Rat der
Europäischen Union

**Brüssel, den 18. September 2017**
**(OR. en)**

**9986/2/17**
**REV 2**

**GENVAL 63**
**CYBER 92**
**CATS 92**

**VERMERK**

| | |
|---|---|
| Absender: | Generalsekretariat des Rates |
| Empfänger: | Delegationen |
| Betr.: | Siebte Runde der gegenseitigen Begutachtungen "Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität"<br>- Entwurf des Abschlussberichts |

Im Einklang mit Artikel 2 der Gemeinsamen Maßnahme 97/827/JI vom 5. Dezember 1997[1] hatte die Gruppe "Allgemeine Angelegenheiten einschließlich Bewertung" (GENVAL) in ihrer Sitzung vom 3. Oktober 2013 beschlossen, dass die siebte Runde der gegenseitigen Begutachtungen die praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität zum Gegenstand haben soll.

Die Delegationen erhalten in der Anlage den Entwurf des Abschlussberichts über die siebte Runde der gegenseitigen Begutachtungen. Im vorliegenden Bericht werden die Schlussfolgerungen und Empfehlungen der bereits gebilligten Gutachten zu jedem einzelnen der Mitgliedstaaten zusammengefasst.

[1] Gemeinsame Maßnahme 97/827/JI vom 5. Dezember 1997 – vom Rat aufgrund des Artikels K.3 des Vertrags über die Europäische Union angenommen – betreffend die Schaffung eines Mechanismus für die Begutachtung der einzelstaatlichen Anwendung und Umsetzung der zur Bekämpfung der organisierten Kriminalität eingegangenen internationalen Verpflichtungen (ABl. L 344 vom 15.12.1997).

Der vom Generalsekretariat des Rates ausgearbeitete Entwurf des Abschlussberichts wurde der Gruppe "Allgemeine Angelegenheiten einschließlich Bewertung" (GENVAL) in ihrer Sitzung am 13. Juni 2017 im Hinblick auf einen ersten Gedankenaustausch vorgelegt.

Die Delegationen wurden gebeten, bis zum 3. Juli 2017 schriftliche Bemerkungen zu dem überarbeiteten Text einzusenden.
Eine überarbeitete Fassung des Berichts (s. Dok. 9986/1/17 REV 1) wurde der horizontale Gruppe "Fragen des Cyberraums" in ihrer Sitzung am 4. September 2017 vorgelegt.

Aufgrund der Bemerkungen einer Delegation wurde der Berichtsentwurf geringfügig überarbeitet (siehe Anlage - Änderungen auf den Seiten 22, 29, 42 und 64, durch Unterstreichung gekennzeichnet). Er wird in der nächsten Sitzung des CATS am 22. September 2017 zur Billigung vorgelegt werden, so dass er anschließend dem AStV und dem Rat zur Information über die Ergebnisse der Begutachtung übermittelt werden kann.

Gemäß Artikel 8 Absatz 4 der oben genannten Gemeinsamen Maßnahme wird der Abschlussbericht auch dem Europäischen Parlament zur Information übermittelt werden.

**ANLAGE**

# Abschlussbericht über die siebte Runde der gegenseitigen Begutachtung "Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität"

**INHALT**

## I – EINLEITUNG

Im Anschluss an die Annahme der Gemeinsamen Maßnahme 97/827/JI vom 5. Dezember 1997 betreffend die Schaffung eines Mechanismus für die Begutachtung der einzelstaatlichen Anwendung und Umsetzung der zur Bekämpfung der organisierten Kriminalität eingegangenen internationalen Verpflichtungen sollen mit diesem Bericht die Feststellungen und Empfehlungen zusammengefasst und Schlussfolgerungen in Bezug auf die siebte Runde der gegenseitigen Begutachtungen gezogen werden.

Im Einklang mit Artikel 2 der genannten Gemeinsamen Maßnahme hatte die Gruppe "Allgemeine Angelegenheiten einschließlich Bewertung" (GENVAL) in ihrer Sitzung vom 3. Oktober 2013 beschlossen, dass die siebte Runde der gegenseitigen Begutachtungen die praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität zum Gegenstand haben soll.

Die Wahl der Cyberkriminalität zum Thema der siebten Runde der gegenseitigen Begutachtungen wurde von den Mitgliedstaaten begrüßt. Aufgrund der Vielzahl unterschiedlicher Straftaten, die unter den Begriff Cyberkriminalität fallen, wurde allerdings vereinbart, dass sich die Begutachtung vor allem auf die Straftaten richten soll, denen die Mitgliedstaaten besondere Aufmerksamkeit widmen möchten. Daher war die Begutachtung auf die Bereiche Cyberangriffe, sexueller Missbrauch von Kindern bzw. Kinderpornografie im Internet und Online-Kartenbetrug ausgerichtet und ermöglichte eine umfassende Untersuchung der rechtlichen und praktischen Aspekte der Bekämpfung von Cyberkriminalität, der grenzübergreifenden Zusammenarbeit und der Zusammenarbeit mit den einschlägigen EU-Agenturen. Von besonderer Bedeutung sind in diesem Kontext die Richtlinie 2011/92/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie[2] (Umsetzungsfrist 18. Dezember 2013) und die

[2] ABl. L 335 vom 17.12.2011, S. 1.

Richtlinie 2013/40/EU über Angriffe auf Informationssysteme[3] (Umsetzungsfrist 4. September 2015).

[3] ABl. L 218 vom 14.8.2013, S. 8.

Der Fragebogen für die siebte Runde der gegenseitigen Begutachtungen wurde von der GENVAL-Gruppe am 27. November 2013 und am 22. Januar 2014 erörtert und anschließend im Wege des Verfahrens der stillschweigenden Zustimmung am 31. Januar 2014 angenommen. Die Reihenfolge der Besuche, vorbehaltlich einiger Anpassungen, und die Zusammensetzung der Gutachterausschüsse im Zusammenhang mit den Beobachtern wurden von der GENVAL-Gruppe am 1. April 2014 angenommen.

Gemäß Artikel 3 der Gemeinsamen Maßnahme 97/827/JI haben die Mitgliedstaaten entsprechend einem schriftlichen Ersuchen des Leiters des Referats DGD 2B des Generalsekretariats des Rates an die Delegationen vom 28. Januar 2014 Sachverständige mit umfangreichen praktischen Kenntnissen auf dem Gebiet benannt. An jeder Begutachtungsmission nahmen drei nationale Sachverständige teil. Weitere Sachverständige von Kommission, Eurojust, Europol und ENISA nahmen an einigen Begutachtungsmissionen als Beobachter teil. Das Generalsekretariat des Rates koordinierte die Missionen, nahm an ihnen mit einem oder zwei Bediensteten je Begutachtung teil, leistete die Vorarbeit für die Begutachtung und unterstützte die Sachverständigen.

Die erste Begutachtungsmission wurde vom 28. bis 31. Oktober 2014 in Frankreich durchgeführt. Die letzte Begutachtungsmission fand vom 27. bis 30. September 2016 in Schweden statt. Alle 28 Begutachtungsmissionen mündeten jeweils in ein ausführliches Gutachten über den betreffenden Mitgliedstaat. Diese Gutachten wurden anschließend von der GENVAL-Gruppe erörtert und gebilligt[4]. Die meisten Gutachten sind auf der Website des Rates verfügbar und öffentlich zugänglich.

[4] Frankreich (7588/2/15 REV 1 DCL 1); Niederlande (7587/15 DCL 1); Vereinigtes Königreich (10952/2/15 REV 2 DCL 1); Rumänien (13022/1/15 REV 1 DCL 1); Slowakei (9761/1/15 REV 1 DCL 1); Estland (10953/15 DCL 1); Slowenien (14586/1/16 REV 1 DCL 1); Italien (9955/1/16 REV 1 DCL 1); Spanien (6289/1/16 REV 1 DCL 1); Bulgarien (5156/1/16 REV 1 DCL 1); Litauen (6520/1/16 REV 1 DCL 1); Malta (7696/1/16 REV 1 DCL 1); Griechenland (14584/1/16 REV 1 DCL 1); Kroatien (5250/1/17 REV 1 DCL 1); Portugal (10905/1/16 REV 1 DCL 1); Zypern (9892/1/16 REV 1 DCL 1); Polen (14585/1/16 REV 1 DCL 1); Tschechische Republik (13203/1/16 REV 1 DCL 1); Ungarn (14583/1/16 REV 1 DCL 1); Lettland (5387/1/17 REV 1 DCL 1); Dänemark (13204/1/16 REV 1 DCL 1 + COR 1); Belgien (8212/1/17 REV 1); Österreich (8185/1/17 REV 1); Deutschland (7159/1/17 REV 1 DCL 1); Luxemburg (7162/1/17 REV 1 DCL 1); Irland (7160/1/17 REV 1 DCL 1); Finnland (8178/17); Schweden (8188/17 REV 1).

Im vorliegenden Dokument werden die Schlussfolgerungen und Empfehlungen der zuvor erstellten spezifischen Gutachten zu den einzelnen Mitgliedstaaten zusammengefasst[5]. Es sei jedoch darauf hingewiesen, dass die Einzelgutachten aufgrund der langen Dauer der Begutachtung gegebenenfalls nicht immer den aktuellen Stand der Dinge exakt widerspiegeln.

[5] Die Einzelgutachten wurden unmittelbar nach dem Besuch in den Mitgliedstaaten erstellt. Es kann vorkommen, dass danach Änderungen, wie z. B. der Abschluss der Umsetzung von Rechtsvorschriften, erfolgt sind, die in den Einzelgutachten noch nicht berücksichtigt sind. In dem Folgebericht zu den Gutachten, der 18 Monate nach Annahme der Gutachten vorzulegen ist, sollte den erfolgten Änderungen Rechnung getragen werden. Bei der Erörterung des Gutachtens in der GENVAL-Gruppe kündigten die Mitgliedstaaten oftmals (künftige) Änderungen an, um den Empfehlungen nachzukommen, die in ihrem Ländergutachten enthalten waren.

## II – ZUSAMMENFASSUNG

- Durch die zunehmende Nutzung des Internets ist Cyberkriminalität ein Kriminalitätsphänomen, das sich immer weiter ausbreitet; zudem gibt es neue Trends und Modi Operandi, und zwar sowohl bei der Cyberkriminalität im engeren Sinne ("stricto sensu"), die der rechtlichen Definition nach Straftaten erfasst, die mit der Nutzung eines Computersystems verbunden ist, als auch bei den durch den Cyberraum ermöglichten Straftaten, d. h. gewöhnliche Straftaten, die unter Einsatz der Informations- und Kommunikationstechnologie (IKT) begangen werden. Daher sind für Fortschritte bei der Bekämpfung der Cyberkriminalität in allen Ländern ein großer politischer Wille, Haushaltsanstrengungen und größere Investitionen in Humanressourcen und technische Ressourcen erforderlich.

- Die Begutachtung hat gezeigt, dass alle Mitgliedstaaten die Bekämpfung der Cyberkriminalität ernst nehmen und über diesbezügliche Strukturen, Ressourcen und Maßnahmen verfügen. Der Umfang des Engagements und die Effizienz sind von Mitgliedstaat zu Mitgliedstaat unterschiedlich, und in einigen Fällen gibt es noch Spielraum für Verbesserungen in Bezug auf bestimmte Aspekte des allgemeinen Ansatzes zur Bekämpfung der Cyberkriminalität. Gleichzeitig wurden einige allgemeine Probleme und Herausforderungen erkannt.

- Zum Zeitpunkt der Begutachtung hatte die Mehrheit der Mitgliedstaaten eine nationale Cybersicherheitsstrategie verabschiedet, die einen Rahmen für die Festlegung der nationalen Prioritäten sowie der zentralen Koordinierungsstrukturen auf strategischer und operativer Ebene im Hinblick auf die Bekämpfung der Cyberkriminalität sowie für die Sicherstellung der Widerstandsfähigkeit gegenüber Cyberangriffen bietet, während einige wenige Mitgliedstaaten noch im Begriff waren, dies zu tun. Einige Mitgliedstaaten hatten ferner einen Aktionsplan für die Umsetzung ihrer nationalen Cybersicherheitsstrategie angenommen.

- Zum Zeitpunkt der Begutachtung hatte die Mehrheit der Mitgliedstaaten das Übereinkommen des Europarats von 2001 über Computerkriminalität (Budapester Übereinkommen) und die meisten von ihnen auch das Zusatzprotokoll betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art unterzeichnet und ratifiziert. Diejenigen Mitgliedstaaten, die dies noch nicht getan haben, wurden aufgefordert, diese Instrumente zu unterzeichnen und zu ratifizieren.

- Einer der wichtigsten festgestellten Mängel betrifft die Erhebung gesonderter Statistiken zur Cyberkriminalität und Cybersicherheit, da die vorliegenden Statistiken unzureichend und fragmentiert sind und keinen Vergleich, sei es zwischen den verschiedenen Regionen innerhalb desselben Mitgliedstaats als auch zwischen den verschiedenen Mitgliedstaaten, ermöglichen. Verlässliche Statistiken sind erforderlich, um sich – im Hinblick auf das Ergreifen geeigneter Maßnahmen und die Bewertung der Wirksamkeit des Rechtsrahmens für die Bekämpfung der Cyberkriminalität – einen Überblick über die Trends und Entwicklungen dieser Form der Kriminalität zu verschaffen und diese zu überwachen und zu analysieren. Den Mitgliedstaaten wurde daher empfohlen, spezifische und umfassende Statistiken zur Cyberkriminalität in den verschiedenen Verfahrensstufen auf der Grundlage eines standardisierten Ansatzes zusammenzustellen.

- Aufgrund der raschen Weiterentwicklung der IKT mit immer ausgefeilteren Methoden und der Komplexität der Cyberkriminalität ist ein hoher Spezialisierungsgrad der in diesem Bereich tätigen Praktiker äußerst wichtig. Aus den Ergebnissen der Begutachtung geht hervor, dass der Spezialisierungsgrad bei den Strafverfolgungsbehörden im Allgemeinen zufriedenstellend oder ausreichend ist, während es bei der Justiz Spielraum für Verbesserungen gibt, da in einigen Mitgliedstaaten die allgemeinen Staatsanwaltschaften und allgemeine Strafgerichte mit Cyberkriminalität befasst sind. Daher wurde den Mitgliedstaaten empfohlen, den Spezialisierungsgrad ihres Justizpersonals, das mit Fällen von Cyberkriminalität befasst ist, zu verbessern.

- Aus den gleichen Gründen hat die Begutachtung deutlich gemacht, wie wichtig regelmäßige und kontinuierliche Fachschulungen zu Cyberkriminalität für die Strafverfolgungsbehörden und die Justiz sind, was unter anderem die optimale Nutzung der Schulungsmöglichkeiten einschließt, die von Stellen der EU (z. B. EC3/Europol, ECTEG, Eurojust, OLAF und CEPOL) entsprechend ihrem Mandat angeboten werden und/oder zu denen diese Stellen einen Beitrag leisten.

- Die Begutachtung hat gezeigt, dass eine enge und wirksame interinstitutionelle Koordinierung und Zusammenarbeit, die auf einem behördenübergreifenden Ansatz auf strategischer und operativer Ebene basiert, zwischen allen beteiligten öffentlichen und privaten Interessenträgern im Bereich Cyberkriminalität und Cybersicherheit ein Schlüsselelement für die effiziente Bekämpfung der Cyberkriminalität und für die Sicherstellung einer hohen Widerstandsfähigkeit der nationalen Cybersicherheitssysteme gegenüber Cyberbedrohungen darstellt. In einigen Mitgliedstaaten ist eine solche Zusammenarbeit jedoch noch nicht ausreichend entwickelt oder kann noch weiter verbessert werden.

- Zu diesem Zweck wurden die Mitgliedstaaten auch dazu angehalten, die etwaige Einrichtung einer zentralen Stelle/Einrichtung zur Koordinierung der Tätigkeiten in diesem Bereich zu erwägen, in der sowohl der öffentliche als auch der private Sektor vertreten sind.

- Eine enge Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor – Finanz- und Bankinstitute, Telekommunikationsunternehmen, Internetdiensteanbieter, NRO, Hochschulen, Unternehmen, Berufsverbände usw. – ist in diesem Zusammenhang von grundlegender Bedeutung, da ihr Fachwissen einen erheblichen Mehrwert für den Erfolg der Ermittlungen zu Cyberstraftaten und der Maßnahmen darstellt, die als Reaktion auf Cybervorfällen ergriffen werden. Die am weitesten fortgeschrittenen Formen der Zusammenarbeit mit dem privaten Sektor werden durch die Schaffung geeigneter Behörden/Arbeitsgruppen institutionalisiert. Öffentlich-private Partnerschaften wurden von den Gutachtern als wichtiges Instrument für eine gute Zusammenarbeit zwischen den Strafverfolgungsbehörden und dem privaten Sektor eingestuft.

- Einige Mitgliedstaaten haben direkte Kontakte zu Internetdiensteanbietern mit Sitz im Ausland, insbesondere in den USA, jedoch ist das Ergebnis von Ersuchen aufgrund der auf Freiwilligkeit beruhenden Zusammenarbeit wenig absehbar, weshalb es für die EU und ihre Mitgliedstaaten von Vorteil wäre, eindeutige Regeln dafür festzulegen, wie Strafverfolgungsbehörden bei ausländischen Internetdiensteanbietern Daten einholen können.

- In einigen Mitgliedstaaten ist es im Einklang mit den nationalen Rechtsvorschriften erlaubt, grundlegende Teilnehmerdaten direkt von ausländischen Diensteanbietern einzuholen, während in anderen Mitgliedstaaten Rechtshilfeverfahren durchgeführt werden müssen, die schneller und wirksamer sein sollten. Die Mitgliedstaaten wurden ersucht, dafür zu sorgen, dass ihre nationalen Rechtsvorschriften so flexibel sind, dass die Zulässigkeit von elektronischem Beweismaterial erleichtert wird, und zwar auch dann, wenn dieses aus einem anderen Land oder direkt von Diensteanbietern stammt.

