Rat der
Europäischen Union

Brüssel, den 9. Juni 2016
(OR. en)

10007/16

JAI 552
COPEN 195
DROIPEN 109
CYBER 67
JAIEX 61
EJUSTICE 121

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	9. Juni 2016
Empfänger:	Delegationen
Nr. Vordok.:	9579/16 + COR 1
Betr.:	Schlussfolgerungen des Rates der Europäischen Union zur Verbesserung der Strafjustiz im Cyberspace - Schlussfolgerungen des Rates (9. Juni 2016)

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Verbesserung der Strafjustiz im Cyberspace, die vom Rat auf seiner 3473. Tagung am 9. Juni 2016 angenommen wurden.

ANLAGE

Schlussfolgerungen des Rates der Europäischen Union zur Verbesserung der Strafjustiz im Cyberspace

ENTSCHLOSSEN, Straftätern keinen sicheren Zufluchtsort im Cyberspace zuzugestehen,

IN ANBETRACHT der immer stärkeren Auswirkungen der Cyberkriminalität, der durch den Cyberspace ermöglichten Kriminalität oder sonstiger krimineller Handlungen, die im Cyberspace einen digitalen Fußabdruck hinterlassen haben,

UNTER BETONUNG der zunehmenden Bedeutung elektronischer Beweismittel in Strafverfahren zu jeglicher Art von Kriminalität, insbesondere bei Terrorismus,

UNTER BETONUNG der Tatsache, dass der Schutz des Cyberspace vor Missbrauch und kriminellen Aktivitäten von großer Bedeutung für das Wohl unserer Volkswirtschaften und Gesellschaften ist und die Strafverfolgungs- und Justizbehörden daher über wirksame Instrumente für die Ermittlung und Verfolgung von Straftaten im Zusammenhang mit dem Cyberspace verfügen müssen,

UNTER HINWEIS darauf, dass die Bekämpfung der Cyberkriminalität eine der Prioritäten in der Europäischen Sicherheitsagenda vom 28. April 2015 ist, die auch eine Zusage der Kommission zum Abbau von Hindernissen, die Untersuchungen über Cyberstraftaten im Wege stehen, insbesondere Vorschriften über den Zugang zu Beweisen und Informationen, enthält,

UNTER HINWEIS auf die Beratungen der Justizminister über die künftigen Herausforderungen für eine effektive Strafverfolgung im digitalen Zeitalter auf der Tagung des Rates (Justiz und Inneres) im Dezember 2015[1],

UNTER HINWEIS auf die Unterstützung der Justizminister für die Entwicklung konkreter Elemente für ein gemeinsames Konzept der EU für die Gerichtsbarkeit im virtuellen Raum, die auf der informellen Tagung des Rates (Justiz und Inneres) vom 26. Januar 2016 bekundet wurde,

[1] Dok. 14369/15.

UNTER HINWEIS auf die gemeinsame Erklärung der EU-Minister für Justiz und Inneres und der Vertreter der EU-Organe zu den Terroranschlägen vom 22. März 2016 in Brüssel, in der betont wurde, dass vorrangig Wege gefunden werden müssen, um elektronische Beweismittel schneller und wirksamer zu sichern und zu erlangen, und zwar durch eine verstärkte Zusammenarbeit mit Drittländern und mit im europäischen Hoheitsgebiet tätigen Dienstleistungserbringern, damit die Einhaltung der Rechtsvorschriften der EU und der Mitgliedstaaten und der direkte Kontakt mit den Strafverfolgungsbehörden verbessert werden, und dass auf der Tagung des Rates (Justiz und Inneres) im Juni konkrete Maßnahmen bezüglich dieser komplexen Frage ermittelt werden müssen[2],

UNTER HINWEIS auf die Mitteilung vom 20. April 2016 an das Europäische Parlament, den Europäischen Rat und den Rat mit dem Titel "Umsetzung der Europäischen Sicherheitsagenda im Hinblick auf die Bekämpfung des Terrorismus und die Weichenstellung für eine echte und wirksame Sicherheitsunion", in der die Kommission zugesagt hat, Lösungen für die Probleme bei der Erlangung digitaler Beweismittel im Rahmen strafrechtlicher Ermittlungen vorzuschlagen,

UNTER HINWEIS auf den Bericht[3] über die Konferenz über die Gerichtsbarkeit im virtuellen Raum vom 7./8. März 2016 in Amsterdam, in dem die Beratungen über mögliche Lösungen zur Verbesserung der Ermittlungen im Cyberspace wiedergegeben werden, insbesondere hinsichtlich der Rechtshilfeverfahren, der Zusammenarbeit mit dem Privatsektor und der Ermittlungen im Cyberspace, wenn der Standort der Daten oder der Ursprung von Cyberangriffen (noch) nicht bekannt sind,

