CYBERCRIME – HELLFELDANALYSE DER AKTEN DES WIENER STRAFLANDESGERICHTS VON 2006–2016

Edith Huber / Bettina Pospisil / Walter Hötzendorfer / Leopold Löschl / Gerald Quirchmayr / Christof Tschohl

Senior Researcher, Donau Universität Krems
Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
edith.huber@donau-uni.ac.at; http://www.donau-uni.ac.at

Junior Researcher, Donau Universität Krems, Zentrum für Infrastrukturelle Sicherheit
Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
bettina.pospisil@donau-uni.ac.at; http://www.donau-uni.ac.at

Senior Researcher, Research Institute AG Co KG
Annagasse 8/1/8, 1010 Wien, AT
walter.hoetzendorfer@researchinstitute.at; http://www.researchinstitute.at

Leitung C4, Bundesministerium für Inneres
Josef-Holaubek Platz 1, 1090 Wien, AT
Leopold.loeschl@bmi.gv.at; http://www.bmi.gv.at

Universitätsprofessor, Universität Wien, Fakultät für Informatik
Währinger Straße 29, 1090 Wien, AT
Gerald.Quirchmayr@univie.ac.at

Wissenschaftlicher Leiter, Research Institute AG Co KG
Annagasse 8/1/8, 1010 Wien, AT
christof.tschohl@researchinstitute.at; http://www.researchinstitute.at

Schlagworte: ***Cybercrime, Computerkriminalität, Hellfeldanalyse, Modus Operandi, Ermittlungswege, Strafen***

Abstract: *Seit 2006 werden in Österreich die Fälle von Computerkriminalität in der amtlichen Kriminalstatistik unter dem Sammelbegriff «Cybercrime» erfasst. Dies war Anlass zurückzublicken und die Fälle der letzten zehn Jahre (2006 – 2016) näher zu betrachten. Dazu wurde eine Aktenanalyse beim Wiener Straflandesgericht durchführt. In diesem Beitrag sollen Modus Operandi, Ermittlungswege und die daraus resultierenden Strafen erläutert werden.*

1. Einleitung

Kaum ein Tag vergeht, an dem die Medien nicht über Cybercrime-Delikte berichten. Aber wie sieht die Situation in Österreich dazu aus? Bereits 1988 wurde mit den Tatbeständen der Datenbeschädigung (§ 126a StGB) und des betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) im Kernstrafrecht gewissermaßen ein «Computerstrafrecht der ersten Generation» eingeführt.[1] Anstoß für die Einführung weiterer Cybercrime-Delikte in Österreich gab schließlich die «Convention on Cybercrime» des Europarates[2]. Als weitere internationale Vorgabe zu nennen ist der EU-Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme.[3] Seit 2006 werden Cybercrime-Delikte in der Kriminalstatistik unter diesem Begriff erfasst. Generell unterscheidet man (a) Cybercrime im engeren Sinn (Core Cybercrime bzw. Cyberdependent Crime): Unter diese

[1] Bergauer 2016.

[2] Convention on Cybercrime (ETS 185) vom 23. November 2001, in Kraft getreten am 1. Juli 2004.

[3] Rahmenbeschluss 2005 / 222 / JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69, 67.

Definition fallen alle Delikte, die es in keiner Variante offline gibt; diese Kategorie umfasst die Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von Netzwerken sowie von Geräten, Daten und Services in diesen Netzwerken. Dazu zählt Hacking, Cyber-Vandalismus, die Verbreitung von Viren etc.; (b) Cybercrime im erweiterten Sinn (Non-cyberspecific Cybercrime bzw. Cyberenabled Crime): Delikte, die unter diese Kategorie fallen, können auch offline existieren. Dazu zählen Delikte, wie z.B. Kreditkartenmissbrauch, Informationsdiebstahl, Geldwäsche, Vergehen gegen das Urheberrecht, Cyberstalking, Cybermobbing sowie die Nutzung, Verbreitung und Zurverfügungstellung kinderpornographischer Inhalte usw.;[4] (c) Verschleierung der Identität: Dies betrifft Täter, die sich einen Online-Avatar zulegen und die Anonymität dazu verwenden, kriminell zu handeln[5], bzw. Täter[6], die sich gestohlener Identitäten oder Fake-Identities bedienen.

Im Rahmen der hier durchgeführten Studie wurde der Frage nach dem tatsächlich bekannten Hellfeld in Wien nachgegangen.[7] Welche Besonderheiten und Facetten lassen sich erkennen? Gibt es Muster und Tendenzen? Dazu wurde auf die Akten des Wiener Straflandesgerichts der Jahre 2006–2016 zurückgegriffen. Im Rahmen dieses Beitrags sollen dabei folgende Forschungsfragen näher beleuchtet werden:[8]

(1) Welche Strategien der Anbahnung und Durchführung (Modus Operandi) von Cybercrime lassen sich identifizieren?

(2) Welche polizeilichen Ermittlungswege haben sich als hilfreich erwiesen und was lässt sich über die weitere Strafverfolgung der ermittelten Täter und Täterinnen aussagen?

(3) Welche Aussagen lassen sich zum durchschnittlichen Strafmaß und typischen Deliktskombinationen treffen?

