KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 22.5.2007
KOM(2007) 267 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT UND DEN AUSSCHUSS DER REGIONEN

Eine allgemeine Politik zur Bekämpfung der Internetkriminalität

{SEK(2007) 641}
{SEK(2007) 642}

MITTEILUNG DER KOMMISSION
AN DAS EUROPÄISCHE PARLAMENT, DEN RAT
UND DEN AUSSCHUSS DER REGIONEN

Eine allgemeine Politik zur Bekämpfung der Internetkriminalität

1. EINFÜHRUNG

1.1. Was ist Internetkriminalität?

Einer der wichtigsten Aspekte im Hinblick auf die Sicherheit der in unserer Gesellschaft immer bedeutsamer werdenden Informationssysteme ist die Bekämpfung der Internetkriminalität. Diese Art von Kriminalität ist bisher nicht einheitlich definiert worden und wird daher häufig auch mit den austauschbaren Begriffen „Cyberkriminalität", „Computerkriminalität" und „Hightechkriminalität" umschrieben. Zum Zwecke dieser Mitteilung werden nachfolgend unter dem Begriff „Internetkriminalität" alle kriminellen Handlungen verstanden, die mittels elektronischer Kommunikationsnetze und Informationssysteme begangen oder gegen derartige Netze und Systeme verübt werden.

In der Praxis wird der Begriff „Internetkriminalität" auf drei Arten von kriminellen Handlungen angewandt. Dabei handelt es sich zum einen um **herkömmliche Straftaten** wie Betrug und Fälschung, worunter im Zusammenhang mit dem Begriff „Internetkriminalität" allerdings besonders solche Delikte dieser Art verstanden werden, die über elektronische Kommunikationsnetze und Informationssysteme (nachfolgend unter dem Begriff „elektronische Netze" zusammengefasst) begangen werden. Zum Zweiten handelt es sich um das Veröffentlichen **illegaler Inhalte** über elektronische Medien (z.B. über den sexuellen Missbrauch von Kindern oder zur Anstachelung zu Rassenhass). Die dritte Kategorie beinhaltet **Straftaten gegen elektronische Netze**, d.h. Angriffe auf Informationssysteme, Denial-of-service-Angriffe und Hacking. Diese Angriffe können sich auch gegen wichtige Infrastrukturen in Europa richten und die in zahlreichen Bereichen bestehenden Frühwarnsysteme beeinträchtigen, was unter Umständen verheerende Folgen für die gesamte Gesellschaft haben könnte. Alle drei Kategorien haben gemein, dass das Ausmaß derartiger Straftaten ebenso wie die geografische Entfernung zwischen der einzelnen Straftat und ihren Auswirkungen beträchtlich sein kann. Daher erfordern die Untersuchungsmethoden häufig auch einen entsprechend großen technischen Aufwand. Diese Gemeinsamkeiten bilden das zentrale Thema dieser Mitteilung.

1.2. Die aktuelle Entwicklung auf dem Gebiet der Internetkriminalität

1.2.1. Allgemeine Entwicklungstrends

Da sich die Internetkriminalität kontinuierlich wandelt und es an verlässlichen Informationen zu diesem Bereich mangelt, ist es schwierig, sich ein genaues Bild der derzeitigen Situation zu machen. Gleichwohl sind folgende allgemeine Entwicklungstrends erkennbar:

- Die Zahl der Internetstraftaten wächst, und die betreffenden Delikte werden immer raffinierter und in zunehmendem Maße über Ländergrenzen hinweg begangen[1].

- Es gibt klare Anzeichen für eine zunehmende Verstrickung organisierter Verbrechergruppen in die Internetkriminalität.

- Gleichzeitig wird in der EU die Strafverfolgung im Wege der grenzübergreifenden Zusammenarbeit der Strafverfolgungsbehörden nicht ausgeweitet.

1.2.2. Herkömmliche Straftaten im Zusammenhang mit elektronischen Netzen

Die meisten Straftaten können unter Rückgriff auf elektronische Netze begangen werden. Besonders verbreitet sind bestimmte, mit Hilfe elektronischer Netze begangene Fälle von Betrug oder versuchtem Betrug, und die Zahl dieser Delikte nimmt zu. Mit Hilfe von Instrumenten wie Identitätsdiebstahl, Phishing[2], Spams und bösartigem Code können groß angelegte Betrugsdelikte verübt werden. Ein weiteres wachsendes Problem ist der illegale nationale oder internationale Handel über das Internet, darunter der Handel mit Drogen, gefährdeten Arten und Waffen.