ZUR KENNTNIS NEHMEND, dass der Ständige Ausschuss für die innere Sicherheit (COSI) eine Reihe von Empfehlungen zur Verbesserung der operativen Zusammenarbeit bei strafrechtlichen Ermittlungen im Cyberspace abgegeben hat[4];

UNTER HINWEIS auf die laufende siebte Runde gegenseitiger Begutachtungen, die der praktischen und operativen Umsetzung der europäischen Maßnahmen zur Verhütung und Bekämpfung von Cyberkriminalität gilt und die einen wichtigen Beitrag zu den Bemühungen um eine stärkere Bekämpfung der Cyberkriminalität darstellt;

---

2 Dok. 7371/16.
3 Dok. 7323/16.
4 Dok. 8634/2/16 REV 2.

UNTER HINWEIS auf die Ergebnisse der Überprüfung des Rechtshilfeabkommens zwischen der EU und den USA[5],

UNTER HINWEIS auf die Schlussfolgerungen des Rates zum Europäischen Justiziellen Netz für Cyberkriminalität[6],

UNTER HINWEIS auf das Übereinkommen des Europarates vom 23. November 2001 über Computerkriminalität und sein Zusatzprotokoll, das von der Union als globaler Referenzrahmen für die Bekämpfung der Cyberkriminalität dargestellt wird,

UNTER HINWEIS auf die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen, durch die aufgrund der gegenseitigen Anerkennung grenzüberschreitende Ermittlungen in der EU schneller und effizienter werden sollen, sowie die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme, in der die Mitgliedstaaten aufgefordert werden, sicherzustellen, dass sie über eine operative nationale Kontaktstelle im Rahmen des bestehenden Netzes der operativen Kontaktstellen, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen, verfügen,

IN ANERKENNUNG der Tatsache, dass diese Instrumente zwar umfangreichere Möglichkeiten für die Strafverfolgung im Cyberspace bieten, es jedoch – auch aufgrund der schnellen Entwicklung der Technologie – weiterhin praktische und rechtliche Hindernisse gibt, z.B. in Fällen, in denen der Ursprung der Cyberangriffe oder der Standort der elektronischen Beweismittel (noch) nicht bekannt oder flüchtig ist oder einander widersprechende Regelungen die Zusammenarbeit mit den Diensteanbietern behindern,

UNTER HINWEIS darauf, dass durch den Cyberspace ermöglichte Kriminalität und Cyberkriminalität Grundrechte und Grundfreiheiten verletzt und der uneingeschränkte Schutz dieser Rechte und Freiheiten sichergestellt werden muss,

IN DER ERKENNTNIS, dass der Schutz der Grundrechte und -freiheiten und die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit für den Einsatz von Ermittlungsmaßnahmen maßgeblich sein sollten,

UNTER HINWEIS auf die Annahme der EU-Rechtsakte zur Reform des Datenschutzes, insbesondere der Datenschutzrichtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr,

---

[5] Dok. 9291/16.
[6] Dok. 10025/16.

UNTER HINWEIS auf die Berichte von 2012 und 2013 der Gruppe zu grenzübergreifenden Aspekten des Ausschusses für das Übereinkommen über Computerkriminalität, denen zufolge mehrere Länder sich bereits auf einer unklaren rechtlichen Grundlage am grenzüberschreitenden Zugang zu Daten über den Anwendungsbereich des Budapester Übereinkommens hinaus beteiligen,

IN ANERKENNUNG der Tatsache, dass die Mitgliedstaaten ein berechtigtes Interesse daran haben, in strafrechtlichen Ermittlungen mindestens den Standort elektronischer Beweismittel oder den Ursprung von Cyberangriffen zu bestimmen,

ENTSCHLOSSEN zu handeln, um die Rechtsstaatlichkeit im Cyberspace aufrechtzuerhalten,

VERFÄHRT DER RAT DER EUROPÄISCHEN UNION WIE FOLGT:

Er ERKENNT AN, dass für künftige Arbeiten im Hinblick auf eine bessere Durchsetzung der Rechtsstaatlichkeit im Cyberspace und eine bessere Erlangung elektronischer Beweismittel in Strafverfahren folgende Leitlinien gelten sollten:

