



KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 26.1.2001  
KOM(2000) 890 endgültig

**MITTEILUNG DER KOMMISSION  
AN DEN RAT, DAS EUROPÄISCHE PARLAMENT,  
DEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND  
DEN AUSSCHUSS DER REGIONEN**

**Schaffung einer sichereren Informationsgesellschaft durch  
Verbesserung der Sicherheit von Informationsinfrastrukturen und  
Bekämpfung der Computerkriminalität**

**eEurope  
2002**

## **Einführung**

Der Übergang Europas zur Informationsgesellschaft zeichnet sich durch weitreichende Entwicklungen in allen Bereichen des menschlichen Lebens aus: in Beruf, Bildung und Freizeit ebenso wie in Staatsführung, Industrie und Handel. Die neuen Informations- und Kommunikationstechniken revolutionieren unsere Volkswirtschaften und Gesellschaften von Grund auf. Der erfolgreiche Aufbau der Informationsgesellschaft ist für Europa von großer Bedeutung im Hinblick auf das Wachstum und die Wettbewerbsfähigkeit seiner Wirtschaft und die Schaffung von Arbeitsplätzen, und er hat weitreichende Auswirkungen in wirtschaftlicher, gesellschaftlicher und rechtlicher Hinsicht.

Im Dezember 1999 startete die Kommission ihre Initiative "eEurope", um sicherzustellen, daß Europa die digitalen Technologien nutzen und eine Informationsgesellschaft entstehen kann, die frei von jedweder Diskriminierung ist. Im Juni 2000 billigte der Europäische Rat auf seiner Tagung in Feira den umfassenden "eEurope"-Aktionsplan und forderte seine Durchführung bis 2002. Der Aktionsplan befaßt sich schwerpunktmäßig mit der Sicherheit von Netzen und der Bekämpfung der Cyberkriminalität.

Informations- und Kommunikationsinfrastrukturen sind heute ein wichtiger Bestandteil unserer Volkswirtschaften. Leider haben auch sie ihre Schwächen, und diese bieten neue Angriffspunkte für kriminelle Handlungen. Diese Handlungen können vielfältige Formen annehmen und grenzübergreifenden Charakter besitzen. Obwohl es aus verschiedenen Gründen keine zuverlässigen Statistiken über derartige Delikte gibt, besteht nur wenig Zweifel daran, daß sie eine Bedrohung für die Investitionen und die Vermögenswerte der Wirtschaft darstellen und die Sicherheit und das Vertrauen in die Informationsgesellschaft gefährden. So haben beispielsweise die jüngsten Angriffe auf Dienste und Virusangriffe großen finanziellen Schaden verursacht.

Mithin besteht in doppelter Hinsicht Handlungsbedarf: Zum einen gilt es, durch Verstärkung der Sicherheit von Informationsinfrastrukturen kriminellen Handlungen vorzubeugen, und zum anderen muß dafür Sorge getragen werden, daß die Strafverfolgungsbehörden über geeignete Mittel verfügen, um unter Wahrung der Grundrechte des einzelnen wirksam gegen derartige Handlungen vorgehen können.

Die Europäische Union hat bereits verschiedene Maßnahmen ergriffen, um schädliche und illegale Inhalte im Internet zu bekämpfen, geistiges Eigentum und personenbezogene Daten zu schützen, den elektronischen Handel und die Verwendung elektronischer Signaturen zu fördern und die Sicherheit von Transaktionen zu erhöhen. Im April 1998 legte die Kommission dem Rat die Ergebnisse einer Studie über die Computerkriminalität ("COMCRIME-Studie") vor. Im Oktober 1999 stellte der Europäische Rat in den Schlußfolgerungen zu seiner Tagung von Tampere fest, daß sich die Bemühungen zur Vereinbarung gemeinsamer Definitionen und Sanktionen auch auf den Bereich der High-Tech-Kriminalität konzentrieren sollten. Das Europäische Parlament hat präzise und allgemein akzeptierte Definitionen EDV-bezogener Straftatbestände sowie eine effiziente Angleichung der einschlägigen (Straf-)Rechtsvorschriften gefordert. Der Rat der Europäischen Union hat einen Gemeinsamen Standpunkt zu den Verhandlungen im Europarat über das Übereinkommen über Cyberkriminalität sowie erste Maßnahmen im Rahmen der unionseigenen Strategie gegen die High-Tech-Kriminalität angenommen. Einige Mitgliedstaaten der EU haben eine führende Rolle bei den diesbezüglichen Maßnahmen der G8 gespielt.

Diese Mitteilung befaßt sich mit der Notwendigkeit und möglichen Formen einer umfassenden politischen Initiative im Zusammenhang mit den allgemeinen Zielen, die sich die Union in bezug auf die Schaffung der *Informationsgesellschaft* und eines *Raums der Freiheit, der Sicherheit und des Rechts* gesetzt hat, um unter Wahrung der fundamentalen Menschenrechte die Sicherheit von Informationsinfrastrukturen zu verbessern und die Cyberkriminalität zu bekämpfen.

Die Kommission ist der Ansicht, daß auf kurze Sicht die klare Notwendigkeit besteht, ein Rechtsinstrument der EU zu schaffen, durch das gewährleistet wird, daß die Mitgliedstaaten mit wirksamen Sanktionen gegen die Kinderpornographie im Internet vorgehen können. Zu diesem Zweck wird die Kommission noch in diesem Jahr einen Vorschlag für einen Rahmenbeschluß vorlegen, der in Zusammenhang mit einem Maßnahmenpaket zur Bekämpfung der sexuellen Ausbeutung von Kindern und des Menschenhandels steht und Bestimmungen über die Angleichung der Vorschriften und der Sanktionen enthält.

Langfristig plant die Kommission Legislativvorschläge zur weiteren Angleichung der materiellen Strafrechtsvorschriften für den Bereich der High-Tech-Kriminalität vorzulegen. In Übereinstimmung mit den Schlußfolgerungen des Europäischen Rats von Tampere vom Oktober 1999 wird die Kommission zudem die Optionen für eine gegenseitige Anerkennung von im Rahmen von Ermittlungsverfahren im Zusammenhang mit Cyberkriminalität ergangenen Anordnungen prüfen.

Parallel dazu beabsichtigt die Kommission, darauf hinzuwirken, daß in den Ländern, in denen noch keine auf die Bekämpfung der Computerkriminalität spezialisierten Polizeidienste bestehen, derartige Dienste auf nationaler Ebene eingerichtet werden, und sie beabsichtigt zudem, geeignete Schulungsmaßnahmen für Strafverfolgungsbeamte zu fördern und europaweite Aktionen zum Thema Informationssicherheit anzuregen.

Auf technischer Ebene wird die Kommission in Übereinstimmung mit dem rechtlichen Rahmen Maßnahmen zur Sensibilisierung von Forschern und Entwicklern sowie zur Verbreitung von Fachwissen ergreifen, um die Anfälligkeit der neuen Technologien gegenüber der Computerkriminalität zu mindern.

Die Kommission beabsichtigt zudem, die Strafverfolgungsbehörden, die Anbieter von Internet-Diensten, die Telekommunikationsbetreiber, Bürgerrechtsorganisationen, die Vertreter der Verbraucher und der Datenschutzbehörden sowie andere interessierte Parteien in einem eigens eingerichteten EU-Forum zusammenzubringen, um ihr gegenseitiges Verständnis und die Zusammenarbeit auf EU-Ebene zu fördern. Ziel des Forums wird es auch sein, das öffentliche Bewußtsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, optimale Sicherheitsbedingungen zu schaffen, Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität aufzuzeigen und die Weiterentwicklung von Frühwarnsystemen und Mechanismen der Krisenbewältigung anzuregen.

## **AUFFORDERUNG ZUR STELLUNGNAHME ZU DIESER MITTEILUNG**

**Die Europäische Kommission fordert die interessierten Parteien auf, zu den in dieser Mitteilung angesprochenen Fragen Stellung zu nehmen. Die Anmerkungen können bis spätestens 23.03. 2001 per E-Mail an folgende Adresse geschickt werden:**

infso-jai-cybercrime-comments@cec.eu.int

**Alle Beiträge werden im Internet veröffentlicht, sofern sich der Absender nicht gegen die Veröffentlichung ausspricht. Anonyme Anmerkungen werden nicht veröffentlicht. Die Kommission behält sich das Recht vor, bei bestimmten Beiträgen (beispielsweise beleidigender Natur) von einer Veröffentlichung abzusehen. Die Anmerkungen werden unter folgender Adresse ins Netz gestellt:**

<http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html>

**Dort werden auch Vorschläge in bezug auf das technische Format sowie nähere Einzelheiten zur Veröffentlichungspolitik aufgeführt. Es wird empfohlen, vor Einsendung etwaiger Anmerkungen diese Website zu besuchen.**

## **ÖFFENTLICHE ANHÖRUNG**

**Die Europäische Kommission veranstaltet des weiteren am 07.03. 2001 eine öffentliche Anhörung interessierter Parteien zu den in der Mitteilung angesprochenen Fragen. Einladungsschreiben zur Einreichung einer Erklärung bei der Anhörung können bis spätestens 20.02. 2001 per E-Mail unter folgender Adresse angefordert werden:**

infso-jai-cybercrime-hearing@cec.eu.int

**Auf dem Postwege können Einladungsschreiben unter folgender Adresse angefordert werden:**

**Europäische Kommission  
Büro BU 33-5/9  
200 Wetstraat/Rue de la Loi  
B-1049 Brüssel  
Belgien**

**Die Europäische Kommission behält sich das Recht vor, die anzuhörenden Parteien nach Zahl der Anträge und nach Themenabdeckung auszuwählen.**

# INHALT

## **Einführung**

- 1. CHANCEN UND GEFAHREN IN DER INFORMATIONSGESELLSCHAFT**
  - 1.1. Antworten auf nationaler und internationaler Ebene**
- 2. DIE SICHERHEIT VON INFORMATIONSinFRASTRUKTUREN**
- 3. COMPUTERKRIMINALITÄT**
- 4. FRAGEN DES MATERIELLEN STRAFRECHTS**
- 5. STRAFVERFAHRENSRECHTLICHE FRAGEN**
  - 5.1. Überwachung des Fernmeldeverkehrs**
  - 5.2. Aufbewahrung von Verkehrsdaten**
  - 5.3. Anonymer Zugang und anonyme Nutzung**
  - 5.4. Die praktische Zusammenarbeit auf internationaler Ebene**
  - 5.5. Strafverfahrensrechtliche Befugnisse und Rechtsprechung**
  - 5.6. Die Beweiskraft von Computerdaten**
- 6. NICHTLEGISLATIVE MAßNAHMEN**
  - 6.1. Spezialisierte Dienststellen auf nationaler Ebene**
  - 6.2. Fachliche Schulung**
  - 6.3. Verbesserte Informationen und gemeinsame Regeln für die Datenaufbewahrung**
  - 6.4. Zusammenarbeit zwischen den verschiedenen Akteuren: das EU-Forum**
  - 6.5. Direkte Maßnahmen der Industrie**
  - 6.6. Von der EU geförderte FTE-Projekte**
- 7. SCHLUßFOLGERUNGEN UND VORSCHLÄGE**
  - 7.1. Vorschläge für legislative Maßnahmen**
  - 7.2. Vorschläge für nichtlegislative Maßnahmen**
  - 7.3. Maßnahmen in sonstigen internationalen Foren**

## 1. CHANCEN UND GEFAHREN IN DER INFORMATIONSGESELLSCHAFT

Die zunehmende Verfügbarkeit und Nutzung von Informationsgesellschaftstechnologien (IST) sowie die wirtschaftliche Globalisierung sind typische Merkmale unserer Zeit. Die weitere technologische Entwicklung und die vermehrte Nutzung von offenen Netzen wie dem Internet wird in den nächsten Jahren große Chancen und neue Herausforderungen mit sich bringen.

Im März 2000 unterstrich der Europäische Rat auf seinem Gipfeltreffen in Lissabon die Bedeutung des Übergangs zu einer wettbewerbsfähigen, dynamischen und wissensbasierten Wirtschaft, und er ersuchte den Rat und die Kommission, einen umfassenden "eEurope"-Aktionsplan zu erstellen, um diese Chance bestmöglich zu nutzen<sup>1</sup>. Der Aktionsplan, der von der Kommission und vom Rat ausgearbeitet und vom Europäischen Rat auf dem Gipfeltreffen von Feira im Juni 2000 angenommen wurde, sieht verschiedene Maßnahmen zur Verbesserung der Sicherheit von Netzen sowie die Ausarbeitung eines koordinierten und kohärenten Konzepts für die Bekämpfung der Cyberkriminalität bis Ende 2002 vor<sup>2</sup>.

Die Informationsinfrastruktur bildet heute eine wichtige Stütze unserer Volkswirtschaften. Die Nutzer müssen sich darauf verlassen können, daß die Informationsdienste verfügbar sind und daß der Fernmelde- und Datenverkehr vor unberechtigtem Zugang oder Manipulationen sicher ist. Von dieser Frage hängt auch ab, wie sich der elektronische Handel weiterentwickelt und ob es gelingt, die Informationsgesellschaft in vollem Umfang zu verwirklichen.

Die neuen digitalen und drahtlosen Techniken sind bereits allgegenwärtig. Sie geben uns die Möglichkeit, stets mobil zu sein und zugleich Zugang zu unzähligen Diensten in ebenso unzähligen Netzen zu haben. Sie erleichtern das Partizipieren, das Lehren und Lernen, das gemeinsame Spiel und die Zusammenarbeit sowie politisches Engagement. Da unsere Gesellschaften immer häufiger auf diese Technologien zurückgreifen, müssen wirksame praktische und rechtliche Mittel eingesetzt werden, um den bestehenden Risiken entgegenzuwirken.

Informationsgesellschaftstechnologien (IST) können dazu genutzt werden, kriminelle Handlungen zu begehen oder zu erleichtern, und sie werden auch bereits dafür genutzt. In den Händen nicht in gutem Glauben, vorsätzlich oder grob fahrlässig handelnder Personen können diese Technologien für Handlungen mißbraucht werden, die das Leben, das Eigentum oder die Würde anderer gefährden oder verletzen bzw. dem öffentlichen Interesse schaden.

Das klassische Sicherheitskonzept sieht eine strenge organisatorische, geografische und strukturelle Einteilung von Informationen nach Art und Grad der Vertraulichkeit vor. In der heutigen digitalen Welt ist eine Einteilung in dieser Form nicht mehr machbar, da die Verarbeitung der Informationen durch eine Vielzahl weit verteilter Stellen erfolgt, die angebotenen Dienste voll auf die Bedürfnisse der mobilen Nutzer zugeschnitten sind und die Interoperabilität der Systeme eine absolute Voraussetzung ist. Innovative Lösungen auf der Grundlage neuer Technologien lösen zunehmend die traditionellen Sicherheitskonzepte ab. Sie verwenden Verschlüsselungstechniken und digitale Signaturen, neue Verfahren der

---

<sup>1</sup> Schlußfolgerungen des Vorsitzes des Europäischen Rats von Lissabon (23. und 24. März 2000), abrufbar unter der Adresse <http://ue.eu.int/de/Info/eurocouncil/index.htm>.

<sup>2</sup> Siehe [http://europa.eu.int/comm/information\\_society/eeurope/actionplan/index\\_de.htm](http://europa.eu.int/comm/information_society/eeurope/actionplan/index_de.htm).

Zugangskontrolle und Authentifizierung sowie verschiedene Softwarefilter<sup>3</sup>. Um die Sicherheit und Zuverlässigkeit von Informationsinfrastrukturen zu gewährleisten, bedarf es nicht nur verschiedener Technologien, sondern auch ihrer richtigen Verwendung und wirksamen Nutzung. Häufig sind sich die Nutzer gar nicht bewußt, daß bestimmte Technologien bereits existieren, oder sie wissen nicht, wie sie sie nutzen können oder warum sie überhaupt notwendig sind.

### **1.1. Antworten auf nationaler und internationaler Ebene**

Computerstraftaten werden über den Cyberspace begangen und machen nicht an den konventionellen Ländergrenzen halt. Sie können grundsätzlich von jedwedem Ort der Welt aus gegen jedweden Computernutzer in der Welt verübt werden. Allgemein besteht Einigkeit darüber, daß sowohl auf nationaler als auch auf internationaler Ebene wirksame Maßnahmen zur Bekämpfung der Computerkriminalität ergriffen werden müssen<sup>4</sup>.

Auf nationaler Ebene mangelt es gleichwohl häufig noch an umfassenden und international ausgerichteten Antworten auf die neuen Herausforderungen in punkto Sicherheit von Netzen und Computerkriminalität. Die meisten Länder konzentrieren ihre Maßnahmen zur Bekämpfung der Computerkriminalität (und insbesondere ihre strafrechtlichen Maßnahmen) auf die nationale Ebene, ohne alternative Präventivmaßnahmen zu berücksichtigen.

Vor allem bei den strafrechtlichen Bestimmungen über das Hacking, den Schutz des Geschäftsgeheimnisses und illegale Inhalte weisen die nationalen Rechtsordnungen weltweit trotz aller Bemühungen internationaler und supranationaler Organisationen noch immer große Unterschiede auf. Beträchtliche Unterschiede bestehen bei den Zwangsmitteln der Strafverfolgungsbehörden (insbesondere bei verschlüsselten Daten und Ermittlungen in internationalen Netzen), bei der gerichtlichen Zuständigkeit in Strafsachen und bei der Verantwortlichkeit von Vermittlern und Anbietern von Online-Inhalten. Die Richtlinie 2000/31/EG ("Richtlinie über den elektronischen Geschäftsverkehr")<sup>5</sup> sieht Änderungen bezüglich der Verantwortlichkeit von Vermittlern in bezug auf bestimmte Mittlertätigkeiten vor. Sie untersagt außerdem den Mitgliedstaaten, den Vermittlern die allgemeine Verpflichtung aufzuerlegen, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen.

