



KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

014057/EU XXIII.GP
Eingelangt am 24/05/07

Brüssel, den 22.5.2007
SEK(2007) 641

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

Begleitdokument zu der

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

Eine allgemeine Politik zur Bekämpfung der Internetkriminalität

Zusammenfassung der Folgenabschätzung

{KOM(2007) 267 endgültig}
{SEK(2007) 642}

Zusammenfassung

1. EINLEITUNG

Die Nutzung des Internets hat in den vergangenen Jahren explosionsartig zugenommen, wobei neue Entwicklungen und Techniken zu einer verstärkten Verunsicherung geführt haben.

Die Kommission hat in ihrem **Legislativ- und Arbeitsprogramm 2007** auf die Notwendigkeit einer umfassenden Aktualisierung ihrer Politik zur Bekämpfung der Internetkriminalität hingewiesen und diesbezüglich die Vorlage einer einschlägigen Mitteilung in Aussicht gestellt.

Bereits zu Beginn der hierfür eingeleiteten Konsultation wurde deutlich, dass es an Daten und Statistiken zu diesem Bereich mangelt. Nicht zuletzt aus diesem Grund gab die Kommission im Jahr 2006 eine **externe Studie**¹ in Auftrag, die die Hauptgrundlage für die anschließende Folgenabschätzung bildete.

Im Rahmen dieser Vorarbeiten hat die Kommission auch verschiedene Legislativ- und sonstige Maßnahmen geprüft, um insbesondere Lücken in den geltenden Rechtsvorschriften zu schließen. Besondere Schwerpunkte hierbei waren das **Europarat-Übereinkommen über Cyberkriminalität**² (nachfolgend „Europarat-Übereinkommen“) und der **Rahmenbeschluss über Angriffe auf Informationssysteme**³ als die in punkto substantielles Recht und Verfahrensrecht umfassendsten einschlägigen Rechtsvorschriften.

Die Kommission möchte auf der Grundlage dieser Vorarbeiten nunmehr eine neue allgemeine politische Initiative in Form einer Mitteilung über die Bekämpfung der Internetkriminalität auf EU-Ebene auf den Weg bringen. Diese Folgenabschätzung befasst sich daher hauptsächlich mit strategischen Überlegungen.

Die Kommission wird streng darauf achten, dass bei der Festlegung und Umsetzung der Politik zur Bekämpfung und strafrechtlichen Verfolgung der Internetkriminalität 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. Die betreffenden Arbeiten werden nach Maßgabe der Mitteilung der Kommission „Berücksichtigung der Charta der Grundrechte in den Rechtsetzungsvorschlägen der Kommission“ - KOM(2005) 172 - aus dem Jahr 2005 durchgeführt werden.

2. PROBLEME UND ZIELE

Mit der raschen Verbreitung des Internet und anderer Informationssysteme ist ein völlig neuer Wirtschaftssektor und ein ebenso neuer, sich rasch über die internen und externen Grenzen der EU bewegender Strom von Informationen, Produkten und Dienstleistungen entstanden.

¹ Studie zur Abschätzung der Auswirkungen einer Mitteilung über die Internetkriminalität (Yellow Window Management Consulting, Vertrag Nr. DG 2006/JLS D 2/03).

² Europarat-Übereinkommen über Cyberkriminalität aus dem Jahr 2001:
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

³ Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme.

Für die Verbraucher und die Bürger im Allgemeinen hat dies viele positive Auswirkungen mit sich gebracht. Gleichzeitig haben sich dadurch aber auch viele neue Möglichkeiten für Kriminelle eröffnet. So ist ein Schema von neuen Straftaten erkennbar, die sich gegen das Internet richten oder mit Hilfe von als Tatinstrument dienenden Informationssystemen begangen werden. Diese Art von kriminellen Handlungen ist in einem ständigen Wandel begriffen, mit dem der Gesetzgeber und die Strafverfolgungsbehörden nur schwer Schritt halten können. Da es sich hierbei im Wesentlichen um grenzüberschreitende Straftaten handelt, besteht die Notwendigkeit, die Zusammenarbeit bei der grenzübergreifenden Strafverfolgung zu verbessern.

