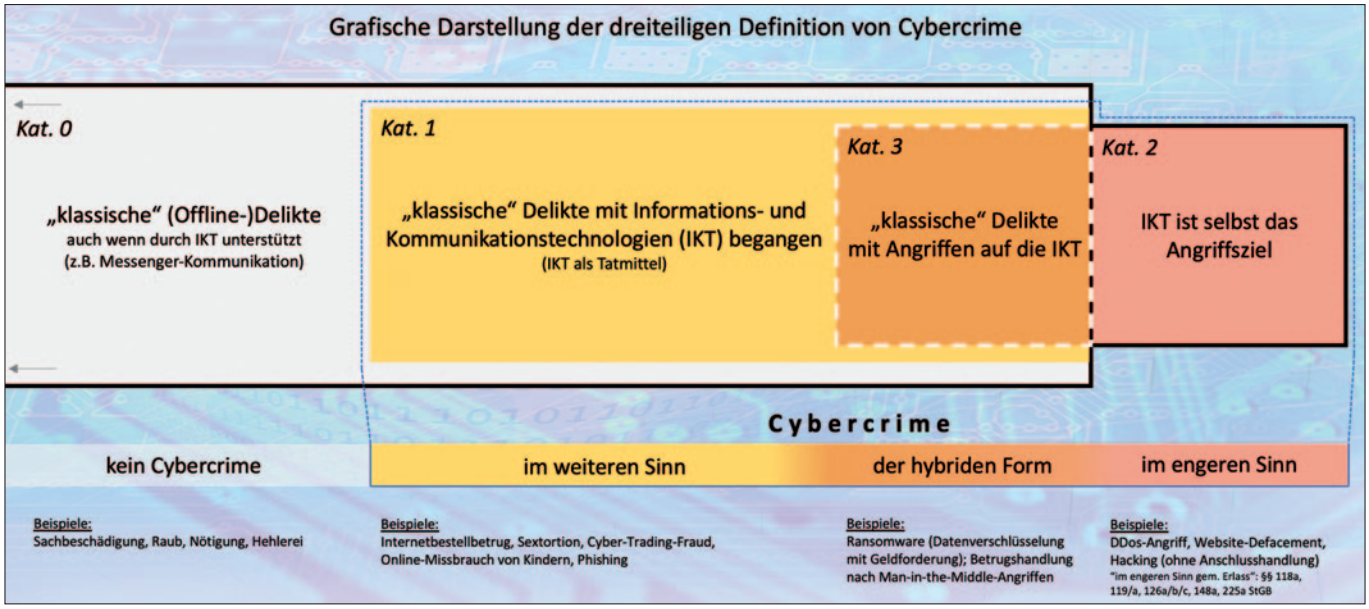


Grafische Darstellung der Definition von Cybercrime samt weiterer Detailspezifizierungen

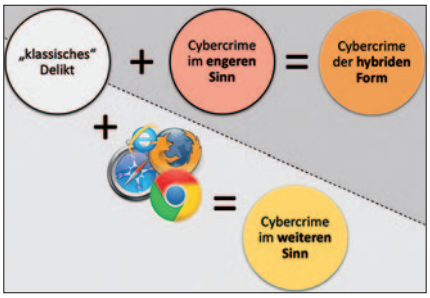
Die Dreiteilung von Cybercrime

Neben der Einteilung von Cybercrime im engeren und im weiteren Sinne gibt es die Kategorie „Cybercrime der hybriden Form".

Die zunehmende Digitalisierung der Gesellschaft führt auch zu einer Zunahme krimineller Aktivitäten im Internet. Dies stellt eine Herausforderung für die Polizei dar, insbesondere im Hinblick auf die Spurensicherung. Zudem ist die Dunkelziffer der Internetkriminalität als außerordentlich hoch einzuschätzen (Baier 2020, Rüdiger 2019).* Das bisherige Begriffsverständnis von Cybercrime im engeren und Cybercrime im weiteren Sinne scheint dieser Deliktsmenge nicht mehr gerecht zu werden, da es für ein organisatorisches Regelwerk der kriminalpolizeilichen Aufgabenwahrnehmung zu holzschnittartig ist.

Drei Kategorien. In der öffentlichen Diskussion werden die Begriffe Internetkriminalität und Computerkriminalität im Wesentlichen gleichbedeutend verwendet. Es gibt jedoch keine einheitliche Definition, was genau darunter zu verstehen ist.

Das Bundeskriminalamt unterscheidet zwischen Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten („Cybercrime im engeren Sinn") oder mittels Informationstechnologie begangen werden („Cybercrime im weiteren Sinn"). Diese Kategorisierung ist international am weitesten verbreitet: Der Begriff „cyber-abhängige Straftaten" ist demnach gleichbedeutend mit Cybercrime im engeren Sinne, während der Begriff „cyber-gestützte Straftaten" als Cybercrime im weiteren Sinne verstanden werden kann.