Auf internationaler und supranationaler Ebene besteht weitgehend Einigkeit darüber, daß die Computerkriminalität wirksam bekämpft werden muß. Verschiedene Organisationen haben ihre diesbezüglichen Maßnahmen koordiniert oder harmonisiert. Im Dezember 1997 billigten die Justiz- und Innenminister der G8 einen 10-Punkte-Aktionsplan, der im Mai 1998 auf dem

---

<sup>3</sup> Der Informationsfluß wird auf sämtlichen Ebenen gefiltert und gesteuert: von der Firewall, die Datenpakete prüft, über Filter für bösartige Software, den E-Mail-Filter, der unerwünschte Werbung auf diskrete Weise herausfiltert, bis zum Browser, der den Zugang zu schädlichen Inhalten blockiert.

<sup>4</sup> Siehe den Aktionsplan "e-Europe"  
([http://europa.eu.int/comm/information\\_society/eeurope/actionplan/index\\_de.htm](http://europa.eu.int/comm/information_society/eeurope/actionplan/index_de.htm)  
sowie die Reden des Kommissionsmitglieds Vitorino  
([http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en\\_brussels.pdf](http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf)) und des französischen Premierministers Lionel Jospin  
(<http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html>).

<sup>5</sup> Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8 Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

Gipfeltreffen der G8 in Birmingham angenommen wurde und zur Zeit umgesetzt wird<sup>6</sup>. Der Europarat arbeitet seit Februar 1997 am Entwurf eines internationalen Übereinkommens über Cyberkriminalität und wird seine Arbeiten voraussichtlich bis Ende 2001 abschließen<sup>7</sup>. Die Bekämpfung der Cyberkriminalität ist auch Gegenstand bilateraler Gespräche zwischen der Europäischen Union und Drittländern. Ferner wurde eine gemeinsame Task Force der Gemeinschaft und der Vereinigten Staaten zum Thema Schutz kritischer Infrastrukturen gebildet<sup>8</sup>.

Auch die Vereinten Nationen und die OECD sind in diesem Bereich tätig, und dieses Thema wird zudem in internationalen Gremien (Global Business Dialogue, Trans-Atlantic Business Dialogue usw.) erörtert<sup>9</sup>.

Auf EU-Ebene erstreckten sich die einschlägigen Legislativmaßnahmen bisher hauptsächlich auf die Bereiche Urheberrecht, Schutz des Grundrechts auf Schutz der Privatsphäre und personenbezogener Daten, Dienste mit bedingtem Zugang, elektronischer Handel, elektronische Signaturen und insbesondere die Liberalisierung des Handels mit Verschlüsselungsprodukten, die indirekt im Zusammenhang mit der Computerkriminalität stehen.

Daneben wurde in den letzten drei bis vier Jahren eine Reihe wichtiger nichtlegislativer Maßnahmen ergriffen, darunter der Aktionsplan der Gemeinschaft zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen, in dessen Rahmen Sensibilisierungsmaßnahmen, Versuche zur Bewertung und Filterung von Inhalten und Hotlines, Initiativen zum Jugendschutz und zum Schutz der Menschenwürde in der Informationsgesellschaft sowie Maßnahmen zur Bekämpfung der Kinderpornographie und zur Überwachung des Fernmeldeverkehrs zu Zwecken der Strafverfolgung kofinanziert werden<sup>10</sup>. Die EU unterstützt schon seit langem Forschungs- und

---

<sup>6</sup> Der EU-Ministerrat Justiz und Inneres vom 19. März 1998 billigte die 10 Grundsätze zur Bekämpfung der High-Tech-Kriminalität, die von der G8 verabschiedet worden waren, und forderte die nicht zu den G8-Ländern gehörenden Mitgliedstaaten der EU auf, Vorkehrungen für den Beitritt zu dem Netz zu treffen (siehe diesbezüglich: <http://ue.eu.int/ejn/index.htm>).

<sup>7</sup> Der Entwurf ist im Internet in Französisch (<http://conventions.coe.int/treaty/fr/projets/cybercrime.htm>) und in Englisch (<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>) abrufbar.

<sup>8</sup> Unter Federführung der gemeinsamen Beratungsgruppe im Rahmen des zwischen der EU und den Vereinigten Staaten abgeschlossenen Abkommens über die Zusammenarbeit in Wissenschaft und Technik.

<sup>9</sup> Die Vereinten Nationen haben ein unlängst aktualisiertes, umfassendes Handbuch über die Verhütung und Eindämmung der Computerkriminalität ("Manual on the prevention and control of computer-related crime") erstellt. Die OECD führte 1983 eine Studie über die Möglichkeit einer internationalen Anwendung und Harmonisierung von Strafgesetzen zur Bewältigung des Problems der Computerkriminalität und des Computermissbrauchs durch. Sie veröffentlichte 1986 unter dem Titel "Computer-Related Crime: Analysis of Legal Policy" einen Bericht, der die bestehenden Gesetzesvorschriften und Reformvorschläge in verschiedenen Mitgliedstaaten untersuchte und eine Mindestliste von Mißbräuchen empfahl, deren Verbot oder strafrechtliche Verfolgung die Länder erwägen sollten. Im Jahre 1992 erarbeitete die OECD außerdem eine Reihe von Leitlinien für die Sicherheit von Informationssystemen, die den Staaten und der Privatwirtschaft bei der Schaffung eines Rahmens für die Sicherheit von Informationssystemen als Grundlage dienen soll.

<sup>10</sup> Siehe auch: Empfehlung 98/560/EG des Rates vom 24. September 1998 zur Steigerung der Wettbewerbsfähigkeit des europäischen Industriezweigs der audiovisuellen Dienste und Informationsdienste durch die Förderung nationaler Rahmenbedingungen für die Verwirklichung eines vergleichbaren Niveaus in bezug auf den Jugendschutz und den Schutz der Menschenwürde; Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und den Informationsdiensten (KOM(96) 483 vom Oktober 1996), <http://europa.eu.int/en/record/green/gp9610/protec.htm>;

Entwicklungsprojekte zur Steigerung der Sicherheit und des Vertrauens in Informationsinfrastrukturen und elektronische Transaktionen, und sie hat unlängst die Mittelausstattung des sich auf diesen Bereich beziehenden IST-Programms erhöht. Des Weiteren wurden im Rahmen von Programmen des dritten Pfeilers (STOP, FALCONE, OISIN und GROTIUS)<sup>11</sup> Forschungs- und operationelle Projekte zur Förderung besonderer Schulungsmaßnahmen für Strafverfolgungsbeamte sowie zum Ausbau der Zusammenarbeit zwischen den Strafverfolgungsbehörden und der Industrie unterstützt.

Der Aktionsplan zur Bekämpfung der organisierten Kriminalität, der vom Rat der Justiz- und Innenminister im Mai 1997 angenommen und vom Europäischen Rat auf seiner Tagung in Amsterdam bestätigt wurde, enthielt eine Aufforderung an die Kommission, bis Ende 1998 eine Studie über die Computerkriminalität zu erstellen. Die Kommission legte diese sogenannte COMCRIME-Studie<sup>12</sup> der Multidisziplinären Arbeitsgruppe "Organisierte Kriminalität" des Rates im April 1998 vor. Mit dieser Mitteilung entspricht die Kommission auch dem Ersuchen des Rates der Justiz- und Innenminister.

Die Kommission hielt es für angemessen, vor Erstellung dieser Mitteilung informelle Gespräche mit Vertretern der nationalen Strafverfolgungsbehörden und Kontrollstellen für den Datenschutz<sup>13</sup> sowie der europäischen Industrie (überwiegend Anbieter von Internet-Diensten und Telekommunikationsbetreiber) zu führen<sup>14</sup>.

Im Lichte der Analyseergebnisse und der Empfehlung der COMCRIME-Studie, der aus den obengenannten Gesprächen gezogenen Schlußfolgerungen, der sich durch den Vertrag von Amsterdam bietenden neuen Möglichkeiten sowie der bereits auf Ebene der EU, der G8 und des Europarates geleisteten Arbeiten beleuchtet diese Mitteilung im folgenden verschiedene Optionen für das weitere Vorgehen der EU gegen die Computerkriminalität. Dabei darf die für die EU-Ebene befürwortete Vorgehensweise selbstverständlich weder zu einer Behinderung oder Fragmentierung des Binnenmarkts noch zu Maßnahmen, die den Schutz der Grundrechte untergraben<sup>15</sup>, führen.

---

Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen - Illegale und schädigende Inhalte im Internet (KOM(96) 487 endg.); Entschließung zur Mitteilung der Kommission über illegale und schädigende Inhalte im Internet (KOM(96)0487 - C4-0592/96); Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (ABl. C 329 vom 4.11.1996, S. 1-6).

<sup>11</sup> Siehe [http://europa.eu.int/comm/justice\\_home/jai/prog\\_de.htm](http://europa.eu.int/comm/justice_home/jai/prog_de.htm).

<sup>12</sup> "Legal Aspects of Computer-related Crime in the Information Society – COMCRIME", Studie von Prof. Dr. Ulrich Sieber (Universität Würzburg) im Auftrag der Europäischen Kommission. Siehe: <http://europa.eu.int/ISPO/legal/en/crime/crime.html>.

<sup>13</sup> Auf EU-Ebene entsenden die nationalen Kontrollstellen für den Datenschutz Vertreter zur EU-Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten, einem unabhängigen, beratenden Gremium, das durch die Richtlinie 95/46/EG eingesetzt wurde (siehe Artikel 29 und 30 der Richtlinie).

<sup>14</sup> Es fanden zwei Unterredungen mit Strafverfolgungsbehörden (10.12.1999 und 1.3.2000), ein Treffen mit Vertretern der Internetindustrie (13.3.2000), ein weiteres Treffen mit einer kleineren Gruppe von Datenschutzexperten (31.3.2000) sowie eine abschließende Sitzung mit allen Beteiligten (17.4.2000) statt. Die Protokolle dieser Sitzungen können schriftlich angefordert werden bei: Europäische Kommission, Referat INFSO/A5 bzw. Europäische Kommission, Referat JAI/B2, Rue de la Loi 200, B-1049 Brüssel (Belgien)

<sup>15</sup> Siehe diesbezüglich die Charta der Grundrechte der Europäischen Union ([http://europa.eu.int/comm/justice\\_home/unit/charte\\_de.htm](http://europa.eu.int/comm/justice_home/unit/charte_de.htm)), Artikel 6 EU-Vertrag sowie die einschlägigen Urteile des Europäischen Gerichtshofs.

## 2. DIE SICHERHEIT VON INFORMATIONSIINFRASTRUKTUREN

In der heutigen Informationsgesellschaft treten globale, von Nutzern verwaltete Netze zunehmend an die Stelle der älteren Generation nationaler Kommunikationsnetze. Einer der Gründe für den Erfolg des Internet ist die Tatsache, daß das Internet den Nutzern den Zugang zu den neuesten Technologien ermöglicht. Das Moore'sche Gesetz<sup>16</sup> besagt, daß sich die Rechenkapazität von Computern alle 18 Monate verdoppelt. Die Kommunikationstechnologie entwickelt sich sogar noch rascher weiter<sup>17</sup>. Dies hat unter anderem dazu geführt, daß sich gegenwärtig die Menge der über das Internet übertragenen Daten binnen eines Zeitraums von weniger als einem Jahr verdoppelt.

Die klassischen Telefonnetze wurden von Staatsunternehmen aufgebaut und betrieben. Die Nutzer besaßen nur geringe Auswahlmöglichkeiten in bezug auf die angebotenen Dienstleistungen und gar keine in bezug auf die Umgebung. Den ersten Datennetzen, die entwickelt wurden, lag die Philosophie einer zentral gesteuerten Umgebung zugrunde, und auch die Sicherheitsvorkehrungen spiegelten diese Philosophie wider.

Das Internet und die anderen neuen Netze unterscheiden sich hiervon beträchtlich, und dementsprechend sind auch andere Sicherheitsvorkehrungen zu treffen. Die Informationen über diese Netze und ihre Steuerung liegen zumeist in den Händen der Nutzer und Dienstanbieter, also an der Peripherie. Der Netzkern ist einfach gestaltet und arbeitet effizient, seine Hauptaufgabe ist die Datenübermittlung. Eine Überprüfung oder Kontrolle von Inhalten findet nur in begrenztem Maße statt. Erst an ihrem endgültigen Bestimmungsort werden die übertragenen Bits zum Klang einer Stimme, zum Abbild einer Röntgenaufnahme oder zur Bestätigung einer Banküberweisung. Für die Sicherheit sind somit in erster Linie die Nutzer selbst zuständig, denn nur sie können ermesen, welcher Natur die Daten sind, die sie erhalten oder verschicken und welche Schutzvorkehrungen erforderlich sind.

Die Nutzerumgebung ist folglich ein wesentlicher Bestandteil der Informationsinfrastruktur. Der Einsatz von Sicherheitstechniken erfordert in diesem Fall die Zustimmung und die Mitwirkung des Nutzers, und er hat bedarfsgerecht zu erfolgen. Diesem Umstand kommt angesichts der wachsenden Zahl von Tätigkeiten, die über ein und dasselbe Endgerät abgewickelt werden, besondere Bedeutung zu: Arbeit, Spiele, Fernsehen, Banküberweisungen - alles erfolgt vom gleichen Gerät aus.

Zahlreiche Sicherheitstechnologien sind heute bereits verfügbar, und es werden ständig neue entwickelt. Die Vorteile der Entwicklung von Sicherheitssoftware mit frei zugänglichem Quellcode werden immer deutlicher. Auch bei den formellen Methoden und der Ermittlung von Kriterien für die Sicherheitsbewertung wurde bereits viel geleistet. Der Einsatz von Verschlüsselungstechnologien und elektronischen Signaturen wird bereits unabdingbar, zumal der drahtlose Zugang zu Daten immer größere Verbreitung findet. Um den unterschiedlichen Anforderungen in bezug auf unsere Kommunikationsumgebung gerecht werden zu können, bedarf es ebenso unterschiedlicher Authentifizierungsmechanismen. In bestimmten Umgebungen kann es erforderlich oder wünschenswert sein, anonym zu bleiben. In anderen

---

<sup>16</sup> Gordon Moore, einer der Mitbegründer von Intel, traf diese Feststellung im Jahre 1965 mit Blick auf die Geschwindigkeit, mit der sich die Dichte von Transistoren in integrierten Schaltkreisen erhöhte. Heutzutage verdoppelt sie sich etwa alle 18 Monate, was sich unmittelbar auf die Preise und die Leistungsfähigkeit von Computerchips auswirkt. Viele Experten gehen davon aus, daß diese Entwicklung noch mindestens zehn Jahre anhält.

<sup>17</sup> So kann ein einziges Glasfaserkabel heute die Datenmenge von 100 Millionen gleichzeitig stattfindenden Telefongesprächen transportieren.

kann es erforderlich sein, ohne Preisgabe der Identität einen bestimmten Nachweis zu erbringen, beispielsweise über die Volljährigkeit oder das Arbeitsverhältnis. In wieder anderen Situationen kann es erforderlich sein, einen Identitätsnachweis zu erbringen. Immer ausgefiltert werden auch die Softwarefilter: Sie schützen uns oder unsere Kinder vor unerwünschten Daten, seien es unerwünschte Inhalte oder Werbesendungen, bösartige Software oder sonstige Angriffe von außen. Die Einführung und Aufrechterhaltung derartiger Sicherheitsvorkehrungen im Internet wie auch in neuen Netzen bringt hohe Kosten für die Industrie und für die Nutzer mit sich. Daher ist es wichtig, Innovationen und die kommerzielle Nutzung von Sicherheitstechnologien und -dienstleistungen anzuregen.

Natürlich sind auch bei gemeinsamen Infrastrukturen wie Datenverbindungen und Name-Servern Sicherheitsaspekte zu beachten: Die Datenübermittlung zwischen Computern erfolgt über physische Verbindungen, die so eingerichtet und geschützt werden müssen, daß die Datenübermittlung selbst bei Störungen und Angriffen und trotz des stetig wachsenden Verkehrsvolumens möglich bleibt. Darüber hinaus hängt die Kommunikation von wichtigen Diensten ab, wie sie von Name-Servern und insbesondere der kleinen Zahl von Root-Name-Servern, die die gewünschten Adressen liefern, erbracht werden. Jede einzelne dieser Komponenten bedarf eines geeigneten Schutzes, dessen Form von dem betreffenden Teil des Name-Spaces sowie der Nutzer-Basis abhängt, für den die Adressenumwandlung erfolgt.

Infolge des Bestrebens, Informationsinfrastrukturtechnologien flexibler und bedarfsgerechter zu gestalten, sind diese zunehmend komplexer geworden, und Sicherheitsaspekte werden bei ihrer Auslegung oftmals nur unzureichend berücksichtigt. Zudem drückt sich die Komplexität dieser Technologien immer häufiger im Einsatz hochentwickelter, ineinandergreifender Softwareprogramme aus, die mitunter Schwachpunkte und Sicherheitslöcher aufweisen, die leicht für Angriffe ausgenutzt werden können. Gerade weil die grenzüberschreitenden Computernetze des Cyberspace immer komplexer und technisch ausgereifter werden, können sie anfällig für neuartige, unvorhergesehene Angriffe werden.

Es gibt bereits verschiedene technologische Schutzmechanismen, und es werden ständig neue entwickelt, um den Schutz weiter zu verbessern. Die bisherigen Antworten umfassen insbesondere folgende Maßnahmen:

- Schutz wichtiger Infrastrukturbestandteile durch Einsatz von Infrastrukturen mit öffentlichem Schlüssel, Entwicklung sicherer Übertragungsprotokolle usw.
- Schutz privater und öffentlicher Umgebungen durch Entwicklung ausgereifter Software, Firewalls, Antivirenprogramme, elektronischer Systeme für die Verwaltung von Zugriffsrechten, Verschlüsselung usw.
- Sichere Authentisierung autorisierter Nutzer, Einsatz intelligenter Chipkarten (Smartcards), biometrische Identifizierung, elektronische Unterschrift, Anwendung aufgabenspezifischer Technologien usw.

All diese Maßnahmen setzen voraus, daß verstärkt an der gemeinsamen Entwicklung von Sicherheitstechnologien gearbeitet wird, um über vereinbarte internationale Standards das notwendige Ineinandergreifen der Lösungen zu gewährleisten.

