgl. Weihmann/Schuch, Kriminalistik, 164.
[310] Förster, in: Kriminalistik 10/2007, 621-623.
[311] Nach DIN 17020, 17025 (Prüflabore).
[312] Vgl. Brandt-Zimmermann, in: Streife Nr. 4 10-11/2011.
[313] Erster Angriff: Kriminalistischer Begriff für Maßnahmen an einem Tatort, die der Sicherung und Asuwertung von Spuren und Beweisen (Personal-, und Sachbeweis) dienen.
[314] Vgl. Kirchhoff, in: Kriminalistik 7/2013 (Kriminalistik-Campus), 491-495.

zei/anderer Sicherheitsbehörden als Arbeitgeber und die Kompetenzen der eigenen IuK-Ermittler geführt werden.[315]

Die skizzierten Herausforderungen können als Forderung nach einer „Kriminalistik der digitalen Welt“[316] zusammengefasst werden.

Vorliegend wurde das Hauptaugenmerk auf polizeiliche Strukturen gelegt, da diese die Ermittlungstätigkeiten vornehmlich eigenverantwortlich durchführen, bis der Fall an die Staatsanwaltschaft abgegeben wird (vgl. § 163 (1), (2) StPO). Um ein beweissicheres Strafverfahren zu gewährleisten, ist es natürlich dennoch wichtig, auch die Staatsanwaltschaft als Organ der Strafrechtspflege in die kriminalstrategischen Überlegungen mit einzubeziehen. Dabei wird die Einrichtung von Sonderdezernaten für die Bearbeitung von IuK-Kriminalität gefordert.[317]
Als Organe der Strafrechtspflege sind Polizei und Staatsanwaltschaft gemäß Art. 20 (3) GG an Recht und Gesetz gebunden. Die kriminalistisch arbeitenden Akteure sind also davon abhängig, was ihnen vom Gesetzgeber als Handlungsinstrument zur Verfügung gestellt wird. Dass dabei der Grad zwischen Sicherheit und Freiheit schmal ist, wurde bereits an mehreren Stellen deutlich. Letztlich hat die NSA-Affäre zu einer Intensivierung dieses Diskurses geführt.

5.2 Juristische Herausforderungen

Die herausgearbeiteten Eigenschaften der IuK-Kriminalität im engeren und im weiteren Sinn eröffnen Raum für Diskussionen, ob die derzeitige Rechtslage ausreichend ist, um das verfassungsrechtlich verankerte Ziel einer effektiven Strafverfolgung zu erreichen. Der Gegenpol dieses Ziels, nämlich der dem Internet ureigenste Freiheitsgedanke, findet seine Entsprechung in dem Grundsatz: Keine Strafverfolgung bzw. Wahrheitsfindung um jeden

[315] Vgl. Fieseler, in: DP 9/2011, 27-28.
[316] Ziercke, in: Kriminalistik 2/2008, 81.
[317] Vgl. Burandt/Tölle, in: Kriminalistik 8-9/2013, 525; Kreitlow, in: Die Polizei 10/2010, 294.

Preis.[318] Die Balance zwischen beiden Polen ist für die freiheitlich demokratische Grundordnung unverzichtbar, in Zeiten des alle Lebensbereiche tangierenden Kriminalitätsphänomens der IuK-Kriminalität allerdings schwierig zu finden, und zwar unabhängig davon, ob von der IuK-Technologie als Tatobjekt oder Tatmittel die Rede ist. Mit Blick auf die Fallzahlenentwicklung, die vielschichtigen dynamischen Wandlungsprozesse des Phänomens, der Auflösung von getrennten Online- und Offlinewelten und nicht zuletzt den Erkenntnissen aus der NSA-Affäre muss die Diskussion dennoch forciert werden. Grob kann dabei zwischen strafrechtlichen und strafprozessrechtlichen Aspekten unterscheiden werden.

5.2.1 Strafrechtliche Aspekte

Den Beginn der Anpassung des Strafrechts markierte die Einführung des 2. WiKG im Jahr 1986. Seither gab es zahlreiche Übereinkommen, Rahmenbeschlüsse und Strafrechtsänderungsgesetze auf nationaler Ebene, europäischer Ebene und auf der Ebene des Europarates. Auf einzelne Rechtsakte wurde bereits während der phänomenologischen Analyse verwiesen. Regelmäßig ging es dabei um die Intensivierung der Zusammenarbeit zwischen nationalen Strafverfolgungs- und Justizbehörden bei der Bekämpfung von Delikten mit Computer- bzw. IuK-Bezug sowie eine Angleichung der nationalen Strafrechtsordnungen. Eine Zusammenfassung dieser Rechtsakte mit internationalen Ausrichtung findet sich bei *Hilgendorf* und *Valerius*.[319] Das Erfordernis internationaler Anstrengungen ist mit Blick auf die phänomenologischen Strukturen (Verlagerung der Kriminalität in den nicht an Staatsgrenzen gebundenen digitalen Raum) offenkundig. Ebenso offenkundig ist allerdings, dass nationale Rechtssysteme sich teils erheblich voneinander unterscheiden. Ein Beispiel lieferte die Ratifizierung der 2004 in Kraft getretenen *Cybercrime-Konvention* des *Europarates*. Die in den USA hohe Wertschätzung der Meinungsfreiheit war mit den Vorgaben des Europarates zu Strafbarkeiten der Verbreitung rassistischen und fremdenfeindlichen Gedankenguts im Internet nicht vereinbar. Folglich mussten diese in einem separaten

[318] Vgl. BGH, 14.06.1960 – 1 StR 683/59; BGH, 03.07.1962 – 3 StR 22/61; BGH, 17.03.1983 – 4 StR 640/82.
[319] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 88-127.

Zusatzprotokoll festgeschrieben werden, da die Konvention seitens der Amerikaner ansonsten nicht unterzeichnet worden wäre.[320] Während die Strafbarkeit von Handlungen also an nationalen Grenzen enden kann, besitzt das Internet keinerlei Grenzen. Damit ist die Überschreitung nationaler Grenzen häufig eine gute Chance für Straffreiheit. Dessen sind sich organisiert agierende Täter bewusst. Dass das Instrument der justiziellen Rechtshilfe bislang nur bedingt tauglich ist, wurde oben erläutert (vgl. Kapitel 5.1).

Insgesamt kann von einer tatsächlichen Annäherung nationaler Strafrechtssysteme seit 1986 nur bedingt die Rede sein. Das *Bundesverfassungsgericht* stellt dazu in seiner Entscheidung zum *Lissabon-Vertrag* der *Europäischen Union* fest: „Die Sicherung des Rechtsfriedens in Gestalt der Strafrechtspflege ist seit jeher eine zentrale Aufgabe staatlicher Gewalt. […] Es ist eine grundlegende Entscheidung, in welchem Umfang und in welchen Bereichen ein politisches Gemeinwesen gerade das Mittel des Strafrechts als Instrument sozialer Kontrolle einsetzt.“[321] Aus diesen Prämissen folgert das Gericht: „Eine Übertragung von Hoheitsrechten über die intergouvernementale Zusammenarbeit hinaus darf in diesem grundrechtsbedeutsamen Bereich nur für bestimmte grenzüberschreitende Sachverhalte unter restriktiven Voraussetzungen zu einer Harmonisierung führen; dabei müssen grundsätzlich substantielle mitgliedstaatliche Handlungsfreiräume erhalten bleiben.“[322] Folglich werden auch zukünftig Einzelfallentscheidungen maßgeblich sein.