- Der zunehmende Einsatz von Verschlüsselung mit immer komplexeren Methoden wird für die Strafverfolgungsbehörden und Nachrichtendienste in allen Mitgliedstaaten mehr und mehr zu einem Problem, da dadurch der Zugang zu einschlägigen Informationen betreffend Cyberkriminalität erschwert oder vollständig verhindert wird. Die Entschlüsselung ist – wenn überhaupt – nur durch den Einsatz hochleistungsfähiger Spezialhardware und -software möglich und die Begutachtung hat gezeigt, dass bei einer perfekten Verschlüsselung die Erfolgschancen sehr gering sind. Viele Mitgliedstaaten nutzen die Entschlüsselungsplattform von Europol, das "Europäische Zentrum zur Bekämpfung der Cyberkriminalität" (EC3). Nach den Feststellungen im Rahmen der Begutachtung könnten die durch Verschlüsselung entstehenden Herausforderungen teilweise dadurch bewältigt werden, dass Forschung und Entwicklung intensiviert und neue Methoden entwickelt werden, aber auch durch eine gute Zusammenarbeit zwischen den verschiedenen beteiligten Behörden. Den Mitgliedstaaten und den EU-Organen wird empfohlen, Lösungen zu prüfen und einen offenen Dialog mit dem Privatsektor zu intensivieren.

- Die Art des elektronischen Beweismaterials kann zu Problemen im Hinblick auf dessen Zulässigkeit führen, die bei anderen Arten von Beweismitteln nicht auftreten. Aus diesem Grund gibt es in einigen Mitgliedstaaten spezielle Vorschriften für die Erhebung von elektronischem Beweismaterial, um dessen Zulässigkeit vor Gericht sicherzustellen. Allerdings hat die Begutachtung gezeigt, dass in den meisten Mitgliedstaaten das Verfahrensrecht überwiegend technologieneutral ist, was bedeutet, dass die allgemeinen Vorschriften und Grundsätze zur Beweiserhebung angewandt werden und das Verfahrensrecht keine besonderen formellen Vorschriften für die Zulässigkeit und Beurteilung von elektronischem Beweismaterial enthält.

- Die Begutachtung hat ergeben, dass Cyberkriminalität im Zusammenhang mit in der "Cloud" gespeicherten Daten im Allgemeinen Probleme bei den Ermittlungen und der Strafverfolgung aufwirft, da die Informationen in der "Cloud" für die Strafverfolgungsbehörden nur schwer auffindbar und zugänglich sind. Je nach konkretem Fall kann elektronisches Beweismaterial der Gerichtsbarkeit eines oder mehrerer EU-Mitgliedstaaten, einschließlich zugleich einer Gerichtsbarkeit außerhalb der EU, zuzuordnen sein. Daher können Zuständigkeitskonflikte auftreten; in solchen Fällen können Eurojust und das EJN um Unterstützung ersucht werden. Die Begutachtung hat deutlich gemacht, wie wichtig es ist, dass diese Herausforderungen auf EU-Ebene und auf internationaler Ebene angegangen werden.

- Die Begutachtung hat die Bedenken der Mitgliedstaaten in Bezug auf das Fehlen eines gemeinsamen Rechtsrahmens zur Vorratsdatenspeicherung auf EU-Ebene bestätigt. Dies hat Auswirkungen auf die Wirksamkeit strafrechtlicher Ermittlungen und von Strafverfolgungsmaßnahmen, insbesondere bei der Erhebung elektronischer Kommunikationsdaten als Beweismittel in Gerichtsverfahren, sowie auf die grenzüberschreitende justizielle Zusammenarbeit. Die Begutachtung hat die Notwendigkeit eines gemeinsamen Ansatzes auf EU-Ebene herausgestellt. Im Rahmen gemeinsamer Überlegungen der Organe der EU und der Mitgliedstaaten wird derzeit die Frage der Vorratsdatenspeicherung angegangen, um rechtliche und praktische Lösungen für die Herausforderungen, die sich aus der Rechtsprechung des EuGH ergeben, zu finden.

- Sexueller Missbrauch von Kindern im Internet in seinen verschiedenen Formen hat in den letzten Jahren erheblich zugenommen. Im Hinblick auf eine wirksame Bekämpfung solcher Formen der Kriminalität wird ein breites Spektrum von Präventivmaßnahmen (u. a. Schulungsmaßnahmen und Aufklärungskampagnen zur Sensibilisierung) und Zwangsmaßnahmen (Sperren des Zugangs oder Entfernen illegaler Inhalte) unter Einbeziehung des öffentlichen und des privaten Sektors durchgeführt, wenn auch in den einzelnen Mitgliedstaaten in unterschiedlichem Ausmaß. Die Begutachtung hat ergeben, dass nur einige Mitgliedstaaten zur Bekämpfung des sexuellen Missbrauchs von Kindern eine spezielle nationale Datenbank für die Opferidentifizierung haben; den anderen Mitgliedstaaten, die nur die "International Child Sexual Exploitation Database" (ICSE-DB) von Interpol nutzen, wurde die Entwicklung einer solchen nationalen Datenbank empfohlen. Mehrere Mitgliedstaaten verfügen über Maßnahmen zur Verhinderung der erneuten Viktimisierung von Kindern, in einigen Fällen auch zum Schutz von Opfern und Zeugen sexuellen Missbrauchs von Kindern während des Strafverfahrens. Ferner wurde festgestellt, dass eine gute Zusammenarbeit zwischen allen einschlägigen Akteuren, insbesondere Strafverfolgungsbehörden, Meldestellen, NRO und Internetdiensteanbieter, ein wesentlicher Faktor für die Bekämpfung dieser Kriminalitätsformen ist.

- In Bezug auf die Cybersicherheit fällt den nationalen Computer-Notfallteams (CSIRT – Computer Security Incident Response Team), die die Mehrheit der Mitgliedstaaten bereits eingerichtet hat, eine entscheidende Rolle bei der Überwachung von Cybervorfällen und der Reaktion darauf zu. Darüber hinaus werden die Mitgliedstaaten in ihrem nationalen Recht die Verpflichtung für Betreiber wesentlicher Dienste verankern, Cybervorfälle mit erheblichen Auswirkungen auf die Verfügbarkeit wesentlicher Dienste unverzüglich den zuständigen Behörden oder dem CSIRT zu melden. Beide Aspekte sind in der NIS-Richtlinie vorgesehen und müssen bis zum 9. Mai 2018 umgesetzt werden.

- Da in Ermittlungen zu Cyberstraftaten im engeren Sinne sowie zu durch den Cyberraum ermöglichten Straftaten oftmals mehr als ein Mitgliedstaat einbezogen sind, sind die Zusammenarbeit und der Informationsaustausch mit und gegebenenfalls durch Einrichtungen der EU – Europol/EC3, Eurojust, EJN, EJCN und ENISA– eine Priorität. Aus dem gleichen Grund wurde ein verstärkter Einsatz gemeinsamer Ermittlungsgruppen (GEG) als wirksames Instrument für die Durchführung grenzüberschreitender Ermittlungen empfohlen.

- Das Internet kennt keine Grenzen und daher ist eine reibungslose und gut funktionierende internationale Zusammenarbeit für eine effiziente Bekämpfung der Cyberkriminalität von entscheidender Bedeutung. Wie die Begutachtung gezeigt hat, sind Rechtshilfeverfahren oftmals langwierig, zeitaufwändig und ineffizient, was sich negativ auf die Ermittlungen auswirkt, zumal elektronisches Beweismaterial aufgrund seiner Volatilität eine zügige Erlangung erfordert. Deshalb ist es notwendig, die Bearbeitung von Rechtshilfeersuchen bei Ermittlungen zu Cyberstraftaten zu beschleunigen. Außerdem wurden die Mitgliedstaaten dazu angehalten, u. a. die Instrumente von Eurojust, EJN und Europol häufiger zu nutzen und informelle Kontakte zu den zuständigen ausländischen Behörden im Hinblick auf schnellere Antworten auf Rechtshilfeersuchen aufzubauen.

## III – NATIONALE CYBERSICHERHEITSSTRATEGIE

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Zum Zeitpunkt der Begutachtung hatten die meisten Mitgliedstaaten eine nationale Cybersicherheitsstrategie und einige von ihnen auch einen Aktionsplan für dessen Umsetzung verabschiedet, während einige Mitgliedstaaten noch im Begriff waren, dies zu tun.

- Im Anschluss an die Entwicklung einer nationalen Cybersicherheitsstrategie und gegebenenfalls eines Aktionsplans ist es unerlässlich, für angemessene Folgemaßnahmen zu sorgen und die Umsetzung der nationalen Strategie eng zu überwachen.

- Aufgrund der raschen Entwicklung der Informations- und Kommunikationstechnologie (IKT) und neuer Arten den Cyberraum betreffender Straftaten müssen die zur wirksamen Bekämpfung der Cyberkriminalität eingesetzten Maßnahmen und Mittel ständig aktualisiert und muss die nationale Cybersicherheitsstrategie daher erforderlichenfalls zeitgerecht überprüft werden.

- Die Einsetzung einer einzigen Stelle mit Koordinierungsaufgaben für die Umsetzung der nationalen Cybersicherheitsstrategie, wie in einigen Mitgliedstaaten geschehen, kann als bewährtes Verfahren angesehen werden, das von anderen Mitgliedstaaten übernommen werden sollte.

- In der kürzlich verabschiedeten Richtlinie (EU) 2016/1148 (NIS-Richtlinie) ist die Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen vorgesehen, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll (Artikel 7).

**EMPFEHLUNGEN**

- ***Mitgliedstaaten, die noch keine nationale Cybersicherheitsstrategie verabschiedet haben, werden dazu angehalten, dies so rasch wie möglich nachzuholen und auch die Annahme eines Aktionsplans in Erwägung zu ziehen; diejenigen, die eine Strategie verabschiedet haben, sollten für ihre ordnungsgemäße Umsetzung sorgen und die mögliche Übertragung der Koordinierungsaufgaben an eine einzige Stelle/Einrichtung sicherstellen.***

- ***Die Mitgliedstaaten sollten ihre nationale Cybersicherheitsstrategie erforderlichenfalls im Einklang mit den einschlägigen Entwicklungen im IKT-Bereich sowie mit den Trends im Bereich der Cyberkriminalität aktualisieren.***

## IV – BUDAPESTER ÜBEREINKOMMEN

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Das Übereinkommen des Europarats von 2001 über Computerkriminalität (Budapester Übereinkommen) ist der erste und einzige internationale Vertrag für die Zwecke der Verfolgung einer gemeinsamen Strafrechtspolitik, die den Schutz der Gesellschaft vor Computerkriminalität zum Ziel hat, unter anderem durch die Annahme geeigneter Rechtsvorschriften und die Förderung der internationalen Zusammenarbeit.

- Das Budapester Übereinkommen regelt Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen, computerbezogene Fälschung, computerbezogenen Betrug, Straftaten mit Bezug zu Kinderpornographie und Urheberrechtsverletzungen.

- Ferner sieht es eine Reihe von Befugnissen und Verfahren wie die umgehende Sicherung und Weitergabe von Daten, die Anordnung der Herausgabe, the Durchsuchung von Computernetzen und die rechtmäßige Überwachung des Telekommunikationsverkehrs vor.

- Artikel 35 enthält Bestimmungen über die Einrichtung des internationalen 24/7-Netzwerks, das für unverzügliche Unterstützung für Zwecke der Ermittlungen oder Verfahren sorgt; hierdurch ist es möglich, Daten einzufrieren und somit elektronisches Beweismaterial zu bewahren. Letzteres stellt ein wichtiges Instrument dar, da hierdurch eine schnelle Möglichkeit für die Sicherung von elektronischem Beweismaterial vor der Übermittlung eines Rechtshilfeersuchens geschaffen wird.

- Das Budapester Übereinkommen wird durch ein Zusatzprotokoll betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art sowie im Hinblick auf den Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch durch das Übereinkommen von Lanzarote ergänzt.
- Zum Zeitpunkt der Begutachtung hatten die meisten Mitgliedstaaten diese Instrumente unterzeichnet und ratifiziert, während einige Mitgliedstaaten dies noch nicht getan hatten. In den Schlussfolgerungen des Rates zur Verbesserung der Strafjustiz im Cyberspace vom 9. Juni 2016 wurde die Aufforderung an die verbleibenden Mitgliedstaaten zur Ratifizierung und uneingeschränkten Umsetzung des Übereinkommens über Computerkriminalität vom 23. November 2001 bekräftigt.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten, die dies noch nicht getan haben, werden dazu angehalten, das Budapester Übereinkommen des Europarats von 2001 über Computerkriminalität sowie das Zusatzprotokoll zu unterzeichnen und zu ratifizieren und diese Instrumente uneingeschränkt umzusetzen.***

## V – STATISTIKEN

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Die Analyse der Rechtsvorschriften der EU belegt eindeutig, dass im Bereich der Cyberkriminalität Statistiken erhoben werden müssen. Gemäß Artikel 14 Absatz 1 der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme sorgen die Mitgliedstaaten dafür, dass ein System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Daten zu den Straftaten im Sinne der Artikel 3 bis 7 bereitsteht.

- Gemäß Artikel 14 Absatz 2 dieser Richtlinie umfassen die statistischen Daten gemäß Absatz 1 zumindest die vorhandenen Daten über die Anzahl der in den Mitgliedstaaten erfassten Straftaten im Sinne der Artikel 3 bis 7 und die Anzahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 7 strafrechtlich verfolgt und verurteilt wurden.

- Darüber hinaus wird den Mitgliedstaaten gemäß Erwägungsgrund 44 der Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie empfohlen, auf nationaler oder lokaler Ebene und in Zusammenarbeit mit der Zivilgesellschaft Mechanismen für die Datensammlung oder Anlaufstellen zu dem Zwecke einzurichten, das Phänomen des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern zu beobachten und zu bewerten.

- Außerdem ergibt sich die Notwendigkeit der Erhebung von Statistiken auf nationaler Ebene grundsätzlich aus den nationalen Rechtsvorschriften der Mitgliedstaaten.

- Statistiken zur Cyberkriminalität sind äußerst wichtig. Auf der einen Seite ermöglichen sie eine ausführliche Analyse und Kenntnis des Ausmaßes der sich abzeichnenden neuen Trends in dieser sich ausbreitenden Form der Kriminalität, so dass im Hinblick auf das Ergreifen geeigneter Maßnahmen ein realistischer Überblick über die Cyberkriminalität – es geht um die Dunkelziffer infolge nicht gemeldeter Straftaten – geboten und die Überwachung der Entwicklungen ermöglicht wird; auf der anderen Seite ermöglichen Statistiken, die Wirksamkeit des Rechtssystems und die Angemessenheit der Rechtsvorschriften bei der Bekämpfung der Cyberkriminalität und beim Schutz der Interessen der geschädigten Bürger zu bewerten.

- Umfassende Statistiken sollten alle Verfahrensstufen erfassen: Ermittlungen, Strafverfolgung, Gerichtsverfahren, die Art der Straftat und die konkrete Ermittlungsmaßnahme, die Anzahl der gemeldeten Straftaten, die Anzahl der geführten Ermittlungen und der Entscheidungen, zu bestimmten Arten von Cyberkriminalität keine Ermittlungen zu führen, die Anzahl der Geschädigten und Klagen der Geschädigten, die Anzahl der Personen, die wegen verschiedener Arten von Cyberkriminalität strafrechtlich verfolgt und verurteilt wurden, die Anzahl der grenzüberschreitenden Fälle, das Ergebnis von Rechtshilfeersuchen und die Dauer des Verfahrens.

- Einer der wichtigsten Mängel, die in der siebten Begutachtungsrunde in der Mehrheit der Mitgliedstaaten festgestellt wurden, betrifft die Erhebung separater Statistiken über Cyberkriminalität im engeren Sinne, über durch den Cyberraum ermöglichte Straftaten und über Cybersicherheitsvorfälle. Die verfügbaren Statistiken sind in den meisten Mitgliedstaaten unzureichend, fragmentiert und nicht vergleichbar.

- Darüber hinaus fehlt in vielen Mitgliedstaaten eine nationale Bestimmung der Begriffe Cyberkriminalität im engeren Sinne und durch den Cyberraum ermöglichte Straftaten, die zu zu statistischen Zwecken herangezogen werden könnte. In vielen Mitgliedstaaten lässt sich der Anteil der Cyberkriminalität an der Gesamtkriminalität nicht bestimmen, in anderen Mitgliedstaaten, die eine gesonderte Statistik zur Cyberkriminalität erheben, wird diese als ein einzelner Wert erstellt; folglich ist weder eine Unterteilung in Kategorien noch eine Unterscheidung zwischen den Fällen, die Cyberkriminalität im engeren Sinne und die durch den Cyberraum ermöglichten Straftaten betreffen, möglich. Nicht alle Mitgliedstaaten erstellen regelmäßig statistische Berichte zum Thema Cyberkriminalität.

- In den meisten Mitgliedstaaten werden justizielle Statistiken getrennt von den Statistiken der Strafverfolgungsbehörden geführt. Da sich die Statistiksysteme zwischen den zuständigen Behörden oft stark unterscheiden und jede Behörde Daten aus unterschiedlichen Quellen mit unterschiedlichen Methoden erhebt und nach unterschiedlichen Kriterien und/oder mit unterschiedlichen Datenbanken, bei denen keine Interoperabilität gegeben ist, verwaltet, kann die Cyberkriminalität nicht in einem einzigen Statistiksystem rückverfolgt werden.

- In vielen Mitgliedstaaten sind die Cyberkriminalitätszahlen, die in den jeweiligen statistischen Systemen erfasst werden, sehr niedrig. In solchen Fällen kann dies Fragen hinsichtlich der Effizienz der Aufdeckung, strafrechtlichen Verfolgung und Ahndung der Cyberkriminalität sowie der Genauigkeit der statistischen Aufzeichnungen aufwerfen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten, die Probleme im Zusammenhang mit einer fehlenden einheitlichen Begriffsbestimmung oder einem mangelnden einheitlichen Verständnis der Cyberkriminalität haben, werden dazu angehalten, eine kohärente nationale Begriffsbestimmung (oder ein kohärentes Verständnis) der Cyberkriminalität zu entwickeln, die (bzw. das) von allen beteiligten Akteuren bei der Bekämpfung der Cyberkriminalität und zur Erhebung von Statistiken anzuwenden ist.***

- ***Die Mitgliedstaaten werden ermutigt, spezifische und separate Statistiken zur Cyberkriminalität im engeren Sinne, zu den durch den Cyberraum ermöglichten Straftaten und zu Cybersicherheitsvorfällen zu erstellen, die sowohl über die Fallzahlen im Deliktbereich Cyberkriminalität informieren als auch den Anteil der Cyberkriminalität am gesamten Lagebild der Kriminalität benennen.***

- ***Die Mitgliedstaaten werden angehalten, einen standardisierten Ansatz zur Erhebung umfassender Statistiken in den verschiedenen strafrechtlichen Verfahrensstufen zu entwickeln, die nach spezifischen Bereichen der Cyberkriminalität, vorzugsweise entsprechend den auf EU-Ebene identifizierten Bereichen, d. h. sexueller Missbrauch von Kindern im Internet, Online-Kartenbetrug und Cyberangriffe, aufgeschlüsselt sind.***

- ***Die Mitgliedstaaten sollten Lösungen prüfen, die die Interoperabilität der verschiedenen Datenbanken, die Cyberkriminalitätsangaben enthalten, ermöglichen, damit rasch Straftäter identifiziert sowie Fälle quantifiziert und abgeglichen werden können.***

- ***Die Mitgliedstaaten sollten den Austausch statistischer Daten unter den verschiedenen nationalen Behörden, die mit der Bekämpfung der Cyberkriminalität befasst sind, erleichtern, insbesondere zwischen Strafverfolgungs- und Justizbehörden.***

## VI – STRUKTUREN – JUSTIZ

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Struktur und Organisation der Justiz variieren je nach Mitgliedstaat, was auch die Zuweisung der Zuständigkeit für Cyberkriminalitätsfälle betrifft.

