Bundeskriminalamt

COD - LITERATUR - REIHE

BAND 15

Informations- und Kommunikationskriminalität

Eine Literaturauswahl

BKA

COD - LITERATUR - REIHE
BAND 15

Informations- und Kommunikationskriminalität

Eine Literaturauswahl anlässlich der Herbsttagung 2003

Inhalt

Begleitwort

Mit dem vorliegenden Band wird erneut eine Literaturauswahl zur Herbsttagung des BKA präsentiert. Dabei wird auf den Fundus des Computergestützten Dokumentationssystems für Literatur (COD-Literatur) zurückgegriffen, für den momentan 130 Zeitschriften und Buchreihen mit polizeirelevanten Schwerpunkten ausgewertet werden.
Ziel ist es, zum diesjährigen Tagungsthema „Informations- und Kommunikationskriminalität“ Literaturnachweise zu den einzelnen Programmpunkten anzuführen, die sowohl als Zusatzinformation als auch für eine weitergehende Beschäftigung mit dem Thema dienen können. Bei der Auswahl wurde in erster Linie auf Informationsgehalt, Aktualität und Umfang des Beitrags sowie auf die Anzahl von weiterführenden Literaturhinweisen und Quellen geachtet.
Bei der Sichtung des gesammelten Materials bildeten sich fünf Themenkomplexe heraus, bestehend aus: Den speziellen Erscheinungsformen der IuK-Kriminalität, die sich hieraus ergebenen kriminalistischen Aspekte, das nationale und internationale Recht und Allgemeines zum Datenschutz und E-Commerce.
Da sich einige der ausgewählten Beiträge mit mehreren Gesichtspunkten der IuK-Kriminalität befassen und somit eine eindeutige thematische Abgrenzung zwischen den Beiträgen nicht immer möglich gewesen ist, wurden bei der Zuordnung Prioritäten gesetzt. So können in einem Beitrag, der unter kriminalistische Aspekte eingeordnet ist, auch rechtliche Fragen behandelt werden.
Das Abkürzungsverzeichnis im Anhang dient zur Erläuterung der Beschreibungselemente eines Dokuments. Das Verzeichnis der Fundstellen beinhaltet alle *hier* aufgeführten Zeitschriften und Buchreihen mit ihren vollständigen Titeln. Eventuelle Signaturangaben beziehen sich auf die Kennzeichnung der BKA-Bibliothek.

Arnim Wallrabe
KI 31-Literaturdokumentation

Wiesbaden, November 2003

Erscheinungsformen

IDN: 20030918

TYP: AUF

SGB: KO; KK

AUT: Mörbel, Richard; Kind, Holger

TIT: Kinderpornografie und das Internet

FST: DNP

JAH: 2003

JGG: 53

HES: 2, S. 11, 13-16

BEI: 6 TAF

FD: Kinderpornografie; Anzeigeerstattung; Zentralstelle für anlassunabhängige Recherchen in Datennetzen; Zentrale Auswertestelle für kinderpornografische Medien ; Internet; Sexueller Missbrauch von Kindern; Statistische Angaben

TEXT: Seit Mitte der 90er Jahre nehmen die Fälle des Besitzes und der Verbreitung kinderpornografischer Darstellungen und des sexuellen Missbrauchs von Kindern unter Verwendung des Internet rasant zu. Wegen der im Internet zunehmend auch ungewollten Konfrontation mit Kinderpornografie erstattet eine Vielzahl von Privatpersonen Anzeige. Die elektronische Anzeige wird nur noch selten bei der örtlich zuständigen Dienststelle erstattet. Die daraus sowie aus Mehrfachanzeigen und nationaler sowie internationaler Doppelarbeit erwachsende erhebliche Diskrepanz zwischen der tatsächlichen Arbeitsbelastung und den statistisch erfassten Fällen lässt sich durch einen Vergleich der PKS-Zahlen mit der Anzahl der alleine in der "Zentralen Auswertestelle für kinderpornografische Schriften" (BKA, OA 37) bearbeiteten Vorgänge erahnen. Kinderpornografische Filme mit europäischen Opfern entstanden fast ausschließlich in einer über längere Zeit bestehenden Abhängigkeitssituation. Der sexuelle Missbrauch im Zusammenhang mit Kinderpornografie wird fast ausschließlich durch Aufdeckung der Tat durch die Polizei beendet. Sowohl bei sexuellem Missbrauch von Kindern, als auch bei Kinderpornografie muss von einem großen Dunkelfeld ausgegangen werden. Seit 1998 wird die "Datei Kinderpornografie" als Verbunddatei betrieben, auf deren Gesamtbestand von derzeit rund 80.000 Daten alle LKÄ zugreifen können. Mit IMK-Beschluss wurde im BKA die "Zentralstelle für anlassunabhängige Recherchen im Datennetz ZaRD" eingerichtet, die 1999 den Wirkbetrieb aufnahm. Seit 2002 ist sie Bestandteil des "Technischen Servicezentrums für Informations- und Kommunikationstechnik" (TeSIT, Fachbereich KI 26 des BKA). Die Arbeit der ZaRD signalisiert, dass eine wirksame Strafverfolgung durch die Polizei auch im Internet gewährleistet ist und sorgt für einen Präventiv-Effekt.

IDN:20020528

TYP:AUF

SGB:DV; KK

AUT:Hetzer, Wolfgang

TIT:Elektronische Geldwäsche?; Internet - Tatort und Tatwerkzeug

FST:Kriminalistik

JAH:2002

JGG:56

HES:2, S. 123-126

BEI:9 QU

FD:Computerkriminalität; Geldwäsche; Internet; Tatort; Tatwerkzeug

TEXT:Die elektronische Datenverarbeitung hat dazu geführt, dass Information und Kommunikation zumindest in Teilbereichen mit fast explosionsartiger Geschwindigkeit verläuft. Im Jahr 2000 hat sich alleine in Deutschland die Zahl der Personen, die das Internet benutzen, um mehr als zehn Millionen vergrößert. Fast das gesamte Wirtschaftswesen ist online gegangen. Bei halbwegs realistischer Betrachtung dürfte es kaum jemanden überraschen, dass die Computerkriminalität einen zunehmend wichtiger werdenden Bereich des Kriminalitätsgeschehens beschreibt. Der Aufwuchs des elektronischen Handels erfordert die Einrichtung entsprechender Zahlungswege und -techniken. Darin steckt ein ungeheuer kriminogenes Potential. Das gilt insbesondere im Hinblick auf die Geldwäsche. Transaktionen, die über das Internet abgewickelt werden, sind nur auf den ersten Blick frei von speziellen Geldwäscherisiken.
Der in der vorliegenden Veröffentlichung nur sehr grob beschriebene Hintergrund lässt immerhin erahnen, dass z.B. auch Glücksspiele im Internet fast ideale Möglichkeiten bieten, um mit Hilfe von Verschleierungen Geldwäsche zu betreiben. Mittlerweile ist beweiskräftig festgestellt, dass Teile der elektronischen Glückspielindustrie von kriminellen Personen und Organisationen benutzt werden.

IDN:20020810

TYP:AUF

SGB:SW; DV; KO

AUT:Schlomann, Friedrich Wilhelm

TIT:Information Warfare

FST:CD Sicherheits-Management

JAH:2002

JGG:26

HES:2, S. 10-12, 14-15, 18-22, 24-26, 28

BEI:3 BILD

FD:Computersabotage; Computermanipulation; Computerstrafrecht; Computerspionage; IT-Sicherheit; Computerkriminalität; Computervirus; Hacker; Internet; Terrorismus; Risikofaktor; Informationsgesellschaft; Volkswirtschaft; Schadensrisiko

TEXT:Ohne elektronische Datenverarbeitung und Kommunikationstechnologie kann ein modernes Unternehmen, keine wichtige Regierungsbehörde und keine entscheidende Militäreinheit heutzutage existieren. Der Begriff "Kritische Infrastruktur" stellt dabei den Lebensnerv eines Landes dar. Unter ihm sind Einrichtungen wie Energieversorgungen, Luftfahrtsunternehmen oder auch Kommunikationstechniken zu verstehen, bei dessen Ausfall durch Angriffe via Internet immense Schäden entstehen können. Dabei ist es durch gezielte Angriffe möglich, das gesellschaftliche Leben eines ganzen Landes lahm zu legen. Für Terroristen bietet das Internet eine perfekte Plattform. Die Bewegungsfreiheit im Netz ist heutzutage unbegrenzt und zudem ist es sehr schwierig, einen User ausfindig zu machen und zu identifizieren. Beispiele für die Aktivitäten verschiedener Hacker sowie gezielte Angriffe von Organisationen gibt es bisher viele. Vor drei Jahren gelang es einer Hackergruppe, einen britischen Aufklärungssatelliten für mehrere Stunden unter ihre Kontrolle zu bringen. Im Kosovo-Konflikt wurde am Beginn der Nato-Luftanschläge auf Serbien der Nato-Internet-Rechner wiederholt attackiert und über Stunden lahm gelegt. Eine weitere Möglichkeit des Internet-Eingriffes ist das Schüren von Konflikten durch gezielte elektronische Attacken wie beim Nordirland-Konflikt. IRA-Helfer veröffentlichten sensible Daten über Militärbasen der britischen Armee.
Planspiele eines simulierten Ernstfalls durch Attacken via Internet in der BRD und in den USA dokumentieren deutlich die mangelhafte Zusammenarbeit aller verantwortlichen Stellen. Der Schutz vor solchen Aktivitäten steht weltweit erst am Anfang. Das wichtigste ist daher, Menschen am Computer zu sensibilisieren und über die Gefahren zu informieren.

IDN: 20020832

TYP: AUF

SGB: KP; PT

AUT: Funk, Albrecht

TIT: Cybercrime; Die Zukunft elektronischer Überwachung

FST: Bürgerrechte & Polizei

JAH: 2002

HES: 71, Nr. 1, S. 6-15

BEI: 18 QU

FD: Internet; Kryptographie; Überwachungsmaßnahme; Datenschutz; Telekommunikationsüberwachung; TKG; TKÜV; Personendaten

TEXT: Bereits Anfang der 90er Jahre haben Sicherheitsbehörden den Missbrauch des Internets durch Kriminelle und die Frage, wie im Cyberspace für Recht und Ordnung gesorgt werden kann, zum Gegenstand von Forderungen nach erweiterten Zuständigkeiten und Eingriffsbefugnissen gemacht. Die Strafverfolgung drohe an den technischen und rechtlichen Hürden der notwendigen elektronischen Überwachung zu scheitern. Der Kontrollverlust von Polizei und Justiz ist auch beherrschendes Thema vieler nationaler und internationaler Expertengremien. Der Ruf nach Kriminalisierung lässt sich jedoch nicht von der Frage trennen, wie der neu geschaffene Raum politisch gestaltet und gebraucht werden soll. Bereits heute kann der gesamte Datenverkehr einer Person durch legale, staatlich genutzte Trojan Horse-Programme technisch überwacht werden. Bei der rechtlichen Ausgestaltung von Eingriffsmaßnahmen muss künftig aus datenschutzrechtlichen Gründen insbesondere auf die strikte Begrenzung staatlicher Eingriffe in die Rechte der Bürger geachtet werden. Der Gesetzgeber bemüht sich derzeit durch drei Maßnahmenbündel die Datenströme digitaler Kommunikation zugänglich zu machen. Dies sind eine abhörfreundliche Architektur, gesetzgeberische Maßnahmen für den Zugriff auf die Daten und das Vorrätighalten durch die privaten Betreiber. Ein besonderes Augenmerk bei der Weiterentwicklung des Cyberspace wird jedoch auf den Bereich der Kryptografie gelegt. Hier wollen die Sicherheitsbehörden möglichst die Herrschaft über die Schlüssel innehaben.

IDN:20011083

TYP:AUF

SGB:DV; SW; KK

AUT:Stenger, Hans Jürgen

TIT:Lies auch im Internet das Kleingedruckte!; Ein Überblick über die neuesten kriminellen Finessen im digitalen Zeitalter

FST:CD Sicherheits-Management

JAH:2001

JGG:25

HES:2, S. 66-68, 70-72, 74

BEI:1 TAB, 1 BILD, 1 TAF

FD:Computersabotage; Internet; PKS; Computervirus; Softwarepiraterie; Schadenshöhe; Datensicherheit

TEXT:Auch wenn Computerviren in der aktuellen Kriminalistik noch keine Berücksichtigung finden, spielen sie doch in der heutigen Kriminalitätswelt eine bedeutende Rolle, vor allen Dingen im Hinblick auf die Schäden, die sie anrichten.
Es muss davon ausgegangen werden, dass jeder zweite Rechner, der über ein öffentliches Netz erreichbar ist, im Laufe eines Jahres böswilligen Attacken ausgesetzt ist. Allerdings ist nicht jede Attacke strafrechtlich relevant. In mehreren tausend Fällen werden allerdings Daten verändert und unerlaubt Zugriffsrechte erlangt. Die PKS beeindruckt mit einer Steigerung der Fallzahlen von 168,5 % in den Fällen der Software-Piraterie im privaten bzw. häuslichen Umfeld und von 333,2 % in Fällen des Missbrauchs im gewerblichen Umfeld. In immer kürzeren Abständen hört man von der Software-Industrie über die wirtschaftlichen Schäden durch Software-Piraterie. Schlecht entwickelt oder gar nicht vorhanden ist das Unrechtsbewusstsein über das Wirtschaftsgut Software. So lange z.B. Lehrer im Leistungskurs Informatik bedenkenlos Raubkopien an die Schüler verteilen, wird sich daran auch nichts ändern. Hier gehören die Ausbildungsinhalte für Lehrer und Schüler um die Raubkopie-Problematik erweitert. Straftaten im Internet werden in der PKS als Straftaten der Computerkriminalität, des Betruges, der Beleidigung oder auch der Hehlerei gezählt. Der wahre Umfang der Internet-Kriminalität ist daher aus der Statistik nicht genau erkennbar, dabei zeigt die tägliche Praxis, dass Straftäter in hohem Maße das Internet wie auch andere Kommunikationsmittel nutzen.

IDN:20012083

TYP:AUF

SGB:KK; KO

AUT:Fritsche, Klaus Dieter

TIT:Wirtschaftsspionage; Schutz der deutschen Wirtschaft vor Ausspähung und Know-how-Abfluss

FST:Kriminalistik

JAH:2001

JGG:55

HES:7, S. 472-476

FD:Betriebsspionage; Wirtschaftsunternehmen; Spionage; Wirtschaftsschaden; Schadenhöhe; Zusammenarbeit; Strafverfolgungsbehörde; Sicherheitsbehörde; Privatwirtschaft; Verfassungsschutz; Industriespionage; Dunkelfeld; Gefahrenabwehr; Informationsschutz; Datenschutz

TEXT:Wirtschaftsspionage hat Interesse an allen Informationen (in bestimmten Bereichen auch an Produkten). Es werden alle Gelegenheiten zur Kontaktaufnahme genutzt - dies gilt auch für Geschäftsreisen nach Russland und in andere GUS-Republiken. Auch dort hat der Überwachungs- und Abschöpfungsapparat mittlerweile wieder seine vormalige Präsenz und Effektivität erreicht. Wir erkennen eine Zunahme der Methode der "offenen Beschaffung" - Hierzu zählen Kontaktgespräche, Geschäftsbesuche, Vertragsabschlüsse, Abfragen im Internet und Auswertung von Veröffentlichungen jeder Art. Jedes Unternehmen muss aus diesen Fakten den Schluss für sich ziehen, sein spezielles Know-how kritisch dahingehend zu überprüfen, inwieweit es Gefahren der Ausspähung ausgesetzt sein kann. Diese Analyse muss in ein Informationsschutzkonzept münden, das unternehmensweit akzeptiert und konsequent umgesetzt wird.