Auf nationaler Ebene bringt die IuK-Kriminalität ebenfalls grundlegende Herausforderungen mit sich. Mit der Einführung des 2. WiKG hat der Gesetzgeber zwar zeitnah auf neue Bedrohungen reagiert und sich durch verschiedene Rechtsakte den Bedrohungen angepasst. Angesichts des technischen Fortschritts und den sich ständig verändernden Tatstrukturen stellt sich jedoch die Frage, wie lange einzelne Verhaltensweisen unter strafrechtlichen Normen subsumiert werden können (vgl. Sonderbetrachtung Phishing). Wenn die Ausgestaltung der Strafrechtsvorschriften der Rechtsprechung überlassen, wird man dem aus dem Rechtsstaatsprinzip abgeleiteten Be-

[320] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 120.
[321] BVerfG, 2 BvE 2/08 v. 30.06.2009, Rn. 355.
[322] BVerfG, 2 BvE 2/08 v. 30.06.2009, Rn. 253.

stimmtheitsgrundsatz (Art. 20 GG) langfristig nicht gerecht werden. Hingegen läuft die regelmäßige Verabschiedung neuer, die Streichung oder Umgestaltung bisheriger Straftatbestände Gefahr, Verhalten/Handlungen zu kriminalisieren oder aber zu de- bzw. entkriminalisieren. Beispielhaft sei an dieser Stelle auf die Ausführungen zu den Urheberrechtsverletzungen, Strafbarkeitslücken im Bereich kinderpornografischer Delikte und Vorverlagerungen der Strafbarkeit von Hacking-Handlungen hingewiesen.
In diesem Zusammenhang muss auch das Unrechtsbewusstsein potenzieller Täter thematisiert werden. Als selbstständiges Element der Schuld ist das Bewusstsein des Täters, durch seine Handlung gegen eine Rechtsnorm zu verstoßen, nämlich eine Strafbarkeitsvoraussetzung. Mangelt es an diesem Unrechtsbewusstsein, kann ein sog. Verbotsirrtum nach § 17 StGB greifen. Dieser führt zu Straffreiheit bzw. Strafbarkeit wegen Fahrlässigkeit. Die Eigenschaften des Internets und das Nutzerverhalten tragen dazu bei, dass Mausklicks und Tastatureingaben ohne unmittelbare Auswirkungen in der physischen Umgebung von dem Täter als nicht strafbar wahrgenommen werden.[323]

Darüber hinaus führt die IuK-Kriminalität zu weiteren grundsätzlichen Fragen, die hier nur kurz skizziert werden sollen – zum Beispiel zum juristischen Tatort, zur strafrechtlichen Handlung und damit zum Gerichtsort. Automatisiert ablaufende Schad-Programme, Internetserver im Ausland, zeitversetzte Schadenseintritte und (im Fall der IuK-Kriminalität i.w.S.) Viktimisierungen, die bei der Strafzumessung aufgrund der Eigenschaft des Internets besonders berücksichtigt werden müssen, werden die Justiz beschäftigen.

Zusammenfassend handelt es sich um weitere Herausforderungen, denen sich das Strafrecht heute und in Zukunft stellen muss. *Dornseif* hat schon 2005 auf diese grundsätzliche Problematik hingewiesen. Er stellte fest, dass das Strafrecht beim Zusammentreffen mit der IuK-Technologie nicht mitgekommen ist und seine Dissertation der Beginn einer rechtsdogmatischen Aufarbeitung des Problemkreises der Computerkriminalität (IuK-Kriminalität)

[323] Vgl. Hilgendorf/Valerius, Computer- und Internetstrafrecht, Rn. 248-254.

sein muss.[324] Rückwärtig gilt es zu erkennen, dass der technische Fortschritt immer wieder zu einer Neuauflage der gleichen rechtsdogmatischen Diskussion führt/führen muss.

5.2.2 Strafprozessrechtliche Aspekte

Die in den Art. 1-19 GG festgeschriebenen Grundrechte sollen die Bürger vor staatlichen Eingriffen schützen. Da das Grundgesetz bereits am 23. Mai 1949 als rechtliche und politische Grundordnung der *Bundesrepublik Deutschland* in Kraft getreten ist, bringt die moderne Informationstechnologie des 21. Jahrhunderts enorme Herausforderungen im Spannungsfeld zwischen effektivem Grundrechtsschutz und staatlichen Befugnisnormen mit sich. Diese Tatsache kann damit belegt werden, dass sich das Bundesverfassungsgericht in den letzten Jahren mehrfach mit Themenkomplexen rund um die IuK-Technologie auseinandersetzen musste.[325] Als wesentliches Ergebnis dieser verfassungsgerichtlichen Auseinandersetzung(en) kann die Bildung des (neuen) *Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme* als Ausprägung des Allgemeinen Persönlichkeitsrechts gemäß Art. 2 (1) i.V.m. Art. 1 (1) GG angesehen werden (sog. IT-Grundrecht).[326] Die Begründung dieses Grundrechts zeugt von der Eigenschaft der IuK-Technologie, unsere Welt und Gesellschaft grundlegend zu verändern. Die Notwendigkeit des Persönlichkeitsschutzes stellt jedoch nur eine Seite der Medaille dar. Gleichzeitig fordern die Sicherheitsbehörden, dass sich in der Politik und der Gesellschaft ein Verständnis dafür entwickeln muss, dass moderne polizeiliche Ermittlungen das Internet und die Telekommunikationsmittel in den Blick nehmen müssen[327] und dass zur Bekämpfung von Straftaten Grundrechte eingeschränkt werden müssen.

Die Diskussion um Ermittlungsbefugnisse ist geprägt von den hiesigen Erkenntnissen der phänomenologischen Analyse. Eine Verlagerung verschie-

[324] Vgl. Dornseif, Phänomenologie der IT-Delinquenz, 29-31 (Vorwort), 38-39..
[325] Vgl. BVerfG, 1 BvR 518/08 v. 04.04.2006 (Rasterfahndung); BVerfG, 1 BvR 370/07 v. 27.02.2008 (Online-Durchsuchung); BVerfG, 1 BvR 256/08, 02.03.2010 (Vorratsdatenspeicherung).
[326] Vgl. BVerfG, 1 BvR 370/07 v. 27.02.2008, 1. Leitsatz.
[327] Vgl. Henrichs, in: Kriminalistik 6/2013, 392.

denster Kriminalitätsbereiche in den virtuellen Raum entspricht beispielsweise der Diskussion um den verdeckten polizeilichen Einsatz im Internet. Der Polizeibeamte und Eingriffsrechtler *Henrichs* und die Autoren *Bönisch* und *Bretscheider*, beide Mitarbeiter des LKA *Hessen*, führen die Rechtsdebatte um verdeckte personale Ermittlungen im Internet auf der Grundlage der Rechtsvorschriften zu den verdeckten personalen Ermittlungen in der Realwelt. Sie differenzieren zwischen *Kriminalistischer List*, *nicht offen ermittelnden Polizeibeamten*[328] und dem Einsatz *Verdeckter Ermittler*[329].[330] Beide Autoren kommen zu dem Ergebnis, dass eine analoge Anwendung der bestehenden Befugnisnormen für den traditionellen Einsatz eines Verdeckten Ermittlers (§ 110a StPO) rechtliche Schwierigkeiten birgt. Der Grundrechtseingriff durch verdeckte personale Ermittlungen im Internet erreicht keineswegs die Qualität der durch verdeckter Ermittlungen herbeigeführten Täuschungen in der Realwelt (Betreten der Wohnung, persönlicher Kontakt, Teilnahme am Rechtsgeschäft). Beide halten die Maßnahme jedoch für zukunftsweisend.[331]