Für eine ausführlichere Befassung mit dieser Problematik sind folgende acht Problembereiche in Betracht gezogen worden:

- die zunehmende Anfälligkeit der Gesellschaft, der Wirtschaft und der Bürger für die mit der Internetkriminalität einhergehenden Risiken,
- die zunehmende Häufigkeit und Raffinesse von Internetdelikten,
- das Fehlen einer kohärenten Politik und Gesetzgebung der EU zur Bekämpfung der Internetkriminalität,
- spezifische Schwierigkeiten bei der operativen Zusammenarbeit zwischen Strafverfolgungsbehörden bei der Bekämpfung der Internetkriminalität,
- die Notwendigkeit, Fähigkeiten und technische Instrumente im Rahmen von Schulungs-, Fortbildungs- und Forschungsmaßnahmen zu entwickeln,
- das Fehlen einer geeigneten Struktur für die Zusammenarbeit zwischen den wichtigsten Betroffenen im öffentlichen und im privaten Sektor,
- die unklare Aufgaben- und Zuständigkeitsverteilung,
- das fehlende Bewusstsein für die von der Internetkriminalität ausgehenden Gefahren.

Bei der Konsultation, die im Hinblick auf die Erstellung dieses Berichts durchgeführt wurde, war auffällig, dass zwischen den unterschiedlichen Betroffenen und zuständigen Stellen wie Strafverfolgungsbehörden und privaten Unternehmen offenbar große Einigkeit über die aktuellen Probleme der EU in diesem Bereich besteht.

2.1. Wer ist betroffen?

Die Internetkriminalität betrifft alle gesellschaftlichen Bereiche, so dass eine Politik zu ihrer Bekämpfung praktisch überall sichtbar ist. Da die Zahl der Bürger, die einen eigenen Computer besitzen, sehr hoch ist, könnten die meisten Bürger - schon in ihrer Eigenschaft als potenzielle Opfer - von Maßnahmen zur Bekämpfung der Internetkriminalität betroffen sein.

Es gibt allerdings deutliche Anzeichen dafür, dass sich immer mehr derartige Straftaten gegen ganz bestimmte Opfergruppen richten. Diesen Gruppen käme eine wirksame Politik zur Bekämpfung der Internetkriminalität mithin sehr zugute. Zu den Betroffenen dürfte ebenso die Industrie der Informationsgesellschaft wie auch die Informationsgesellschaft insgesamt

zählen, da mit überaus positiven Auswirkungen zu rechnen sein dürfte, wenn Sicherheitsvorkehrungen oder die Sicherheit allgemein verbessert würden.

2.2. Ist die EU berechtigt, tätig zu werden?

Angesichts der Größe und des Umfangs der bestehenden Sicherheitsbedrohungen besteht die möglicherweise immer dringender werdende Notwendigkeit, gegen die Internetkriminalität vorzugehen. Die auf die Internetkriminalität zurückgehenden Sicherheitsprobleme sind globaler Natur und können daher nicht allein auf nationaler Ebene angegangen werden. Da es sich hier um eine sich über Ländergrenzen hinwegsetzende Bedrohung handelt, sollten auch die Gegenmaßnahmen zumindest teilweise grenzübergreifend sein. Es steht zwar zweifelsfrei fest, dass die Bekämpfung der Internetkriminalität auch in Zukunft auf nationaler Ebene am wichtigsten sein und am wirksamsten durchgeführt werden wird, aber es besteht eindeutig die Notwendigkeit, die von den einzelnen Ländern unternommenen Anstrengungen auf EU-Ebene miteinander zu verbinden und gegebenenfalls zu ergänzen.

