RAT DER EUROPÄISCHEN UNION

Brüssel, den 4. April 2012 (10.04)
(OR. en)

8543/12

ENFOPOL 94
TELECOM 72

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	30. März 2012
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	COM(2012) 140 final
Betr.:	MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität

Die Delegationen erhalten in der Anlage das Kommissionsdokument COM(2012) 140 final.

Anl.: COM(2012) 140 final

EUROPÄISCHE KOMMISSION

Brüssel, den 28.3.2012
COM(2012) 140 final

MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT

Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität

MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT

Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität

1. EINLEITUNG: DIE EUROPÄISCHE ANTWORT AUF DIE GRENZÜBERSCHREITENDE KRIMINALITÄT

Das Internet ist zu einem festen und unentbehrlichen Bestandteil unserer Gesellschaft und Wirtschaft geworden. Achtzig Prozent aller jungen Europäer schließen über soziale Netze im Internet Kontakt miteinander und mit der Welt[1], und alljährlich werden weltweit im elektronischen Handel rund 8 Billionen EUR[2] umgesetzt. Im gleichen Maße, wie sich unser tägliches Leben und unser wirtschaftliches Handeln zunehmend online abspielt, nimmt jedoch auch die Kriminalität im Online-Bereich zu: Jeden Tag werden weltweit über eine Million Menschen[3] Opfer von Cyberstraftaten, deren Palette vom Verkauf gestohlener Kreditkarten (für gerade mal einen Euro) über den Identitätsdiebstahl und den mit Hilfe des Internets verübten sexuellen Missbrauch von Kindern bis hin zu schweren Cyberangriffen auf Einrichtungen und Infrastrukturen reicht.

Durch die Cyberkriminalität entsteht der Gesellschaft ein großer Schaden. Dieser beläuft sich laut einem unlängst erschienenen Bericht[4] auf weltweit rund 388 Mrd. EUR jährlich und macht die Cyberkriminalität somit sogar einträglicher als der gesamte weltweite Handel mit Marihuana, Kokain und Heroin zusammen. Derartige Zahlen sind zwar mit Vorsicht zu genießen, da der Begriff „Cyberkriminalität“ mitunter unterschiedlich definiert wird und sich dadurch auch unterschiedliche Schadensvolumen ergeben, aber es besteht Einigkeit darüber, dass die Cyberkriminalität eine überaus einträgliche, nur mit geringem Risiko verbundene Verbrechensform ist, die sich zunehmend ausbreitet und deren Schaden immer größer wird. In einer Zeit, in der die Förderung des Wirtschaftswachstums oberstes Gebot ist, ist daher eine stärkere Bekämpfung der Cyberkriminalität von wesentlicher Bedeutung, wenn es darum geht, das Vertrauen der Bürger und der Unternehmen in die Sicherheit der Onlinekommunikation und des Internethandels zu wahren. Außerdem trägt dies zur Erreichung der Wachstumsziele der Strategie „Europa 2020“[5] und der Digitalen Agenda für Europa[6] bei.

Die digitale Revolution der vergangenen Jahre ist in erster Linie auf die Freiheit im Internet zurückzuführen. Im Internet gibt es nämlich weder Ländergrenzen noch eine globale Kontrollinstanz. Diese Onlinefreiheit sollten wir nach Maßgabe der Charta der Grundrechte der Europäischen Union fördern und schützen, gleichzeitig aber auch versuchen, die Bürger

---

1 Eurostat, „Internetzugang und –nutzung“, 14. Dezember 2010.

2 McKinsey Global Institute, „Internet Matters: the Net's sweeping impact on growth, jobs and prosperity“, Bericht vom Mai 2011, Zugriff am 8. Februar 2012).