2. Methodische Vorgehensweise

Zur Beantwortung der Forschungsfragen wurde eine Aktenanalyse der Cybercrime-Delikte der Jahre 2006–2016 am Wiener Straflandesgericht durchgeführt. Dazu wurden Cybercrime-Delikte im engeren Sinn sowie Cybercrime-Delikte im weiteren Sinn analysiert.[9] Delikte der Kinderpornographie (Pornographische Darstellung Minderjähriger) sowie der Anbahnung von Sexualkontakten zu Unmündigen fanden in dieser Auswertung keine Berücksichtigung. Ausgehend von dieser Grundbetrachtung lagen im Wiener Straflandesgericht im Untersuchungszeitraum rund 5'400 Akten der Staatsanwaltschaft und des Gerichts vor. Zur genauen Beantwortung der Forschungsfragen, welche unter anderem auch auf die Charakterisierung der Täter abzielten, wurde anschließend jene Gruppe an Akten herangezogen, bei denen es zu einer Gerichtsverhandlung kam. Dies waren N=399 Fallakten. Diese Zahlen sprechen für sich und lassen zu Beginn schon eine sehr geringe Aufklärungsquote erkennen. Aus den Akten wurde eine Zufallsstichprobe mittels Listenauswahl gezogen. Da es sich hier um eine Art der Wahrscheinlichkeitsauswahl handelt, kann von der Stichprobe auf die Grundgesamtheit geschlossen werden.[10] Aus den Fallakten wurde somit eine repräsentative Stichprobe von (n=89) gezogen. Bei

4 McGuire/Dowling 2013; Kirwan/Power 2013.

5 Kirwan/Power 2013.

6 An dieser Stelle sei festgehalten, dass für die allgemeine Bezeichnung von Personengruppen, zwecks besserer Lesbarkeit, die männliche Form genommen wird, z.B. also Täter (gemeint Täter und Täterinnen, Hacker und Hackerinnen).

7 Das Forschungsvorhaben wurde im Rahmen der österreichischen Sicherheitsforschung KIRAS, Programmlinie 2–3 gefördert. Projektname «CERT-Komm II».

8 Alle Forschungsergebnisse, wie Täterprofil, Opferprofil, Modus Operandi, erfolgreiche Analyse über die Ermittlungswege sowie eine Analyse über die verhängten Straften und angeklagten Paragraphen sind im E-Book: «Die Cyberkriminellen aus Wien», 2006–2016, Krems 2018, ausführlich nachzulesen.

9 Im Rahmen des vorliegenden Forschungsvorhabens wurden folgende Cybercrime-Delikte des StGB im engeren Sinn untersucht: §§ 118a (Widerrechtlicher Zugriff auf ein Computersystem), 119 (Verletzung des Telekommunikationsgeheimnisses), 119a (Missbräuchliches Abfangen von Daten), 126a (Datenbeschädigung), 126b (Störung der Funktionsfähigkeit eines Computersystems), 126c (Missbrauch von Computerprogrammen oder Zugangsdaten), 148a (Betrügerischer Datenverarbeitungsmissbrauch sowie 225a (Datenfälschung).

10 Diekmann 2009.

den verbleibenden 5'001 Akten wurde der Strafantrag gegen Täter «unbekannt» gestellt bzw. sind die Akten noch von der Staatsanwaltschaft in Bearbeitung. Als Forschungsmethode zur Analyse der Akten wurde eine quantitative Aktenanalyse nach Dölling[11] herangezogen. Zur Ermittlung des Modus Operandi wurde der Tathergang qualitativ mit der Inhaltsanalyse nach Mayring[12] ausgewertet. Dazu wurden Kategorien ermittelt, die einen Vergleich des Modus Operandi zulassen. Der Zeitraum, in dem die Aktenanalyse durchgeführt wurde, war von Jänner 2017 bis Juni 2017.

3. Ergebnisse[13]

3.1. Strategien der Anbahnung und Durchführung von Cybercrime – Modus Operandi

Die Differenzierung des Tathergangs stellt eine besondere Herausforderung dar, da es je nach Technologieentwicklung und Kreativität der Täter variierende Muster gibt. Im Vergleich zu klassischen Kriminalitätsdelikten ist die Beschreibung eines Modus Operandi relativ schwierig, da nicht das Delikt selbst, sondern eine Vielzahl von Faktoren und Variablen, dafür verantwortlich sind. Die behandelten Akten wurden nach folgenden Faktoren analysiert:

- Häufigkeit: n=
- Cybercrime-Art: Cybercrime im engeren Sinn, Cybercrime im erweiterten Sinn
- Täter: Merkmalsträger
- Opfer: Merkmalsträger
- Komplexität: leicht – mittel – schwierig
- Motiv: extrinsisch vs. intrinsisch
- Beziehungsstatus: zwischen Täter und Opfer
- Opferwahl: nicht gerichtet, zielgerichtet, skalpellartig[14]
- Methode: Merkmalsträger
- Anklage nach StGB: Paragraphen
- Technik: Merkmalsträger
- Fallbeispiel

Nach diesen Kriterien konnten elf verschiedene Typen unterschieden werden, von denen neun wissenschaftlich bewertet wurden. Methodisch wurde die Ausgestaltung des Modus Operandi mittels einer qualitativen Inhaltsanalyse der Gerichtsakten durchgeführt.