Cybercrime: Eine neue, dritte Kategorie (hybride Form) ergibt sich durch die Kombination zweier Aspekte

Neben dieser zweiteiligen Kategorisierung gibt es international dreiteilige Kategorisierungen, die zusätzlich den Begriff „cyber-assisted crime" kennen. Darunter versteht man den Einsatz von Computern bei klassischen Straftaten, bei denen die Informationstechnologie die Tatbegehung erleichtert, etwa wenn die Täter das Internet zur Kommunikation nutzen oder mögliche Einbruchsobjekte mit Hilfe von Satellitenbildern aus dem Internet auskundschaften. Diese dritte Kategorie ist jedoch nicht dem Begriff „Cybercrime" zuzuordnen. Vielmehr handelt es sich dabei um ein Tätigkeitsfeld der IT-Forensik, bei dem die digitale Spurensicherung (z. B. Sicherung von Chatverläufen) bei klassischen (offline) Straftaten zum Einsatz kommt. Analoge und digitale Spurensicherung greifen zunehmend ineinander.

Die Einteilung von Cybercrime sollte dennoch auf drei Grobkategorisierungen erweitert werden. Neben Cybercrime im engeren und weiteren Sinne erscheint eine dritte „neue" Kategorie – die hybride Form – sinnvoll:

Cybercrime der hybriden Form liegt vor, wenn klassische Delikte (1) mit einem Angriff auf Informations- und Kommunikationstechnologien (2) kombiniert werden.

Ein Beispiel hierfür ist ein Ransomware-Angriff: (1) Die Forderung des Täters nach Zahlung eines „Lösegeldes" für die Freigabe der verschlüsselten Daten erfüllt den Tatbestand der Erpressung (§ 144 StGB = klassisches Delikt). Während (2) das vorherige Einschleusen von Schadprogrammen in fremde Computersysteme zur Verschlüsselung von Daten (§ 126a StGB) Cybercrime im engeren Sinne darstellt. 1 + 2 = Cybercrime der hybriden Form. Die Grafik in der Mitte zeigt (mit den

Grafiken: Alexander Riedler

schwarz umrandeten Kreissymbolen), dass es grundsätzlich nur „klassische“ Straftaten und speziell definierte Cybercrime im engeren Sinne gibt. Während die hybride Form aus der Kombination dieser beiden Deliktsformen entsteht, definiert sich Cybercrime im weiteren Sinne als Kombination eines klassischen Delikts mit der Tatbegehung „im Internet“.

Sinnvolle Kategorisierung von Cybercrime. Die Betrachtung der unterschiedlichen Definitionen führt zu einem neuen Kategorisierungsvorschlag für Cybercrime, der in der großen Grafik auf der vorderen Seite in vereinfachter Form dargestellt ist. Diese Darstellung baut auf den etablierten Bezeichnungen Cybercrime im engeren und weiteren Sinne auf und ergänzt diese um die soeben vorgestellte dritte Kategorie Cybercrime der hybriden Form:

- *Kategorie 0 (kein Cybercrime)* = „Klassische“ (offline) Delikte. Hierbei handelt es sich um Straftatbestände, die in der analogen Welt passieren und eventuell unter Zuhilfenahme von IKT (cyber-unterstützte Kriminalität) begangen wurden (z. B. bewaffneter Raub – mit Bestellung der Waffe im Internet).
- *Kategorie 1 (Cybercrime im weiteren Sinn)* = „Klassische“ Delikte unter Zuhilfenahme von IKT als Tatmittel (z. B. Betrug über Internetverkaufsplattformen).
- *Kategorie 2 (Cybercrime im engeren Sinn)* = IKT ist selbst das Angriffsziel.
- *Kategorie 3 (Cybercrime der hybriden Form)* = „Klassische“ Delikte mit Angriffen auf die IKT (z. B. Datenverschlüsselung mit Lösegeldforderung als Form der Datenbeschädigung in Verbindung mit Erpressung).

Diese neue Vierteilung (Kat. 0 bis 3) aller Straftaten bzw. Dreiteilung von Cybercrime (Kat. 1 bis 3) soll helfen, den Begriff „Cybercrime“ handhabbar zu machen. Eine solche Definition erscheint hilfreich, wenn es darum geht, organisatorische Zuständigkeiten im Zusammenhang mit der Bekämpfung von Cybercrime festzulegen. So könnten sich technisch spezialisierte Cybercrime-Einheiten sinnvollerweise auf die Kategorien 2 und 3 konzentrieren. Bei Sachverhalten der Kategorie 1 werden die bekannten deliktischen Zuständigkeitsregelungen der Ermittlungseinheiten nicht durchbrochen.

Bei komplexen und/oder komplizierten Ermittlungen innerhalb der Kategorie 1 kann jedoch eine spezialisierte Cybercrime-Einheit kooperativ tätig werden.

Alexander Riedler

Der Autor, Alexander Riedler, BA MA MA MSc ist in der Kriminaldienstreform des Bundeskriminalamts Leiter der Arbeitsgruppe Cybercrime im Fachbereich Land/Bezirk. Er war in Oberösterreich für die Errichtung des Piloten zu einer Cybercrime-Einheit sowie eines Cybercrime-Training-Centers verantwortlich.

Anmerkungen:

** Vgl. Rüdiger, Thomas-Gabriel (2019): Haben wir eine Unrechtskultur im digitalen Raum? In: Kriminalistik. Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis. Ausgabe 1/2019, S. 37-41.*

Vgl. Baier, Dirk (2020): Cybercrime-Opfererfahrungen in der Schweiz. In: Kriminalistik. Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis. Ausgabe 6/2020, S. 407-413.