RAT DER EUROPÄISCHEN UNION

Brüssel, den 11. November 2008 (19.11)
(OR. en)

15569/08

ENFOPOL 224
CRIMORG 190

VERMERK

des	Vorsitzes
für den	AStV/Rat
Nr. Vordokument:	15236/08 CRIMORG 181 ENFOPOL 214
Betr.:	Entwurf von Schlussfolgerungen des Rates über eine konzertierte Arbeitsstrategie und konkrete Maßnahmen zur Bekämpfung der Cyberkriminalität

Der Rat (Justiz und Inneres) hat auf seiner Tagung vom 24. und 25. Juli 2008 den Gedanken des Vorsitzes begrüßt, einen Plan zur Bekämpfung der Cyberkriminalität in der EU auszuarbeiten, d.h. zum einen die Schaffung sowohl nationaler Melde-Plattformen als auch einer europäischen Melde-Plattform und zum anderen die Erarbeitung einer konzertierten Arbeitsstrategie und konkreter Maßnahmen zur Bekämpfung der Cyberkriminalität. Am 24. Oktober 2008 hat der Rat Schlussfolgerungen zur Errichtung von nationalen Plattformen und einer europäischen Plattform für Hinweise auf Internetstraftaten angenommen.

Vom Vorsitz wurde ein Entwurf von Schlussfolgerungen des Rates über eine konzertierte Arbeitsstrategie und konkrete Maßnahmen zur Bekämpfung der Cyberkriminalität vorgelegt. Dieser Entwurf von Schlussfolgerungen des Rates wurde jüngst in der Sitzung der Gruppe "Polizeiliche Zusammenarbeit" vom 5. November 2008 erörtert und dann vom Ausschuss "Artikel 36" auf dessen Tagung vom 10. November 2008 gebilligt. Der so erarbeitete Entwurf von Schlussfolgerungen ist in der Anlage enthalten.

Der Ausschuss der Ständigen Vertreter wird gebeten, dem in der Anlage enthaltenen Entwurf von Schlussfolgerungen zuzustimmen und diese dem Rat zur Annahme zu unterbreiten.

ANLAGE

Entwurf von Schlussfolgerungen des Rates über eine konzertierte Arbeitsstrategie und konkrete Maßnahmen zur Bekämpfung der Cyberkriminalität

DER RAT –

AUFGRUND FOLGENDER FESTSTELLUNGEN:

- Eines der Ziele der Europäischen Union besteht darin, durch gemeinsame Maßnahmen der Mitgliedstaaten im Bereich der polizeilichen und der justiziellen Zusammenarbeit schrittweise einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen.

- Der Schutz der europäischen Bürger ist eine der grundlegenden Aufgaben Europas. Daher muss die Union in der Lage sein, neue Formen der Kriminalität aufzuspüren und ihr Handeln anzupassen, so dass sie rasch reagieren kann.

- Die Zahl der Internet-Straftaten hat in den letzten Jahren beständig zugenommen, wobei diese, da das Internet keine Grenzen kennt, in immer stärkerem Maße länderübergreifend sind.

- Eine Strategie zur Bekämpfung der organisierten Kriminalität und der Computerkriminalität wurde auf der Tagung des Europäischen Rates in Tampere im Oktober 1999 zur Priorität erklärt. Seither ist diese Priorität im Rahmen umfangreicher Arbeiten der europäischen Organe bestätigt worden, insbesondere in der Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen vom 22. Mai 2007 mit dem Titel "Eine allgemeine Politik zur Bekämpfung der Internetkriminalität" und in dem Rahmenbeschluss 2005/222/JI vom 24. Februar 2005 über Angriffe auf Informationssysteme [1], den die Kommission 2009 aktualisieren will.

- Bis spätestens 15. September 2010 wird die Kommission eine Bewertung der Durchführung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten vornehmen.

[1] ABl. L 69 vom 16.3.2005, S. 67.

- Die Kommission und der Europarat haben bereits Fortschritte bei der Verstärkung der Partnerschaft zwischen den staatlichen Behörden und dem Privatsektor zur Bekämpfung der Cyberkriminalität erzielt.

