Rat der
Europäischen Union

Brüssel, den 23. November 2016
(OR. en)

14711/16

LIMITE

CYBER 137
JAI 976
ENFOPOL 429
GENVAL 122
COSI 192
COPEN 352

VERMERK

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Nr. Vordok.:	13993/16
Betr.:	Verschlüsselung: Herausforderungen für die Strafjustiz im Zusammenhang mit dem Einsatz von Verschlüsselung - künftige Schritte - Sachstandsbericht

Einleitung

1. Das Internet hat die Kommunikation unserer heutigen Welt verändert; Verschlüsselungstechniken werden derzeit weltweit Teil dieser neuen Kommunikationsmodelle. Die Verschlüsselung dient sowohl den legitimen Bedürfnissen hinsichtlich Privatsphäre und Sicherheit und der Wahrnehmung der Grundrechte des Einzelnen als auch den Bedürfnissen von Unternehmen und Regierungen hinsichtlich eines funktionierenden und sicheren Cyberraums. Die Unternehmen haben begonnen, in Instrumente zu investieren und/oder Instrumente zu entwickeln, die höchstmöglichen Schutz bieten und bei denen zum Schutz der Privatsphäre ihrer Kunden und zur Erhöhung der Cybersicherheit eine leistungsfähige Verschlüsselung zum Einsatz kommt. Alle Bemühungen, die Verschlüsselung oder die Sicherheitsprotokolle allgemein aufzuweichen, könnten nicht nur private Informationen der Menschen und sensible Geschäftsinformationen dem Missbrauch durch andere Parteien preisgeben, sondern auch erhebliche Risiken für die Computer- und Netzsicherheit mit sich bringen.

2. In der Praxis kann jedermann Verschlüsselung einsetzen, um seine persönlichen Daten und/oder Mitteilungen zu sichern und zu schützen. Eine sichere Datenverarbeitung ist ein wichtiger Bestandteil des Schutzes personenbezogener Daten, und die Verschlüsselung wird in der kürzlich erlassenen allgemeinen Datenschutzverordnung als eine der Sicherheitsvorkehrungen anerkannt. Unternehmen, öffentlichen Verwaltungen und Einzelpersonen wird nahegelegt, zum Schutz ihrer Daten und elektronischen Kommunikation auf Verschlüsselung zurückzugreifen. Die Datenschutzrichtlinie für elektronische Kommunikation legt außerdem nahe, Verschlüsselungstechnologien zum Schutz der Kommunikation der Nutzer einzusetzen. Die Möglichkeiten der Verschlüsselungstechnologien werden jedoch auch von Kriminellen ausgenutzt, um ihre Daten und etwaige Beweise zu verbergen, ihre Kommunikation zu schützen und ihre finanziellen Transaktionen zu verschleiern.

3. Europols Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA) 2016 zufolge ist eine leistungsfähige Verschlüsselung für den elektronischen Geschäftsverkehr und andere Internettätigkeiten äußerst wichtig, hängt eine angemessene Sicherheit jedoch davon ab, dass die Strafverfolgungsbehörden in der Lage sind, bei Straftaten erfolgreich zu ermitteln. Der Einsatz von Verschlüsselung nimmt der Strafverfolgung entscheidende Möglichkeiten der Beweiserhebung, insbesondere in Anbetracht dessen, dass sie nicht mehr nur auf Desktop-Computer beschränkt ist, sondern in zunehmendem Maße auf mobilen Geräten verfügbar ist und viele kommerziell zugängliche Kommunikationsplattformen nunmehr standardmäßig verschlüsseln (in zunehmendem Maße durch eine Verschlüsselung der Daten von Endstelle zu Endstelle, die dazu führt, dass Dienste nicht überwacht werden können).

4. Auf dem strategischen Seminar zum Thema "Schlüssel zum Cyberraum", das am 2. Juni 2016 von Eurojust veranstaltet wurde, haben Experten Informationen über verschiedene Fragen einschließlich Verschlüsselung ausgetauscht. Die Diskussion konzentrierte sich vor allem auf den Zugang zu verriegelten mobilen Geräten und insbesondere auf die Möglichkeit, zuvor erfasste Fingerabdrücke von Verdächtigen zum Entriegeln eines verriegelten Geräts zu nutzen, um Zugang zu den Daten zu erhalten. Es bestand allgemeines Einvernehmen über die Notwendigkeit, die Privatsphäre der Bürgerinnen und Bürger auch durch Verschlüsselung zu schützen, jedoch sollte sorgfältig zwischen dieser Notwendigkeit und dem Erfordernis der Kriminalitätsbekämpfung, die wiederum eine höhere Sicherheit aller Bürger gewährleistet, abgewogen werden.

