Harchuk Nataliya, *Senior Teacher of Foreign languages Department of the National Academy of Internal Affairs*

CYBERKRIMINALITÄT IN DEUTSCHLAND

Die moderne Gesellschaft ist global vernetzt, wir kommunizieren in Sekundenschnelle mit Freunden, Bekannten und Geschäftspartnern weltweit. Mit den positiven Möglichkeiten der Internetnutzung gehen aber auch negative Begleiterscheinungen einher: Cyberkriminellen bieten sich vielfältige Tatgelegenheiten. Straftaten verlagern sich ins Internet, neue Kriminalitätsphänomene entstehen.

Die Kategorie Cyberkriminalität umfasst die beiden Bereiche *Computerkriminalität* und *Internetkriminalität*. Unter dem Begriff Computerkriminalität werden in Deutschland Straftaten eingeordnet, bei denen lediglich ein Computer ohne die Verwendung des Internets genutzt wird. Formen der Computerkriminalität können dabei die Computersabotage, der Computerbetrug, die Computerspionage, die Softwarepiraterie oder der Computermissbrauch sein.

Die Bezeichnung Internetkriminalität schließt in der Unterscheidung zur Computerkriminalität Straftaten ein, die mit den Techniken des Internets begangen werden oder auf dem Internet basieren. Da mittlerweile nahezu jede Straftat der Cyberkriminalität im Kontext mit der Verwendung des Internets steht, stellt die Internetkriminalität einen starken Schwerpunkt im Bereich der Cyberkriminalität dar.

Die Statistiken des Bereichs Cyberkriminalität zeigen unter anderem die Entwicklung der Fallzahlen von einzelnen Formen der Computer- oder Internetkriminalität in Deutschland, die finanziellen Schäden durch Cyberkriminalität sowie die Länder mit dem höchsten Aufkommen von Schadprogrammen. Die Umfragen beleuchten den Informationsstand zur Cyberkriminalität, die Änderung der Internetgewohnheiten in Deutschland aufgrund von Sicherheitsbedenken, den Grad der Besorgnis sowie die wirkliche Wahrnehmung vor einzelnen Formen der Cyberkriminalität.

Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.

Aktuell verbreitete Erscheinungsformen von Cybercrime sind gekennzeichnet durch die Infektion und Manipulation von Computersystemen mit Schadsoftware, z.B.:

- persönliche Daten und Zugangsberechtigungen des Nutzers abgreifen und missbräuchlich nutzen zu können (Identitätsdiebstahl)
- darauf befindliche Daten / Dateien des Nutzers mittels sog. Ransomware, zu verschlüsseln, um "Lösegeld" zu erpressen,
- sie "fernsteuern" zu können, in sog. Botnetzen zusammenzuschalten und für weitere kriminelle Handlungen einzusetzen.

Bei Cybercrime ist von einem sehr großen Dunkelfeld auszugehen. Das heißt, dass vermutlich nur ein kleiner Teil der Straftaten in diesem Bereich zur Anzeige gebracht wird bzw. der Polizei und/oder den Strafverfolgungsbehörden bekannt ist.

Im Bundeskriminalamt wurden frühzeitig Einheiten aufgebaut, die sich mit den Erscheinungsformen der Cybercrime befassen Zur Durchführung von Ermittlungsverfahren, der Koordinierung nationaler und internationaler Aktivitäten, der Analyse und Lagebeschreibung aktueller Cybercrime-Phänomene besteht im BKA die Gruppe SO 4 – Cybercrime der *Abteilung Schwere und Organisierte Kriminalität (SO)*

Innerhalb dieser Einheit befinden sich u.a. folgende Arbeitsbereiche:

- ✓ Zentrale Ansprechstelle Cybercrime (ZAC)
- ✓ Operative Auswertung Cybercrime
- ✓ Ermittlungsunterstützung / Internetrecherche
- ✓ Zentralstelle Sexualstraftaten z.B. von Kindern und Jugendlichen

Cyberkriminalität kann in verschiedensten Formen vorliegen, also durch dieVerwirklichung diverser Straftatbeständezutage treten. In der Cybercrime-Konvention des Europarats werden für die Internetkriminalität als Beispiele Verbrechen wieDatenmissbrauch oder auchUrheberrechtsverletzungen genannt.

In dem Handbuch zur Vorbeugung und Kontrolle von Computerverbrechen (englisch: Manual on the Prevention and Control of Computer Related Crime) führen die Vereinten Nationen hinsichtlich der Computerkriminalität folgende Beispiele an:

- Betrug
- Fälschung
- unerlaubter Zugriff auf Daten

Die Ermittlungen der Polizei wegen Cyberkriminalität werden nicht selten dadurch erschwert, dass sogenannte Hacker oftmals sozial unauffällig sind und nicht über lange Vorstrafenregister verfügen. In der Regel handelt es sich bei den Tätern um Schüler, Auszubildende oder Studenten – also keineswegs um IT-Experten -, die zurückgezogen leben und vornehmlich Kontakte auf informativer Basis pflegen, anstatt freundschaftliche Bindungen aufzubauen.

Grundsätzlich lassen sich zwei Reaktionsbereiche unterteilen, wenn es zu Straftaten kommt, die der Cyberkriminalität zuzuordnen sind. Zum einen sollten betroffene Personen ihre eigene Datensicherheit überprüfen, um so auch präventiv gegen Täter gewappnet zu sein.

Zum anderen sollte die Polizei bei erfahrener Internetkriminalität der erste Kontakt für Opfer sein. Diese verfügt unter Umständen über Expertengruppen oder Kompetenzzentren, die sich gezielt mit der Problematik der Cyberkriminalität auseinandersetzen.

List of references

1. Internetkriminalität / Cybercrime - https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html
2. Kriminalitätsstatistik: Cyberkriminalität nimmt in Deutschland zu - [http://de.ubergizmo.com/2017/04/24/kriminalitaetsstatistik-cyberkriminalitaet-nimmt-in-deutschland-zu-2.html
3. Cyberkriminalität – Gefangen im Netz von - Virenattackenhttp://www.anwalt.org/cyberkriminalitaet/
4. Kennzahlen zur Cyberkriminalität - https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/
5. http://www.spiegel.de/netzwelt/netzpolitik/cybercrime-bericht-2015-des-bka-40-millionen-schaden-in-deutschland-a-1104988.html