IDN:20012362

TYP:AUF

SGB:DV; SW

AUT:Meinel, Carolyn

TIT:Sabotage im Internet

FST:Spektrum der Wissenschaft

JAH:2001

HES:12, S. 56-61, 63

BEI:3 BILD, 3 TAF

FD:Internet; Hacker; Computervirus; Virusprogramm; Datensicherheit

TEXT:Der Beitrag beschreibt eine Krankheit, die das World Wide Web heimsuchte. Eine solche Web-Krankheit trat im Jahr 2001 auf und löste höchste Besorgnis über die Widerstandsfähigkeit des Internets aus. Anlass war die Attacke des Web-Wurms "Code-Red", der mehrere hunderttausend Internet Information Server (IIS) der Fa. Microsoft innerhalb weniger Stunden infizierte und spürbar zur Verlangsamung des Internets führte. Das Stopfen von Sicherheitslücken sowie die Reparatur des angerichteten Schadens kostete mehrere Milliarden Dollar. Am bedrückendsten ist jedoch die Vorstellung einiger Forscher, dass "Code-Red" nur ein Vorläufer noch aggressiverer Internet-Seuchen sein könnte, die das gesamte Internet lähmen oder gar ganz zerstören würden.
Der Autor schildert weitere durchgeführte Angriffe auf das World Wide Web, die Gefahren, die von solchen Attacken ausgehen und die Bemühungen der mit der Sicherheit des Internet verantwortlichen Institutionen.

IDN:20001403

TYP:AUF

SGB:DV; SW

AUT:Geiger, Gebhard

TIT:"Information Warfare"; Bedrohung und Schutz IT-abhängiger gesellschaftlicher Infrastrukturen

FST:DuD

JAH:2000

JGG:24

HES:3, S. 129-136

BEI:31 QU

FD:Information Warfare; Cyberwar; Informationstechnik [Infrastruktur]; Computersabotage; IT-Sicherheit; Sicherheitsmängel; Bedrohungspotential; Bedrohungsanalyse; Sicherheitspolitik; Militär; Informationsgesellschaft

TEXT:Die Infrastrukturen der Hochtechnologieländer sind durch Computerspionage und -sabotage verwundbar. Elektronische Angriffe und (Zer-) Störungsakte mit politischer oder krimineller Motivation können über die globalen öffentlichen Informationsnetze erfolgen. Gefährdet sind praktisch alle informationsabhängigen Funktionsbereiche von Politik, Verwaltung, Wirtschaft, öffentlicher Güterversorgung und Verkehr. Neben dem "klassischen" Schutzbedarf (Datenschutz, Vertraulichkeit und Sicherheit der Telekommunikation) wird daher die Sicherheit nationaler und internationaler Informationsinfrastrukturen nach Überzeugung des Autors zu einer vordringlichen politischen Aufgabe.

IDN:20002515

TYP:VOR

SGB:KO; KK

AUT:Paulus, Manfred

TIT:Pädo-Kriminelle im Datennetz; Eine Herausforderung (nicht nur) für Polizei und Justiz; Vortrag, gehalten am 12.11.1999 vor der Kriminalistischen Studiengemeinschaft e.V. Bremen

FST:Kriminalistik

JAH:2000

JGG:54

HES:6, S. 390-394

FD:Kinderpornographie; Sexueller Missbrauch von Kindern; Kind; Pädophilie; Internet; Erscheinungsform; Beweisführung; Ermittlungsarbeit; Provider; Datennetz [Kriminalität]; Strafverfolgung

TEXT:Die sexuell motivierte Kriminalität an Kindern wurde durch alle bisher getroffenen Maßnahmen nicht zurückgedrängt und nicht wirksam bekämpft. Vielmehr besteht der begründete Verdacht, dass sie zunimmt. So ist sexuelle Gewalt gegen Kinder eine der wichtigsten kriminalistischen, aber auch gesellschaftlichen Herausforderungen unserer Zeit. Die Deliktsbereiche "Sexuelle Gewalt gegen Kinder" und "Kinderpornografie" sind gekennzeichnet von zutiefst gesellschaftlichen Problemen, die nur gesamtgesellschaftlich abbaubar oder gar lösbar sind. Das Bundeskriminalamt in Wiesbaden betreibt seit 1998 die "Zentralstelle Kinderpornografie", unter anderem mit dem Ziel, pädophile (Tarn-)Organisationen, sowie deren Tausch- und Handelswege zu erkennen, kinderpornografisches Material zusammenzuführen, Täter und Opfer zu identifizieren. Gesetzgebung, Polizei und Justiz müssen ihren Beitrag zur Verbesserung der Situation im Bereich sexueller Gewalt gegen Kinder (weiterhin) leisten. Sie haben Vorsorge dafür zu treffen, dass die modernen Informations- und Kommunikationstechniken zum Nutzen und nicht zum Schaden der heutigen und der kommenden Generation Verwendung finden können.

IDN:20001162

TYP:AUF

SGB:SW

AUT:Hunnius, Gerhard

TIT:Hacker und Viren: Die Welt in der Internet-Falle?

FST:KES

JAH:2000

JGG:16

HES:3, S. 22-32; 4, S. 22-25

BEI:38 TAF

FD: Sicherheitsmaßnahme; Internet; Informationstechnik; Unternehmenssicherheit; Hacker; Zugriffsschutz; Computervirus; Risikoanalyse; Gefahrenpotential; Informationssicherheit

TEXT: Zum neunten Mal seit 1985 haben der SecuMedia Verlag und die Fachzeitschrift KES die Befragung zur Sicherheit in der Informationstechnik durchgeführt. 176 Unternehmen haben sich an der Studie beteiligt.
Die Ergebnisse der KES-Utimaco-Sicherheitsstudie zeigen: Eine Virenkatastrophe, wie sie durch "I LOVE YOU" und seine Nachfolger verursacht wurde, war vorhersehbar. Schon 1999 schlichen sich Viren in 45% der Fälle per E-Mail in Unternehmen ein. Prominentestes Beispiel war der Word-Makrovirus "Melissa". Obwohl Makroviren bereits damals die Hauptinfektionsquelle darstellten, hatte ein Großteil der Anwender keinen Verdacht geschöpft - mit I LOVE YOU hat sich die Geschichte nun wiederholt.
Der Autor beschäftigt sich zunächst mit der Risikosituation in den Unternehmen:
Unverändert gelten Irrtum und Nachlässigkeit der Mitarbeiter als das bedrohlichste Risiko für die IT-Sicherheit in den Unternehmen. An zweiter Stelle folgen die Software-Anomalien und Informations- Diebstahl/Spionage und zwar mit steigender Tendenz. An dritter Stelle folgen hardwarebedingte Defekte.
Über die Hälfte der Unternehmen hat eine schriftlich fixierte Strategie für Informationsverarbeitung und 42% haben eine schriftlich fixierte Strategie für IT-Sicherheit.
Die Maßnahmen der Unternehmen zur Verbesserung der IT-Sicherheit werden vorgestellt und abschließend ihre Planungen für die Zukunft vorgestellt.
Hauptpunkte der zukünftigen IT-Sicherheit sind:

- Verschlüsselung
- Authentisierung
- Kryptographische Verfahren
- Infrastrukturorientierte Maßnahmen
- Vorsorge für längere Ausfälle
- Notfall-Dokumentation
- Überspannungsschutz
- Zugriffsschutz durch Zugangs- und Zugriffsrechtregelungen.

IDN:20002703

TYP:AUF

SGB:SW; DV

AUT:Wittmann, Jürgen

TIT:Die Wege der Hacker in die Firmenrechner; Computerkriminalität aus dem Netz

FST:WIK

JAH:1999

JGG:20

HES:5, S. 69-72

BEI:14 QU

FD:Netzwerk; Computerkriminalität; Internet; Hacker; Datenspionage; Computervirus; Gefahrenpotential; Risikoanalyse; Sicherheitsmaßnahme

TEXT:Offene Netze lassen im Grundsatz einen Zugriff durch jedermann in eine dokumentierte Struktur der Netze und auf alle angeschlossenen Rechner und deren Daten zu. Insbesondere diese Möglichkeit des Internet wird für kriminelle Machenschaften genutzt. Hierzu zählen u.a. Betrug, Erpressung, Angriff auf Leben und Gesundheit durch Manipulation sicherheitsrelevanter Systeme, Diebstahl geistigen Eigentums, Pornographie, Computerviren sowie politischer Extremismus. Mit der Freigabe der Daten für andere Benutzer sind diese Missbrauchsgefahren auch in geschlossenen Netzen gegeben. Hier treten häufig zusätzliche Computerkriminalitätsformen wie Betriebsspionage, Sabotage oder Datenveränderung mit falschen User-Zugriffen auf. Dieser Beitrag behandelt Vorsichtsmaßnahmen im Internet, Angriffe mit "trojanischen Pferden", Computerviren, Informationssammlung im Internet, Ausspähen von Systemen, "Spuren" im Netz und Datenübertragungsprotokolle.

IDN:20000600

TYP:AUF

SGB:KO; DV

AUT:Bernhardt, Ute; Ruhmann, Ingo

TIT:Information Warfare als neue Bedrohung der Grundrechte

FST:DANA

JAH:1999

JGG:21

HES:4, S. 11-17

BEI:1 TAF, 26 QU

FD:Information Warfare; Informationssystem; Kommunikationssystem; Informationstechnik; Computerkriminalität; Computersabotage; Datenmanipulation; Chiffrierung; IT-Sicherheit; ; Internet; Hacker; Kryptographie

TEXT:Bei Information Warfare geht es um die systematische Nutzbarkeit von Daten und Informationen im Konfliktfall. Darin zusammengefasst sind die beiden Aktivitäten Netwar und Cyberwar. Netwar bedeutet, das Wissen der Bevölkerung eines Konfliktgegners und ihr Selbstbild zu stören und zu modifizieren. Cyberwar bedeutet die Durchführung und Vorbereitung militärischer Operationen nach informationsbezogenen Prinzipien; er bedeutet die Störung und Zerstörung von Informations- und Kommunikationssystemen eines Gegners, sowie Täuschung über die eigene Lage und Stärke. Informationstechnik wird als Kriegswaffe benutzt. Unter Cyberterrorismus werden Information-Warfare-Aktivitäten durch einzelne oder kleine Gruppen verstanden. Cyberterrorismus stellt sich als Bedrohungsszenario dar, das im Kontext mit Information Warfare entsprechenden Aktivitäten zusätzliche Glaubwürdigkeit verleiht. In Bezug auf den Cyberterrorismus beschreiben die Autoren die vorhandenen Ansätze in der Bundesrepublik Deutschland und die Bekämpfung in den USA.

Kriminalistische Aspekte

IDN: 20030542

TYP: AUF

SGB: RE; DV

AUT: Klein, Florian; Kotulla, Arnt

TIT: Die Problematik der Spam-Emails in Verbindung mit der Bewerbung von Mehrwertdiensten (Dialern)

FST: Die Kriminalprävention

JAH: 2003

JGG: 7

HES: 1, S. 26-31

BEI: 23 QU

FD: Internet; Spam-E-mail; Computerbetrug; Computerkriminalität; Ermittlungsarbeit

TEXT: Durch sog. Spam-E-mails wird unerwünschte elektronische Werbung im Internet an einen sehr großen Adressatenkreis verteilt. Die Masse der dafür genutzten Email-Adressen wird durch Kniffe und Tricks aus dem Internet gewonnen bzw. von öffentlich zugänglichen Stellen, wie z.B. von www-Seiten aller Art, in Foren, Newsgroups oder Chatrooms erlangt. In vielen Spam-E-mails wird für Inhalte pornographischer oder illegaler Natur geworben, welche über Telefonmehrwertdienste kostenpflichtig zugänglich sind (190-er Nummern). Bislang galt es als schwierig, den sog. Spammern und Dialern (Inhaber der Mehrwertdienste) das Handwerk zu legen, da die Rückverfolgung im Netz aufgrund der Nutzung meist unsicherer ausländischer (asiatischer) Proxyserver sehr aufwändig wäre. Heute, bei zunehmender Befassung und Analyse dieser Kriminalitätsformen, sind die Spammer nur noch bis zu einem kleinen Grad anonym. Jetzt hat man die Möglichkeit, spätestens bei Einsetzen des Geldflusses die Verfolgung aufgrund des vorhandenen Datenmaterials und des Wissens der Internet-User erfolgreich anzusetzen.

IDN: 20030594

TYP: AUF

SGB: KK; RE

AUT: Soiné, Michael

TIT: Verdeckte Ermittler als Instrument zur Bekämpfung von Kinderpornographie im Internet

FST: NStZ

JAH: 2003

JGG: 23

HES: 5, S. 225-230

BEI: 76 QU

FD: Internet; Kinderpornographie; Verdeckter Ermittler; Ermittlungsarbeit; Polizeiarbeit; StGB P 34; StGB P 184; StPO P 110 a; StPO P 110 b; StPO P 110 c; StPO P 110 d; StPO P 110 e; Deliktart; Strafverfolgung; Ermittlungsverfahren

TEXT: Der Beitrag widmet sich den strafprozessualen Einsatzvoraussetzungen und Befugnissen von verdeckten Ermittlern bei der Verfolgung pädophiler Straftaten im Internet. In diesem Zusammenhang werden auch Möglichkeiten der Rechtfertigung von "einsatzbedingten Straftaten" im Netz der Netze erörtert. Die Bekämpfung von Kinderpornographie im Internet rechtfertigt den strafprozessualen Einsatz von verdeckten Ermittlern. Greift ein verdeckter Ermittler dabei in Einzelfällen in das Recht auf informationelle Selbstbestimmung von Tatverdächtigen ein und verwirklicht er damit einen Straftatbestand, kommt eine Rechtfertigung gemäß § 34 StGB in Betracht, sofern man diese Regelung hier für anwendbar hält. Da jedoch die Strafverfolgung langfristig nur dann wirklich effizient sein kann, wenn die staatlichen Eingriffsbefugnisse den Erfordernissen einer formalisierten Sozialkontrolle und Konfliktverarbeitung genügen, bedarf es einer klarstellenden und erweiterten Eingriffsbefugnis für verdeckte Ermittler, die dem vom Bundesverfassungsgericht aufgestellten Gebot der Normenklarheit entspricht.

IDN: 20030608

TYP: AUF

SGB: DV; KK

AUT: Becker, Christoph; Grunwald, Lukas; Hoffmann, Martin; Lessing, Günter; Steiner, Eugen

TIT: Wer suchet, der findet; Was bei der forensischen Analyse von IT-Systemen zu beachten ist

FST: KES

JAH: 2003

JGG: 19

HES: 1, S. 68-70, 72-77

BEI: 2 TAF

FD: Beweissicherung; Computerkriminalität; Informationstechnik; Forensik; Krisenmanagement; Organisationsstruktur

TEXT: Die Bedeutung der IT-Forensik in Krisenfällen liegt im Nachvollzug deliktischer Handlungen und dem Sicherstellen rechtsgültigen Beweismaterials. In der vorliegenden Veröffentlichung werden Maßnahmen genannt, die die Suche nach Beweismitteln vereinfachen. Nach dem Auffinden dieser Beweismittel müssen Ergebnisse in einem Bericht zusammengefasst werden, der juristisch einwandfrei formuliert ist, um in einem Prozess einen technisch nicht versierten Richter den vorliegenden Sachverhalt eindeutig widerzuspiegeln. Insofern ist die IT-Forensik keine Sache für Einzelkämpfer, sondern für ein Team, in das neben Techniker auch Manager, Revisoren, Juristen und eventuell Wirtschaftsprüfer gehören.