- Da sich die IKT rasch fortentwickelt und Cyberkriminalität vielschichtig ist und immer komplizierter wird, hängen erfolgreiche Ermittlungen, die Strafverfolgung und eine Verurteilung in Cyberkriminalitätsfällen in hohem Maße davon ab, wie kompetent und erfahren die für die Ermittlungen und Gerichtsverfahren zuständigen Behörden sind. Ein hohes Verständnis- und Wissensniveau sowie eine Spezialisierung der Justiz in diesem Bereich sind daher von größter Bedeutung.

- Allerdings zeigen die Ergebnisse der gegenseitigen Begutachtung, dass Staatsanwälte und Richter, die mit Cyberkriminalität und damit verbundenen Straftaten befasst sind, nicht immer in zufriedenstellendem Maße spezialisiert sind und über Fachwissen verfügen..

- In einer erheblichen Anzahl von Mitgliedstaaten befassen sich die allgemeinen Staatsanwaltschaften mit Cyberkriminalität, und in keinem Mitgliedstaat gibt es besondere Gerichte oder Richter, die für Ermittlungen und Rechtsprechung in Cyberkriminalitätsfällen benannt wurden. Hingegen verfügen einige Mitgliedstaaten über besondere Staatsanwälte oder Strukturen innerhalb der Staatsanwaltschaften, die sich mit Straftaten im Bereich der Cyberkriminalität befassen. In einigen Mitgliedstaaten liegt die Zuständigkeit für derartige Straftaten in der Regel faktisch bei besonderen Staatsanwälten und Richtern, die im Bereich der Cyberkriminalität geschult wurden oder Erfahrung in diesem Bereich haben.

- In einigen Mitgliedstaaten gibt es nationale Netzwerke von Cyberstaatsanwälten, die auf Cyberkriminalität spezialisiert sind, was als bewährte Verfahrensweise angesehen werden kann, da sie den Austausch von Wissen und Erfahrung ermöglichen und die Verbreitung bewährter Verfahrensweisen unter Praktikern fördern.

- Die Gutachter hatten den Mitgliedstaaten empfohlen, mit der Unterstützung von Eurojust ein europäisches Netzwerk von Richtern, die auf die Bekämpfung der Cyberkriminalität spezialisiert sind, zu schaffen, um die justizielle Zusammenarbeit in diesem Bereich zu verbessern und zu fördern. In der Zwischenzeit wurde dieses Ziel erreicht, da im Juni 2016 das Europäische Justizielle Netz gegen Cyberkriminalität (EJCN), das bereits seine Arbeit aufgenommen hat, durch Schlussfolgerungen des Rates eingerichtet wurde.
  Die Sachkenntnisse und Erfahrungen, die in dem Netzwerk ausgetauscht werden, können dazu beitragen, den Spezialisierungsgrad der Justiz in den Mitglied zu erhöhen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten den Spezialisierungsgrad ihrer Justiz im Hinblick auf die effiziente Verfolgung und Ahndung von Cyberstraftaten im engeren Sinne und von durch den Cyberraum ermöglichten Straftaten erhöhen. Zu diesem Zweck sollten sie erwägen, besondere Stellen oder interne Strukturen/Einheiten einzurichten und/oder besondere Staatsanwälte und Richter mit guten Kenntnissen und großem Wissen über Cyberkriminalität für die Bearbeitung solcher Fälle zu benennen.***

- ***Die Mitgliedstaaten sollten erwägen, auf nationaler Ebene Netzwerke von auf Cyberkriminalität spezialisierten Staatsanwälten und Richtern als zusätzliches Instrument einzurichten, um diese Kriminalitätsform wirksamer bekämpfen zu können.***

## VII – STRUKTUREN – STRAFVERFOLGUNGSBEHÖRDEN

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Die Struktur und die Organisation der Strafverfolgungsbehörden variieren in den verschiedenen Mitgliedstaaten erheblich, was auch die Zuweisung der Zuständigkeit für Cyberkriminalität betrifft. In einigen Mitgliedstaaten arbeiten besondere Organisationseinheiten auf der Grundlage eines zweiteiligen Ansatzes, der die strategische Planung und die operativen Tätigkeiten beinhaltet, während diese Funktionen in anderen Mitgliedstaaten von verschiedenen Behörden und Stellen getrennt wahrgenommen werden.

- Effiziente Organisation, internationale Integration und professionelle Kompetenz der Strafverfolgungsbehörden, die Ermittlungen im Zusammenhang mit Cyberstraftaten führen, sind wichtige Faktoren für die wirksame Bekämpfung dieser Kriminalitätsform. Ein hohes Maß an Wissen und Spezialisierung der Strafverfolgungsbehörden ist aus den gleichen Gründen wie bei der Justiz ebenfalls von entscheidender Bedeutung, damit wirksam gegen diese vielschichtige und komplizierte Kriminalitätsform vorgegangen werden kann.

- Die gegenseitige Begutachtung ergab allgemein, dass die Strafverfolgungsbehörden in höherem Maße spezialisiert sind als die Justiz, ihre Spezialisierung aber in vielen Fällen noch verbessert werden kann.

- In den meisten Mitgliedstaaten gibt es besondere zentrale Strukturen oder Organisationseinheiten für Cyberkriminalität im Innenministerium und/oder bei der Polizei, die für die Prävention und Bekämpfung der Cyberkriminalität auf nationaler Ebene zuständig sind, sodass die Koordinierung der Ermittlungen zu Cyberkriminalität im ganzen Land mit einem hohen Spezialisierungsgrad in diesem Bereich sichergestellt wird. Dies erleichtert auch die Kommunikation zwischen der Polizei und den Staatsanwälten. In mehreren Mitgliedstaaten gibt es ferner dezentralisierte besondere Organisationseinheiten auf lokaler und/oder regionaler Ebene, die speziell in Fällen von Cyberkriminalität ermitteln.

- Einigen Mitgliedstaaten wurde empfohlen, die Polizei umzustrukturieren und einschlägige Maßnahmen zu ergreifen, um die Humanressourcen zu verstärken und eine effektive, intensive Schulung der Polizei und ausreichende technische Ausstattung zur Bekämpfung der Cyberkriminalität bereitzustellen. Außerdem müssen die Ausstattung und die Ressourcen der Strafverfolgungsbehörden ständig aktualisiert werden, um der ständigen Weiterentwicklung und Diversifizierung der Modi Operandi im Bereich der Cyberkriminalität Rechnung zu tragen.

- Die wichtigsten Hindernisse für erfolgreiche Ermittlungen zu Cyberstraftaten sind unter anderem die rasche Entwicklung der Technologie und die neuen und komplexen Modi Operandi, die zunehmende Professionalität und Erfahrung der Cyberstraftäter, die Tatsache, dass Cyberkriminalität leicht die gerichtliche Zuständigkeit mehrerer Länder betreffen kann, die Schwierigkeiten dabei, Zugang zu elektronischem Beweismaterial in Bezug auf Cyberkriminalität zu erhalten, und die Herausforderungen im Zusammenhang mit dem Einsatz von Verschlüsselung, TOR und Anonymisierung.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten den Spezialisierungsgrad der Strafverfolgungsbehörden, die mit Cyberstraftaten befasst sind, aufrechterhalten und gegebenenfalls verbessern. Mitgliedstaaten, die dies noch nicht getan haben, sollten die Einrichtung von Fachdienststellen bei den Strafverfolgungsbehörden erwägen, um Cyberkriminalität auch auf regionaler/lokaler Ebene wirksamer zu bekämpfen.***

- ***Die Mitgliedstaaten sollten die Schaffung eines Netzes von auf Cyberkriminalität spezialisierten Polizeibeamten auf nationaler Ebene in Erwägung ziehen, das dazu beitragen könnte, einen Kommunikationskanal zwischen dem öffentlichen und dem privaten Sektor und der Polizei herzustellen.***

- ***Die Mitgliedstaaten sollten die Stärkung des nichttechnischen Polizeipersonals in den Bezirks- oder Regionalstrukturen sowie die Gewährleistung einer ausreichenden technischen Ausstattung, die ihren Anforderungen entspricht, erwägen.***

## VIII – ZUSAMMENARBEIT UND KOORDINIERUNG AUF NATIONALER EBENE

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Da die Cyberkriminalität einen bereichsübergreifenden Charakter hat und die Verantwortung für die Sicherheit des Cyberraums auf nationaler Ebene in der Regel zwischen verschiedenen Akteuren mit unterschiedlichen Zuständigkeiten und Fähigkeiten, ob öffentlich oder privat, militärisch oder zivil, kollektiv oder einzeln, geteilt wird, ist ein multidisziplinärer Ansatz von zentraler Bedeutung für die wirksame Prävention und Bekämpfung der Cyberkriminalität und die Gewährleistung der Widerstandsfähigkeit gegenüber Cyberangriffen.

- In diesem Zusammenhang ist eine enge und wirksame interinstitutionelle Koordinierung und Zusammenarbeit zwischen den verschiedenen Behörden und öffentlichen Stellen auf operativer und strategischer Ebene sowie zwischen den zentralen und lokalen/regionalen Behörden im Hinblick auf die Koordinierung von Initiativen und die Intensivierung des Datenaustausches, der technischen Unterstützung und der Ermittlungsmethoden von wesentlicher Bedeutung.

- Eine Zusammenarbeit zwischen Polizei, Staatsanwaltschaften und nationalen Nachrichtendiensten bei der Bekämpfung der Cyberkriminalität kann – unter Wahrung einer strikten Trennung der Aufgaben und Befugnisse dieser Organe, die in bestimmten Mitgliedstaaten vorgeschrieben ist – auch von Nutzen sein, um Unterstützung in technischer Hinsicht (Überwachung des Telekommunikationsverkehrs, Know-how usw.) oder Erkenntnisse für die strafrechtlichen Ermittlungen und die Strafverfolgung, insbesondere für die Erhebung und Verarbeitung von elektronischem Beweismaterial, zu erhalten.

- Die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor ist ebenfalls entscheidend für erfolgreiche Ermittlungen, Strafverfolgung und Verurteilung bei Cyberkriminalität im engeren Sinne und durch den Cyberraum ermöglichten Straftaten sowie für die Reaktion auf Cyberbedrohungen und -angriffe (weitere Einzelheiten siehe folgendes Kapitel).

- Zusammen mit dem Rechtsrahmen für die Zusammenarbeit zwischen den Behörden, sofern festgelegt, bilden in der Regel die nationale Cybersicherheitsstrategie und – soweit vorhanden – der Aktionsplan für ihre Umsetzung den allgemeinen Rahmen für die Koordinierung und Zusammenarbeit zwischen allen öffentlichen Einrichtungen und Behörden mit Zuständigkeit im Bereich der Cybersicherheit sowie mit dem privaten Sektor, um die Abgrenzung der Aufgaben und Zuständigkeiten sicherzustellen.

- Die ordnungsgemäße Umsetzung der nationalen Cybersicherheitsstrategie ist daher ein wesentlicher Faktor für Synergien und für die Maximierung der Bereitschaft und Reaktionsfähigkeit bei der Bekämpfung der Cyberkriminalität und der Stärkung der Cybersicherheit.

- Aus der Begutachtung geht hervor, dass die Formen, Modalitäten und Ebenen der Zusammenarbeit und Koordinierung zwischen den einschlägigen Akteuren, die mit der Bekämpfung der Cyberkriminalität und der Gewährleistung der Cybersicherheit befasst sind, in den verschiedenen Mitgliedstaaten unterschiedlich sind. In einigen Mitgliedstaaten gibt es keinen rechtlichen Rahmen für die Zusammenarbeit zwischen den Behörden in Fällen von Cyberkriminalität und die Behörden, die mit Ermittlungen zur Cyberkriminalität und ihrer strafrechtlichen Verfolgung befasst sind, arbeiten informell zusammen. Einige Mitgliedstaaten haben fortschrittlichere und effizientere Formen der Interaktion entwickelt, die in den Einzelgutachten als bewährte Verfahrensweisen aufgeführt wurden.

- Der beste Weg, um das einwandfreie Funktionieren des Systems sicherzustellen, ist ein strukturierter Mechanismus, und zwar insbesondere wenn die Koordinierungsaufgaben für Fragen der Cybersicherheit und für die Strategien zur Bekämpfung der Cyberkriminalität einer einzigen institutionellen Behörde (z. B. Ministerien oder Dienststellen in ihrer Organisationsstruktur) oder einer einzigen "Ad hoc"-Stelle oder -Einrichtung zugewiesen wurden. Eine solche einzige Institution/Einrichtung, die einen institutionellen Rahmen für die Zusammenarbeit bereitstellt, in dem sowohl öffentliche als auch private mit der Bekämpfung von Cyberkriminalität und der Gewährleistung der Cybersicherheit befasste Akteure vertreten sind, besteht in einigen Mitgliedstaaten bereits und wurde in anderen Mitgliedstaaten zum Zeitpunkt der Begutachtung in Erwägung gezogen.

- Einige Mitgliedstaaten, in denen Unzulänglichkeiten im Rahmen der gegenseitigen Begutachtung festgestellt wurden, unternehmen Anstrengungen zur Stärkung der bestehenden Strukturen und Verfahren für die Zusammenarbeit und Koordinierung, um die Prävention und Bekämpfung der Cyberkriminalität wirksamer zu gestalten.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten der institutionellen Koordinierung und Zusammenarbeit zwischen allen einschlägigen Akteuren bei der Prävention und der Bekämpfung der Cyberkriminalität und der Gewährleistung der Cybersicherheit auf der Grundlage eines multidisziplinären Ansatzes Vorrang einräumen, um Synergien sowie Bereitschaft und Reaktionsfähigkeit zu optimieren.***

- ***Zu diesem Zweck werden die Mitgliedstaaten insbesondere dazu angehalten, einen strukturierten Rahmen für die Zusammenarbeit einzuführen oder zu stärken und unter Umständen eine zentrale Stelle/Einrichtung oder Plattform zu schaffen, in der sowohl der öffentliche als auch der private Sektor vertreten sind und die Koordinierungsaufgaben wahrnimmt und befugt ist, Lösungen für festgestellte Probleme vorzuschlagen.***

## IX – ZUSAMMENARBEIT ZWISCHEN DEM ÖFFENTLICHEN UND DEM PRIVATEN SEKTOR

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Eine enge Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor ist von wesentlicher Bedeutung, da die Bekämpfung der Cyberkriminalität sehr komplex ist, was bedeutet, dass die Strafverfolgungsbehörden diese Form der Kriminalität nur unter Mitwirkung des privaten Sektors (Finanz- und Bankinstitute, Telekommunikationsunternehmen, Internetdiensteanbieter, NRO, Hochschulen, Unternehmen, Berufsverbände usw.) erfolgreich bekämpfen können.

- Von einer solchen Zusammenarbeit könnten beide Sektoren profitieren, weil dadurch die Möglichkeit geschaffen wird, ein breites Spektrum von kooperierenden Organisationen einzubinden und Synergien zwischen ihnen sicherzustellen, was zur Erhöhung des Cybersicherheitsniveaus beiträgt.

- Der Beitrag der privaten Akteure im Hinblick auf Fachkenntnisse, technische Unterstützung und Austausch von Informationen über Cyberbedrohungen und Trends im Bereich der Cybersicherheit ist sehr wertvoll für den Erfolg der Ermittlungen und der Maßnahmen zur Bewältigung von Cybervorfällen. Ferner ist es sinnvoll, Staatsanwälte in Kontakte mit dem privaten Sektor einzubinden, um sicherzustellen, dass Beweismittel im Einklang mit den geltenden Rechtsvorschriften erhoben werden und in Gerichtsverfahren zulässig sind.

- Nach den Ergebnissen der Begutachtung variiert der Umfang der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor in den einzelnen Mitgliedstaaten; im Allgemeinen ist die Zusammenarbeit besser entwickelt und effizienter, wenn sie stärker strukturiert ist und in einem von Vertrauen gekennzeichneten Umfeld stattfindet. In einigen Mitgliedstaaten wurden im Rahmen der Begutachtung bewährte Verfahrensweisen festgestellt, während hervorgehoben wurde, dass die Zusammenarbeit in anderen Mitgliedstaaten verbessert werden muss.

- In einigen Mitgliedstaaten ist der Rückgriff auf öffentlich-private Partnerschaften in der nationalen Cybersicherheitsstrategie vorgesehen, wobei dies allerdings in einigen Fällen auf bestimmte Bereiche beschränkt ist. Grundlage können Vereinbarungen (MoU) oder vergleichbare informelle Übereinkünfte sein.

- Nicht alle Mitgliedstaaten haben jedoch einen förmlichen Rahmen für öffentlich-private Partnerschaften ausgearbeitet und in einigen Mitgliedstaaten finden Zusammenarbeit, Sitzungen und Austausch von Informationen über Vorfälle, Trends und Entwicklungen mit dem privaten Sektor auf informeller und nicht auf einer gesetzlichen Grundlage statt.

- Die am weitesten fortgeschrittenen Formen der Zusammenarbeit mit dem privaten Sektor wurden in den Mitgliedstaaten festgestellt, in denen eine solche Zusammenarbeit durch die Schaffung angemessener Einrichtungen/Arbeitsgruppen für die Zusammenarbeit zwischen dem privaten Sektor und der öffentlichen Verwaltung bzw. den Strafverfolgungsbehörden institutionalisiert ist.