5. In Anbetracht der zunehmenden Bedeutung des Themas fand auf der informellen Tagung der Justizminister im Juli dieses Jahres eine politische Aussprache über Verschlüsselung statt. Dabei wurden die damit zusammenhängenden Probleme anerkannt und ein Mandat zur weiteren Prüfung erteilt. Es wurden unterschiedliche Standpunkte zur Vorgehensweise vorgebracht, die von der Beibehaltung des Status quo beim Schutz der Privatsphäre und bei den Unternehmensstandards bis hin zur Entwicklung wirksamerer Instrumente für die Strafverfolgungsbehörden und sogar bis hin zur Ausdehnung der Lösungen über die Strafjustiz hinaus auf andere Bereiche reichten.

Problemstellung

6. Aufgrund der Ergebnisse der politischen Diskussion hat der Vorsitz beschlossen, mittels eines Fragebogens noch detailliertere Informationen zusammenzustellen, um die aktuelle Lage aus der Sicht der Strafverfolgungsbehörden in den Mitgliedstaaten einzuschätzen und auf dieser Grundlage Optionen für weitere Schritte in Betracht ziehen.

7. Es gingen Antworten aus 25 Mitgliedstaaten und von Europol ein. Sie zeigen, dass sich die meisten Mitgliedstaaten über folgende Punkte einig sind:

   - Bei strafrechtlichen Ermittlungen stößt man häufig oder fast immer auf Verschlüsselung. (Nur fünf Delegationen erklärten, selten darauf zu stoßen).

   - Es wurden Erfahrungen sowohl mit online-Verschlüsselung (in Form verschlüsselter E-Mails oder anderer Formen elektronischer Kommunikation und/oder kommerzieller Anwendungen wie Facebook, Skype, WhatsApp oder Telegram) als auch mit offline-Verschlüsselung (am häufigsten bei strafrechtlichen Ermittlungen, in deren Zusammenhang verschlüsselte digitale Geräte und Verschlüsselungsanwendungen festgestellt wurden) gesammelt.

- Weder der Verdächtige noch der Beschuldigte, der im Besitz eines digitalen Geräts/elektronischer Daten ist, ist rechtlich verpflichtet, den Strafverfolgungsbehörden die Verschlüsselungscodes/Passwörter bereitzustellen, da sie zumeist nicht verpflichtet sind, sich selbst zu belasten. In einigen Mitgliedstaaten wurden jedoch unterschiedliche legislative Schritte unternommen, die derartige Möglichkeiten entweder gegenüber dem Verdächtigen und/oder Dritten zulassen.

- Diensteanbieter sind nach innerstaatlichem Recht verpflichtet, den Strafverfolgungsbehörden Verschlüsselungscodes/Passwörter zur Verfügung zu stellen; eine richterliche Anordnung ist nicht immer erforderlich. In den Antworten wird indes nicht unterschieden, ob diese Verpflichtung nur für die Anbieter elektronischer Kommunikationsdienste gilt oder sich auch auf die Anbieter von Diensten der Informationsgesellschaft erstreckt.

- Unter bestimmten, im innerstaatlichen Recht festgelegten Umständen dürfen verschlüsselte Datenströme überwacht werden, damit entschlüsselte Daten erlangt werden; häufig ist eine vorherige richterliche Anordnung erforderlich.

- Der nationale Rechtsrahmen zur Sicherung verschlüsselter elektronischer Beweismittel wird anders als die allgemeinen Rechtsvorschriften über elektronische Beweismittel als hinreichend wirksam betrachtet.

- Der Mangel an ausreichenden technischen Kapazitäten sowohl bei effizienten technischen Lösungen für die Entschlüsselung als auch bei der entsprechenden Ausrüstung stellt eine der drei größten Herausforderungen dar, gefolgt vom Mangel an ausreichenden Finanzmitteln und der Personalkapazität (sowohl quantitativ als auch hinsichtlich der Personalschulung).