2.3. Ziele

Das allgemeine strategische Ziel der vorgeschlagenen Politik zur Beseitigung der oben genannten Probleme lässt sich wie folgt formulieren:

Ausbau und bessere Koordinierung der Maßnahmen zur Bekämpfung der Internetkriminalität auf nationaler, europäischer und internationaler Ebene

Dieses allgemeine strategische Ziel lässt sich in fünf strategische, nachfolgend nach ihrer vorgeschlagenen Priorität geordneten Unterziele untergliedern:

- Verbesserung der operativen grenzübergreifenden Strafverfolgungsmaßnahmen zur Bekämpfung der Internetkriminalität im Allgemeinen sowie schwer wiegender Formen der Internetkriminalität im Besonderen und Verbesserung des Austausches von Informationen, sachdienlichen Erkenntnissen und bewährten Praktiken zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und anderer Länder,
- Einführung geeigneter operativer Instrumente für die Zusammenarbeit und die Festlegung gemeinsamer Ziele des öffentlichen und des privaten Sektors sowie Verbesserung des Austausches von Informationen, sachdienlichen Erkenntnissen und bewährten Praktiken zur Bekämpfung der Internetkriminalität zwischen dem öffentlichen und dem privaten Sektor auf EU-Ebene,
- Einrichtung einer politischen Plattform und von geeigneten Strukturen zur Entwicklung einer konsequenten EU-Politik zur Bekämpfung der Internetkriminalität in Zusammenarbeit mit den Mitgliedstaaten und den zuständigen EU-Stellen und internationalen Organisationen sowie Steigerung der Effizienz der bestehenden rechtlichen und institutionellen Rahmen insbesondere durch Klärung der Zuständigkeiten und Aufgaben aller Beteiligten,
- Bekämpfung der wachsenden Gefahr, die von schweren Formen der Internetkriminalität ausgeht, durch Förderung von Fähigkeiten, Kenntnissen und technischen Werkzeugen einschließlich Verbesserung der einschlägigen Fortbildungs- und Forschungsmaßnahmen,

- Steigerung des allgemeinen Bewusstseins für die von der Internetkriminalität ausgehende Gefahr besonders bei den Verbrauchern und anderen möglichen Opfergruppen.

3. STRATEGISCHE POLITISCHE OPTIONEN

Aufgrund der Eigenarten der Internetkriminalität muss jede gegen sie gerichtete Politik vielseitig sein. Die Polizei muss, um wirklich effizient vorgehen zu können, herkömmliche Strafverfolgungsmaßnahmen mit zusätzlichen Instrumenten wie Selbstregulierungselementen und Strukturen für die Zusammenarbeit zwischen den verschiedenen Beteiligten kombinieren. Einige Problembereiche und strategische Ziele dieser Initiative sind bereits weiter oben vorgestellt worden. Um diese Ziele verwirklichen zu können, bedarf es unterschiedlicher, miteinander zu verknüpfender Maßnahmen. Die Kommission hat auf der Grundlage der Ergebnisse der umfangreichen Konsultation zu diesem Thema vier allgemeine politische Optionen ausgearbeitet, die jeweils verschiedene spezifische Maßnahmen umfassen:

3.1. Allgemeine politische Option 1: Beibehaltung des Status quo / keine größeren neuen Maßnahmen

Bei dieser Möglichkeit würden zum jetzigen Zeitpunkt von Seiten der Kommission keine allgemeinen horizontalen Maßnahmen in dieser Frage ergriffen. Die Kommission würde lediglich

- kontinuierlich prüfen, ob gezielte Rechtsvorschriften oder politische Maßnahmen erforderlich sind und bei Bedarf geeignete Maßnahmen ergreifen,
- die auf EU- und internationaler Ebene bestehenden Projekte zur Bekämpfung der Internetkriminalität im Blick behalten,
- weitere Projekte in bestimmten, für die Bekämpfung der Internetkriminalität relevanten Zielbereichen ins Leben rufen, jedoch keine horizontal ausgerichtete politische Initiative ergreifen.