- Im Rahmen der Begutachtung haben die Gutachter festgestellt, dass öffentlich-private Partnerschaften ein wichtiges Instrument für eine gute Zusammenarbeit zwischen den Strafverfolgungsbehörden und dem privaten Sektor, insbesondere mit Internetdiensteanbietern und dem Finanzsektor, vor allem Banken, aber auch mit NRO, den CSIRT und den Betreibern kritischer Infrastrukturen, sind. Für die Entfernung illegaler Inhalte, die Entschlüsselung, die Abwehr von Cyber-Angriffen usw. kann dies von Nutzen sein.

- Die Zusammenarbeit mit Diensteanbietern ist besonders hilfreich, sowohl um von ihrer Sachkenntnis zu profitieren als auch im Hinblick auf den Zugang zu grundlegenden Teilnehmerinformationen. Durch die Durchführung von Risikobewertungen, das Ergreifen geeigneter Sicherheitsmaßnahmen und die Anwendung eines strukturierten Sicherheitskonzepts können die Anbieter elektronischer Kommunikationsnetze und -dienste nicht nur das Auftreten bestimmter Formen von Cyberkriminalität verhindern, sondern auch die Strafverfolgungsbehörden mit der Bereitstellung von Beweisen unterstützen.

- Nach den Ergebnissen der Begutachtung ist es notwendig, Lösungen für einen klaren und angemessenen Rahmen zur Regelung der Beziehungen der Justizbehörden mit Internetdiensteanbietern in der gesamten EU zu finden. Zu diesem Zweck könnten Verfahren, die es den Behörden ermöglichen, zügig Antworten auf ihre Anfragen zu erhalten, und die Einrichtung eines Systems von Sanktionen bei Nichteinhaltung/mangelnder Zusammenarbeit/Versäumnis ( Geldbußen oder Geldstrafen) eine solche Zusammenarbeit verbessern.

- Ein Dialog mit den wichtigsten Internetbetreibern, Hostingunternehmen und Internetzugangs- und -diensteanbietern in der EU und auf internationaler Ebene könnte ihre Zusammenarbeit im Rahmen strafrechtlicher Ermittlungen verbessern.

- Die wirksame Zusammenarbeit zwischen den Strafverfolgungsbehörden einerseits und den Finanzinstituten und Geschäftsbanken andererseits ist ebenfalls von grundlegender Bedeutung bei der Bekämpfung von Card-present-Betrug und sonstigen Formen des Betrugs im Internet, damit diese Arten von Betrug erkannt, der private Sektor über neue Trends aufgeklärt und Vorsichtsmaßnahmen aufgezeigt werden.

- In einigen Mitgliedstaaten wird eine solche Zusammenarbeit durch spezielle Bankenverbände oder bankenübergreifende Ausschüsse, die für die Bekämpfung von Betrug in Zahlungssystemen und mit Zahlungsmitteln eingerichtet wurden und zu regelmäßigen Sitzungen unter Beteiligung der Polizei zusammentreten, unterstützt. In einem Mitgliedstaat wurde die Einbindung der Polizei in den beratenden Ausschuss des nationalen Bankenverbands von den Gutachtern als bewährte Verfahrensweise eingestuft.

- In anderen Mitgliedstaaten ist die Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Banken und Finanzinstituten wenig strukturiert und auf Kontakte und/oder Sitzungen beschränkt, mit denen die Zusammenarbeit und der Austausch von Informationen über Fragen im Zusammenhang mit Cyberkriminalität sichergestellt werden soll.

- In einigen Mitgliedstaaten besteht für den privaten Sektor eine Meldepflicht bei Cyberkriminalität, während in anderen Mitgliedstaaten eine solche Meldung nicht obligatorisch ist oder nur bestimmte Teile des privaten Sektors oder eine bestimmte Art von Cyberstraftaten betrifft.

- In einigen Fällen erfolgt die Meldung von Cyberstraftaten auf freiwilliger Basis. Allerdings ergab die Begutachtung, dass in einigen Mitgliedstaaten die Finanz- und Kreditinstitute und Internetdiensteanbieter zögern, derartige Straftaten zu melden und strafrechtliche Verfahren mit dem Ziel der Feststellung der strafrechtlichen Verantwortung des Täters zu unterstützen. Sie sind mehr an der schnellstmöglichen Beseitigung des Schadens interessiert, der aus der Veröffentlichung und Berichterstattung in den Medien, die sich auf ihre Glaubwürdigkeit und ihr Ansehen negativ auswirkt, resultieren könnte.

- Einigen Ländergutachten zufolge ist in Fällen, in denen der private Sektor Opfer oder Geschädigter ist, die Zusammenarbeit mit den Strafverfolgungsbehörden in der Regel gut, da der Sektor die Sicherung von Beweisen, ihre Auslegung und ihre Übergabe an die Strafverfolgungsbehörden vornimmt.

- Der private Sektor spielt auch eine wichtige Rolle beim Kinderschutz sowie bei Präventions- und Aufklärungsmaßnahmen in diesem Bereich; private Verbände und NRO, die in diesem Bereich tätig sind, arbeiten mit den Strafverfolgungsbehörden bei der Bekämpfung der sexuellen Ausbeutung im Internet zusammen und leisten durch die Steuerung von Meldungen über Missbrauch einen wichtigen Beitrag.

- Den Schlussfolgerungen der Begutachtung zufolge würde ein Dialog mit dem privaten Sektor über die verbindlichen Berichterstattungsanforderungen hinaus auf jeden Fall bessere Ergebnisse bei der Bekämpfung von Cyberstraftaten ermöglichen.

- Die Behörden sollten zudem, wie es in mehreren Mitgliedstaaten der Fall ist, mit Hochschulen, Bildungseinrichtungen, sozialen Diensten, Unternehmen, Berufsverbänden, Medien und sonstigen Organisationen und Unternehmen zusammenarbeiten, um den negativen Auswirkungen der Computerkriminalität im engeren Sinne und der durch den Cyberraum ermöglichten Kriminalität auf die Informationssicherheit im Land vorzubeugen und sie auszugleichen. Besonders die Zusammenarbeit mit Hochschulen ist für Sensibilisierung, Ausbildung und Forschung und Entwicklung (F&E) sehr wichtig.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten und die EU-Organe sollten weitere Überlegungen über Methoden anstellen, die eine Aufrechterhaltung und Ausweitung der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor (Banken, Telekommunikationsunternehmen und Diensteanbieter), auch unter Einbeziehung von Staatsanwälten und möglicherweise Richtern, ermöglichen.***

- ***Die Mitgliedstaaten sollten strukturierte öffentlich-private Partnerschaften im Hinblick auf die Gewährleistung eines klaren Rahmens für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor mit eindeutigen Regeln und Pflichten nutzen, wobei möglicherweise zwischen Präventivmaßnahmen zum einen und Ermittlungs- und Strafverfolgungstätigkeiten zum anderen zu unterscheiden wäre.***

- ***Die Mitgliedstaaten sollten den privaten Sektor dazu anhalten, Informationen mit den Behörden auszutauschen und gegebenenfalls in den nationalen Rechtsvorschriften eine für den privaten Sektor geltende Meldepflicht für Cybervorfälle vorzusehen, die insbesondere Kreditinstitute und andere kritische Infrastrukturen zur unverzüglichen Meldung der gegen sie selbst und/oder gegen ihre Kunden gerichteten Cybervorfälle verpflichten würde.***

- ***Die Europäische Union und ihre Mitgliedstaaten sollten darüber nachdenken, wie die Zusammenarbeit zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und Diensteanbietern verbessert werden könnte, was auch die Möglichkeit einschließt, dass die EU Vereinbarungen mit einigen von ihnen schließt, um die Zusammenarbeit bei strafrechtlichen Ermittlungen zu erleichtern.***

## X – ERMITTLUNGSMETHODEN

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Angesichts der großen Bandbreite von Cyberstraftaten kann es keine allgemein erprobten und bewährten Verfahren oder Methoden für die Ermittlungen zu solchen Straftaten geben. Alle Ermittlungen und Ansätze hängen von den konkreten Umständen ab, und die Ermittlungsverfahren und -methoden müssen sich am konkreten Fall orientieren.

- Insbesondere im Bereich der Cyberkriminalität ändern sich die Modi Operandi, die Software und die Instrumente, die angewandt werden, ständig und in kurzen Abständen. Die Ermittlungstechniken müssen daher ständig im Einklang mit den Entwicklungen der Cyberkriminalität aktualisiert werden (z. B. mit spezieller Ermittlungs-Computersoftware).

- Neben allgemeinen Ermittlungsmethoden werden zur Aufklärung von Cyberstraftaten auch besondere Ermittlungsmethoden eingesetzt. Es gibt eine Reihe von Möglichkeiten: Die am häufigsten angewandten besonderen Ermittlungsmethoden, die insbesondere bei der Bearbeitung von Fällen der sexuellen Ausbeutung von Kindern besonders wirksam sind, sind die Überwachung des Telekommunikationsverkehrs, die Sicherung von Daten und verdeckte Ermittlungen.
  Bei letzteren, die vor allem dann hilfreich sind, wenn die Ermittlungen nicht unter Einsatz technischer Mittel geführt werden können, wird verdeckt in Foren und Boards ermittelt. Allerdings sind derartige Ermittlungen nur dann erfolgversprechend, wenn sie langfristig angelegt sind.

- Andere besondere Ermittlungsmethoden basieren auf neuen technischen Möglichkeiten für die Online-Bekämpfung von Computerkriminalität, z. B. Online-Überwachung oder andere Methoden wie Hardware-Zugangssperren und spezielle Bitkopierer, Durchsuchung und Beschlagnahme per Fernzugriff (z. B. wenn eine Strafverfolgungsbehörde sich einen direkten Zugang zu einem verdächtigen Computer verschafft, anstatt sich diesen zu beschaffen), IP-Rückverfolgung, Open-Source-Recherchen im Internet, Sicherung von Daten von Datenträgern und aus dem Internet (Webseiten, Log-Dateien). Besondere Methoden werden auch bei mobilen Geräten angewandt (z. B. UFED).

- Allerdings ist die Anwendung besonderer Ermittlungsmethoden nicht immer in den nationalen Rechtsvorschriften der Mitgliedstaaten vorgesehen. In einigen Mitgliedstaaten ist dafür eine richterliche Anordnung erforderlich.

**EMPFEHLUNGEN**

- ***Diejenigen Mitgliedstaaten, die dies noch nicht getan haben, werden dazu angehalten, in ihren nationalen Rechtsvorschriften die Möglichkeit der Anwendung besonderer Ermittlungsmethoden vorzusehen, um Ermittlungen in Fällen von Cyberkriminalität zu erleichtern.***

## XI – VERSCHLÜSSELUNG

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Durch die zunehmende Verfügbarkeit und Nutzung von sicheren und vertrauenswürdigen Verschlüsselungstechnologien werden die Sicherheit, die sichere Übermittlung und Vertraulichkeit von Computerdaten und folglich der Schutz der Privatsphäre der Bürgerinnen und Bürger und der wirksame Datenschutz im Cyberraum gewährleistet.

- Jedoch wird es aufgrund der zunehmenden Verwendung der Verschlüsselung – sowohl bei der Datenspeicherung als auch bei der Kommunikation über das Internet – mit immer differenzierteren Methoden zusehends schwieriger oder fast unmöglich, die Verschlüsselung zu überwinden, was in allen Mitgliedstaaten immer mehr zu einem Problem wird.

- Die Verschlüsselung wird oftmals von Straftätern eingesetzt, um rechtswidriges Material, das in ihrem Besitz ist, sowie ihre Kommunikation zu schützen, und erschwert die Ermittlungen zu Cyberkriminalität. Da die Verschlüsselung bei vielen Anwendungen standardmäßig vorgesehen ist, stellt die Erlangung von Beweismaterial, das in verschlüsselter Form vorliegt, die Strafverfolgungsbehörden oftmals vor Probleme.

- Durch die Verschlüsselung wird der Zugang zu relevanten Informationen in Bezug Cyberkriminalität – insbesondere zur Identifizierung von Kommunikations- oder Computerdaten im Besitz von Tatverdächtigen oder Straftätern – nicht nur bei kriminaltechnischen Untersuchungen, sondern auch bei allen anderen Arten von Ermittlungen erschwert oder sogar vollständig verhindert. Darüber hinaus gestaltet sich das Abfangen oder die Auslegung von Material aufgrund der Verwendung einer Ende-zu-Ende-Verschlüsselung durch eine zunehmende Anzahl von Diensteanbietern schwierig.

- Hier gibt es keine Standardlösung, weder für verschlüsselte Daten noch für verschlüsselte Kommunikation. Nach Prüfung des Einzelfalls können ggf. gezielte Maßnahmen, wie z. B. spezielle Maßnahmen zur Telekommunikationsüberwachung oder Entschlüsselungsmaßnahmen, eingesetzt werden.

- In diesem Zusammenhang besteht die erste Herausforderung darin, die verschlüsselten Inhalte, und die Form der Verschlüsselung mit der erforderlichen Ausstattung zu erkennen. Das größte Problem ist jedoch die Entschlüsselung selbst, die nur durch den mit hohen Investitionen und erheblichen Kosten verbundenen Einsatz spezieller hochleistungsfähiger Hardware und Software möglich ist.

- Zur Lösung dieser Probleme ist es nötig, mit dem aktuellen Stand der Technik im Bereich der Verschlüsselung vertraut zu sein und Schwächen bei Algorithmen und Implementierungen zu untersuchen, auch um mögliche Fehler ausnutzen zu können.

- Die Begutachtung hat gezeigt, dass in der Regel einige Erfolge erreicht werden, wenn sehr einfache Formen von Verschlüsselungsmethoden verwendet werden, und dass Schlüssel mittels geeigneter Software, die eine Entschlüsselung ermöglicht, ermittelt bzw. rückgerechnet werden können. Einfache Passwörter lassen sich durch entsprechende Hardware und Programme "knacken".

- Die Ermittlungsbehörden können erheblich zur erfolgreichen Entschlüsselung von Passwörtern beitragen, wenn sie den IT-Forensik-Experten Informationen im Zusammenhang mit dem Passwort selbst (mögliche Passphrasen, Phrasensegmente, Zeichensatz, Passwortlänge usw.) und alle elektronischen Beweismittel oder Geräte zur Verfügung stellen. Dies erweist sich jedoch nicht immer als wirksam.

- Aus den Feststellungen der Begutachtung geht hervor, dass in bestimmten Fällen eine komplexere Verschlüsselung durch einen Brute-Force-Angriff – d.h. Ausprobieren aller möglichen Codes – oder Wörterbuchangriffe – d. h. Verwendung ausgesuchter Begriffe zur Passwortsuche (Passwort-Mining) – erfolgreich entschlüsselt werden konnte; möglich war dies auch, wenn sich der Tatverdächtige zur Zusammenarbeit bereit erklärt hat und das zur Entschlüsselung erforderliche Passwort – oder die Passphrase – mitgeteilt hat. Allerdings sind die betroffenen Personen nicht immer willens, mit den Behörden zusammenzuarbeiten, und es gibt keine Mittel, um sie zur Zusammenarbeit zu zwingen.

- Bei Dateien, die durch eine robuste Verschlüsselung geschützt sind (z.B. AES-256-verschlüsselte Archive), oder im Falle einer Festplattenverschlüsselung (z.B. TrueCrypt, BitLocker, FileVault2, WinRar oder PGP) können Brute-Force- oder Wörterbuchangriffe extrem zeitaufwändig sein (Monate oder, in einigen Fällen, sogar Jahre) und eine erhebliche Rechenleistung (spezielle kommerzielle Software und Netzcluster-Infrastruktur) erfordern. Dennoch kann es sich in Fällen, in denen die Täter technisch fortschrittliche Passwörter oder komplexe Algorithmen verwenden, als unmöglich erweisen, den Verschlüsselungsschutz zu durchbrechen; in bestimmten Fällen wird der Entschlüsselungsprozess eingestellt.

- In einigen Mitgliedstaaten wird die Entschlüsselung in Zusammenarbeit mit Privatunternehmen durchgeführt, deren Sachkenntnis sich als nützlich erweist, insbesondere wenn die Verschlüsselungsmethoden sehr komplex sind. In mehreren Mitgliedstaaten sind Privatunternehmen hingegen nicht an der Entschlüsselung im Rahmen von strafrechtlichen Ermittlungen beteiligt; dies ist den nationalen kriminaltechnischen Instituten vorbehalten.

- Die Ressourcen und Dienste von Europol, insbesondere das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), bieten die Möglichkeit der Nutzung einer Entschlüsselungsplattform an, und einige Mitgliedstaaten machen von dieser Möglichkeit Gebrauch.

- Den Feststellungen der Begutachtung zufolge lassen sich die durch Verschlüsselung bewirkten Herausforderungen teilweise bewältigen, indem Forschung intensiviert und neue Methoden – darunter intelligentere Analysen des bzw. der von einem Tatverdächtigen verwendeten Passwortmuster und eine dynamische Aggregation der Rechenleistung – entwickelt werden.

- Auch eine gute Zusammenarbeit zwischen den verschiedenen beteiligten Behörden, insbesondere Strafverfolgungsbehörden, IT-Forensik-Stellen und Staatsanwälten, ist unerlässlich, da es sich aufgrund der daraus entstehenden Kosten nicht jede Dienststelle oder Behörde leisten kann, Hard- und Software zur Passwortwiederherstellung zu erwerben.

- Die Zusammenarbeit zwischen den Mitgliedstaaten im Bereich der Entschlüsselung wird durch die gemeinsame Nutzung von Ressourcen und Erfahrungen und die Teilnahme an gemeinsamen Einsätzen sichergestellt. Falls Beweismittel zur Entschlüsselung an andere Behörden weitergeleitet werden müssen, kann dies über die Kanäle von Europol und Interpol erfolgen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten in spezielle Hard- und Software mit angemessener Rechenleistung sowie in entsprechend geschultes Personal investieren, um auch in komplexen Fällen von verschlüsselten Dateien und verschlüsselter Kommunikation eine Entschlüsselung sicherzustellen.***

- ***Ferner sollten die Mitgliedstaaten die Zusammenarbeit zwischen allen einschlägigen Akteuren, gegebenenfalls auch mit Privatunternehmen, sicherstellen, um die Entschlüsselungsfähigkeiten der zuständigen Behörden zu verbessern.***

- ***Die Mitgliedstaaten sollten Forschung und Entwicklung intensivieren, um neue und wirksamere Entschlüsselungsmethoden zu entwickeln, und die Einrichtungen von Europol, d. h. die Entschlüsselungsplattform Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (EC3), bei komplexeren Fällen von Verschlüsselung nutzen.***

- ***Den Mitgliedstaaten und den EU-Organen wird empfohlen, Lösungen zu prüfen und einen offenen Dialog mit dem Privatsektor zu intensivieren.***

## XII – ELEKTRONISCHES BEWEISMATERIAL

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Eine erhebliche Zahl von Mitgliedstaaten hat in ihren nationalen Rechtsvorschriften den Begriff "elektronischse Beweismaterial" nicht definiert. Die Begriffe, die im Übereinkommen des Europarats über Computerkriminalität (im Folgenden "Budapester Übereinkommen") und der Richtlinie 2013/40/EU vom 12. August 2013 über Angriffe auf Informationssysteme verwendet werden, dienen als Bezugsrahmen.