3 Norton Cybercrime Report 2011, Symantec, 7. September 2011, Zugriff am 6. Januar 2012.

4 Ibid.

5 Europa 2020 - Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum (KOM(2010) 2020 vom 3. März 2010).

6 Eine Digitale Agenda für Europa (KOM(2010) 245 endg. vom 26. August 2010).

vor organisierten kriminellen Vereinigungen, die diese Offenheit für ihre Zwecke missbrauchen wollen, zu schützen. Da sich keine andere Verbrechensform so sehr über Ländergrenzen hinwegsetzt wie die Cyberkriminalität, müssen die Strafverfolgungsbehörden ebenfalls über Ländergrenzen hinweg koordiniert zusammenarbeiten, und zwar in gleichem Maße mit staatlichen wie mit privaten Akteuren. Genau hier kann die EU einen erheblichen Nutzen bewirken – und das tut sie auch.

Die Europäische Union hat bereits verschiedene Initiativen zur Bekämpfung der Cyberkriminalität ergriffen, darunter die im Jahr 2011 erlassene Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und die voraussichtlich noch im Jahr 2012 erlassene Richtlinie über Angriffe auf Informationssysteme, durch die insbesondere der Einsatz von Cyberkriminalitätswerkzeugen wie Botnetzen[7] unter Strafe gestellt werden soll. Außerdem hat Europol seine Maßnahmen zur Bekämpfung der Cyberkriminalität verstärkt und eine zentrale Rolle bei der unlängst durchgeführten Fahndungsaktion „Operation Rescue“ gespielt, bei der die Polizei im Anschluss an eine der größten Untersuchungen, die jemals von Strafverfolgungsbehörden weltweit unternommen wurden, 184 des Kindesmissbrauchs verdächtigte Personen festgenommen und über 200 Missbrauchsopfer ermittelt hat. Dank der Mithilfe von Europol-Analysten, denen es gelang, die Sicherheitsvorrichtungen eines zentralen Computerservers des betreffenden Netzes zu „knacken“, konnten dabei die Namen und die Machenschaften der des Kindesmissbrauchs verdächtigten Personen aufgedeckt werden.

Die Bekämpfung der Cyberkriminalität, deren wichtigstes Rechtsinstrument das Europarat-Übereinkommen über Computerkriminalität[8] ist, hat nach wie vor vorrangige Bedeutung. Sie ist Bestandteil des EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität[9] und der Anstrengungen zur Entwicklung einer Gesamtstrategie der EU zur Stärkung der Sicherheit im Internet. Zudem arbeitet die EU auf diesem Gebiet eng mit internationalen Partnern zusammen, beispielsweise in der unlängst eingesetzten gemeinsamen Arbeitsgruppe der EU und der USA für die Bereiche Cybersicherheit und -kriminalität.

Trotz dieser Fortschritte stehen einer effizienten Untersuchung von Cyberstraftaten und einer wirksamen Verfolgung der Täter auf EU-Ebene noch immer Hindernisse entgegen: Grenzen der Gerichtsbarkeit, unzureichende Möglichkeiten für den Austausch sachdienlicher Erkenntnisse, technische Probleme bei der Ermittlung der Täterherkunft, ungleiche Kapazitäten für Untersuchungen und computerforensische Maßnahmen, Mangel an Fachpersonal und uneinheitliche Zusammenarbeit mit anderen für die Sicherheit im Internet

---

7 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates (KOM(2010) 517 endg. vom 30. September 2010). Botnetze bestehen aus mit bösartiger Software infizierten Computern, die aus der Ferne aktiviert und so für bestimmte Maßnahmen wie Internetangriffe missbraucht werden können.

8 Europarat-Übereinkommen über Computerkriminalität (unterzeichnet am 23. November 2001 in Budapest), auch „Budapester Konvention gegen Datennetzkriminalität“ genannt, nebst „Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art“.

9 Im Rahmen des EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität für den Zeitraum 2011-2013 werden acht vorrangige Ziele verfolgt, darunter die „verstärkte Bekämpfung der Cyberkriminalität und des kriminellen Missbrauchs des Internets durch organisierte kriminelle Gruppen“.

zuständigen Stellen. Mit Hilfe des Stabilitätsinstruments versucht die EU unter anderem, den sich rasch ausbreitenden grenzüberschreitenden Bedrohungen im Zusammenhang mit der Cyberkriminalität in Entwicklungs- und Schwellenländern zu begegnen, denen es oftmals an Kapazitäten zur Bekämpfung dieser Form der organisierten Kriminalität mangelt.