- Die praktischen Lösungen für eine effektivere Durchführung der Strafverfolgung im Cyberspace sollten den Rechtsrahmen für Datenschutz und Grundrechte uneingeschränkt Rechnung tragen;
- es sollten eine verstärkte Zusammenarbeit mit Diensteanbietern oder andere vergleichbare Lösungen in Betracht gezogen werden, die eine rasche Offenlegung von Daten ermöglichen; für die Erlangung bestimmter Datenkategorien, insbesondere von Teilnehmerdaten, könnten weniger strenge rechtliche Verfahren in Erwägung gezogen werden, die allen Beteiligten zugute kämen;
- die Rechtshilfeverfahren in Bezug auf elektronische Daten sollten beschleunigt und vereinfacht werden; durch eine stärkere Zusammenarbeit mit den Diensteanbietern oder andere vergleichbare Lösungen ließen sich die Rechtshilfeersuchen zwischen den zuständigen Behörden mengenmäßig verringern;

- die Verfahren der gegenseitigen Anerkennung sollten im Hinblick auf eine effektive Sicherung und Erlangung elektronischer Beweismittel effizient genutzt werden;
- anhand der Überprüfung der Anknüpfungspunkte für die Zuständigkeit für Ermittlungsmaßnahmen[7] im Cyberspace sollten auch in Fällen, in denen der Datenstandort (noch) nicht bekannt oder flüchtig ist, andere Maßnahmen in Betracht gezogen werden;

er ERACHTET es als erforderlich, mit den einschlägigen Drittländern und privaten Parteien zusammenzuarbeiten, damit die einzelnen Maßnahmen für eine effektive Strafverfolgung im Cyberspace eine kombinierte Wirkung entfalten;

er VERTRITT DIE AUFFASSUNG, dass der Entwicklung eines gemeinsamen Konzepts der EU für die Verbesserung der Strafjustiz im Cyberspace Priorität eingeräumt werden sollte. Dabei sollte die Kohärenz mit den derzeitigen Arbeiten am Rahmen des Budapester Übereinkommens des Europarates gewahrt werden;

ER GELANGT DAHER ZU DEM SCHLUSS, DASS

I. DIE ZUSAMMENARBEIT MIT DEN DIENSTEANBIETERN INTENSIVIERT WERDEN MUSS.

Zu diesem Zweck

1. wird die KOMMISSION ersucht, zwecks Erlangung besonderer Kategorien von Daten, insbesondere Teilnehmerdaten, sofern diese nach dem Recht der Drittländer zulässig ist, einen gemeinsamen Rahmen für die Zusammenarbeit mit den Diensteanbietern oder eine andere vergleichbare Lösung auszuarbeiten, die eine rasche rechtmäßige Offenlegung solcher Daten ermöglicht[8]. Die Kommission wird ersucht, dies in Verbindung mit den Mitgliedstaaten und den betreffenden Drittländern und in Zusammenarbeit mit dem Privatsektor zu tun.

---

[7] Der Begriff "Zuständigkeit für Ermittlungsmaßnahmen" bezieht sich in diesen Schlussfolgerungen auf die Zuständigkeit der einschlägigen Behörden für die Durchführung einer Ermittlungsmaßnahme. Gemäß diesen Schlussfolgerungen sollte ein gemeinsames Konzept der EU im Hinblick auf die Verbesserung der Ermittlungen im Cyberspace in besonderen Fällen, in denen die bestehenden Rahmen nicht ausreichen, geprüft werden.

[8] Erfordert ein Ersuchen um Daten eine Weitergabe personenbezogener Daten durch die Behörde eines Mitgliedstaats, so müssen die einschlägigen Datenschutzvorschriften eingehalten werden.

2. Solche Lösungen sollten gemeinsam vereinbarte Anforderungen, einschließlich der Anforderungen der Notwendigkeit und der Verhältnismäßigkeit, für die Ersuchen an Diensteanbieter enthalten, die den rechtmäßigen Zugang zu in ihrem Besitz befindlichen Daten ermöglichen. Dabei ist anzustreben, widersprüchliche Auslegungen sowie Konflikte zwischen den bestehenden Regelungen zu vermeiden und das Problem der Nichtoffenlegung der angefragten Daten zu behandeln. Die Lösungsvorschläge dürfen Regelungen auf nationaler Ebene nicht entgegenstehen.

3. Zu diesem Zweck wird die KOMMISSION in Verbindung mit den Mitgliedstaaten ersucht, bei den Diensteanbietern die mögliche Verwendung vereinheitlichter Formulare und Instrumente wie in Abschnitt II beschrieben zu sondieren, um die Authentifizierung zu erleichtern, schnelle Verfahren sicherzustellen und die Transparenz und Nachweis-Führung beim Prozess zur Sicherung und Erlangung elektronischer Beweismittel zu verbessern.