Ähnlich wie im Bereich des Strafrechts führt der auf verschiedenen Ebenen stattfindende Wandel des Modus Operandi der IuK-Kriminalität zu Anwendungs- und Anpassungsschwierigkeiten im Bereich strafprozessualer Ermittlungsbefugnisse. Es besteht also die Gefahr, dass sich Täter durch neue Begehungsweisen einer strafrechtlichen Verfolgung entziehen. Da dies einer ‚Bankrotterklärung' des Staates gleichkommen würde, ist, wie bereits deutlich gemacht, weitere Anpassung gefordert. *Ziercke* konstatierte schon 2007, dass die Täter einen technologischen Vorsprung haben. Er forderte technikoffene und damit flexible Rahmenbedingungen, die „[…] am Ende des Gesetzgebungsverfahrens nicht bereits veraltet sind."[332] Dabei muss außerdem berücksichtigt werden, dass sich kaum ein kriminalistischer und kriminologischer Konsens im Bereich der wachsenden IuK-Kriminalität i.w.S. finden lässt. *Zierckes* appellierte 2007: „Das bedeutet, dass wir eine breite Auswahl

[328] Nicht offen ermittelnde Polizeibeamte: Ein nur im Einzelfall verdeckt auftretender Polizeibeamter. Es besteht für einen konkreten Eintelfall ein Ermittlungsauftrag (z.B. Scheinkauf), vgl. Weihmann/Schuch, Kriminalistik, 563.

[329] Verdeckter Ermittler: Polizeibeamter, der auf Dauer unter einer ihm verliehenen, veränderten Identität ermittelt und dessen Ermittlungsauftrag wesentlich weiter gefasst ist, vgl. Weihmann/Schuch, Kriminalistik, 563-564.

[330] Henrichs, in:Kriminalistik 11/2012, 632;Bönisch/Bretschneider, in:Die Polizei 4/2013, 99.

[331] Henrichs, in:Kriminalistik 11/2012, 635;Bönisch/Bretschneider, in:Die Polizei 4/2013, 105.

[332] Ziercke, in: Kriminalistik 2/2008, 79.

an Instrumenten in unserem Instrumentenkasten benötigen, die von der Schwere der Sozialschädlichkeit eines Delikts genau so wie vom speziellen Modus Operandi der Täterseite abhängig sind.“[333] Aus heutiger Sicht, also beinahe sieben Jahre nach *Zierckes* Worten, muss erkannt werden, dass das Verhältnis zwischen technischem Fortschritt der IuK-Kriminalität und effizienten Ermittlungsbefugnissen gleich geblieben ist – eine Angleichung steht nach wie vor aus.

Singelnstein, der präzise und ausführlich die Möglichkeiten und Grenzen der bestehenden strafprozessualen Ermittlungsmaßnahmen erläutert[334], kommt hingegen zu dem Ergebnis, dass eine professionelle Strafverfolgung ohne weiteres mit den bestehenden Befugnissen möglich ist (Stand: 2012). Der Jurist sieht die Gefahr der Erstellung von Persönlichkeitsprofilen gegeben und folgert, dass rechtlich nicht alles zulässig und wünschenswert ist, was technisch möglich ist. Dieser grundlegenden Aussage stimmt der Autor dieser Arbeit zu. Die Forderung Zierckes nach flexiblen, technikoffenen Ermittlungsbefugnissen und einer breiten Auswahl an Instrumenten kann gefährlich sein. Wichtig ist daher, dass die bestehenden Ermittlungsbefugnisse genutzt werden.

Und dennoch – die phänomenologische Analyse hat gezeigt, dass eine generelle Ablehnung von neuen oder angepassten Ermittlungsbefugnissen utopisch ist. Die Kriminalitätslandschaft wird sich zukünftig weiter verändern und es ist eine Frage der Zeit, bis bestehende Ermittlungsbefugnisse unzureichend werden, um dem Anspruch der Strafverfolgung gerecht zu werden. Auch *Singelnstein* ist sich dessen bewusst. Schließlich erörtert er Voraussetzungen für die Einführung neuer Befugnisse. *Singelnstein* setzt einen strengen Verhältnismäßigkeitsgrundsatz, konkrete, handhabbare und praktische strafprozessuale Maßstäbe und formelle Verfahrensvorschriften wie den Richtervorbehalt voraus.[335] Zusammenfassend beziehen sich diese Voraussetzungen auf die Ausgestaltung von Gesetzen. Dieser Ansatz ist nach hiesiger Meinung entscheidend, um die notwendige Balance zwischen den wi-

[333] Ziercke, in: Kriminalistik 2/2008, 79.
[334] Vgl. Singelnstein, in: NStZ 11/2012, 593-606.
[335] Vgl. Singelnstein, in: NStZ 11/2012, 606.

derstreitenden Positionen zu finden. Das Spannungsfeld zwischen Sicherheit und Freiheit bleibt.

Das Dilemma des Status Quo, einschließlich seiner internationalen Dimension, wird in der Diskussion um das Instrument der *Vorratsdatenspeicherung* offensichtlich. Die neue Bundesregierung will sich dieser Diskussion annehmen und das Problem lösen. Dabei geht es um die Verpflichtung der jeweiligen Provider (Anbieter), Telefon- und Internetverbindungsdaten jedes Nutzers verdachtsunabhängig zu speichern und unter gewissen Voraussetzungen den Strafverfolgungsbehörden zur Verfügung zu stellen. Eine Richtlinie des Europäischen Parlaments mit diesem Inhalt trat im Mai 2006 in Kraft[336] und wurde durch den Deutschen Bundestag im November 2007 in nationales Recht umgesetzt. Über 30.000 Bürger reichten in der Folge eine Sammelverfassungsbeschwerde beim *Bundesverfassungsgericht* ein. Im Urteil vom 02. März 2010 erklärte das Bundesverfassungsgericht die *Vorratsdatenspeicherung* in der bisherigen Ausgestaltung für rechtswidrig und forderte den Gesetzgeber zu einer verfassungskonformen Neugestaltung auf.[337] Diese Neugestaltung ist bislang nicht geschehen. Die Frist zur Umsetzung der EU-Richtlinie ist inzwischen abgelaufen, *Deutschland* befindet sich in einem „europarechtswidrige[n] Zustand“[338] und es fehlt an einer wichtigen Ermittlungsbefugnis zur Bekämpfung schwerer Straftaten.

In diesem Zusammenhang muss ein weiteres Instrument erwähnt werden, das der *Vorratsdatenspeicherung* sehr ähnlich ist. Bei der sogenannten *Bestandsdatenauskunft* geht es um das Auskunftsersuchen von Sicherheitsbehörden bezüglich Daten eines Telekommunikationsteilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.[339] Die Nähe zur *Vorratsdatenspeicherung* drängt sich auf. Auch die *Bestandsdatenauskunft* war am 24. Januar 2012 Gegenstand einer verfassungsgerichtlichen Auseinandersetzung in der entschieden wurde, dass die *Bestandsdatenauskunft* bis spätestens Ende Juni 2013 neu geregelt werden

[336] Vgl. Richtlinie 2006/24/EG.
[337] Vgl. BVerfG, 1 BvR 256/08 v. 02.03.2010.
[338] Sensburg, in: Kriminalistik 6/2013, 393.
[339] Vgl. § 3 Nr. 3 TKG.

musst.[340] *Bundestag* und *Bundesrat* haben das neue Gesetz inzwischen verabschiedet.[341] Eine rechtliche Würdigung und Einschätzung der Neuregelung hat *Henrichs* vorgenommen. Neben dem Gewinn einer strafprozessualen Befugnis (insbesondere die Möglichkeit der Zuordnung von dynamischen IP-Adresse – sprich, Rückverfolgung von Internetnutzern) bemängelt er weiterhin die nicht vorhandenen Speicherungsfristen von Verbindungsdaten gemäß § 96 TKG und befürchtet eine erneute Verfassungsbeschwerde gegen die zum 01. Juli 2013 eingeführte Neuregelung. Kritisiert wird besonders die Ausgestaltung des Gesetzes, die den Behörden wohl zu viel Freiraum lässt. Hier findet sich *Singelnsteins* Ansatz einer strengen Ausgestaltung des Gesetzes wieder.