Um diesen Herausforderungen zu begegnen, hat die Kommission die Einrichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität zu einem vorrangigen Ziel der EU-Strategie der inneren Sicherheit[10] erhoben. Sie hat eine Machbarkeitsstudie[11] über die Schaffung eines solchen Zentrums auf Ersuchen des Rates[12] durchgeführt und schlägt nunmehr die Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität vor, das Teil von Europol sein und als Anlaufstelle für die Bekämpfung der Cyberkriminalität dienen soll. In dieser auf der Machbarkeitsstudie fußenden Mitteilung werden nachfolgend die vorgeschlagenen Kernfunktionen des Zentrums vorgestellt, und es wird erläutert, warum das Zentrum im Europäischen Polizeiamt angesiedelt werden sollte und wie seine Errichtung vonstatten gehen könnte. Bevor das Zentrum seinen Betrieb aufnehmen kann, sollte allerdings noch sein Ressourcenbedarf näher geprüft werden. Der Errichtung des Zentrums wird in geeigneter Weise bei der anstehenden Überarbeitung der Rechtsgrundlage von Europol Rechnung getragen werden.

2. VORSCHLAG ZUR ERRICHTUNG EINES EUROPÄISCHEN ZENTRUMS ZUR BEKÄMPFUNG DER CYBERKRIMINALITÄT

Damit das Europäische Zentrum zur Bekämpfung der Cyberkriminalität unter Wahrung des Subsidiaritätsgrundsatzes einen zusätzlichen Nutzen bewirken kann, wird vorgeschlagen, dass sich das Zentrum vorrangig mit folgenden Deliktformen der Cyberkriminalität befassen sollte:

(i) von organisierten kriminellen Vereinigungen begangene Cyberstraftaten, insbesondere Straftaten mit hohen illegalen Erträgen (z.B. Online-Betrug);

(ii) Cyberstraftaten mit schwerwiegenden Folgen für die Opfer (z.B. mit Hilfe des Internets begangener sexueller Missbrauch von Kindern) und

(iii) Cyberstraftaten (einschließlich Cyberangriffe) gegen kritische Infrastrukturen und Informationssysteme in der Union[13].

Da sich die Cyberkriminalität ständig weiterentwickelt, sollte zudem die Möglichkeit bestehen, sowohl nach Maßgabe der Anforderungen der Mitgliedstaaten tätig zu werden als auch auf neue von der Cyberkriminalität ausgehende Gefahren für die Union zu reagieren.

---

10 „Spätestens 2013 soll die EU über ein Zentrum für Cyberkriminalität verfügen, das (…) den Mitgliedstaaten und den Organen der EU erlauben soll, operationelle und analytische Kapazitäten für einschlägige Ermittlungen aufzubauen und die Zusammenarbeit mit internationalen Partnern zu verstärken“ (EU-Strategie der inneren Sicherheit: fünf Handlungsschwerpunkte für mehr Sicherheit, KOM(2010)673 endg. vom 22. November 2010).

11 Abschließender Bericht vom Februar 2012.

12 Schlussfolgerungen des Rates „Allgemeine Angelegenheiten“ betreffend einen Aktionsplan zur Umsetzung der konzertierten Strategie für die Kriminalitätsbekämpfung (Luxemburg, 26. April 2010).

13 Im Sinne der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008, die zurzeit überarbeitet wird. Bei der Schaffung des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität würden weitere Entwicklungen berücksichtigt.

