

# Kriminalität im Internet

[14.05.2001]

In den 60er Jahren beabsichtigte das amerikanische Verteidigungsministerium die militärische Nutzbarkeit von Computernetzwerken zu verbessern. Aus der Erkenntnis heraus, dass die Landesverteidigung von miteinander verbundenen Computersystemen abhängig war, sollte ein System entwickelt werden, das auch bei Ausfall von einzelnen Verbindungen, Leitungen oder Netzknotenpunkten die Kommunikationsfähigkeit bzw. die Verbindung von Militärrechnern sichert. Beauftragt wurden seinerzeit mehrere amerikanische Universitäten, dadurch erhielt das so entstehende Netz neben seiner militärischen auch eine wissenschaftliche Funktion. In den 80er Jahren zog sich das Militär dann aus dem Internet zurück und richtete eigene, vom Internet abgetrennte Netze ein, um den universitären Bereich von der Landesverteidigung zu trennen.

Die Philosophie derjenigen, die nun noch das Internet nutzen war vom Ziel einer offenen Kommunikation geprägt. Informationen sollten frei zugänglich sein, Autoritäten wie Politik, Militär und Justiz sei zu misstrauen. Jegliches Eingreifen wurde als Zensurmaßnahme eingestuft, als Störung empfunden und mit einer Umleitung umgangen. Diese von den Internet-Nutzern gewollte Freiheit, die man auch als Rebellion oder Anarchie bezeichnen könnte, führte zu dem weitverbreiteten Schlagwort des "rechtsfreien Raums Internet", da sie eine staatliche Kontrolle weitgehend unmöglich macht. Unter den Internet-Nutzern ist diese Philosophie noch heute weit verbreitet.

Das Internet ist aber kein "rechtsfreier Raum". Ziel der freiheitlich demokratischen Grundordnung der Bundesrepublik Deutschland ist es, den Menschen ein selbstbestimmtes, freies Leben zu ermöglichen. Zum Schutze dieser Freiheit haben wir uns daher Gesetze gegeben, die das Leben in seinem Miteinander, Nebeneinander und manchmal Gegeneinander regeln sollen.

Auch für das Internet, für die Kommunikation mit Hilfe dieser neuen Techniken gelten diese Gesetze schon heute. Das Internet ist insofern nie ein "rechtsfreier Raum" gewesen. Die Durchsetzbarkeit von Gesetzen stößt jedoch sehr oft auf technische Hindernisse. Die Internationalität des Internet weist darüber hinaus allen nationalen Regelungen ihre Grenzen auf.

Während die Globalisierung es den internationalen Kriminellen ermöglicht hat, praktisch ohne Grenzen zu agieren, sind Regierungen und Strafverfolgungsbehörden weiterhin auf ihre nationalen Grenzen beschränkt. Die Polizeibehörden können mit den technisch auf höchstem Stand operierenden Organisationen nicht mithalten.

Der Missbrauch der neuen Technologien stellt die Polizei und die Rechtsprechung auf der ganzen Welt vor bislang unbekannte Probleme, da sie es mit hoch spezialisierten Kriminellen und mit unglaublich komplizierten Technologien zu tun haben.

## **Straftaten im und unter Ausnutzung des Internet:**

- gewaltverherrlichende Darstellungen
- Verbreitung / Besitz von Kinderpornographischen Dateien
- Veröffentlichung rechts- und linksextremistischer sowie ausländerfeindlicher Inhalte
- Wirtschaftskriminalität und Betrug im Zusammenhang mit e-commerce

- Softwarepiraterie und sonstige Urheberrechtsverletzungen
- Betäubungsmittel- und Waffenkriminalität
- Hacking und Computersabotage
- Verbotene Glücksspiele
- Organisierte Kriminalität
- persönliche anonyme Bedrohungen und daraus resultierende Nötigungstatbestände
- Geldwäsche

Ein Consulting-Unternehmen in Washington untersuchte im Jahr 2000 die Behauptung, dass es derzeit auf internationaler Ebene an umfassenden Antworten auf die Kriminalität im Internet fehle. Heraus kam, dass es von 52 Staaten 33 bis heute versäumt haben, überhaupt Strafgesetze für Computerkriminalität zu schaffen. Zehn der übrigen Staaten haben bislang nur fünf oder weniger Cybervergehen erfasst. Gerade einmal neun Länder kannten Tatbestände für sechs oder mehr Computerstraftaten. Die USA kannten immerhin neun von zehn Cybervergehen bzw. -verbrechen.

Solange Cyberkriminalität nicht grenzüberschreitend strafrechtlich erfasst wird, ist eine internationale Verfolgung unmöglich!

