Council Logo

RAT DER EUROPÄISCHEN UNION

Brüssel, den 22. März 2001 (04.04) (OR. en)

7273/01

LIMITE

ENFOPOL 22
CRIMORG 35

VERMERK

des	Vorsitzes
für	die Gruppe "Polizeiliche Zusammenarbeit"
Nr. Vordokument:	6446/98 CK4 13, KOM(2000) 890 endg. = 5894/01 CRIMORG 14 ECO 22
Betr.:	Kontaktstellennetz der G8 zur Bekämpfung der High-Tech-Kriminalität – Entwurf einer Empfehlung des Rates

DER RAT DER EUROPÄISCHEN UNION -

in Anbetracht des Standpunkts des Rates vom 19. März 1998, mit dem die Mitgliedstaaten ersucht wurden, sich dem allzeit erreichbaren Informationsnetz der G8 zur Bekämpfung der High-Tech-Kriminalität anzuschließen, sowie des Umstands, dass der Rat die Grundsätze des Netzes gebilligt hat,

im Hinblick auf die vor Kurzem veröffentlichte Mitteilung der Kommission "Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" [KOM(2000) 890 endg. vom 26.1.2001],

in Erwägung nachstehender Gründe:

(1) Die Grundsätze des G8-Netzes nationaler Kontaktstellen zur Bekämpfung der High-Tech-Kriminalität wurden auf der G8-Tagung der Justiz- und Innenminister am 9. und 10. Dezember 1997 in Washington DC angenommen. Die Grundsätze wurden durch einen Aktionsplan für die Schaffung des Netzes und ein Verzeichnis der Verpflichtungen, welche die einzelnen Staaten mit dem Beitritt zu dem Netz eingehen, ergänzt. In dem Aktionsplan fordert die G8 auch Länder außerhalb des Kreises der G8 dazu auf, dem Netz beizutreten.

(2) Ein globales Netz wie das G8-Netz weist große Vorteile auf, und es kann zu Recht davon ausgegangen werden, dass es immer mehr an Bedeutung gewinnen wird. Wenn den Strafverfolgungsnetzen zur Bekämpfung der IT-Kriminalität nur wenige Länder angehören, ist es diesen nicht möglich, im grenzenlosen Cyberspace einen ausreichenden Überblick zu gewinnen oder mit hinreichender Effizienz vorzugehen.

(3) Dem Netz liegt die Idee zugrunde, dass die verschiedenen Arten der High-Tech-Kriminalität rasch und mit großer Professionalität anzugehen sind. Der Schwerpunkt liegt auf der Sicherung von Beweismitteln in einem Umfeld, in dem Informationen rasch verloren gehen oder vernichtet werden können. Sind die ersten Maßnahmen der Strafverfolgungsbehörden nicht sachgerecht oder werden sie zu spät ergriffen, können somit mögliche Ermittlungen in Fällen, die diese Deliktsart betreffen, behindert oder sogar zunichte gemacht werden. Ein anderer Zweck des Netzes besteht darin, es den dem Netz angehörenden Ländern zu ermöglichen, sich einen Überblick über die Computerkriminalität zu verschaffen, da diese oft gleichzeitig an verschiedenen Orten in verschiedenen Ländern auftritt.

(4) Das Netz wurde in den Jahren 1998-2000 schrittweise aufgebaut, und es werden weiterhin Bemühungen unternommen, die Anzahl der beteiligten Länder zu erhöhen. Auf einer Sachverständigentagung auf hoher Ebene im November 2000 bei Europol waren sich die Teilnehmer darin einig, die Ausweitung des G8-Netzes offiziell zu empfehlen.

(5) Zur Zeit gehören dem Netz folgende Länder an: Australien, Brasilien, Dänemark, Deutschland, Finnland, Frankreich, Italien, Japan, Kanada, Luxemburg, Russland, Schweden, Spanien, USA und Vereinigtes Königreich. Somit sind neun EU-Mitgliedstaaten dem Netz beigetreten.

(6) Die EU-Mitgliedstaaten, die dem G8-Netz nicht beigetreten sind, gehören dem Interpol-System der Zentralen Nationalen Referenzstellen (NCRP) an. Zurzeit sind über 60 Länder mit dem Interpol-Netz verbunden. Eine NCRP ist in aller Regel eine spezialisierte Dienststelle. Die NCRP von Interpol bieten jedoch nicht immer einen siebentägigen Dauerdienst rund um die Uhr neben dem Bereitschaftsdienst der Meldestellen der Nationalen Zentralbüros an. Die Zusammenarbeit im Rahmen des NCRP-Netzes von Interpol beruht auf denselben Grundsätzen, die auch sonst für die Interpol-Zusammenarbeit gelten. Dies bedeutet, dass Maßnahmen, die Zwangsmittel beinhalten, beispielsweise zur Sicherung von Beweismitteln, normalerweise nicht über diesen Weg durchgeführt werden. In den Grundsätzen des G8-Netzes wird hervorgehoben, dass rasche Maßnahmen erforderlich sind, wenn es um das Einfrieren oder Sichern von Beweismitteln in Computersystemen oder -netzen geht. Zwischen den beiden Strafverfolgungsnetzen besteht kein Konkurrenzverhältnis. Im Gegenteil: sie ergänzen sich vielmehr. Den EU-Mitgliedstaaten, die im G8-Netz nicht vertreten sind, sollte es daher möglich sein, ihre für die Interpol-Zusammenarbeit zuständigen spezialisierten Dienststellen an einen siebentägigen, rund um die Uhr erreichbaren Dauerdienst anzuschließen.

(7) Erfahrungen beispielsweise aus dem weltweit verbreiteten "Love letter"-Virus im Mai 2000 zeigen, dass das G8-Netz sowohl erweitert als auch verbessert werden muss. Der tatsächliche Betrieb eines siebentägigen Dauerdienstes rund um die Uhr in Form spezialisierter Dienststellen in den Ländern, die dem Netz beigetreten sind, stellt eine wichtige Verbesserung dar. Heute kommt es vor, dass Meldestellen eine Nachricht erhalten und diese erst weiterleiten, nachdem die spezialisierte Dienststelle ihren Dienst aufgenommen hat. In Verbindung mit Feiertagen kann ein solches Verfahren zu einem fatalen Zeitverlust führen.

(8) Als weiterer gemeinsamer Standard wäre es auch wünschenswert, dass es sich bei der als nationale Kontaktstelle bezeichneten Dienststelle tatsächlich um eine spezialisierte Dienststelle handelt, die empfohlene internationale Verfahren für Ermittlungen im Bereich der High-Tech-Kriminalität anwendet, und dass die Stelle alle zweckdienlichen Maßnahmen - natürlich unter gebührender Berücksichtigung der nationalen Rechtsvorschriften - ergreifen kann -

EMFPIEHLT

- denjenigen Mitgliedstaaten, die dem zur Bekämpfung der High-Tech-Kriminalität geschaffenen G8-Kontaktstellennetz mit einem siebentägigen Dauerdienst rund um die Uhr noch nicht beigetreten sind, dies zu tun,

- den Mitgliedstaaten, sicherzustellen, dass die als Kontaktstelle benannte Stelle einen siebentägigen Dauerdienst rund um die Uhr aufrechterhält und dass es sich bei der Kontaktstelle tatsächlich um eine spezialisierte Dienststelle handelt, die bewährte Praktiken bei der Aufklärung von IT-Delikten anwendet. Die Kontaktstelle sollte auch in der Lage sein, operative Maßnahmen zu ergreifen.