3.1.1. Typ 1: Technische Hilfsmittel

Diese Variante stellt das aufwändigste Muster dar und entspricht dem typischen Bild des Cyber-Kriminellen. Sie geht davon aus, dass die Täter einen hohen Wissensstand über die Funktionsweise von IT-Security haben und Programmierkenntnisse besitzen. Das kriminelle Potential ist sehr hoch und die Komplexität facettenreich. Die hier durchgeführte Aktenanalyse zeigt natürlich nur jene Fälle (n=7), die auch bei Gericht behandelt wurden. Die Anzahl der Anklagen ist relativ gering, da in diesen Fällen davon ausgegangen werden kann, dass die Täter sich gut tarnen können. Die Beziehung zwischen Tätern und Opfer, basiert zumeist auf einer

11 Dölling 1995.

12 Mayring 2000; Mayring 2010.

13 Vgl. dazu Huber/Pospisil 2018.

14 Dazu wurde die Kategorisierung nach Art des Angriffs dem deutschen BSI (Bundesamt für Sicherheit und Informationstechnik in Deutschland) (Michael Hange, B. Cyber-Sicherheit: Herausforderung in einer vernetzten Welt; Bonn, 2012.) als Grundlage verwendet. Bei ungerichteten Angriffen wählt der Täter seine Opfer nicht persönlich. Ziel ist möglichst viele Opfer zu erreichen. Gezielte Angriffe hingegen richten sich an ein bestimmtes Opfer. Es wird eine Methode des Angriffs gewählt, die das Opfer auf jeden Fall erreicht. Bei skalpellartigen Angriffen bedienen sich die Täter mehrerer Methoden, um das Opfer zu erreichen. Diese Angriffe sind komplex und werden strategisch lange vorbereitet.

institutionellen Ebene, wobei die Opfer Firmen oder Institutionen sind. Dennoch ist diese Aussage hier auch mit Vorbehalt und immer unter Berücksichtigung der verwendeten Forschungsmethode zu verstehen. Wie bereits zu Beginn des Beitrags beschrieben, wurden hier nur jene Gerichtsakten untersucht, bei denen es zu einer Anklageerhebung vor Gericht kam. Analysen von Kapersky-Lab[15] zeigen, dass es bei den meisten Cybercrime-Attacken dieser Art kein Verhältnis zwischen Tätern und Opfern gibt. Diese Delikte in Wien resultieren meist aus einer Kombination des extrinsischen Motivs einen möglichst hohen finanziellen Gewinn zu erzielen und intrinsischen Motiven, wie der mutwilligen Schädigung. Die Tat wird mit speziellen und komplexen Techniken durchgeführt. Verbrechen dieser Art erfordern eine erhebliche Planung und Präzision. Die Täter verwenden beispielsweise Verschlüsselungstechniken, versenden Schadsoftware. Es wurden unterschiedlichste Strategien und Methoden angewandt um das Opfer zu schädigen. So findet man durchaus häufiger Methoden des klassischen Hackings in Kombination mit Social Engineering.

3.1.2. Typ 2: Illegale Überweisungen

Illegale Überweisungen finden häufiger (n=9) statt, da der Aufwand dieses Verbrechen zu begehen, relativ niedrig ist. Die Täter finden sich in allen sozialen Schichten, Altersklassen und Geschlechtern. Die Planung ist meist banal und die Tat geschieht aus finanziellen Motiven heraus. Es erfordert keine speziellen Informatikkenntnisse um illegale Überweisungen durchzuführen. Der Täter verschafft sich online oder offline Zugang zu den Bankdaten und führt die illegale Überweisung durch. Solche Fälle entstehen nicht immer aus einer sorgfältigen Planung, sondern aus der Möglichkeit heraus. Unachtsamkeit der Opfer ist oft die Ursache solcher Verbrechen, da z.B. die Überweisungskenndaten offen auf dem Schreibtisch herum lagen. In den meisten Fällen besteht keine Beziehung zwischen Täter und Opfer. Typisch für diese Fälle ist, dass die Gelegenheit den Dieb macht. Die Unachtsamkeit der Opfer wird ausgenutzt.

3.1.3. Typ 3: Bankomatkarte/Kreditkarte (Betrug/Diebstahl)

Bankomat-/Kreditkartenbetrug und -diebstähle kommen in den untersuchten Akten am häufigsten (n=26) vor. Ähnlich wie bei Typ 2, den illegalen Überweisungen, handelt es sich hier um niederschwellige Kriminalität, bei der keine speziellen Kenntnisse im IT-Security- oder Informatiksektor notwendig sind. Diese Delikte passieren insofern offline, als die jeweilige Karte physisch gestohlen wird.[16] In diesen Fällen kann zwischen Opfer und Täter ein Bekanntschaftsverhältnis bestehen. Das Delikt wird verübt, wenn sich die Situation ergibt. Es gibt keine langen, komplexen Planungen. Häufig werden Bank- und Kreditkarte zur Finanzierung der Beschaffungskriminalität herangezogen. Besonderes Kennzeichen dieses Modus Operandi ist, dass in allen Fällen nach § 148a StGB angeklagt wurde. Die Einordnung als Cybercrimes ergibt sich dadurch, dass z.B. der Täter auf den Bankomaten zugreift. Damit ist die betrügerische Datenverarbeitung gegeben. Die Beschaffung der Bankdaten erfolgt in fast allen Fällen offline.