2.1. Kernfunktionen und -aufgaben des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte die folgenden vier Kernfunktionen haben:

(a) Europäische Anlaufstelle für Informationen über Cyberstraftaten

Durch eine Informationsverknüpfungsfunktion würde sichergestellt, dass Informationen über Cyberstraftaten aus umfangreichen öffentlichen, privaten und offenen Quellen zusammengetragen und die verfügbaren polizeilichen Daten auf diese Weise angereichert werden könnten. Die Lücken, die derzeit noch zwischen den Informationen bestehen, welche von den für die Sicherheit im Internet und für die Bekämpfung der Cyberkriminalität zuständigen Stellen übermittelt werden, könnten auf diese Weise Schritt für Schritt geschlossen werden. Zusammengetragen würden Informationen über Cyberstraftaten, über die Vorgehensweisen der Täter und über verdächtige Personen. Dadurch würde das Wissen über Cyberstraftaten ebenso verbessert wie die Verhütung, die Aufdeckung und die Verfolgung derartiger Straftaten, und es würden Anregungen für Kontakte zwischen Strafverfolgungsbehörden, dem CERT-Netz (IT-Notfallteams) und im Privatsektor tätigen Spezialisten für die Sicherheit von Informations- und Kommunikationstechnologien (IKT) gegeben. Bei dem Informationsaustausch müssten natürlich die zwischen den verschiedenen Beteiligten vereinbarten Vertraulichkeitsabkommen und -regeln eingehalten werden.

Die Informationsverknüpfungsfunktion wäre zudem nützlich für die Verbesserung der Berichterstattung über Cyberstraftaten und den diesbezüglichen Informationsaustausch. Die Kommission möchte daher alle Mitgliedstaaten ermutigen, eine Pflicht zur Meldung schwer wiegender Cyberstraftaten[14] an ihre nationalen Strafverfolgungsbehörden einzuführen. Die nationalen Polizeidienste könnten so mehr Informationen über Cyberstraftaten an das Europäische Zentrum zur Bekämpfung der Cyberkriminalität übermitteln, und das Zentrum könnte diese Informationen dann verbreiten, damit möglicherweise auf das gleiche Ziel hinarbeitende Kollegen in anderen Mitgliedstaaten in Kenntnis gesetzt werden und von den Informationen des jeweils anderen profitieren können.

Dabei geht es darum, den Kenntnisstand über die Cyberkriminalität in Europa mit der Zeit zu verbessern, damit hochwertige Strategieberichte über Entwicklungen und Bedrohungen erstellt, sich auf umfassende Kriminalitätsstatistiken stützende Erkenntnisse gewonnen und die Informationssammlung und -auswertung dank einer aus einer Vielzahl von Quellen schöpfenden Informationsgrundlage verbessert werden können.

(b) Europäische Sammelstelle für cyberkriminalitätsspezifisches Fachwissen zur Unterstützung der Mitgliedstaaten beim Aufbau geeigneter Kapazitäten

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte die Mitgliedstaaten mit seinem Fachwissen und durch Schulungsmaßnahmen bei der Eindämmung von Cyberdelikten unterstützen. Hauptschwerpunkt dabei sollte die Unterstützung von Strafverfolgungsbehörden sein, wobei aber auch Schulungsmaßnahmen für Mitarbeiter von Justizbehörden angeboten werden sollten. Die bereits bestehenden Initiativen von Europol,

---

[14] Darunter Cyberstraftaten nach Artikel 3 bis 7 des unterbreiteten Vorschlags für eine Richtlinie über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates (KOM(2010)517 endg. vom 30. September 2010).

CEPOL und den Mitgliedstaaten würden nach Maßgabe einer gründlichen Bedarfsanalyse zusammengelegt, damit sie einfacher zu koordinieren wären und einander besser ergänzen könnten. Die Palette der angebotenen Schulungsmaßnahmen sollte von umfassenden technischen Schulungen bis hin zu allgemeinen Maßnahmen für Polizeibedienstete, Staatsanwälte und Richter reichen, durch die letztere ihre Fähigkeit zur Behandlung von Fällen auf dem Gebiet der Cyberkriminalität verbessern können.

