Zusammenfassung

Es gibt mehrere Faktoren, die die Bekämpfung von Cyberkriminalität einzigartig und schwierig machen. Cyberkriminalität ist naturgemäß grenzenlos und entwickelt sich rasch, manchmal schneller als nationale Behörden reagieren können. Durch den horizontalen Charakter der Cyberkriminalität wird das Problem noch komplexer: fast jede Art von Kriminalität kann heutzutage im Internet auftreten. Elektronische Beweismittel für solche Straftaten können aufgrund der Volatilität der Daten schwer zu erheben sein und besondere Fachkenntnisse erfordern. Die justizielle Zusammenarbeit ist für die rechtzeitige Sicherung elektronischer Beweismittel unverzichtbar, um deren Zulässigkeit in Gerichtsverfahren zu gewährleisten. Die internationale justizielle Zusammenarbeit kann durch erhebliche Unterschiede in den nationalen Rechtsrahmen (z. B. in Bezug auf strafbares Verhalten oder Vorschriften über die Vorratsdatenspeicherung) und durch Zuständigkeitskonflikte erschwert werden. Das gesamte Phänomen der Cyberkriminalität verändert das traditionelle Rechtskonzept des Territorialitätsprinzips aufgrund des supranationalen Charakters der Beweismittel, die erforderlich sind, um eine erfolgreiche Verfolgung von Cyberkriminellen zu gewährleisten.

Daher erfordert eine wirksame nationale Reaktion auf Cyberkriminalität häufig eine Zusammenarbeit auf mehreren Ebenen. Eine verstärkte internationale Zusammenarbeit ist von entscheidender Bedeutung, da der Cyberraum international und grenzüberschreitend ist. „Cybersicherheitsstrategie der Europäischen Union: Ein offener, sicherer und geschützter Cyberraum“ legt den Schwerpunkt auf die Schaffung eines Cyberraums, der den Zugang zum Internet fördert und das Wachstum des Marktes sicherstellt, gleichzeitig aber darauf abzielt, eine Abwehrfähigkeit gegenüber Cyberangriffen zu erreichen und Cyberkriminalität zu bekämpfen, wobei ein angemessenes Gleichgewicht zwischen den Grundrechten der Bürgerinnen und Bürger einerseits und der Rechtsstaatlichkeit anderseits gewahrt wird ([1]). Darüber hinaus fördert die Strategie den Einsatz von Instrumenten der internationalen Zusammenarbeit bei der Bekämpfung der Cyberkriminalität sowie die damit verbundene polizeiliche und justizielle Zusammenarbeit in Drittländern, in denen Cyberkriminelle tätig sind. ([2]).

Die Schlussfolgerungen des Rates zu „Abwehrfähigkeit, Abschreckung und Abwehr“: die Cybersicherheit in der EU wirksam erhöhen’ ([3]) ergänzen die Cybersicherheitsstrategie der EU, indem sie die Notwendigkeit hervorheben, böswillige Cyberaktivitäten zu verhindern, abzuschrecken, zu erkennen und darauf zu reagieren. Sie betonen, dass den Behörden die Instrumente zur Aufdeckung, Ermittlung und Verfolgung von Cyberkriminalität zur Verfügung gestellt werden müssen.

Eurojust konzentriert sich auf die Bekämpfung der Cyberkriminalität mit dem Ziel, die justizielle Zusammenarbeit in diesem Bereich zu stärken, insbesondere durch die Erleichterung der zügigen Bearbeitung justizieller Rechtshilfeersuchen – ein entscheidender Faktor bei der Lösung des Problems der Datenvolatilität und der Schließung von Lücken, die sich aus der Anwendung unterschiedlicher nationaler Vorschriften für die Vorratsdatenspeicherung ergeben – sowie durch die frühzeitige Einbeziehung der Justiz in Cyberstraftaten, um sicherzustellen, dass die Daten während der Ermittlungsphase gemäß den geltenden Vorschriften erhoben werden und somit in nachfolgenden Gerichtsverfahren als zulässiges elektronisches Beweismaterial vorgelegt werden können. Darüber hinaus produziert Eurojust entweder strategische Produkte im Bereich der Cyberkriminalität oder trägt wesentlich zur Herstellung solcher Produkte bei, wodurch Fachleute bei der Entwicklung der erforderlichen Cyberspezifikationen unterstützt werden ([4]).

([1]) Rat der Europäischen Union, Schlussfolgerungen des Rates zur gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik zur Cybersicherheitsstrategie der Europäischen Union: Ein offener, sicherer und geschützter Cyberraum, Brüssel, 22.7.2013 (12109/13)

([2]) Eurojust engagiert sich für mehrere Projekte zum Kapazitätsaufbau im Bereich der Cyberkriminalität, wie das Sirius-Projekt (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), das Europa-Mittelmeer-Projekt Justiz (https://www.euromed-justice.eu/) und das Projekt GLACY+ (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Rat der Europäischen Union, Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, Brüssel, 20.11.2017 (14435/17).

([4]) Weitere Informationen finden Sie im Abschnitt „Veröffentlichungen und Projekte von Eurojust im Bereich Cyberkriminalität“ im

Dieser Bericht soll einen Überblick über die Arbeit von Eurojust im Bereich der Cyberkriminalität geben. Die operative Arbeit von Eurojust bietet einen ausgezeichneten Einblick in die gemeinsamen Herausforderungen, mit denen Fachleute konfrontiert sind, sowie in bewährte Verfahren zur Bewältigung dieser Herausforderungen. Die Fallarbeit von Eurojust ist eine nützliche Informationsquelle über besondere Hindernisse für die justizielle Zusammenarbeit und darüber, wie diese überwunden werden können, und trägt zur Diskussion darüber bei, wie das Phänomen der Cyberkriminalität am besten angegangen werden kann. Die Erfolgsgeschichte ist ein Kapitel, in dem Fallbeispiele vorgestellt werden. Schließlich werden die Veröffentlichungen und Projekte von Eurojust, die für den Bereich Cyberkriminalität von Interesse sind, aufgelistet.

vorliegenden Dokument.