3.1.4. Typ 4: Glücksspiel

Eine spezielle Ausformung ist Cybercrime zum Zwecke der Finanzierung von Spielsucht (n=5). Besonders betroffen davon sind Männer (100%), die nach neuen Möglichkeiten suchen, ihre Sucht zu finanzieren. Im typischen Fall verhält es sich so, dass der Täter persönliche Daten von Opfern nutzt, um sich Zugang zu Glücksspielportalen zu verschaffen. Diese Daten können persönliche Daten, wie Telefonnummer, E-Mail, Adresse oder aber auch Bankdaten sein. Dieser Typ ähnelt sehr dem Typ 2 Bankomatkarte/Kreditkarte (Betrug/Diebstahl), eben mit der Besonderheit der Finanzierung der Spielsucht. Die Täter dieser Ausprägung haben wenig Schulbildung und sind sehr häufig arbeitslos. Die Tat erfordert keine speziellen IT-Security und/oder

[15] https://de.securelist.com/internetfahige-bohrmaschine-demonstriert-angemessenen-schutz-im-internet-der-dinge/72833/, Website zuletzt besucht am 24. Juli 2017.

[16] In den untersuchten Akten waren keine Fälle von Bankdaten-, Kreditkarten- oder Bankomatkartendiebstählen durch Malware bekannt. Zur Verurteilung in Wien kamen ausschließlich Fälle, bei denen die Karten offline gestohlen wurden.

Informatikkenntnisse. Daher kennzeichnet diese Fälle auch die Anklage im Sinne des Paragraphen 148a. Auch hier ergibt sich die Einordnung als Cybercrime dadurch, dass widerrechtlich auf ein Datenverarbeitungssystem, in diesem Fall das Spielportal, zugegriffen wird. Die Beschaffung der Bezahldaten erfolgt zumeist offline.

3.1.5. Typ 5: Identitätsdiebstahl – Online-Shopping

Ein weiterer Typ ist der Identitätsdiebstahl zum Zwecke des Online-Shoppings (n=15). Auch bei diesen Fällen kann man von niederschwelliger Kriminalität sprechen, wie bei Typ 3 und Typ 4. Angeklagt wurden die Tatverdächtigen ebenso nur unter dem Paragraphen 148a StGB. Der Unterschied zu den vorherigen Delikten liegt darin, dass die gestohlenen Daten online zum Einkaufen von Produkten und Dienstleistungen verwendet werden. Das Motiv ist häufig finanzieller Natur, Täter sind jedoch teilweise auch intrinsisch motiviert. Es gibt durchaus Fälle, in denen dieses Vorgehen bewusst eingesetzt wird, um sich an jemandem zu rächen. Typisches Fallbeispiel dazu ist, dass der Täter mit dem Opfer privat vertraut ist. Das Opfer hat die Bezahldaten im Browser abgespeichert. Der Täter ergreift die Möglichkeit, loggt sich mit dem Profil des Opfers ein und kauft ein. Bei diesem Tathergang findet man auch zahlreiche Frauen als Täterinnen. Ebenso, wie bei den anderen Delikten des Identitätsdiebstahls benötigt es hier keine speziellen Kenntnisse der IT, um dieses Verbrechen zu begehen. Opfer sind die Firmen, die betrogen wurden und die Privatpersonen selbst. Problematisch ist dabei die Tatsache, dass das Opfer der Firma, also dem Online-Shop, beweisen muss, dass es nicht persönlich eingekauft hat. Die Firmen hingegen möchten natürlich treue Kunden nicht verlieren und sind somit ebenso im Dilemma der eindeutigen Zuordnung der Bestellung und der erbrachten Leistung.

3.1.6. Typ 6: Datenmissbrauch bei Firmen

Eine der neuen und spannenden Ausprägungen von Cybercrime findet man in Typ 6 (n=10). Diese ist zum einen immens gefährlich für Unternehmen, und zum anderen schwer kriminologisch zu erfassen. Bei den Tätern handelt es sich um Personen, die bewusst ihr Wissen oder ihre Berechtigungen in einem Unternehmen missbrauchen, um sich dadurch einen Vorteil zu verschaffen bzw. um das Unternehmen bewusst zu schädigen. Diese Fälle sind komplexer in der Planung und erfordern eine Strategie. In den meisten Fällen liegt eine intrinsisch motivierte Tathandlung vor. Der Täter fühlt sich durch das Unternehmen schlecht behandelt, ausgenutzt und verspürt den Drang sich zur rächen bzw. die gewonnenen Informationen zum eigenen Vorteil einzusetzen. Dennoch bedeutet dies nicht, dass es sich bei den Tätern in diesen Fällen um Informatik-Profis handelt. Vielmehr kommen Personen als Täter in Frage, die sehr gute Anwenderkenntnisse im IT-Bereich bzw. in dem von ihnen betreuten Bereich besitzen. Die Täter nutzen Insider-Wissen und verschaffen sich dadurch einen Vorteil. Interessant bei den Tätertypen dieses Profils ist, dass es sich ausschließlich um Männer handelt, die eine höhere Schulbildung zum Teil Universitätsabschluss besitzen. Sie nutzen zum einen ihr eigenes Wissen über die IT-Systeme oder verschaffen sich Zugang zu Informationen durch Social Engineering. Betrachtet man die angeklagten Paragraphen nach dem StGB, so erkennt man schnell, dass hier fast das gesamte Spektrum an Cybercrime-Anklagemöglichkeiten (nämlich §§ 118a, 119, 119a, 123, 126a, 126b, 126c, 124) zu finden ist. Das typische Muster ist, dass der Täter Daten des Unternehmens an die Konkurrenz oder andere weitergibt.