Eindringlichstes Beispiel dafür sind die Seiten im Internet, auf denen gewaltverherrlichende, rechtsextremistische oder pornographische Inhalte über Internet verbreitet werden. Die Inhalte werden sehr oft über Rechner in das Internet eingestellt, die sich in den USA befinden. Bei der komplizierten Rückverfolgung der Spuren, die auf die Anbieter solcher Internetseiten hinweisen, stoßen die Strafverfolgungsbehörden in Deutschland immer an ihre rechtlichen Grenzen. In den USA sind viele der bei uns strafrechtlich relevanten Tatbestände durch die dort sehr weit ausgelegte Meinungsfreiheit geschützt. Ein Rechtshilfeersuchen scheitert in solchen Fällen stets daran, dass die USA nur Rechtshilfe bei solchen strafrechtlichen Ermittlungen gewährt, in denen die Tatbestände nicht nur in Deutschland, sondern auch in den USA unter Strafe gestellt sind. Ein Zustand, der für jeden, der eine solche Internetseite einmal gesehen hat, unerträglich und nicht hinnehmbar ist. Juristisch bestehen jedoch keine Möglichkeiten dagegen vorzugehen.

Auch rein praktisch dürfte die weitere Verbreitung solcher Seiten auch in Deutschland und damit der freie Zugang über das Internet kaum zu verhindern sein. Wie bereits oben beschrieben, herrscht im Internet die Philosophie vor, dass jegliches Eingreifen als Zensurmaßnahme eingestuft, als Störung empfunden und darauf mit einer Umleitung reagiert wird. Selbst wenn also einzelne Provider in Deutschland sich weigern würden, die entsprechenden Seiten weiterzuleiten, würden sich sicherlich andere, nicht so namhafte Anbieter finden, die stattdessen die Seiten weiterleiten. Auch die User würden sicherlich in solchen Fällen verstärkt versuchen, genau auf diese Seite zurückzugreifen, nicht der Inhalte wegen, die sie vielleicht im Einzelfall auch ablehnen mögen, aber infolge der Grundphilosophie.

#### **Cyberkriminalität in Zahlen:**

Der Anstieg der Cyberkriminalität in den ersten drei Quartalen im Jahr 2000 betrug gegenüber allen 1999 bekannt gewordenen Internet-Straftaten 54 Prozent. In den kommenden vier Jahren wird ein Anstieg der Cyberkriminalität um 100 Prozent vorausgesagt.

Schon heute beträgt der durch Cyberkriminalität verursachte Schaden nach Experten-Schätzungen 100 Milliarden Mark jährlich.

Im Jahr 1999 hat das BKA bei 80 Prozent registrierten Fälle von Kriminalität im Internet Spuren in die USA, nach Kanada, Japan und Russland verfolgt.

Die Entwicklung der Kriminalität folgt der technischen Entwicklung, während staatliche Gegenmaßnahmen erst mit einem gewissen Zeitabstand folgen.

#### **Europarat und Europäische Kommission:**

Die Europäische Kommission veröffentlichte im Januar 2001 einen Vorschlag zur Bekämpfung computerbezogener Verbrechen. Ein europäisches Forum, bestehend aus Strafverfolgungsbehörden, Telekommunikations-Service-Providern, Konsumentengruppen und Datenschützern soll die Kooperation auf europäischer Ebene verstärken.

#### **In einem Entwurf für den Vertrag über Cyberkriminalität des Europarates werden Angleichungen der Gesetze auf dem Gebiet der High-Tech-Kriminalität in vier Bereichen gefordert:**

- Verbrechen gegen die Vertraulichkeit und Integrität von Computerdaten und -systemen;
- mittels Computer begangene Verbrechen;
- illegale Inhalte;
- Verbrechen im Zusammenhang mit dem Schutz geistigen Eigentums und verwandter Rechte.

Der Europäischen Kommission gehen diese Vorhaben nicht weit genug. Sie will noch in diesem Jahr neue Vorschläge zur Bekämpfung der Kinderpornographie als einen ersten Schritt zur Harmonisierung nationaler Gesetze unterbreiten. Auch gegen Fremdenfeindlichkeit und Rassismus im Internet will sie vorgehen. Es laufen auch Überlegungen, wie die Bemühungen im Kampf gegen illegalen Drogenhandel über das Internet verbessert werden können. Die Kommission unterstützt die Schaffung neuer Abhörmöglichkeiten bei neuen Technologien und kommt zu der Feststellung, dass internationale Koordination nötig sei, um an die Service-Provider und Telekommunikationsunternehmen neue technische Abhörerforderungen stellen zu können.

#### **Es besteht zur Zeit noch keine feste Meinung zu folgenden Angelegenheiten:**

- anonymer Zugang und Nutzung des Internet,
- grenzüberschreitende Durchsuchung,
- Speicherung von Verbindungsdaten.

Es wurde festgehalten, dass diese schwierigen Fragen zunächst von den Strafverfolgungsbehörden und der Industrie zu diskutieren seien, um akzeptable Lösungen zu finden, bei denen sich Rechte und Pflichten in der Waage halten.

#### **Erweiterung der Zuständigkeit von EUROPOL:**

Die Europäische Kommission unterstützt auch die Erweiterung der Zuständigkeit von EUROPOL für Cyberkriminalität. Frankreich sieht die Rolle von EUROPOL vor allem programmatisch. Sie soll darin bestehen, eine Basis für die operative Begegnung der Probleme im Kampf gegen Cyberkriminalität zur Verfügung zu stellen.