1.2.3. Illegale Inhalte

In Europa wächst die Zahl der Webseiten mit illegalen Inhalten, auf denen Material über den sexuellen Missbrauch von Kindern angeboten, zu terroristischen Handlungen aufgestachelt oder Gewalt, Terrorismus, Rassismus und Fremdenfeindlichkeit verherrlicht wird. Ein strafrechtliches Vorgehen gegen derartige Webseiten ist äußerst schwierig, da die Webseitenanbieter und -betreiber oftmals in anderen Ländern und zudem häufig außerhalb der EU ansässig sind. Webseiten lassen sich rasch in ein anderes Land (auch außerhalb der EU) verlegen, und zwischen den Ländern bestehen zum Teil erhebliche Unterschiede bei den einschlägigen Straftatbeständen.

1.2.4. Straftaten gegen elektronische Netze

Eine immer größere Bedeutung spielen groß angelegte, häufig über sogenannte Botnets[3] verübte Angriffe gegen Informationssysteme, Organisationen und Einzelpersonen. Zudem sind unlängst Zwischenfälle mit systematischen, gut koordinierten und groß angelegten direkten Angriffen auf wichtige Informationsinfrastrukturen eines Staates beobachtet worden. Die Verschmelzung von Technologien und die rasant fortschreitende Vernetzung von Informationssystemen, die diese Systeme angreifbarer gemacht haben, erleichtern derartige Angriffe. Diese sind oft gut organisiert und verfolgen erpresserische Ziele. Dabei darf davon ausgegangen werden, dass überhaupt nur ein geringer Teil derartiger Angriffe gemeldet wird, weil beispielsweise einem Unternehmen geschäftliche Nachteile entstehen können, wenn bekannt wird, dass es Sicherheitsprobleme hat.

---

[1] Die in dieser Mitteilung zum Ausdruck gebrachten Standpunkte zu den gegenwärtigen Entwicklungstrends wurden größtenteils aus der von der Kommission im Jahr 2006 in Auftrag gegebenen Studie zur Bewertung der Auswirkungen einer Mitteilung über die Internetkriminalität (Vertrag Nr. JLS/2006/A1/003) übernommen.

[2] Der Begriff „Phishing“ bezeichnet den Versuch, im Rahmen der elektronischen Kommunikation auf betrügerische Weise an sensible Daten wie Passwörter oder Kreditkarteninformationen zu gelangen, indem sich die Täter als vertrauenswürdige Personen ausgeben.

[3] Unter einem Botnet oder Bot-Netz (die Kurzform von Roboter-Netzwerk) versteht man ein fernsteuerbares Netz von infizierten Rechnern.

1.3. Ziele

Angesichts dieser sich rasch ändernden Entwicklung ist es dringend erforderlich, sowohl auf nationaler Ebene als auch auf EU-Ebene gegen sämtliche Formen der Internetkriminalität vorzugehen, welche eine wachsende Bedrohung für kritische Infrastrukturen, die Gesellschaft, die Wirtschaft und die Bürger darstellen. Der Schutz gegen die Internetkriminalität wird häufig durch Aspekte wie die Frage der Bestimmung der zuständigen Gerichtsbarkeit, die anwendbaren Rechtsvorschriften, die grenzübergreifende Strafverfolgung oder die Zulässigkeit und Verwendung von elektronischen Beweismitteln erschwert, weil Internetkriminalität zumeist über Ländergrenzen hinweg verübt wird. Um dieser Bedrohung entgegenzuwirken, möchte die Kommission eine allgemeine politische Initiative ins Leben rufen, durch die die Koordinierung der Maßnahmen zur Bekämpfung der Internetkriminalität auf europäischer und auf internationaler Ebene verbessert werden soll.

Ziel ist eine schärfere Bekämpfung der Internetkriminalität auf nationaler, europäischer und internationaler Ebene. Die Mitgliedstaaten und die Kommission messen insbesondere der Weiterentwicklung einer spezifischen EU-Politik schon seit längerem vorrangige Bedeutung bei. Der Schwerpunkt der Initiative wird auf den Strafverfolgungs- und Strafrechtsaspekten des Vorgehens gegen die Internetkriminalität liegen, und die diesbezügliche Politik wird darauf abstellen, andere Maßnahmen der EU zur Verbesserung der allgemeinen Sicherheit im Internet sinnvoll zu ergänzen. Sie wird sich auf folgende Aspekte beziehen: Verbesserung der operativen Zusammenarbeit bei der Strafverfolgung, Verbesserung der politischen Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten, politische und rechtliche Zusammenarbeit mit Drittländern, Sensibilisierung, Schulungsmaßnahmen, Forschung, Verstärkung des Dialogs mit der Wirtschaft und mögliche Legislativmaßnahmen.