IDN: 20030933

TYP: AUF

SGB: KP; RE; DV

AUT: Dieterle, Peter; Schrötel, Uwe; Bux, Uwe

TIT: Information Warfare; Ein neues Aufgabenfeld für die Polizei?

FST: Kriminalistik

JAH: 2003

JGG: 57

HES: 6, S. 330, 332-349

BEI: 26 QU

FD: Computerkriminalität; BSI; Information Warfare; Informationstechnik; Internet; Kommunikationstechnik; Polizei; Spionage; USA; Wirtschaftsspionage; Gefahrenabwehrrecht; Europa; IT-Sicherheit; Risikoanalyse; Sicherheitspolitik; Rechtsgrundlage; Strafverfolgung; Internationale Zusammenarbeit

TEXT: Was passiert, wenn gänzlich unerwartet die IT-Systeme zusammenbrechen sollten? Wäre die Polizei auf einen umfassenden Cyber-Angriff vorbereitet, könnte sie mit solch einer Katastrophe umgehen und könnte sie ihre Aufgaben noch wahrnehmen? Nach Meinung der Fachleute, sollte sich die deutsche Polizei dieser Problematik dringend annehmen. Die hinsichtlich einer zivilen Komponente erweiterte Definition des Information Warfare umfasst den Einsatz informationstechnischer Mittel zur Störung, Lähmung oder Zerstörung der Informationsversorgung ziviler Ziele wie Organisationen, Unternehmen, Verwaltungen und Einzelpersonen. Denn wie fast alle technischen Errungenschaften birgt auch das Internet seine Gefahren. Daten beinhalten Informationen, die je nach Gehalt sehr begehrt sind. Die stets zunehmende Zahl von Informationssystemen und die immer engere Vernetzung dieser Systeme untereinander führen zu einer als hoch anzusetzenden Wahrscheinlichkeit von Zwischenfällen und Angriffen. Das Schadenspotential, das elektronische Angriffe auf Informationsinfrastrukturen haben, ist immens. Bedrohungen für diese Informationsinfrastrukturen sind international existent. Konsequenterweise muss auch die Bekämpfung international koordiniert erfolgen. Bei tatsächlich erfolgten Angriffen ist nach festgelegten Prioritäten vorzugehen. Kritische Infrastrukturen haben dabei Vorrang vor wirtschaftlichen Interessen. Aber auch im privaten Sektor müssen Rangfolgen akzeptiert werden. So ist z.B. die Behebung von Schäden in Netzen der Flugsicherung vordringlicher als die sofortige Wiederherstellung der Kommunikationsstruktur für Unternehmen. Für den Schutz der kritischen Infrastruktur ist ein Frühwarnsystem einzurichten.

IDN: 20030955

TYP: AUF

SGB: RE; KP

AUT: Kugelmann, Dieter

TIT: Bekämpfung rassistischer und fremdenfeindlicher Computerstraftaten; Das Zusatzprotokoll des Europarates

FST: DuD

JAH: 2003

JGG: 27

HES: 6, S. 345-347

BEI: 8 QU

FD: Computerkriminalität; Rassismus; Fremdenfeindlichkeit; Internet; Strafbarkeit; Europarat; Europa; Konvention; Strafverfolgung; Europäische Union; EDV-Einsatz; Kommunikation

TEXT: Im Jahre 2001 schuf der Europarat die Cyber-Crime-Konvention, die im Schwerpunkt die Zusammenarbeit der Vertragsstaaten zur Verfolgung von Computerstraftaten und zur Rechtsdurchsetzung zum Inhalt hat. Die Konvention gibt gewisse Straftatbestände vor, welche Computersysteme als Mittel der Begehung nutzen und die das innerstaatliche Recht enthalten soll. Das Hacking oder die Begehung von Betrug oder Fälschung mittels Computer sollen strafbar sein. Diese Strafbarkeit ist die Voraussetzung für eine Kooperation der Vertragsstaaten bei der Verfolgung derartiger Straftaten. Der Konvention sind inzwischen 35 Staaten beigetreten, darunter alle Mitgliedsstaaten der Europäischen Union außer Dänemark. Auch Japan, Kanada, Südafrika und die Vereinigten Staaten von Amerika haben als Nichtmitgliedsstaaten des Europarates die Konvention unterzeichnet. Armenien und Kroatien haben sie inzwischen für sich in Kraft gesetzt (Stand 5.2.2003). Die Cyber-Crime-Konvention klammert die Strafbarkeit bestimmter Inhalte der Kommunikation aus, bis auf die Ausnahme der Kinderpornographie.

IDN:20020301

TYP:AUF

SGB:DV; KK; RE

AUT:Bauer, Gerhard

TIT:Grenzenlose Kriminalität - machtlose Gesellschaft?; Das Internet - Forum einer globalen Informationsgesellschaft und Spielwiese für Kriminelle; Eine Nachlese zur Kooperationstagung "Kriminalität im Internet - Strategien zu ihrer Bekämpfung" der DBB Akademie und der DPolG

FST:Polizeispiegel

JAH:2002

JGG:37

HES:2, S. 41, 43, 45-48

BEI:31 QU

FD:Internet; Datenschutz; Ermittlungsmethode; Computerkriminalität; Informations- und Kommunikationstechnik; Präventivmaßnahme; Teledienstgesetz; Strafrecht

TEXT:Ihren Wissensdurst zu stillen ist der legitime Wunsch einer aufgeklärten Gesellschaft. Dieser Wissensdurst wird durch das Internet gelöscht. Die schier unermesslichen Quellen der Kreativität und Schaffenskraft der Menschen wird uns durch dieses Medium vor Augen geführt. Es gibt an diesen recht neuen Medium aber viele negative Seiten. Denn das besondere Merkmal des Internets, sich ohne persönlichen Kontakt global austauschen zu können, verringert Hemmschwellen von Menschen, über Sachverhalte zu reden, Neigungen preiszugeben oder Dinge zu tun, die sie in der realen Welt nie tun würden. Durch die Flucht in das neue und anonyme Medium Internet versuchen die Täter dem Verfolgungsdruck in der realen Welt zu entgehen. Unter Verschleierung der wahren Identität können Personen mit abnormer Veranlagung oder extremen Absichten problemlos Kontakt zu Gleichgesinnten suchen und aufnehmen, ohne befürchten zu müssen auf Ablehnung zu stoßen oder zur Verantwortung gezogen zu werden. Das Bundeskriminalamt registrierte im Jahr 2000 im Internet unter anderem 1.587 Fälle der Kinderpornografie, 94 Fälle der Tierpornografie und 387 Fälle politisch motivierter Kriminalität. Die Akzeptanz des Internet in Deutschland ist gegenwärtig noch stark vom Alter und Geschlecht des Benutzers geprägt. Dabei befinden sich die weiblichen Anwender in der Minderzahl. Kriminell ist das Verhalten von ca. 3 bis 5 % der Internetnutzer. Computerattacken sollen nach Möglichkeit schon im Ansatz unterbunden werden. Dazu hat der Bundesinnenminister die Task Force "Sicheres Internet" im Februar 2000 eingerichtet. Fest steht auch, dass das Strafprozessrecht vor dem Hintergrund der modernen Technik novellierungsbedürftig ist.

IDN: 20020835

TYP: AUF

SGB: RE; KK

AUT: Kant, Martina

TIT: Internet-Streifen; Recherchen ohne Verdacht im weltweiten Datennetz

FST: Bürgerrechte & Polizei

JAH: 2002

HES: 71, Nr. 1, S. 29-36

BEI: 19 QU

FD: Ermittlungsarbeit; Internet; Kinderpornographie; Staatsschutz; INTERMIT; BKAG P 2; BayPAG; Rechtsgrundlage; Bundeskriminalamt; Verfassungsschutz; Überwachungsmethode

TEXT: Bei Polizei- und Verfassungsschutzbehörden sind seit einigen Jahren Organisationseinheiten eingerichtet worden, die anlassunabhängig sog. "virtuelle Streifenfahrten" im Internet durchführen. Der Beitrag stellt zunächst die Bereiche vor, in dem diese Recherchen im WWW (world wide web) stattfinden: Kinderpornografie, Wirtschafts- und Computerkriminalität sowie Staatsschutzdelikte. Nach einem Exkurs zu den Strategien und Ermittlungsmethoden sowie nach Erwähnung automatischer Web-Überwachungstools der obengenannten Behörden endet der Beitrag mit der Behauptung, dass die surfenden Behörden sich in einer rechtlichen Grauzone bzw. sogar in der Illegalität befinden. Weder das BKAG noch z.B. das BayPAG können als rechtliche Grundlage für die momentanen Aktivitäten der surfenden Dienststellen herangezogen werden. Nach Ansicht der Autorin ist sogar zu befürchten, dass die Polizei über den Einstieg einer anlassunabhängigen Internet-Recherche auf eine totale Überwachung des Internets hinzielt.

IDN: 20021117

TYP: VOR

SGB: RE; KK

AUT: Pätzel, Claus

TIT: www. Nepper, Schlepper, Bauernfänger.com; Aktuelle Sicherheitsprobleme und Delikte in und um das Internet; Vortrag des Autors, den er auf einer internationalen Tagung in Berlingen/ Schweiz am 29.11.2001 zum Thema "Herausforderung - auch für die Justiz?" hielt

FST: DRiZ

JAH: 2002

JGG: 80

HES: 6, S. 231-235

BEI: 26 QU

FD: Internet; Rechtsgeltung; Strafverfolgung; Internationale Rechtshilfe; Territorialitätsprinzip; Betrug; Kreditkartenmissbrauch; Kinderpornographie; Fahndungserfolg; Sexueller Missbrauch von Kindern; Rechtshilfe

TEXT: Die weit verbreitete kriminelle Nutzung des Internets als Tathilfsmittel hat im Bereich der Strafverfolgung für neue Probleme gesorgt. Dies gilt insbesondere für Betrugsdelikte und Kinderpornographie, auf die ausführlich Bezug genommen wird. Jeder Staat hat das Problem zu bewältigen, dass strafbare Inhalte in Ländern ins Netz gestellt werden, in denen diese Inhalte als legal angesehen werden. Des Weiteren muss mit den im jeweiligen Staat gegebenen prozessualen Mitteln ausgekommen werden. Neben den allgemeinen Problemen der Strafverfolgung wird gerade bei den international ausgerichteten Delikten der Internetkriminalität immer deutlicher, dass sich an der Umständlichkeit von Auslandsermittlungen so gut wie nichts geändert hat. Vereinfachungen auf dem Gebiet der Rechtshilfe sind dringend geboten.

IDN: 20021280

TYP: AUF

SGB: KO; KK; DV

AUT: Picko, Helmut

TIT: Der Computer als Tat- und Beweismittel: Computerkriminalität - Dialer

FST: Der Kriminalist

JAH: 2002

JGG: 34

HES: 7-8, S. 282-286

BEI: 7 TAF, 1 TAB, 30 QU

FD: Beweismittel; Computerbetrug; Computerkriminalität; Internet; Technologie; Telefonwählgerät; Manipulationsprogramm; Telekommunikationsdaten; Verbindungsdaten; Datenfernübertragung; Ermittlungsarbeit

TEXT: Diese nicht abschließende Darstellung eines neuen, stark verbreiteten Modus Operandi zeigt: Auch Phänomene mit scheinbar einfachen technischen Hintergründen fordern den Kriminalisten als spezialisierten Sachbearbeiter heraus. Andere Phänomene, wie z. B. das Hacking oder das Defacement, stellen sich in Sachbearbeitung und forensischer Datensicherung und -auswertung noch weit komplexer dar. Die Entwicklung des Internets schreitet mit enormer Geschwindigkeit voran, was zu immer neuen Tatbegehungsformen und damit auch zu neuen Herausforderungen für die Polizei führen wird.

IDN:20010609

TYP:AUF

SGB:KK

AUT:Huber, Peter

TIT:Ermittlung und Strafverfolgung bei Internetattacken

FST:DSWR

JAH:2001

JGG:30

HES:3, S. 63-66

BEI:2 QU

FD:Computerbetrug; Computersabotage; Datenmanipulation; Hacker; Internet; Ermittlungsarbeit; Computervirus; Straftat

TEXT:Das Ausmaß der Gesetzesübertretungen, die im Internet begangen werden, ist unbegrenzt. Denkbar ist fast der gesamte Straftatenkatalog des Strafgesetzbuches. Regelmäßig wird das Internet als Instrument zur Begehung von Straftaten genutzt, z.B. bei der illegalen Verbreitung von kinderpornografischen Darstellungen oder auch rechtsextremistischen Gedankengutes. Dabei ist die Tatsache, dass diese illegalen Informationen über das Internet verbreitet werden, statt wie bisher z.B. per Post, Telefon etc., unerheblich, da bei den Definitionen von Straftaten allgemein zwischen dem Weg der Verbreitung bzw. den verwendeten Mitteln nicht unterschieden wird. Geahndet werden ebenso das Ausspähen von Daten, das Verändern und Löschen von Daten, die Computersabotage und der Computerbetrug. Die PP 202 a, 263 a, 303 a und 303 b des Strafgesetzbuches machen zu diesem Thema eindeutige Aussagen. Will sich ein Unternehmen oder eine Privatperson der Polizei mitteilen, so scheitert es oft am geeigneten Ansprechpartner. Ein einheitlicher Kommunikationsablauf könnte da Abhilfe schaffen, genauso wie die IT-Ausbildung der Polizeibeamten, die zwischenzeitlich gefördert und vorangetrieben wird. Ermittelt die Polizei über Sachverhalte, die den Verdacht einer Straftat begründen, so sollten Daten, die damit in Zusammenhang stehen, gesichert und - soweit rechtlich zulässig - an sie übergeben werden.

IDN:20011574

TYP:AUF

SGB:KK

AUT:Krader, Gabriela

TIT:Kampf gegen die Internetkriminalität

FST:DuD

JAH:2001

JGG:25

HES:6, S. 344-347

BEI:25 QU

FD: Internet [Cyberkriminalität]; Überwachungssystem; Telekommunikationsordnung [TDSV; TKÜV]; Datenschutz

TEXT:Im Kampf gegen die Internetkriminalität werden auf internationaler und nationaler Ebene zunehmend "schwerere Geschütze" aufgefahren. Insbesondere die Umsetzung der zukünftig im Bereich der Telekommunikation und des Internets geforderten Überwachungsverfahren stellt die Anbieter entsprechender Dienstleistungen vor große Herausforderungen. Der Beitrag gibt Hintergrundinformationen zur Entwicklung der TK- und Internetüberwachung auf internationaler und nationaler Ebene und stellt die wichtigsten Regelungen geplanter oder bereits beschlossener Rechtsakte und Maßnahmen zur Bekämpfung der Cyberkriminalität vor. Nach einer Gesamtanalyse der möglichen Auswirkungen, werden die aus Sicht der TK- und Internetdienstanbieter wesentlichen rechtspolitischen Forderungen vorgestellt.