Es sollte ein Cyberkriminalitätsschalter eingerichtet werden, über den bewährte Praktiken und Wissen ausgetauscht sowie Anfragen mitgliedstaatlicher und internationaler Strafverfolgungsbehörden, der Justizbehörden, des Privatsektors und gesellschaftlicher Organisationen entgegengenommen und beantwortet werden können (beispielsweise bei Cyberangriffen oder neuen Formen des Onlinebetrugs).

Auf diesem Wege sollten zudem Sachverständigengruppen für den Bereich Cyberkriminalität (u.a. die von der EU eingesetzte Taskforce „Cyberkriminalität“) und Fachleute für die Bekämpfung des mit Hilfe des Internets verübten sexuellen Missbrauchs von Kindern beraten und unterstützt werden. Auch sollte dieser Schalter mit dem im Aufbau befindlichen Netz von Exzellenzzentren für die Bekämpfung der Cyberkriminalität (wie dem „2Centre“) und der Forschungsgemeinschaft zusammenarbeiten.

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte die Mitgliedstaaten ferner dabei unterstützen, eine auf allgemeinen Standards fußende Anwendung für die Meldung von Cyberstraftaten über das Internet zu entwickeln und einzuführen, über die Meldungen verschiedener Akteure wie Unternehmen, nationale bzw. staatliche IT-Notfallteams und Bürger an nationale Strafverfolgungsbehörden bzw. Meldungen der nationalen Strafverfolgungsbehörden an das Europäische Zentrum zur Bekämpfung der Cyberkriminalität weitergeleitet werden können.

Auch sollte das Zentrum zum Austausch bewährter Praktiken in den Bereichen Strafjustiz und –verfolgung beitragen bzw. diesen Austausch erleichtern. Eine effiziente Einbindung der Justiz in die Bekämpfung schwerer Cyberstraftaten ist eine unabdingbare Voraussetzung für eine bessere strafrechtliche Verfolgung der Täter in den Mitgliedstaaten.

(c) Unterstützung der von den Mitgliedstaaten durchgeführten Untersuchungen über Cyberstraftaten

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte operative Unterstützung für Untersuchungen über Cyberstraftaten leisten und zu diesem Zweck beispielsweise die Einsetzung gemeinsamer Untersuchungsteams zur Aufklärung von Cyberstraftaten und den Austausch operativer Informationen aus laufenden Untersuchungen fördern.

Zudem sollte das Zentrum hochwertige computerforensische Unterstützung in Form von Anlagen, Speichermöglichkeiten und Tools sowie Sachverständigenwissen auf dem Gebiet der Datenverschlüsselung für Untersuchungen über Cyberdelikte zur Verfügung stellen.

(d) Sprachrohr aller mit Untersuchungen über Cyberstraftaten befassten Strafverfolgungs- und Justizbediensteten in der EU

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität könnte mit der Zeit zu einer zentralen Anlaufstelle für mit Untersuchungen über Cyberstraftaten befasste Ermittler in der

EU ausgebaut werden und diesen als Sprachrohr dienen bei Diskussionen mit der IKT-Industrie und anderen Unternehmen des Privatsektors sowie mit der Forschungsgemeinschaft, mit Verbraucherverbänden und mit gesellschaftlichen Organisationen über die Frage, wie die Prävention von Cyberdelikten und die Koordinierung gezielter Forschungsmaßnahmen verbessert werden könnten.

Das Zentrum wäre die optimale Schnittstelle zu den von Interpol ergriffenen Maßnahmen zur Bekämpfung der Cyberkriminalität und zu anderen internationalen Polizeidienststellen, die sich speziell mit der Bekämpfung derartiger Delikte befassen. Es könnte zudem die Beiträge zu laufenden Initiativen zur Steuerung des Internet und zu der mit einem unbefristeten Mandat ausgestatteten Sachverständigengruppe der Vereinten Nationen zum Thema Cyberkriminalität koordinieren.

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte ferner mit Organisationen wie dem INSAFE[15]-Netz bei Aufklärungskampagnen zusammenarbeiten und diese Organisationen über von ihm ermittelte Veränderungen auf dem Gebiet der Cyberkriminalität auf dem Laufenden halten, um ein umsichtiges und sicheres Onlineverhalten zu fördern.