Bei der Festlegung und Umsetzung der Politik zur Bekämpfung und strafrechtlichen Verfolgung der Internetkriminalität werden die Grundrechte und insbesondere die Meinungsfreiheit sowie der Schutz der Privatsphäre, der Schutz der Familie und der Schutz personenbezogener Daten in vollem Umfang gewahrt bleiben. Etwaige im Rahmen dieser Politik ausgearbeitete Legislativmaßnahmen werden vorab auf ihre Vereinbarkeit mit diesen Rechten und insbesondere mit der EU-Grundrechtscharta geprüft werden. Zudem werden alle diese politischen Initiativen nach Maßgabe von Artikel 12 bis 15 der „Richtlinie über den elektronischen Geschäftsverkehr“[4] durchgeführt werden, sofern diese anwendbar sind.

Das Ziel dieser Mitteilung lässt sich in drei operative Unterziele untergliedern:

- Verbesserung und Erleichterung der Absprache und Zusammenarbeit zwischen den mit der Bekämpfung der Internetkriminalität befassten Stellen sowie sonstigen zuständigen Behörden und Sachverständigen in der Europäischen Union;

- Entwicklung eines kohärenten politischen Rahmens der EU für die Bekämpfung der Internetkriminalität in Absprache mit den Mitgliedstaaten, den innerhalb der EU oder auf internationaler Ebene zuständigen Organisationen und sonstigen Beteiligten;

---

[4] 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 (ABl. L 178 vom 17.7.2000, S. 1).

- Schärfung des Bewusstseins für die durch die Internetkriminalität verursachten Kosten und Gefahren.

2. GELTENDE RECHTSINSTRUMENTE ZUR BEKÄMPFUNG DER INTERNETKRIMINALITÄT

2.1. Bestehende Instrumente und Maßnahmen auf EU-Ebene

Die vorliegende Mitteilung über eine allgemeine Politik zur Bekämpfung der Internetkriminalität knüpft an die Mitteilung „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" aus dem Jahr 2001[5] (nachfolgend „Mitteilung aus dem Jahr 2001") an. Darin wurden seinerzeit umfassende verfahrensrechtliche Bestimmungen zur Bekämpfung von inländischen und grenzüberschreitenden Straftaten vorgeschlagen. In der weiteren Folge ergingen mehrere weitere wichtige Vorschläge zu diesem Bereich, darunter insbesondere der Vorschlag für den Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme[6]. In diesem Zusammenhang ist darauf hinzuweisen, dass zudem weitere, allgemeinere Rechtsvorschriften erlassen worden sind, die ebenfalls bestimmte Aspekte der Bekämpfung der Internetkriminalität abdecken, so beispielsweise der Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[7].

Der Rahmenbeschluss 2004/68/JI zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie[8] ist ein gutes Beispiel für die besondere Bedeutung, die die Kommission dem **Schutz von Kindern** und insbesondere dem Kampf gegen alle Formen von Material über den sexuellen Missbrauch von Kindern, das in verbotener Weise und unter Rückgriff auf Informationssysteme veröffentlicht wird, beimisst. Dieses vorrangige horizontale Ziel wird die Kommission auch in Zukunft weiterverfolgen.

Um gegen die Bedrohungen für die Sicherheit der Informationsgesellschaft vorzugehen, hat die Europäische Gemeinschaft einen dreigleisigen Ansatz entwickelt, der auf spezifische Maßnahmen zur Stärkung der Netz- und Informationssicherheit, auf die Schaffung eines rechtlichen Rahmens für die elektronische Kommunikation und auf die Bekämpfung der Internetkriminalität abstellt. Diese drei Teilaspekte könnten zwar in gewissem Umfang separat verfolgt werden, aber die zahlreichen Abhängigkeiten, die zwischen ihnen bestehen, machen eine enge Koordinierung unabdingbar. In diesem Zusammenhang nahm die Kommission im Jahr 2001 parallel zu ihrer Mitteilung über die Internetkriminalität die Mitteilung „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz"[9] an. Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) verpflichtet die Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten, die Sicherheit ihrer Dienste zu gewährleisten und enthält zudem Bestimmungen zur Bekämpfung von Spam und Spyware. Der Politikansatz zur Netz- und Informationssicherheit ist im Wege mehrerer einschlägiger

---

5 KOM(2000) 890 vom 26.1.2001.
6 ABl. L 69 vom 16.3.2005, S. 67.
7 ABl. L 149 vom 2.6.2001, S. 1.
8 ABl. L 13 vom 20.1.2004, S. 44.
9 KOM(2001) 298.