- In der Praxis versteht man unter elektronischem Beweismaterial im Allgemeinen Informationen, die mittels elektronischer Geräte erzeugt, gespeichert oder übermittelt werden und die Feststellung des Vorliegens oder Nichtvorliegens einer Straftat, die Identifizierung der Person, die eine solche Straftat begangen hat, und die Bestimmung der für die Klärung eines Falls erforderlichen Umstände gestatten.

- Hierunter fallen u. a. Registrierungsinformationen, Verlaufsdaten des Internetverkehrs, Inhaltsdaten, Bilddateien, IP-Adressen, E-Mails, elektronische Dokumente, digitale Videodateien, Audiodateien und Imagedateien, Datenbanken, Tabellenkalkulationsdaten, Cookies, elektronische Ausdrucke, elektronische Buchführung, Daten der elektronischen Standortbestimmung über GPS, Protokolle über getätigte Bankgeschäfte usw.

- Der Erhebung, Analyse und Verwendung von elektronischem Beweismaterial kommt in Strafverfahren eine stets größere Bedeutung zu, nicht nur im Bereich der Cyberkriminalität, sondern auch im Zusammenhang mit jeder anderen Straftat, bei der elektronisches Beweismaterial eine Rolle spielen könnten.

- Die Art des elektronischen Beweismaterials und der Umstand, dass es leicht manipuliert oder gefälscht werden kann, kann zu Problemen im Hinblick auf dessen Zulässigkeit führen, die bei anderen Arten von Beweismitteln nicht auftreten.
  Aus diesem Grund gibt es in einigen Mitgliedstaaten spezielle Vorschriften für die Erhebung von elektronischem Beweismaterial, um dessen Zulässigkeit vor Gericht sicherzustellen. Dies kann u. a. die Erhebung durch einen fachkundigen Sachverständigen umfassen, um die Integrität des elektronischen Beweismaterials oder die korrekte Dokumentation der Beweiskette in Bezug darauf sicherzustellen, wie das Beweismaterial ursprünglich erlangt wurde, wer es bearbeitet hat, wie es bearbeitet wurde und ob es in irgendeiner Weise verändert wurde.

- Einige Mitgliedstaaten befolgen für die Zwecke der Erhebung von elektronischem Beweismaterial die bewährten Verfahren für die IT-Forensik, wie sie im Übereinkommen des Europarates über Computerkriminalität oder in internationalen Leitlinien als Leitlinien der Vereinigung der leitenden Polizeibeamten (ACPO) festgelegt wurden; diese gelten auch für die Speicherung und Weitergabe von elektronischem Beweismaterial.

- Allerdings hat die Begutachtung gezeigt, dass in den meisten Mitgliedstaaten das Verfahrensrecht überwiegend technologieneutral ist, was bedeutet, dass die allgemeinen Vorschriften und Grundsätze zur Beweiserhebung angewandt werden und das Verfahrensrecht keine besonderen Vorschriften für die Zulässigkeit und Beurteilung von elektronischem Beweismaterial enthält; letzteres unterliegt den gleichen Bedingungen wie alle anderen Beweismittel und wird vom Richter im Einklang mit den allgemeinen Strafverfahrensvorschriften bewertet.

- Daher ist elektronisches Beweismaterial in Strafverfahren generell zulässig, wenn es in rechtmäßiger Weise erlangt wurde und für das Verfahren relevant ist. Dies gilt auch für elektronisches Beweismaterial, das außerhalb der Staatsgrenzen durch Zusammenarbeit mit den Mitgliedstaaten im Wege der internationalen Rechtshilfe oder durch eine direkte Zusammenarbeit mit ausländischen Internetdiensteanbietern erlangt wurde.

- Jedoch sollte das Fehlen einer Regelung für die Methodik der Erhebung und Vorlage von elektronischem Beweismaterial vor Gericht, wie aus einem Ländergutachten hervorgeht, grundsätzlich kein Hindernis für die wirksame Verfolgung von Cyberstraftaten sein, da die Zulässigkeit von elektronischem Beweismaterial unter die allgemeinen Rechtsvorschriften über Beweismittel fällt.

- In einigen wenigen Mitgliedstaaten ist elektronisches Beweismaterial, wie die meisten traditionellen Beweismittel, vor Gericht zulässig und wird vom Richter im Einklang mit dem Grundsatz der freien Beweiswürdigung beurteilt. Dies bedeutet, dass alles, was in einem Fall als Beweismittel von Nutzen sein kann, grundsätzlich vor Gericht gebracht werden kann; das Gericht entscheidet dann von Fall zu Fall, welcher Wert jedem Beweismittel beigemessen wird. Gemäß den Schlussfolgerungen der Begutachtung kann dies als bewährtes Verfahren betrachtet werden.

- Wenn die Vorschriften über die Zulässigkeit von Beweismitteln hingegen ziemlich streng sind, so kann dies zu Hindernissen für elektronisches Beweismaterial führen, insbesondere wenn sie aus einem anderen Land, z. B. durch Rechtshilfeersuchen, erlangt wurden.

- Die – oftmals im Auftrag eines Richters/Staatsanwalts handelnde – Polizei kann auf die am Ort der Durchsuchung gespeicherten Daten sowie auf Ferndaten oder, in Übereinstimmung mit den internationalen Übereinkommen, auf im Ausland gespeicherte Daten zugreifen. Wenn die Klärung strafverfahrensrelevanter Sachverhalte die Sicherung gespeicherter Computerdaten – einschließlich operativer Daten, die durch das Computersystem oder auf einem Datenträger (z. B. CD, DVD, Mobiltelefone) gespeichert wurden –, im Hinblick auf deren Aufnahme in die Strafakten erfordert, werden die betreffenden Gegenstände in der Regel im Einklang mit den einschlägigen Bestimmungen der Strafprozessordnung der Mitgliedstaaten beschlagnahmt.

- Falls elektronisches Beweismaterial im Internet vorliegt oder sich im Besitz der Dienstanbieter befindet, ist die direkte Zusammenarbeit mit letzteren unerlässlich, damit die erforderlichen Daten erlangt und Maßnahmen ergriffen werden können, um die Vernichtung oder Veränderung von Daten zu verhindern. Allerdings ist es nicht in allen Mitgliedstaaten möglich, direkten Zugriff auf elektronisches Beweismaterial in einem anderen Land oder in der "Cloud" zu erhalten, sodass in derartigen Fällen Rechtshilfeverfahren zu befolgen sind.

- Damit diesen Schwierigkeiten begegnet werden kann, müssen laut den Schlussfolgerungen der Begutachtung die derzeitigen Rechtshilfeverfahren im Ergebnis schneller und wirksamer sein und die Ermittlungsbehörden müssen in der Lage sein, sehr rasch Anfragen an viele verschiedene Länder zu richten.

- In bestimmten Mitgliedstaaten ist es gemäß den nationalen Rechtsvorschriften erlaubt, Informationen direkt von ausländischen Anbietern zu erlangen, sofern dies auch nach dem Recht des Staates zulässig ist, in dem der Anbieter seinen Sitz hat. Ein gemeinsamer Rahmen für den Austausch von Teilnehmerdaten und neue Ansätze auf EU-Ebene in Bezug auf die Zuständigkeit für Ermittlungsmaßnahmen sind – wie andere Themen – Gegenstand der derzeit auf EU-Ebene auf der Grundlage der Schlussfolgerungen des Rates vom 9. Juni 2016 zur Verbesserung der Strafjustiz im Cyberspace durchgeführten Arbeiten.

- Die Verfahren und Formen für die Bereitstellung von elektronischem Beweismaterial in Ermittlungen als Teil der Verfahrensakte in einem Format, das die Prüfung durch die Staatsanwälte und Richter ermöglicht, unterscheiden sich je nach Mitgliedstaat.

- Die Beschlagnahme von Computerhardware, die elektronisches Beweismaterial enthält, ist offenbar nicht die beste Lösung, da es für eine durch Cyberkriminalität geschädigte Person schwierig sein kann, den Verlust ihrer für die Dauer der Ermittlungen beschlagnahmten digitalen Ausstattung hinzunehmen.

- Alternativ können zur Sicherung von elektronischem Beweismaterial die gespeicherten Daten auf ein anderes Speichermedium (z. B. DVD oder Festplatte) kopiert (gespiegelt) und in diesem Format zur Verfügung gestellt werden und/oder insbesondere lesbare Daten (z. B. Textnachrichten) oder Bilddateien ausgedruckt und auch in Papierform zur Verfügung gestellt werden.

- In der Regel wird bei im Ausland beschafftem elektronischen Beweismaterial die gleiche Vorgehensweise angewandt. Wenn jedoch in dem Land, das zur Erhebung des Beweismaterial beigetragen hat, besondere Auflagen gelten, müssen diese von der Polizei und den Staatsanwälten beachtet werden.

- Wenn der Staatsanwalt und die Richter, die in Gerichtsverfahren elektronisches Beweismaterial bearbeiten müssen, dieses in einer Form erhalten, die nur mit IT-Ausstattung abgerufen und beurteilt werden kann, und hierfür spezifische Kenntnisse erforderlich sind – was auch für die Prüfung der Echtheit des elektronischen Beweismaterials gilt –, kann ein kriminaltechnischer Sachverständiger hinzugezogen werden.

- Laut den Ergebnissen der Begutachtung würde spezifische High-Tech-Hard- und -Software für die bessere Identifizierung und Erlangung von elektronischem Beweismaterial es den Behörden der Mitgliedstaaten ermöglichen, mit vergleichbarem elektronischen Beweismaterial zu arbeiten und zu kooperieren.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten über angemessene High-Tech-Hard- und -Software für die Identifizierung und Erlangung von elektronischem Beweismaterial verfügen, sodass die Behörden der Mitgliedstaaten mit vergleichbarem elektronischen Beweismaterial arbeiten und kooperieren können.***

- ***Die Mitgliedstaaten sollten sicherstellen, dass ihre nationalen Verfahrensrechtsvorschriften ausreichend flexibel sind, um die Zulässigkeit von elektronischem Beweismaterial zu vereinfachten, und zwar auch dann, wenn es aus einem anderen Land stammt und z. B. im Wege von Rechtshilfeersuchen erlangt wurde.***

- ***Die Mitgliedstaaten sollten in Erwägung ziehen, gegebenenfalls unter Einbeziehung von Eurojust und des Europäischen Justiziellen Netzes für Cyberkriminalität einen ständigen Dialog mit dem privaten Sektor einzuleiten und fortzuführen und Methoden zu erörtern, mit denen sich sicherstellen lässt, dass die Erhebung von elektronischem Beweismaterial so erfolgt, dass es vor Gericht zulässig ist.***

- ***Die EU und ihre Mitgliedstaaten sollten auf der Grundlage des gegenwärtigen Expertenprozesses in Bezug auf den Zugang zu elektronischem Beweismaterial die Ausarbeitung eines EU-Rahmens erwägen, der die für Strafverfolgungszwecke geltenden Regeln für den Zugang zu im Besitz von Diensteanbietern befindlichen Daten festlegt. Ein solcher Rahmen sollte die Beziehungen zwischen Strafverfolgungsbehörden und Internetdiensteanbietern regulieren und eindeutige Regeln und Aufgaben festlegen.***

## XIII – CLOUD-COMPUTING

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Die Cyberkriminalität betreffend Daten in der "Cloud" wurde von einer beträchtlichen Anzahl von Mitgliedstaaten als ein für Ermittlungen und für die Strafverfolgung problematischer Bereich genannt.

- Einige Mitgliedstaaten hatten zum Zeitpunkt der Begutachtung keine Erfahrung mit dieser Art von Ermittlungen gegen Cyberkriminalität, und folglich war die Frage der gerichtlichen Zuständigkeit im Hinblick auf die Cloud-Speicherung noch nicht vor ihren nationalen Gerichten geprüft worden, was bedeuten könnte, dass eine Reihe von Fällen der Cyberkriminalität in der Praxis nach wie vor nicht verfolgt wird; es wurde jedoch eingeräumt, dass sie zwangsläufig mit solchen Situationen konfrontiert sein würden.

- Dieses Phänomen kann in Zukunft zu erheblichen Problemen führen, da Cloud-Lösungen immer beliebter werden und die Nutzung von Cloud-basierter Speicherung und entsprechenden Diensten immer mehr zur gängigen Praxis wird, und zwar nicht nur für juristische und natürliche Personen, sondern auch für Straftäter.

- Aufgrund der verwendeten Technologien sowie angesichts der Speicherkapazität der Server und der Größenvorteile werden Daten ständig rund um den Globus verschoben und können in Teile fragmentiert sein, die erst beim Abruf zusammengefügt werden. Ein besonderes Problem bei Straftaten im Zusammenhang mit der "Cloud" ist daher die Bestimmung des physischen Orts, an dem die Straftat tatsächlich begangen wurde, was sich als schwer, sehr kompliziert und langwierig erweisen kann. Deshalb sind Informationen und die Server, auf denen sich Daten in der "Cloud" befinden, für die Strafverfolgungsbehörden nicht leicht auffindbar und abrufbar.

- Durch das Fehlen von Informationen bleibt es den Ermittlungsbeamten verwehrt, digitale Hinweise zu erlangen, und kann die Identifizierung des Täters sowie die Bestimmung des Zeitpunkts der Straftat, des Orts der Straftat und des Tatinstruments erschwert werden, was ggf. dazu führt, dass Fälle von Cyberkriminalität ungestraft bleiben und Personen immer wieder geschädigt werden.

- Auch die Anbieter von Cloud-Speicherung können Schwierigkeiten bei der Lokalisierung des tatsächlichen (territorialen) Standorts der Daten haben; selbst die Eigentümer der Daten wissen häufig nicht, wo sich diese befinden.

- Da Straftaten betreffend Daten in der "Cloud" die gerichtliche Zuständigkeit mehrerer Mitgliedstaaten oder eine gerichtliche Zuständigkeit außerhalb der EU betreffen können, werden durch das Cloud-Computing nicht nur Probleme im Hinblick auf das nationale, sondern auch auf das internationale Recht aufgeworfen, die auf der Souveränität der Staaten und dem Territorialitätsprinzip basieren.

- Selbst wenn der Standort festgestellt wurde, sehen die nationalen Rechtsvorschriften in einigen Mitgliedstaaten keine extraterritoriale gerichtliche Zuständigkeit vor oder können Cyberstraftaten betreffend Daten in der "Cloud" nur verfolgt werden, wenn diese Daten von den betroffenen Mitgliedstaaten aus zugänglich sind.

- Kompetenzkonflikte hinsichtlich der Zuständigkeit für den Erlass einer Anordnung zur Erlangung elektronischen Beweismaterials können entstehen, wenn zwei oder mehrere Mitgliedstaaten die gerichtliche Zuständigkeit für die Straftat begründen können; in diesen Fällen können die Mitgliedstaaten zur Überwindung von Konflikten dieser Art auf die Dienste von Eurojust und auf gemeinsame Ermittlungsgruppen zurückgreifen.

- Die Begutachtung hat ergeben, dass es zwei Hauptmöglichkeiten für die Erlangung von in der "Cloud" gespeicherten Daten gibt: Der direkte Zugriff auf den Inhalt solcher Profile und Speichereinrichtungen wird durch Zustimmung des Benutzers/Eigentümers des Profils oder Kontos erlangt. Kann der Standort der Informationen bestimmt werden, so können auch Rechtshilfeverfahren eingeleitet werden, wobei indes zu bedenken ist, dass sie oftmals langwierig und ineffizient sind.

- Die andere Möglichkeit, Anbieter direkt zur Bereitstellung bestimmter Daten aufzufordern, erweist sich in der Praxis häufig als sehr schwierig, da es Anbieter gibt, die nicht mit ausländischen Strafverfolgungsbehörden zusammenarbeiten und nicht jedes Ersuchen beantworten.

- Im Hinblick auf die Überwindung dieser Schwierigkeiten zeigte die Begutachtung, dass Sondervereinbarungen mit einigen Cloud-Anbietern (z. B. Google, Yahoo usw.) abgeschlossen werden könnten, um Verzögerungen zu verringern und Informationen in vor Gericht zulässigen Formaten zu erlangen. Einige Maßnahmen zur Lösung dieses Problems werden derzeit auf der Ebene der EU im Rahmen des gegenwärtigen Expertenprozesses zu elektronischem Beweismaterial geprüft, beispielsweise einheitliche Ansprechpartner sowohl auf der Seite der Mitgliedstaaten als auch auf der Seite der Diensteanbieter und ein Rechtsrahmen der EU für Ermittlungsmaßnahmen bei einem Diensteanbieter, der die Behörden in die Lage versetzt, einen Diensteanbieter in einem anderen Mitgliedstaat zu ersuchen ("Vorlageersuchen") oder zu verpflichten ("Vorlageanordnung"), Informationen über einen Nutzer offenzulegen usw.

- Gemäß dem Übereinkommen des Europarats über Computerkriminalität sind grenzüberschreitende Maßnahmen allerdings nur in einer sehr begrenzten Zahl von Fällen zulässig, z. B mit rechtmäßiger Einwilligung der Person, die in Fällen, in denen die Zuständigkeit bekannt ist, rechtmäßig zur Offenlegung der Daten befugt ist. In Fällen, in denen der Standort der Daten außerhalb des Hoheitsgebiets der Übereinkommensparteien liegt, finden diese Bestimmungen keine Anwendung.

- In Anbetracht der vorstehenden Ausführungen konnte bislang noch keine angemessene Lösung für das Problem der Cloud-Speicherung gefunden werden. Die verschiedenen Möglichkeiten, die im Völkerrecht für eigenständiges Handeln oder im Rahmen der Rechtshilfe vorgesehen sind, haben sich im Hinblick auf Ermittlungen zu Cyberkriminalität als beschränkt erwiesen, wenn die Daten in der "Cloud" gespeichert werden.