Ebenso wichtig ist, daß künftige Rahmenkonzepte für Sicherheitsaspekte zu einem festen Bestandteil der Gesamtarchitektur gemacht werden, so daß bereits bei der Auslegung auf Gefahren und Schwachstellen geachtet wird. Bei den traditionellen, nachträglich angepaßten Konzepten hingegen mußten aufgetretene Sicherheitslücken, die von immer raffinierteren Kriminellen ausgenutzt worden waren, nachträglich beseitigt werden.

Das EU-Programm für Technologien der Informationsgesellschaft (IST)<sup>18</sup> und insbesondere die Arbeiten<sup>19</sup> zum Thema "Informations- und Netzsicherheit und andere vertrauensschaffende Technologien" befassen sich mit der Entwicklung von Fähigkeiten und Technologien, die uns in die Lage versetzen, die Computerkriminalität zu begreifen und ihr zu begegnen. Darunter fallen unter anderem technische Hilfsmittel, die vor Verletzungen persönlicher Rechte wie dem auf Schutz der Privatsphäre und dem auf Schutz personenbezogener Daten schützen und sich zur Bekämpfung der Computerkriminalität eignen. Im Zusammenhang mit dem IST-Programm wurde zudem eine Initiative zum Thema Zuverlässigkeit ins Leben gerufen. Sie soll das Interesse für die Zuverlässigkeit von Technologien und für zuverlässigkeitsrelevante Techniken und somit das Vertrauen in eng verflochtene Informationsinfrastrukturen und eng vernetzte, eingebettete Systeme dauerhaft stärken. Ein zentraler Aspekt der Initiative ist die internationale Zusammenarbeit. So wurden in Zusammenarbeit mit dem amerikanischen Innenministerium im Rahmen des IST-Programms bereits Arbeitskontakte zur Defense Advanced Research Projects Agency (DARPA) und zur National Science Foundation (NSF) geknüpft und eine gemeinsame Task Force der Gemeinschaft und der Vereinigten Staaten zum Thema Schutz kritischer Infrastrukturen gebildet<sup>20</sup>.

Schließlich trägt auch die Umsetzung der Sicherheitsverpflichtungen, die sich insbesondere aus den Datenschutzrichtlinien<sup>21</sup> der EU ergeben, zu einer größeren Sicherheit der Netze und der Datenverarbeitung bei.

### **3. COMPUTERKRIMINALITÄT**

Die modernen Informations- und Kommunikationssysteme machen es möglich, jederzeit von jedem Ort der Welt aus illegale Handlungen zu begehen. Bisher liegen keine zuverlässigen Statistiken vor, die Aufschluß über das volle Ausmaß der Computerkriminalität geben könnten. Die Zahl der bisher aufgedeckten und gemeldeten Übergriffe dürfte das wahre Ausmaß des Problems eher verschleiern. Aufgrund begrenzter Vorsicht und Erfahrung der Systemverwalter und Nutzer werden viele Eindringversuche gar nicht bemerkt. Zudem melden viele Unternehmen Fälle von Computermißbrauch nicht, um kein schlechtes Bild in der Öffentlichkeit abzugeben und um ihre Anfälligkeit für weitere Angriffe nicht publik werden zu lassen. Viele Polizeidienste führen keine Statistik über die Verwendung von Computern und Kommunikationssystemen für Straftaten.

---

<sup>18</sup> Das IST-Programm der Europäischen Kommission ist Teil des Fünften Rahmenprogramms, das von 1998 bis 2002 läuft. Weitere Informationen sind unter der Adresse <http://www.cordis.lu/ist> erhältlich.

<sup>19</sup> Im Rahmen der IST-Leitaktion 2 ("Neue Arbeitsmethoden und elektronischer Geschäftsverkehr").

<sup>20</sup> Unter Federführung der gemeinsamen Beratungsgruppe im Rahmen des zwischen der EU und den Vereinigten Staaten abgeschlossenen Abkommens über die Zusammenarbeit in Wissenschaft und Technik.

<sup>21</sup> Siehe Artikel 4 der Richtlinie 97/66/EG (enthält u.a. eine Bestimmung über die Pflicht, Sicherheitsrisiken zu melden) sowie Artikel 17 der Richtlinie 95/46/EG.

Gleichwohl ist davon auszugehen, daß sich die Zahl illegaler Handlungen in dem Maße erhöhen wird, wie die Verwendung von Computern und Netzen zunimmt. Daher ist es erforderlich, stichhaltige Belege für das Ausmaß der Computerkriminalität zusammenzutragen.

Diese Mitteilung bezieht sich auf die Computerkriminalität im weitesten Sinne, d.h. auf jedwede Straftat, bei der in irgendeiner Form auf Informationstechnologie zurückgegriffen wird. Gleichwohl wird der Begriff "Computerkriminalität" unterschiedlich definiert und häufig synonym mit den Begriffen "High-Tech-Kriminalität" und "Cyberkriminalität" verwendet. Auf jeden Fall läßt sich eine Unterscheidung zwischen computerspezifischen Straftaten und herkömmlichen Straftaten vornehmen, die mit Hilfe der Computertechnik begangen werden. Ein passendes Beispiel hierfür ist der Zollbereich: Dort wird das Internet nachweislich für typische Verstöße gegen die Zollbestimmungen (Schmuggel, Fälschungsdelikte usw.) genutzt. Während die computerspezifischen Straftaten eine Aktualisierung der in den nationalen Rechtsordnungen definierten Straftatbestände notwendig machen, erfordern die mit Hilfe der Computertechnik begangenen, herkömmlichen Straftaten eine verbesserte Zusammenarbeit und bessere Verfahrensvorschriften.

Beide Arten von Straftaten werden durch die über Grenzen hinweggehende Verfügbarkeit von Informations- und Kommunikationsnetzen sowie durch den Umstand begünstigt, daß der Datenverkehr nicht erfaßbar und äußerst kurzlebig ist. Diese Eigenschaften machen es erforderlich, die bestehenden Verfahren zur Bekämpfung von illegalen Handlungen, die in oder mit Hilfe von Netzen und Systemen begangen werden, zu überdenken.

Zahlreiche Länder haben bereits Rechtsvorschriften zur Bekämpfung der Computerkriminalität erlassen. Auch in den Mitgliedstaaten der Europäischen Union ist bereits eine Reihe von Rechtsinstrumenten geschaffen worden. Abgesehen vom Beschluß des Rates zur Bekämpfung der Kinderpornographie im Internet gibt es zwar noch keine Rechtsinstrumente der EU, die sich direkt mit der Computerkriminalität befassen, doch es existiert bereits eine Reihe indirekt anwendbarer Rechtsinstrumente.

Die im Zusammenhang mit der Computerkriminalität auf Ebene der EU oder der Mitgliedstaaten erlassenen Rechtsvorschriften befassen sich in erster Linie mit folgenden Delikten:

*Rechtswidrige Eingriffe in die Privatsphäre:* Mehrere Länder haben Strafrechtsvorschriften erlassen, die sich gegen die rechtswidrige Sammlung, Speicherung, Änderung, Publikmachung oder Verbreitung personenbezogener Daten richten. Auf EU-Ebene wurden zwei Richtlinien für einen einheitlichen Schutz der Privatsphäre in bezug auf die Verarbeitung personenbezogener Daten angenommen<sup>22</sup>. Artikel 24 der Richtlinie 95/46/EG sieht vor, daß die Mitgliedstaaten geeignete Maßnahmen ergreifen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und daß sie insbesondere die Sanktionen festlegen, die bei Verstößen gegen die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind. Die Grundrechte des Schutzes der Privatsphäre und des

---

<sup>22</sup> Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation. Nach Artikel 24 der Richtlinie 95/46/EG sind die Mitgliedstaaten verpflichtet, Sanktionen festzulegen, die bei Verstößen gegen die Datenschutzbestimmungen anzuwenden sind.

Schutzes personenbezogener Daten sind überdies in der Charta der Grundrechte der Europäischen Union enthalten.

*Inhaltsbezogene Delikte:* Angesichts der vor allem über das Internet erfolgenden Verbreitung von pornografischen Inhalten und insbesondere von Kinderpornographie sowie von rassistischen Äußerungen und Aufrufen zur Gewalt stellt sich die Frage, wie derartigen Handlungen auf strafrechtlicher Ebene begegnet werden kann. Die Kommission hat diesbezüglich stets die Meinung vertreten, daß alles, was off-line verboten ist, auch on-line verboten werden sollte. So können die Verfasser und Anbieter<sup>23</sup> derartiger Inhalte heute strafrechtlich verfolgt werden. Der Rat hat einen Beschluß zur Bekämpfung der Kinderpornographie im Internet<sup>24</sup> angenommen.

Die Frage der Verantwortlichkeit von Vermittlern, deren Netze oder Server für die Übermittlung oder Speicherung von Informationen Dritter verwendet werden, wurde in der Richtlinie über den elektronischen Geschäftsverkehr aufgegriffen.

*Wirtschaftsdelikte, unberechtigter Zugang und Sabotage:* Zahlreiche Länder haben Rechtsvorschriften zur Bekämpfung von per Computer begangenen Wirtschaftsdelikten erlassen, in denen neue Straftatbestände im Zusammenhang mit dem unberechtigten Zugang zu Computersystemen (Hacking, Computersabotage, Verbreitung von Computerviren, Ausspähen oder Fälschung von Daten, Computerbetrug usw.<sup>25</sup>) sowie neue Begehungsformen (z.B. Manipulation per Computer anstelle der Täuschung eines Menschen) definiert werden. Das Tatobjekt ist dabei häufig nicht physisch greifbar (Geld auf Bankkonten, Computerprogramme usw.). Auf EU-Ebene gibt es noch keine Rechtsinstrumente, die sich gegen derartige illegale Handlungen richten. Allerdings hat, was die Prävention betrifft, die unlängst angenommene, überarbeitete Verordnung über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck entscheidend zur größeren Verfügbarkeit von Verschlüsselungsprodukten beigetragen.

*Verstöße gegen das Urheberrecht:* Zu diesem Bereich sind bisher zwei Richtlinien erlassen worden, die sich mit dem rechtlichen Schutz von Computerprogrammen bzw. Datenbanken befassen<sup>26</sup>, direkten Bezug auf die Informationsgesellschaft nehmen und auch die Möglichkeit von Sanktionen vorsehen. Der Rat hat einen Gemeinsamen Standpunkt zu einem Vorschlag für eine Richtlinie über das Urheberrecht und der verwandten Schutzrechte in der Informationsgesellschaft<sup>27</sup> angenommen, dessen Annahme für Anfang 2001 erwartet wird. Die Richtlinie sieht u.a. Sanktionen für Verstöße gegen das Urheberrecht und verwandte Schutzrechte sowie für die Umgehung technischer Maßnahmen zum Schutze dieser Rechte

---

<sup>23</sup> Nicht zu verwechseln mit dem Anbieter des betreffenden Internet-Dienstes.

<sup>24</sup> ABl. L 138 vom 9.6.2000, S. 1.

<sup>25</sup> Die jüngsten Angriffe auf große Internetpräsenzen sowie die Verbreitung des "LoveBug"-Virus haben ein großes Medienecho gefunden. Gleichwohl sollten diese Vorkommnisse in die richtige Perspektive gerückt werden: Vorsätzliche oder durch ein Versehen ausgelöste Angriffe auf Dienste sowie E-Mail-Viren gibt es bereits seit vielen Jahren (bekannte Beispiele sind der "Morris-Wurm" und der "IBM Xmas-tree"-Virus), und es existieren zahlreiche Produkte und Verfahren für ihre Beseitigung. Zudem arbeitet die Internetgemeinde eng zusammen, wenn es darum geht, den jeweiligen Schaden in Grenzen zu halten. Gleiches gilt im übrigen für das Spamming.

<sup>26</sup> Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen (ABl. L 122 vom 17.5.1991, S. 42–46).

Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. L 77 vom 27.3.1996, S. 20–28).

<sup>27</sup> Gemeinsamer Standpunkt des Rats im Hinblick auf die Annahme einer Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (Dok. CS/2000/9512).

vor. Zum Thema Softwareachahmung und -piraterie wird die Kommission bis spätestens Ende 2000 eine Mitteilung vorlegen, in der sie eine Bestandsaufnahme des mit dem Grünbuch von 1998 eingeleiteten Konsultationsprozesses vornehmen und einen einschlägigen Aktionsplan ankündigen wird. Mit der zunehmenden wirtschaftlichen Bedeutung des Internet entstehen neue Streitigkeiten um Bereichsnamen, bei denen es um Erscheinungen wie dem Cybersquatting, dem Warehousing und dem Reverse Hijacking geht. Dabei entsteht logischerweise die Forderung nach Vorschriften zur Regelung derartiger Probleme<sup>28</sup>.

Ein weiterer Punkt, den es zu regeln gilt, ist die Durchsetzung der Steuervorschriften: Bei geschäftlichen Transaktionen, bei denen der Nutzer einer elektronischen Dienstleistung in der EU ansässig ist, entsteht in der Regel eine steuerliche Verpflichtung in dem Land, in dem die Dienstleistung erbracht wird<sup>29</sup>. Bei Nichterfüllung der steuerlichen Pflichten können gegen den betreffenden Wirtschaftsbeteiligten zivil- und bisweilen auch strafrechtliche Sanktionen wie die Beschlagnahme von Bankkonten und anderen Vermögenswerten verhängt werden. Obwohl die freiwillige Erfüllung der steuerlichen Pflichten natürlich die vorzuziehende Alternative ist, muß letzten Endes auch immer die Möglichkeit gegeben sein, die Erfüllung der Steuerpflichten mit Zwangsmitteln durchzusetzen.

Bei der Verwirklichung dieses Ziels kommt der Zusammenarbeit der Steuerbehörden zentrale Bedeutung zu. Die Möglichkeiten zum Schutz legaler Transaktionen können auch zum Schutz illegaler Transaktionen mißbraucht werden. So können die Möglichkeiten, die der sichere elektronische Geschäftsverkehr bietet, auch beim Drogenhandel genutzt werden. Daher wird es darauf ankommen, Prioritäten zu setzen.

Im Zusammenhang mit der Frage des Schutzes der Opfer der Computerkriminalität müssen auch die Themen Haftung, Schadensersatz und Entschädigung bei Computerstraftaten angesprochen werden. Damit Vertrauen entstehen kann, bedarf es nicht nur des Einsatzes geeigneter Technologien, sondern auch flankierender rechtlicher und wirtschaftlicher Garantien. Diese Fragen gilt es in bezug auf sämtliche Delikte der Computerkriminalität zu prüfen.

Es bedarf wirksamer, global oder zumindest auf EU-Ebene angeglicherer Instrumente sowohl des materiellen Strafrechts als auch des Verfahrensrechts, die die Opfer der Computerkriminalität schützen und es ermöglichen, die Täter zur Verantwortung zu ziehen. Gleichzeitig darf jedoch nicht vergessen werden, daß das Recht auf Kommunikation, Privatsphäre und Datenschutz sowie auf Informationszugang und -verbreitung in modernen Demokratien grundrechtlich verankert ist. Aus diesem Grund ist es wünschenswert, wirksame Präventivmaßnahmen anwenden zu können, um die Notwendigkeit von Zwangsmaßnahmen zu begrenzen. Etwaige notwendige Legislativmaßnahmen zur Bekämpfung der Computerkriminalität müssen somit beiden Aspekten in geeigneter Weise gerecht werden.

---

<sup>28</sup> Mitteilung der Kommission an den Rat und das Europäische Parlament: Organisation und Verwaltung des Internet, Internationale und europäische Grundsatzfragen 1998–2000 (KOM(2000) 202 vom April 2000).

<sup>29</sup> Die Kommission hat eine Reihe von Änderungen des Mehrwertsteuersystems der EU vorgeschlagen, durch die geklärt werden soll, in welchem Land bei derartigen Transaktionen Steuerpflicht besteht (KOM(2000) 349 - Vorschlag für eine Richtlinie des Rates zur Änderung der Richtlinie 77/388/EWG bezüglich der mehrwertsteuerlichen Behandlung bestimmter elektronisch erbrachter Dienstleistungen). Der Vorschlag wird gegenwärtig vom Rat und vom Parlament geprüft. Unter bestimmten Umständen kann jedoch auch der Dienstleister steuerpflichtig sein. Dies gilt selbst dann, wenn sich dieser nicht in dem Land, in dem die Steuerpflicht besteht, aufhält.

#### 4. FRAGEN DES MATERIELLEN STRAFRECHTS

Durch Angleichung der materiellen Strafrechtsvorschriften für den Bereich der High-Tech-Kriminalität könnte ein Mindestschutz für die Opfer der Cyberkriminalität (und beispielsweise der Kinderpornographie) gewährleistet, der Anforderung der beiderseitigen Strafbarkeit (wonach bestimmte Formen der Rechtshilfe nur möglich sind, wenn die betreffenden Handlungen in beiden beteiligten Ländern strafbar sind) genüge getan und für die Industrie größere Klarheit (beispielsweise in bezug auf die Definition illegaler Inhalte) geschaffen werden.

Ein Rechtsinstrument der EU zur Angleichung des materiellen Strafrechts auf dem Gebiet der Computerkriminalität steht bereits seit dem Gipfeltreffen des Europäischen Rates von Tampere<sup>30</sup> im Oktober 1999 auf der politischen Tagesordnung der EU. In Tampere wurde die High-Tech-Kriminalität als ein Bereich einer beschränkten Zahl von Bereichen genannt, in denen Bemühungen zur Vereinbarung gemeinsamer Definitionen, Tatbestandsmerkmale und Sanktionen unternommen werden sollten. Sie ist ferner Gegenstand der Empfehlung Nr. 7 der vom Rat der Justiz- und Innenminister auf der Tagung vom 27. März 2000 angenommenen EU-Strategie für den Beginn des neuen Jahrtausends zur Prävention und Bekämpfung der organisierten Kriminalität<sup>31</sup> sowie des Arbeitsprogramms der Kommission für das Jahr 2000 und des von der Kommission vorgeschlagenen und vom Rat der Justiz- und Innenminister ebenfalls auf der März-Tagung angenommenen Anzeigers der Fortschritte beim Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts<sup>32</sup>.