Maßnahmen weiterentwickelt worden, darunter die unlängst angenommene Mitteilung „Eine Strategie für eine sichere Informationsgesellschaft“[10], in der ein Rahmen und eine erneuerte Strategie für einen gezielteren, kohärenten Ansatz zur Netz- und Informationssicherheit vorgeschlagen wurde, die unlängst veröffentlichte Mitteilung über die Bekämpfung von Spam, Späh- und Schadsoftware[11] und die Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Jahr 2004[12]. Hauptziel der ENISA ist die Entwicklung von Fachwissen zur Intensivierung der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor und zur Unterstützung der Kommission und der Mitgliedstaaten. Von großer Bedeutung für die Bekämpfung der Internetkriminalität sind auch die **Forschungsergebnisse** auf dem Gebiet von Technologien zum Schutz von Informationssystemen. Informations- und Kommunikationstechnologien sowie Sicherheitsaspekte zählen daher auch zu den Zielen des Siebten Forschungsrahmenprogramms der EU für den Zeitraum 2007-2013[13]. Zudem könnte die Überprüfung des bestehenden rechtlichen Rahmens für die elektronische Kommunikation Änderungen im Hinblick auf eine größere Wirksamkeit der sich auf Sicherheitsfragen beziehenden Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation und der Richtlinie 2002/22/EG („Universaldienstrichtlinie“) zur Folge haben[14].

2.2. Bestehende internationale Instrumente

Da Informationsnetze die gesamte Welt umspannen, kann eine auf die EU beschränkte Politik zur Bekämpfung der Internetkriminalität nicht wirklich wirksam sein. Angriffe auf Informationssysteme und sonstige Straftaten können nicht nur länderübergreifend zwischen Mitgliedstaaten begangen, sondern auch ohne Mühe von außerhalb der gerichtlichen Zuständigkeit der EU liegenden Ländern begangen werden. Aus diesem Grund wirkt die Kommission aktiv in internationalen Gesprächs- und Kooperationsgremien wie der Lyon-Rom-Arbeitsgruppe der G8 zur Bekämpfung der Hightechkriminalität und den einschlägigen Projekten von Interpol mit. Auch die Arbeiten des allzeit erreichbaren Informationsnetzes der G8 über die grenzüberschreitende Hightechkriminalität[15], an dem zahlreiche Länder und auch die meisten EU-Staaten teilnehmen, werden von der Kommission aufmerksam verfolgt. Das Netz ermöglicht eine rasche Kontaktaufnahme zwischen den allzeit erreichbaren Kontaktstellen der teilnehmenden Länder in Fällen, in denen elektronisches Beweismaterial vorliegt und dringend Amtshilfe ausländischer Strafverfolgungsbehörden benötigt wird.

Die wohl wichtigste europäische und völkerrechtliche Rechtsvorschrift auf diesem Gebiet ist das Europarat-Übereinkommen über Cyberkriminalität aus dem Jahr 2001[16]. Das im Jahr 2004 angenommene und in Kraft getretene Übereinkommen enthält gemeinsame Definitionen der verschiedenen Arten von Internetkriminalität und bildet die Grundlage für eine funktionierende justizielle Zusammenarbeit zwischen den teilnehmenden Ländern. Zahlreiche Länder (darunter die Vereinigten Staaten und weitere Nicht-EU-Länder sowie alle EU-Mitgliedstaaten) haben das Übereinkommen bereits unterzeichnet. Gleichwohl haben einige

---

10 KOM(2006) 251.

11 KOM(2006) 688.

12 Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1).

13 Die Europäische Union hat bereits im Rahmen des 6. Rahmenprogramms für Forschung und technologische Entwicklung mehrere einschlägige (und erfolgreiche) Forschungsprojekte gefördert.

14 Siehe KOM(2006) 334, SEK(2006)816 und SEK(2006) 817.

15 Siehe Artikel 35 des Europarat-Übereinkommens über Cyberkriminalität.

16 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Mitgliedstaaten das Übereinkommen oder das Zusatzprotokoll zum Übereinkommen über Cyberkriminalität über die strafrechtliche Verfolgung rassistischer oder fremdenfeindlicher Handlungen, die mittels Computernetzen begangen werden, noch nicht ratifiziert. Aufgrund der großen Bedeutung, die dem Abkommen von allen Beteiligten beigemessen wird, wird die Kommission die Mitgliedstaaten und die betroffenen Drittländer ermutigen, das Übereinkommen zu ratifizieren und die Möglichkeit des Beitritts der Europäischen Gemeinschaft zu dem Übereinkommen zu prüfen.