- Die Kommission wird eine Mitteilung über die künftigen Prioritäten im Bereich der Freiheit, der Sicherheit und des Rechts in Europa vorlegen, die einen Ausblick auf das nächste Mehrjahresprogramm (2010–2014) enthalten wird und auch auf die Bekämpfung der Cyberkriminalität eingehen dürfte.

- In dem Umstand, dass der Rat Schlussfolgerungen zur Schaffung nationaler Mechanismen angenommen hat, mit denen eine europäische Plattform für Hinweise auf Internetstraftaten [1] errichtet werden kann, kommt die Absicht zum Ausdruck, die Zusammenarbeit bei der Strafverfolgung zu verstärken, indem die Strafverfolgungsbehörden mit umfangreichen und wirksamen Mitteln ausgestattet werden.

- Schließlich scheint die Ausarbeitung eines umfassenden Programms zur Bekämpfung der Cyberkriminalität auf Unionsebene die am besten geeignete Vorgehensweise zu sein, um Lösungen für alle Fragen zu finden, die sich in diesem Zusammenhang stellen oder in naher Zukunft stellen könnten, und um die Umsetzung dieser Lösungen zu überwachen –

1. ERACHTET es als wichtig, gegen die verschiedenen Ausprägungen der Cyberkriminalität vorzugehen, wobei die Mitgliedstaaten und die Kommission eine gemeinsame Arbeitsstrategie festlegen sollten, bei der das Übereinkommen des Europarates über Computerkriminalität inhaltlich berücksichtigt wird.

   Ziel dieser Strategie sollte es sein, noch wirkungsvoller den vielfältigen Straftaten begegnen zu können, die mit Hilfe elektronischer Netze begangen werden. Diese nehmen so beunruhigende Formen an wie etwa Kinderpornographie, sexuelle Gewalt in jeglicher Form und terroristische Handlungen jedweder Art, wie sie in dem Rahmenbeschluss 2002/475/JI vom 13. Juni 2002 aufgeführt sind.

   Außerdem sollte die Strategie dazu beitragen, der spezifischen Gefährdung zu begegnen, der elektronische Netze (durch groß angelegte Angriffe gegen Informationssysteme) ausgesetzt sind.

---

[1] Dok. 13243/08 ENFOPOL 162 CRIMORG 140.

Gegenstand dieser Strategie sollten schließlich auch die Mittel zur Bekämpfung herkömmlicher Kriminalitätsformen sein, die über das Internet begangen werden, wie Identitätsbetrug, Identitätsdiebstahl, betrügerischer Verkauf, Finanzstraftaten, illegaler Handel im Internet, insbesondere Rauschgift- und Waffenhandel;

2. IST DER AUFFASSUNG, dass bei der Suche nach einer wirksamen Reaktion auf diese verschiedenen Bedrohungen im Zusammenhang mit den elektronischen Netzen horizontale Maßnahmen erforderlich sind, wie beispielsweise

   a) ein Ausbau der Partnerschaft zwischen den staatlichen Behörden und dem Privatsektor im Hinblick auf die gemeinsame Ausarbeitung von Methoden zur Ermittlung der durch die Straftaten verursachten Schäden und zu deren Prävention sowie im Hinblick auf die Übermittlung sachdienlicher Informationen über die Häufigkeit der erlittenen Straftaten durch die geschädigten Unternehmen an die Strafverfolgungsbehörden. Insbesondere wird empfohlen, dass sich die Kommission mit den Einzelheiten der Umsetzung der Leitlinien befasst, die auf der Octopus-Konferenz über Computerkriminalität – die am 1. und 2. April 2008 unter der Schirmherrschaft des Europarates stattgefunden hat – angenommen wurden und die auf eine Verbesserung der Partnerschaft zwischen den staatlichen Behörden und dem Privatsektor bei der Bekämpfung der Cyberkriminalität abzielen. In diesem Zusammenhang nimmt der Rat Kenntnis von den im Anhang wiedergegebenen Empfehlungen, die im Anschluss an die Sachverständigensitzung ausgesprochen wurden, die von der Kommission am 25./26. September 2008 veranstaltet wurde;