IDN:20011575

TYP:AUF

SGB:RE

AUT:Bäumler, Helmut

TIT:Eine sichere Informationsgesellschaft?; Zur europäischen Bekämpfung der Computerkriminalität

FST:DuD

JAH:2001

JGG:25

HES:6, S. 348-352

BEI:7 Qu

FD:Computerkriminalität; Informationsgesellschaft; Europarat; Datenschutz; Internet; Grundrechtsschutz; Rechtshilfe; Europol

TEXT:Die Bekämpfung der Kriminalität im Internet ist Gegenstand umfassender europäischer Regulierungsbemühungen. Die Kommission der Europäischen Union hat am 21. Januar 2001 eine Mitteilung KOM (2000) 890 endg. über die "Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" zur Diskussion gestellt.
Größere Beachtung hat der Entwurf der Cyber-Crime-Konvention des Europarates gefunden, dessen 25. Version die Parlamentarische Versammlung mit gewissen Einschränkungen am 24. April zugestimmt hat und der jetzt noch den Ministerrat sowie die nationalen Parlamente passieren muss. Die Bestrebungen zielen auf eine Ausweitung und Koordinierung der Befugnisse der Strafverfolgungsbehörden und werden weitgehende Grundrechtsbeschränkungen nach sich ziehen.

IDN:20011684

TYP:AUF

SGB:RE; KP

AUT:Hilbrans, Sönke

TIT:Erfassungskonflikte im Cyberspace

FST:DANA

JAH:2001

JGG:24

HES:2, S. 16-21

BEI:49 QU

FD:Ermittlungsmethode; Computerkriminalität; Datennetz; Grundrechtsschutz; Informationsgesellschaft; Deliktart; Rechtsgrundlage; Rechtsschutz; Internet; Strafverfolgung; Datenschutz

TEXT:Der Autor beschäftigt sich mit dem Entwurf einer Cyber-Crime-Convention (CCC) als Indikator für den Zustand des Grundrechtsschutzes in der internationalen Informationsgesellschaft. Eine geschlossene Definition von Cyber-Crime gibt es nicht. Es bleibt ein Oberbegriff für alle Straftaten, die unter Zuhilfenahme von Datennetzen verübt werden.
Mit dem CCC-Entwurf wird ein internationaler Mindestbestand an Kontrollinstrumenten formuliert: Zugriff der nationalen Sicherheitsbehörden auf in Computer gespeicherten Informationen, den Inhalt von Telekommunikation, auf Bestandsdaten und auf Verbindungsdaten. Neben der Standardisierung der Ermittlungsmethoden zielt der CCC-Entwurf auf die Internationalisierung der Strafverfolgung, d.h. auf die internationale Verfügbarkeit der zu gewinnenden Erkenntnisse.
Eine CCC soll ein Verfassungsbaustein für die virtuelle Welt der Datennetze sein. Sie kann nur Grundrechtsschutz auf dem kleinsten gemeinsamen Nenner bieten. Dabei steht der nationale Grundrechtsschutz gegen die völkerrechtliche Kooperationspflicht.

IDN:20011685

TYP:AUF

SGB:KK; KP; RE; DV

AUT:Weichert, Thilo

TIT:Cyber-Crime-Bekämpfung und Datenschutz

FST:DANA

JAH:2001

JGG:24

HES:2, S. 5-15

BEI:53 QU

FD:Wirtschaftskriminalität; Tatmittel; Bekämpfungsmaßnahme; Datenschutzrecht; Internet; Grundrechtsschutz; Strafverfolgungsrecht; Telekommunikationsverkehr; Überwachungsbefugnis; Computerkriminalität; Europäische Union; Rechtshilfeabkommen; Kontrollverfahren

TEXT:Cybercrime ist eine neue Verbrechensvariante im Internet. Es handelt sich hierbei im Schwerpunkt um Wirtschaftskriminalität. In der breiten Öffentlichkeit herrscht immer noch der Eindruck, dass das Internet vorrangig zur Begehung von Straftaten oder sonstigen Rechtsverstößen existiert. Vielmehr ist es ein Kommunikationsmittel, das völlig neue Möglichkeiten zur Verwirklichung von Freiheitsrechten eröffnet und zunehmend als wichtiger Wirtschaftsfaktor anzusehen ist. Leider wird das Internet auch zum Begehen von Straftaten genutzt. Das Internet ist kein rechtsfreier Raum. Bei dessen Nutzung sind die Gesetze, von staatlichen Stellen insbesondere auch die Grundrechte, zu beachten.
Da es Rechtsverstöße gibt, muss es auch eine Verfolgung von im Netz begangenen Straftaten geben. Den Strafverfolgungsbehörden müssen hierfür sowohl rechtlich wie auch technisch die erforderlichen und angemessenen Möglichkeiten und Mittel zur Verfügung gestellt werden. Der Beitrag befasst sich ausführlich mit der Bekämpfung der Cyber-Kriminalität und dessen Konflikt mit dem Datenschutz.

IDN:20011871

TYP:AUF

SGB:KK; KO

AUT:Kubica, Johann

TIT:Internetkriminalität - Wesentliche Erscheinungsformen und Bekämpfungsmaßnahmen

FST:Die Kriminalpolizei

JAH:2001

JGG:19

HES:3, S. 75-80

BEI:21 QU

FD:Internet, Computerkriminalität; Informations- und Kommunikationstechnik; Kriminalphänomenologie; Softwarepiraterie; Deliktart; Definition [Computerdelikt, IuK-Delikt]; Computerbetrug; Bekämpfungsmaßnahme; Präventivmaßnahme

TEXT:Internetkriminalität gehört zur Computerkriminalität, zur Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnik (IuK-Technik). Nach einer polizeilichen Definition was IuK-Kriminalität umfasst und was computerspezifische Straftaten sind, werden wesentliche Phänomenbereiche der Internetkriminalität beleuchtet. Es werden strafbare Inhalte im Internet, der Internetbetrug, strafbare Angriffe und Bedrohungen und Softwarepiraterie erläutert. Die neuen Formen der Internetkriminalität erfordern entsprechend neue und in die Zukunft gerichtete Maßnahmen zur Verhütung und Verfolgung solcher Straftaten. Einige dieser Ansätze werden vorgestellt:

- Personelle und organisatorische Maßnahmen der Polizei
- Task-Force "Sicheres Internet"
- Zusammenarbeit mit Providern
- Präventionsansätze beim E-Commerce-Betrug
- Rechtliche Anpassung
- Internationale Initiativen.

IDN:20010051

TYP:AUF

SGB:RE; KK

AUT:Meseke, Bodo

TIT:Ermittlungen im Internet - Positionen und Dissonanzen; Rechtliche Konfliktpunkte bei der Bekämpfung von Kriminalität im Internet

FST:Kriminalistik

JAH:2000

JGG:54

HES:4, S. 245-249

BEI:8 QU

FD:Internet; Durchsuchung; Beweissicherung; Datenschutz; Kriminalitätsbekämpfung; Sicherstellung, Verantwortlichkeit; Provider; Beschlagnahme; Überwachungsmaßnahme; StPO P 100 a; StPO P 110; StPO P 94; StPO P 99; StPO P 102; StPO P103; Telekommunikationsgesetz; Fernmeldeanlagengesetz; TDG

TEXT:Um sinnvolle kriminalpolizeiliche Ermittlungen durchführen zu können, ist zunächst der Verantwortliche für das fragliche Angebot zu bestimmen. Als Rechtsgrundlage dienen hier das IuDKG und das Teledienstgesetz. Daraus ergibt sich in Bezug auf die Verantwortlichkeit eine Unterscheidung der Diensteanbieter in "content-", "service-" und "access-provider". Diese Begriffe können aber wegen vorkommender Überschneidungen nicht immer getrennt werden.
Die zur Zeit noch vorhandenen rechtlichen Konfliktpunkte liegen im Bereich der §§ 94, 100 a, 110, 99, 102, 103 StPO, § 12 FAG, § 4 TDSV, § 2 TDG und der §§ 89 und 90 TKG. Der Beitrag gibt einen Überblick über diese gesetzlichen Regelungen und deren Bedeutung für die Bekämpfung der Kriminalität in Datennetzen.

IDN:20011107

TYP:TAV

SGB:DV; KK; RE

AUT:Tonscheck, Michael

TIT:Ermittlungen im Internet - Technische Möglichkeiten und rechtliche Grundlagen

TAT:Polizeitechnik im Wandel [internationales Seminar]

ORT:Münster; BR Deutschland

DAT:2000 [05.06.-08.06.]

VER:PFA [Münster, BR Deutschland]

FST:PFA-Schlussbericht [Krim 6-93]

JAH:2000

JGG:22/2000 [Schlussbericht-Nr.]

HES:S. 129-150

FD:Internet; Straftat; Ermittlungsmethode; BKA; Telekommunikationsgesetz; Teledienstegesetz; Teledienste-Datenschutzgesetz; Verantwortlichkeit; E-Mail

TEXT:Das Bundeskriminalamt begegnet der steigenden Internetkriminalität mit der Bildung eines entsprechenden Aufgabenschwerpunkts. Internetkriminalität definiert sich als Straftaten der IuK-Kriminalität, die unter Ausnutzung des Internets begangen werden und solchen, die gegen die Technik des Internets gerichtet sind. Die Ermittlungsansätze zielen auf die Feststellung eines möglichen strafrechtlich "Verantwortlichen" und damit einer für die weitere Sachbearbeitung zuständigen Strafverfolgungsbehörde durch Ermittlung des Teilnehmers, dem zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zugeordnet war, Ermittlungen über die Hostbezeichnung/Domäne und Ermittlung des Inhabers einer E-Mail-Adresse.

IDN:20020869

TYP:TAV

SGB:RE; DV

AUT:Zapfe, Michael

TIT:Zentrale und anlassunabhängige Recherchen in Datennetzen

TAT:Rechtsfragen im Zusammenhang mit dem Internet [Seminar]

ORT:Münster; BR Deutschland

DAT:2000 14.11-16.11.]

VER:PFA [Münster, BR Deutschland]

FST:PFA-Schlussbericht [Recht 05.01-944]

JAH:2000

JGG:44/2000 [Schlussbericht-Nr.]

HES:S. 67-76

BEI:3 TAB

FD:BKA; Zentralstelle für anlassunabhängige Recherchen [ZaRD]; Internet; Datennetz; IuK-Kriminalität; Recherche; Telekommunikationsgesetz; Teledienstgesetz; Kinderpornographie

TEXT:In Ausführung des IMK-Beschlusses vom 20.11.1998 erfüllt das BKA den Auftrag der zentralen anlassunabhängigen Recherche in Datennetzen im Fachreferat OA 34, bei der "Zentralstelle zur anlassunabhängigen Recherche in Datennetzen" (ZaRD). Unter anlassunabhängiger Recherche in Datennetzen versteht man die "nicht extern initiierte Suche nach strafbaren Inhalten im INTERNET und Online-Diensten, einschließlich der Weiterverfolgung von dabei festgestellten, strafrechtlich relevanten Sachverhalten mit Beweissicherung bis zur Feststellung der Verantwortlichen und der örtlichen Zuständigkeiten von Polizei und Justiz". Rechtsgrundlage für die anlassunabhängige Recherche in Datennetzen ist § 2 (2) Nr. 1 i.V.m. § 2 (1) BKAG. Die Befugnisnorm reicht aus, da bei anlassunabhängigen Recherchen in offen zugänglichen Informationsquellen, hier dem INTERNET, regelmäßig keine Eingriffe in das allgemeine Persönlichkeitsrecht (APR) vorliegen. Eilmaßnahmen im Verdachtsfall werden gem. § 163 StPO getroffen. Die Erhebung von Informationen mittels verdeckter Maßnahmen oder zum Zwecke der Gefahrenabwehr sind durch den Auftrag und die Befugnisnorm der ZaRD nicht gedeckt. Die Recherchen der ZaRD werden deliktsübergreifend in allen Internetdiensten, wie IRC, WWW, Usenet (Newsgroups), FTP sowie den Online-Diensten AOL und T-ONLINE durchgeführt.

IDN:20002499

TYP:AUF

SGB:RE; KP

AUT:Derksen, Roland

TIT:Perspektiven für eine wirksame Bekämpfung von Rechtsradikalismus und Rassismus im Internet

FST:ZFIS

JAH:1999

JGG:3

HES:3, S.150-160

BEI:Zahlr. QU

FD:Deliktart; Rechtsextremismus; Internet; Rechtsradikalismus; Rassismus; Mailbox; Computernetz; Bekämpfungsstrategie; Strafverfolgung; Propaganda; Sanktionierung; Rechtsgrundlage; Internationale Rechtshilfe; Zusammenarbeit

TEXT:Es werden Perspektiven für eine wirksame Bekämpfung von Rechtsradikalismus und Rassismus im Internet aufgezeigt. Das Internet wird international im erheblichen Umfang zur Verbreitung von rechtsradikalen und rassistischem Gedankengut genutzt. Die von den meisten Staaten übernommene Verpflichtung zur Bekämpfung von rassistischer Propaganda kann diese nicht alleine erfüllen, wenn als Verbreitungsmedium internationale Computernetze genutzt werden. Der Autor diskutiert die Anwendbarkeit des deutschen Strafrechts und die Verantwortung von Providern für im Internet zugängliche Dateninhalte nach dem Gesetz über die Nutzung von Telediensten und dem Staatsvertrag über Mediendienste. Eine wirkungsvolle Bekämpfung von inkriminierten Dateninhalten im Internet erfordert neben einer Harmonisierung der nationalen Strafrechtssysteme die Intensivierung der internationalen Zusammenarbeit der Strafverfolgungsorgane. Die Selbstregulierung des Internets durch Nutzer und Anbieter ist eine wichtige Ergänzung zu den staatlichen Bemühungen und den Initiativen internationaler Organisationen, rechtswidrigen und schädigenden Inhalten im Internet Einhalt zu gebieten.

Nationales und internationales Recht

IDN: 20030561

TYP: AUF

SGB: RE

AUT: Roßnagel, Alexander; Pfitzmann, Andreas

TIT: Der Beweiswert von E-Mail

FST: NJW

JAH: 2003

JGG: 56

HES: 17, S. 1209-1214

BEI: 74 QU

FD: Willenserklärung; Urkundenbeweis; Anscheinsbeweis; Elektronischer Rechtsverkehr; Signaturgesetz; Digitale Signatur; Elektronischer Geschäftsverkehr; E-mail

TEXT: Der Geschäftsverkehr nutzt zunehmend die Vorteile elektronischer Kommunikation. In diesen werden auch Willenserklärungen in Form von E-Mails ausgetauscht, deren Beweiswert bislang umstritten ist. Erste Urteile maßen einer E-Mail keinerlei Beweiswert zu. Zum Teil wird jedoch ein Anscheinsbeweis für E-Mails gefordert. Der Verfasser diskutiert den Beweiswert von E-Mails für ihre Integrität und Authentizität und untersucht die Argumente, die für einen Anscheinsbeweis von E-Mails sprechen könnten. Im Ergebnis wird aufgezeigt, dass die Argumentation für E-Mails als Anscheinsbeweis sich als nicht tatkräftig erweist. Ein Anscheinsbeweis würde zu einem nicht tragbaren Verlust an Rechtssicherheit führen.