- Laut den Schlussfolgerungen der Begutachtung sollte geprüft werden, wie die Verfahren verbessert werden können, um wirksame Ermittlungen und eine wirksame Strafverfolgung bei Cyberkriminalität betreffend Daten in der "Cloud" sicherzustellen und gleichzeitig die Schwierigkeiten zu berücksichtigen, die aufgrund etwaiger positiver Kompetenzkonflikte auftreten können.

- Zu diesem Zweck könnte es auch nützlich sein, eine Prüfung der bestehenden rechtlichen Rahmenbedingungen und/oder der Probleme im Zusammenhang mit Ermittlungen zu erwägen, damit klare Regeln und Verfahren in Bezug auf Cyberkriminalität betreffend Daten in der "Cloud" bestehen.

- Die Mitwirkung der Mitgliedstaaten in internationalen Foren (z. B. Cybercrime Convention Committee (T-CY)), in denen Lösungen für diese Fragen erörtert werden, wurde im Rahmen der Begutachtung ebenfalls als nützlich hervorgehoben.[6]

- Ein Mitgliedstaat unterbreitete Vorschläge für den Zugriff auf Daten in der "Cloud" wie beispielsweise die Bereitstellung der Möglichkeit, virtuelle Suchen in Rechenzentren in anderen Ländern durchzuführen, ohne dass zunächst der physische Standort des Servers identifiziert werden muss, und/oder Datendiensteanbieter anzuweisen, den Strafverfolgungsbehörden Passwörter zur Verfügung zu stellen, damit diese auf die Daten zugreifen können.

[6] Das T-CY hat das Mandat für Verhandlungen über ein Zusatzprotokoll zu diesen Fragen angenommen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten den Abschluss von Sondervereinbarungen mit den zentralen Cloud-Anbietern in Erwägung ziehen, um Verzögerungen zu verringern und vor Gericht zulässige Daten zu erlangen.***

- ***Die EU sollten die mit Cloud-Computing verbundenen Herausforderungen weiter angehen, um Lösungen zu finden, mit denen die Fähigkeit zu Cyberkriminalitäts-ermittlungen erhöht werden kann, einschließlich im Rahmen des gegenwärtigen Expertenprozesses zu elektronischem Beweismaterial.***

## XIV – VORRATSDATENSPEICHERUNG IM BEREICH DER ELEKTRONISCHEN KOMMUNIKATION

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Mit der Ungültigerklärung der Richtlinie 2006/24/EG durch das Urteil des Europäischen Gerichtshofs vom 8. April 2014 (verbundene Rechtssachen C-293/12 und C-594/12, "Digital Rights Ireland und Seitlinger und andere") ist eine Situation der Rechtsunsicherheit entstanden, insbesondere in Bezug auf den rechtlichen Status der nationalen Rechtsvorschriften zur Umsetzung der Richtlinie. Die Mitgliedstaaten verfahren unterschiedlich in Bezug auf das Urteil sowie die Beibehaltung, Änderung, Ersetzung oder Aufhebung der Umsetzungsrechtsvorschriften oder ihre Ungültigerklärung durch die nationalen Gerichte.

- Mehrere Mitgliedstaaten haben die negativen Auswirkungen des oben genannten Urteils auf die Wirksamkeit der strafrechtlichen Ermittlungen und der Strafverfolgung auf nationaler Ebene – insbesondere im Hinblick auf die Zuverlässigkeit und Zulässigkeit des auf der Erhebung elektronischer Kommunikationsdaten beruhenden Beweismaterials vor Gericht – sowie auf die grenzüberschreitende justizielle Zusammenarbeit zwischen den Mitgliedstaaten und auf internationaler Ebene (begrenzte Fähigkeit zur Bereitstellung und Erlangung von Beweismaterial) betont. Die fehlende Sicherung von Daten bzw. die Vorratsdatenspeicherung nur für einen begrenzten Zeitraum erschwert es oder macht es sogar unmöglich, elektronisches Beweismaterial in den Mitgliedstaaten zu sichern.

- Mehrere Mitgliedstaaten betonten, dass ein gemeinsamer Ansatz auf EU-Ebene – einschließlich der Möglichkeit eines neuen Rechtsrahmens, mit dem die Bedingungen und Fristen für die Vorratsdatenspeicherung in den Mitgliedstaaten harmonisiert werden könnten – einen Zusatznutzen darstellen würde.

- In der Zwischenzeit hat der Europäische Gerichtshof in seinem Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 "Tele 2 und Watson" vom 21. Dezember 2016 festgestellt, dass eine nationale Regelung, die die allgemeine Speicherung aller Verkehrs- und Standortdaten vorsieht, die Grenzen des Notwendigen überschreitet, und die Kriterien und Bedingungen präzisiert, die von den nationalen Regelungen der Mitgliedstaaten über die Vorratsdatenspeicherung erfüllt werden müssen.

- Im Rahmen gemeinsamer Überlegungen zwischen den Organen der EU und den Mitgliedstaaten wird derzeit die Frage der Vorratsdatenspeicherung im Hinblick auf mögliche rechtliche und praktische Lösungen für die Herausforderungen, die sich aus der Rechtsprechung des EuGH ergeben, angegangen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten und die Organe der EU sollten die gemeinsamen Überlegungen mit dem Ziel fortsetzen, rechtliche und praktische Lösungen für die Frage der Vorratsdatenspeicherung im Bereich der elektronischen Kommunikation auf nationaler und auf EU-Ebene unter Berücksichtigung der Grundsätze, die in der jüngsten Rechtsprechung des EuGH verankert sind, zu finden.***

## XV – MASSNAHMEN GEGEN KINDERPORNOGRAFIE UND SEXUELLEN MISSBRAUCH IM INTERNET

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Die Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie war zum Zeitpunkt der Begutachtung in der Mehrheit der Mitgliedstaaten umgesetzt. Der derzeitige Stand der Umsetzung dieser Richtlinie in nationale Maßnahmen kann unter folgendem Link abgerufen werden: http://eur-lex.europa.eu/legal-content/DE/NIM/?uri=celex%3A32011L0093

- Aufgrund der Entwicklungen in Gesellschaft und Technik, durch die sowohl die Gelegenheiten für die Kommunikation und die Verbreitung von Informationen als auch die Möglichkeiten, strafbare Handlungen online zu begehen, zugenommen haben, hat der sexuelle Kindesmissbrauch über das Internet (Grooming, Sexting, Cyber-Mobbing usw.) in den letzten Jahren stark zugenommen. Im Hinblick auf eine wirksame Bekämpfung dieser Formen der Kriminalität wird in den Mitgliedstaaten ein breites Spektrum an Präventiv- und Zwangsmaßnahmen unter Einbeziehung des öffentlichen und des privaten Sektors umgesetzt.

- In einigen Mitgliedstaaten besteht eine nationale Datenbank für die Identifizierung der Opfer zur Bekämpfung des sexuellen Missbrauchs von Kindern oder sie wurde zum Zeitpunkt der Begutachtung gerade eingerichtet. In der Mehrzahl der Mitgliedstaaten fehlt jedoch eine solche nationale Datenbank oder sie war zum Zeitpunkt der Begutachtung nicht hinreichend entwickelt. In diesen Fällen nutzen die Strafverfolgungsbehörden nur internationale Datenbanken und Instrumente, insbesondere die Interpol-Datenbank über die sexuelle Ausbeutung von Kindern (International Child Sexual Exploitation Database, ICSE-DB), die sich als wirksames Erkenntnisgewinnungs- und Ermittlungsinstrument für die Identifizierung von Opfern und Tätern erwiesen hat, da sie den Fachermittlern den weltweiten Austausch von Daten ermöglicht.

- Wenn die Polizei in einem Mitgliedstaat das Opfer nicht über die Datenbank identifizieren kann, jedoch einen hinreichenden Verdacht in Bezug auf die mögliche Identität eines Kindes hat, kann sie eines oder mehrere Abbildungen des Opfers zur Identifizierung mit Schulen austauschen, was als bewährtes Verfahren angesehen werden kann.

- Zur Vermeidung einer erneuten Viktimisierung von Kindern werden in den Mitgliedstaaten verschiedene Ansätze angewandt: Neben dem Blockieren und/oder Entfernen kinderpornografischen Materials gibt es andere Maßnahmen wie Auflistung der als gefährlich für Minderjährige eingestuften Medien in einem Index, Beschränkung der Kontakte mit dem Straftäter, Betreuung und Beratung der Opfer durch NRO sowie spezifische Maßnahmen zum Schutz der Opfer und Zeugen von sexuellem Kindesmissbrauch vor negativen Folgen während der Strafverfahren.

- In einigen wenigen Mitgliedstaaten gibt es zwar keine spezifischen Maßnahmen, um eine erneute Viktimisierung von Kindern zu vermeiden, jedoch wird zu diesem Zweck mit NRO, spezialisierten nichtpolizeilichen Stellen und Einrichtungen mit Zuständigkeiten im Bereich des Schutzes von Minderjährigen oder der EMPACT-Teilpriorität zum Cyberkriminalitätsbereich "Kindesmissbrauch im Internet" ("Online Child Abuse") zusammengearbeitet.

- In den Mitgliedstaaten sind verschiedene rechtliche, technische, organisatorische und Informationsmaßnahmen zur Bekämpfung von sexueller Ausbeutung bzw. sexuellem Missbrauch im Internet, Sexting, Cyber-Mobbing und Kindersextourismus vorhanden. Mehrere Mitgliedstaaten verfügen zum Zwecke der Identifizierung der Kinder und Täter sowie zur Durchführung der Ermittlungen über Fachdienststellen oder -bedienstete, die ausschließlich mit Material, das sexuellen Missbrauch von Kindern enthält, befasst sind. Ein bewährtes Verfahren in einem Mitgliedstaat sind Beurteilungen der in dem betreffenden Bereich tätigen Polizeibeamten bei der Einstellung und deren jährliche psychologische Untersuchung.

- In allen Mitgliedstaaten wurden in unterschiedlichem Umfang Präventivmaßnahmen zur Förderung der sicheren Nutzung des Internets durch Minderjährige umgesetzt, die oft unter der Leitung der jeweiligen staatlichen Behörden und in Zusammenarbeit mit den Fachdienststellen und den NRO, die mit Kindern arbeiten, entwickelt wurden. Einige Projekte in diesem Bereich werden von der EU kofinanziert, wie das europäische Netzwerk für mehr Sicherheit im Internet (INSAFE) im Rahmen des Programms "Sichereres Internet" der Europäischen Kommission.

- Zu den Präventivmaßnahmen zählen beispielsweise Schulungsprojekte und Aufklärungskampagnen mit dem Ziel, die Zielgruppen (Schüler, Eltern, Pädagogen und andere Gruppen) für die wichtigsten potenziellen Risiken, mit denen Minderjährige bei der Nutzung des Internets konfrontiert sind, zu sensibilisieren und entsprechend zu schulen und eine verantwortungsvolle Nutzung des Internets zu entwickeln. Die in einem Mitgliedstaat angewandten modernen Methoden, bei denen Kinder Kinder unterrichten, wurden als bewährtes Verfahren betrachtet. In einigen Mitgliedstaaten veranstaltet auch die Polizei solche Tätigkeiten oder ist daran beteiligt.

- Medienerziehung ist ebenfalls ein wirkungsvolles Instrument zur Verhütung des sexuellen Kindesmissbrauchs, insbesondere für Kinder und Jugendliche, und in einigen Mitgliedstaaten werden Informationen über ein sicheres Verhalten im Internet für Kinder auf speziellen Websites veröffentlicht. Andere Mitgliedstaaten haben Broschüren oder Handbücher oder "Schulleitfäden" zum Thema sichere und effiziente Nutzung des Internets, Cyber-Mobbing usw. ausgearbeitet.

- Die Mehrheit der Mitgliedstaaten verfügt über eine Hotline, über die anonym Darstellungen des sexuellen Missbrauchs von Kindern gemeldet werden können und die häufig auch als Notrufnummer für Kinder, Jugendliche und Eltern dient und unter der anonyme und kostenlose Beratung per Telefon und Internet (Websites oder Plattformen) bereitgestellt wird, z. B. auch in Bezug auf die Frage, wie man Anzeige bei der Polizei erstattet. Auf einer europäischen Online-Plattform – www.reportchildsextourism.eu – sind alle nationalen Meldesysteme in Europa angegeben.

- Die meisten Mitgliedstaaten verfügen über strafrechtliche Bestimmungen über Straftaten und Sanktionen für reisende Kindersexualstraftäter oder wenden andere Maßnahmen an, darunter Maßnahmen gegen die Werbung für Missbrauchsgelegenheiten und Kindersextourismus, wie dies in Artikel 21 der Richtlinie 2011/93/EU vorgesehen ist. Maßnahmen, die auf die verbesserte Aufdeckung dieser besonderen Form der Kriminalität abzielen, umfassen Überwachungs- oder Meldesysteme in Bezug auf reisende Sexualstraftäter, Maßnahmen unter Einbindung der Tourismus- und Reisebranche und des auswärtigen Dienstes, Entsendung von Verbindungsbeamten ins Ausland, Einziehung des Reisepasses von wegen Kindesmissbrauchs verurteilten Personen usw.

- Zu den allgemeinen Maßnahmen zur frühzeitigen Erkennung des sexuellen Missbrauchs von Kindern im Internet gehören beispielsweise das Absuchen des Internets und verdeckte Ermittlungen, was sich als ein wirksames Instrument zur Bekämpfung der sexuellen Ausbeutung von Kindern im Internet in Echtzeit erwiesen hat, sowie Filtersysteme, die jedoch nicht in allen Mitgliedstaaten angewendet werden oder häufig für Internetdiensteanbieter nicht obligatorisch sind.

- Zwangsmaßnahmen in Fällen des sexuellen Missbrauchs von Kindern im Internet, die das Sperren des Zugangs, das Entfernen von Inhalten und das Deaktivieren von Webseiten einschließen, werden in den Mitgliedstaaten nicht einheitlich angewendet, und zwar in verfahrenstechnischer Hinsicht auch in der Frage, ob eine vorherige gerichtliche Anordnung oder eine nachträgliche gerichtliche Bestätigung der polizeilichen Maßnahmen erforderlich ist.

- In den meisten Mitgliedstaaten werden rechtliche und praktische Maßnahmen ergriffen, um audiovisuelles kinderpornografisches Online-Material permanent aus dem Internet zu löschen. Der "Löschungsansatz" kann als Maßnahme zur Lösung des Problems angesehen werden; mit dem Ansatz wird indes nicht verhindert, dass die Bilder oder Videos von Minderjährigen weiterhin auf anderen Internetseiten gezeigt werden. In anderen Mitgliedstaaten wird der Ansatz der Zugangssperre zusätzlich oder ausschließlich eingesetzt; dieser Ansatz besteht darin, den Zugang zu Webseiten mit kinderpornografischem Material zu sperren, indem solches Material vorübergehend unzugänglich gemacht wird.

- Wenn das Material auf Servern im Ausland gehostet ist, werden in der Regel internationale Kanäle, nämlich Europol und sein sicheres Informationsaustauschsystem SIENA oder Interpol und seine Initiative "Access Blocking", genutzt; außerdem können die Hotlines gleichzeitig durch Meldung an INHOPE (internationaler Verband der Internet-Meldestellen) sicherstellen, dass Material, das sexuellen Missbrauch von Kindern enthält und für ein einzelnes Land bestimmt ist, aber im Ausland gespeichert ist, aus dem Internet entfernt werden kann.

- In einigen Mitgliedstaaten werden Websites mit Material, das sexuellen Missbrauch von Kindern enthält, gesperrt und unzugänglich gemacht, und zwar unabhängig davon, ob die Sites innerhalb oder außerhalb der EU gehostet sind, was als bewährtes Verfahren angesehen wurde.

- Wesentliche Voraussetzung für die Durchführung der oben genannten Maßnahmen ist eine gute Zusammenarbeit zwischen allen einschlägigen Akteuren wie den Strafverfolgungsbehörden, Hotlines, NRO und Diensteanbietern. In einigen Mitgliedstaaten sind Letztere verpflichtet, geeignete Maßnahmen zu ergreifen, um die Möglichkeit der Nutzung dieses Materials zu unterbinden, indem der Zugang gesperrt oder Inhalte aus dem Internet entfernt werden, während in anderen Mitgliedstaaten die nationalen Rechtsvorschriften keine derartige Verpflichtung vorsehen, wobei aber die oben genannten Maßnahmen im Einzelfall aufgrund einer gerichtlichen Anordnung ergriffen werden können.

- Die Zusammenarbeit zwischen den Strafverfolgungsbehörden und den inländischen Diensteanbietern ist in den Mitgliedstaaten im Allgemeinen gut, und oft löschen die Anbieter Material, das sexuellen Missbrauch von Kindern enthält, zügig und freiwillig nach entsprechender Mitteilung durch die Strafverfolgungsbehörden, selbst wenn sie dazu nicht verpflichtet sind. Ein in einem Mitgliedstaat genutztes Tool, mit dem durch Anklicken einer Schaltfläche mit einem bei allen Anbietern identischen Bildsymbol gemeldet werden kann, dass eine bestimmte Website Material enthält, das sexuellen Missbrauch von Kindern zeigt, wurde als beispielhaftes bewährtes Verfahren genannt.

**EMPFEHLUNGEN**

- ***Diejenigen Mitgliedstaaten, die dies noch nicht getan haben, sollten eine nationale Datenbank speziell für die Identifizierung der Opfer zur Bekämpfung des sexuellen Missbrauchs von Kindern entwickeln oder Zugang zur Interpol-Datenbank bieten. Die Mitgliedstaaten sollten außerdem in Erwägung ziehen, ein nationales Netz für den Austausch von Informationen zur Opferidentifizierung einzurichten.***

- ***Diejenigen Mitgliedstaaten, die dies noch nicht getan haben, sollten die Entwicklung spezifischer Maßnahmen in Erwägung ziehen, um eine erneute Viktimisierung von Kindern zu vermeiden, einschließlich Maßnahmen zum Schutz der Opfer und Zeugen von sexuellem Kindesmissbrauch vor negativen Folgen während der Strafverfahren.***

- ***Die Mitgliedstaaten sollten für eine gut funktionierende Zusammenarbeit zwischen allen einschlägigen Akteuren sorgen, um Straftaten gegen Kinder im Internet wirksam zu bekämpfen, und die Einführung einer Verpflichtung für Diensteanbieter erwägen, wonach diese geeignete Maßnahmen, wie etwa das Sperren des Zugangs, das Entfernen von Inhalten und das Deaktivieren von Websites, zu ergreifen haben.***

## XVI – MECHANISMUS ZUR BEWÄLTIGUNG VON CYBERANGRIFFEN

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme war zum Zeitpunkt der Begutachtung in der Mehrheit der Mitgliedstaaten umgesetzt. Der derzeitige Stand der Umsetzung dieser Richtlinie in nationale Maßnahmen kann unter folgendem Link abgerufen werden: http://eur-lex.europa.eu/legal-content/DE/NIM/?qid=1506328148248&uri=CELEX%3A32013L0040

- Cyberangriffe stellen eine Bedrohung dar, die immer mehr um sich greift, die Methoden und Instrumente für die Durchführung solcher Angriffe werden immer ausgefeilter, und das Spektrum der Cyberangriffe, die den Cyberraum bedrohen, ist sehr breit. Die Begutachtung hat insbesondere gezeigt, dass ein erheblicher Anstieg von Ransomware-Angriffen – eine Art Schadprogramm, das den Zugang zu Daten sperrt, bis Lösegeld gezahlt wird – zu verzeichnen ist.