- Die Notwendigkeit praktisch ausgerichteter Maßnahmen wurde als wichtiger erachtet als die Annahme neuer Rechtsvorschriften auf EU-Ebene (mit Ausnahme einer Delegation, die bei der Vorratsdatenspeicherung und der rechtmäßigen Überwachung neue EU-Bestimmungen für erforderlich hielt).

8. Bei jedem künftigen Schritt berücksichtigt werden sollten die politischen Rahmenbedingungen, die in den Schlussfolgerungen des Rates über die Verbesserung der Strafjustiz im Cyberspace und zum Europäischen Justiziellen Netz für Cyberkriminalität festgelegt wurden, die beide unter niederländischem Vorsitz im Juni vom JI-Rat angenommen wurden, sowie die darauf beruhenden laufenden Prozesse zu elektronischen Beweismitteln in Anbetracht der Verschlüsselung eines erheblichen Teils der elektronischen Daten, zur Schaffung eines Rahmens für die Zusammenarbeit mit Diensteanbietern aufgrund ihrer maßgeblichen Rolle und zur Verbesserung der Praxisarbeit der Richter und Staatsanwälte, die mit Cyberstraftaten/durch den Cyberspace ermöglichten Straftaten oder mit Ermittlungen im Cyberraum befasst sind, indem für sie ein spezielles Forum für den Austausch von Fachwissen zur Unterstützung der Wahrnehmung ihrer Aufgaben bereitgestellt wird.

Weiteres Vorgehen

9. In der Sitzung der horizontalen Gruppe "Fragen des Cyberraums" vom 28. Oktober 2016 hat der Vorsitz als möglichen künftigen Ansatz in der Frage der Verschlüsselung ein vierstufiges Vorgehen vorgestellt. Die Mitgliedstaaten begrüßten die Initiative des Vorsitzes und befürworteten im Großen und Ganzen die vorgeschlagenen Schritte. Sie sprachen sich dafür aus, im gegenwärtigen Stadium den Verschlüsselungsvorgang und den Expertenprozess in Bezug auf elektronische Beweismittel voneinander zu trennen, ohne auszuschließen, dass diese beiden Vorgänge in Zukunft koordiniert und möglicherweise aufeinander abgestimmt werden müssen und der Schwerpunkt auf politische und praktische Lösungen und weniger auf die Gesetzgebung gelegt werden muss. Die Delegationen würdigten die Verschlüsselung als Instrument zur Wahrung der Privatsphäre und der Cybersicherheit in der Gesellschaft. Sie betonten, dass nicht der Eindruck vermittelt werden darf, als solle die Verschlüsselung abgeschwächt werden. Die Sicherheit von Personen im Cyberspace sollte vielmehr durch eine ausgewogene Lösung sichergestellt werden, die sowohl die Wahrung der Menschenrechte als auch die Sicherheit des Einzelnen und der Gesellschaft garantiert. Sie unterstrichen die Bedeutung von Ausbildungsmaßnahmen und begrüßten die Initiative von Europol und ENISA, eine gemeinsame Arbeitsgruppe für Internetsicherheit einzusetzen, die Lösungen zur Bekämpfung des Missbrauchs der Verschlüsselung und Anonymität im Internet erörtern, bewerten und ausarbeiten soll.

10. Die anhand der Ergebnisse der ersten Beratungen der Gruppe "Fragen des Cyberraums" abgestimmte vierstufige Vorgehensweise wurde dem CATS am 18. November 2016 vorgestellt und fand breite Zustimmung. Die Mitgliedstaaten unterstrichen die Notwendigkeit, sowohl die technischen als auch die (straf)rechtlichen Aspekte zu behandeln und den Schwerpunkt der künftigen Beratungen auf praktische Lösungen zu legen, die die Arbeit der Strafverfolgungsbehörden erleichtern, ohne die Verschlüsselung als solche und den Schutz der Privatsphäre der Bürgerinnen und Bürger zu untergraben. Die Mitgliedstaaten betonten erneut, dass diesbezüglich ein angemessenes Gleichgewicht hergestellt werden muss. Sie stellten fest, dass die Kommission am besten in der Lage ist, den Reflexionsprozess anzuleiten und dafür Sorge zu tragen, dass die Verbindung zum Expertenprozess in Bezug auf elektronische Beweismittel bestehen bleibt und Überschneidungen vermieden werden und gleichzeitig die beiden Prozesse voneinander getrennt bleiben.