Die Kommission hat die Arbeiten des Europarats am Entwurf des Übereinkommens über Cyberkriminalität aufmerksam verfolgt. Der Entwurf sieht derzeit vier Kategorien von Straftaten vor: 1.) Verstöße gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen; 2.) Computerstraftaten; 3.) inhaltsbezogene Straftaten; 4.) Verstöße gegen das Urheberrecht und ähnliche Rechte.

Die Angleichung auf EU-Ebene könnte noch weiter als das Übereinkommen des Europarats gehen, denn dieses sieht lediglich ein bestimmtes Mindestmaß an internationaler Angleichung vor. Sie könnte noch vor dem Inkrafttreten des Übereinkommens umgesetzt werden<sup>33</sup>. Die Computerkriminalität fiel somit unter das Gemeinschaftsrecht, und es würden Zwangsmaßnahmen auf EU-Ebene möglich.

Die Kommission möchte alles dafür tun, daß die Europäische Union in der Lage ist, wirksame Maßnahmen insbesondere gegen die Kinderpornographie im Internet zu ergreifen. Sie begrüßt den Beschluß des Rates zur Bekämpfung der Kinderpornographie im Internet, teilt jedoch die Auffassung des Europäischen Parlaments, daß eine weitere Angleichung der einschlägigen nationalen Rechtsvorschriften erforderlich ist. Die Kommission beabsichtigt, zu diesem Zweck noch in diesem Jahr einen Vorschlag für einen Rahmenbeschluß des Rates vorzulegen, der unter anderem Bestimmungen über die Angleichung der Vorschriften und der Sanktionen zu diesem Bereich enthält<sup>34</sup>.

---

<sup>30</sup> Siehe <http://db.consilium.eu.int/de/Info/eurocouncil/index.htm>.

<sup>31</sup> ABl. C 124 vom 3.5.2000.

<sup>32</sup> Siehe [http://europa.eu.int/comm/dgs/justice\\_home/pdf/com2000\\_782de.pdf](http://europa.eu.int/comm/dgs/justice_home/pdf/com2000_782de.pdf)

<sup>33</sup> Bevor das Übereinkommen des Europarates in Kraft treten kann, muß es erst noch ratifiziert werden.

<sup>34</sup> Diese Initiative ist Bestandteil eines Pakets von Vorschlägen, das - wie in der Mitteilung der Kommission über weitere Maßnahmen zur Bekämpfung des Frauenhandels vom Dezember 1998 angekündigt - auch allgemeinere Aspekte der Bekämpfung der sexuellen Ausbeutung von Kindern und des Menschenhandels abdeckt. Der Vorschlag für einen Rahmenbeschluß des Rates liegt der Mitteilung der Kommission an den

In Übereinstimmung mit den Schlußfolgerungen von Tampere wird die Kommission ferner einen Legislativvorschlag im Rahmen von Titel VI des Vertrags über die Europäische Union unterbreiten, der auf die Angleichung der Strafrechtsvorschriften für den Bereich der High-Tech-Kriminalität abstellt. Der Vorschlag wird auf den Arbeiten des Europarats aufbauen und sich insbesondere mit der Notwendigkeit einer Angleichung der Rechtsvorschriften der Mitgliedstaaten in bezug auf das Hacking und Angriffe auf Dienste befassen. Er wird ferner einheitliche EU-weite Definitionen zu diesem Bereich enthalten. Der Vorschlag könnte insofern sogar noch weiter als das geplante Übereinkommen des Europarats gehen, als er die Einführung von Mindeststrafen für schwere Fälle von Hacking und schwere Angriffe auf Dienste in allen Mitgliedstaaten vorsieht.

Des weiteren wird die Kommission prüfen, inwieweit Maßnahmen zur Bekämpfung von Rassismus und Fremdenfeindlichkeit im Internet ergriffen werden können, und sie wird gegebenenfalls einen Vorschlag für einen Rahmenbeschluß des Rates im Rahmen von Titel VI des Vertrags über die Europäische Union vorlegen, der sich mit rassistischen oder fremdenfeindlichen Handlungen im Online- wie im Offline-Bereich befaßt. Dabei wird sie unter anderem die Auswertungsergebnisse berücksichtigen, die ihr in Kürze in bezug auf die Umsetzung der Gemeinsamen Maßnahme vom 15. Juli 1996 betreffend die Bekämpfung von Rassismus und Fremdenfeindlichkeit<sup>35</sup> durch die Mitgliedstaaten vorliegen werden. Diese Gemeinsame Maßnahme war ein erster Schritt zur Angleichung der Strafrechtsvorschriften zur Bekämpfung von Rassismus und Fremdenfeindlichkeit. Gleichwohl ist eine weitere Angleichung auf EU-Ebene unabdingbar. Die Bedeutung und die Brisanz dieses Themas wurde erst unlängst am 20. November 2000 deutlich, als ein französisches Gericht den Internet-Dienstanbieter Yahoo dazu verurteilte, französischen Nutzern den Zugang zu Webseiten zu sperren, auf denen Nazi-Memorabilien zum Verkauf angeboten werden<sup>36</sup>.

Schließlich wird die Kommission prüfen, wie die Wirksamkeit der Maßnahmen gegen den Drogenhandel im Internet verbessert werden kann, denen im Rahmen der vom Europäischen Rat in Helsinki gebilligten Drogenstrategie der Europäischen Union (2000-2004)<sup>37</sup> große Bedeutung beigemessen wird.

## **5. STRAFVERFAHRENSRECHTLICHE FRAGEN**

Aufgrund der Natur der Computerstraftaten stellen sich insofern sowohl auf nationaler als auch auf internationaler Ebene zahlreiche verfahrensrechtliche Fragen, als hier unterschiedliche Hoheitsgewalten, Gerichtsbarkeiten und Rechtsordnungen ins Spiel kommen. Mehr noch als sonstige grenzüberschreitende Straftaten, stellen Computerstraftaten aufgrund der ihnen eigenen Geschwindigkeit, Mobilität und Flexibilität eine große Herausforderung für die geltenden strafverfahrensrechtlichen Bestimmungen dar.

Durch die Angleichung der Befugnisse der Strafverfolgungsbehörden wird sich der Schutz vor Computerstraftaten verbessern, denn so wird sichergestellt, daß die Strafverfolgungsbehörden in ihrem Zuständigkeitsbereich einschlägige Ermittlungen

---

Rat und an das Europäische Parlament über die Bekämpfung des Menschenhandels und der sexuellen Ausbeutung von Kindern bei, die gleichzeitig zu dieser Mitteilung veröffentlicht wird.

<sup>35</sup> ABl. L 185 vom 24.7.1996, S. 5-7.

<sup>36</sup> Tribunal de Grande Instance de Paris, Urteil Nr. 00/05308 vom 20. November 2000.

<sup>37</sup> Mitteilung der Kommission über einen Aktionsplan der Europäischen Union zur Drogenbekämpfung 2000 – 2004 (KOM (1999) 239 endg., [http://europa.eu.int/comm/justice\\_home/pdf/action\\_de.pdf](http://europa.eu.int/comm/justice_home/pdf/action_de.pdf))

durchführen und den Amtshilfeersuchen anderer Länder rasch und wirksam Folge leisten können.

Ebenso wichtig ist es, dafür Sorge zu tragen, daß strafrechtliche Maßnahmen, die ja generell in die Zuständigkeit der Mitgliedstaaten sowie unter Titel VI EU-Vertrag fallen, im Einklang mit dem Gemeinschaftsrecht stehen. Nach ständiger Rechtsprechung des Europäischen Gerichtshof dürfen derartige Rechtsvorschriften weder zu einer Diskriminierung von Personen führen, denen das Gemeinschaftsrecht einen Anspruch auf Gleichbehandlung verleiht, noch die vom Gemeinschaftsrecht garantierten Grundfreiheiten beschränken<sup>38</sup>. Die Frage der Verleihung neuer Befugnisse an die Strafverfolgungsbehörden ist somit vor dem Hintergrund des Gemeinschaftsrechts und ihrer möglichen Auswirkungen auf die Privatsphäre des einzelnen zu prüfen.

### 5.1. Überwachung des Fernmeldeverkehrs

In der Europäischen Union gilt der allgemeine Grundsatz der Vertraulichkeit des Fernmeldeverkehrs (und der diesbezüglichen Verkehrsdaten). Eine Überwachung ist widerrechtlich, sofern sie nicht durch eine Rechtsvorschrift für spezifische Fälle und begrenzte Zwecke als notwendig zugelassen wird. Dies leitet sich aus Artikel 8 der Europäischen Menschenrechtskonvention ab, auf die in Artikel 6 EU-Vertrag Bezug genommen wird, sowie insbesondere aus den Richtlinien 95/46/EG und 97/66/EG.

Alle Mitgliedstaaten verfügen über einen rechtlichen Rahmen, der es den Strafverfolgungsbehörden erlaubt, eine gerichtliche Anordnung bzw. (in zwei Mitgliedstaaten) eine von einem leitenden Minister persönlich genehmigte Anordnung zur Überwachung des Verkehrs im öffentlichen Fernmeldenetz einzuholen<sup>39</sup>. Die einschlägigen Vorschriften, deren Anwendung in Übereinstimmung mit dem Gemeinschaftsrecht zu erfolgen hat, enthalten Bestimmungen zum Schutz der Privatsphäre und beschränken so beispielsweise Überwachungsmaßnahmen auf schwere Straftaten und machen sie davon abhängig, daß sie tatsächlich erforderlich und angemessen sind und daß die betreffenden Personen über die Überwachung in Kenntnis gesetzt werden, sobald dies nicht mehr zu einer Behinderung der Untersuchung führen kann. In vielen Mitgliedstaaten sehen die einschlägigen Rechtsvorschriften zudem vor, daß die (staatlichen) Telekommunikationsbetreiber Überwachungsvorkehrungen einrichten müssen. Der Rat verabschiedete 1995 eine Entschließung<sup>40</sup>, die auf die Koordinierung der Überwachungsanforderungen abstellte.

---

<sup>38</sup> Rs. C-274/96, Bickel & Franz (1998), Slg. S. I-7637, Rdn. 17; Rs. C-186/87, Cowan (1989), Slg. S. 195, Rdn. 19. Insbesondere dürfen die administrativen oder strafrechtlichen Maßnahmen nicht über den Rahmen des unbedingt Erforderlichen hinausgehen, die Kontrollmodalitäten dürfen nicht so beschaffen sein, daß sie die vom Vertrag gewollte Freiheit einschränken, und es darf daran keine Sanktion geknüpft sein, die so außer Verhältnis zur Schwere der Tat steht, daß sie sich als Behinderung der Freiheit erweist (Rs. C-203/80, Casati (1981), Slg. S. 2595, Rdn. 27).

<sup>39</sup> In zwei Mitgliedstaaten sind überwachte Telefongespräche nicht als Beweismittel in Strafverfahren zugelassen.

<sup>40</sup> Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (ABl. C 329 vom 4.11.1996, S. 1–6). Im Anhang zu der Entschließung werden Anforderungen im Hinblick auf die Überwachung durch die Strafverfolgungsbehörden aufgeführt, denen die Mitgliedstaaten bei der Definition und Umsetzung ihrer einschlägigen nationalen Politik und Maßnahmen Rechnung tragen sollen. Der österreichische Ratsvorsitz legte 1998 einen Entwurf für eine Entschließung des Rates vor, mit der die Entschließung von 1995 auf neue Technologien wie das Internet oder die Satellitenkommunikation ausgeweitet werden sollte. Der Entwurf wurde in zwei Ausschüssen des Europäischen Parlaments (Ausschuß für bürgerliche Freiheiten und innere Angelegenheiten sowie

Die herkömmlichen Betreiber von Telekommunikationsnetzen und insbesondere jene Betreiber, die Fernsprechdienste anbieten, haben bereits in der Vergangenheit mit den Strafverfolgungsbehörden zusammengearbeitet, um die rechtmäßige Überwachung des Fernmeldeverkehrs zu ermöglichen. Infolge der Liberalisierung des Telekommunikationsmarktes und der verstärkten Nutzung des Internet sind zahlreiche neue Unternehmen in diesen Markt eingetreten, die nun ebenfalls mit den Überwachungsanforderungen konfrontiert werden. Daher ist es erforderlich, Fragen bezüglich der einschlägigen Vorschriften, der technischen Machbarkeit, der Kostenverteilung und der wirtschaftlichen Auswirkungen im Dialog zwischen Staat, Industrie und den sonstigen interessierten Parteien (wie beispielsweise den Datenschutzbehörden) zu erörtern.

Die neuen Technologien machen es erforderlich, daß die Mitgliedstaaten zusammenarbeiten, um sich die Möglichkeit der rechtmäßigen Überwachung des Fernmeldeverkehrs zu bewahren. Etwaige neue technische Überwachungsanforderungen der Mitgliedstaaten an die Telekommunikationsbetreiber und Anbieter von Internet-Diensten sollten nach Ansicht der Kommission zuvor auf internationaler Ebene koordiniert werden, um eine Verzerrung des Binnenmarkts zu vermeiden, die Kosten für die Industrie so gering wie möglich zu halten und den Anforderungen in bezug auf den Schutz der Privatsphäre und den Datenschutz gerecht zu werden. Die neuen Standards sollten nach Möglichkeit veröffentlicht und transparent gemacht werden und keine Schwächung der Kommunikationsinfrastrukturen nach sich ziehen.

Im Kontext des Übereinkommens über die Rechtshilfe in Strafsachen<sup>41</sup> wurde unter anderem Einigkeit über ein Konzept zur Erleichterung der Zusammenarbeit bei der rechtmäßigen Überwachung des Fernmeldeverkehrs<sup>42</sup> erzielt. Das Übereinkommen enthält unter anderem Bestimmungen über die Überwachung von per Satellit übertragenen Telefongesprächen<sup>43</sup> und über die Überwachung der Kommunikation einer Zielperson, die sich im Hoheitsgebiet eines anderen Mitgliedstaats befindet<sup>44</sup>. Nach dem Dafürhalten der Kommission stellen die sich auf die Überwachung beziehenden Bestimmungen des Übereinkommens über die Rechtshilfe in

---

Ausschuß für Recht und Bürgerrechte) erörtert, die jedoch zu unterschiedlichen Schlußfolgerungen gelangten: Während der erstgenannte Ausschuß die Ansicht vertrat, die Entschließung diene der Klarstellung und Aktualisierung der Entschließung von 1995 und sei daher annehmbar, lehnte der andere Ausschuß den Entwurf wegen der Gefahr möglicher Menschenrechtsverletzungen und der den Betreibern drohenden Kosten ab und forderte die Kommission auf, nach Inkrafttreten des Vertrags von Amsterdam einen neuen Entwurf zu erstellen. Weder der Rat noch seine Arbeitsgruppen haben sich mit diesem Vorschlag in den vergangenen Monaten aktiv befaßt.

<sup>41</sup> Die die Überwachung betreffenden Bestimmungen des am 29. Mai 2000 angenommenen Übereinkommens (ABl. C 197 vom 12.7.2000) beziehen sich nur auf die Rechtshilfe zwischen den Mitgliedstaaten der Europäischen Union, nicht gegenüber Drittstaaten.

<sup>42</sup> So sieht das Übereinkommen bestimmte Mindestvorkehrungen zum Schutz der Privatsphäre und zum Datenschutz vor.

<sup>43</sup> Ursprünglich war es bei den Verhandlungen darum gegangen, die Möglichkeit der Überwachung von Zielpersonen zu schaffen, die auf dem Gebiet des überwachenden Mitgliedstaats Satellitentelefone verwenden. Aus technischen Gründen ist es erforderlich, die Überwachung in den betreffenden Bodenstationen vorzunehmen. Somit entstand die Erfordernis, den Mitgliedstaat, auf dessen Gebiet sich die betreffende Bodenstation befindet, um technische Hilfe zu ersuchen. Hierfür sieht das Übereinkommen zwei Möglichkeiten vor: 1) ein beschleunigtes Rechtshilfverfahren, bei dem der Mitgliedstaat, in dem sich die betreffende Bodenstation befindet, von Fall zu Fall um Hilfe zu ersuchen ist, und 2.) eine technische Lösung, bei der der Zugang zur Bodenstation durch den überwachenden Mitgliedstaat per Fernzugriff erfolgt und somit keine individuellen Ersuchen erforderlich sind.

<sup>44</sup> Für diesen Fall sieht das Übereinkommen vor, daß sowohl der ersuchende Mitgliedstaat als auch der ersuchte Mitgliedstaat eine Überwachungsanordnung nach geltendem nationalen Recht einholen muß. In dem Übereinkommen ist zudem festgelegt, unter welchen Bedingungen ein Mitgliedstaat die Kommunikation einer sich auf dem Gebiet eines anderen Mitgliedstaats befindenden Zielperson überwachen kann, ohne den betreffenden Mitgliedstaat um technische Hilfe ersuchen zu müssen.

Strafsachen das Maximum des derzeit Möglichen dar. Das Übereinkommen ist Technologie-neutral formuliert, und bevor Überlegungen über etwaige Verbesserungen angestellt werden, sollte zunächst geprüft werden, wie sich das Übereinkommen in der Praxis bewährt. Die Kommission wird seine Umsetzung gemeinsam mit den Mitgliedstaaten, der Industrie, den Nutzern und den Datenschutzbehörden prüfen, um zu gewährleisten, daß die einschlägigen Initiativen wirksam, transparent und ausgewogen sind.

Der wahllose Gebrauch bzw. Mißbrauch von Überwachungsmöglichkeiten, insbesondere auf internationaler Ebene, wirft Menschenrechtsfragen auf und untergräbt das Vertrauen der Bürger in die Informationsgesellschaft. Die Kommission hat mit großer Besorgnis Berichte zur Kenntnis genommen, denen zufolge es bereits zu einem derartigen Mißbrauch gekommen sein soll<sup>45</sup>.