3.1.7. Typ 7: Schwachstellenausnutzung

Das Charakteristische bei Typ 7 (n=4), dem Schwachstellenausnutzer, ist, dass er bei einer Firma eine IT-Schwachstelle oder eine allgemeine Schwachstelle erkennt und auch ausnutzt. Um solche Taten zu begehen, muss man soweit IT-Security-Kenntnisse besitzen, dass man die Schwachstelle erkennt und auch weiß, wie man sie zum eigenen Vorteil nutzt. Oftmals eignen sich die Täter ihr Wissen mittels der Trial-and-Error-Methode an, d.h. sie probieren etwas aus, erkennen dann die Schwachstelle und nutzten diese aus. Die ausgenutzten Schwachstellen liegen auch nicht immer zwangsläufig in IT-Netzwerken; so werden auch Schwachstellen ausgenutzt, die zwar eine Anbindung an das Internet haben, aber primär eine andere Funktion. Ein Beispiel dafür ist das illegale Umleiten einer Telefonanalage. Der Täter leitet die Telefonanlage auf eine ausländische Mehrwertnummer um. Nichtsdestotrotz sind diese Verbrechen leicht bis mittel komplex. Die Technik, die dafür

verwendet werden kann, gibt es offline und online. Eindeutige Muster in der Technik kann man nicht erkennen. Die Taten werden sowohl von Männern als auch von Frauen begangen.

3.1.8. Typ 8: Fälschung

Eines der ältesten Verbrechen der Welt: die Fälschung (n=4). Mit den Methoden der Bildverarbeitung hat dies nun auch Einzug in die Computerkriminalität gefunden. Fälschungsdelikte sind mittel bis höher komplex, da man seine eigene oder die Identität eines anderen verändern muss. Dies erfordert Planung und strategisches Denken sowie gute Kenntnisse in Bildverarbeitung. Ein typisches Beispiel dafür ist das Fälschen von Dokumenten, um sich bei einer Stelle einen Vorteil zu verschaffen, z.B. bei Banken oder durch Fälschen von Bewerbungsunterlagen.

3.1.9. Typ 9: Rache

Dieser Typ (n=4) stellt eine Besonderheit dar, da er sich zum Teil aus den anderen Typen zusammensetzt. Wesentliches Unterscheidungsmerkmal ist die bewusste Planung der Tat als Racheakt. Opfer sind immer Privatpersonen, die mittels Identitätsdiebstahl, Kreditkarten-/Bankdatenbetrug oder anderen Formen geschädigt werden sollen. Interessant dabei ist, dass die Täter oftmals strategisch aus den Motiven der Rache die systematische Vernichtung des Opfers planen. Dazu sind ihnen mehrere Mittel recht. Täter können in diesen Fällen sowohl Frauen als auch Männer sein. Man kann dies auch als eine Ausweitung des Cyberstalkings betrachten. Besonders interessant sind dahingehend die neuesten Entwicklungen angesichts des § 107c StGB, der vermutlich künftig in solchen Fällen häufiger zur Anwendung kommt.[17]

3.2. Polizeiliche Ermittlungswege und weitere Strafverfolgung

Zur Überführung der Täter wurde eine Vielzahl von Ermittlungsmethoden angewandt. Da im Rahmen dieser Studie nur jene Akten analysiert wurden, welche zu einer Hauptverhandlung und somit meist einer Strafe führten, lässt die Erhebung der Ermittlungswege einige Schlüsse in diesem Zusammenhang zu. Die Analyse der Akten der letzten zehn Jahre zeigt, welche Ermittlungsarten nun zu einer Anklage der Täter führten. In einem weiteren Schritt wurde analysiert, welche Ermittlungsmetoden darüber hinaus tatsächlich in einem signifikanten Zusammenhang mit einer möglichen Verurteilung der Täter stehen. Dabei wurden folgende Ermittlungswege untersucht:

- Erkennungsdienstliche Behandlung: § 65 SPG
- DNA-Identitätsfeststellung: §67 SPG, §124 StPO, § 117 Z 5 StPO
- Beschlagnahme: § 115 StPO, § 109 Z 2 StPO
- Durchsuchung von Personen: § 119 Abs 2 StPO, § 117 Z 3 StPO
- Polizeiliche Beobachtung (Observation): § 130 StPO, § 129 Z 1 StPO
- Techn. Mittel: § 136 StPO, § 141 StPO, § 134 Z 4 StPO
- Überwachung der Telekommunikation: § 135 Abs 3 StPO, § 134 Z 3 StPO
- Verdeckter Ermittler: § 131 StPO, § 129 Z 2 StPO
- Auskunft zu IP-Adressen: § 53 Abs 3a SPG, § 76a StPO, § 135 Abs 2 StPO, § 134 Z 2 StPO
- Keine