IDN: 20031089

TYP: GUS

SGB: RE; DV

AUT: Lehmann, Michael

TIT: Die IT-relevante Umsetzung der Richtlinie Urheberrecht in der Informationsgesellschaft; Ein Überblick zu den wesentlichen Änderungen des deutschen Urheberrechts durch das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft

FST: CR

JAH: 2003

JGG: 19

HES: 8, S. 553-557

BEI: 44 QU

FD: Urheberrecht; Informationstechnik; Völkerrecht; EG-Richtlinie; Nationales Recht; Europäisches Gemeinschaftsrecht; Rechtsreform; Informationszugangsrecht; Neue Medien; Internet; Vervielfältigung; Digitaltechnik; Eigentumserwerb; Öffentlichkeit; Informationsgesellschaft; Kunstwerk; Verwertungsrecht; UrhG P 19 a; UrhG P 15 Abs 3; UrhG P 95 a; UrhG P 95 c; Raubkopie; Softwarepiraterie; Sicherungssystem; Hacker; Rechtsschutz

TEXT: Die Reform des deutschen Urheberrechts dient der Umsetzung der Urheberrechtsrichtlinie und geht zurück auf die völkerrechtlichen Verpflichtungen aus dem WIPO Copyright Treaty (WCT) und dem WIPO Performances and Phonograms Treaty (WPPT). Für den IT-Bereich besonders bedeutsame Veränderungen sind das Recht der interaktiven Zugänglichmachung, der neue Begriff der Öffentlichkeit, der Schutz technischer Maßnahmen und der Schutz von Informationen zur Rechtewahrnehmung. Dieser Beitrag greift diese IT-relevanten Schwerpunkte heraus und stellt sie im Zusammenhang vor.

IDN: 20031485

TYP: AUF

SGB: RE; DV

AUT: Ernst, Stefan

TIT: Hacker und Computerviren im Strafrecht

FST: NJW

JAH: 2003

JGG: 56

HES: 45, S. 3233-3239

BEI: 85 QU

FD: Computervirus; Hacker; Internet; Computerkriminalität; Computerspionage; Strafrecht; Strafrechtspolitik; StGB P 202 a; StGB P 303 a; StGB P 303 b; Spam-E-mail; Datenmanipulation; Datenverarbeitung; Tatbestandsmerkmal

TEXT: In jüngerer Zeit erschüttern mehr und mehr Berichte über Computerviren und weitere spektakuläre Angriffe auf bzw. über das Internet die Benutzer von Computern und des weltweiten Datennetzes. Die wirtschaftlichen Schäden sind schon jetzt immens. Zugleich verstärken verschiedene Staaten auch offiziell in diesem Bereich nicht nur ihre kriminalistischen, sondern auch ihre (defensiven und offensiven) militärischen Ressourcen für den Cyber oder Infowar (information warfare). Die ersten virtuellen Konflikte wurden bereits ausgetragen. Führende deutsche Politiker fordern gleichzeitig, das Strafrecht in diesem Bereich anzupassen. Der Beitrag erläutert die Reichweite des für Hackerangriffe und Computerviren geltenden Strafrechts.

IDN:20020318

TYP:AUF

SGB:RE; DV

AUT:Scheffler, Hauke

TIT:Einsatz einer Pay-TV Piraten-SmartCard - strafrechtliche Würdigung

FST:CR

JAH:2002

JGG:18

HES:2, S. 151-156

BEI:29 QU

FD:Fernsehen; Verschlüsselung; Signalverarbeitung; Fernsehbildübertragungssystem; Dechiffrierung; Hacker; Chipkarte; Datenmanipulation; Raubkopie; Strafbarkeitsbedingung; Tatbestandsmerkmal; Leistungserschleichung; StGB P 265 a; Computerbetrug; StGB P 263 a; Anbieter; Kaufvertrag; Vermögensschaden

TEXT:Der Verfasser geht der Frage nach, ob die Verwendung einer Pay-TV "Piraten-Smartcard" ein Erschleichen von Leistung nach § 265 a StGB oder einen Computerbetrug nach § 263 a StGB darstellt. Er nimmt im Rahmen des Computerbetrugs insbesondere zu der umstrittenen Frage Stellung, ob es bei dem Einsatz einer solchen Karte zu einer unmittelbaren Vermögenseinbuße bei dem Programmanbieter kommt. Im Ergebnis wird festgestellt, dass die Verwendung einer Pay-TV "Piraten-Smartcard" vom Tatbestand des Computerbetrugs erfasst wird und damit das Erschleichen von Leistungen nach § 265 a StGB aufgrund materieller Subsidiarität zurücktritt.

IDN: 20020773

TYP: AUF

REG: AUS

SGB: RE; KK

AUT: Pallasky, Ansgar

TIT: USA Patriot Act - Neues Recht der TK-Überwachung

FST: DuD

JAH: 2002

JGG: 26

HES: 4, S. 221-225

BEI: 45 QU

FD: Internationaler Terrorismus; Bekämpfungsmaßnahme; Terrorismusbekämpfung; Befugniserweiterung; Gesetzesänderung; Überwachungsbefugnis; Informationsgewinnung; Telekommunikationsüberwachung; Telefonüberwachung; Durchsuchung; USA; Strafverfolgung; Spionageabwehr; Internet; Zuständigkeitsregelung; Anti-Terror-Gesetz

TEXT: Zur künftigen Verhinderung terroristischer Anschläge wie dem vom 11.09.2001 brachte der US-Kongress den sogenannten USA Patriot Act auf den Weg, der als Gesetz am 26.10.2001 zu geltendem Recht wurde. Der USA Patriot Act besteht aus zehn Kapiteln, in denen im Wesentlichen Informationsgewinnungsbefugnisse und Überwachungsrechte sowie Gesetze zur Geldwäschebekämpfung erweitert, die StPO im Terrorismusbekämpfungsbereich verschärft, eine Strafverschärfung für bestimmte Straftaten eingeführt, das Einwanderungsrecht abgeändert und die Bereitstellung von Fördermitteln für die Arbeit bestimmter Behörden autorisiert werden. Im Rahmen der Änderungen des Überwachungsrechtes wurden die Möglichkeiten zulässigen Wiretappings, das grundsätzlich untersagt ist, erweitert. Erweitert wurde auch der Anwendungsbereich des Gesetzes, das die Voraussetzungen zur Nutzung des sogenannten Pen-Registers sowie des Map-and-Trace regelt und zwar auf neue elektronische Kommunikationsmittel. Die Ermittlung von Content ist hier zwar ausdrücklich ausgeschlossen, allerdings ergibt sich mangels genauer Definition die Schwierigkeit der Abgrenzung von Content und Non-Content. Auch die Gerichtszuständigkeit für die Anordnung der Maßnahme wurde in diesem Zusammenhang geändert. Mit dem USA Patriot Act können zudem Search Warrants bei der Untersuchung des nationalen und internationalen Terrorismus bei jedem Gericht beantragt werden, in dessen Zuständigkeitsbereich terroristische Aktivitäten aufgetreten sind. Eine vergleichbare Regelung wurde auch für die Durchsuchung in geöffneten e-mail-Nachrichten eingeführt. Voicemail-Nachrichten sind nunmehr e-mail-Nachrichten gleichgestellt, so dass für diese kein Wiretap mehr benötigt wird. Auch die Benachrichtigungspflichten bei Wohnungsdurchsuchungen wurden mit dem USA Patriot Act gelockert. Diese Regelungen gelten für die Strafverfolgung innerhalb der USA. Sollen die Maßnahmen im Rahmen der Spionageabwehr eingesetzt werden, gelten andere Standards, die durch den USA Patriot Act aber ebenfalls herabgesetzt wurden. Einige der vorgenommenen Änderungen unterliegen der sogenannten Sunset-Regelung und sind nur bis 31.12.2005 wirksam. Die Ausweitung der

Überwachungsrechte ist bedenklich, zum Teil in besonderem Maße. Es bestehen Zweifel, ob zur Verhinderung von Anschlägen wie denen vom 11.09.2001 eine derartige Ausweitung tatsächlich notwendig ist.

IDN: 20020839

TYP: AUF

SGB: RE; DV

AUT: Hilbrans, Sönke

TIT: Die Cybercrime-Konvention; Ein Schritt zum weltweiten Fahndungsnetz

FST: Bürgerrechte & Polizei

JAH: 2002

HES: 71, Nr. 1, S. 54-58

BEI: 4 QU

FD: Internet; Computerkriminalität; Telekommunikationsüberwachung; Internationale Zusammenarbeit; Datenschutz; Strafverfolgung; Bekämpfungskonzept; Europarat

TEXT: Im Digitalzeitalter gibt es für Individuen wie für wettbewerbsorientierte Gesellschaften nur zwei stabile Zustände: online oder tot. Entsprechend erscheint die Politik der inneren Sicherheit "im Netz" als vorrangige Aufgabe moderner Daseinsfürsorge. Wegen der steigenden wirtschaftlichen und politischen Bedeutung der "Netze" ist die Bekämpfung der Straftaten, die in oder unter Zuhilfenahme des Internet oder anderer Telekommunikations- oder Datennetze begangen werden, ein wichtiges Ziel der Kriminalitätsbekämpfung geworden. Nach langer Diskussion haben sich die 43 Mitgliedsstaaten des Europarates unter Mitwirkung von Kanada, den USA, Japan und Südafrika auf die Cybercrime Convention (CCC) verständigt. Die Konvention soll ermöglichen, dass die o.a. Straftaten zukünftig effektiver und international bekämpft werden können. Die CCC zielt auf die Ausstattung der Polizeien der Signaturstaaten mit weitreichenden Eingriffsbefugnissen, ohne Gegengewichte im Sinne der Grundrechte zu schaffen.
Folgende Themen werden in dem Aufsatz besprochen:

- Das materielle Strafrecht der CCC
- Die Ermittlungsmethoden neuen Typs, die die Bekämpfung der Cyberkriminalität erfordert
- Die Internationalisierung der Strafverfolgung
- Darf es im Cyberspace keine Privatheit geben?

IDN: 20021721

TYP: ENT

SGB: RE; DV

AUT: Breital, Norbert

TIT: Bundesdeutsche Strafgewalt und grenzüberschreitende Internetkriminalität; BGH-Entscheidung vom 12.12.2000 - 1 StR 184/00

FST: Die Polizei

JAH: 2002

JGG: 93

HES: 10, S. 269-278

BEI: 103 QU

FD: Internet; Strafverfolgung; Rechtsgeltung; Territorialitätsprinzip; Auslandstat; Handlungsunrecht; Erfolgsdelikt; Abstraktes Gefährdungsdelikt; Tatortbestimmung; Grenzüberschreitende Kriminalität; Weltrechtspflegeprinzip; Internationales Strafrecht; Rechtsanwendung; Internationaler Vergleich

TEXT: Ergänzend zur Besprechung dieser BGH-Grundsatzentscheidung leistet der Aufsatz einen Beitrag zum internationalen Strafrecht des StGB mit rechtsvergleichenden Anmerkungen. Es wird festgestellt, dass nahezu alle Staaten, die sich bereits mit dem Problem der Strafbarkeit von ausländischen Internet-Inhalten beschäftigt haben, ihr Strafrecht auf diese Angebote anwenden. Zum Teil wird sogar eine umfassende Allzuständigkeit für alle Internet-Inhalte angenommen. Der Großteil der Rechtsordnungen stellt auf die Unterscheidung zwischen Erfolgs- und Handlungsdelikten ab, jedoch zumeist mit dem Ergebnis, dass die Kommunikationsdelikte als Erfolgsdelikte der eigenen Strafgewalt unterliegen. Der BGH wird bei abstrakten Gefährdungsdelikten den in seiner Grundsatzentscheidung angedeuteten Mittelweg beschreiten. Er wird den emanzipierten Erfolgsbegriff des § 9 StGB als Erfolgsauswirkung im weiteren Sinne interpretieren und dem § 9 StGB unterstellen.

IDN: 20030041

TYP: AUF

SGB: RE; KP

AUT: Koch, Arnd

TIT: Nationales Strafrecht und globale Internet-Kriminalität; Zur Reform des Strafanwendungsrechts bei Kommunikationsdelikten im Internet

FST: GA

JAH: 2002

JGG: 149

HES: 12, S. 703-713

BEI: 71 QU

FD: Grenzüberschreitende Kriminalität; Internet; Kriminalphänomenologie; Straftat; Deliktart; Strafverfolgung; Zuständigkeit

TEXT: Keiner der in Rechtsprechung und Literatur entwickelten Vorschläge vermochte auf die Frage nach den Grenzen deutscher Zuständigkeit für grenzüberschreitende Kommunikationsdelikte eine überzeugende Antwort zu geben. Dass auch nach mehrjähriger wissenschaftlicher Diskussion bislang keine befriedigende Lösung gefunden werden konnte, darf nicht als Versagen der Strafrechtswissenschaft missverstanden werden. Deutlich wird lediglich, dass nationales Strafrecht gegen die globale Verbreitung bestimmter Internet-Inhalte von vornherein machtlos ist. Wenn sich das Strafanwendungsrecht nicht in realitätsfernen symbolischen Zuständigkeitsbehauptungen erschöpfen will, bleibt nur der Ausweg einer Selbstbeschränkung. Im Interesse der Rechtsklarheit könnte daher § 9 StGB um folgenden Absatz 3 ergänzt werden: "Ist eine Tat durch die Verbreitung von Informationen in weltweiten Datennetzen (Internet) begangen worden, so gilt das deutsche Strafrecht vorbehaltlich § 6 StGB nur dann, wenn der Täter vom Inland aus gehandelt hat." Eine solche Lösung bedeutet keine Kapitulation vor via Internet verbreiteten Kommunikationsdelikten. Um das eigentliche Ziel, die Verbannung bestimmter Inhalte aus dem Netz, erreichen zu können, müssen vielmehr andere Wege beschritten werden. In Betracht kommen vor allem Bemühungen um eine allmähliche Angleichung der Strafrechtsordnungen sowie Appelle an die Selbstkontrolle der Internet-Unternehmen. Diese Wege mögen langwierig und mühsam erscheinen - erfolgversprechender als die Aufstellung undurchsetzbarer nationalstaatlicher Zuständigkeitsbehauptungen sind sie allemal.

IDN:20011669

TYP:AUF

SGB:RE; KP

AUT:Kugelmann, Dieter

TIT:Die "Cyber-Crime" Konvention des Europarates

FST:DuD

JAH:2001

JGG:25

HES:4, S. 215-223

BEI:39 QU

FD:Bekämfpungsmaßnahme [EU-Konvention]; Telekommunikationsgesetz; Europäisches Übereinkommen; Telekommunikationsverkehr; Deliktart; Überwachungsmaßnahme; Provider; Mitwirkung; Europarat; Internet; Strafbarkeit; Computerkriminalität; Datenschutz; Strafverfolgung; Internationale Zusammenarbeit; Tatbestandsmerkmal; Tatwerkzeug [Internet, PC]

TEXT:Die nationalen Regelungen zur Gewährleistung der Überwachung der Telekommunikation für Zwecke der inneren Sicherheit sind vor dem Hintergrund einer internationalen Koordinierung der Telekommunikationsüberwachung zu sehen. In diesem Zusammenhang wird derzeit die Cyber-Crime Konvention vor dem Europarat verhandelt. Die Konvention zielt gemäß ihrer Präambel auf die strafrechtliche Verfolgung von Handlungen, die gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen. Netzwerken und Computerdaten sowie den Missbrauch solcher Systeme, Netzwerke und Daten gerichtet sind. Zu diesem Zweck sollen die Strafverfolgungsbehörden mit ausreichenden Kompetenzen ausgestattet werden. Mit der Cyber-Crime Konvention würde das erste rechtsverbindliche internationale Rechtsinstrument geschaffen werden, das dem grenzüberschreitenden und weltweit vernetzten Charakter der Kriminalität im Internet Rechnung trüge. Der Autor erörtert Ziele und Rahmenbedingungen der angestrebten Konvention, geht auf die in Frage kommenden Straftaten ein und bewertet die Möglichkeiten zu deren Bekämpfung.