## **5.2. Aufbewahrung von Verkehrsdaten**

Zum Zwecke der Aufklärung und Verfolgung von mit Nutzung von Kommunikationsnetzen wie dem Internet begangenen Straftaten greifen die Strafverfolgungsbehörden häufig auf Verkehrsdaten zurück, die die Dienstanbieter zum Zwecke der Rechnungslegung aufbewahren. Da jedoch der in Rechnung gestellte Preis für eine Kommunikation immer seltener von der Entfernung und vom Bestimmungsort abhängt und die Dienstanbieter inzwischen immer häufiger Festtarife anbieten, wird bald nicht mehr die Notwendigkeit bestehen, Verkehrsdaten für die Rechnungslegung aufzubewahren. Die Strafverfolgungsbehörden hegen die Befürchtung, daß ihnen dadurch mögliches Beweismaterial verloren geht. Sie fordern daher, die Dienstanbieter zu verpflichten, bestimmte Verkehrsdaten für einen bestimmten Mindestzeitraum aufzubewahren, in dem die Daten dann für Strafverfolgungszwecke genutzt werden könnten<sup>46</sup>.

Gemäß den beiden EU-Richtlinien zum Schutz persönlicher Daten, von denen die Richtlinie 95/46/EG allgemeine und die Richtlinie 97/66/EG spezifische Beschränkungen vorsieht, sind Verkehrsdaten unmittelbar nach Beendigung der betreffenden Fernmeldedienstleistung zu löschen oder zu anonymisieren, sofern sie nicht für die Rechnungslegung benötigt werden. Bei festtariflichem oder kostenlosem Zugang zu Fernmeldediensten dürfen die Dienstanbieter grundsätzlich keine Verkehrsdaten aufbewahren.

Die Datenschutzrichtlinien der EU sehen auch vor, daß die Mitgliedstaaten Rechtsvorschriften erlassen können, die die Pflicht zur Datenlöschung beschränken, sofern dies beispielsweise für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von Telekommunikationssystemen notwendig ist<sup>47</sup>.

Etwaige einzelstaatliche Legislativmaßnahmen, die die Aufbewahrung von Verkehrsdaten für Strafverfolgungszwecke vorsehen, müßten jedoch die Voraussetzung erfüllen, daß die ins Auge gefaßten Maßnahmen angemessen, erforderlich und verhältnismäßig sind, wie es die einschlägigen gemeinschafts- und völkerrechtlichen Vorschriften (Richtlinien 97/66/EG und

---

<sup>45</sup> Der lange und umfassend dokumentierte Bericht von Herrn Campbell über das Überwachungsnetz ECHELON ([http://www.gn.apc.org/duncan/stoa\\_cover.htm](http://www.gn.apc.org/duncan/stoa_cover.htm)) war bereits Gegenstand einer öffentlichen Anhörung im Europäischen Parlament. Dem Bericht nach wurde ECHELON, obwohl ausschließlich für nationale Sicherheitszwecke konzipiert, auch zur Wirtschaftsspionage eingesetzt. Das Europäische Parlament hat einen nichtständigen Untersuchungsausschuß eingesetzt, der sich mit dieser Materie befaßt und dem Parlament binnen Jahresfrist einen Bericht vorlegen wird.

<sup>46</sup> Hierunter fielen auch strafrechtliche Ermittlungen in Fällen, in denen zwar kein Bezug zu Computern oder Kommunikationsnetzen besteht, aber die Daten dennoch zur Aufklärung beitragen können.

<sup>47</sup> Art. 14 der Richtlinie 97/66/EG sowie Art. 13 der Richtlinie 95/46/EG.

95/46/EG, Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 usw.) erfordern. Dies gilt insbesondere für Maßnahmen, die eine routinemäßige Aufbewahrung von Daten über einen Großteil der Bevölkerung vorsehen.

In einigen Mitgliedstaaten laufen gesetzgeberische Initiativen, die für Dienstanbieter die Verpflichtung oder die Möglichkeit vorsehen, nach der Erbringung der betreffenden Dienstleistung bestimmte Verkehrsdaten, die zwar nicht für die Rechnungslegung, aber für strafrechtliche Ermittlungen benötigt werden, aufzubewahren.

Die Initiativen unterscheiden sich zwar in bezug auf ihren sachlichen Geltungsbereich und ihre Form beträchtlich, gründen sich jedoch allesamt auf die Erwägung, daß den Strafverfolgungsbehörden mehr Daten zur Verfügung stehen sollten als dies der Fall ist, wenn die Dienstanbieter nur solche Daten verarbeiten, die sie unbedingt für die Erbringung ihres Dienstes benötigen. Die Kommission prüft diese Initiativen derzeit im Lichte der geltenden Gemeinschaftsvorschriften.

Das Europäische Parlament hat ein offenes Ohr für Fragen, die die Privatsphäre des einzelnen berühren, und es hat sich bisher generell für einen umfassenden Schutz personenbezogener Daten eingesetzt. In den Diskussionen um Maßnahmen zur Bekämpfung der Kinderpornographie im Internet hat es sich gleichwohl dafür ausgesprochen, eine allgemeine Pflicht zur Aufbewahrung von Verkehrsdaten für einen Zeitraum von mindestens drei Monaten einzuführen<sup>48</sup>.

Dies verdeutlicht die Bedeutung des Kontexts, in dem eine so heikle Frage wie die Aufbewahrung von Verkehrsdaten erörtert wird, und es zeigt auch, vor welcher Herausforderung die Politiker in ihrem Bemühen um ausgewogene Entscheidungen stehen.

Die Kommission ist der Auffassung, daß jedwede Lösung für die komplexe Frage der Aufbewahrung von Verkehrsdaten gut durchdacht sein und den unterschiedlichen Interessen, die hier eine Rolle spielen, in ausgewogener Weise Rechnung tragen muß. Dies wird nur möglich sein, wenn es gelingt, die fachlichen Kenntnisse und Fähigkeiten der Regierungen, der Industrie, der Datenschutzbehörden und der Nutzer zu bündeln. Wünschenswert wäre daher ein einheitliches Vorgehen aller Mitgliedstaaten, das es ermöglicht, die angestrebte Effizienz und Verhältnismäßigkeit zu erreichen und das verhindert, daß sich sowohl die Strafverfolgungsbehörden als auch die Internetgemeinde mit einem Stückwerk unterschiedlicher technischer und rechtlicher Vorschriften auseinandersetzen müssen.

In dieser Frage ist einer Vielzahl ebenso wichtiger wie unterschiedlicher Interessen Rechnung zu tragen. Einerseits vertreten die Datenschutzbehörden die Auffassung, daß unter Anerkennung der Bedürfnisse für eine effiziente Strafverfolgung das effizienteste Mittel zur Verringerung unannehmbarer Risiken für die Privatsphäre darin besteht, Daten des Telekommunikationsverkehrs prinzipiell nicht nur für Zwecke der Strafverfolgung aufzubewahren<sup>49</sup>. Andererseits haben die Strafverfolgungsbehörden darauf hingewiesen, daß

---

<sup>48</sup> Legislative Entschließung mit der Stellungnahme des Europäischen Parlaments zum Entwurf einer Gemeinsamen Maßnahme - vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union angenommen - zur Bekämpfung der Kinderpornographie im Internet, Änderung 17 (ABl. C 219 vom 30.7.1999, S. 71).

<sup>49</sup> "Eine breit angelegte erkundende oder auch allgemeine Überwachung muß verboten sein. (...) Unter Anerkennung der Bedürfnisse für eine effiziente Strafverfolgung besteht das effizienteste Mittel zur

sie es für erforderlich halten, eine bestimmte Mindestmenge von Verkehrsdaten für einen bestimmten Mindestzeitraum aufzubewahren, um strafrechtliche Ermittlungen zu erleichtern.

Die Industrie hat ein Interesse daran, in die Bekämpfung von Straftaten wie dem Hacking oder dem Computerbetrug eingebunden zu werden, sollte jedoch nicht mit Maßnahmen konfrontiert werden, die unverhältnismäßig teuer sind. Um zu vermeiden, daß der Internetzugang teuer und für den Nutzer schwerer erschwinglich wird, müßten die wirtschaftlichen Auswirkungen etwaiger Maßnahmen gründlich analysiert und in Bezug zu ihrer Wirksamkeit im Hinblick auf die Bekämpfung der Cyberkriminalität gesetzt werden. Zudem müßte sichergestellt werden, daß alle aufbewahrten Verkehrsdaten angemessen geschützt werden.

Der Industrie wird in jedem Falle eine Schlüsselrolle bei der Schaffung einer sichereren Informationsgesellschaft zufallen. Die Nutzer müssen Vertrauen in die Sicherheit der Informationsgesellschaft haben und sich vor Straftaten und Verletzungen ihrer Privatsphäre sicher fühlen können.

Die Kommission befürwortet und unterstützt die Schaffung eines konstruktiven Dialogs zwischen den Strafverfolgungsbehörden, der Industrie, den Datenschutzbehörden, den Verbraucherverbänden und den sonstigen interessierten Parteien. Im Rahmen des vorgeschlagenen EU-Forums (siehe Punkt 6.4 dieser Mitteilung) wird die Kommission alle Beteiligten auffordern, die komplexe Frage der Aufbewahrung von Verkehrsdaten vorrangig und ausgiebig zu erörtern, um gemeinsam geeignete, ausgewogene und angemessene Lösungen zu finden, bei denen das Grundrecht auf Schutz der Privatsphäre und auf Datenschutz vollauf gewahrt bleibt<sup>50</sup>. Auf der Grundlage der Ergebnisse dieser Debatte wird die Kommission anschließend ermessen können, inwieweit es etwaiger legislativer oder nichtlegislativer Maßnahmen auf Gemeinschaftsebene bedarf.

### **5.3. Anonymer Zugang und anonyme Nutzung**

Strafverfolgungsexperten haben die Befürchtung geäußert, daß Anonymität zu Nichtverantwortlichkeit führen und so die Ergreifung bestimmter Täter ernsthaft behindern könnte. In manchen Ländern ist es bereits möglich, mit im voraus bezahlten Telefonkarten anonym mobil zu telefonieren. Manche Dienst- bzw. Zugangsanbieter (darunter auch Remailer-Dienste und Internetcafés) bieten einen anonymen Zugang zum Internet sowie dessen anonyme Nutzung an. Ein gewisses Maß an Anonymität ist zudem bei der dynamischen Zuweisung der Internetadresse gegeben, bei der die Adressen den Nutzern nicht dauerhaft, sondern nur für die jeweilige Sitzung zugewiesen werden.

---

Verringerung unannehmbarer Risiken für die Privatsphäre darin, daß Daten des Telekommunikationsverkehrs im Prinzip nicht nur für Zwecke der Strafverfolgung aufbewahrt werden sollten und nationale Gesetzgebungen Betreiber von Telekommunikationsdiensten, Telekommunikationsdienstleistungen und Internet-Provider nicht dazu verpflichten sollten, historische Daten des Telekommunikationsverkehrs über einen längeren Zeitabschnitt aufzubewahren, als denjenigen, der für Zwecke der Rechnungsschreibung erforderlich ist." (Empfehlung 3/99 der durch Artikel 29 der Richtlinie 95/46/EG eingesetzten Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten vom 7. September 1999, [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp20de.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp20de.pdf)).

<sup>50</sup> wie in der Europäischen Menschenrechtskonvention (Artikel 8, "Gebot der Achtung der privaten Sphäre"), in der Charta der Grundrechte der Europäischen Union, im EU-Vertrag und in den Datenschutzrichtlinien der Europäischen Gemeinschaft vorgesehen

Vertreter der Industrie haben sich in den Gesprächen mit der Kommission gegen eine vollständige Anonymität ausgesprochen und dies unter anderem mit ihren eigenen Sicherheitsanforderungen sowie mit den Anforderungen in bezug auf die Betrugssicherheit und die Integrität der Netze begründet. Der London Internet Exchange (LINX)<sup>51</sup>, einer der bedeutendsten europäischen Internet-Austauschpunkte, hat auf seine Leitlinien für eine gute fachliche Praxis hingewiesen, die sich im VK als nützlich erwiesen haben. Andere Vertreter der Industrie sowie Datenschutzexperten haben erklärt, ohne Anonymität sei es nicht möglich, die Wahrung der Grundrechte zu garantieren.

Die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten hat eine Empfehlung zum Thema Anonymität im Internet<sup>52</sup> veröffentlicht, in der sie feststellt: "Daher steht die Frage der Anonymität im Internet eindeutig im Mittelpunkt eines Dilemmas für Regierungen und internationale Organisationen. Einerseits ist die Möglichkeit, anonym zu bleiben, wesentlich, wenn die Grundrechte auf Achtung der Privatsphäre und freie Meinungsäußerung im Cyberraum bewahrt werden sollen. Andererseits erstickt die Fähigkeit zur Online-Teilnahme und Kommunikation ohne Offenbarung der eigenen Identität schon im Keim die Initiativen, die gegenwärtig für andere ordnungspolitische Kernbereiche entwickelt werden, wie die Bekämpfung illegaler und schädigender Inhalte, Finanzbetrug oder Verstöße gegen das Urheberrecht. Natürlich ist eine solche offensichtliche Kollision zwischen verschiedenen ordnungspolitischen Zielen nicht neu. (...) Im Zusammenhang mit den traditionelleren Kommunikationsarten im Offline-Bereich, wie Brief- und Paketpost, Telefon, Zeitungen oder Rundfunk und Fernsehen wurde ein ausgewogenes Verhältnis zwischen diesen Zielen hergestellt. Gegenwärtig stehen Entscheidungsträger vor der Herausforderung sicherzustellen, daß dieser ausgewogene Ansatz, der Grundrechte gewährleistet, zugleich aber unter begrenzten und ganz bestimmten Umständen verhältnismäßige Beschränkungen dieser Rechte erlaubt, in dem neuen Cyberraumkontext beibehalten wird. Im Vordergrund werden dabei das Ausmaß und die Grenzen der Fähigkeit einzelner zur anonymen Online-Teilnahme stehen."

In der Abschlusserklärung zur europäischen Ministerkonferenz über die Nutzung der globalen Informationsnetze, die vom 6. bis 8. Juli 1997 in Bonn stattfand, wurde der Grundsatz anerkannt, daß die Möglichkeit des Nutzers, bei Offline-Medien anonym zu bleiben, auch für den Online-Bereich gegeben sein sollte. Die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe stellt diesbezüglich in ihrer obengenannten Empfehlung fest: "Es besteht ein eindeutiges Einvernehmen darüber, daß die Tätigkeit im Internet nicht von den sonst angewandten Rechtsgrundsätzen ausgenommen werden darf. Internet ist kein gesetzloser Freiraum, in dem die Regeln der Gesellschaft nicht gelten. Gleichmaßen sollte aber die Fähigkeit von Regierungen und Behörden, die Rechte einzelner zu beschränken und potentiell rechtswidriges Verhalten zu überwachen, im Internet nicht größer als in der Offline-Außenwelt sein. Das Erfordernis, daß Beschränkungen der Grundrechte und Grundfreiheiten im Hinblick auf andere Ziele der öffentlichen Ordnung angemessen gerechtfertigt, notwendig und verhältnismäßig sind, muß auch im Cyberraum gelten." Die Gruppe führt des weiteren detailliert aus, wie dies in spezifischen Fällen (beispielsweise im Zusammenhang mit E-Mails und Newsgroups) erreicht werden kann<sup>53</sup>. Die Kommission schließt sich diesen Ausführungen an.

---

<sup>51</sup> <http://www.linx.net/noncore/bcp/>

<sup>52</sup> Empfehlung 3/97 vom 3. Dezember 1997  
([http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wp6de.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp6de.pdf)).

<sup>53</sup> Siehe [http://europa.eu.int/comm/internal\\_market/de/media/dataprot/index.htm](http://europa.eu.int/comm/internal_market/de/media/dataprot/index.htm).

#### 5.4. Die praktische Zusammenarbeit auf internationaler Ebene

In jüngster Vergangenheit haben international abgestimmte Strafverfolgungsmaßnahmen wie die gegen Pädophilenringe gerichteten Operationen "Starburst" und "Cathedral" gezeigt, wie wertvoll die koordinierte internationale Zusammenarbeit zwischen Strafverfolgungs- und Justizbehörden sein kann, wenn es darum geht, im Vorfeld von Maßnahmen Informationen auszutauschen oder zu vermeiden, daß andere Mitglieder eines kriminellen Netzes durch Festnahmen oder Beschlagnahmen gewarnt werden. In Fällen, in denen herkömmliche Straftaten wie Fälschungs- oder Schmuggeldelikte mit Hilfe des Internets begangen wurden, hat sich das Internet bereits als wertvolles und effizientes Instrument für polizeiliche oder zollrechtliche Ermittlungen erwiesen. Allerdings sind dabei auch die großen rechtlichen und operationellen Schwierigkeiten deutlich geworden, denen sich die Strafverfolgungs- und Justizbehörden bei der Organisation der Maßnahmen gegenüber sehen: Vorbereitung von grenzübergreifenden Beweismitteln und Rechtshilfeersuchen, Identifizierung der Opfer, Rolle der zwischenstaatlichen Organisationen für polizeiliche Fragen (insbesondere Interpol und Europol) usw.

Was die praktische Zusammenarbeit auf internationale Ebene anbelangt, so werden internationale Netze für den Informationsaustausch immer wichtiger für die Polizei- und Zollbehörden.

Die G8-Länder haben ein allzeit erreichbares Informationsnetz eingerichtet, das sich aus Anlaufstellen der Strafverfolgungsbehörden zusammensetzt. Seine Hauptaufgabe ist die Beantwortung dringender Ersuchen um Kooperation in Fällen, in denen elektronische Beweismittel eine Rolle spielen. Das Netz hat sich bereits wiederholt als überaus nützlich erwiesen. Der Rat der Justiz- und Innenminister begrüßte auf seiner Tagung vom 19. März 1998 die 10 von den G8 gebilligten Grundsätze zur Bekämpfung der High-Tech-Kriminalität und forderte die nicht zu den G8-Ländern gehörenden Mitgliedstaaten der EU auf, dem Netz beizutreten<sup>54</sup>. Die an dem Netz beteiligten Anlaufstellen sollten auf direktem Wege zusammenarbeiten und so die bestehenden Rechtshilfestrukturen und Kommunikationskanäle sinnvoll ergänzen<sup>55</sup>.