3.2.1. Eingesetzte Ermittlungswege

Die Ergebnisse zeigen, dass in vielen Fällen keine spezielle Ermittlungsmethode zum Einsatz kam. Stattdessen stellten sich in diesen Fällen oft ohnehin vorgeschriebene Einvernahmen durch Staatsanwaltschaft und Polizei als zielführend heraus. Dies hat auch mit dem hohen Anteil an Geständnissen zu tun. Im Folgenden werden

[17] § 107c StGB «Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems» gibt es seit Ende 2015. Im Jahr 2016 wurden 302 Fälle zur Anzeige gebracht (Bundesministerium für Inneres Kriminalstatistik 2016; Wien, 2017).

wir jene Fälle genauer betrachten, in welchen es zum Einsatz weiterführender Ermittlungsmethoden kam, da die einfache Vernehmung nicht ausreichend war um eine Hauptverhandlung einzuleiten.

Am häufigsten kommt die Methode die Beschlagnahme (19%), die Auskunft über Bankkonten und Bankgeschäfte (17%) sowie die Durchsuchung von Personen (9%) zum Einsatz. Beschlagnahmt wurden dabei vorwiegend Schriftstücke (15%) und Datenträger (12%). Weniger häufig kamen die neueren Methoden Überwachung der Telekommunikation (8%) sowie Auskunft zu IP-Adressen (7%) zum Einsatz. Dies könnte einerseits dadurch erklärt werden, dass ein Großteil der Verurteilungen im Bereich des Identitätsdiebstahls stattfinden (siehe Kapitel 3.1.). Diese zeichnen sich zumeist durch eine geringe Komplexität aus, sodass aufwändigere Ermittlungsmethoden, wie, z.B. die Auskunft zu IP-Adressen, nicht zum Einsatz kommen. Wie die oben angeführte Analyse zeigt, werden zu mehr als 50% Identitätsdiebstähle durchgeführt, wobei der Diebstahl meist offline erfolgt. Der eigentliche Cybercrime-Vorfall findet erst durch das illegale Zugreifen auf ein IT-System statt, also beispielsweise, dass mit der Bankomatkarte das Geld abgehoben wird. Fraglich bleibt, ob es eine Abhängigkeit zwischen der gewählten Ermittlungsmethode und der Aufklärungsquote gibt. So könnte entweder (1) der fehlende Einsatz der neuen Ermittlungsmethoden dazu führen, dass eher Betrugs- und Identitätsdiebstahlsdelikte aufgeklärt werden, anstatt technisch komplexerer Delikte. Oder (2) durch das häufigere Auftreten von eben solchen Delikten mit geringerer technischer Komplexität, ist der Einsatz der neuen technischen Ermittlungsmethoden nicht in größerem Maße notwendig. Dies ist eine Frage, welche sich nur mit Blick auf die ungeklärten Fälle (N=5001) beantworten lassen würde. Eine weitere Ermittlungsmethode ist die Durchsuchung von Räumen. Diese wurde in nur insgesamt 31 Fällen durchgeführt. Dabei wurden meist eine private Wohnung (20%) oder Geschäftsräume (4%) durchsucht. Dieses Ergebnis ist auf die Tatsache zurückzuführen, dass viele Täter ohne Beschäftigung sind. Der Tatort ist daher die private Wohnung der Täter. Darüber hinaus kommt noch die Ermittlungsmethode der Datenauswertung zum Einsatz. Darunter versteht man die Auswertung von digitalen Daten, die im Laufe der Ermittlungen gewonnen wurden. Am häufigsten ausgewertet wurden Fotos/Videos (23%), Nachrichten (12%) sowie Anruferlisten (11%). Sehr viel seltener wurden digitale Tatmittel (4%), Logfiles (4%) und digitale Beute (2%) ausgewertet. Auch hier findet sich somit das bereits bei den Ermittlungsmethoden angesprochene Phänomen, welches einen wie auch immer gearteten Zusammenhang vermuten lässt.

Eine weitere spannende Betrachtung ist die Zuordnung des Modus Operandi nach den angeklagten Delikten. Wie Tabelle 1 zu entnehmen ist, werden bis auf Typ 6: Datenmissbrauch bei Firmen, alle anderen Delikte auch dem § 148a angeklagt. Hier gilt es zu hinterfragen, ob das gesamte Spektrum der Anklagemöglichkeiten immer ausgenutzt wird.

Delikt	Typ 1	Typ 2	Typ 3	Typ 4	Typ 5	Typ 6	Typ 7	Typ 8	Typ 9
§ 118a						x			
§ 119						x			
§ 119a						x			
§ 123						x			
§ 124						x			
§ 126a	x					x			x
§ 126b						x			
§ 126c	x	x				x		x	
§ 148a	x	x	x	x	X		x	x	x

Tabelle 1: Modus Operandi und angeklagte Paragraphen der Computerkriminalität Fallakten (n=) 89, Verdächtige (n=) 118, Akten des Wr. Straflandesgerichts, 2006–2016

3.2.2. Zusammenhang zwischen Ermittlungsmethoden und Verurteilung

Um näher zu betrachten, unter welchen Voraussetzungen es in den untersuchten Fällen zu einer Verurteilung kommt, wurden außerdem Korrelations- und PRE-Maße errechnet. Im Rahmen dieser Analyse wurde die nominale Variable «Verurteilung», die beschreibt ob es in einem Fall zu einer Verurteilung kam oder nicht, mit den Ermittlungsmethoden in Beziehung gesetzt.