DIE KOMMISSION wird aufgefordert, spätestens im Dezember 2016 einen Bewertungsbericht über die diesbezüglichen Fortschritte und bis Juni 2017 Ergebnisse vorzulegen.

II. DIE VERFAHREN DER RECHTSHILFE (UND GEGEBENENFALLS DER GEGENSEITIGEN ANERKENNUNG) VEREINFACHT WERDEN MÜSSEN

Zu diesem Zweck

4. wird die KOMMISSION ersucht, in Verbindung mit den MITGLIEDSTAATEN und erforderlichenfalls mit Drittstaaten vorrangig Möglichkeiten zu finden, um durch die Vereinfachung der Verfahren der Rechtshilfe und gegebenenfalls der gegenseitigen Anerkennung elektronische Beweismittel schneller und effektiver zu sichern und zu erlangen;
5. wird die KOMMISSION hierzu ersucht, in Verbindung mit den MITGLIEDSTAATEN, EUROJUST und Drittstaaten zu prüfen und Empfehlungen abzugeben, wie gegebenenfalls vorhandene Standardformulare und -verfahren im Hinblick auf Ersuchen um Sicherung und Erlangung elektronischer Beweismittel angepasst werden können;
6. wird die KOMMISSION im Hinblick auf eine noch effizientere Nutzung solcher Standardformulare und -verfahren zur Erlangung elektronischer Beweismittel ersucht, in Verbindung mit den MITGLIEDSTAATEN, EUROJUST, der CEPOL und erforderlichenfalls mit Drittstaaten gegebenenfalls mit Hilfe der vorhandenen elektronischen Instrumente und unter Achtung der Zuständigkeiten und der Kommunikationswege gemäß den bestehenden Rechtsrahmen Folgendes zu entwickeln:
    - ein sicheres Online-Portal für elektronische Ersuchen und Antworten betreffend elektronische Beweismittel und die entsprechenden Verfahren, einschließlich der fakultativen Verwendung von Maschinenübersetzung für derartige Ersuchen, sowie für deren Verfolgung und Rückverfolgung;
    - Leitlinien und spezielle Ausbildungsmodule in Zusammenarbeit mit dem Europäischen Netz für die Aus- und Fortbildung von Richtern und Staatsanwälten, dem Europäischen Justiziellen Netz für Cyberkriminalität und erforderlichenfalls mit den Behörden der Drittländer für die effiziente Nutzung der vorhandenen Rahmen für die Sicherung und Erlangung elektronischer Beweismittel, einschließlich Leitlinien zur Klärung der Frage, wann gemäß den geltenden Vorschriften nicht auf Instrumente der Rechtshilfe oder der gegenseitigen Anerkennung zurückgegriffen werden muss;

DIE KOMMISSION wird aufgefordert, bis Dezember 2016 einen Zwischenbericht über die diesbezüglichen Fortschritte und spätestens im Juni 2017 Ergebnisse vorzulegen. Die KOMMISSION wird ersucht, das Online-Portal spätestens im Dezember 2017 vorzustellen.

7. wird die KOMMISSION in Verbindung mit den MITGLIEDSTAATEN und erforderlichenfalls mit Drittstaaten ersucht, zusätzliche Maßnahmen zu prüfen, um u.a. mittels des Rechtshilferahmens zwischen der EU und den USA elektronische Beweismittel effektiver zu sichern und zu erlangen;
8. wird die KOMMISSION ersucht, im Hinblick auf den volle Ausnutzung der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen ("EEA-Richtlinie") zum Zwecke der Sicherung und Erlangung elektronischer Beweismittel in der EU die bis zum 22. Mai 2017 vorzunehmende Umsetzung dieser Richtlinie durch die Mitgliedstaaten weiterhin zu beobachten und zu unterstützen;
9. werden die MITGLIEDSTAATEN ersucht,
   - das Übereinkommen über Computerkriminalität vom 23. November 2001 zu ratifizieren und uneingeschränkt umzusetzen;
   - die EEA-Richtlinie zügig, spätestens bis zum 22. Mai 2017 umzusetzen;
   - ausreichende Kapazitäten zur Bearbeitung von Rechtshilfeersuchen mit Bezug auf Ermittlungen im Cyberraum sicherzustellen und dem Personal sachdienliche Schulungen zur Bearbeitung dieser Ersuchen zur Verfügung zu stellen;
   - die Nutzung der bestehenden, täglich rund um die Uhr erreichbaren Kontaktstellen zu optimieren und vermehrt gemeinsame Ermittlungsgruppen einzusetzen, um den Informationsaustausch zu erleichtern und/oder die Rechtshilfeverfahren zu beschleunigen.