Dieser Exkurs in eine zentrale Ermittlungsbefugnis, die von verschiedenen Sicherheitsakteuren seit Jahren gefordert wird[342], verdeutlicht eindrucksvoll die Schwierigkeiten und verschiedenen Rollen in der Debatte zwischen Sicherheit ohne Freiheit und Freiheit ohne Sicherheit. Der Journalist *Matthias Zahn* kommentierte die Neuregelung der *Bestandsdatenauskunft* in einem Audiokommentar der ARD mit dem Ergebnis: „Die Verfassungsrichter sind längst die obersten Datenschützer der Republik. Nicht, weil sie es unbedingt sein wollten, sondern weil die Politik versagt.“[343] Dies ist kein wünschenswerter Zustand. Der Wunsch, IuK-Kriminalität zu bekämpfen, mündet in gesellschaftlichen ‚Unruhen‘ und juristischen Auseinandersetzungen. So findet eine Verlagerung des Problems statt, ohne jenes der IuK-Kriminalität zuvor gelöst zu haben. Grundsatzdiskussion darüber, was die Gesellschaft will und Kompromisse sind notwendig.

[340] Vgl. BVerfG, 1 BvR 1299/05 v. 24.12.2012, Rn. 188-190.
[341] Vgl. BT-Drucks. 17/12879, 17/12034; BR-Drucks. 251/13.
[342] Vgl. Burandt/Tölle, in: Kriminalistik 8-9/2013, 524; Ziercke, in: Kriminalistik 2/2008, 80.
[343] Zahn, Kommentar zur Bestandsdatenauskunft v. 03.05.2013, 18:07 Uhr, www.ard.de.

6 Fazit / Ausblick

Im Mittelpunkt dieser Arbeit stand die Frage, ob die IuK-Kriminalität ein neues Kriminalitätsphänomen oder das Ergebnis eines Wandels des Modus Operandi ist.

Diese forschungsleitende Frage wurde bereits durch die Zwischenergebnisse der Kapitel 4.3.2 und 4.3.4 behandelt. Zusammenfassend gilt, dass die hier diskutierte IuK-Kriminalität bereits 1986 durch die Einführung des 2. WiKG bzw. durch die erstmalige kriminalstatistische Erfassung der Computerkriminalität im Jahre 1987 begründet wurde. Seitdem führten und führen technische und gesellschaftliche Wandlungsprozesse zu starken Veränderungen dieses Kriminalitätsphänomens. Die Missbrauchsmöglichkeiten der modernen IuK-Technologie steigen durch eine zunehmende Vernetzung der Gesellschaft kontinuierlich. Das gilt sowohl für die Delikte der IuK-Kriminalität i.e.S. als auch für die der IuK-Kriminalität i.w.S. Dennoch hat die Analyse gezeigt, dass die Straftaten der IuK-Kriminalität phänomenologisch gleich geblieben sind bzw. bleiben. Folglich ist die aktuelle IuK-Kriminalität das Ergebnis eines Wandels des Modus Operandi. Das bedeutet, dass sich die Beweisfindung, Beweissicherung und Beweisführung im Strafverfahren den sich ständig verändernden Tatbegehungsweisen möglichst schnell anpassen muss. Für diese notwendige Anpassung sind die folgenden, weiteren Ergebnisse dieser Arbeit von entscheidender Bedeutung:

- Die Straftaten der IuK-Kriminalität unterscheiden sich durch eine Vielzahl kriminalistischer, kriminologischer und juristischer Faktoren. Pauschale Aussagen zu Bekämpfungsmöglichkeiten der IuK-Kriminalität sind kaum möglich. Die Kategorisierung des Kriminalitätsphänomens in einen engeren und einen weiteren Sinn hat Schwächen und die Zahlen der PKS sind wenig aussagekräftig.

- Für die Zukunft müssen die Organe der Strafrechtspflege zweierlei erkennen. Einerseits ist die Diskussion um digitale Bedrohungen nicht neu. Andererseits führen aber die steigenden Missbrauchsmöglichkeiten zu einer

wachsenden Diskrepanz zwischen Bedrohung, Schutz- und Bekämpfungsmöglichkeiten.

- Der von *Edward Snowden* angeschobene Diskurs zwischen Sicherheit und Freiheit ist für das Gleichgewicht einer Demokratie von entscheidender Bedeutung. Die Debatte muss mit Blick auf die aktuellen und zukünftigen Herausforderungen durch die moderne IuK-Technologie fortgeführt werden.

- Die Gesellschaft muss insgesamt verstehen, dass es sich bei der Bedrohung durch die IuK-Kriminalität vielfach um ein ‚hausgemachtes' Problem handelt, welches auf dem Verhalten der Menschen beruht. Faszination, Naivität und Angst – in sehr unterschiedlichen Ausprägungen – sind die Triebfedern dieses Verhaltens. Kernelement ist die Preisgabe persönlicher Daten, die sowohl kommerziell als auch zu kriminellen Zwecken genutzt werden.

- Die Menschen glauben, dass das Internet einer nicht beeinflussbaren Logik folgt, die zu komplex ist, als dass man diese verstehen könnte. *Morozov*, der diese Denkweise als ‚Internetzentrismus' bezeichnet, widerspricht und appelliert daran, zu erkennen, dass die Ausgestaltung der Informationstechnologie grundsätzlich keinen physikalischen Gesetzmäßigkeiten und damit keiner unbeeinflussbaren Logik unterliegt. „Es gibt verschiedene Möglichkeiten, die Welt zu vernetzen, und die Art, wie wir sie heute vernetzen, könnte sich auf lange Sicht schädlich für die Demokratie erweisen."[344] Die Art und Weise der Vernetzung unserer Gesellschaft ist seit jeher allein durch die wirtschaftlichen Interessen und skrupellosen Mächte des *Silicon Valley* bestimmt. Es handelt sich um ein Monopol der Ökonomie hinsichtlich der Ausgestaltung des Internets.[345]

- Das Monopol der Ökonomie begann bereits 1992 mit der Veröffentlichung/Privatisierung der Technologie des *World Wide Web*. Seither existiert kein Gegenpol in Form von staatlicher Kontrolle. Die einseitigen Interessen der Ökonomie haben zu einem erheblichen Ungleichgewicht mit entsprechenden Konsequenzen geführt. Dazu gehört auch, dass die IuK-Kriminalität

[344] Morozov, in: FAZ, 15.01.2014, 25; vgl. auch: FAZ, 10.12.2013, 27/29.
[345] Vgl. Morozov, in: FAZ, 15.01.2014, 25.

sich in der hier gezeigten Art und Weise entwickeln konnte. Entscheidend ist also nicht die Frage der Kategorisierung des Internets in ‚gut' oder ‚schlecht' sondern vielmehr die Frage nach der Gestaltung des Internets und nach dem Einfluss auf eben diese Gestaltung.