   b) eine Verbesserung des Kenntnisstands und der Schulung der an der Bekämpfung der Cyberkriminalität in Europa beteiligten Akteure. Insbesondere wäre es zweckdienlich, ein Netz der Leiter der für die Bekämpfung der Cyberkriminalität zuständigen polizeilichen Dienststellen zu schaffen. Diese Initiative würde eine Ergänzung zu den Arbeiten der in diesem Bereich tätigen Expertengruppen darstellen, wobei es nicht nur um künftige Bedrohungen geht, sondern auch um Verfahren für Sofortmaßnahmen bei schwerwiegenden Zwischenfällen, wie bei der unter der Schirmherrschaft von Europol eingesetzten Gruppe oder den von der Kommission eingerichteten gemeinsamen Forschungsstellen;

   c) eine Intensivierung der internationalen technischen Zusammenarbeit mit Drittländern, die es immer häufiger mit der Geißel der Cyberkriminalität aufnehmen müssen, sowie technische Unterstützung;

3. ERSUCHT angesichts dessen die Mitgliedstaaten und die Kommission, auf Fallstudien basierende Maßnahmen einzuführen, wobei insbesondere der technologischen Entwicklung Rechnung zu tragen ist, um kurz- und mittelfristig operative Instrumente auszuarbeiten, wie beispielsweise

a) kurzfristig:

- die Schaffung einer europäischen Plattform für Hinweise auf Internetstraftaten;

- die Ausarbeitung – in Konsultation mit privaten Betreibern – einer europäischen Mustervereinbarung über die Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Betreibern;

- Festlegung einer Definition des Begriffs des Identitätsbetrugs im Internet in Übereinstimmung mit dem nationalen Recht;

- die Schaffung nationaler Rahmeninstrumente und der Austausch bewährter Praktiken im Hinblick auf Cyberpatrouillen, die ein modernes Instrument zur Bekämpfung der Cyberkriminalität darstellen, und damit Schaffung der Voraussetzungen für die Weitergabe von Informationen über Aliasnamen auf europäischer Ebene im Einklang mit den nationalen Rechtsvorschriften über den Datenaustausch;

- der Einsatz gemeinsamer Ermittlungs- und Untersuchungsteams;

- eine Lösung der Probleme, die sich aus dem Roaming in den elektronischen Netzen und durch die Anonymität vorab bezahlter Telekommunikationsprodukte ergeben;

b) mittelfristig:

- der Austausch über Vorkehrungen zur Sperrung und/oder Schließung von kinderpornographischen Websites in den Mitgliedstaaten. Die Diensteanbieter sollten bestärkt werden, derartige Maßnahmen zu ergreifen. Sofern erforderlich, könnte die europäische Plattform als Instrument zur Erstellung einer gemeinsamen schwarzen Liste dienen;

- Erleichterung von Ferndurchsuchungen, sofern diese nach nationalem Recht vorgesehen sind, so dass die Ermittlungsteams mit Zustimmung des Gastlandes raschen Zugang zu den Informationen erhalten können;

- Ausarbeitung vorläufiger Definitionen für Kategorien von Straftaten und statistischer Indikatoren zur leichteren Erhebung vergleichbarer statistischer Daten zu den verschiedenen Formen der Cyberkriminalität, und dies unter Berücksichtigung der Arbeiten, die die Europäische Union derzeit in diesem Bereich durchführt;

4. ERSUCHT die Kommission, eine Bewertung der Fortschritte vorzunehmen, die bei der Vorbereitung der Durchführung der unter den Nummern 2 und 3 genannten Maßnahmen erzielt worden sind, und ersucht daher die Mitgliedstaaten, die Kommission über ihre Beiträge zu unterrichten;

5. PLÄDIERT dafür, dass im Rahmen des nächsten Mehrjahresprogramms für den Bereich Freiheit, Sicherheit und Recht (2010–2014) zusätzliche längerfristige Maßnahmen konzipiert werden.