3. WEITERENTWICKLUNG SPEZIFISCHER INSTRUMENTE ZUR BEKÄMPFUNG DER INTERNETKRIMINALITÄT

3.1. Verstärkung der operativen Zusammenarbeit zwischen Strafverfolgungsbehörden und der Schulungsmaßnahmen auf EU-Ebene

Ein großer Schwachpunkt auf dem Gebiet der Justiz, Freiheit und Sicherheit ist nach wie vor, dass es an geeigneten Strukturen für eine unmittelbare **grenzübergreifende operative Zusammenarbeit** mangelt bzw. die vorhandenen Strukturen nicht ausreichend genutzt werden. Die herkömmliche Amtshilfe hat sich in dringenden Fällen von Internetkriminalität als langsam und ineffizient erwiesen, und neue Kooperationsstrukturen sind noch nicht ausreichend entwickelt worden. Zwar erfolgt in Europa eine enge Zusammenarbeit zwischen den nationalen Justiz- und Strafverfolgungsbehörden im Rahmen von Europol, Eurojust und anderen Strukturen, doch besteht die klare Notwendigkeit, die Zuständigkeiten zu verstärken und zu klären. Die Ergebnisse der von der Kommission diesbezüglich unternommenen Konsultation legen den Schluss nahe, dass diese wichtigen Kooperationskanäle nicht optimal genutzt werden. Daher bedarf es eines besser koordinierten operativen und strategischen Ansatzes der EU, der auch den Austausch von Informationen und bewährten Praktiken einschließt.

Die Kommission möchte künftig besonderes Gewicht auf **Schulungsmaßnahmen** legen. Es hat sich gezeigt, dass es die technologische Weiterentwicklung erforderlich macht, das Personal von Strafverfolgungs- und Justizbehörden kontinuierlich in Fragen der Bekämpfung der Internetkriminalität zu schulen. Daher ist geplant, die von der EU gewährte finanzielle Unterstützung für multinationale Fortbildungsprogramme zu verstärken und besser zu koordinieren. Darüber hinaus wird die Kommission in enger Zusammenarbeit mit den Mitgliedstaaten und anderen kompetenten Einrichtungen wie Europol, Eurojust, der Europäischen Polizeiakademie (EPA) und dem Europäischen Netz für die Aus- und Fortbildung von Richtern und Staatsanwälten (EJNT) versuchen, die einschlägigen Schulungs- und Fortbildungsprogramme aufeinander abzustimmen und miteinander zu verbinden.

Die Kommission wird noch im Jahr 2007 eine **Zusammenkunft** für Strafverfolgungsexperten der Mitgliedstaaten, von Europol, der EPA und des EJTN veranstalten, bei der erörtert werden soll, wie die strategische und die operative Zusammenarbeit sowie die Schulungsmaßnahmen zur Bekämpfung der Internetkriminalität in Europa verbessert werden können. Eines der Gesprächsthemen wird die mögliche Einrichtung einer ständigen Kontaktstelle der EU für den Informationsaustausch und einer Schulungsplattform der EU für Schulungen zur Bekämpfung der Internetkriminalität bilden. Das für 2007 vorgesehene Treffen wird den Auftakt zu einer ganzen Reihe von für die nahe Zukunft vorgesehenen Zusammenkünften bilden.

3.2. Verstärkter Dialog mit der Wirtschaft

Sowohl der private als auch der öffentliche Sektor hat ein Interesse daran, gemeinsame Methoden zur Erkennung und Verhütung von aus kriminellen Handlungen resultierenden Schäden zu entwickeln. Eine auf gegenseitigem Vertrauen fußende und auf Schadensminderung abzielende Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor bietet nicht zuletzt auch mit Blick auf die Bekämpfung der Internetkriminalität aussichtsreiche Chancen für eine wirksame Verbesserung der Sicherheit. Die Kommission wird diesen Aspekt ihrer Politik zur Bekämpfung der Internetkriminalität zu gegebener Zeit in die von ihr ins Auge gefasste globale EU-Politik zur Förderung des Dialogs zwischen dem öffentlichen und dem privaten Sektor, die den gesamten Bereich der Sicherheit in der EU abdecken wird, integrieren. Diese Politik wird insbesondere im Rahmen des Europäischen Forums für Sicherheitsforschung und Innovation (European Security Research and Innovation Forum, ESRIF) weiterentwickelt werden, das die Kommission in Kürze einzurichten gedenkt und an dem die wichtigsten Betroffenen aus dem öffentlichen und dem privaten Sektor teilnehmen werden.

Die Entwicklung moderner Informationstechnologien und elektronischer Kommunikationssysteme erfolgt weitgehend durch die Privatwirtschaft. So führen private Unternehmen Gefahrenabschätzungen durch, stellen Verbrechensbekämpfungsprogramme auf und entwickeln technische Lösungen zur Kriminalitätsverhütung. Die Wirtschaft hat sich bisher in Bezug auf die Unterstützung der Behörden bei der Bekämpfung der Internetkriminalität (und insbesondere der Verbreitung von Kinderpornografie[17] und sonstigen illegalen Inhalten über das Internet) sehr entgegenkommend gezeigt.