- Einige Mitgliedstaaten greifen in Fällen von Cyberangriffen auf technische Unterstützung des privaten Sektors zurück, da Privatunternehmen über gute Sachkenntnisse verfügen und mit besserer Ausstattung zu geringeren Kosten arbeiten. Darüber hinaus können sie dabei helfen, die Auswirkungen der Angriffe auf Infrastrukturen zu bewerten und umfassende Lagebilder zu erstellen.

- In einigen Mitgliedstaaten gibt es bereits einen strukturierten, behördenübergreifenden Ansatz, in bestimmten Fällen basierend auf einer öffentlich-privaten Partnerschaft, während in anderen Mitgliedstaaten ein solcher Ansatz nicht ausreichend entwickelt wurde oder gänzlich fehlt und die Koordinierungsmechanismen für die Reaktion auf Cyberangriffe in erster Linie auf der Grundlage einer informellen Zusammenarbeit funktionieren.

- Zum Zeitpunkt der Begutachtung hatte die Mehrzahl der Mitgliedstaaten bereits ein nationales CSIRT eingerichtet oder war gerade im Begriff, dies zu tun, während einige wenige Mitgliedstaaten dies noch nicht unternommen hatten.

- Die wichtigsten Aufgaben der CSIRTs bestehen in der Überwachung und Reaktion in Bezug auf Cybervorfälle, Frühwarnungen, Alarmmeldungen und Risiken- und Vorfallanalysen sowie im Aufbau der Zusammenarbeit mit dem Privatsektor.

- In einigen Mitgliedstaaten geht die Rolle der nationalen CSIRTs über diese Aufgaben hinaus, da sie Datenbanken über Bedrohungen und Vorfälle verwalten, den Austausch von Informationen zwischen den verschiedenen Einrichtungen unterstützen, Beratung und Unterstützung für den Schutz der Computersysteme des öffentlichen und des privaten Sektors bereitstellen, proaktive Maßnahmen zur Verringerung des Risikos von Computersicherheitsvorfällen ergreifen, Sensibilisierungs- und Schulungsmaßnahmen durchführen, als Mittler zwischen Privatsektor, Wissenschaft und Polizei auftreten und die nationale Kontaktstelle für die internationale Zusammenarbeit bilden.

- Staatliche CSIRTs sind überwiegend für das Krisenmanagement zuständig und ergreifen Maßnahmen zur Bewältigung von Cyberbedrohungen und -vorfällen, die den öffentlichen Sektor, aber in vielen Fällen auch kritische Infrastrukturen und in einigen Fällen den privaten Bereich – was jedoch in der Regel in den Zuständigkeitsbereich anderer CSIRTs im privaten Sektor fällt – betreffen.

- In einigen Mitgliedstaaten übernehmen die staatlichen CSIRTs Koordinierungs- und Überwachungsfunktionen für andere relevante Akteure, was sich als bewährtes Verfahren erwiesen hat; dies gilt insbesondere in denjenigen Mitgliedstaaten, in denen der Mechanismus zur Bewältigung von Cyberangriffen ziemlich komplex ist und/oder eine bedeutende Anzahl von verschiedenen CSIRTs sowohl im öffentlichen als auch im privaten Sektor parallel existiert.

- CSIRTs verfügen nicht über die Befugnisse der Strafverfolgungsbehörden gegenüber Privatpersonen, sondern spielen in Bezug auf Angriffe krimineller Art (nicht alle Cybervorfälle sind strafbare Handlungen) eine wichtige Rolle bei der Unterstützung der Ermittlungen, da sie zur Bereitstellung von Informationen und zur Sicherung von elektronischem Beweismaterial beitragen können. Daher ist es sehr wichtig, dass CSIRTs gut mit den Strafverfolgungsbehörden zusammenarbeiten, da die wirksame Erlangung von Informationen und Beweisen für die Ermittlung bei Cyberangriffen wichtig ist, vor allem in Anbetracht dessen, dass Daten sehr dynamisch sind und leicht verloren gehen können. Soweit erforderlich, können nachrichtendienstliche Einrichtungen in die Ermittlungen bei Cybervorfällen einbezogen werden.

- Gemäß der Richtlinie (EU) 2016/1148 (NIS-Richtlinie), die bis zum 9. Mai 2018 in nationales Recht umzusetzen ist, sollten die Mitgliedstaaten über gut funktionierende CSIRTs verfügen, die bestimmte Anforderungen erfüllen, um effiziente Kapazitäten zur Bewältigung von Vorfällen und Risiken und zur Sicherstellung einer wirksamen Zusammenarbeit auf Unionsebene zu gewährleisten.

- Digitale Widerstandsfähigkeit lässt sich nicht von staatlicher Seite alleine erreichen; auch dem privaten Sektor fällt hier eine wichtige Rolle zu, was insbesondere für Betreiber wesentlicher Dienste und von Informationssystemen sowie Netzbetreiber gilt, die direkt in das Risikomanagement und die Absicherung ihrer Netze und Dienste involviert sind.

- Gemäß der NIS-Richtlinie stellen die Mitgliedstaaten sicher, dass die Betreiber wesentlicher Dienste die Sicherheit ihrer Netze und Informationssysteme schützen und den zuständigen Behörden oder CSIRTs unverzüglich jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Bereitstellung eines Dienstes hat. Nach der vollständigen Umsetzung der NIS-Richtlinie werden Einrichtungen, die die Kriterien der Definition des Begriffs "Betreiber wesentlicher Dienste" erfüllen, daher rechtlich verpflichtet sein, Vorfälle zu melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben.

- Zum Zeitpunkt der Begutachtung gab es in einigen Mitgliedstaaten bereits eine Verpflichtung für den privaten Sektor, den Strafverfolgungsbehörden Cybervorfälle zu melden. In einigen Fällen allerdings galt diese Verpflichtung nur für bestimmte Teile des privaten Sektors oder für bestimmte Arten von Vorfällen, oder es gab keine Sanktionen bei Nichteinhaltung der Meldepflicht.

- In einigen Fällen erfolgt die Meldung auf freiwilliger Basis, obwohl keine förmliche Verpflichtung gilt; jedoch besteht, wie in einigen Gutachten hervorgehoben, häufig ein Meldungsdefizit, da die Anbieter die Schädigung ihres guten Rufs befürchten. Nach den Feststellungen der Begutachtung besteht ohne Meldepflicht die reale Gefahr, dass die meisten Cybervorfälle den Behörden nicht gemeldet werden. Wie in einem Einzelgutachten betont wird, können die Strafverfolgungsbehörden, um einen Anreiz zur Meldung zu setzen, betroffen Anbieter darauf hinweisen, dass die Ermittlungen geheim bleiben und gute Ergebnisse erzielt werden können, ohne dass ihr Ansehen leidet.

- Nach den Feststellungen der Begutachtung besteht ohne Meldepflicht allerdings die reale Gefahr, dass die meisten Cybervorfälle den Behörden nicht gemeldet werden.

- Eine Meldepflicht, insbesondere bei schweren Straftaten, ist nicht nur für Strafverfolgungszwecke – d. h. zur Erleichterung einer raschen und vollständigen Lageerfassung sowie zur schnelleren Umsetzung gezielter Gegenmaßnahmen – wichtig, sondern hilft den Behörden auch dabei, sich einen besseren Überblick über die Bedrohungen zu verschaffen, umfassende Statistiken über die Anzahl der Cybersicherheitsvorfälle zu führen und die richtigen Vorsichtsmaßnahmen zu ergreifen. Daher wurde die Festlegung eines geeigneten Rechtsrahmens, mit dem eine Meldepflicht eingeführt wird, wie in einigen Mitgliedstaaten geschehen, von den Gutachtern als gute Verfahrensweise angesehen.

- Zur Gewährleistung eines hohen Cybersicherheitsniveaus und sicherheitsbewusster Verhaltensweisen bei der Führungsebene und bei Entwicklern und Benutzern sind sicherheitsbezogene Verbesserungen erforderlich; aus diesem Grund ist die Sensibilisierung auf allen Ebenen, wie sie in bestimmten Mitgliedstaaten bereits erfolgt, ein wichtiger Bestandteil eines wirksamen Ansatzes für die Cybersicherheit.

- Da Cyberbedrohungen und -angriffe mitunter eine grenzübergreifende Dimension haben, erweist sich EMPACT als nützliche Plattform zur Verbesserung der Zusammenarbeit zwischen den Mitgliedstaaten, den einschlägigen Institutionen und Agenturen sowie den Partnern aus dem privaten Sektor im Hinblick auf die Produktion und Verbreitung von Software zur Bekämpfung von Schadsoftware (Anti-Malware) und auf die Abwehr von Netzangriffen auf die Infrastruktur.

- Erwähnenswert ist die enge Zusammenarbeit zwischen den CSIRTs der drei baltischen Staaten, die im November 2015 eine Vereinbarung unterzeichnet haben, in der sie zusagen, die Zusammenarbeit im Bereich der Cybersicherheit und des Schutzes der IT-Systeme und -netze zu intensivieren.

- Bei der Abwehr von Cyberangriffen außerhalb der EU wird der formelle Weg der Rechtshilfe beschritten. Da jedoch der Zeit bei Cyberkriminalität (aufgrund der Volatilität der Daten) entscheidende Bedeutung zukommen kann, werden auch die direkte Zusammenarbeit und der Informationsaustausch zwischen den Polizeikräften – direkt oder über Europol und Interpol – für eine schnellere und effizientere Zusammenarbeit genutzt. Einige Mitgliedstaaten nutzen auch das 24/7-Kontaktstellennetzwerk der G7.

- Die Digitale Agenda für Europa bietet einen Anreiz für die Mitgliedstaaten, bis 2012 ein gut funktionierendes Netzwerk aus nationalen CSIRTs einzurichten, das ganz Europa abdeckt. Die Europäische Kommission forderte die Mitgliedstaaten auf, die Zusammenarbeit zwischen den nationalen CSIRTs zu intensivieren und bestehende Kooperationsmechanismen wie die Gruppe der europäischen staatlichen CSIRTs zu erweitern.

- Kommunikation und Zusammenarbeit gibt es auch auf internationaler Ebene über die CSIRTs-Netzwerke, die – wie das International Watch and Warning Network (IWWN), FIRST, die European Government CERTs Group (EGC) und TF-CSIRT – weltweit gebildet wurden, um bei Cybervorfällen zu kooperieren, was die gegenseitige Unterstützung bei der Bewältigung von IT-Situationen und IT-Krisenmanagement einschließt; ein Beleg hierfür ist die Durchführung regelmäßiger Übungen. CSIRTs-Netzwerke können teils ähnliche Schwerpunkte, z. B. CSIRTs auf staatlicher/Behördenebene, und teils unterschiedliche Schwerpunkte haben, z. B. Teams aus Wirtschaft, Wissenschaft und Behörden.

**EMPFEHLUNGEN**

- ***Um ein angemessenes Schutz- und Sicherheitsniveau im nationalen Cyberraum sicherzustellen, sollten die Mitgliedstaaten für einen effizienten institutionellen Rahmen auf der Grundlage eines behördenübergreifenden Ansatzes sowie im Wege einer gut funktionierenden Zusammenarbeit zwischen allen einschlägigen Akteuren im Bereich der Cybersicherheit, einschließlich gegebenenfalls des Privatsektors, sorgen.***

- ***Im Einklang mit der NIS-Richtlinie sollten diejenigen Mitgliedstaaten, die dies noch nicht getan haben, ein nationales CSIRT einrichten. Zur Gewährleistung eines hohen Cybersicherheitsniveaus sollten die Mitgliedstaaten erwägen, ihre staatlichen CSIRTs mit Funktionen auszustatten, die es ihnen ermöglichen, als zentrale Koordinierungsstelle für andere CSIRTs und Akteure, die an der Verhütung von Cyberbedrohungen und der Reaktion auf Cybersicherheitsvorfällen beteiligt sind, zu agieren.***

- ***Zu diesem Zweck sollten die Mitgliedstaaten auch prüfen, die staatlichen CSIRTs mit der Sammlung und der Analyse von Cybervorfällen zu betrauen, ihre Fähigkeit zur Bewältigung von Bedrohungen zu verbessern und Softwaresysteme zu Frühwarnzwecken zu entwickeln und spezielle Schulungen zum Thema Cyberkriminalität und Cybersicherheit bereitzustellen.***

- ***Im Einklang mit der NIS-Richtlinie sollen die Mitgliedstaaten sicherstellen, dass die Betreiber wesentlicher Dienste Cybervorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, unverzüglich melden.***

- ***Die Mitgliedstaaten sind aufgerufen, sich an den EMPACT-Maßnahmen gegen Cyberangriffe sowie an dem in der NIS-Richtlinie vorgesehenen CSIRTs-Netzwerk und gegebenenfalls sonstigen Netzwerken dieser Art zu beteiligen.***

## XVII – ZUSAMMENARBEIT MIT EU-AGENTUREN

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Da die Cyberkriminalität im engeren Sinne und durch den Cyberraum ermöglichte Straftaten sowie deren Untersuchung häufig mehrere Mitgliedstaaten betreffen, stellen die Zusammenarbeit und der Austausch von Informationen mit den EU-Agenturen eine Priorität dar.

- Europol/EC3, Eurojust, EJN und ENISA spielen dabei eine wichtige Rolle mit einer großen Bandbreite von Tätigkeiten, darunter die Erstellung von Analysen zu den Trends im Bereich der Cyberkriminalität, Koordinierung internationaler Ermittlungen und internationaler Strafverfolgung, gegenseitiger Austausch von Informationen, Analyse von kriminalpolizeilichen Erkenntnissen, Beweismaterial und Daten und Beiträge zu Schulungsmaßnahmen auf EU-weiter Basis. Ihre Fachkenntnisse und Einrichtungen ermöglichen die gegenseitige Zusammenarbeit zwischen den Mitgliedstaaten und ihren jeweiligen Strafverfolgungsbehörden und Staatsanwaltschaften.

- Eurojust fällt eine wichtige Rolle bei der Koordinierung internationaler strafrechtlicher Ermittlungen und internationaler Strafverfolgung und der Bereitstellung von Rechtshilfe im Bereich der grenzüberschreitenden Zusammenarbeit sowie der Übermittlung von Beweismaterial zwischen den Mitgliedstaaten zu, was sich in komplexen Fällen von Cyberkriminalität als besonders nützlich erweist. Eurojust trägt auch dazu bei, die Zusammenarbeit mit den zuständigen Behörden von Mitgliedstaaten und von Drittstaaten im Bereich der Cyberkriminalität zu erleichtern und zu beschleunigen.

- Eurojust sammelt und verbreitet ferner Fallstudien und bewährte Verfahren, trägt zu Schulungsmaßnahmen im Bereich der Cyberkriminalität bei und fördert den Austausch von Erfahrungen zwischen fachkundigen Staatsanwälten und Richtern im Bereich der Cyberkriminalität, insbesondere durch Unterstützung des Europäischen Justiziellen Netzes gegen Cyberkriminalität.

- Europol erleichtert die Zusammenarbeit und den Austausch von Informationen zwischen den Mitgliedstaaten und stellt operative Produkte und Dienstleistungen für Ermittlungsdienste, kriminaltechnische und operative Schulung sowie Sensibilisierungsmaterialien bereit. Das "Europäische Zentrum zur Bekämpfung der Cyberkriminalität" (EC3) hat zum Ziel, die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU zu stärken und auf diese Weise dazu beizutragen, die europäischen Bürgerinnen und Bürger, Unternehmen und Regierungen vor Online-Kriminalität zu schützen. Das EC3 leistet in drei wichtigen Bereichen operative Unterstützung und Ermittlungsunterstützung für die nationalen Cyberkriminalitäts-Ermittlungsdienste: Online-Betrug, sexuelle Ausbeutung von Kindern im Internet und Cyberangriffe auf kritische Infrastrukturen und Informationssysteme in der Europäischen Union. Diese Tätigkeiten werden vom Team für Erkenntnisarbeit zu Cyberkriminalität (Cyber Intelligence Team - CIT) unterstützt, dessen Analysten Informationen zu Cyberkriminalität aus öffentlichen, privaten und offenen Quellen sammeln und verarbeiten und neue Bedrohungen und Muster ermitteln. Neben dem EC3 agiert die Gemeinsame Taskforce gegen die Cyberkriminalität (Joint Cybercrime Action Taskforce - J-CAT), die an den größten internationalen Fällen von Cyberkriminalität, die die Mitgliedstaaten der EU und ihre Bürgerinnen und Bürger betriffen, arbeitet. Die praktischen Erfahrungen zeigen, dass die frühe Einbeziehung der fachkundigen Verbindungsbeamten, die der J-CAT angehören, in die Koordinierung größerer Operationen gegen Cyberkriminalität einen zusätzlichen Nutzen hat.

- Die Mitgliedstaaten bekunden der Unterstützung und Koordinierung durch Europol/EC3, Eurojust und EJN über ihre Kontaktstellen allgemeine Anerkennung und betrachten ihre Rolle als entscheidend für die Stärkung des gegenseitigen Vertrauens zwischen den Ermittlungsbehörden und Staatsanwaltschaften sowie zur Erleichterung der internationalen Zusammenarbeit, auch mit Drittstaaten.

- Die Rolle der ENISA bei der Sammlung von Cyberwarnungen und deren Übermittlung durch automatisierte Systeme trägt ebenfalls entscheidend zur Stärkung der technischen Sicherheit der Informationssysteme bei.