ANHANG ZUR ANLAGE

1. Die Strafverfolgungsbehörden und der Privatsektor [1] sollten bestärkt werden, strategische und operative Informationen auszutauschen, um ihre Fähigkeit zur Erkennung und Bekämpfung neuer Formen von Cyberkriminalität zu stärken. Die Strafverfolgungsbehörden sollten bestärkt werden, die Diensteanbieter über Entwicklungen im Bereich der Cyberkriminalität zu informieren.

2. Insbesondere wird den Mitgliedstaaten nahe gelegt, standardisierte Systeme für den sicheren Austausch operativer und strategischer Informationen zwischen Strafverfolgungsbehörden und Privatsektor einzurichten. Als wesentliche Bestandteile eines solchen Systems sind unter anderem folgende Strukturen und Verfahren zu nennen:

3. Ständige Kontaktstellen: Es sollten ständige Kontaktstellen bei den Strafverfolgungsbehörden und vergleichbare Stellen im Privatsektor eingerichtet werden, um die Präzision und Effizienz der Anfrage- und Antwortprozesse zu verbessern. Die entsprechenden Stellen im Privatsektor sollten ferner Notdienste einrichten, die außerhalb der Bürozeiten erreichbar sind und auf dringende Anfragen der Strafverfolgungsbehörden antworten können. Was als dringend gilt, ist in Absprache zwischen den Strafverfolgungsbehörden und dem Privatsektor festzulegen.

4. Der Privatsektor und die Strafverfolgungsbehörden werden darin bestärkt, sich gegenseitig durch Ausbildungs- und Schulungsmaßnahmen sowie weitere Unterstützungsmaßnahmen bei ihren jeweiligen Aufgaben zu unterstützen.

5. Musteranfrageformular: Auf einzelstaatlicher Ebene – und wenn möglich gemeinsam mit Drittstaaten – sollten die Strafverfolgungsbehörden das Formular für die Absendung und Beantwortung von Anfragen einheitlich gestalten und strukturieren. Der Privatsektor sollte zur Beantwortung von Anfragen der Strafverfolgungsbehörden dieses Formular verwenden. Als Mindestvoraussetzung gilt, dass Anfragen der Strafverfolgungsbehörden in jedem Fall schriftlich, vorzugsweise in elektronischer Form, erfolgen und folgende Angaben enthalten sollten:

   – Aktenzeichen

   – Bezugnahme auf Rechtsgrundlage

[1] Der Begriff "Privatsektor" umfasst nicht nur Unternehmen des Privatsektors, sondern auch andere Akteure, die in der Informations- und Kommunikationstechnologie (IKT) eine Rolle spielen, darunter die Computer Emergency Response Teams (CERTs).

– genaue Nennung der gewünschten Daten

– Zeitzone

– Angaben zur Verifizierung des Absenders der Anfrage.

6. Einstufung der Anfragen nach Prioritäten: Die Strafverfolgungsbehörden und der Privatsektor sollten ein Prioritätensystem für die Einstufung der an den Privatsektor gerichteten Anfragen vereinbaren.

7. Die Strafverfolgungsbehörden und der Privatsektor sollten die Kosten im Auge behalten, die mit der Generierung und Beantwortung von Anfragen verbunden sind. Die entsprechenden Verfahren sollten unter Berücksichtigung der finanziellen Auswirkungen der betreffenden Tätigkeiten entwickelt werden und es sollte die Frage der Kostenerstattung oder einer angemessenen Entschädigung für die betreffenden Seiten geprüft werden.

8. Die Europäische Kommission, die Mitgliedstaaten und die Akteure des Privatsektors sind aufgefordert, den Austausch bewährter Praktiken in den unter den Nummern 1–7 genannten Bereichen zu erleichtern, um eine stärkere Annäherung der einzelstaatlichen Mechanismen und schließlich die Einrichtung eines Systems für den Austausch strategischer und operativer Informationen auf EU-Ebene zu ermöglichen.