3.2. Allgemeine politische Option 2: Schaffung eines allgemeinen rechtlichen Rahmens

Bei dieser Möglichkeit würde eine Politik angenommen, die darauf ausgerichtet wäre, schrittweise Vorschläge zur Schaffung eines allgemeinen rechtlichen Rahmens für die Bekämpfung der Internetkriminalität vorzulegen. Diese Politik würde folgendes einschließen:

- die Kommission würde systematisch Vorschläge für an einander angeglichenen bzw. einheitliche Straftatbestände insbesondere in der EU aber auch auf internationaler Ebene vorlegen,
- die Kommission würde gemeinsame Mindeststandards für die strafrechtliche Verfolgung dieser Delikte und die betreffenden Strafen in der EU vorschlagen,
- es würden offizielle Plattformen für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor sowie für die Bereiche Schulung und Forschung eingerichtet,

- es würde ein offizielles Netz der Strafverfolgungsbehörden aufgebaut.

3.3. Allgemeine politische Option 3: Aufbau informeller Netze zur Bekämpfung der Internetkriminalität mit Sachverständigen aus dem öffentlichen und aus dem privaten Sektor

Bei dieser Möglichkeit würde die Kommission entweder allein oder aber in Zusammenarbeit mit anderen Einrichtungen Netze oder Arbeitsgruppen für Sachverständige auf dem Gebiet der Bekämpfung der Internetkriminalität einrichten und gleichzeitig ein freiwilliges Zertifizierungssystem für Betreiber, Erzeuger und Verbraucher einführen. Dies würde folgende Maßnahmen umfassen:

- Einrichtung eines informellen Gremiums aus Sachverständigen der Strafverfolgungsbehörden für die Bekämpfung der Internetkriminalität,
- Einrichtung einer informellen Plattform bzw. eines informellen Netzes für Sachverständige aus dem öffentlichen und dem privaten Sektor auf dem Gebiet der Bekämpfung der Internetkriminalität.

3.4. Allgemeine politische Option 4: ein kohärenter strategischer Ansatz

Bei dieser Möglichkeit würde eine kohärente Strategie für die Bekämpfung der Internetkriminalität auf EU-Ebene entwickelt. Zentrale Maßnahme wäre die Schaffung eines strategischen Rahmens für eine EU-Politik zur Bekämpfung der Internetkriminalität, die das allgemeine Ziel verfolgen würde, bessere Leitlinien für konkrete Maßnahmen zu schaffen und eine optimale Nutzung der vorhandenen Mittel zu ermöglichen. Weitere wichtige operative Aspekte dieser Strategie wären:

- eine verbesserte Zusammenarbeit der Strafverfolgungsbehörden auf EU-Ebene,
- die Einrichtung einer strategischen Struktur für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor bei der Bekämpfung der Internetkriminalität,
- die Förderung der Schaffung eines Rahmens für eine globale länderübergreifende Zusammenarbeit auf diesem Gebiet,
- gezielte Legislativmaßnahmen (sofern erforderlich).

4. BEWERTUNG DER POLITISCHEN OPTIONEN UND AUSWAHL EINER POLITISCHEN OPTION

4.1. Bewertung

Die Prüfung der allgemeinen politischen Optionen erfolgte auf der Grundlage folgender Kriterien:

- gesellschaftliche Auswirkungen
- wirtschaftliche Auswirkungen
- den Behörden entstehende Kosten

- Übereinstimmung mit den politischen Zielen
- Nutzen und Berücksichtigung des Subsidiaritätsgrundsatzes
- Machbarkeit

Die Schlussfolgerungen dieser Prüfung lassen sich folgt zusammenfassen:

4.1.1. Allgemeine politische Option 1

Diese Option wurde, was die Bewältigung der bestehenden Herausforderungen anbelangt, eindeutig für unzureichend befunden. Die Auswirkungen eines jeden Ansatzes „ohne neue Maßnahmen“ sind von vornherein begrenzt, und da naturgemäß nicht vorhersagbar ist, welche Kriminalitätsformen sich in Zukunft entwickeln werden, lässt sich auch nur schwer abschätzen, ob der Rückgriff auf diese Option überhaupt nennenswerte positive Auswirkungen hätte. Angesichts der zunehmenden Bedeutung dieser Kriminalitätsform bestünde vielmehr sogar die große Gefahr, dass sich ein Vorgehen „ohne neue Maßnahmen“ auf lange Sicht negativ auswirken würde.