- In der aktuellen Debatte um nationale Anstrengungen, sich nach der NSA-Affäre von der amerikanischen Informationsstruktur abzugrenzen (‚Balkanisierung'), wird die Macht des *Silicon Valley* und dessen Kampf um den Machterhalt besonders deutlich.[346] In Sorge um ihren lenkenden Einfluss warnen die Konzerne des *Silicon Valley* vor einem Zusammenbruch der Einheit des Netzes und einem Rückschritt in der Entwicklung zu einer vernetzten Welt. Morozov hingegen sieht darin die Chance, die Gesellschaft auf dem „Winterschlaf wachzurütteln"[347] und die Vorstellung zu überwinden, dass das Internet in seiner derzeitigen Ausgestaltung alternativlos ist. Eine Dezentralisierung der IT-Infrastruktur ist schließlich kein technologisches Hemmnis für einen globalen Datenfluss.[348]

Der Autor dieser Arbeit folgt der dargelegten Argumentation *Morozovs.* Sowohl für die Bekämpfung der IuK-Kriminalität an sich als auch für das gesamtgesellschaftliche Gleichgewicht der Demokratie steht schlussendlich die Forderung nach „Mehr Politik!"[349], denn ihre Aufgabe ist es, die Gesellschaft zu gestalten. Die Strafrechtspflege hat sich daran zu orientieren. Es geht um eine „politische[n] Agenda […], die zu Gerechtigkeit, überlegtem Handeln und dem Schutz der Privatsphäre beiträgt."[350] Ob die Maßnahmen der neuen *deutschen Bundesregierung* (die Diskussion um den Internet-Ausschuss des *Deutschen Bundestags*, die Frage der Ministerzuständigkeit für Internetfragen, um die digitale Agenda der *Bundesregierung*, die Verhandlungen über *‚No Spy'-Abkommen*, die Debatte um ein von den USA unabhängiges *‚EU-Internet'*)[351] Schritte in die richtige Richtung sind, wird sich zeigen. Mit *Nikolai*

[346] Morozov, in: SZ, 20.01.2014, 9.
[347] Morozov, in: SZ, 20.01.2014, 9.
[348] Vgl. Morozov, in: SZ, 20.01.2014, 9.
[349] Morozov, in: FAZ, 15.01.2014, 25.
[350] Morozov, in: FAZ, 15.01.2014, 25.
[351] Zu den genannten Maßnahmen, vgl. von Leitner, in: FAZ, 26.11.2013, 25; Gropp, in: FAZ, 23.12.2013, 17; Kaube, in: FAZ, 09.11.2013, 1; Stalinski, in: tagesschau.de, 19.12.2013, www.tagesschau.de.

Horns Worten bedarf es eines ‚Kategorischen Netzimperativs', der da lautet: „Handle im Netz gemäß denjenigen Grundsätze, von denen du zugleich wollen kannst, dass sie als handlungsregelnde Maßstäbe auch im analogen Leben gelten!"[352]. Erste konkrete Aussagen in diese Richtung wurden nun vom *deutschen Bundesinnenminister de Maizière* vernommen. In seiner Ministerrede zu den wichtigsten Themen der neuen Legislaturperiode forderte er einem „Ordnungsrahmen"[353] für das Internet und betonte, dass es „um den Erhalt und den Schutz des Netzes als geordneten Freiheitsraum […]"[354] geht. Bis diesen Worten Taten folgen und es der Politik als gestaltende Kraft gelingt, den Kategorischen Netzimperativ durch gesetzgebende Maßnahmen zumindest ansatzweise zu implementieren, bleibt (nicht nur) die IuK-Kriminalität eine große Herausforderung für die Organe der Strafrechtspflege im 21. Jahrhundert.

[352] Horn, in: FAZ, 27.12.2013, 7.
[353] de Maizière, Rede des Bundesinnenministers im Bundestag (gesprochenes Wort), 30.01.2014, www.bund.bmi.de.
[354] de Maizière, Rede des Bundesinnenministers im Bundestag (gesprochenes Wort), 30.01.2014, www.bund.bmi.de.

7 Verzeichnisse und Anhang

7.1 Abbildungen

7.2 Bücher, Sammelbandbeiträge und andere Literatur

Berners-Lee, Tim — Der Web-Report. Übersetzt aus dem Amerikanischen von: Majetschak, Beate, München 1999.

Bundeskriminalamt (Hrsg.) — Polizeiliche Kriminalstatistik. Jahrbücher 1987-2012, Wiesbaden 1988-2013.

Bundeskriminalamt (Hrsg.) — Cybercrime. Bundeslagebild 2012, Wiesbaden 2013.

Bundeskriminalamt (Hrsg.) — Polizeiliche Kriminalstatistik 2012. Tabellenerläuterungen.

Bundeskriminalamt (Hrsg.) — Polizeiliche Kriminalstatistik 2011-2012. Grundtabelle „Tatmittel Internet".

Bundeskriminalamt (Hrsg.) — Cybercrime. Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime, Wiesbaden.

Bundesministerium des Innern (Hrsg.) — Polizeiliche Kriminalstatistik 2012. IMK-Kurzbericht 2012, Berlin 2013.

Bundesministerium des Innern (Hrsg.) — Cyber-Sicherheitsstrategie für Deutschland, Berlin 2011.

Bundesministerium des Innern / Bundesministerium der Justiz (Hrsg.) — Zweiter Periodischer Sicherheitsbericht, Berlin 2006.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) (Hrsg.) — Netzgesellschaft. Eine repräsentative Untersuchung zur Mediennutzung und dem Informationsverhalten der Gesellschaft in Deutschland, Berlin 2011.

Dimbath, Oliver — Einführung in die Soziologie, Paderborn 2011.

Dornseif, Maximilian	Phänomenologie der IT-Delinquenz, Bonn 2005 (zugleich Dissertation Universität Bonn 2005).
Duden (Hrsg.)	Die deutsche Rechtschreibung, 26., völlig neu bearbeitete und erweiterte Auflage, Berlin / Mannheim / Zürich 2013.
Ernst, Stefan (Hrsg.)	Strafrechtliche Fragen, in: Hacker, Cracker und Computerviren. Recht und Praxis der Informationssicherheit, Köln 2004, Rz. 228-418 (S. 78-146).
Foucault, Michel	Geschichte der Gouvernementalität 2. Die Geburt der Biopolitik: Vorlesungen am Collège de France 1978-1979. Übersetzt aus dem Französischen von: Schröder, Jürgen, Frankfurt a.M. 2004.
Glasenapp, Jörn	Chat, in: Faulstich, Werner (Hrsg.): Grundwissen Medien, 5. vollständig überarbeitete und erheblich erweiterte Auflage, Stuttgart / Paderborn 2005, S. 148-156.
Gleß, Sabine	Beweisrechtsgrundsätze grenzüberschreitender Strafverfolgung, in: Amelung, Knut / Böse, Martin / Duttge, Gunnar u.a. (Hrsg.): Neue Schriften zum Strafrecht, Band 2, Baden-Baden 2006 (zugleich Habilitationsschrift Universität Münster 2004/2005).
Göppinger, Hans (Begr.)	Kriminologie, 6., vollständig neu bearbeitete und erweiterte Auflage, München 2008.
Groß, Hans (Begr.) / Geerds, Friedrich (Bearb.)	Handbuch der Kriminalistik, Band 1, 10. völlig neu bearbeitete Auflage, Berlin 1977.
Haferkamp, Hans	Kriminalität ist normal, Stuttgart 1972.
Hilgendorf, Eric / Valerius, Brian	Computer- und Internetstrafrecht. Ein Grundriss, 2. Auflage, Berlin / Heidelberg 2012.
Huber, Melanie	Kommunikation im Web 2.0. Twitter, Facebook & Co, 2. überarbeitete Auflage, Konstanz 2010.
Industrie- und Handelskammer Nord (Hrsg.)	Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime, Hamburg 2013.
Jaspersen, Thomas	Intranet / Extranet, in: Faulstich, Werner (Hrsg.): Grundwissen Medien, 5. vollständig überarbeitete und erheblich erweiterte Auflage, Stuttgart / Paderborn 2005, S. 294-302.
Jofer, Robert	Strafverfolgung im Internet. Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzwerken, in: Lang, Peter (Hrsg.): Europäische Hochschulschriften, Reihe 2, Rechtswissenschaften, Band 2555, Frankfurt a.M. 1999 (zugleich Disseration Universität München 1998).
Kaiser, Günther	Kriminologie. Eine Einführung in die Grundlagen, 8. neu bearbeitete und erweiterte Auflage, Heidelberg 1989.
Kindhäuser, Urs	Strafrecht. Besonderer Teil 1. Straftaten gegen Persönlichkeitsrechte, Staat und Gesellschaft, 6., völlig neu überarbeitete Auflage, Baden-Baden 2014.