IDN:20012047

TYP:AUF

SGB:RE

AUT:Breyer, Patrick

TIT:Die Cyber-Crime-Konvention des Europarats

FST:DuD

JAH:2001

JGG:25

HES:10, S. 592-600

BEI:49 QU

FD:Computerkriminälität; Europarat; Cyber-Crime-Konvention; Überwachungsbefugnis; Informationelle Selbstbestimmungsrecht; Telekommunikation; Ermittlungsbefugnis; Menschenrecht; Datenschutz; Internationale Zusammenarbeit; Rechtshilfe

TEXT:Der Autor untersucht die Cyber-Crime-Konvention des Europarates und hält fest, dass die CCC einseitig auf die Effektivität der Strafverfolgung ausgerichtet ist, während der Schutz der beteiligten Bürger soweit er überhaupt zugelassen wird, allein den einzelnen Vertragsstaaten überlassen wird. Weder die Bestimmungen über innerstaatliche Ermittlungsbefugnisse noch die Vorschriften über die internationale Zusammenarbeit sehen substanzielle rechtsstaatliche Sicherungen zum Menschenrechts- und Datenschutz vor; stattdessen wird deren Missachtung Vorschub geleistet.

IDN:20012048

TYP:AUF

SGB:DV; RE

AUT:Dix, Alexander

TIT:Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV

FST:DuD

JAH:2001

JGG:25

HES:10, S. 588-591

BEI:11 QU

FD:Computerkriminalität; Telekommunikationsüberwachung; Internet; Kriminalitätsbekämpfung; Datenschutz; Strafverfolgung; Datenfernübertragung; Personenbezogene Daten ; Güterabwägung; Europäisches Gemeinschaftsrecht; Rechtssicherheit

TEXT:Eine Verbesserung der internationalen Zusammenarbeit bedarf die Bekämpfung der Cyber-Kriminalität, die nicht unbedingt identisch ist mit der Datennetzkriminalität. Zu unterscheiden ist zwischen Angriffen auf die Sicherheit des Netzes oder einzelner vernetzter Rechner und der Nutzung des Netzes zur Vorbereitung von Straftaten. Soweit es um die Bekämpfung von internetgestützter Kriminalität geht, für die das Netz nicht Angriffsziel, sondern Medium ist, muss eine sorgfältige Abwägung zwischen den Interessen der Strafverfolgung und dem Recht der Nutzung auf Schutz ihrer Privatsphäre und auf unbeobachtete Nutzung der neuen Medien stattfinden. Dabei ist auch ein grundsätzliches Recht auf anonymen oder pseudonymen Zugang und Nutzung von Netzangeboten anzuerkennen. Auch die Bekämpfung der Cyberkriminalität rechtfertigt es nicht, dass die TK-Netze entgegen ihrem ursprünglichen Zweck generell zu Überwachungsnetzen umgewidmet werden. Nur im Einzelfall kann es ausnahmsweise gerechtfertigt sein, bei einem konkreten Verdacht und unter Einhaltung rechtsstaatlicher Garantien auf vorhandene personenbezogene Daten für Strafverfolgungszwecke zuzugreifen, die zu Zwecken der Kommunikation verarbeitet werden.

IDN:20020113

TYP:AUF

SGB:RE

AUT:Hilgendorf, Eric

TIT:Die Neuen Medien und das Strafrecht

FST:ZStW

JAH:2001

JGG:113 [Bd]

HES:4, S. 650-680

BEI:112 QU

FD:Kriminalpolitik; Datenverarbeitung; Rechtsgrundlage; Bekämpfungsmaßnahme [Politik]; Internet; Computerkriminalität; Erscheinungsform; Internationales Strafrecht; Strafbarkeit; Deliktart

TEXT:Die weltweite Ausbreitung des Internets und anderer Datennetze und die dadurch ermöglichten grenzüberschreitenden Datenströme stellen die Rechtsordnungen der einzelnen Staaten vor erhebliche Probleme. Dies gilt insbesondere für das Strafrecht, denn es steht nach traditionellem Verständnis im Mittelpunkt der einzelstaatlichen Souveränität. Publikationen im Internet sind grundsätzlich weltweit zu empfangen. Ein nationales Strafrecht scheint deshalb mit der Bewältigung der Kriminalität im Datennetz von vornherein überfordert zu sein. Ein internationales Strafrecht existiert bislang nur in Ansätzen in Form des Völkerstrafrechts.
In diesem Beitrag geht es um die Frage, wie das deutsche Strafrecht auf die Herausforderungen durch die Datennetzkriminalität reagieren kann. Dazu werden einige Typen der neuen Kriminalitätsform vorgestellt. Danach wird der CompuServe-Fall, der besonderes Aufsehen erregt hat, näher beleuchtet. Im Anschluss daran kommen die Strafanwendungsregeln zur Sprache, die im sogenannten "internationalen Strafrecht" enthalten sind. Abschließend werden die Möglichkeiten eines transnationalen Strafrechts für das Internet erörtert.

IDN:20020866

TYP:TAV

SGB:RE; DV

AUT:Soiné, Michael

TIT:Strafverfolgung, Polizei und Internet

TAT:Rechtsfragen im Zusammenhang mit dem Internet [Seminar]

ORT:Münster; BR Deutschland

DAT:2000 [14.11-16.11.]

VER:PFA [Münster, BR Deutschland]

FST:PFA-Schlussbericht [Recht 05.01-944]

JAH:2000

JGG:44/2000 [Schlussbericht-Nr.]

HES:S. 15-36

BEI:Zahlr. QU

FD:Strafverfolgung; Internet; Straftat; ; StGB, Beweisgewinnung; Strafprozessrecht; Datenerhebung; Datennetz; Öffentlichkeitsfahndung; Territorialitätsprinzip; Verdeckter Ermittler; Fahndung

TEXT:Der Referent beschreibt in seinem Vortrag die Rolle der Polizei bei der Strafverfolgung im Internet und setzt sich dabei zunächst mit der materiellen Frage nach dem Handlungsort i.S.d. StGBs auseinander. Danach befasst er sich mit der Problematik der Anwendung des deutschen Strafprozessrechts bei Datenerhebung im Ausland durch die deutsche Polizei, z.B. beim Einsatz eines verdeckten Ermittlers im Rahmen der Strafverfolgung, wenn also der deutsche Hoheitsbereich überschritten wird. Im Mittelpunkt steht hierbei die Beweisgewinnung in Datennetzen. In seinem letzten Abschnitt geht der Referent auf die Öffentlichkeitsfahndung im Internet ein, wobei er zunächst feststellt, dass das bloße Zugänglichmachen von Fahndungsaufrufen über das Internet keine inlandsstaatliche Auslandstätigkeit in Form eines Eingriffs in Hoheitsrechte ausländischer Staaten darstellt. Anschließend werden verschiedene Arten der Öffentlichkeitsfahndung beschrieben.

IDN:20020871

TYP:TAV

SGB:RE; DV

AUT:Köhler, Peter

TIT:Die Aufgaben der Staatsanwaltschaft bei der Bekämpfung der Internetkriminalität

TAT:Rechtsfragen im Zusammenhang mit dem Internet [Seminar]

ORT:Münster; BR Deutschland

DAT:2000 [14.11-16.11.]

VER:PFA [Münster, BR Deutschland]

FST:PFA-Schlussbericht [Recht 05.01-944]

JAH:2000

JGG:44/2000 [Schlussbericht-Nr.]

HES:S. 95-118

FD:Jugendmedienschutz; Kinderpornographie; Kindesmissbrauch; Sodomie; Verbreitung pornographischer Schriften; Internet; Täteridentifizierung

TEXT:Das Internet bestimmt immer mehr den Ablauf unseres Alltags. Das Internet hat die Probleme der Strafverfolgung insbesondere von Jugendmedienschutzdelikten ganz erheblich verschärft. Nahezu 80 Prozent der Netzinhalte haben irgend etwas mit Pornographie zu tun. Die einfache Pornographie (§ 184 Abs. 1 StGB) unterliegt allgemeinen Vertriebs- und Werbeverboten, soweit Personen unter 18 Jahren die Möglichkeit der Kenntnisnahme haben. Die qualifizierte Pornographie (§ 184 Abs. 3 ff. StGB) – Gewalttätigkeiten, Sodomie und Kindesmissbrauch – darf weder hergestellt noch verbreitet werden. Die Verbreitung kinderpornographischer Schriften (zumeist Bilddateien) im Internet stellt sich als ein großes Problem für Polizei und Justiz dar. Die Zahl der Ermittlungsverfahren aufgrund anlassabhängiger und anlassunabhängiger Internetrecherchen nimmt ständig zu, es reichen aber die personellen Ressourcen nicht aus, um eine zeitnahe und effektive Strafverfolgung zu gewährleisten. Eine Selbstkontrolle der Netzanbieter bringt kaum Entlastung. Vielmehr haben deren Lockangebote für neue Kunden nicht selten Strafverfolgungshindernisse zur Folge, weil Täter mangels einer Registrierung nicht identifiziert werden können. Die justitielle Bewältigung der Verbreitung von Kinderpornographie im Internet mündet zumeist in Strafverfahren gegen Besitzer einschlägigen Materials; Verbreitungshandlungen lassen sich nicht immer nachweisen. Nicht zu vernachlässigen sind die Möglichkeiten des Verfalls und der Einziehung als Rechtsfolgen der Tat. Vorteile bringt das Internet aufgrund der Möglichkeiten einer wirksamen Öffentlichkeitsfahndung zur Aufklärung von erheblichen Straftaten und Festnahme gefährlicher Straftäter. Das Internet ist unkontrollierbar. Reelle Chancen, diesen Zustand zu ändern, gibt es nicht. Jedoch sollten Regelungen gefunden werden, um künftig den Auswüchsen besser begegnen zu können.

IDN:20020872

TYP:TAV

SGB:RE; DV; KP

AUT:Scheren, Martin

TIT:Die Bekämpfung der Internetkriminalität in Europa

TAT:Rechtsfragen im Zusammenhang mit dem Internet [Seminar]

ORT:Münster; BR Deutschland

DAT:2000 [14.11-16.11.]

VER:PFA [Münster, BR Deutschland]

FST:PFA-Schlussbericht [Recht 05.01-944]

JAH:2000

JGG:44/2000 [Schlussbericht-Nr.]

HES:S. 119-142

BEI:LITVZ. S. 142

FD:Internet; Strafverfolgung; Europa; Europäische Union; Internationale Zusammenarbeit

TEXT:Durch die zunehmende Vernetzung haben nationalstaatliche Grenzen in der virtuellen Welt viel von ihrer Bedeutung verloren. Daher haben die Phänomene der Internetkriminalität oft eine internationale Dimension, die neue Kooperationsformen der Strafverfolgungsbehörden der verschiedenen Staaten erforderlich macht. Der Vortrag befasst sich mit den europäischen Initiativen zur Bekämpfung der Internetkriminalität. Der weitreichendste Ansatz ist dabei die "Cybercrime-Konvention", die zur Zeit vom Europarat ausgearbeitet wird. Sie enthält neben Vorschriften über das materielle Strafrecht sowie das Strafprozessrecht Regelungen für eine vereinfachte internationale Zusammenarbeit.

IDN:20000827

TYP: AUF

SGB: RE

REG: AUS/INL

AUT: Schwarzenegger, Christian

TIT:Der räumliche Geltungsbereich des Strafrechts im Internet; Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich

FST:ZStrR

JAH:2000

JGG:118 [Bd]

HES:2, S. 109-130

BEI:3 TAB, 80 QU

FD:Grenzüberschreitende Kriminalität; Computerkriminalität; Hacker; Gefährdungsdelikt; Internet; Schweiz; Territorialprinzip; Österreich; Opportunitätsprinzip; Legalitätsprinzip; Rechtsvergleich; Erfolgsdelikt; Rechtsgeltung

TEXT:Nationalstaatliche Grenzen sind für die Täter von Internetdelikten nahezu irrelevant geworden. Da aber noch kein internationales Strafrecht zur Verfolgung dieser Taten existiert, müssen sie weiterhin nach nationalstaatlichem Strafrecht verfolgt werden. Dabei ergibt sich eine Reihe von Fragen bezüglich des materiellen und formellen Strafrechts, die in diesem Aufsatz anhand der Rechtslage in der Schweiz im Vergleich mit Deutschland und Österreich erläutert werden.
Zunächst wird erörtert, wo der Gerichtsstand bei Internetdelikten liegt und ob die Verfolgung nach dem Legalitäts- oder Opportunitätsprinzip erfolgt.
Im Mittelpunkt steht aber der räumliche Geltungsbereich des Schweizer Strafrechts im Internet. Es wird zwischen dem Ort der Ausführung und dem Ort des Erfolges der Straftat unterschieden. Mit der Einbeziehung des Erfolgseintritts wird die Deckungsgleichheit des Territorialprinzips mit dem Herrschaftsgebiet des Staates aufgegeben.
Damit ist - nicht nur für die Schweiz - folgendes Dilemma gegeben: Die Strafanwendungsrechte der Schweiz, Deutschlands und Österreichs erfassen eine kaum zu bewältigende Anzahl von Auslandstaten. Bei allen Internetdelikten kann ein dem Tatbild entsprechender Erfolg unabhängig von der Ausführungshandlung zur Anknüpfung der Tat im Inland führen.
Eine klare internationale Abgrenzung der Strafanwendungsrechte, ein effizientes Auslieferungs- und Rechtshilferecht sowie die Harmonisierung der materiell-rechtlichen Strafnormen sind deshalb notwendig.
Dennoch ist an eine schnelle internationale Lösung nicht zu denken. Für wesentliche Kriminalitätsbereiche wird auf absehbare Zeit das nationale Strafrecht maßgebend bleiben.

IDN:20002091

TYP:AUF

SGB:DV; SW; KP

AUT:Fuhrmann, Heiner

TIT:IT-Sicherheit und Verletzlichkeit aus rechtlicher Sicht; Sicherheit im staatlichen Interessengefüge

FST:DUD

JAH:2000

JGG:24

HES:3, S. 144-149

BEI:18 QU

FD:IT-Sicherheit; Informationstechnologie; Sicherheitstechnik; Informationstechnik; Öffentliche Sicherheit; Rechtsgüterschutz; Wirtschaftspolitik; Sicherungskonzept; Rechtsgrundlage; Sicherheitspolitik

TEXT:In diesem Beitrag wird untersucht, inwieweit rechtliche Entscheidungen die Berücksichtigung von Sicherheit im technischen Entwurfsprozess verlangen. Dazu wird zunächst dargelegt, auf welcher Grundlage der Verfassungsstaat sich überhaupt mit Sicherheitsfragen befassen und diese verbindlich regeln kann. Anschließend werden die Besonderheiten der IT-Sicherheit und ihre Rolle im gegenwärtigen gesetzlichen Gefüge bestimmt. In dem so abgesteckten Umfeld kann dann die Entwurfsmethode der verletzlichkeitsreduzierenden Technikgestaltung bewertet werden. Es zeigt sich, dass sie zur Verwirklichung zentraler rechtsstaatlicher Ziele und aktueller wirtschaftspolitischer Interessen hervorragend geeignet ist.
Einige gesetzliche Regelungen greifen verletzlichkeitsreduzierende Ansätze bereits auf. Für eine effiziente Verfolgung staatlicher Sicherheitsinteressen bietet sich eine Ausweitung dieser Komponenten an.