Die Einrichtung eines solchen Netzes ist auch im Entwurf für das Übereinkommen des Europarats vorgesehen. Auch der Beschluß des Rates zur Bekämpfung der Kinderpornographie im Internet, der Gemeinsamer Standpunkt zu den Verhandlungen im Europarat über das Übereinkommen über Cyberkriminalität<sup>56</sup> und der Beschluß des Rates zur Annahme des Aktionsplans der G8<sup>57</sup> sehen die Einrichtung rund um die Uhr besetzter Anlaufstellen vor, doch auf EU-Ebene sind diesbezüglich bisher keine konkreten Initiativen ergriffen worden.

---

<sup>54</sup> Neben den G8-Staaten sind dem Netz bisher fünf Mitgliedstaaten der EU beigetreten.

<sup>55</sup> Auf dem Weltkongreß gegen die kommerzielle sexuelle Ausbeutung von Kindern, der am 28. August 1996 in Stockholm stattfand, wurde vorgeschlagen, Interpol in das Netz einzubinden. Der Beschluß des Rates zur Bekämpfung der Kinderpornographie im Internet sieht zudem die Zusammenarbeit mit Europol vor.

<sup>56</sup> "Die Mitgliedstaaten sollten die Festlegung von Bestimmungen unterstützen, die die internationale Zusammenarbeit erleichtern; hierzu gehören auch Bestimmungen über eine möglichst umfassende Rechtshilfe. Das Übereinkommen sollte eine zügige Zusammenarbeit bei computerbezogenen und computergestützten Straftaten erleichtern. Zu dieser Form der Zusammenarbeit kann auch die Einrichtung von rund um die Uhr besetzten Ansprechstellen bei den Strafverfolgungsbehörden gehören, die die derzeitigen Rechtshilfestrukturen ergänzen." (Artikel 1 Absatz.4)

<sup>57</sup> Siehe [www.usdoj.gov/criminal/cybercrime/action.htm](http://www.usdoj.gov/criminal/cybercrime/action.htm) sowie [www.usdoj.gov/criminal/cybercrime/principles.htm](http://www.usdoj.gov/criminal/cybercrime/principles.htm).

Da auf diesem Gebiet geeignetes Fachwissen und ein rasches Eingreifen erforderlich ist, sollten die vom Rat vorgegebenen Maßnahmen unverzüglich umgesetzt werden. Um erfolgreich arbeiten zu können, müßten die Anlaufstellen des Netzes mit rechtlich und technisch qualifiziertem Personal ausgestattet werden, was entsprechende Schulungsmaßnahmen voraussetzt.

Ebenso besteht die Notwendigkeit, die Zusammenarbeit und den Informationsaustausch zwischen den Zollbehörden zu intensivieren. Hier gilt es, die bestehenden Formen der Zusammenarbeit auszubauen und neue Möglichkeiten der Durchführung gemeinsamer Maßnahmen und des Informationsaustauschs zu entwickeln. Die Zollbehörden sind sich zunehmend darin einig, daß internationale Informationsnetze aufgebaut werden sollten, um den Informationsaustausch bei gleichzeitiger Wahrung der Datenschutzbestimmungen zu erleichtern. Auch muß in diesem Bereich verstärkt in moderne Computersysteme und in Schulungsmaßnahmen investiert werden, damit die Zollbehörden ihre Aufgaben effizienter erfüllen können.

### **5.5. Strafverfahrensrechtliche Befugnisse und Rechtsprechung**

Sind die gesetzlich vorgeschriebenen Voraussetzungen geschaffen, muß es den nationalen Strafverfolgungsbehörden möglich sein, in Computern gespeicherte Daten landesweit rasch genug auffindig zu machen und zu beschlagnahmen, um der Vernichtung strafrechtlicher Beweismaterialien zuvorzukommen. Die Strafverfolgungsbehörden sind der Ansicht, daß sie über Zwangsmittel verfügen müssen, die es ihnen erlauben, innerhalb ihres Zuständigkeitsbereiches Computersysteme zu durchsuchen und Daten zu beschlagnahmen, die Aushändigung bestimmter Computerdaten anzuordnen oder die prompte Aufbewahrung bestimmter Daten gemäß den geltenden rechtlichen (Sicherheits-)Bestimmungen anzuordnen oder zu bewirken. Die diesbezüglichen Sicherheitsbestimmungen und Verfahren sind bisher jedoch noch nicht angeglichen worden.

Wenn Strafverfolgungsbehörden beim Zugriff auf einen Computer feststellen, daß weitere, über das ganze Land verteilte Computer und Netze in den betreffenden Fall verwickelt sind, können sich bestimmte Fragen stellen. Noch komplizierter kann es werden, wenn eine Strafverfolgungsbehörde bei der Durchsuchung eines Computers oder auch nur bei einer einfachen Ermittlung feststellt, daß ein Zugriff auf Daten in einem oder mehreren anderen Ländern erfolgt oder erforderlich ist. Diese Frage berührt wichtige hoheits-, menschen- und strafrechtliche Aspekte und erfordert ein ausgewogenes Vorgehen.

In derartigen Fällen können sich die geltenden rechtlichen Instrumente der internationalen Zusammenarbeit in Strafsachen (Rechtshilfe) als ungeeignet oder unzureichend erweisen, da ihre Umsetzung in der Regel einen Zeitraum von mehreren Tagen, Wochen oder Monaten erfordert. Mithin bedarf es eines Mechanismus, der es einem Land ermöglicht, auf rasche und effiziente Weise und unter Wahrung der Grundsätze der nationalen Souveränität sowie der Verfassungs- und Menschenrechte (einschließlich der Bestimmungen zum Schutz der Privatsphäre und zum Datenschutz) strafrechtliche Ermittlungen anzustellen und Beweismaterial einzuholen oder zumindest sicherzustellen, daß bei der grenzübergreifenden Strafverfolgung keine wichtigen Beweisstücke verloren gehen.

Im Rahmen der Arbeiten des Europarats am Entwurf des Übereinkommens über Cyberkriminalität werden unter anderem verschiedene neue Vorschläge geprüft, die eine Aufbewahrungspflicht für bestimmte Daten zum Zwecke spezifischer Ermittlungen vorsehen. Daneben gibt es noch eine Reihe politisch schwieriger und bislang ungelöster Fragen wie das Thema grenzüberschreitende Durchsuchungen und Beschlagnahmen. Hier sind noch weitere

Gespräche aller Beteiligten erforderlich, bevor etwaige konkrete Initiativen ins Auge gefaßt werden können.

Die von den G8-Staaten eingesetzte Arbeitsgruppe "High-Tech-Kriminalität" hat sich bereits mit dem Thema grenzüberschreitende Durchsuchungen und Beschlagnahme auseinandergesetzt und sich auf eine Reihe einstweiliger Grundsätze<sup>58</sup> verständigt, ohne einer späteren, langfristigen Vereinbarung vorgreifen zu wollen. Zu klären ist allerdings noch die wichtige Frage, unter welchen Bedingungen und in welchen Situationen eine grenzüberschreitende, beschleunigte Durchsuchung bzw. Beschlagnahme ohne vorherige Benachrichtigung des betreffenden Landes möglich ist. Auch müssen dabei geeignete Bestimmungen zur Wahrung der Grundrechte vorgesehen werden. Im Gemeinsamen Standpunkt der EU zu den Verhandlungen im Europarat über das Übereinkommen über Cyberkriminalität wurde diese Frage offen gelassen<sup>59</sup>.

Bei grenzübergreifenden Computerstraftaten ist es wichtig, daß eindeutig festgelegt ist, welches Land für die Strafverfolgung zuständig ist. Vor allem muß vermieden werden, daß sich überhaupt kein Land zuständig fühlt. Eine der wichtigsten Bestimmungen des Entwurfs für das Übereinkommen des Europarats sieht vor, daß sich das Land, auf dessen Hoheitsgebiet oder durch dessen Staatsangehörigen die Straftat begangen wurde, für zuständig erklärt. Erklärt sich mehr als ein Land für zuständig, so sollten die betroffenen Länder gemeinsam bestimmen, in welchem Land der Gerichtsstand geeigneterweise liegen sollte. Gleichwohl wird dabei viel davon abhängen, ob eine effiziente bilaterale oder multilaterale Konsultation zustandekommt. Die Kommission wird diese Frage weiterverfolgen und prüfen, ob es weiterer Maßnahmen auf EU-Ebene bedarf.

Die Kommission hat an den Gesprächen auf Ebene des Europarats und der G8 teilgenommen und erkennt an, daß diese verfahrensrechtlichen Fragen überaus komplex und schwierig sind. Gleichwohl kann eine wirksame Zusammenarbeit bei der Bekämpfung der Cyberkriminalität auf EU-Ebene einen wichtigen Beitrag zur Schaffung einer sichereren Informationsgesellschaft und eines Raums der Freiheit, der Sicherheit und des Rechts leisten.

Die Kommission gedenkt ihre Gespräche mit allen Beteiligten in den kommenden Monaten fortzusetzen, um auf den bisherigen Arbeiten aufzubauen. Diese Thematik wird auch im weiteren Kontext ihrer Arbeiten zur Umsetzung der Schlußfolgerungen des Europäischen Rats von Tampere vom Oktober 1999 behandelt werden. Der Europäische Rat hat die Kommission auf seiner Tagung in Tampere unter anderem ersucht, bis zum Dezember des Jahres 2000 ein Maßnahmenprogramm zur Umsetzung des Grundsatzes der gegenseitigen Anerkennung anzunehmen. Die Kommission hat bereits eine Mitteilung über die gegenseitige Anerkennung von Endentscheidungen in Strafsachen<sup>60</sup> veröffentlicht. Als Teil ihres Beitrags zum Arbeitsprogramm über die gegenseitige Anerkennung von Gerichtsbeschlüssen sowie im

---

<sup>58</sup> Pressemitteilung der Ministerkonferenz der G8-Staaten zur Bekämpfung transnationaler organisierter Kriminalität, Moskau, 19.-20. Oktober 1999 (siehe <http://www.usdoj.gov/criminal/cybercrime/action.htm> sowie <http://www.usdoj.gov/criminal/cybercrime/principles.htm>).

<sup>59</sup> "Vorbehaltlich verfassungsrechtlicher Grundsätze und spezifischer Schutzklauseln zur angemessenen Wahrung der Souveränität, der Sicherheit, der öffentlichen Ordnung oder anderer wesentlicher Interessen anderer Staaten kann eine grenzüberschreitende Durchsuchung von Computern zum Zwecke von Ermittlungen bei im Übereinkommen genauer festzulegenden schweren Straftaten in Ausnahmefällen, insbesondere in Dringlichkeitsfällen, erwogen werden, zum Beispiel soweit dies erforderlich ist, um die Vernichtung oder Veränderung von Beweisen für die betreffende schwere Straftat oder die Begehung einer Straftat zu verhindern, die wahrscheinlich zum Tode oder zu einer schweren körperlichen Verletzung einer Person führt." (Artikel 1 Absatz 7; ABl. L 142 vom 5. Juni 1999)

<sup>60</sup> KOM(2000) 495 endg. vom 26.7.2000.

Hinblick auf die Vorlage eines Legislativvorschlags im Rahmen von Titel VI EU-Vertrag wird die Kommission zudem die Optionen für eine Anerkennung von im Rahmen von Ermittlungsverfahren im Zusammenhang mit Cyberkriminalität ergangenen Anordnungen prüfen.

## **5.6. Die Beweiskraft von Computerdaten**

Strafverfolgungsbehörden müssen in der Lage sein, offensichtlich beweiskräftige Computerdaten, zu denen sie Zugang erhalten haben, abzurufen und im Hinblick auf ihre Verwendung im Rahmen der strafrechtlichen Ermittlung und Verfolgung zu überprüfen. Dies ist keine leichte Aufgabe, da elektronische Daten sehr kurzlebig sind und leicht manipuliert, gefälscht, mit technischen Mitteln geschützt oder gelöscht werden können. Sie ist Gegenstand der Computerkriminaltechnik, die sich mit der Entwicklung und dem Einsatz von wissenschaftlichen Protokollen und Verfahren für die Durchsuchung von Computern und die Analyse abgerufener Daten und die Erhaltung ihrer Authentizität befaßt.

Auf Ersuchen der Experten der G8-Länder hat sich die IOCE (International Organisation of Computer Evidence) bereit erklärt, Empfehlungen in bezug auf die Schaffung von Standards (einschließlich der Definition gebräuchlicher Bezeichnungen), die zu verwendenden Ermittlungsmethoden und -techniken und die Einführung eines einheitlichen Formats für kriminaltechnische Ersuchen auszuarbeiten. Sowohl auf Ebene der auf Computerkriminalität spezialisierten Ermittlungsstellen der Mitgliedstaaten als auch über die durch das Fünfte Rahmenprogramm (IST-Programm) geförderten Forschungs- und Entwicklungsmaßnahmen müßte die EU an diesen Arbeiten beteiligt werden.

## **6. NICHTLEGISLATIVE MAßNAHMEN**

Es ist erforderlich, auf nationaler und internationaler Ebene geeignete Rechtsvorschriften zu erlassen. Sie allein reichen jedoch nicht aus, um die Computerkriminalität und den Mißbrauch von Netzen wirksam zu bekämpfen. Daher bedarf es bestimmter nichtlegislativer Maßnahmen, die die legislativen Maßnahmen sinnvoll ergänzen. Diese Maßnahmen sind größtenteils bereits in den Empfehlungen der COMCRIME-Studie und im 10-Punkte-Aktionsplan der G8 genannt worden und bei allen Beteiligten des informellen Konsultationsprozesses, der dieser Mitteilung vorausgegangen ist, auf breite Zustimmung gestoßen. Sie sehen unter anderem folgende Maßnahmen vor:

- Einrichtung nationaler, auf die Bekämpfung der Computerkriminalität spezialisierter Polizeidienststellen in den Ländern, in denen diese noch nicht bestehen;
- Verbesserung der Zusammenarbeit zwischen den Strafverfolgungsbehörden, der Industrie, den Verbraucherorganisationen und den Datenschutzbehörden;
- Förderung von geeigneten Initiativen der Industrie bzw. von Bürgergruppen, beispielsweise zur Entwicklung von Sicherheitsprodukten.

Das Thema Verschlüsselung dürfte in diesem Zusammenhang weiter eine wichtige Rolle spielen. Die Verschlüsselung kann die Abwicklung und Akzeptanz von neuen Diensten wie dem elektronischen Geschäftsverkehr entscheidend erleichtern und wesentlich zur Verhütung der Internetkriminalität beitragen. Die Kommission hat ihre diesbezügliche Politik in ihrer

Mitteilung über Sicherheit und Vertrauen in elektronische Kommunikation<sup>61</sup> aus dem Jahre 1997 dargelegt. Sie hat darin auch ihren Willen bekundet, sämtliche Einschränkungen in bezug auf den freien Warenverkehr mit Verschlüsselungsprodukten in der Gemeinschaft abzuschaffen. In der Mitteilung wurde darauf hingewiesen, daß nationale Einschränkungen des freien Warenverkehrs mit Verschlüsselungsprodukten mit dem Gemeinschaftsrecht vereinbar sein müssen und daß die Kommission insbesondere mit Blick auf die sich auf den freien Warenverkehr beziehenden Vertragsbestimmungen, die einschlägigen Entscheidungen des Europäischen Gerichtshofs und die Bestimmungen der Datenschutzrichtlinien prüfen wird, ob derartige nationale Einschränkungen gerechtfertigt und angemessen sind. Die Kommission erkennt an, daß die Verschlüsselung neue und schwierige Herausforderungen für die Strafverfolgungsbehörden mit sich bringt.

Sie begrüßt daher die unlängst angenommene, überarbeitete Verordnung über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck, die entscheidend zur größeren Verfügbarkeit von Verschlüsselungsprodukten beigetragen hat, erkennt allerdings auch an, daß parallel hierzu der Dialog zwischen den Nutzern, der Industrie und den Strafverfolgungsbehörden verbessert werden muß. Die Kommission beabsichtigt, diesen Dialog über das vorgeschlagene EU-Forum über High-Tech-Kriminalität zu fördern. Die EU-weite Verfügbarkeit von erforderlichenfalls auf der Grundlage gemeinsamer Bewertungskriterien zugelassenen Sicherheitsprodukten (einschließlich jener für eine starke Verschlüsselung) würde die Möglichkeiten für die Kriminalitätsbekämpfung verbessern und das Vertrauen der Nutzer in die Informationsgesellschaft stärken.

### **6.1. Spezialisierte Dienststellen auf nationaler Ebene**

Aufgrund der technischen und rechtlichen Komplexität bestimmter Computerstraftaten ist es erforderlich, spezialisierte Dienststellen auf nationaler Ebene einzurichten. Diese müssen mit fachlich qualifiziertem, multidisziplinärem Personal (Strafverfolgung und Justiz) sowie mit geeigneten technischen Mitteln ausgestattet sein und rasch erreichbare Anlaufstellen darstellen, die

- Informationsersuchen zu vermuteten Straftaten umgehend nachkommen. Dafür wird es erforderlich sein, einheitliche Formate für den Austausch derartiger Informationen festzulegen, was – wie die Gespräche der G8-Experten gezeigt haben - wegen der Unterschiede in der nationalen Rechtskultur keine leichte Aufgabe werden dürfte;
- als Schnittstellen für nationale und internationale Hotlines<sup>62</sup> auf Strafverfolgungsebene Beschwerden der Internet-Nutzer über illegale Inhalte nachgehen;

---

<sup>61</sup> KOM(97) 503 endg.

<sup>62</sup> Derartige Hotlines bestehen bisher nur in einer begrenzten Zahl von Ländern. Als Beispiele zu nennen sind hier die "Cybertip Line" in den Vereinigten Staaten und die Internet Watch Foundation (IWF) im VK, die seit Dezember 1996 eine Telefon- und E-Mail-Hotline betreibt, über die die Bürger Internetinhalte melden können, die ihrer Ansicht nach illegal sind. Die IWF prüft jeweils, ob die Inhalte tatsächlich illegal sind und informiert gegebenenfalls die Internet-Dienstleister und die Polizei. Weitere Überwachungsstellen existieren in Norwegen (Redd Barna), in den Niederlanden (Meldpunt), in Deutschland (NewsWatch, Freiwillige Selbstkontrolle Multimedia, Jugendschutz), in Österreich (ISPAA) und in Irland (ISPAI). Im Rahmen des DAPHNE-Programms der EU führt das Childnet International derzeit ein Projekt durch, das sich direkt mit dieser Frage befaßt (Forum über internationale Hotline-Anbieter in Europa). Die Sachverständigen der UNESCO haben auf ihrer Tagung in Paris im Januar 1999 ebenfalls die Einrichtung landesweiter Hotlines befürwortet und die Einrichtung von Hotline-Netzen oder eines internationalen "elektronischen Wachturms" angeregt.