Ein Problem ist der mangelnde Austausch von Informationen, Fachwissen und bewährten Praktiken zwischen dem öffentlichen und dem privaten Sektor. Um Geschäftsmodelle und Geschäftsgeheimnisse zu schützen, scheuen Privatunternehmen häufig davor zurück (oder sind gesetzlich auch gar nicht eindeutig dazu verpflichtet), der Polizei sachdienliche Informationen über gegen sie verübte Straftaten zu melden. Für eine effiziente und geeignete Kriminalitätsbekämpfungspolitik der Behörden können derartige Informationen gleichwohl von großer Bedeutung sein. Ferner ist geplant, die Möglichkeiten für eine Verbesserung des sektorübergreifenden Informationsaustausches im Lichte der geltenden Rechtsvorschriften über den Schutz personenbezogener Daten zu prüfen.

Die Kommission spielt eine wichtige Rolle in den verschiedenen mit der Bekämpfung der Internetkriminalität befassten gemeinsamen Gremien des öffentlichen und des privaten Sektors wie beispielsweise der Sachverständigengruppe „Betrugsprävention“[18]. Die Kommission ist davon überzeugt, dass eine allgemeine Politik zur Bekämpfung der Internetkriminalität, um Wirkung entfalten zu können, auch eine Strategie für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor einschließlich der gesellschaftlichen Organisationen umfassen muss.

Um die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor auf diesem Gebiet auszuweiten, wird die Kommission noch im Jahr 2007 eine Konferenz für Strafverfolgungsexperten und Vertreter des Privatsektors (insbesondere Internet-

---

[17] Ein Beispiel für die Zusammenarbeit auf diesem Gebiet war unlängst die Kooperation zwischen den Strafverfolgungsbehörden und den Kreditkartenunternehmen, welche der Polizei dabei behilflich waren, die Käufer von kinderpornografischem Material im Internet zu ermitteln.

[18] Siehe http://ec.europa.eu/internal_market/payments/fraud/index_de.htm

Diensteanbieter) ausrichten, auf der Möglichkeiten für eine Verbesserung der operativen Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor in Europa ausgelotet werden sollen[19]. Auf der Konferenz sollen allesamt Themen erörtert werden, die für beide Sektoren von Nutzen sein können, also beispielsweise

- die Verbesserung der operativen Zusammenarbeit bei der Bekämpfung von Straftaten und illegalen Inhalten im Internet, insbesondere von terroristischen Handlungen, Kinderpornografie und sonstigen aus Sicht des Kinderschutzes besonders schweren Straftaten,

- Vereinbarungen zwischen dem öffentlichen und dem privaten Sektor über das EU-weite Blockieren von Webseiten mit illegalen und insbesondere mit kinderpornografischen Inhalten,

- Die Entwicklung eines europäischen Modells für den Austausch von erforderlichen und sachdienlichen Informationen zwischen dem privaten und dem öffentlichen Sektor, das eine Atmosphäre des gegenseitigen Vertrauens schafft und den Interessen aller Beteiligten Rechnung trägt.

- Aufbau eines Netzes von Ansprechpartnern für die Strafverfolgungsbehörden im privaten und im öffentlichen Sektor.

3.3. Rechtsvorschriften

Eine allgemeine Angleichung der Straftatbestände und der nationalen Strafrechtsvorschriften auf dem Gebiet der Internetkriminalität ist noch nicht angebracht, da mit diesem Begriff zurzeit noch zu viele unterschiedliche Delikte abgedeckt werden. Da eine wirksame Zusammenarbeit zwischen Strafverfolgungsbehörden in den meisten Fällen nur möglich ist, wenn die betreffenden Straftatbestände zumindest teilweise angeglichen wurden, muss es weiterhin auf lange Sicht darum gehen, die Rechtsvorschriften der Mitgliedstaaten noch weiter einander anzugleichen[20]. Ein wichtiger Fortschritt auf dem Wege zur Angleichung bestimmter zentraler Tatbestände wurde bereits in Form des Rahmenbeschlusses über Angriffe auf Informationssysteme aus dem Jahr 2005 erzielt. Wie bereits ausgeführt wurde, sind seither jedoch neue Bedrohungen aufgetaucht, und die Kommission beobachtet die diesbezügige Entwicklung sehr aufmerksam, da es sehr wichtig ist, die Notwendigkeit etwaiger weiterer Rechtsvorschriften kontinuierlich zu bewerten. Die Überwachung dieser neuen Bedrohungen wird eng koordiniert mit dem Europäischen Programm zum Schutz kritischer Infrastrukturen.