IDN:20010532

TYP:AUF

SGB:DV; RE

AUT:Bartsch, Michael

TIT:Computerviren und Produkthaftung

FST:CR

JAH:2000

JGG:16

HES:11, S. 721-725

BEI:39 QU

FD:Produkthaftung [Software]; Computervirus; Haftung; Software; BGB P 823; Sicherheitsmangel; IT-Sicherheit; Rechtssicherheit; Eigentumsrecht

TEXT:Software muss vielen Qualitätskriterien genügen, insbesondere hinsichtlich der Funktionsfähigkeit, der Korrektheit und dem Fehlen von Schadensneigungen. Die große Virenattacke "I LOVE YOU" hat die enorme Verletzlichkeit der EDV-Welt gezeigt und hohe Schäden verursacht.
Der Autor geht in seinem Aufsatz der Frage der außervertraglichen Haftung nach. Im Rahmen der rechtlichen Prüfung des § 823 BGB als Anspruchsgrundlage kommt er zu dem Schluss, dass eine Haftung des Herstellers unzweifelhaft ist. Ausblickend wird festgestellt, dass Produkte mit Sicherheitsfunktionen künftig unter Berücksichtigung der wirtschaftlichen Machbarkeit den erwartbaren Angriffen standhalten müssen.

IDN:20000481

TYP:AUF

SGB:RE

AUT:Sieber, Ulrich

TIT:Internationales Strafrecht im Internet; Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace

FST:NJW

JAH:1999

JGG:52

HES:29, S. 2065-2073

BEI:Zahlr. QU

FD:Internationales Strafrecht; Internet; Cyberspace; Nationales Recht; Territorialitätsprinzip; Rechtsanwendung; Verbreitung jugendgefährdender Schriften; Kinderpornographie; Volksverhetzung; Gewaltverherrlichung; Rassismus; Rechtsgeltung; Anwendungsbereich; StGB P 3; StGB P 9; Rechtskreistheorie

TEXT:Im Zuge des Zusammenwachsens nationaler und internationaler Computernetze zu einem globalen Cyberspace ist es möglich, Straftaten in einem Staat mit Auswirkungen in anderen Staaten zu begehen.
Im Mittelpunkt der deutschen Diskussion über Straftaten im Internet steht hier die Verbreitung von kinderpornographischen, gewaltverherrlichenden, rassistischen und nationalsozialistischen Darstellungen, die in ausländischen Computersystemen abfragbar sind. Durch die transnationale Deliktsbegehung im Internet wird die Frage aufgeworfen, inwieweit das nationale Strafrecht überhaupt anwendbar ist. Der Beitrag analysiert die Anwendbarkeit des deutschen Strafrechts im globalen Cyberspace vor allem aufgrund des Territorialitätsprinzips der §§ 3, 9 StGB. Auch die damit aufgeworfene Problematik des internationalen Strafrechts hat vor allem deswegen Bedeutung, weil die einschlägigen Straftaten im globalen Cyberspace von den verschiedenen Rechtsordnungen differenziert beurteilt werden.

IDN:20000798

TYP:AUF

SGB:RE; KK

AUT:Heinzmann, Peter L.; Ochsenbein, Andreas

TIT:Strafrechtliche Aspekte des Internet; Technische und rechtliche Grundlagen; Lösungen und Möglichkeiten

FST:Kriminalistik

JAH:1998

JGG:52

HES:7, S. 513-520; 8-9, S. 599-606; 10, S. 685-688

BEI:11 TAF, 1 TAB, Zahlr. QU

FD:Internet; Strafverfolgung; Strafrecht; Informationsfluss; Kommunikation; Ermittlungsarbeit; Fahndung; Provider; Kriminalitätskontrolle; Verantwortlichkeit; Technische Beschreibung

TEXT:Den meisten ist bekannt, dass das Internet eine universelle Kommunikationsplattform ist, wo alle einfach und günstig Informationen senden und empfangen können. Die Gefahr von Straftaten sollte jedoch dabei nicht vergessen werden: z.B. Computerdelikte, Urheberrechtsverletzungen, Geldwäscherei usw. Es soll zu neuen Ansatzpunkten zur Bestimmung der strafrechtlich Verantwortlichen beigetragen werden und Hinweise für sinnvolle Strafverfolgung sollen gegeben werden. Außerdem spielen die Bereiche Ermittlung und Fahndung im Zusammenhang mit der örtlichen Zuständigkeit im Internet eine Rolle, z.B. verdeckte Ermittlungen.
Die Möglichkeiten zur Sperre von Informationsdiensten und deren Überwachung hält sich als logische Folge der Netzarchitektur in etwa die Waage mit den Möglichkeiten zur Umgehung genau dieser Maßnahmen. Das hat zur Folge, dass der, der hier mit technischen Maßnahmen einzugreifen versucht, Gegenmaßnahmen und damit einen Wettlauf provoziert, der kontraproduktiv ist und Kräfte bindet. Im Ergebnis hat sich daher die Strafverfolgung auf den Urheber der rechtswidrigen Netzinhalte zu konzentrieren. Schärfere Gesetze bringen hier kaum eine Verbesserung der Situation, wohl aber eine internationale Annäherung der Rechtsnormen, wofür es bereits jetzt einige Anhaltspunkte gibt.

Datenschutz

IDN:20020904

TYP:AUF

SGB:SW

AUT:Winkel, Olaf; Andersen, Uwe; Hecht, Volker; Tackenberg, Helen

TIT:Der Schutz von sensiblen Informationen und kritischen Infrastrukturen in der mittelständischen Wirtschaft als politische Herausforderung; Neue Bedrohungen und Präventionsstrategien in der Informationsgesellschaft

FST:Die Kriminalprävention

JAH:2002

JGG:6

HES:1, S. 19-27; 2, S. 57-62

BEI:53 QU

FD:IT-Sicherheit; Wirtschaftsunternehmen; Informationsschutz; Wirtschaftsspionage; Sicherheitsmassnahme; Sicherheitsmanagement; Untersuchungsergebnis

TEXT:Im Jahr 2000 führten Wissenschaftler des Horst Görtz- Institutes für IT-Sicherheit an der Ruhr-Universität Bochum im Auftrag des Bundeswirtschaftsministeriums (BMWi) eine Studie zum Thema "Die Förderung von IT-Sicherheit in kleinen und mittleren Unternehmen(KMU) - eine Abschätzung des vordringlichen wirtschaftspolitischen Handlungsbedarf" durch. Nachdem Fachleute des BMWi die Ergebnisse der Studie intern geprüft und ausführlich diskutiert haben, sind sie kürzlich zur Veröffentlichung freigegeben worden. In dem vorliegenden Aufsatz werden die wesentlichen Aspekte der Studie und insbesondere natürlich die Ergebnisse und Empfehlungen komprimiert dargelegt.

IDN:20011670

TYP:AUF

SGB:DV; RE

AUT:Hülsmann, Franz Werner; Mörs, Sven, Schaar, Peter

TIT:Mobilkommunikation und Datenschutz

FST:DuD

JAH:2001

JGG:25

HES:4, S. 196-204

FD:Telekommunikationsverkehr; Datenschutzrecht; IT-Sicherheit; Mobilfunk; Kommunikationssystem; Datenübermittlung; Telefondatenerfassung; Telekommunikationsdaten; Verbindungsdaten; Personenbezogene Daten; Fernmeldegeheimnis; Funknetz; Satellitenkommunikation

TEXT:Die Übertragung von personenbezogenen oder vertraulichen Daten mittels mobiler Kommunikationsdienste unterliegt besonderen Risiken, die sich aus dem eingesetzten Übertragungsmedium Luft ergeben. Das grundrechtlich geschützte Fernmeldegeheimnis erstreckt sich sowohl auf die Inhaltsdaten als auch auf die näheren Umstände des Fernmeldeverkehrs. Angesichts des bislang nur unvollkommenen strafrechtlichen und technischen Schutzes von unverschlüsselt über die Luftschnittstelle übertragenen Informationen ist eine bessere technische Sicherung zwingend erforderlich. Neben dem BDSG ist die Telekommunikations-Datenschutzverordnung (TDSV) eine der maßgebenden Rechtsvorschriften zur Einhaltung des Datenschutzes. Außer den terrestrischen Diensten, wie Mobiltelefone, Funkruf und Mobile Datenübertragung (Modacom), werden in dem Beitrag auch Schutzmaßnahmen für Satellitenkommunikationssysteme dargestellt.

IDN:20011683

TYP:AUF

SGB:RE; SW

AUT:Köhntopp, Marit; Pfitzmann, Andreas

TIT:Gibt es einen sinnvollen Kompromiss zwischen der Verhinderung von Cybercrime und Datenschutz?

FST:DANA

JAH:2001

JGG:24

HES:2, S. 21-27

BEI:1 TAB, 3 TAF, 28 QU

FD:Computerkriminalität; Bekämpfungsmaßnahme; Datenschutz; Datensicherheit; Sicherheitstechnik; Informationsgesellschaft; Informations- und Kommunikationstechnologie; IT-Sicherheit; Verschlüsselung; Internet

TEXT:Ein sinnvoller Kompromiss zwischen der Verhinderung von Cybercrime und Datenschutz wird dringend gesucht. Doch es ist unklar, ob ein solcher Kompromiss überhaupt existiert, der kompatibel ist zu der Informations- und Kommunikationstechnologie (IT), die heute verfügbar ist oder die wir in den nächsten Jahrzehnten erwarten können. Der Beitrag stellt die bekannten verfügbaren Datensicherheitstechniken vor und diskutiert deren möglichen Einsatz durch verschiedene Akteure. Außerdem werden die Seiteneffekte von Techniken zur Verhinderung und Aufklärung von Cybercrime betrachtet.
Datenschutz ist sowohl für den einzelnen Menschen als auch für die demokratische Gesellschaft als Ganzes wichtig. Fühlen sich Menschen beobachtet, so wagen sie es nicht, sich frei zu verwirklichen. Auch Datensicherheit ist den Menschen ein Grundbedürfnis. In einer Welt, in der Cybercrime schwere Schäden verursachen kann, ist es wichtig, Cybercrime soweit wie möglich zu verhindern, ohne dass zugleich Datenschutz und Datensicherheit gefährdet werden. Nur so können die Menschen Vertrauen zu einem Leben in der Informationsgesellschaft entwickeln.

IDN:20000712

TYP:INT

SGB:KP

TIT:IT und Sicherheit sind untrennbar; Interview mit dem Bundesinnenminister Otto Schily

FST:KES

JAH:2000

JGG:16

HES:1, S. 6-10

FD:Informationstechnik; Innere Sicherheit; Informationsgesellschaft; Sicherheitsmassnahme; Datenschutz

TEXT:In einem Gespräch mit Bundesinnenminister Otto Schily hebt dieser den Stellenwert der Informationstechnik für die moderne Gesellschaft hervor und betont gleichzeitig, dass es eine staatliche Aufgabe ist, Rahmenbedingungen zu bieten, die die Entfaltung von elektronischem Handel überhaupt erst ermöglichen. So ist es der Bundesrepublik gelungen, durch das Signaturgesetz frühzeitig im Bereich der Sicherheit eine Rahmenrichtlinie zu entwerfen, die sich nunmehr in einen Wettbewerbsvorteil für deutsche Unternehmen umsetzen lässt. Daneben muss der Staat aber im Rahmen von Kriminalitätsbekämpfung und Strafverfolgung dafür Sorge tragen, dass im Internet keine rechtsfreien Räume entstehen. Das Jahr - 2000 - Problem hat gezeigt, wie abhängig die moderne Gesellschaft von der Funktionsfähigkeit ihrer Computer ist. Andererseits hat gerade die effiziente Bewältigung dieses Problems in Deutschland gezeigt, dass Abhängigkeit nicht bedeutet, dass man ausgeliefert ist. Als weitere Punkte werden in dem Interview angesprochen:

- Innere Sicherheit in einer sich zunehmend vernetzenden Welt
- Notwendigkeit einer Vereinheitlichung der Rechtsnormen im Internet auf internationaler Ebene
- Möglichkeit eines Angriffs auf kritische IT-Infrastrukturen, Gefahren des Cyberwar
- Wirtschaftsspionage und die neue Rolle der Geheimdienste
- Aufgaben des BSI
- Zukunft und Notwendigkeit der Kryptoregulierung.

IDN:20010121

TYP:SEB

SGB:SW; DV

AUT:Büllingen, Franz; Hillebrand, Annette; Stamm, Peter

TIT:IT-Sicherheit als Standortfaktor; Die deutsche Kryptoindustrie im globalen Wettbewerb

FST:DuD

JAH:2000

JGG:24

HES:10, S. 598-602

BEI:3 TAF, 2 QU

PQU:Büllingen, F. u.a. - Position und Chancen der deutschen IT-Sicherheitsindustrie im globalen Wettbewerb, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi). Bad Honnef, WIK GmbH, 2000

FD:Volkswirtschaft; Wettbewerb; IT-Sicherheit; Sicherheitsindustrie; Kryptologie; Verschlüsselungsverfahren; Software; Anbieter; Wirtschaftspolitik; Marktordnung; Wirtschaftsstandort

TEXT:Die Studie "Position und Chancen der deutschen IT-Sicherheitsindustrie im globalen Wettbewerb" gliedert sich in folgende Themen:

- Gesamtwirtschaftliche Bedeutung der deutschen Kryptoindustrie
- Kryptopolitik in Deutschland
- Trends der US-Kryptoindustrie
- Forschung und Entwicklung.

Das Fazit sieht folgendermaßen aus:
Es sollen Verschlüsselungsverfahren und -produkte ohne Restriktionen entwickelt, hergestellt, vermarktet und genutzt werden dürfen. Diese ordnungspolitische Entscheidung stellt die effizienteste Maßnahme zur Stärkung der Position und Leistungsfähigkeit der deutschen Kryptoanbieter dar und bietet eine wichtige Grundlage für alle weiteren, diesem Ziel dienenden Maßnahmen. Auch wenn die Unternehmen eine liberale Kryptopolitik als wichtigsten politischen Beitrag zur Unterstützung ihrer Wettbewerbsposition bewerten, darf die Wirkung dieser "weichen" Maßnahmen nicht unterschätzt werden. Als erster Erfolg kann gewertet werden, dass es immer mehr gelingt, das Thema "IT-Sicherheit" in das Zentrum der öffentlichen Diskussion zu rücken.