4.1.2. Allgemeine politische Option 2

Bezüglich dieser Option wurde die Schlussfolgerung gezogen, dass ein solcher Ansatz nur mit großer Vorsicht und auch nur auf lange Sicht verfolgt werden könnte. Er würde ausführliche rechtliche Machbarkeitsstudien und lange politische Verhandlungen erfordern. Er könnte zwar insgesamt sehr große Auswirkungen haben, aber da es nicht sehr wahrscheinlich ist, dass kurzfristig wirkliche Fortschritte erzielt werden, ist diese Option, was das kurzfristige Vorgehen anbelangt, mit zu großer Ungewissheit verbunden. Fraglich ist auch, ob die politischen Ziele auf Ebene der konkreten Umsetzung der politischen Maßnahmen ebenso wirksam verwirklicht würden wie auf politischer und theoretischer Ebene. Ferner bestünde, falls diese Option verfolgt würde, die Gefahr, dass die operative Ebene der Bekämpfung der Internetkriminalität nicht ausreichend in strategische politische Entscheidungen eingebunden wäre. Angesichts der großen damit verbundenen Auswirkungen müsste zudem geklärt werden, welche Rolle der Kommission in diesem Zusammenhang zufällt. Außerdem ließe sich möglicherweise auch behaupten, dass ähnliche Ergebnisse auch mit weniger weit gehenden Maßnahmen möglich wären.

4.1.3. Allgemeine politische Option 3

Bezüglich dieser Option wurde die Schlussfolgerung gezogen, dass sie aus strategischer Sicht überaus interessant ist, wenngleich sich ihr Nutzen und ihre konkreten Auswirkungen nur schwer abschätzen lassen. Es bestünde das Risiko, dass die neuen Netze nur wenige konkrete Ergebnisse ermöglichen würden. Die Kommission wäre eigentlich in der idealen Position, um die Selbstregulierungsmaßnahmen in diesem Bereich zu koordinieren, doch bei dieser Option würde sie eher die Rolle eines Koordinators und Vermittlers spielen als die eines strategischen Richtungsgebers.

4.1.4. Allgemeine politische Option 4

Bezüglich dieser Option wurde die Schlussfolgerung gezogen, dass sie mehrere höchst sachdienliche Maßnahmen auf strategischer Ebene ermöglicht. Es lassen sich nur sehr wenige negative Auswirkungen oder größere Hindernisse erkennen. Als Nachteil könnte angeführt

werden, dass die unmittelbaren Auswirkungen der Politik eher gering sind. Dies gilt allerdings nur für die kurzfristigen Auswirkungen: Wenn geeignete Durchführungsmaßnahmen ergriffen werden, sind sehr große Auswirkungen möglich. Welche konkreten Folgen im Einzelnen zu erwarten wären, lässt sich gleichwohl nur schwer abschätzen, da die strategischen Maßnahmen erst zu einem späteren Zeitpunkt in operative Maßnahmen umzusetzen wären und auch erst dann die genauen Auswirkungen ermittelt würden.

Es wird erneut darauf hingewiesen, dass die direkten Auswirkungen der vorgeschlagenen Strategien begrenzt sind und dass die spezifischen Maßnahmen, die nachfolgend im Rahmen einer dieser Strategien ergriffen werden, dann separat ausgewertet werden. Anders ausgedrückt: Zum jetzigen Zeitpunkt ist nur eine vorläufige Bewertung bzw. Abschätzung möglich.