- Allerdings sind die Dienste und Produkte, die Eurojust, Europol, EJN und ENISA hinsichtlich der Cyberkriminalität bereitstellen können, nicht immer vollständig bekannt und werden daher von den entsprechenden Praktikern in den Mitgliedstaaten nicht in vollem Umfang genutzt.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten die von Eurojust, EJN und Europol bereitgestellten Dienste und Produkte in Bezug auf Cyberkriminalität bestmöglich nutzen und eine enge Zusammenarbeit zwischen den nationalen CSIRTs und der ENISA sicherstellen.***

- ***Eurojust, Europol und die ENISA sollten erwägen, verstärkt auf ihre Dienste und die bestehenden Möglichkeiten der Zusammenarbeit und Spezialausbildung, die sie im Bereich Cyberkriminalität bieten, aufmerksam zu machen und aktiv Veranstaltungen zur Stärkung der internationalen Zusammenarbeit im Hinblick auf die Bekämpfung der Cyberkriminalität zu unterstützen.***

- ***Europol sollte ferner das SIENA-System bestmöglich in Ermittlungen einsetzen, die Sichtbarkeit von EMPACT-Projekten erhöhen, J-CAT möglichst optimal nutzen, den Mitgliedstaaten einen einheitlichen Ansatz für die strukturellen Elemente der kriminalpolizeilichen Datenbanken zur Bekämpfung von Cyberkriminalität vorschlagen und die Annahme einer gemeinsamen Taxonomie zur Cyberkriminalität fördern.***

- ***Die ENISA sollte untersuchen, wie sie das Konzept der Cyberwarnungen, die über automatisierte Systeme gesammelt und übermittelt werden, standardisieren könnte, sodass die Statistiken über diese Warnungen in allen Mitgliedstaaten vergleichbar und harmonisiert sind.***

## XVIII – GEMEINSAME ERMITTLUNGSGRUPPEN (GEG)

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Aufgrund der oftmals grenzübergreifenden Dimension der Cyberkriminalität kann die Beteiligung an international koordinierten Ermittlungen bei der wirksamen Verfolgung von Cyberkriminalität von Vorteil sein.

- Im Rahmen der EU bilden die gemeinsamen Ermittlungsgruppen (GEG) ein Instrument der internationalen Zusammenarbeit in grenzüberschreitenden Fällen; dies erfolgt auf der Grundlage einer Vereinbarung zwischen den zuständigen Behörden zweier oder mehrerer Mitgliedstaaten – in den Bereichen Justiz und Strafverfolgung – zur gemeinsamen Durchführung strafrechtlicher Ermittlungen.

- Zum Zeitpunkt der Begutachtung hatten sich mehrere Mitgliedstaaten an gemeinsamen Ermittlungsgruppen in Bezug auf Cyberstraftaten beteiligt, einige davon häufiger als andere, während dies bei weiteren Mitgliedstaaten noch nie der Fall gewesen ist.

- Die Beteiligung an gemeinsamen Ermittlungsgruppen wird von den teilnehmenden Mitgliedstaaten allgemein als positive Erfahrung dargestellt; diese Mitgliedstaaten betrachten die gemeinsamen Ermittlungsgruppen als wirksames Instrument für die Durchführung grenzüberschreitender Ermittlungen, da ein direkter Informationsaustausch zwischen den Ermittlern und eine rechtzeitige Beweiserhebung ermöglicht wird, ohne gesonderte formelle Rechtshilfeersuchen stellen zu müssen.

- Angesichts der langwierigen Rechtshilfeverfahren trägt die Nutzung von GEG zur zeitlichen Verkürzung von Ermittlungen sowie zur Stärkung des Vertrauens zwischen den nationalen Behörden bei.

- Obwohl die Beteiligung von Europol und Eurojust bei der Einsetzung der GEG und bei deren Tätigkeit nicht vorgeschrieben ist, wie von einigen Mitgliedstaaten angegeben, können die beiden Stellen eine wichtige Rolle dabei spielen, die Effizienz und operative Fähigkeit der GEG sicherzustellen. Die Möglichkeit der Finanzierung von gemeinsamen Ermittlungsgruppen durch Eurojust und Europol wird von einigen Mitgliedstaaten als entscheidend angesehen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten werden ermutigt, die Praktiker für die Möglichkeiten und Vorteile einer GEG und deren Nutzung in Fällen der Cyberkriminalität zu sensibilisieren, um die Ermittlungen wirksamer zu gestalten.***

- ***Die Organe, Einrichtungen und sonstigen Stellen der EU, insbesondere Eurojust und Europol, sollten die Bildung gemeinsamer Ermittlungsgruppen weiterhin unterstützen und fördern und angemessene Finanzmittel bereitstellen, sodass die Mitgliedstaaten die gemeinsamen Ermittlungsgruppen häufiger nutzen können.***

## XIX – RECHTSHILFE

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Für die wirksame Bekämpfung der Cyberkriminalität sind aufgrund ihres überwiegend grenzübergreifenden Charakters oftmals eine reibungslose und gut funktionierende internationale Zusammenarbeit und die Nutzung der Rechtshilfe erforderlich.

- Die nationalen Rechtsvorschriften der Mitgliedstaaten enthalten keine spezifischen Bestimmungen über Rechtshilfeersuchen in Fällen der Cyberkriminalität, sodass die allgemeinen Verfahren und Bedingungen für die Rechtshilfe gelten.

- Die meisten Mitgliedstaaten sind Vertragsparteien des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (Rechtshilfeübereinkommen), das gemäß Artikel 34 des Vertrags über die Europäische Union und dessen Zusatzprotokoll von 2001 abgeschlossen wurde. Sie beteiligten sich ferner am Schengen-Besitzstand und wenden ihn an; aufgrund dieses Besitzstands finden die Bestimmungen über die justizielle Zusammenarbeit im Schengener Übereinkommen ebenfalls Anwendung, was insbesondere für Mitgliedstaaten, die nicht Vertragsparteien des Rechtshilfeübereinkommens sind, relevant ist. Bei Mitgliedstaaten, die weder Vertragsparteien der oben genannten multilateralen Übereinkünfte noch von bilateralen Abkommen sind, basiert die Rechtshilfe auf dem Grundsatz der Gegenseitigkeit.

- Justiziellen Rechtshilfeersuchen gehen in der Regel Ersuchen um eine umgehende Sicherung gespeicherter Computerdaten als elektronisches Beweismaterial gemäß Artikel 29 des Budapester Übereinkommens vom 22. November 2001 über Computerkriminalität voraus.

- Die Frist für die Beantwortung eines Rechtshilfeersuchens kann einige Monate betragen, hängt aber von verschiedenen Umständen ab, beispielsweise der Frage, ob die Rechtshilfe auf der Grundlage eines internationalen Abkommens oder der Gegenseitigkeit bereitgestellt wird; im letzteren Fall ist die Antwortzeit sogar noch länger, da die Zusicherung der Gegenseitigkeit zuerst noch empfangen/gewährt werden muss.

- In dem sich rasch verändernden Bereich der Cyberkriminalität führt die Langwierigkeit der Rechtshilfeverfahren dazu, dass sie eher ineffizient sind, was sich negativ auf die Durchführung und den Erfolg der Ermittlungen auswirkt, da elektronisches Beweismaterial flüchtig ist und Daten im Falle von Verzögerungen verloren gehen können. Deshalb erscheint es allgemein notwendig, die Bearbeitung von Rechtshilfeersuchen bei Ermittlungen von Cyberstraftaten zu straffen. Die Verbesserung der Qualität von Rechtshilfeersuchen kann sich erheblich auf die Beschleunigung ihrer Ausführung in anderen Ländern auswirken.

- Als Alternative zum offiziellen Weg der Rechtshilfeersuchen nutzen einige Mitgliedstaaten die Kanäle von Europol, Eurojust und EJN, wie z. B. J-CAT (EC3), oder Interpol, das Kontaktstellennetzwerk der G7, Netzwerke von Verbindungsbeamten oder bilaterale Kontakte, um schnellere Reaktionen zu erhalten; allerdings ist zu berücksichtigen, dass die Zulässigkeit der Daten als Beweismaterial vor Gericht überprüft werden muss, wenn diese weniger formellen Kanäle genutzt werden.

- Die Unterstützung, die Eurojust zur Erleichterung der Kommunikation sowie zur Beschleunigung der Ausführung dringender Anfragen nicht nur gegenüber Mitgliedstaaten, sondern auch gegenüber Drittländern bereitstellt, wird als sehr nützlich angesehen, vor allem in Anbetracht der Anwesenheit von als Verbindungsbeamten dienenden Staatsanwälten aus den USA, Norwegen und der Schweiz bei Eurojust.

- Wie in vielen Einzelgutachten angegeben, beziehen sich viele der Rechtshilfeersuchen in Bezug auf Cyberkriminalität auf die Erlangung bestimmten Beweismaterials im Besitz von Diensteanbietern. Da viele Diensteanbieter im Hoheitsgebiet der USA ansässig sind, wird im Hinblick auf Drittländer Rechtshilfe in Strafsachen im Bereich Cyberkriminalität in erster Linie in und von den Vereinigten Staaten beantragt, mit denen eine reibungslose Zusammenarbeit überaus wichtig ist.

- Viele Mitgliedstaaten haben jedoch Schwierigkeiten in dieser Hinsicht, insbesondere auf dem Gebiet der Vorratsdatenspeicherung und der Weitergabe der IP-Adressen von Kontoinhabern bei Facebook und anderen sozialen Netzwerken. Wie von den Gutachtern in einigen Einzelgutachten angegeben, ist die Frage der Datenbankzugänglichkeit der sozialen Netzwerke mit Ursprung in den USA ein ständiges Problem, von dem alle Mitgliedstaaten betroffen sind.

- Die USA stellen hohe formale und inhaltliche Anforderungen an solche Ersuchen, insbesondere in Bezug auf den Zusammenhang zwischen der Straftat und dem konkreten Beweismaterial, um dessen Übermittlung ersucht wird.

- Nach den Ergebnissen der Begutachtung wäre es sinnvoll, an internationalen Lösungen zur Verbesserung der Rechtshilfeverfahren mit Drittstaaten wie den USA zu arbeiten. Die Verwendung eines Formulars für Anträge auf umgehenden Erlass einer Anordnung mit Zustimmung der Vollstreckungsbehörden in einem bestimmten Staat kann als gute Verfahrensweise angesehen werden kann.

- Nach den einschlägigen Rechtsvorschriften der Vereinigten Staaten über eine Durchsuchung einer Online-Quelle oder die Erlangung von E-Mail-Daten und Inhalten einer bei einem Diensteanbieter gespeicherten Kommunikation ist ein Durchsuchungsbefehl erforderlich, der das Kriterium des "hinreichenden Verdachts" erfüllen sollte. Dieses Verfahren ist sehr zeitaufwändig und führt in vielen Fällen nicht zur Erledigung des Ersuchens.

- Einige Mitgliedstaaten erklärten, dass sich informelle und persönliche Kontakte mit den zuständigen Behörden von Drittstaaten vor Übermittlung eines Rechtshilfeersuchens als nützlich erwiesen haben, um eine bessere und schnellere Erledigung solcher Ersuchen sicherzustellen.

- Die Einrichtung eines Registrierungssystems für Rechtshilfeersuchen und eines entsprechenden Verwaltungssystems würde es ermöglichen, dass eine Rechtssache von der Registrierung bis zur Antwort an das ersuchende Land verfolgt werden kann, und kann daher als gute Vorgehensweise betrachtet werden.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten sondieren, wie die Qualität der Rechtshilfeersuchen, die sie an andere Länder übermitteln, weiter verbessert werden kann, insbesondere, um zu gewährleisten, dass sie hinreichend vollständig sind, und sollten Methoden prüfen, um die Antworten auf Rechtshilfeersuchen zu beschleunigen und die Qualität solcher Antworten zu verbessern.***

- ***Den Mitgliedstaaten wird empfohlen, die Effizienz des Kommunikationsprozesses mit anderen Mitgliedstaaten und Drittländern zu verbessern und die Festlegung von Methoden zu prüfen, mit denen eine Rechtssache von der Registrierung bis zur Antwort an das ersuchende Land verfolgt werden kann, beispielsweise ein Registrierungssystem für Rechtshilfeersuchen.***

- ***Die Mitgliedstaaten werden aufgefordert, die Instrumente von Eurojust, EJN und Europol stärker zu nutzen und informelle Kontakte mit den zuständigen ausländischen Behörden im Hinblick auf schnellere Antworten auf Rechtshilfeersuchen aus Drittländern aufzubauen.***

- ***Die EU sollte weiter an Lösungen zur Verbesserung und Beschleunigung der Kommunikation zwischen Mitgliedstaaten und Drittländern, insbesondere den USA, arbeiten, vor allem im Hinblick auf den Austausch operativer Informationen sowie auf die Erledigung von Rechtshilfeersuchen.***

- ***Die EU sollte in Erwägung ziehen, einen Rahmen für eine direkte Zusammenarbeit mit den entsprechenden Diensteanbietern außerhalb der EU zu schaffen.***

## XX – SCHULUNG

### WICHTIGSTE FESTSTELLUNGEN UND SCHLUSSFOLGERUNGEN

- Angesichts des raschen technologischen Fortschritts und des sich wandelnden Charakters der Cyberkriminalität und der deshalb notwendigen Anpassung an neue Entwicklungen und ausgefeiltere Modi Operandi sind regelmäßige und kontinuierliche Fachschulungen zum Thema Cyberkriminalität und Cybersicherheit für Praktiker auf allen Ebenen, auch am Anfang ihrer beruflichen Laufbahn, von entscheidender Bedeutung für erfolgreiche Ermittlungen und die erfolgreiche strafrechtliche Verfolgung von Cyberkriminalität im engeren Sinne und von durch den Cyberraum ermöglichten Straftaten.

- In den meisten Mitgliedstaaten werden erhebliche Anstrengungen, Mittel und Humanressourcen in Fachschulungen im Bereich der Cyberkriminalität für die Strafverfolgungsbehörden investiert, wobei nicht alle Mitgliedstaaten das gleiche Ausbildungsniveau in der Justiz aufweisen und in einigen Mitgliedstaaten Schulungen für die Justiz, sofern sie angeboten werden, nicht vorgeschrieben sind.

- Vor dem Hintergrund der technischen Besonderheiten der Cyberkriminalität bedarf es indes bei den Strafverfolgungsbehörden, aber auch bei den für die betreffenden Fälle zuständigen Richtern eines hohen Kenntnisniveaus, sodass Fachschulungen – auch in Bezug auf die Erhebung, Analyse und Verwendung elektronischen Beweismaterials – ebenfalls von grundlegender Bedeutung für die mit Cyberkriminalität befassten Strafverfolgungsbehörden, Staatsanwälte und Richter sind.

- In einigen Mitgliedstaaten werden zusätzlich zu den von öffentlichen Stellen (Polizei- oder Justizakademien oder -einrichtungen usw.) bereitgestellten Schulungen auch Schulungen zum Thema Cyberkriminalität von externen Einrichtungen, wie z. B. Hochschulen und privaten Unternehmen, die in diesem Sektor tätig sind und deren Fachkenntnisse sich für eine qualitativ hochwertige Schulung als sehr nützlich erweisen, oder von NRO bereitgestellt. Einige Mitgliedstaaten haben hoch spezialisierte Exzellenzzentren für die Schulung im Bereich Cyberkriminalität eingerichtet.

- In einigen Mitgliedstaaten wird eine solche Aus- und Fortbildung auch in Form von Fernunterricht, E-Learning oder auch Podcasts angeboten, was als gute Vorgehensweise und effektive Schulungsmethode angesehen werden kann.

- Zusätzlich zu Schulungsmaßnahmen auf nationaler Ebene stellen auch einschlägige Stellen der EU – EC3/Europol, ECTEG *(European Cybercrime Training and Education Group)*, Eurojust, OLAF, CEPOL und ENISA – spezielle Schulungen zum Thema Cyberkriminalität bereit oder tragen zu ihnen bei; im Allgemeinen wird diese Möglichkeit von den Mitgliedstaaten jedoch nicht voll ausgeschöpft.

- Einige Mitgliedstaaten verfügen über einen speziellen Haushaltsrahmen für Schulungen im Bereich Cyberkriminalität. In einigen Mitgliedstaaten sollten weitere Anstrengungen unternommen werden, um die Fachschulungen zum Thema Cyberkriminalität für alle Kategorien von Beamten, die an solchen Fällen beteiligt sind, zu verbessern.

- Nach den Feststellungen der Begutachtung kann ein integrierter Ansatz für die gemeinsame Schulung von Richtern, Staatsanwälten und Strafverfolgungsbehörden dazu beitragen, die Kenntnisse über Cyberkriminalität zu verbessern, und kann als Plattform für den Austausch von Erfahrungen und bewährten Verfahren in Bezug auf Cyberkriminalität sowie für die Erörterung der Hindernisse in Bezug auf die Zulässigkeit von Beweismitteln fungieren. Die gegenseitige Begutachtung ergab, dass nur wenige Mitgliedstaaten bereits über diese Art von gemeinsamen Schulungen verfügen.

**EMPFEHLUNGEN**

- ***Die Mitgliedstaaten sollten ein umfassendes, den gesamten Lebenszyklus von Cyberkriminalitätsfällen abdeckendes Schulungsangebot für alle Interessenträger und Praktiker im Bereich der Bekämpfung von Cyberkriminalität und insbesondere mehr regelmäßige Schulungen für die Justiz bereitstellen und die Zuweisung von Haushaltsmitteln für Schulungen zum Thema Cyberkriminalität in Erwägung ziehen.***

- ***Die Mitgliedstaaten sollten erwägen, gemeinsame Schulungen im Bereich Cyberkriminalität für Strafverfolgungsbehörden, Staatsanwälte und Richter abzuhalten und E-Learning-Methoden zu nutzen.***

- ***Die Mitgliedstaaten sollten die Ausbildungsmöglichkeiten, die sowohl von Einrichtungen der EU wie beispielsweise EC3/Europol, ECTEG, Eurojust, OLAF, CEPOL und ENISA als auch von akademischen Einrichtungen und Privatunternehmen bereitgestellt werden, bestmöglich nutzen und die Einrichtung von Exzellenzzentren zur Bereitstellung von Fachschulungen zum Thema Cyberkriminalität in Betracht ziehen.***

- ***Die Organe der EU sollten die EU-Finanzmittel für die Unterstützung der Mitgliedstaaten bei der Organisation einer stärker spezialisierten Ausbildung der nationalen Praktiker in Bezug auf Cyberkriminalität erhöhen.***