2.2. Standort

Die Machbarkeitsstudie hat ergeben, dass es sinnvoll wäre, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität in den bestehenden Strukturen von Europol anzusiedeln.

Dies hätte mehrere Vorteile: Zum einen spielt Europol eine anerkannte Rolle unter den Mitgliedstaaten und anderen Hauptakteuren wie Interpol und den internationalen Strafverfolgungsbehörden, und es besitzt bereits ein Mandat zur Bekämpfung der Computerkriminalität[16]. Zum anderen besteht die Kerntätigkeit von Europol darin, zum Wohle aller Bürger für mehr Sicherheit in Europa zu sorgen, indem es die Strafverfolgungsbehörden der EU durch den Austausch und die Analyse von sachdienlichen strafrechtlichen Informationen über Straftaten unterstützt. Eine Ansiedlung des Zentrums innerhalb von Europol wäre mit seinem Rechtsrahmen vereinbar.

2.3. Mittelbedarf

Im Rahmen der Machbarkeitsstudie sind verschiedene Szenarien samt Mittelbedarf analysiert worden. Der Mittelbedarf wird insbesondere im Lichte etwaiger sonstiger, möglicherweise von Europol künftig übernommener Aufgaben und des allgemeinen Rahmens der Personalausstattung von EU-Agenturen näher zu prüfen[17] sein. Diese Prüfung wird insbesondere vor dem Hintergrund der Neufassung der Rechtsgrundlage für Europol und der laufenden Diskussion über den von der Kommission vorgeschlagenen Fonds für innere Sicherheit zu erfolgen haben. Gleichwohl scheint aber bereits jetzt klar zu sein, dass Personalabstellungen von Seiten der Mitgliedstaaten erforderlich wären.

---

15 Europäisches Netzwerk von Sensibilisierungszentren zur Förderung einer sicheren und verantwortungsvollen Nutzung des Internet und von Mobilgeräten durch junge Menschen.

16 Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), Artikel 4 Absatz 1 in Verbindung mit dem Anhang.

17 Diese Prüfung hat nach Maßgabe der allgemeinen Personal- und Haushaltsvorgaben für Agenturen gemäß dem Haushaltsplan 2013 und dem nächsten mehrjährigen Finanzrahmen zu erfolgen.

Die Kommission wird sich bei der Abschätzung des Ressourcenbedarfs von drei Überlegungen leiten lassen: Erstens wird davon ausgegangen, dass die Cyberkriminalität und die betreffende Fallarbeit nicht massiv, sondern moderat zunehmen werden, zweitens werden die Mitgliedstaaten ihre eigenen Kapazitäten zur Bekämpfung der Cyberkriminalität weiter ausbauen, und drittens würde sich das Zentrum nur mit bestimmten Formen der Cyberkriminalität befassen.

2.4. Steuerung

Im Falle der Ansiedlung des Zentrums innerhalb von Europol wäre es wichtig, andere Hauptakteure in die strategische Ausrichtung des Zentrums einzubinden. Daher schlägt die Kommission vor, innerhalb der Führungsstruktur von Europol einen für das Europäische Zentrum zur Bekämpfung der Cyberkriminalität zuständigen Programmausschuss einzusetzen, in dem der Leiter des Zentrums den Vorsitz führt. Somit könnten andere Beteiligte wie Eurojust, CEPOL und die Mitgliedstaaten (über ihre Vertreter in der EU-Taskforce „Cyberkriminalität“), die Europäische Agentur für Netz- und Informationssicherheit (ENISA) und die Kommission eigenes Fachwissen einbringen, ohne dass ein unnötiger Verwaltungsaufwand entstehen würde. Der Programmausschuss könnte darauf achten, dass das Zentrum in verantwortungsvoller Weise seinen Aufgaben im Zusammenhang mit der Bekämpfung der Cyberkriminalität nachgeht und so dafür sorgen, dass bei allen Tätigkeiten des Zentrums mit allen Beteiligten partnerschaftlich verfahren, ihr Sachverstand anerkannt und ihrem Mandat Rechnung getragen wird.