Die Ergebnisse zeigen, dass ein signifikanter (0,001) mittelmäßig starker Zusammenhang (Kontingenzkoeffizient = 0,311) zwischen den Variablen «Verurteilung» und «Ermittlung» besteht. Dies bedeutet, dass eine Verurteilung eindeutig mit den gesetzten Ermittlungen korreliert. Auch die konkretere Variable «Beschlagnahme» steht einem signifikant (0,007) positiven Zusammenhang (Kontingenzkoeffizient=0,264) mit einer Verurteilung.

In einem nächsten Schritt wurde der Frage nachgegangen, unter welchen Voraussetzungen sich die Wahrscheinlichkeit, dass es zu einer Verurteilung kommt, erhöht. Dazu wurde eine logistische Regression errechnet (Modellgüte = 85,6%). Diese zeigt an, wie stark eine Variable X durch andere Variablen A, B, C erklärt werden kann. Ob es nun zu einer Verurteilung kommt oder nicht, wird durch die gesetzten Ermittlungen, die Beschlagnahmen, die Durchsuchungen und Datenauswertungen bereits zu 21,2% (Nagelkerke R-Quadrat Wert) erklärt. Im Speziellen stechen allgemeine Ermittlungsmethoden hervor. Diese umfassen die am Anfang von Kapitel 2.2 genannten Methoden. Wird eine dieser Ermittlungsmethoden eingesetzt, erhöht sich die Wahrscheinlichkeit, dass eine Verurteilung ausgesprochen wird um das Sechsfache. Die Fehlerwahrscheinlichkeit bei Annahme dieser Kausalität liegt bei lediglich 1,7%, der Zusammenhang ist somit signifikant.

Dieses Ergebnis bedeutet nun aber nicht automatisch, dass in jedem Fall durch den Einsatz genannter Ermittlungsmethoden die Wahrscheinlichkeit erhöht wird, dass es zu einer Verurteilung kommt. Vielmehr ist anzunehmen, dass sich diese auffindbare Korrelation durch eine vermittelnde Variable erklärt. Diese wird jene des konkreten Falls sein. So gibt es Fälle bzw. Delikte bei welchen es sinnvoll und möglich ist, die genannten Ermittlungsmethoden einzusetzen, welche mit hoher Wahrscheinlichkeit zu einer Verurteilung führen. Andere Fälle bzw. Delikte hingegen können mit diesen Methoden nicht hinreichend untersucht werden, was deren schlechtere Aufklärungs- bzw. Verurteilungsquote erklären könnte.

Um diese Annahme bestätigen oder verwerfen zu können und somit aussagekräftige Einsichten in dieses Thema zu erhalten, wäre es notwendig die Aktenanalyse auf solche Akten zu erweitern, in welchen es zu keiner Verurteilung kam.

3.3. Deliktkombinationen und Strafausmaß

3.3.1. Modus Operandi nach angeklagten Paragraphen

Man kann eindeutig festhalten, dass § 148a StGB, Betrügerischer Datenverarbeitungsmissbrauch, am häufigsten dazu herangezogen wird, um Cybercrime-Delikte zur Anklage zu bringen. Die in Kapitel 3.1. dargestellten Varianten des Modus Operandi zeigen ein einheitliches Bild. In fast allen Tathergangstypen, außer Typ 6, Datenmissbrauch bei Firmen, wurde § 148a angeklagt. Dies untermauert auch die hier durchgeführte Analyse, bei der in 81% der Fälle der § 148a auch angeklagt wurde. Dies untermauert wiederum die Erkenntnis, dass der Modus Operandi nicht nach den unterschiedlichen Deliktarten zu differenzieren ist. Dennoch lässt sich eine Gemeinsamkeit erkennen: Betrachtet man ausschließlich die Tathergangstypen des Identitätsdiebstahls (Illegale Überweisungen, Diebstahl der Bank-/Kreditkarte, Identitätsdiebstahl zum Zwecke des Glücksspiels und Identitätsdiebstahl zum Zwecke des Online-Shoppings), so kann man sagen, dass hier ausschließlich der § 148a zur Anwendung kam.

3.3.2. Typische Kombinationen in der Anklage

Des Weiteren wurde der Frage nachgegangen, welche typischen Anklagekombinationen es gab. Dabei konnten folgende Varianten erkannt werden:

Variante 1 «Auskundschaften von Betriebsgeheimnissen»: Zugriff auf ein Computersystem, Verletzung und Auskundschaftung von Betriebsgeheimnissen (für das Ausland), Datenbeschädigung. Angeklagt wurden dabei folgende Paragraphen des StGB: 118a, 122, 123, 124 und 126a.

Variante 2 «Auskundschaften von Amtsgeheimnissen»: Verletzung des Telekommunikationsgeheimnisses, Abfangen von Daten, Störung eines Computersystems, Missbrauch der Amtsgewalt und des Amtsgeheimnisses. Angeklagt wurden dabei folgende Paragraphen des StGB: 119, 119a, 126b, 302 und 310.