III. DIE VORSCHRIFTEN ÜBER DIE ZUSTÄNDIGKEIT FÜR ERMITTLUNGSMASSNAHMEN IM CYBERSPACE ÜBERPRÜFT WERDEN SOLLTEN.

Zu diesem Zweck

10. wird DIE KOMMISSION ersucht, im Lichte der politischen Orientierung, die die Justizminister auf der Tagung des Rates vom Juni 2016 erteilt haben, und in Zusammenarbeit mit den MITGLIEDSTAATEN, EUROJUST und EUROPOL, Möglichkeiten für ein gemeinsames Konzept der EU für die Zuständigkeit für Ermittlungsmaßnahmen im Cyberspace in Situationen zu sondieren, in denen die bestehenden Rahmen nicht ausreichen, z.B. wenn mehrere Informationssysteme in verschiedenen Gerichtsbarkeiten gleichzeitig genutzt werden, um eine einzige Straftat zu verüben, wenn sich einschlägige elektronische Beweismittel innerhalb kurzer Zeit zwischen verschiedenen Gerichtsbarkeiten bewegen oder wenn der Standort der elektronischen Beweismittel oder der Ort der kriminellen Handlung mit ausgeklügelten Methoden verschleiert werden, so dass es zu einem "Standortverlust" kommt.[9]
11. Unter Berücksichtigung der Besonderheiten der jeweiligen Situation sollte festgestellt werden,

    - welche Anknüpfungspunkte eine Grundlage für die Zuständigkeit für Ermittlungsmaßnahmen im Cyberspace bieten können;
    - ob – und wenn ja, welche – Ermittlungsmaßnahmenunabhängig von physischen Grenzen eingesetzt werden können.

12. Zu berücksichtigen sind dabei:

    - die Art und die Schwere der Straftaten, die andernfalls ungestraft bleiben könnten;
    - mögliche Grundlagen für die Zuständigkeit für Ermittlungsmaßnahmen, und zwar anhand von Anknüpfungspunkten wie beispielsweise dem Ort, an dem der Diensteanbieter seinen Sitz hat, den wirtschaftlichen Tätigkeiten eines Diensteanbieters im ermittelnden Staat, d.h. wenn der Diensteanbieter Waren oder Dienstleistungen im Hoheitsgebiet des ermittelnden Staates anbietet ("geschäftliche Verbindung"), dem gewöhnlichen Aufenthaltsort der beschuldigten oder verdächtigen Person und/oder dem Aufenthaltsort der geschädigten Person;

[9] Dies sind lediglich Beispiele. Die Kommission wird ersucht, Lösungen für diese oder ähnlich gravierende Situationen, die ein solches Vorgehen rechtfertigen würden, zu prüfen.

- die Anwendung und Wirksamkeit innerstaatlicher Vorlageanordnungen auf der Grundlage derartiger möglicher Anknüpfungspunkte im Hinblick auf die Zuständigkeit für Ermittlungsmaßnahmen im Cyberspace;
- eine Kooperationslösung für den direkten grenzüberschreitenden Zugriff auf Daten ohne technische Unterstützung;
- geeignete Schutzmaßnahmen wie der Schutz der Grundrechte und -freiheiten sowie personenbezogener Daten und die Grundsätze der Verhältnismäßigkeit und der Subsidiarität als Leitprinzipien für den Einsatz von Ermittlungsmaßnahmen, um deren Rechtmäßigkeit zu gewährleisten;
- mögliche Analogien zu anderen grenzübergreifenden rechtlichen Regelungen wie z.B. dem Open-Sky-Abkommen und dem Seerechtsübereinkommen, den EU-Vorschriften zum Datenschutz und dem Wettbewerbsrecht der EU;
- die Auswirkungen eines solchen Ansatzes auf den geltenden Rechtsrahmen.

DIE KOMMISSION wird ersucht, spätestens im Dezember 2016 über die Fortschritte bei der Entwicklung dieses Ansatzes zu berichten und bis Juni 2017 die Ergebnisse ihrer Bewertung vorzulegen. Die Bewertung sollte konkrete Elemente für ein gemeinsames Konzept der EU sowie Vorschläge für dessen Umsetzung einschließlich der Möglichkeit einer diesbezüglichen Gesetzgebungsinitiative umfassen.