Kindler, Waldemar	Freiheit braucht Sicherheit – Sicherheit braucht Freiheit, in: Bundeskriminalamt (Hrsg.): Informations- und Kommunikationskriminalität, Polizei+Forschung, Band 27, München 2004, S. 147-157.
Klau, Peter	Das Internet. Weltweit vernetzt, 2. unveränderte Auflage, Vaterstetten 1994.
Landeskriminalamt NRW (Hrsg.)	Cybercrime in NRW – Entwicklung und Bewertung. Lagebild 2012, Düsseldorf 2013.
Lang, Norbert / Bekavac, Bernard	World Wide Web, in: Faulstich, Werner (Hrsg.): Grundwissen Medien, 5. vollständig überarbeitete und erheblich erweiterte Auflage, Stuttgart / Paderborn 2005, S. 433-453.
Lauber, Achim / Wagner, Ulrike	Podcasts und Internetradio – Wie sich Jugendliche und junge Erwachsene die neuen Medien zwischen Radio und Internet aneignen, in: Zerfaß, Ansgar / Welker, Martin / Schmidt, Jan (Deutsche Gesellschaft für Online-Forschung e.V.) (Hrsg.): Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum, Köln 2008, S. 168-184.
Medienpädagogischer Forschungsverbund Südwest (Hrsg.) (MPFS)	JIM-Studie 2012. Jugend, Information, (Multi-) Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger, Stuttgart 2012.
Miller, Daniel	Das wilde Netzwerk. Ein ethnologischer Blick auf Facebook. Übersetzt aus dem Englischen von: Jakubzik, Frank, Berlin 2012.
Mühler, Kurt	Sozialisation. Eine soziologische Einführung, Paderborn 2008.
Münchener Kommentar zum Strafgesetzbuch	Band 4, München 2003 ff.
Negroponte, Nicholas	Being digital, London / Hodder / Stoughton 1995.
Palfrey, John / Gasser, Urs	Generation Internet. Die Digital Natives: Wie sie leben, was sie denken, wie sie arbeiten. Übersetzt aus dem Amerikanischen von: Reinhart, Franka / Topalova, Violeta, München 2008.
Passig, Kathrin / Lobo, Sascha	Internet. Segen oder Fluch, Berlin 2012.
Pierrot, Olivier	Sachverhalte, in: Ernst (Hrsg.): Hacker, Cracker und Computerviren. Recht und Praxis der Informationssicherheit, Köln 2004, Rz. 1-227 (S. 1-77).
Ratzel, Max-Peter	Lage, Bedrohungsszenarien und Handlungsbedarf, in: Bundeskriminalamt (Hrsg.): Informations- und Kommunikationskriminalität, Polizei + Forschung, Band 27, München 2004, S. 33-51.
Schirrmacher, Frank	EGO. Das Spiel des Lebens, München 2013.
Schneider, Hans-Joachim	Kriminologie, Berlin / New York / de Gruyter 1987.

Schwind, Hans-Dieter	Kriminologie. Eine praxisorientierte Einführung mit Beispielen, 21. neu bearbeitete und erweiterte Auflage, Heidelberg / München / Landsberg u.a. 2011.
Ständige Konferenz der Innenminister und –senatoren der Länder (Hrsg.) (IMK)	Programm Innere Sicherheit. Fortschreibung 2008/2009, Potsdam 2009.
Statistisches Bundesamt (Hrsg.)	Statistisches Jahrbuch. Deutschland und Internationales, Wiesbaden 2013.
Weihmann, Robert / Schuch, Claus Peter	Kriminalistik. Für Studium, Praxis und Führung, 12. überarbeitete Auflage, Hilden 2011.
Wernert, Manfred	Internetkriminalität. Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen, Stuttgart 2011.
Wisotzky, Rolf	Der polizeiliche Staatsschutz und der Weg in die moderne Kommunikationstechnologien, in: Bundeskriminalamt (Hrsg.): Festschrift für Horst Herold zum 75. Geburtstag. Das Bundeskriminalamt am Ausgang des 20. Jahrhundert, Wiesbaden 1998, S. 479-504.

7.3 Zeitungs- und Zeitschriftenartikel

Beck, Simon Markus	Lehrermobbing durch Videos im Internet – ein Fall für die Staatsanwaltschaft?, in: Multimedia und Recht, Heft 2/2008, S. 77-82.
Becker, Sven / von Bredow, Rafaela / Darnstädt, Thomas u.a.	Der Terrorist und die Brandstifter, in: Der Spiegel, Heft 31/2011, S. 70-80.
Blaustein, Manfred	Sexueller Missbrauch von Kindern – Über Täter und Täterinnen, in: der kriminalist, Heft 10/2013, S. 6-12.
Boie, Johannes / Obermaier, Frederik	Reise ins Internet. Wie das World Wide Web funktioniert und wo seine Schwachstellen liegen, in: Süddeutsche Zeitung, 3./4.08.2013, S. 6-7.
Bönisch, Markus / Bretschneider, Harald	Der verdeckte polizeiliche Einsatz im Internet, in: Die Polizei, Heft 4/2013, S. 99-105.
Brandt-Zimmermann, Anita	Angriffe auf Daten und Informationen deutscher Behörden. Der größte Risikofaktor ist der Mensch, in: Streife, Nr. 4 10/11 2011, S. 18-20.
Braun, Stefan	„Diese Affäre beunruhigt mich sehr“, in: Süddeutsche Zeitung, 27./28.07.2013, S. 5.
Breyer, Patrick	Die Cyber-Crime-Konvention des Europarates, in: Datenschutz und Datensicherheit, 25 (2001), S. 592-600.

Buermeyer, Ulf	Der strafrechtliche Schutz drahtloser Computernetzwerke (WLANs), in: Online-Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht, Heft 8/2004, S. 285-294.
Bünder, Helmut / Gropp, Martin	Ein Großangriff auf deutsche Internetnutzer, in: Frankfurter Allgemeine Zeitung, 22.01.2014, S. 15.
Burandt, Klaus / Tölle, Ralf	Cybercrime – nicht nur in der Großstadt, in: Kriminalistik, Heft 8-9/2013, S. 523-525.
Burgheim, Joachim / Friese, Hermann	Unterscheidungsmerkmale realer und vorgetäuschter Sexualdelikte, in: Kriminalistik 8-9/2006, S. 510-516.
Dworschak, Manfred	Kinderjahre einer Revolution, in: Der Spiegel, Heft 17/2013, S. 98-103.
Feltes, Thomas	Was beeinflusst die polizeiliche Aufklärungsquote, in: Kriminalistik, Heft 4/2009, S. 196-204.
Fieseler, Jörn	Diskussion um Cybercops und Vorratsdatenspeicherung, in: Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei, Heft 9/2011, S. 27-28.
Förster, Christian	Der polizeiliche Sachverständige für IT-Forensik, in: Kriminalistik, Heft 10/2007, S. 621-623.
Frankfurter Allgemeine Zeitung	Ziercke: Cyberkriminalität ist unvergleichbare Bedrohung, 13.11.2013, S. 1.
Frankfurter Allgemeine Zeitung	Mehr als 340 Täter sollen Kinder missbraucht haben, 16.11.2013, S. 10.
Frankfurter Allgemeine Zeitung	Chinas unheimliches Interesse am Internetgeld, 20.11.2013, S. 17.
Frankfurter Allgemeine Zeitung	Deutschland darf kein schlafwandelnder Riese sein, 04.10.2013, S. 2.
Frankfurter Allgemeine Zeitung	Chronik einer Affäre, 25.10.2013, S. 4.
Frankfurter Allgemeine Zeitung	Die Demokratie verteidigen im digitalen Zeitalter, 10.12.2013, S. 27/29.
Frankfurter Allgemeine Zeitung	Achtzehnjähriger gesteht, 02.04.2012, S. 7.
Frankfurter Allgemeine Zeitung	Emden gedenkt Lenas, 13.04.2012, S. 8.
Frankfurter Allgemeine Zeitung	Die Unterwelt liebt auch das virtuelle Geld, 31.05.2013, S. 20.
Frankfurter Allgemeine Zeitung	Zwei Wochen Arrest für Aufruf zur Lynchjustiz, 31.05.2012, S. 9.
Gatzke, Wolfgang	Kriminalität im Netz, in: Kriminalistik, Heft 2/2012, S. 75-78.
Gropp, Martin	Das Internet erreicht die Politik, in: Frankfurter Allgemeine Zeitung, 23.12.2013, S. 17.