2.5. Zusammenarbeit mit den Hauptakteuren

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte eine koordinierte Antwort auf Cyberstraftaten ermöglichen und zu diesem Zweck nicht nur die Zusammenarbeit zwischen EU-Agenturen erleichtern, sondern auch als zentrale Anlaufstelle der EU für diesen Bereich dienen.

(a) Mitgliedstaaten

Hauptzweck des Zentrums ist die Unterstützung der Mitgliedstaaten bei der Bekämpfung der Cyberkriminalität. Sowohl der genannte Cyberkriminalitätsschalter als auch die dem Zentrum gesetzten Zielvorgaben wie eine genauere Bedrohungsanalyse und eine mit besseren Informationen untermauerte operative Unterstützung würden allen mit Untersuchungen über Cyberstraftaten befassten Ermittlern in ganz Europa zugute kommen. Die Mitgliedstaaten könnten ihre Anliegen über ihre Vertreter aus der EU-Taskforce „Cyberkriminalität" im Programmausschuss des Zentrums vortragen. Darüber hinaus wären weitere Investitionen der Mitgliedstaaten in ihre nationalen Strukturen zur Bekämpfung der Cyberkriminalität nötig, um geeignete Schnittstellen für die Zusammenarbeit mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität zu schaffen.

(b) EU-Agenturen und sonstige Akteure

Die zuständigen Agenturen (vor allem Eurojust, CEPOL und die ENISA) sowie das IT-Notfallteam der EU würden unmittelbar in die Arbeit des Zentrums eingebunden: zum einen durch die Mitwirkung im Programmausschuss, zum anderen durch eine je nach Bedarf erfolgende operative Zusammenarbeit.

(c) Internationale Partner

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte danach streben, zu einem Informationsknotenpunkt der EU für cyberkriminalitätsspezifische Fragen und zu einem wertvollen Gesprächspartner für internationale Stellen zu diesem Themenbereich zu werden. Das Zentrum sollte deshalb gemeinsam mit Interpol und den strategischen Partnern der EU in aller Welt an besser koordinierten Antworten für die Bekämpfung von Cyberstraftaten arbeiten und dafür Sorge tragen, dass die Anliegen der Strafverfolgungsbehörden bei der Weiterentwicklung des Cyberspace berücksichtigt werden.

(d) Privatsektor, Forschungsgemeinschaften und gesellschaftliche Organisationen

Für die Bekämpfung der Cyberkriminalität ist es von größter Bedeutung, dass zwischen dem Privatsektor und den Strafverfolgungsbehörden Vertrauen aufgebaut wird. Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte die Zusammenarbeit zwischen Europol und dessen bestehenden und neuen Partnern festigen und vertrauenswürdige Netze und Plattformen für den Informationsaustausch mit der Wirtschaft und anderen Akteuren wie der Forschungsgemeinschaft und gesellschaftlichen Organisationen aufbauen. Dadurch sollten der gemeinschaftsübergreifende Informationsaustausch über bestimmte Themen wie die Frühwarnung vor Cyberbedrohungen ebenso erleichtert werden wie gemeinsame, nach „Taskforce"-Manier erarbeitete Antworten auf Cyberangriffe und andere Formen der Cyberkriminalität.

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität sollte ferner einen Beitrag zu den allgemeinen Anstrengungen leisten, die Privatunternehmen mit beträchtlichem digitalem Vermögen (z.B. Banken und Onlinehändler) unternehmen, um Cyberstraftaten zu bekämpfen, um sich besser vor diesen zu schützen und um die Angriffspunkte, die neue Technologien für Cyberdelikte bieten können, auf ein Minimum zu reduzieren.

Es liegt im beiderseitigen Interesse der Strafverfolgungsbehörden und des Privatsektors, sich rascher und besser ein Bild von der aktuellen Bedrohung durch Cyberdelikte machen zu können und darauf hinzuwirken, dass dank einer besseren Aufdeckung neuer Vorgehensweisen der Täter letztere rasch festgenommen und so ganze Netze von Cyberstraftätern ausgehoben werden können.