Variante 3 «Betrug und Datenbeschädigung»: Datenbeschädigung, Missbrauch von Computerprogrammen oder Zugangsdaten, betrügerischer Datenverarbeitungsmissbrauch und schwerer Betrug. Angeklagt wurden dabei folgende Paragraphen des StGB: 126a, 126c, 148a, 146 und 147.

Variante 4 «Betrug in Bezug auf den Zahlungsverkehr»: Betrügerischer Datenverarbeitungsmissbrauch, schwerer Betrug, gewerbsmäßiger Betrug, Entfremdung unbarer Zahlungsmittel. Angeklagt wurden dabei folgende Paragraphen des StGB: 148a, 146, 147, 148 und 241e.

Variante 5 «Organisierter Betrug»: Betrügerischer Datenverarbeitungsmissbrauch, schwerer Diebstahl durch Einbruch oder mit Waffe bzw. gewerbsmäßig oder im Rahmen einer kriminellen Vereinigung sowie Entfremdung unbarer Zahlungsmittel. Angeklagt wurden dabei folgende Paragraphen des StGB: 148a, 127, 128, 129, 130 und 241e.

3.3.3. Verhandlungen und Urteile

Die meisten der hier untersuchten Fälle haben eine Verfahrensdauer von bis zu einem halben Jahr (36%). Zumeist gibt es Zeugen (73%), jedoch wird die Tat größtenteils vom Opfer selbst aufgedeckt (77%). Sowohl bei der polizeilichen (25%), wie auch bei der staatsanwaltschaftlichen Vernehmung (40%) kommt es in den meisten Fällen zu einem Geständnis. Rund die Hälfte der Befragten hat einen Pflichtverteidiger, nur 8,5% leisten sich einen Wahlverteidiger und mehr als ein Viertel verzichtet darauf, sich anwaltlich vertreten zu lassen. Es werden äußerst selten Rechtsmittel wie Berufung und Revision eingelegt (9%) und noch deutlich seltener hat ein Rechtsmittel Erfolg (2%). In 68% der Fälle kommt es zu einer Verurteilung. Der Großteil der Täter erhält eine bedingte Freiheitsstrafe von bis zu 8 Monaten und eine Probezeit von 3 Jahren. Auch unbedingte Freiheitsstrafen, Zusatzfreiheitsstrafen und Therapieverordnungen finden sich in den Fällen.

4. Schlussfolgerungen

Der Blick auf die Cybercrime-Fälle von 2006–2016 ist ernüchternd. Die Aufklärungsquote ist gering. Im Vergleich zu anderen Kriminalitätsdelikten kann man keinen eindeutigen Zusammenhang zwischen dem Modus Operandi und angeklagten Paragraphen feststellen. Am häufigsten kommt es zu Verurteilungen bei Delikten des Identitätsdiebstahls, wobei man hier sagen muss, dass ein Großteil des Delikts offline erfolgt. Man kann daher die Entwicklung erkennen, dass immer mehr Diebstahlsdelikte eine Online-Komponente aufweisen und immer mehr Delikte der Kleinkriminalität im Internet erfolgen. Delikte des High-Tech-Crime, also jene Cybercrime-Attacken (beispielsweise das Versenden von Malware oder Hacking), die spezielle Informatikkenntnisse erfordern, werden nur in geringer Zahl aufgeklärt. Grund dafür ist, dass eine Vielzahl von Angriffen nicht rückverfolgt werden kann, insbesondere da sich die Täter im Ausland befinden. Obwohl eine Korrelation zwischen den eingesetzten Ermittlungsmethoden und der Verurteilung von Tätern festgestellt werden kann, bleibt fraglich, wie mit jenen Fällen umgegangen werden soll, bei welchen diese genannten und erfolgreichen Ermittlungsmethoden nicht eingesetzt werden oder werden können. Hierzu bedürfte es einer umfassenderen Untersuchung, in der insbesondere auch jene Fälle betrachtet werden, in denen es zu keiner Verurteilung kam.

5. Literatur

Bergauer, C., Das materielle Computerstrafrecht, Jan Sramek Verlag, Wien 2016.

Bundesministerium für Inneres, Kriminalstatistik 2016; Wien, 2017.

Diekmann, A. Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen. Reinbek: Rowohlt, 2009.

Dölling, D., Probleme der Aktenanalyse in der Kriminologie. In Die Täter-Individualprognose (S. 129–141). Heidelberg, 1995.

Hange, B. Michael, Cyber-Sicherheit: Herausforderung in einer vernetzten Welt; Bonn, 2012.

Huber, E./Pospisil B. (Hrsg.), Die Cyberkriminellen von Wien – eine Analyse von 2006–2016, Krems an der Donau, 2018.

Kirwan, G./Power, A., Cybercrime; Cambridge University Press, 2013.

Mayring, P., Qualitative Content Analysis. Forum Qualitative Social Research, S. 1–10., 2000.

Mayring, P., Qualitative Inhaltsanalyse. In: Handbuch Qualitative Forschung in der Psychologie (S. 601–613), 2010.

McGuire, M./Dowling, S., Cyber crime: A review of the evidence. 2013.