Gropp, Martin / Knop, Carsten	„Wir merken, dass uns die Nutzer mehr Fragen stellen“, in: Frankfurter Allgemeine Zeitung, 16.09.2013, S. 22.
Heinz, Wolfgang	60 Jahre Polizeiliche Kriminalstatistik. Vergangenheit, Gegenwart und Zukunft, in: Kriminalistik, Heft 7/2013, S. 458-462.
Henrichs, Axel	Polizeiliche Befugnisse zu Ermittlungsmaßnahmen mit TK- und Internetbezug. Neuregelung zur Bestandsdatenauskunft ab 1. Juli 2013, in: Kriminalistik, Heft 6/2013, S. 388-392.
Henrichs, Axel	Verdeckte personale Ermittlungen im Internet, in: Kriminalistik, Heft 11/2012, S. 632-636.
Hilgendorf, Eric / Hong, Seung-Hee	Cyberstalking. Eine neue Variante der Internetkriminalität, in: Kommunikation und Recht, Heft 4/2003, S. 168-172.
Horn, Nikolai	Die ungeahnte Macht, in: Frankfurter Allgemeine Zeitung, 27.12.2013, S. 7.
Jakobs, Joachim	Zur Datensicherheit äußern sie sich nicht!, in: Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei, Heft 7/2013, S. 9-11.
Janovsky, Thomas	Internet und Verbrechen. Die virtuelle Komponente der Kriminalität, in: Kriminalistik, Heft 7/1998, S. 500-503.
Kaube, Jürgen	Wider einen Internetminister, in: Frankfurter Allgemeine Zeitung, 09.11.2013, S. 1.
Kerner, Hans-Jürgen	Ist die Kriminalitätslage in unserem Lande schlimmer geworden?, in: Der Bürger im Staat. Sicherheit und Kriminalität, Heft 1/2003, S. 4-8.
Kirchhoff, Martin	IuK-Kriminalität (Cyberkriminalität). Grundkompetenzen im Bachelorstudium der Polizei, in: Kriminalistik, Heft 7/2013 (Kriminalistik-Campus), S. 491-495.
Knop, Carsten	Angela Merkel im Neuland der Häme, in: Frankfurter Allgemeine Zeitung, 20.06.2013, S. 9.
Knop, Carsten / Finsterbusch, Stephan	Die nächte Cebit führt die „Big Data“-Debatte, in: Frankfurter Allgemeine Zeitung, 29.08.2013, S. 15.
Kreitlow, Jörn	Strategie zur Bekämpfung der IuK-Kriminalität, in: Die Polizei, Heft 10/2010, S. 290-297.
Leitner von, Felix	Der Bauplan für ein sicheres Internet, in: Frankfurter Allgemeine Zeitung, 26.11.2013, S. 25.
Levin, Ilya / Schwarz, Michael	Zum polizeirechtlichen Umgang mit sog. Facebook-Partys – „Ab geht die Party und die Party geht ab!“ – oder doch nicht?, in: Die Polizei, Heft 3/2012, S. 72-79.
Lindner, Christian	Ordnung für den Datenmarkt – eine erste Agenda, in: Frankfurter Allgemeine Zeitung, 14.08.2013, S. 25.
Morozov, Evgeny	Mehr Politik!. Übersetzt aus dem Englischen von: Bischoff, Michael, in: Frankfurter Allgemeine Zeitung, 15.01.2014, S. 25.

Morozov, Evgeny	Der Preis der Heuchelei. Übersetzt aus dem Englischen von: Fienbork, Matthias, in: Frankfurter Allgemeine Zeitung, 24.07.2013, S. 25/27.
Morozov, Evgeny	Die Welt ist nicht genug. Übersetzt aus dem Englischen von: Graff, Bernd, in: Süddeutsche Zeitung, 20.01.2014, S. 9.
Müller-Jung, Joachim	Wird „Big Data“ zur Chiffre für den digitalen GAU?, in: Frankfurter Allgemeine Zeitung, 06.03.2013, S. N1-N2.
Nestler, Franz	Von Blumen und Bitcoins, in: Frankfurter Allgemeine Zeitung, 20.11.2013, S. 16.
Nonnenmacher, Günther	Gauck mahnt, in: Frankfurter Allgemeine Zeitung, 27.07.2013, S. 1
Oerting, Troels	Das Europäische Cybercrime Centre (EC3) bei Europol, in: Kriminalistik, Heft 12/2012, S. 705-706.
Paul, Werner	Die Computerkriminalität in der Statistik, in: Neue Juristische Woche-Computerreport, Heft 1/1995, S. 42-45.
Poerting, Peter	Umfang und Struktur der Computerkriminalität, in: Kriminalistik, Heft 2/1986, S. 595-615.
Robertz, Frank J.	Herausforderung Cybercrime, in: Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei, Heft 9/2011, S. 28-33.
Rüdiger, Thomas-Gabriel / Denef, Sebastian	Soziale Medien – Muss sich die Polizei neu ausrichten?, in: Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei, Heft 11/2013, S. 4-11.
Schindhelm, Michael	Kultur zum Selbermachen, in: Süddeutsche Zeitung, 10./11.11.2012, S. 2.
Schirrmacher, Frank	Wir wollen nicht, in: Frankfurter Allgemeine Sonntagszeitung, 25.08.2013, S. 37.
Seidl, Alexander	Online-Abzocke und Datenklau – Die digitale Alltagskriminalität, in: Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei, Heft 7/2013, S. 4-9.
Seidl, Alexander / Fuchs, Katharina	Die Strafbarkeit des Phishings nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes, in: Online-Zeitschrift für Höchstrichterliche Rechtsprechung, Heft 2/2010, S. 85-92.
Sensburg, Patrick Ernst	Verkehrsdatensicherung. Ein neuer Vorschlag von CDU/CSU, in: Kriminalistik, Heft 6/2013, S. 393-395.
Sieben, Günther / von zur Mühlen, Rainer A.H.	Zur Diskussion: Computerkriminalität. Computerkriminalität – Viel Lärm um nichts?, in: Datenverarbeitung-Steuern-Wirtschaft-Recht-Zeitschrift, Heft 23/1973, S. 252-254.
Sieber, Ulrich	Computerkriminalität und Informationsstrafrecht. Entwicklungen der internationalen Informations- und Risikogesellschaft, in: Computer und Recht, Heft 2/1995, S. 100-113.
Siemons, Mark	Amerika und China im Cyberkrieg, in: Frankfurter Allgemeine Zeitung, 26.11.2013, S. 27.