- computergestützte Ermittlungstechniken (weiter)entwickeln, die zur Aufdeckung, Ermittlung und Verfolgung von Computerstraftaten dienen;
- als führende Zentren für Fachwissen aus dem Bereich Cyberkriminalität den Austausch von Erfahrungen und guten fachlichen Praktiken organisieren.

Einige Mitgliedstaaten der EU haben bereits derartige spezialisierte Dienststellen für die Bekämpfung von Computerstraftaten eingerichtet. Die Kommission ist der Ansicht, daß die Einrichtung derartiger Dienststellen Vorrecht der Mitgliedstaaten ist, und sie ermutigt die Mitgliedstaaten, entsprechende Schritte zu unternehmen. Die Ausstattung dieser Dienststellen mit der neuesten Hard- und Software und die Schulung ihres Personals erfordern einen hohen Kostenaufwand sowie Prioritätensetzungen und Entscheidungen auf geeigneter politischer Ebene<sup>63</sup>. Besonders wertvoll können hier die Erfahrungen der bereits existierenden Dienststellen dieser Art in den Mitgliedstaaten sein. Die Kommission wird den Austausch derartiger Erfahrungen anregen.

Die Kommission ist ferner der Auffassung, daß Europol durch Koordinierung, Analysen und sonstige Unterstützung für die spezialisierten einzelstaatlichen Dienststellen einen zusätzlichen Nutzen auf EU-Ebene bewirken kann. Die Kommission wird sich daher dafür einsetzen, die Zuständigkeit Euopols auf die Cyberkriminalität auszudehnen.

## **6.2. Fachliche Schulung**

Es bedarf erheblicher Anstrengungen zur fortlaufenden fachlichen Schulung des Personals der Polizei- und Justizbehörden. Im Bereich der Computerkriminalität ändern sich die kriminellen Techniken und Fähigkeiten der Täter schneller als bei den traditionellen Erscheinungsformen der Kriminalität.

Einige Mitgliedstaaten haben Initiativen zur hochtechnologischen Schulung von Mitarbeitern der Strafverfolgungsbehörden ins Leben gerufen. Diese könnten den Mitgliedstaaten, die noch keine derartigen Schritte ergriffen haben, Ratschläge und Anleitungen geben.

Einzelne Projekte, mit denen dies (in Form von Erfahrungsaustauschen und Seminaren über gemeinsame Schwierigkeiten für die betreffenden Berufsgruppen) erreicht werden soll, wurden im Rahmen von Programmen der Kommission (insbesondere STOP, FALCONE und GROTIUS) gefördert. Die Kommission wird weitere Aktionen in diesem Bereich (z.B. zur Computer- und Online-Ausbildung) vorschlagen.

Im November 2000 hat Europol ein einwöchiges Fortbildungsseminar für Mitarbeiter von Strafverfolgungsbehörden der Mitgliedstaaten veranstaltet, das sich schwerpunktmäßig mit Fragen der Kinderpornographie befaßt hat. Dieser Themenbereich könnte auf die Computerkriminalität allgemein ausgeweitet werden. Auch Interpol ist bereits seit Jahren auf diesem Gebiet aktiv. Seine einschlägigen Initiativen könnten auf einen größeren Teilnehmerkreis zugeschnitten werden.

---

<sup>63</sup> Zu den in den Vereinigten Staaten gesammelten Erfahrungen siehe Michael A. Sussmann: "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", *Duke Journal of Comparative and International Law*, Vol. 9, Spring 1999, S. 464.

Die G8-Länder haben Initiativen organisiert, die den Erfahrungsaustausch zwischen Strafverfolgungsbehörden und die Festlegung von gemeinsamen Ermittlungstechniken anhand konkreter Fälle ermöglichen. Eine weitere Initiative im Schulungsbereich wird für Anfang 2001 erwartet. Die den G8 angehörenden Mitgliedstaaten der EU könnten ihre dort gewonnenen Erfahrungen mit den anderen Mitgliedstaaten teilen.

Bei der Bekämpfung der Kinderpornographie im Internet könnte die Einrichtung einer zentralen, internationalen und digitalen Bibliothek für kinderpornografische Bilder die Suche nach Opfern und Tätern, die Ermittlung von Straftatbeständen und die Schulung von fachlich spezialisierten Polizeibeamten erleichtern<sup>64</sup> (die Bilder dürften natürlich nur den spezialisierten einzelstaatlichen Strafverfolgungsstellen über das Internet zur Verfügung gestellt werden, und es müßten die erforderlichen Bedingungen und Einschränkungen in bezug auf den Zugang und den Schutz der Privatsphäre gegeben sein).

### **6.3. Verbesserte Informationen und gemeinsame Regeln für die Datenaufbewahrung**

Einheitliche Regeln für die Datenaufbewahrung in Polizei- und Justizbehörden und geeignete Werkzeuge für die statistische Analyse von Computerstraftaten könnten den Strafverfolgungs- und Justizbehörden die Speicherung, Analyse und Auswertung der in diesem Bereich gesammelten formellen Informationen erleichtern.

Der Privatsektor benötigt derartige Statistiken zudem für eine angemessene Risikobewertung und eine Kosten-Nutzen-Analyse im Hinblick auf die Risikobewältigung.

Der Kommission wurde eine ständig aktualisierte Datenbank über die Vorschriften zum Bereich Computerkriminalität zugänglich gemacht, die im Rahmen der COMCRIME-Studie eingerichtet wurde. Die Kommission wird prüfen, wie sie den Inhalt (einschließlich Rechtsvorschriften, Gerichtssachen und Literatur) und die Benutzerfreundlichkeit der Datenbank verbessern kann.

### **6.4. Zusammenarbeit zwischen den verschiedenen Akteuren: das EU-Forum**

Eine effiziente Zusammenarbeit zwischen Staat und Industrie im Rahmen der einschlägigen Rechtsvorschriften gilt als wichtiger Bestandteil jedweder öffentlichen Politik zur Bekämpfung der Computerkriminalität<sup>65</sup>. Die Vertreter der Strafverfolgungsbehörden haben eingeräumt, daß sie nicht immer klar und präzise genug zu verstehen gegeben haben, was sie

---

<sup>64</sup> Eine sehr erfolgreiche Initiative auf diesem Gebiet war das vom schwedischen Kriminalamt entwickelte und von der Kommission im Rahmen des STOP-Programms geförderte "Excalibur"-Projekt, das in Zusammenarbeit mit Polizeikräften aus Deutschland, dem VK, den Niederlanden und Belgien sowie mit Europol und Interpol durchgeführt wurde. Auch die Erfahrungen aus dem "Perkeo"-Projekt des Bundeskriminalamts (BKA) und aus dem (ebenfalls im Rahmen des STOP-Programms geförderten) "Surfimage"-Projekt des französischen Innenministeriums sollten hierbei berücksichtigt werden.

<sup>65</sup> Die Justiz- und Innenminister der G8-Staaten wiesen in einer zum Abschluß ihrer Washingtoner Konferenz vom 9./10. Dezember 1997 angenommenen Verlautbarung zu den Grundsätzen und zum 10-Punkte-Aktionsplan zur Bekämpfung der High-Tech-Kriminalität darauf hin, daß der industrielle Sektor die globalen Netze konzipiert, einrichtet und betreibt und auch in erster Linie für die Entwicklung technischer Standards verantwortlich ist. Daher müsse sich der industrielle Sektor auch an der Entwicklung und Verbreitung sicherer Systeme beteiligen, die dazu dienen können, Computermißbrauch aufzudecken, elektronisches Beweismaterial zu sichern und den Aufenthaltsort und die Identität von Kriminellen zu ermitteln. Der Beschluß des Rates zur Bekämpfung der Kinderpornographie im Internet sieht vor, daß die Mitgliedstaaten einen konstruktiven Dialog mit der Industrie aufnehmen und unter Einbindung der Industrie zusammenarbeiten, indem sie ihre Erfahrungen austauschen.

von den Dienst Anbietern benötigen. Die Vertreter der Industrie haben sich überwiegend dafür ausgesprochen, die Zusammenarbeit mit den Strafverfolgungsbehörden zu verbessern; gleichzeitig haben sie auf die Notwendigkeit hingewiesen, daß dabei bestimmte Grundsätze wie eine ausgewogene Gewichtung des erforderlichen Schutzes der Grund- und Bürgerrechte (und insbesondere des Schutzes der Privatsphäre)<sup>66</sup>, der Notwendigkeit, gegen Kriminalität vorzugehen und der den Dienst Anbietern entstehenden wirtschaftlichen Belastung eingehalten werden müssen.

Die Industrie und die Strafverfolgungsbehörden können ihre Zusammenarbeit dazu nutzen, die Öffentlichkeit stärker für die Gefährdung durch Kriminelle im Internet zu sensibilisieren, bewährte Sicherheitspraktiken zu verbreiten und wirksame Werkzeuge und Verfahren für die Kriminalitätsbekämpfung zu entwickeln. In einigen Mitgliedstaaten wurden bereits einschlägige Initiativen ins Leben gerufen, darunter das "Internet Crime Forum" im VK, die wohl älteste und weitreichendste Initiative dieser Art<sup>67</sup>.

Die Kommission begrüßt diese Initiativen und ist der Ansicht, daß derartige Initiativen in allen Mitgliedstaaten ins Leben gerufen werden sollten. Sie beabsichtigt, ein EU-Forum einzurichten, das Vertreter der Strafverfolgungsbehörden, der Internet-Dienst Anbieter, der Telekommunikationsbetreiber, der Bürgerrechtsorganisationen, der Verbraucher und der Datenschutzbehörden sowie anderer interessierter Parteien mit dem Ziel vereint, die Zusammenarbeit auf EU-Ebene zu fördern. Zunächst ist daran gedacht, von den Mitgliedstaaten benannte Beamte, Technologieexperten, von der durch Artikel 29 eingesetzten Arbeitsgruppe benannte Sachverständige zum Thema Privatsphäre sowie in enger Absprache mit der Industrie und den Verbraucherverbänden benannte Vertreter der Industrie und der Verbraucher zusammenzubringen. Später soll das Forum dann zudem Vertreter der einschlägigen einzelstaatlichen Initiativen umfassen.

Das EU-Forum wird offen und transparent agieren, die einschlägigen Dokumente werden jeweils im Internet veröffentlicht werden, und alle interessierten Parteien werden Gelegenheit erhalten, ihren Standpunkt darzulegen.

Das Forum wird unter anderem folgende Aufgaben haben:

- Einrichtung von rund um die Uhr besetzten Anlaufstellen für den Kontakt zwischen Staat und Industrie in Bereichen, in denen derartige Stellen angebracht erscheinen;
- Entwicklung eines geeigneten Standardformats für Auskunftersuchen der Strafverfolgungsbehörden an die Industrie, damit die Strafverfolgungsbehörden zur Kommunikation mit den Dienst Anbietern verstärkt auf das Internet zurückgreifen können;

---

<sup>66</sup> Gemäß den Datenschutzrichtlinien der EU, der Europäischen Konvention nr. 108 zum Schutze der Menschenrechte und Grundfreiheiten sowie dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sowie den einschlägigen nationalen Rechtsvorschriften.

<sup>67</sup> Dem 1997 eingerichteten Forum gehören Polizeibeamte, Vertreter des britischen Innenministeriums, Datenschützer und Vertreter der Internet-Industrie an. Es tritt drei- bis viermal im Jahr zusammen und hat mehrere ständige Arbeitsgruppen.

- Förderung der Entwicklung und/oder Anwendung von Verhaltensregeln und bewährten Praktiken sowie Austausch derartiger Verhaltensregeln mit Staat und Industrie in anderen Ländern<sup>68</sup>;
- Förderung des Austauschs von Informationen über Entwicklungstrends bei der High-Tech-Kriminalität zwischen den verschiedenen Parteien und insbesondere zwischen der Industrie und den Strafverfolgungsbehörden;
- Ermittlung der aus Sicht der Strafverfolgungsbehörden bedenklichen Aspekte der Entwicklung neuer Technologien;
- Förderung der Weiterentwicklung von Frühwarn- und Krisenbewältigungsmechanismen für die Verhütung, Ermittlung und Behandlung möglicher Bedrohungen oder Störungen von Informationsinfrastrukturen;
- ein gegebenenfalls verstärkter Expertenbeitrag zu den laufenden Arbeiten im Rat und in anderen internationalen Gremien (Europarat, G8 usw.);
- Förderung der Zusammenarbeit zwischen den interessierten Parteien einschließlich der Ausarbeitung gemeinsamer Grundsätze der Strafverfolgungsbehörden, der Industrie und der Nutzer (z.B. durch Ausarbeitung eines Abkommens oder von in Übereinstimmung mit dem geltenden Rechtsrahmen stehenden Verhaltenskodexen).

## **6.5. Direkte Maßnahmen der Industrie**

Die Bekämpfung der Computerkriminalität liegt zu einem großen Teil auch im Interesse der breiteren Öffentlichkeit. Wenn das Vertrauen der Verbraucher in den elektronischen Geschäftsverkehr gestärkt werden soll, müssen Maßnahmen zur Vorbeugung gegen die Computerkriminalität als Bestandteil der guten Geschäftspraxis akzeptiert werden. Zahlreiche Industriezweige (z.B. in den Bereichen Banken, elektronische Kommunikation, Kreditkarten und Urheberrechte) mitsamt ihrer Kunden sind durch Computerstraftaten gefährdet. Die Unternehmen schützen generell ihre Namen und Warenzeichen und betreiben so aktive Betrugsverhütung. Die Verbände der Software- und Audioindustrie haben eigene Teams, die Fällen von Piraterie (einschließlich Internet-Piraterie) nachgehen (z.B. in der britischen Phonindustrie). In einigen Mitgliedstaaten haben Internet-Dienstleister Hotlines eingerichtet, über die illegale und schädliche Inhalte gemeldet werden können.

Die Kommission hat bereits einige dieser Initiativen im Rahmen des Rahmenprogramms im Bereich Forschung, technologische Entwicklung und Demonstration, des Aktionsplans zur Förderung der sicheren Nutzung des Internet<sup>69</sup> und der unter Titel VI fallenden Programme wie STOP und DAPHNE gefördert.

Auf dem EU-Forum werden gute fachliche Praktiken aus diesen Bereichen ausgetauscht werden.

---

<sup>68</sup> Bei Verhaltensregeln im Sinne von Artikel 27 der Richtlinie 95/46/EG würde dies unter Mitwirkung der nach Artikel 29 eingesetzten Arbeitsgruppe zum Thema Datenschutz sowie der nationalen Datenschutzbehörden erfolgen. Derartige Verhaltensregeln könnten auch Fragen abdecken, die unter die Richtlinie 97/66/EG fallen (z.B. Überwachungsmaßnahmen).

<sup>69</sup> Nähere Informationen zu diesem Aktionsplan sind unter der Adresse <http://158.169.50.95:10080/iap/> abrufbar.

## 6.6. Von der EU geförderte FTE-Projekte

Der Schwerpunkt des Programms für Forschung, technologische Entwicklung und Demonstration auf dem Gebiet der Benutzerfreundlichkeit in der Informationsgesellschaft (IST-Programm), das Teil des Fünften Rahmenprogramms für den Zeitraum 1998-2002 ist, liegt auf der Entwicklung und Einführung vertrauensschaffender Technologien. Letztere umfassen sowohl Technologien zur Förderung der Informations- und Netzsicherheit als auch technische Werkzeuge und Methoden zur Bekämpfung der Computerkriminalität sowie zum Schutz vor einem Mißbrauch des Grundrechts auf Schutz der Privatsphäre und auf Datenschutz sowie anderer persönlicher Rechte.

Im Rahmen des IST-Programms und insbesondere der Arbeiten zum Thema "Informations- und Netzsicherheit und andere vertrauensschaffende Technologien" im Rahmen der Leitaktion 2 ("Neue Arbeitsmethoden und elektronischer Geschäftsverkehr") sollen Fähigkeiten und Technologien entwickelt werden, die es möglich machen, neue technologische Herausforderungen im Zusammenhang mit der Verhütung und Bekämpfung der Computerkriminalität zu verstehen und zu bewältigen und die in punkto Sicherheit und Schutz der Privatsphäre bestehenden Anforderungen auf EU-Ebene, auf Ebene der virtuellen Gemeinschaften und auf Ebene des Einzelnen zu erfüllen.

Um den Herausforderungen in bezug auf die Vertrauenswürdigkeit in geeigneter Weise begegnen und Computerstraftaten verhüten und untersuchen zu können, wurde im Zusammenhang mit dem IST-Programm zudem eine Initiative zum Thema Zuverlässigkeit ins Leben gerufen. Sie soll das Interesse für die Zuverlässigkeit von Technologien und für zuverlässigkeitsrelevante Techniken und somit das Vertrauen in eng verflochtene Informationsinfrastrukturen und eng vernetzte, eingebettete Systeme dauerhaft stärken. Ein zentraler Aspekt der Initiative ist die internationale Zusammenarbeit. So wurden in Zusammenarbeit mit dem amerikanischen Innenministerium im Rahmen des IST-Programms bereits Arbeitskontakte zur Defense Advanced Research Projects Agency (DARPA) und zur National Science Foundation (NSF) geknüpft und unter Federführung der gemeinsamen Beratungsgruppe im Rahmen des zwischen der EU und den Vereinigten Staaten abgeschlossenen Abkommens über die Zusammenarbeit in Wissenschaft und Technik eine gemeinsame Task Force der Gemeinschaft und der Vereinigten Staaten zum Thema Schutz kritischer Infrastrukturen gebildet<sup>70</sup>.