Nichtsdestoweniger sollte bereits zum jetzigen Zeitpunkt über gezielte Rechtsvorschriften zur Bekämpfung der Internetkriminalität nachgedacht werden. Ein besonderer Punkt, der eine gesetzliche Regelung erforderlich machen könnte, ist die in Verbindung mit **Identitätsdiebstahl** begangene Internetkriminalität. Allgemein wird unter „Identitätsdiebstahl“ der Diebstahl und die Verwendung von personenbezogenen Daten (Beispiel: Kreditkartennummer) zur Begehung einer anderen Straftat verstandenen. In den meisten Mitgliedstaaten wird eine solche Handlung zumeist als Betrugsdelikt oder eine andere

---

[19] Die Konferenz ist als Fortführung des in Abschnitt 6.4 der Mitteilung über die Computerkriminalität vorgestellten EU-Forums anzusehen.

[20] Dieses langfristige Ziel wurde bereits in der Mitteilung von 2001 (auf Seite 3) angesprochen.

Straftat verfolgt, nicht jedoch als „Identitätsdiebstahl“, da Betrug als schwereres Verbrechen gilt. Identitätsdiebstahl ist in keinem Mitgliedstaat ein eigenständiger Straftatbestand. Da er sich jedoch leichter nachweisen lässt als Betrug, wäre der Zusammenarbeit der Strafverfolgungsbehörden in der EU sehr damit gedient, wenn es einen solchen Straftatbestand in allen Mitgliedstaaten gäbe. Die Kommission wird daher noch im Jahr 2007 eine Konsultation in die Wege leiten, um zu ermitteln, ob hier rechtlicher Handlungsbedarf besteht.

3.4. Erhebung von statistischen Daten

Es herrscht Einigkeit darüber, dass der derzeitige Informationsstand über die Kriminalitätshäufigkeit weitgehend unzureichend ist und vor allem noch viel verbessert werden muss, um die Daten der einzelnen Mitgliedstaaten miteinander vergleichen zu können. Zu diesem Zweck hat die Kommission in ihrer Mitteilung „Entwicklung einer umfassenden und kohärenten EU-Strategie zur Messung von Kriminalität und Strafverfolgung: EU-Aktionsplan 2006-2010“[21] einen ehrgeizigen Fünfjahresplan zur Lösung dieses Problems aufgestellt. Die in dem Aktionsplan vorgesehene Sachverständigengruppe soll ein geeignetes Forum für die Ausarbeitung einschlägiger Indikatoren zur Messung des Ausmaßes der Internetkriminalität bilden.

4. DAS WEITERE VORGEHEN

Die Kommission möchte nunmehr die allgemeine Politik zur Bekämpfung der Internetkriminalität weiterentwickeln. Allerdings kann diese Politik die von den Mitgliedstaaten und von anderen Einrichtungen ergriffenen Maßnahmen lediglich ergänzen, da die Befugnisse der Kommission auf strafrechtlichem Gebiet begrenzt sind. Die wichtigsten Maßnahmen werden den Rückgriff auf eines, mehrere oder alle in Kapitel 3 genannten Instrumente erfordern und zudem im Rahmen des Finanzprogramms zur Kriminalitätsverhütung und –bekämpfung gefördert werden. Im Einzelnen handelt es sich hierbei um folgende Maßnahmen:

4.1. Allgemeine Bekämpfung der Internetkriminalität

- Ausbau der operativen Zusammenarbeit zwischen den Strafverfolgungs- und Justizbehörden der Mitgliedstaaten; eingeleitet wird diese Maßnahme durch eine spezifische Sachverständigensitzung im Jahr 2007, in deren Rahmen beispielsweise ein zentraler Ansprechpartner der EU für Fragen der Bekämpfung der Internetkriminalität eingesetzt werden könnte;

- Verstärkung der finanziellen Unterstützung für Maßnahmen zur Verbesserung der Schulung von Strafverfolgungs- und Justizbeamten im Umgang mit Fällen von Internetkriminalität und Koordinierung aller multinationaler Schulungsmaßnahmen auf diesem Gebiet über eine dafür einzurichtende Schulungsplattform der EU;

- Förderung eines stärkeren Engagements der Mitgliedstaaten und der Behörden im Hinblick auf die Ergreifung wirksamer Maßnahmen zur Bekämpfung der Internetkriminalität und der Bereitstellung ausreichender Ressourcen;

---

[21] KOM(2006) 437 vom 7.8.2006.