IDN:20000621

TYP:AUF

SGB:SW; KO; DV

AUT:Winkel, Olaf

TIT:Die Gewährleistung von Datensicherheit für Unternehmen und öffentliche Verwaltung – ein unterschätztes Problem; Wirtschaftsspionage auf dem Vormarsch

FST:Europäische Beiträge zu Kriminalität und Prävention

JAH:1998

HES:4, S. 17-22

BEI:31 QU

FD:Datensicherheit; Netzwerk; Gefahrenpotential; Wirtschaftsspionage; Datenfernübertragung; Internet; Datenspionage; Kommunikationsnetz; Hacker; Sicherheitsplanung; Präventionsmaßnahme

TEXT:In dem Maße, wie gesellschaftliche Transaktionen über informationstechnische Netzwerke abgewickelt werden, gewinnt die Frage nach der Sicherheit von Informationen und Kommunikationsbeziehungen eine neue Qualität. Ein besonderes Problem stellt die Wirtschaftsspionage dar, die unter den veränderten technischen Vorzeichen des elektronischen Zeitalters zunehmend neue und effektivere Wege geht. Um die durch sie verursachten Schäden einzudämmen und geeignete Voraussetzungen für die Verbreitung von Electronic Commerce und Teleadministration zu schaffen, müssen die Unternehmen und Behörden die bestehenden Sicherheitslücken schließen und ein modernes Sicherheitsmanagement implementieren. Gerade kleine und mittlere Betriebe und Kommunalverwaltungen unterer Größenklassen sind dabei aber auf externe Unterstützung angewiesen. Da erfolgreiche Interventionen Wissen über die konkreten Probleme voraussetzen, sollten Stand und Perspektiven der Telekooperationssicherheit in Wirtschaft und Verwaltung näher untersucht werden.

Aspekte des E-Commerce

IDN: 20020566

TYP: AUF

SGB: RE

AUT: Spindler, Gerald

TIT: Das Gesetz zum elektronischen Geschäftsverkehr - Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip

FST: NJW

JAH: 2002

JGG: 55

HES: 13, S. 921-927

BEI: 97 QU

FD: Verantwortlichkeit; EG-Richtlinie; Anbieter; E-Commerce; Haftungsrecht; Informations- und Kommunikationsdienstegesetz; Teledienstegesetz

TEXT: Das Gesetz zum elektronischen Geschäftsverkehr novelliert unter anderem die Regelungen der Verantwortlichkeit der Diensteanbieter. Während sich auf den ersten Blick keine grundlegenden Änderungen gegenüber dem früheren Rechtszustand ergeben, zeigen sich bei näherer Analyse zahlreiche bedeutende Abweichungen, die zum Teil die Haftung verschärfen. Ein weiterer Kernpunkt liegt in der Einführung des Herkunftslandprinzips, das in zahlreichen Fällen das nationale Recht zurückdrängt. Dieser Beitrag befasst sich mit den Kernregelungen des EGG/Elektronischer Geschäftsverkehr-Gesetz, den Neuregelungen der Verantwortlichkeit der Diensteanbieter, flankiert von einem umfassenden Herkunftslandprinzip.

IDN:20010831

TYP:AUF

SGB:KK; DV

AUT:Koch, Karl Friedrich

TIT:Electronic Commerce; Chancen auch für Kriminelle?

FST:Kriminalistik

JAH:2001

JGG:55

HES:3, S. 179-185

BEI:1 TAF, 19 QU

FD:Elektronischer Zahlungsverkehr; E-Commerce; Internet; Bekämpfungskonzept; Datendiebstahl; Datenmanipulation; Kommunikationstechnik

TEXT:Im Rahmen einer Strategischen Kriminalitätsanalyse hatte sich das BKA im Dezember 1998 die Aufgabe gestellt, kriminalitätsfördernde Bedingungen zu identifizieren, die durch die Nutzung des Electronic Commerce entstanden sind. Die Wachstumsprognosen zum E-Commerce zeigen einen dynamischen Aufwärtstrend. Jedoch wird derzeit nur jeder zehnte elektronische Geschäftsabschluss mit privaten Endkunden getätigt. Eine abschließende Auflistung der kriminellen Möglichkeiten im Zusammenhang mit dem E-Commerce ist aufgrund der vielfältigen Nutzungsalternativen nicht möglich. Viele User betrachten das Internet als scheinbar "rechtsfreien" Raum, eine große Zahl hält die Abläufe bei der Geschäftsabwicklung für sicher. Besondere Probleme eröffnen sich im Zusammenhang mit der Sicherstellung und dem Beweiswert digitaler Dateien. Die am Projekt beteiligten Experten gehen von einem großen Dunkelfeld aus. Statistisch aussagekräftige Daten für eine realistische Lageeinschätzung liegen derzeit nicht vor. Die Bekämpfung des Deliktfeldes E-Commerce kommt nur langsam in Gang. Politik, Justiz und Polizei sind aufgefordert, sich intensiv mit diesen neuen Kriminalitätsphänomen auseinander zu setzen, um bestehende Konzepte und gesetzliche Bestimmungen zu überarbeiten bzw. die in der Analyse genannten Lösungsansätze umsetzen zu können.

IDN:20011069

TYP:AUF

SGB:DV; SW; RE

AUT:Miedbrodt, Anja; Mayer, Patrick

TIT:E-Commerce - Digitale Signaturen in der Praxis

FST:MDR

JAH:2001

JGG:55

HES:8, S. 432-436

BEI:44 QU

FD:Elektronischer Rechtsverkehr; Datenschutzrecht; Elektronischer Handel; Digitale Signatur; Signaturgesetz; Zertifizierung; Datensicherheit; Internet; Verschlüsselungsverfahren; Schlüsselverwaltung; EG-Richtlinie

TEXT:In den vergangenen Jahren hat der Geschäftsverkehr über offene elektronische Netze den Bereich der reinen Informationsübermittlung verlassen. Zunehmend werden auch online-Banking, Vertragsabschüsse und Steuererklärungen direkt über das Netz vorgenommen. Vertraulichkeit, Datenschutz, Nichtabstreitbarkeit abgegebener Erklärungen sowie die Authentizität und die Integrität der übermittelten Informationen sind wichtige Voraussetzungen für die geschäftliche Nutzung der Netze. Zertifizierungsstellen sollen als vertrauenswürdige Dritte Verbindungsglied der Kommunikationspartner sein, indem sie eindeutige und sichere Signierschlüssel ausstellen oder bestehende Schlüssel bestätigen. Auf Grund einer Signaturrichtlinie der EU vom 13.12.1999 hat nunmehr auch Deutschland am 09.03. 2001 ein auf dieser Richtlinie beruhendes Signaturgesetz beschlossen, welches sich im Wesentlichen auf die Voraussetzungen elektronischer Signaturen bezieht. Auch die übrigen EU-Mitgliedsstaaten müssen bis zum 19.07.2001 eine Umsetzung in nationales Recht vollzogen haben.

IDN:20002427

TYP:AUF

SGB:RE; KP

AUT:Bleiweiß, Christian

TIT:Rechtliche Aspekte des "Electronic Commerce"

FST:JA

JAH:2000

JGG:32

HES:6, S. 506-511

BEI:49 QU

FD:Electronic Commerce; Elektronischer Zahlungsverkehr; Urheberrecht; Rechtsgeschäft; Internet; Wettbewerbsrecht; Datenschutz; Verbraucherschutz

TEXT:Das Internet hat sich als virtueller Markt zum Online-Banking, Download von MP3-Sound-Dateien oder zur CD- oder Buchbestellung herausgebildet. Es stellt sich die Frage, ob diese Geschäfte nach dem deutschen Recht zu beurteilen sind, da sich die Vertragsparteien bei Internetkäufen in verschiedenen Ländern aufhalten und oft dritte Länder als virtuelle Plattformen für Abschlüsse herhalten. Die rechtliche Auseinandersetzung mit dem E-Commerce steht noch am Anfang. Das große Problem ist die Klärung, welches Recht anzuwenden ist, ein grenzüberschreitendes "Cyber-Law" ist aber aufgrund der Vielgestaltigkeit lokalen Rechts nahezu ausgeschlossen.

IDN:20010196

TYP:TAV

SGB:KP; KK

AUT:Arm, Harald

TIT:Electronic Commerce; Markt der Zukunft - auch für Kriminelle?

TAT:Forum 1999

ORT:Wiesbaden; BR Deutschland

DAT:1999 [15.06.-16.06.]

VER:BKA [Wiesbaden, BR Deutschland]

FST:Informationen aus dem Kriminalistischen Institut [Krilog 2.5-111-1999]

JAH:1999

HES:S. 11-26

FD:Elektronischer Handel; E-Commerce; Datensicherheit; Hacker; Internationale Zusammenarbeit; Internet; Digitalisierung; Elektronischer Zahlungsverkehr; Meldedienst; Digitale Unterschrift

TEXT:Eine deutlich ansteigende Anzahl von Geschäftsabwicklungen im Bereich des Electronic Commerce lässt den Schluss zu, dass in diesem Bereich künftig auch mehr kriminelle Aktivitäten festzustellen sein werden. Die Erkenntnisse zu diesem Kriminalitätsphänomen sind jedoch gering, denn ein realistischer polizeilicher Lagebericht steht nicht zur Verfügung und die Anzahl der über den IuK-Meldedienst bekannt gewordenen Straftaten weist pro Jahr lediglich zwischen 5 und 20 Delikten aus. Als kriminogene Faktoren haben sich neben der Basistechnologie und der Digitalisierung auch die Anonymität, die Virtualität und Ubiquität des Internet erwiesen. Die gesetzgeberischen Maßnahmen sind unzureichend, um E-Commerce wirkungsvoll bekämpfen zu können, wie auch die Präventions- bzw. Repressionsbestrebungen der Länder in diesem Deliktsfeld. Außer der Schaffung eines größeren Problembewusstseins ist es unabdingbar, die Sicherheitsvorkehrungen im Internet zu verbessern und die Anonymität zu reduzieren. Die polizeiliche Kompetenz - auch auf internationaler Ebene - muss ausgebaut werden, wobei internationale Standards auch für Sicherheitsaspekte benötigt werden. Die Gesetzgebung ist den Erfordernissen, insbesondere hinsichtlich der Auskunfts- und Speicherungspflicht, anzupassen. Für die Zulassung von Providern sollten spezielle Kriterien entwickelt werden.

IDN:20012080

TYP:SRR

SGB:KO; KK; KP

AUT:Autorengemeinschaft "Strategische Kriminalitätsanalyse"

TIT:Electronic Commerce; Markt der Zukunft - auch für Kriminelle?; Projektabschlussbericht des Teams "Strategische Kriminalitätsanalyse" des Bundeskriminalamtes

FST:BKA - Informationen aus dem Kriminalistischen Institut [Krilog 6.21-463]

JAH:1999

HES:141 S.

BEI:LITVZ S. 135-141

FD:Electronic Commerce; Internet; Datenschutz; Kriminalitätslage; Lagebild; Dunkelfeld; Anzeigeverhalten; Bekämpfungsmaßnahme; Präventivmaßnahme; Elektronischer Zahlungsverkehr; Kryptografie; Digitale Signatur

TEXT:Aus dem Inhalt:
- Electronic Commerce und das Internet als Rahmen (Internet-based commerce solutions) - erforderliche technische und organisatorische Komponenten für den Internet-Verkehr
- Anwendungsgebiete des E-Commerce
- Prognosen zur Entwicklung des E-Commerce
- Der Vergleich zwischen E-Commerce und herkömmlichem Handel
- Die Definition von Electronic Commerce für das SKA-Projekt
- Kriminogene Faktoren und mögliche Kriminalität im Zusammenhang mit Electronic Commerce
- Kriminalitätslage, Bekämpfungssituation, Handlungsbedarf und Lösungsansätze, Bewertung der Erkenntnisse aus dem Projekt, Umsetzungsmaßnahmen
- Sonstige Dienste des Internet
- Formen des elektronischen Zahlungsverkehrs
- Kryptografie
- Digitale Signatur

Verzeichnis der Fundstellen

Zitiertitel	*Vollständiger Titel des Periodikums*
Bürgerrechte und Polizei	Bürgerrechte und Polizei
CD Sicherheits-Management	CD Sicherheits-Management
CR	Computer und Recht - Zeitschrift für die Praxis des Rechts der Informationstechnologien
DANA	Datenschutz Nachrichten
Die Kriminalpolizei	Die Kriminalpolizei - Vierteljahreszeitschrift der Gewerkschaft der Polizei
Die Kriminalprävention	Die Kriminalprävention - Europäische Beiträge zu Kriminalität und Prävention, Zeitschrift des Europäischen Zentrums für Kriminalprävention
Die Polizei	Die Polizei - Fachzeitschrift für die öffentliche Sicherheit mit Beiträgen aus der Polizei-Führungsakademie
DNP	Die Neue Polizei - Die aktuelle Fachzeitschrift für die Aus- und Fortbildung
DRiZ	Deutsche Richterzeitung - Organ des Deutschen Richterbundes, Bund der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte
DSWR	DSWR - Datenverarbeitung Steuer Wirtschaft Recht, Zeitschrift für Praxisorganisation, Betriebswirtschaft und elektronische Datenverarbeitung
DuD	DuD - Datenschutz und Datensicherheit, Recht und Sicherheit in Informationsverarbeitung und Kommunikation
Europäische Beiträge zu Kriminalität und Prävention	Europäische Beiträge zu Kriminalität und Prävention
GA	Goltdammer's Archiv für Strafrecht
Informationen aus dem Kriminalistischen Institut	Informationen aus dem Kriminalistischen Institut
JA	JA - Juristische Arbeitsblätter, Zeitschrift für Studenten und Referendare
KES	kes - Die Zeitschrift für Informations-Sicherheit
Kriminalistik	Kriminalistik - Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis
MDR	Monatsschrift für Deutsches Recht - Zeitschrift für die Zivilrechtspraxis
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
PFA-Schlussbericht	Schlussbericht / Polizei-Führungsakademie
Polizeispiegel	Polizeispiegel / Deutsche Polizeigewerkschaft im DBB
Spektrum der Wissenschaft	Spektrum der Wissenschaft
WIK	WIK - Zeitschrift für die Sicherheit der Wirtschaft
ZFIS	ZFIS - Zeitschrift für Innere Sicherheit in Deutschland und Europa
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Abkürzungsverzeichnis

IDN **Identifikationsnummer**
Eindeutige Kennzeichnung eines Literaturnachweises

TYP **Dokumenttyp**
Art der dokumentierten Veröffentlichung. Hier:

AUF - Aufsatz	VOR - Vortrag	TAV - Tagungsvortrag
INT - Interview	SEB - Sekundärbericht	GUS - Gesetzgebungsübersicht
SRR - Schriftenreihe	ENT - Entscheidungsbesprechung	

REG **Regionenzuordnung**
Themenkreis bezieht sich auf Ausland und/oder Inland

SGB **Sachgebiet**
Schwerpunkt des Dokuments. Hier:

DV - Datenverarbeitung	KK - Kriminalistik	KO - Kriminologie
KP - Kriminalpolitik	PT - Polizeitechnik	RE - Recht
SW - Sicherheitswesen		

AUT **Autor oder Autorengemeinschaft**

TIT **Titel**
Hauptsachtitel und gegebenenfalls Untertitel

TAT **Tagungstitel**

ORT **Tagungsort**

DAT **Tagungsdatum**

VER **Tagungsveranstalter**

FST **Fundstelle** (s. Fundstellenverzeichnis S. 72)

JAH **Erscheinungsjahr**

JGG **Jahrgang / Band**

HES **Heft / Seitenangabe**

BEI **Beigaben**
BILDer; ***TAB***ellen; ***TAF***eln; ***K***ar***T***en; Literatur***QU***ellen; ***LIT***eratur***V***er***Z***eichnis; ***ANL***agen

PQU **Primärquellenverweis**

FD **Freie Deskriptoren**
Inhaltskennzeichnende Suchbegriffe

TEXT **Kurzreferat**