3. AHRPLAN ZUR ERRICHTUNG DES EUROPÄISCHEN ZENTRUMS ZUR BEKÄMPFUNG DER CYBERKRIMINALITÄT

3.1. Maßnahmen bis Ende 2013

Um die Anfangsbetriebsfähigkeit des Zentrums herstellen zu können, wird die Kommission in enger Zusammenarbeit mit Europol prüfen, wie hoch der Personal- und Finanzbedarf für die Einsetzung eines Implementierungsteams bis zum Ende des derzeitigen Finanzrahmens der EU wäre. Das Implementierungsteam hätte beispielsweise die Aufgabe, die Leistungsanforderungen des Zentrums und seine Organisationsstruktur festzulegen und Indikatoren für die Bewertung seiner Leistung zu entwickeln.

Im Hinblick auf die Schaffung einer umfassenden Datenverknüpfungsfunktion sollte das Implementierungsteam geeignete Verbindungen zum IT-Notfallteam der EU sowie gegebenenfalls zur ENISA herstellen. Um die Berichterstattung über Cyberstraftaten zu

verbessern, sollte zudem eine Karte der Interoperabilität zwischen den bestehenden Online-Berichterstattungssystemen für Cyberdelikte in den Mitgliedstaaten erstellt werden.

Es sollte ein Cyberkriminalitätsschalter eingerichtet werden. Zu seiner Unterstützung könnte eine spezielle sichere Onlineplattform für die betreffende Gemeinschaft geschaffen werden. Die derzeitigen Schulungsmaßnahmen von Europol, CEPOL und der Europäischen Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG) könnten analysiert und in Absprache mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität und seinem Programmausschuss verschlankt werden. Auch sollte der Schulungsbedarf unter Berücksichtigung der Anforderungen von Richtern und Staatsanwälten geprüft werden. Nach Maßgabe der Analyseergebnisse könnte sodann ein einführender Schulungskurs über die Bekämpfung der Cyberkriminalität aufgelegt werden, an dem auch Mitglieder der Strafgerichtsbarkeit teilnehmen könnten.

Zudem müsste eine genauere Schätzung des Personal- und Finanzbedarfs vorgenommen bzw. in den Beschlüssen für den nächsten mehrjährigen Finanzrahmen vorgesehen werden. Die Ergebnisse dieser Schätzung könnten dann in die Weiterentwicklung des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität einfließen.

4. SCHLUSSFOLGERUNG

Da das organisierte Verbrechen seine Machenschaften zunehmend auf den Onlinebereich ausweitet, gilt es für die Strafverfolgung, hiermit Schritt zu halten. Die EU kann den Mitgliedstaaten und der Wirtschaft geeignete Werkzeuge für die Bekämpfung der Cyberkriminalität zur Verfügung stellen, die eine moderne und sich stetig weiterentwickelnde Bedrohung darstellt, welche definitionsgemäß nicht an Landesgrenzen Halt macht. Falls die erforderlichen personellen und finanziellen Ressourcen bereitgestellt werden können, würde ein Europäisches Zentrum zur Bekämpfung der Cyberkriminalität geschaffen, das als zentrale Anlaufstelle für den europaweit geführten Kampf gegen die Cyberkriminalität dienen und zu diesem Zweck Fachwissen bündeln, strafrechtliche Untersuchungen unterstützen und EU-weite Lösungen fördern sowie in der ganzen Union das Bewusstsein für die Problematik der Cyberkriminalität schärfen würde. Auch würde das Zentrum als solches zur Erhaltung eines offenen Internets und der legitimen digitalen Wirtschaft sowie zum Schutz der EU-Bürger und -Unternehmen bei Onlinetätigkeiten beitragen.

Der Rat wird ersucht, diesen Vorschlag anzunehmen, und das Europäische Parlament und andere wichtige Beteiligte werden gebeten, zur Entwicklung des Zentrums beizutragen.