#### **Angriffe auf automatisierte Datenverarbeitungsvorgänge**

- das Schreiben und die Verbreitung von Viren,

- Einbrüche in, Veränderung von oder Manipulationen an fremden Betriebssystemen,
- Veränderungen von Datenbeständen sind bislang außerhalb der Reichweite von EUROPOL'S Mandat.

Die offizielle Definition von Computerkriminalität in diesem Zusammenhang soll lauten, "alle Arten von Angriffen auf automatisierte Datenverarbeitungssysteme".

Der Vorstand von EUROPOL soll nun weitere Ratschläge bzgl. der französischen Vorschläge ausarbeiten und feststellen, welche Auswirkungen dies für EUROPOL, seine Mitarbeiter und das Budget hätte, bevor der Europäische Rat für Justiz und Inneres eine formelle Vereinbarung über diese neue Aufgabe für EUROPOL schließen kann.

EUROPOL wird dann das Mandat haben, Informationen über Computerangriffe zwischen den Mitgliedsstaaten auszutauschen. Darüber hinaus wird EUROPOL dann sowohl analytische Arbeitsdaten über Computerangriffe sammeln, die für strategische Zwecke gedacht sind, als auch operationale Arbeitsdaten, die grenzüberschreitenden Ermittlungen dienen.

#### **Eckpunkte für eine gewerkschaftspolitische Diskussion:**

- Die Polizei muss in die Lage versetzt werden mit den technischen Entwicklungen Schritt zu halten. Durch die polizeiliche Präsenz im Netz muss Druck auf potentielle Straftäter erzeugt und sie müssen verunsichert werden. Dazu sind bei konkreten Verdachtslagen aber auch anlaßunabhängig Recherchen durchzuführen ("Netzwerkfahndung"). Allen muss bekannt werden, dass das, was im Leben strafbar ist, auch im Netz strafbar ist.
- Dringend erforderlich sind Internetzugänge für alle Polizeidienststellen, die entsprechenden Haushaltsmittel für die IT-Ausstattung der Polizei müssen durch die Politik bereitgestellt werden. Alle Polizeibeschäftigten müssen an das Internet herangeführt werden, evtl. Berührungspunkte der Kolleginnen und Kollegen im Zusammenhang mit dem Einsatz moderner Technik sind zu berücksichtigen. Die interne und externe Fortbildung im IT-Bereich muss ausgebaut werden.
- Service- bzw. Schwerpunktdienststellen sind zu schaffen, in denen eigene IT-Experten flächendeckend anlassbezogen die Ermittlungstätigkeiten unterstützen. Das dazu erforderliche Personal ist bereitzustellen, daneben sind Meldestellen für IUK-Kriminalität im Internet zu schaffen.
- Die Globalisierung der Kriminalität erfordert eine Zusammenarbeit der Polizei auf europäischer und internationaler Ebene. Diese ist durch bessere Koordinierung und effektivere Strafverfolgung sowie gleiche Vorgehensweise aller Polizistinnen und Polizisten bei Strafverfolgungsmaßnahmen herbeizuführen. Eine gesetzliche Harmonisierung innerhalb der G8-Staaten ist dringend erforderlich. Dazu zählt auch die Kriminalisierung von Computer-Straftaten innerhalb und außerhalb der G8-Staaten.
- Ein bundeseinheitliches Lagebild unter Einbeziehung von Erkenntnissen der Dunkelfeldforschung ist zu erstellen, die Internetkriminalität sollte durch Europol analysiert werden, es sollte ein regelmäßiger Austausch von Beweisdaten erfolgen.
- In Zusammenarbeit mit den Providern sollten technische Standards geschaffen werden, die die öffentliche Sicherheit unterstützen. Dazu gehört auch eine Fortschreibung der Regelungen des § 12 Fernmeldeanlagen-gesetz (FAG). Die Provider sollten gesetzlich verpflichtet werden, Verbindungsdaten nicht nur zu Rechnungslegungszwecken aufzubewahren, sondern auch, um Verbindungsdaten an die Polizei zu Ermittlungszwecken übermitteln zu können.

- Bildidentifizierungs- bzw. Filterprogramme sind zu entwickeln, weiterzuentwickeln und zu beschaffen, um gewaltverherrlichende, pornographische und rechtsextremistische Inhalte effektiver verfolgen und bekämpfen zu können.
- Es sind einwandfreie Methoden der Beweissicherung zu entwickeln, insbesondere unter Berücksichtigung von Kryptierungsproblematiken.
- Die gesetzlichen Grundlagen müssen weiterentwickelt werden. Davon betroffen sind u.a. die Katalogtaten des § 100 a StPO im Bereich Kinder- und Gewaltpornographie, im der Bereich der Computersabotage und des § 12 FAG. Außerdem sind klare gesetzliche Ermächtigungen für die Erhebung der Log-Files zu schaffen und der Opferschutz zu stärken.

**Der Bundesvorstand hat den vorstehenden Diskussionsgrundlagen in seiner Sitzung am 09./10.05.2001 zugestimmt.**