- Unterstützung von Forschungsmaßnahmen für eine bessere Bekämpfung der Internetkriminalität;

- Veranstaltung von mindestens einer Konferenz (im Jahr 2007) für Vertreter von Strafverfolgungsbehörden und privaten Einrichtungen insbesondere zum Zwecke des Aufbaus einer Zusammenarbeit bei der Bekämpfung von über das Internet und über bzw. gegen elektronische Netze begangenen Straftaten und zur Förderung eines effizienteren Austausches von nicht personenbezogenen Daten sowie konkrete Kooperationsprojekte zwischen öffentlichen und privaten Stellen als Folgemaßnahme zu den Schlussfolgerungen dieser Konferenz;

- Anregung von und Teilnahme an gemeinsamen Maßnahmen öffentlicher und privater Stellen zur Stärkung des Bewusstseins (insbesondere der Verbraucher) für die durch die Internetkriminalität verursachten Kosten und Gefahren unter Vermeidung eines etwaigen Vertrauensverlustes der Verbraucher und Nutzer durch Überbetonung der negativen Aspekte der Sicherheitsvorkehrungen;

- Förderung der weltweiten Bekämpfung der Internetkriminalität und aktive Mitwirkung bei der diesbezüglichen Zusammenarbeit;

- Förderung und Unterstützung grenzübergreifender Projekte, die der einschlägigen Politik der Kommission entsprechen (beispielsweise Projekte der G 8, die in Übereinstimmung mit den Länder- und Regionalstrategiepapieren über die Zusammenarbeit mit Drittländern stehen);

- konkrete Maßnahmen, die alle Mitgliedstaaten und die betroffenen Drittländer dazu bewegen sollen, das Europarat-Übereinkommen über Cyberkriminalität und das einschlägige Zusatzprotokoll zu ratifizieren und die Möglichkeit des Beitritts der Europäischen Gemeinschaft zu dem Übereinkommen zu prüfen;

- Analyse (in Zusammenarbeit mit den Mitgliedstaaten) des Phänomens koordinierter und groß angelegter Angriffe auf Informationsinfrastrukturen von Mitgliedstaaten mit Blick auf die Verhinderung und Bekämpfung solcher Angriffe, einschließlich koordinierter Reaktionen, Informationsaustausch und bewährten Praktiken.

4.2. Bekämpfung von über elektronische Netze begangenen herkömmlichen Straftaten

- Einleitung einer gründlichen Analyse im Hinblick auf die Ausarbeitung eines Vorschlags für eine einschlägige EU-Rechtsvorschrift gegen Identitätsdiebstahl;

- Förderung der Entwicklung von technischen Methoden und Verfahren zur Bekämpfung des illegalen Handels im Internet (beispielsweise im Rahmen von Kooperationsprojekten zwischen dem öffentlichen und dem privaten Sektor);

- Fortsetzung und Weiterentwicklung der Arbeiten in bestimmten Zielbereichen wie der Bekämpfung des Betrugs mit bargeldlosen Zahlungsmitteln in elektronischen Netzen (Sachverständigengruppe „Betrugsprävention“).

4.3. Illegale Inhalte

- Entwicklung weiterer Maßnahmen gegen die Verbreitung von bestimmten illegalen Inhalten im Internet (insbesondere Material über den sexuellen Missbrauch von Kindern und zur Aufstachelung zu terroristischen Handlungen), vor allem im Wege des Follow-up zur Umsetzung des Rahmenbeschlusses zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie;

- Ermutigung der Mitgliedstaaten zur Bereitstellung ausreichender finanzieller Mittel zur Unterstützung der Arbeit der Strafverfolgungsbehörden und insbesondere der von diesen ergriffenen Maßnahmen zur Ermittlung der Opfer von Fällen von sexuellem Missbrauch, über die im Internet Material verbreitet wird;

- Einleitung und Unterstützung von Maßnahmen zur Bekämpfung illegaler Inhalte, die Minderjährige zu Gewalttaten und sonstigen schweren Straftaten verleiten können (bestimmte Online-Videospiele mit extremer Gewalt);

- Einleitung und Förderung eines Dialogs zwischen den Mitgliedstaaten und mit Drittländern über technische Methoden zur Bekämpfung illegaler Inhalte und über Verfahren zur Schließung von illegalen Webseiten (auch im Hinblick auf den möglichen Abschluss einschlägiger formeller Abkommen mit Nachbarländern und sonstigen Ländern);

- Abschluss von freiwilligen Abkommen und Übereinkommen auf EU-Ebene zwischen Behörden und privaten Einrichtungen (insbesondere Internet-Diensteanbieter) über Verfahren zur Blockierung und Schließung von Webseiten mit illegalen Inhalten.

4.4. Folgemaßnahmen

Die Kommission wird die in dieser Mitteilung vorgestellten, als nächste Schritte vorgesehenen Maßnahmen zur Verbesserung der Zusammenarbeit in der EU weiter vorantreiben, ihre Fortschritte ermitteln und dem Rat und dem Europäischen Parlament Bericht erstatten.