Singelnstein, Tobias	Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in: Neue Zeitschrift für Strafrecht, Heft 11/2012, S. 593-606.
Straub, Ursula / Witt, Rainer	Polizeiliche Vorkenntnisse von Vergewaltigern, in: Kriminalistik 1/2003, S. 19-30.
Süddeutsche Zeitung	Wechselstube der Unterwelt, 31.05.2013, S. 18.
Süss, Sonja	Magst Du Sex haben, in: Frankfurter Allgemeine Sonntagszeitung, 24.03.2013, S. 2.
Voit, Bernhard	Wirksamer Schutz kritischer Infrastrukturen durch Koordination und Kommunikation aller Systeme, in: S+S report, Nr. 2 6/2013, S. 54-59.
Weber, Roman	Phishing: Brauchen wir einen Sondertatbestand zur Verfolgung des Internetphishings?, in: Online-Zeitschrift für Höchstrichterliche Rechtsprechung, Heft 12/2004, S. 406-410.
Wiedemann, Carolin	Leistet endlich Widerstand, in: Frankfurter Allgemeine Sonntagszeitung, 21.07.2013, S. 37.
Wiedemann, Peter	Tatwerkzeug Internet, in: Kriminalistik, Heft 4/2000, S. 229-239.
Wilde, Sebastian	Ich brauche jemanden, in: Frankfurter Allgemeine Zeitung, 13.09.2013, S. 39.
Ziercke, Jörg	Polizei in der digitalen Welt. Referat anlässlich der BKA-Herbsttagung vom 20.-22. November 2007, in: Kriminalistik, Heft 2/2008, S. 76-81.

7.4 Internet- und sonstige Quellen

Best, Benjamin / Schwering, Uwe / Delpierre, Hevré Martin	Die Story im Ersten: Im Griff der Zockermafia, 14.10.2013, 23:30 Uhr, verfügbar unter: http://www.daserste.de/information/reportage-dokumentation/dokus/sendung/ndr/14102013-die-story-im-ersten-im-griff-der-zockermafia100.html, abgerufen am: 04.01.2014.
BKA (Hrsg.)	Bericht der AG Projektgruppe Internet, Aktenzeichen OA 34-2, Wiesbaden 25.02.1997 (nicht veröffentlicht).
Bott, Klaus	Normalität des Verbrechens, in: KrimLex-Online, verfügbar unter: http://www.krimlex.de/artikel.php?BUCHSTABE=&KL_ID=126, abgerufen am: 26.01.2014.
Bundeskriminalamt (Hrsg.)	Zentralstelle für anlassunabhängige Recherchen in Datennetzen, verfügbar unter: http://www.bka.de/nn_206376/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard__node.html?__nnn=true, abgerufen am: 29.12.2013.

De Maizière, Thomas	Rede des Bundesinnenministers im Bundestag v. 30.01.2014 (gesprochenes Wort), verfügbar unter: http://www.bmi.bund.de/SharedDocs/Reden/DE/2014/01/rede-min-bt.html?nn=3314802, abgerufen am: 31.01.2014.
Die Welt-Online	Jeden Tag eine Million Opfer von Cybercrime, 19.02.2013, verfügbar unter: http://www.welt.de/politik/deutschland/article113747004/Jeden-Tag-eine-Million-Opfer-von-Cybercrime.html, abgerufen am: 04.01.2013.
Ester, Marc-Aurél / Benzmüller, Ralf	GData Software AG. Whitepaper 2009. Underground Economy, Bochum 2009.
Europäische Union (Hrsg.)	Vertrag über eine Verfassung für Europa, Brüssel 06.08.2004 (29.10.2004).
Gispert, Laura	Die Debatte rund um das Urheberrecht, in: FAZ-Online, verfügbar unter: www.faz.net/aktuell/feuilleton/debatten/urheberrecht/urheberrecht-chronik-der-aktuellen-debatte-11761139.html, abgerufen am: 04.01.2014.
Heise-Online	CIA berichtet von Cyber-Angriffen auf Energieversorger, in: Heise-Online. Newsticker, 19.01.2008, 11:57 Uhr, verfügbar unter: http://www.heise.de/newsticker/meldung/CIA-berichtet-von-Cyber-Angriffen-auf-Energieversorger-180390.html, abgerufen am: 03.01.2014.
Industrie- und Handelskammer Schleswig-Holstein / Landeskriminalamt Schleswig-Holstein (Hrsg.)	Hohe Dunkelziffer und großer Informationsbedarf, Schleswig-Holstein 2008. (Studie wurde von der IHK Schleswig-Holstein übersandt liegt als pdf-Datei vor).
Karliczek, Kali-Maria	Perseveranz, in: KrimLex-Online, verfügbar unter: http://www.krimlex.de/artikel.php?BUCHSTABE=P&KL_ID=134, abgerufen am: 04.01.2014.
Landwehr, Andreas Christopher	Viktimisierung, in: KrimLex-Online, verfügbar unter: http://www.krimlex.de/artikel.php?BUCHSTABE=V&KL_ID=202, abgerufen am: 04.01.2014.
Ministerium für Inneres und Kommunales des Landes Nordrhein Westfalen (Hrsg.)	Bekämpfung der Kriminalität unter Ausnutzung von Informations- und Kommunikationstechnik durch die Polizei des Landes Nordrhein-Westfalen (Bekämpfung der IuK-Kriminalität), RdErl. des MIK NRW vom 29.02.2012, 423-62.18.09.
Stalinski, Sandra	Entscheidung im Bundestag. Internet-Ausschuss kommt vorerst nicht, in: tagesschau.de, 19.12.2013, 15:17 Uhr, verfügbar unter: http://www.tagesschau.de/inland/internetausschuss102.html, abgerufen am: 27.01.2014.

Stern-Online	Sicherheitslücken bei mTAN-Verfahren. So leicht plündern Hacker fremde Bankkonten, 21.11.2013, 14:40 Uhr, verfügbar unter: http://www.stern.de/tv/sterntv/sicherheitsluecken-bei-mtan-verfahren-so-leicht-pluendern-hacker-fremde-bankkonten-2069062.html, abgerufen am: 05.01.2014.
Trepte, Sabine / Reinecke, Leonard	Sozialisation im Social Web: Eine Forschungsagenda zu den Wirkungen des Web 2.0, im Rahmen eines DFG-Forschungsprojekts der Universität Hamburg.
Zahn, Markus	Kommentar zur Bestandsdatenauskunft v. 03.05.2013, 18:07 Uhr, verfügbar unter: http://www.tagesschau.de/inland/bundesrat358.html, abgerufen am: 03.01.2014.
Ziercke, Jörg	Cybercrime – Bedrohung, Intervention, Abwehr. BKA Herbsttagung vom 12-13. November 2013, Begrüßungsrede (gesprochenes Wort), verfügbar unter: http://www.bka.de/nn_243818/DE/Publikationen/Herbsttagungen/2013/Redebeitraege/herbsttagung2013Redebeitraege_node.html?__nnn=true, abgerufen am: 05.01.2014.

Stand der wissenschaftlichen Literatur:	ca. August 2013
Stand der medialen Berichterstattung:	ca. 31. Januar 2014
Letztes Datum der Quellenauswertung:	05. Februar 2014

Ehrenwörtliche Erklärung

Durch meine Unterschrift versichere ich, dass ich die vorstehende Masterarbeit selbstständig und ohne fremde Hilfe verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel verwendet und Zitate als solche kenntlich gemacht habe. Die Arbeit war in dieser oder ähnlicher Form noch nicht Bestandteil einer Prüfungsleistung.

Wuppertal, den 09.02.2014 Torben Huckenbeck