Die Gemeinsame Forschungsstelle der Kommission (GFS), die bereits die Zuverlässigkeits-Initiative im Rahmen des IST-Programms unterstützt hat, wird ihre Anstrengungen darauf konzentrieren, in Rücksprache mit den anderen interessierten Parteien (und insbesondere mit Europol) gemeinsame Maßnahmen zu konzipieren, einheitliche Indikatoren zu entwickeln und harmonisierte Statistiken zu erstellen. Ziel dabei wird sein, rechtswidrige Handlungen zu klassifizieren und das Verständnis dafür zu fördern, worin sie bestehen, wie sich geografisch verteilen, in welchem Maße sie zunehmen und wie wirksam die Gegenmaßnahmen sind. Bei Bedarf wird die GFS dabei auch andere Forschungsgruppen hinzuziehen und ihre Arbeiten und Ergebnisse berücksichtigen. Sie wird einen Internetauftritt zu diesem Thema einrichten und das EU-Forum über den Fortgang seiner Arbeiten unterrichten.

---

<sup>70</sup> Nähere Informationen über das IST-Programm sind unter der Adresse [www.cordis.lu/ist](http://www.cordis.lu/ist) abrufbar.

## 7. SCHLUßFOLGERUNGEN UND VORSCHLÄGE

Um Computerkriminalität verhüten und wirksam bekämpfen zu können, müssen folgende Bedingungen gewährleistet sein:

- Verfügbarkeit präventiver Technologien: Dies setzt rechtliche Rahmenbedingungen voraus, die Platz und Anregungen für Innovationen und Forschungsmaßnahmen schaffen. Auch mit öffentlichen Mitteln unterstützte Maßnahmen zur Entwicklung und Anwendung geeigneter Sicherheitstechnologien können hierfür in Frage kommen.
- ein geschärftes Bewußtsein für mögliche Sicherheitsrisiken und Möglichkeiten ihrer Bekämpfung;
- adäquate materielle und verfahrensrechtliche Vorschriften zur Bekämpfung der inländischen und der grenzüberschreitenden Kriminalität: Die nationalen Vorschriften des materiellen Strafrechts müssen so umfassend und effizient sein, daß sie den Straftatbestand des schweren Computermißbrauchs erfassen, abschreckende Sanktionen vorsehen, Probleme infolge fehlender beiderseitiger Strafbarkeit<sup>71</sup> beseitigen und die internationale Zusammenarbeit erleichtern. Die strafverfahrensrechtlichen Vorschriften sollten in Übereinstimmung mit den im Gemeinschaftsrecht vorgesehenen Grundsätzen und Ausnahmebestimmungen sowie mit der Europäischen Menschenrechtskonvention die Möglichkeit vorsehen, daß die Strafverfolgungsbehörden in den Fällen, in denen die wohlbegründete Notwendigkeit hierfür besteht, zwecks Aufklärung einer Computerstraftat unverzüglich und landesweit Computerdaten ermitteln, beschlagnahmen und sicher kopieren können. Nach dem Dafürhalten der Kommission stellt die Vereinbarung, die bezüglich der sich auf die Kommunikationsüberwachung beziehenden Bestimmungen im Übereinkommen über die Rechtshilfe in Strafsachen getroffen wurde, das Maximum des derzeit Möglichen dar. Die Kommission wird ihre Umsetzung gemeinsam mit den Mitgliedstaaten, der Industrie und den Nutzern prüfen, um zu gewährleisten, daß die einschlägigen Initiativen wirksam, transparent und ausgewogen sind;
- Verfügbarkeit einer ausreichenden Zahl von fachlich geschulten und gut ausgerüsteten Mitarbeitern von Strafverfolgungsbehörden: Eine enge Zusammenarbeit mit den Internet-Diensteanbietern und Telekommunikationsbetreibern bei Schulungsmaßnahmen wird weiter angeregt werden;
- Verbesserte Zusammenarbeit zwischen allen Beteiligten (Nutzer, Verbraucher, Industrie, Strafverfolgungs- und Datenschutzbehörden): Sie spielt eine entscheidende Rolle bei der Untersuchung von Computerstraftaten und beim Schutz der öffentlichen Sicherheit. Die Rechte und Pflichten der Industrie müssen klar geregelt sein. Die Regierungen müssen anerkennen, daß die Anforderungen der Strafverfolgungsbehörden Belastungen für die Industrie bedeuten können und sinnvolle Maßnahmen treffen, die diese Belastungen so gering wie möglich halten. Gleichzeitig muß die Industrie in ihren Geschäftspraktiken auch Aspekte der öffentlichen Sicherheit berücksichtigen. Dazu wird es zunehmend der aktiven Mitarbeit und Unterstützung der einzelnen Nutzer und Verbraucher bedürfen;

---

<sup>71</sup> Viele Rechtsordnungen sehen vor, daß bestimmte Formen der Rechtshilfe und eine Auslieferung nur möglich sind, wenn die betreffenden Handlungen in beiden beteiligten Ländern strafbar sind.

- Fortlaufende Initiativen der Industrie bzw. von Bürgergruppen. Bereits vorhandene Hotlines für die Meldung von illegalen und schädlichen Inhalten können auf andere Formen des Mißbrauchs ausgeweitet werden. Die Industrie sollte eine Selbstregulierung vornehmen und mit einer größtmöglichen Zahl interessierter Parteien ein Abkommen vereinbaren, so daß auf vielfältige Weise ein Beitrag zur Verhütung und Bekämpfung der Computerkriminalität, zur Sensibilisierung und zur Vertrauensstärkung geleistet werden kann;
- Die Errungenschaften und Möglichkeiten der Forschung und technologischen Entwicklung müssen optimal genutzt werden. Der Schwerpunkt muß darauf gelegt werden, finanzierbare und wirksame Entwicklungen auf dem Gebiet der Sicherheitstechnologie und anderer vertrauensschaffender Technologien in die politischen Initiativen der EU zu integrieren.

Die EU sollte bei all ihren Beschlüssen berücksichtigen, daß die beitrittswilligen Länder schrittweise in die Staatengemeinschaft der EU sowie in die internationale Zusammenarbeit eingebunden und nicht zu Zufluchtstätten der Computerkriminalität werden sollen. Daher sollte in Erwägung gezogen werden, Vertreter dieser Länder an manchen oder allen einschlägigen Gremien der EU zu beteiligen.

Die Vorschläge der Kommission lassen sich wie folgt unterteilen:

### **7.1. Vorschläge für legislative Maßnahmen**

Die Kommission wird Vorschläge für folgende, unter Titel VI des Vertrags über die Europäische Union fallende Legislativmaßnahmen unterbreiten:

- Angleichung der Rechtsvorschriften der Mitgliedstaaten in bezug auf Kinderpornographiedelikte. Wie bereits in der Mitteilung der Kommission über weitere Maßnahmen zur Bekämpfung des Frauenhandels vom Dezember 1998 angekündigt, wird diese Initiative Bestandteil eines Pakets von Vorschlägen sein, das auch allgemeinere Aspekte der sexuellen Ausbeutung von Kindern und des Menschenhandels abdeckt. Es wird in völliger Übereinstimmung mit dem Bestreben des Europäischen Parlaments stehen, der österreichischen Initiative für einen Ratsbeschluß über die Bekämpfung der Kinderpornographie einen Rahmenbeschluß zur Angleichung der einschlägigen Rechtsvorschriften folgen zu lassen. Auch steht dies in Übereinstimmung mit den Schlußfolgerungen von Tampere und der EU-Strategie für den Beginn des neuen Jahrtausends zur Prävention und Bekämpfung der organisierten Kriminalität. Zudem ist dies Bestandteil des Maßnahmenplans für die Fortschritte beim Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts.
- weitere Angleichung der materiellen Strafrechtsvorschriften für den Bereich High-Tech-Kriminalität. Dies schließt Straftaten wie das Hacking und Angriffe auf Dienste ein. Des Weiteren wird die Kommission prüfen, inwieweit Maßnahmen zur Bekämpfung von Rassismus und Fremdenfeindlichkeit im Internet ergriffen werden können, und sie wird gegebenenfalls einen Vorschlag für einen Rahmenbeschluß im Rahmen von Titel VI des Vertrags über die Europäische Union vorlegen, der sich mit rassistischen oder fremdenfeindlichen Handlungen im Online- wie im Offline-Bereich befaßt. Schließlich wird die Kommission prüfen, welche Maßnahmen in diesem Zusammenhang gegen den illegalen Drogenhandel ergriffen werden können.

- Anwendung des Grundsatzes der gegenseitigen Anerkennung von im Rahmen von Ermittlungsverfahren im Zusammenhang mit Cyberkriminalität ergangenen Anordnungen und Erleichterung von strafrechtlichen, durch Computerstraftaten begründeten Ermittlungen, an denen mehr als ein Mitgliedstaat beteiligt ist, unter Wahrung der einschlägigen Grundrechte. Dieser Vorschlag entspricht dem Entwurf des Maßnahmenprogramms zur Umsetzung des Grundsatzes der gegenseitigen Anerkennung, in dem auf die Notwendigkeit hingewiesen wird, Vorschläge in bezug auf die Übermittlung und das Einfrieren von Beweisstücken zu prüfen.

Im Lichte ihrer Konsultationen und insbesondere der Ergebnisse, die das vorgeschlagene EU-Forum in diesem Bereich erzielt, wird die Kommission der Notwendigkeit Rechnung tragen, Maßnahmen (insbesonderer legislativer Art) zum Thema Aufbewahrung von Verkehrsdaten zu ergreifen.

## **7.2. Vorschläge für nichtlegislative Maßnahmen**

Es werden folgende Maßnahmen vorgeschlagen:

- Die Kommission richtet ein EU-Forum ein, in dem Strafverfolgungsbehörden, Dienstanbieter, Netzbetreiber, Verbrauchergruppen und Datenschutzbehörden unter Vorsitz der Kommission gemeinsam darauf hinarbeiten, das öffentliche Bewußtsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, gute fachliche Praktiken zum Schutz von Informationstechnologien zu fördern, Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität zu entwickeln, die Weiterentwicklung von Frühwarnsystemen und Mechanismen der Krisenbewältigung anzuregen und so insgesamt die Zusammenarbeit auf EU-Ebene zu verbessern. Dies wäre eine EU-eigenes Gremium nach Vorbild der erfolgreich arbeitenden Foren in bestimmten Mitgliedstaaten. In den Mitgliedstaaten, in denen noch keine derartigen Foren vorhanden sind, würde die Kommission ihre Einrichtung anregen. Das EU-Forum würde die Zusammenarbeit zwischen den einzelstaatlichen Foren fördern und erleichtern.
- Die Kommission setzt ihre Arbeiten zur Stärkung der Sicherheit und des Vertrauens im Rahmen ihrer Initiative "eEurope", des Aktionsplans der Gemeinschaft zur Förderung der sicheren Nutzung des Internet, des IST-Programms und des nächsten Rahmenprogramms im Bereich Forschung, technologische Entwicklung und Demonstration fort. Im Dialog mit allen interessierten Parteien fördert sie insbesondere die Verfügbarkeit von sicheren Produkten und Diensten sowie die freiere Verwendung starker Verschlüsselung.
- Im Rahmen der bestehenden Programme fördert die Kommission weitere Projekte zur Schulung des Personals von Strafverfolgungsbehörden in Fragen der High-Tech-Kriminalität und zur Unterstützung von Forschungsmaßnahmen auf dem Gebiet der Computerkriminaltechnik.
- Die Kommission prüft die Bereitstellung von Finanzmitteln für Maßnahmen zur Verbesserung von Inhalt und Benutzerfreundlichkeit der durch die COMCRIME-Studie eingerichteten Datenbank über die nationalen Rechtsvorschriften der Mitgliedstaaten, und sie führt eine spezifische Studie durch, die ihr ein genaueres Bild von Art und Ausmaß der Computerkriminalität in den Mitgliedstaaten vermitteln soll.

### **7.3. Maßnahmen in sonstigen internationalen Foren**

Auch in den sonstigen internationalen Foren, in denen Fragen der Cyberkriminalität erörtert werden (Europat, G8 usw.), wird die Kommission weiterhin eine führende Rolle bei der Koordinierung zwischen den Mitgliedstaaten spielen. Die Initiativen der Kommission auf EU-Ebene werden den in anderen internationalen Foren erzielten Fortschritten in vollem Umfang Rechnung tragen und dabei auf eine EU-weite Angleichung abstellen.

\* \* \* \* \*

## **FINANZBOGEN**

### **1. BEZEICHNUNG DER MASSNAHME**

Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität.

### **2. HAUSHALTSLINIEN**

B5 302

B5 820

B6 1110, B6 2111, B6 1210

### **3. RECHTSGRUNDLAGE**

Art. 95, 154 und 155 EG-Vertrag sowie Art. 29 und 34 EU-Vertrag.

### **4. BESCHREIBUNG DER MASSNAHME**

#### **4.1. Allgemeines Ziel**

Die Kommission richtet ein EU-Forum ein, in dem Strafverfolgungsbehörden, Internet-Diensteanbieter, Telekommunikationsbetreiber, Bürgerrechtsorganisationen, Vertreter der Verbraucher, Datenschutzbehörden sowie andere interessierte Parteien unter Vorsitz der Kommission zusammengebracht werden, um ihr gegenseitiges Verständnis und ihre Zusammenarbeit auf EU-Ebene zu fördern. Ziel des Forums wird es auch sein, das öffentliche Bewußtsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, optimale Sicherheitsbedingungen zu schaffen, Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität aufzuzeigen und die Weiterentwicklung von Frühwarnsystemen und Mechanismen der Krisenbewältigung anzuregen. Alle einschlägigen Dokumente werden auf einer eigens eingerichteten Website veröffentlicht.

#### **4.2. Dauer der Maßnahme und eventuelle Verlängerung**

2001 bis 2002. Im Jahre 2002 wird nach einer Auswertung entschieden, ob das Forum weitergeführt werden soll.

### **5. EINSTUFUNG DER EINNAHMEN UND AUSGABEN**

#### **5.1. Nichtobligatorische Ausgaben**

#### **5.2. Getrennte Mittel**

## 6. ART DER EINNAHMEN UND AUSGABEN

<b>Sitzungen: Reisekostenerstattung für Sachverständige</b>			
B5 302A	2001		27.000 €
B5 302A	2002		40.500 €
<b>Betrieb des Forums und seiner Website</b>			
B6 1110	2001	JRC: Dienstreisen	10.000 €
B6 2111	2001	JRC: spezifische Mittel (Verschiedenes)	15.000 €
B6 1210	2001	JRC: Betriebskosten	50.000 €
B6 1110	2002	JRC: Dienstreisen	10.300 €
B6 2111	2002	JRC: spezifische Mittel (Verschiedenes)	15.450 €
B6 1210	2002	JRC: Betriebskosten	51.500 €
<b>Studien zu spezifischen Fragen</b>			
B6 2111	2001	JRC: spezifische Mittel (Studien)	25.000 €
B6 2111	2002	JRC: spezifische Mittel (Studien)	25.750 €
Insges.	2001 + 2002		270.500 €

## 7. FINANZIELLE AUSWIRKUNGEN

### **Berechnungsmethode für die Gesamtkosten der Maßnahme (Verhältnis der individuellen Kosten zu den Gesamtkosten):**

Erstattung der Reisekosten der Sitzungsteilnehmer. Voraussichtlich werden im Jahre 2001 2 Sitzungen stattfinden und im Jahre 2002 3 Sitzungen. Je Sitzung erhalten 15 Sachverständige die Kosten erstattet. Die Erstattungskosten werden auf durchschnittlich 900 € pro Person veranschlagt.

Sowohl in bezug auf das Personal als auch in bezug auf spezifische Mittel werden die Kosten von Infrastruktur und administrativer bzw. technischer Unterstützung im Verhältnis zur Zahl der den betreffenden Tätigkeiten zugewiesenen Beamten ausgewiesen. Der Mittelbedarf für Studien wurde auf der Grundlage berechnet, daß pro Jahr 2 Studien mit einem Personalaufwand von jeweils 1 Mann-Monat durchgeführt werden.

## 8. BETRUGBEKÄMPFUNGSMASSNAHMEN

Routinekontrollen, ansonsten sind keine weiteren Maßnahmen zur Betrugsprävention geplant.

## 9. KOSTEN-NUTZEN-ANALYSE

### 9.1. Spezifische und quantifizierte Ziele; Zielgruppen

Förderung des gegenseitigen Verständnisses und der Zusammenarbeit verschiedener Interessengruppen. Zielteilnehmer: Strafverfolgungsbehörden, Internet-Diensteanbieter, Telekommunikationsbetreiber, Bürgerrechtsorganisationen, Vertreter der Verbraucher, Datenschutzbehörden sowie andere interessierte Parteien.

### 9.2. Begründung der Maßnahme

Die Einrichtung des Forums verfolgt den Zweck, das gegenseitige Verständnis verschiedener Interessengruppen sowie ihre Zusammenarbeit auf EU-Ebene zu fördern. Ziel des Forums wird es auch sein, das öffentliche Bewußtsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, optimale Sicherheitsbedingungen zu schaffen, Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität aufzuzeigen und die Weiterentwicklung von Frühwarnsystemen und Mechanismen der Krisenbewältigung anzuregen.

### 9.3. Monitoring und Auswertung der Maßnahme

Die Kommission organisiert und leitet die Forumssitzungen. Sie betreut zudem den eigens eingerichteten Internetauftritt. Im Jahre 2002 wird geprüft, inwieweit eine Fortsetzung des Forums im Jahre 2003 erforderlich ist.

## 10. VERWALTUNGS-AUSGABEN

Der Personalbedarf wird durch vorhandenes Personal gedeckt.

### 10.1. Auswirkung auf die Gesamtstellenzahl

Art der Stelle	Mit der Maßnahmendurchführung zu betrauendes Personal		Quelle		Dauer
	Dauerplanstellen	Planstellen auf Zeit	Vorhandene Ressourcen der GD	Zusätzliche Ressourcen	
A-Beamte Oder Zeitbedienstete der Laufbahngruppe A B-Personal C-Personal	0,05	1,75 0,15	1,75 0,15 0,05		Pro Jahr, 2 Jahre
Sonstige Ressourcen					
Insgesamt	0,05	1,9	1,95		

### 10.2 Gesamtkostenaufwand für Personal

	Betrag	Berechnungsmethode (2001 - 2002)
Beamte	421.200 €	2 Jahre x 108.000 € x 1,95 Personaleinheiten