11. Bei den Beratungen brachten einige Delegationen konkret die Rolle von Diensteanbietern zur Sprache und schlugen vor, deren Verantwortlichkeiten und Pflichten genauer zu untersuchen. Andere Delegationen erinnerten an die Notwendigkeit, in Anbetracht der raschen technologischen Entwicklung vorausschauend zu handeln und die einschlägigen EU-Agenturen wie Europol und Eurojust in diesen Prozess eng einzubeziehen.

12. Das Europäische Justizielle Netz gegen Cyberkriminalität trat am 24. November 2016 zu seiner Auftaktveranstaltung zusammen, bei der auch technische und rechtliche Fragen im Zusammenhang mit der Verschlüsselung sowie die rechtlichen Hindernisse bei verdeckten Ermittlungen im Internet thematisiert wurden. Bei künftigen Treffen wird das Netz die Beratungen über diese Fragen voraussichtlich fortsetzen und sich über bewährte Verfahren und einschlägige nationale Rechtsvorschriften austauschen.

13. Daher wird der Rat ersucht,

– **eine Bilanz der bisherigen Fortschritte zu ziehen und**

– **die nachstehend unter den Buchstaben A bis D dargelegte vierstufige Vorgehensweise als Grundlage für die künftige Arbeit auf diesem Gebiet zu billigen:**

A. *Einleitung eines Reflexionsprozesses unter der Leitinitiative der Kommission über die Herausforderungen, die der Einsatz der Verschlüsselung für die Strafverfolgung mit sich bringt, mit dem Ziel, praktische Lösungen herauszuarbeiten, die mittels eines integrierten Ansatzes und Rahmens der EU die Offenlegung verschlüsselter Daten/Anlagen ermöglichen würde. Um Kohärenz zu gewährleisten und Doppelarbeit zu vermeiden, sollten bei diesem Reflexionsprozess die Fortschritte des laufenden Expertenprozesses in Bezug auf elektronische Beweismittel und des Prozesses zur Entwicklung eines gemeinsamen Rahmens für die Zusammenarbeit mit den Diensteanbietern zwecks Erlangung besonderer Kategorien von Daten berücksichtigt und gegebenenfalls die dabei erzielten Ergebnisse übernommen werden.*

B. *Sondierung der Möglichkeiten für eine Verbesserung der Fachkompetenz sowohl auf nationaler als auch auf EU-Ebene zur Bewältigung der aktuellen und künftigen Herausforderungen im Zusammenhang mit der Verschlüsselung, unter anderem durch eine Stärkung der bei Europol bereits vorhandenen technischen Fähigkeiten und die Förderung ihrer Nutzung durch die Mitgliedstaaten in den jeweiligen Grenzen ihres Mandats sowie durch die Weiterentwicklung von Europol zu einem Europäischen Kompetenzzentrum für Verschlüsselung. Die Unterstützung seitens anderer einschlägiger EU-Einrichtungen wie der ENISA könnte ebenfalls in Betracht gezogen werden.*

C. *Aufforderung der Mitglieder des Europäischen Justiziellen Netzes für Cyberkriminalität, in sein Forum für Beratungen, Informationsaustausch, bewährte Verfahren und Fachwissen auch die praktischen/operativen Aspekte im Zusammenhang mit der Verschlüsselung einzubeziehen. Eine enge Zusammenarbeit und Konsultationen mit Europol, Eurojust und dem Netz scheinen unverzichtbar, um den Herausforderungen im Zusammenhang mit der Verschlüsselung zu begegnen.*

D. *Vertiefung der praktischen/operativen Aspekte der von EU-Einrichtungen angebotenen Schulungen für die Strafverfolgungsbehörden auf dem Gebiet der Verschlüsselung und verstärkte Bemühungen um den Kapazitätsaufbau, um sicherzustellen, dass Fachkräfte über angemessene und aktuelle Kenntnisse und Fähigkeiten zur Erlangung elektronischer Beweismittel und den Umgang damit verfügen.*