4.2. Auswahl einer politischen Option

Die Analyse hat eindeutig ergeben, dass Option 4 die beste Lösung ist. Außerdem weist Option 4 auch die größte Übereinstimmung mit den in Abschnitt 2.4 genannten allgemeinen Zielen auf.

Die Option „Keine Maßnahmen“ scheint nicht sinnvoll zu sein. Ein passiver Ansatz würde wahrscheinlich zahlreiche bilaterale Kooperationsprojekte zur Bekämpfung der Internetkriminalität ins Leben rufen, bei denen nie die Möglichkeit bestünde, die Vorteile, die ein horizontaler Austausch von bewährten Praktiken oder Synergieeffekte mit sich bringen, zu nutzen. Allgemeine Rechtsvorschriften zur Einrichtung neuer EU-Gremien zwecks Angleichung von Straftatbeständen und Klärung der Aufgaben und Zuständigkeiten aller Beteiligten könnten zwar ein interessanter Lösungsansatz sein, doch die Prüfung der politischen Situation hat eindeutig ergeben, dass Vorschläge für allgemeine und horizontale Rechtsvorschriften nur geringe Aussicht hätten, angenommen zu werden. Außerdem haben nur sehr wenige der Befragten die Überzeugung geäußert, dass dies derzeit von größter Priorität ist. Nichtsdestotrotz könnten allgemeine Rechtsvorschriften langfristig durchaus von Bedeutung sein. Auch die Schaffung neuer informeller Strukturen für die Zusammenarbeit zwischen Strafverfolgungsdiensten oder zwischen dem öffentlichen und dem privaten Sektor auf EU-Ebene könnte langfristig durchaus eine gute Idee sein, doch unter den Betroffenen scheint Einigkeit darüber zu bestehen, dass die vorhandenen Strukturen ausreichend sind, obschon ihre Effizienz dringend verbessert werden müsste. Als Ergebnis dieser Analyse wurde der Vorzug mithin der „kohärenten Strategie“ von Option 4 gegeben. Es sei darauf hingewiesen, dass bei dieser bevorzugten Option gleichwohl nicht ausgeschlossen ist, dass eine offizielle Struktur eingerichtet wird (Option 3) oder zu einem späteren Zeitpunkt allgemeine Rechtsvorschriften (Option 2) erlassen werden. „Bevorzugt“ bedeutet in diesem Fall nämlich auch, dass neue Maßnahmen jederzeit möglich sind.

Sowohl bei der vorbereitenden Analyse als auch in den betreffenden Diskussionen hat sich klar gezeigt, dass die strategischen Ziele der Politik zur Bekämpfung der Internetkriminalität am ehesten mit Hilfe einer „kohärenten Strategie“ verwirklicht werden können. Eine solche Strategie dürfte überaus positive Auswirkungen auf die Bekämpfung der grenzüberschreitenden Internetkriminalität haben, da die Aufgaben und Befugnisse aller Beteiligten geklärt bzw. gestärkt würden. Auch würde der Dialog zwischen dem öffentlichen und dem privaten Sektor sowie das gegenseitige Verständnis verbessert, was viele positive Nebenwirkungen mit sich bringen könnte. Wirtschaftlich betrachtet könnte diese bevorzugte Option zum einen große Synergieeffekte bewirken und zum anderen einen Rückgang der

durch einschlägige Straftaten bedingten Schäden und Ausgaben für individuelle Sicherheitsprogramme ermöglichen.

Voraussichtlich wird es allerdings einige Jahre dauern, bis die von dieser Option erwarteten Ergebnisse sichtbar werden. Es fällt daher zum jetzigen Zeitpunkt schwer, sämtliche potenziellen Auswirkungen abzuschätzen. Dies gilt umso mehr, als die Einzelheiten dieser Politik noch gar nicht im Detail festgelegt worden sind. Daher wird es erforderlich sein, die genauen Auswirkungen der einzelnen Bestandteile dieser Politik zu einem späteren Zeitpunkt einer Folgenabschätzung zu unterziehen.